Event-triggered attack detection and identification in power-electronics-based DC microgrid

This paper was downloaded from TechRxiv (<https://www.techrxiv.org>).

LICENSE

CC BY-NC-SA 4.0

SUBMISSION DATE / POSTED DATE

04-12-2020 / 15-01-2021

CITATION

Gong, Sicheng (2020): Event-triggered attack detection and identification in power-electronics-based DC microgrid. TechRxiv. Preprint. <https://doi.org/10.36227/techrxiv.13335653.v2>

DOI

[10.36227/techrxiv.13335653.v2](https://doi.org/10.36227/techrxiv.13335653.v2)

Event-triggered attack detection and identification in power-electronics-based DC microgrid

Sicheng Gong, *Student Member, IEEE*

Abstract—This paper proposes a novel event-triggered attack detection mechanism for converter-based DC microgrid system. Under a distributive network framework, each node collects its neighbours' relative data to regulate its own output for local stabilization. Without power line current data, hardly can an agent directly identify the source of unexpected power flow, especially under an organized attack composed of voltage variations and corresponding deceptive messages. In order to recognize traitors who broadcast wrong data, target at system distortion and even splitting, an efficient attack detection and identification strategy is mandatory. After the attack detector is triggered, each relative agent refuses to trust any received data directly before authentication. Through proposed two-step verification by comparing theoretical estimated signals with received ones, both self sensors and neighbour nodes would be inspected, and the attacker was difficult to hide himself. Through simulation on SIMULINK/PLECS and hardware experiments on dSpace Platform, the effectiveness of proposed detection algorithm has been proved.

Index Terms—Event-triggered mechanism, attack detection, DC/DC converter, transient wave analysis.

I. INTRODUCTION

DUE to stochastic nature of renewable energy generation(REG), DC interconnection is advantageous for REG-integrated power system and EV charging infrastructure as its looser grid code and saved rectifiers, which merely pays attention to voltage magnitude and owns higher tolerance for system oscillations[1]–[3]. Moreover, integration facility and low conversion loss highlights the necessity of DC system deployment, especially in offshore or railway application scenarios[4], [5]. DC microgrid can be a economical and reliable scheme for REG-integrated power system, and its rapid emergence proves its priority to conventional AC grids[6]–[8]. Nonetheless, without external power regulation or internal topology reconfiguration, the global stability of DC microgrid can still be fragile and easily influenced by power imbalance under a limited self regulation capacity.

In order to improve DC microgrid reliability, there exists a common solution of redundant battery energy storage(BES) embedment for power regulation, which plays an alternative role of external regulator[9]–[11]. However, BES is commonly expensive and only intended for periodic or random power variation[12]. It is impossible to regulate long-term constant power variations considering its finite capacity. Precisely,

under deliberate biased node voltage or accidental node fault, power imbalance in DC microgrid will exist for a long time until relative nodes are classified and removed actively. BES cannot support for a long time under such attack or fault, so rapid attack or fault detection is expected. Relay protection technology is industrially mature and easy to employ, while anti-attack is more difficult due to possible data incredibility. The situation becomes more severe in distributive network considering a lack of central controller and instant measurement data sharing. A distributed attack identification strategy should be designed, providing a credible reference for next's'te, will ensure each node's personal and global stability in final.

A brief survey on attack detection for cyber-physical systems has been conducted in [13], including central controller and distributive controller scenarios in general cyber-physical systems. Regarding distributive power system, a model-based physical attack detection strategy for generation control has been proposed in [14], and intrusion detection in distributed frequency control for microgrid was investigated in [15]. Besides, several model-free methods were discussed to detect false data injection attack in power grid as well, for instance sparse optimization, wavelet transform and deep neural networks[16], [17]. All detection methods above are intended for AC grid. Specific physical properties of DC microgrid should be taken into consideration additionally.

For an emerging converter-dominated DC microgrid, signal temporal logic formalism can be employed to detect attacks and evaluate relative impacts on system stability[18], while it cannot help identify the attack source. In [19], a stealth cyber-attack detection strategy using cooperative vulnerability factors was proposed, while based on a hypothesis that neighbours' output current signals are accessible and trustworthy. A distributed cyber-attack detection scheme using a Luenberger observer has been investigated in [20], while it still relies on two trustworthy nodes. All strategies above cannot realize attack source identification merely depending on self data utilization. The motivation of the present work in this paper is to address this challenge.

Event-triggered mechanism can save computation and communication resource in a dynamical system, while still ensuring stable system performance[21]. Accordingly, this paper proposes a novel event-triggered attack detection and identification strategy, utilizing a nonlinear relationship between switching duty ratio and converter performance, in order for rapid and accurate attack detection in most scenarios only relying on self data. Through transient wave analysis during two-step examinations, no malicious node can hide himself

M.Gong was with the Department of Electrical Engineering, Technical University of Denmark, Lyngby, 2800, Denmark. E-mail: s190027@student.dtu.dk.

This work has been submitted to the IEEE for possible publication. Copyright may be transferred without notice, after which this version may no longer be accessible.

Fig. 1: Simple DC grid case utilizing Buck-Boost converters

and a reconfigured network topology will remove those attack and ensure global stability eventually.

The rest of this paper is organized as follows. Section II represents general structure of DC microgrid, including several hypothesis for future analysis simplification. The detailed categorization of DC microgrid attack has been illustrated in Section III. Then DC microgrid characteristics are analyzed in Section IV, which provides theoretical foundation for attack detection mechanism discussed in Section V. Simulation and hardware verification are implemented in Section VI and a conclusion is provided in Section VII.

II. SYSTEM DESCRIPTION AND MODELING

The configuration of investigated system including subsystem modules and DC transmission lines is shown in Fig. 1(a), where parallel diodes are not shown limited by figure size while widespread employed in most industrial scenarios. Periodic communication between each other is mandatory to reach a power balancing consensus. There are several assumptions employed during strategy investigation, which finally ensure proposed methods' effectiveness.

A. Subsystem module

The subsystem module, as an independent agent, plays a key role in microgrid, who exchanges electrical power with other agents and gives priority to internal stability guarantee. For modelling simplification, the subsystem is assumed composed of an ideal stable voltage source and a bidirectional Buck-Boost converter interface. The converter duty ratio determines node output voltage, finally influencing its neighbours' states through relative transmission lines. In this paper, the MOSFET and diode are assumed ideal for modeling simplification.

The converter topology can be flexible, while a conventional unidirectional Buck converter is not recommended. As illustrated in Fig. 2, when external injection current I_e is raising, the equivalent current I_i flowing in inductor L will be decreased. I_i keeps positive in normal scenarios, while possibly negative in extreme scenarios shown in Fig. 3. If I_e is large enough to push capacitor voltage higher than input voltage V_{dc} transiently, there would exist inverse current flowing in L , eventually leading to continuous current injection even the switcher turns off.

Fig. 2: Schematic of unidirectional Buck converter

Fig. 3: Current profile of inductor in Buck converter

Correspondingly, Boost and Buck-Boost converter are robust against potential shooting injection current. As switching signals are generated by each agent's own controller and only based on its local and received data. Under a stable power sharing consensus, the duty ratio should be constant and it can only change when receiving other nodes' personal requests or reaching another consensus.

B. Sensors

A complete agent in DC microgrid is composed of a subsystem module and inner sensors. The sensor is integrated into converters for status monitoring. Industrially, its sampling frequency is commonly equal or similar to switching frequency, which means there is no possibility of quick duty ratio derivation only depending on sensing data. If the duty ratio changes, no other agent or attacker is unable to find duty ratio in several switching periods, unless being informed directly by converter controller. Such prerequisite is fundamental to ensure the validity of proposed attack detection strategy.

A trustworthy inner inductor current sensor in converter is mandatory, and subsystem output power measurement can be an alternative. In accordance with converter topology, these two values can be estimated from each other, and (1) elaborates the calculation in a Buck-Boost converter case. The converter output current can be another alternative likewise. With all internal sensors betrayed simultaneously, the converter controller is assumed blind and even instigated, as there is no trustworthy reference for the magnitude of transformed electrical power.

$$I_L = \frac{P_s}{D \cdot U_{in}} \quad (1)$$

where P_s denotes measured inner output power and I_L denotes estimated inductor current. D is duty ratio of switcher near to inner source. U_{in} is inner voltage level, estimated by converter output voltage signals.

If inner voltage level was measured and trustworthy as well, there would be no need for converter output voltage sensor examination. That explains why only estimated value of U_{in} is utilized in this paper. The distribution line current sensor is designed discredited in our investigated cases likewise.

Fig. 4: DC microgrid attack categories

Actually, with detailed transmission line current data, neighbourhood attackers have no way to hide himself. The attack is only effective only when line current data is inaccessible for attacked nodes.

The trust level and availability of all sensors during attack detection are summarized in Tab I. Three colors indicates three potential while incompatible scenarios. A low trust level denotes relative signals should be authenticated before employment, while signals with high trust level is assumed reliable in any scenarios.

TABLE I: Table of sensor during attack detection

Measurement	Trust level	Availability
Converter inner voltage	Low	No/Yes/Yes
Converter output voltage	Low	Yes/No/Yes
Converter inductor current		
/ Subsystem output power	High	Yes
/ Converter output current		
Neighbour output voltage	Low	Yes
Transmission line current	-	No

C. DC distribution line and network topology

The DC distribution line is assumed equivalent to a lumped resistor and in parallel with ground capacitors on its terminals. For modelling simplification, the terminal ground capacitance can be merged into node output capacitance. Moreover, considering oscillation nature of converter output, a cascade inductor can be added in series with the resistor to ensure high-frequency model accuracy.

The network topology is essential to each node for its own parameter tuning in attack detection strategy. There is no restriction on DC microgrid topology, meaning that each node is able to disconnect or reconnect with other nearby nodes actively, while topology reconfiguration should always notify all nodes every time. The network parameters are assumed trustworthy and accessible for all participants, including topology, relative line impedance and admittance.

III. OPERATION PRINCIPLE OF DC MICROGRID ATTACK

The main target of grid attack is to cause a divergence between signal and reality, resulting in massive power imbalance in grid and finally dragging grid to another stable point or triggering relay protection directly. Grid attack can be categorized into three patterns, as shown in Fig. 4, including signal shielding, signal substitution and agent instigation.

The jammed or substituted signals should be dropped actively for receivers, and a robust local controller should be integrated to ensure inner stability. Regarding an instigated

agent, all innocent neighbour nodes should ignore its commands and isolate it until external intervention. Meanwhile, when Sybil attack is detected, an innocent agent is expected to disconnect with all external DC links initiatively for self protection.

A. Signal shielding

Sensor destruction, cyber-link destruction and cyber-link jamming are typical attacking methods to shield signals. Without measurement data and communication, the agent is highly potential to lose physical synchronization with its neighbours under unexpected oscillations. In communication protocol vulnerability analysis, the jamming attack is frequently discussed, for instance denial of service (DoS) and selective packet delay[22]. Since cyber-link jamming may occur as well in normal scenarios, the jamming attack would not trigger external intervene quickly.

However, direct equipment damage can lead to an opposite situation, which means less space for further attack action. Considering physical destruction is also expensive and risky for attackers, cyber-link jamming can be a suitable choice for signal shielding attack. Mere jamming attack is difficult to influence local stability, hence it is commonly combined with other attack options and comes efficient and powerful.

B. Signal substitution

Both sensor instigation and message substitution are intended for signal substitution attack, and the latter one includes package manipulation and repetition, which are expensive to implement due to message authorization mechanism. Meanwhile, combining with signal shielding, only a few cyber-links and sensors need to be focused considering the system has no choice but to rely on these links or sensors for communication and measurement. The ratio of attack efficacy to attack expenses can be increased a lot through such combination.

C. Agent instigation

Byzantine attack and Sybil attack are distinguished from the magnitude of instigated agents[23], [24]. Instead of instigating several nodes in Byzantine attack, Sybil attack indicates a high penetration ratio of traitors. These instigated agents will generate and distribute fake information, which means mismatching between its physical behavior and declaration, aiming to tract system to another state or system splitting.

An instigated node commonly claimed a false voltage level, and its neighbour nodes would decrease their output voltage accordingly. Afterwards, with its actual high voltage, excessive power will flow into those neighbour nodes, finally destabilizing those inner subsystems and forcing them kicked out of global grid. Such attack methods can also work together with signal shielding, imposing severer impacts on network.

IV. CHARACTERISTIC OF CONVERTER-BASED DC MICROGRID

Attack detection are difficult for an islanded DC/DC converter, as linearly scaled measurement signals are immune

Fig. 5: Current profile of inductor in Boost converter

to duty ratio variations, hence switching controller can be completely manipulated through deceptive voltage signals. Meanwhile, in a converter-based DC network, due to nonlinear properties imported from other converters, malicious signals are hard to mask themselves only through linearization strategy. In advance of detection strategy discussion, it is essential to figure out network characteristics with determined passive component parameters, eventually quantifying their influences on converter performances.

A. Discontinuous current mode(DCM)

For unidirectional DC/DC converters including conventional nonisolated Boost converter and Buck-Boost converter, discontinuous current flowing over inductor is possible, especially when there exists a large voltage gap between two converters. Regarding a boost converter, as illustrated in Fig. 5, its expected stable output voltage can be derived using voltage-second balancing equation in continuous current mode(CCM) as

$$U_{in}(DT) - (U_o - U_{in})((1-D)T) = 0 \quad (2)$$

$$U_o = \frac{U_{in}}{1-D} \quad (3)$$

with U_o being output voltage. T is switching period.

There exists a quasi-linear relationship between input and output voltage with a constant duty ratio, even internal components are not ideal. A converter with constant D and U_i is assumed as a constant voltage source if it stays in CCM. Moreover, with high input voltage, its neighbours may be forced to reduce their own output current and even work in DCM. For a converter in DCM, its output voltage are calculated based on power balancing rule (4) and sectional voltage-second balancing (5).

$$\underbrace{\frac{U_e - U_o}{Z} U_o T}_{\text{external injection}} + \underbrace{\frac{I_p}{2} (t + DT) U_{in}}_{\text{internal provision}} = \underbrace{\frac{U_o^2}{R} T}_{\text{load consumption}} \quad (4)$$

$$(U_o - U_i) \cdot t = U_i \cdot D \cdot T \quad (5)$$

with U_e, Z being external converter output voltage and connection line resistance. t is derived diode conducting time according to voltage-second balancing.

It can be rewritten as

$$U_o^2 \left(\frac{1}{R} + \frac{1}{Z} \right) - U_o \left(\frac{U_{in}}{R} + \frac{U_{in} + U_e}{Z} \right) + \left(\frac{U_e U_{in}}{Z} - \frac{I_p U_{in} D}{2} \right) = 0 \quad (6)$$

$$I_p = \frac{U_{in}}{L} DT \quad (7)$$

where $U_o = 0$ is a trivial solution and I_p is peak inductor current.

In order to ensure U_o is real, it proposes a prerequisite regarding determined variables as

$$\left(\frac{U_{in}}{R} + \frac{U_{in} + U_e}{Z} \right)^2 - 4 \left(\frac{1}{R} + \frac{1}{Z} \right) \left(\frac{U_e U_{in}}{Z} - \frac{I_p U_{in} D}{2} \right) \geq 0 \quad (8)$$

DCM constrain (9) should be checked as well after relative solutions $U_{o(1)}, U_{o(2)}$ are calculated.

$$t < (1-D)T \quad (9)$$

Both $U_{o(1)}$ and $U_{o(2)}$ are stable solutions to U_o if they are real and meet (9). In real application, the final stable value of U_o depends on previous converter state and actions. Meanwhile, in a DC network, such equivalence is hard to implement as a DCM node commonly has several direction interconnections with other nodes sharing correlated voltage. A simple iteration method can be applied to derive stable voltage as

Algorithm 1: DCM voltage derivation

Result: U_o
 $U_o^{(0)}$ is set U_o in CCM;
 $U_e^{(0)}$ is set according to $U_o^{(0)}$;
 $i = 0$, ϵ is set a small number ;
while $U_o^{(i)} - U_o^{(i-1)} \leq \epsilon$ and $i \geq 2$ **do**
 Solve (6) using $U_e^{(i)}$;
 if $U_{o(1)}^{(i)}$ or $U_{o(2)}^{(i)}$ is nontrivial **then**
 $U_o^{(i+1)} = U_{o(n)}^{(i)}$, where $U_{o(n)}^{(i)}$ is nontrivial;
 $U_e^{(i+1)}$ are updated assuming DCM node as a constant voltage source of $U_o^{(i+1)}$;
 else
 if unused nontrivial $U_{o(n)}^{(j)}$ ($j \leq i$) exists **then**
 Recall unused nontrivial solutions;
 else
 Print("No DCM with such duty ratio");
 Break;
 end
 end
 $i = i + 1$;
end

The buck-boost converter in DCM is more complicated due to three potential solutions. t is reformulated as

$$t = \frac{U_{in}}{U_o} DT \quad (10)$$

The simplified equation can be rewritten as

$$U_o^3 \left(\frac{1}{R} + \frac{1}{Z} \right) - U_o^2 \left(\frac{U_e}{Z} \right) - U_o \left(\frac{I_p U_{in} D}{2} \right) - U_{in} \left(\frac{I_p U_{in} D}{2} \right) = 0 \quad (11)$$

Three potential solutions should still meet (9). In these quadratic equations, all analytical solutions are nonlinear to U_i , which will strongly support future designed attack identification strategies.

B. Impulse current injection

Global network state vectors including voltage vector $\mathbf{U}$ and current output vector $\mathbf{I}$ can be written as (12)-(15).

$$\mathbf{I} = \mathbf{Y}\mathbf{U} \quad (12)$$

$$\mathbf{U} = [U_1 \ \dots \ U_i \ \dots \ U_N]^T \quad (13)$$

$$\mathbf{I} = [I_1 \ \dots \ I_i \ \dots \ I_n]^T \quad (14)$$

$$Y_{ij} = \begin{cases} -y_{ij} & i \neq j \\ \sum_{k=1}^n y_{ik} & i = j \end{cases} \quad (14)$$

$$y_{ij} = \begin{cases} \frac{1}{z_{ij}} & E(i, j) \neq 0 \\ 0 & E(i, j) = 0 \end{cases} \quad (15)$$

where y_{ij} is the admittance of transmission line between node i and node j . $\mathbf{Y}$ is the admittance matrix of network.

The converter combined with inner voltage source can be simplified as current source as shown in Fig. 1(b). With active duty ratio variation and transiently stable inductor current from node i , I_i is equivalent to the sum of previous stable current and impulse current. Utilizing each node's output ground capacitor, whose capacitance is denoted as C_i , the impulse part should satisfy a relationship in (16)-(18) in a linear circuit.

$$\mathbf{C}[i, j] = \begin{cases} C_i & i = j \\ 0 & i \neq j \end{cases} \quad (16)$$

$$\mathbf{I}_{imp} = [0 \ \dots \ I_{imp}^i \ \dots \ 0]^T$$

$$I_{imp}^i = \Delta\alpha_i \cdot I_{cov}^i = -\Delta\alpha_i \cdot \frac{I_{out}^i}{1 - \alpha_i} \quad (17)$$

$$\mathbf{C}\mathbf{U}(s) = \frac{\mathbf{I}_{imp}(s) - \mathbf{I}(s)}{s} \quad (18)$$

where I_{imp}^i represents impulse current generated by adjusted duty ratio, and I_i represents converters inner inductor current. $\Delta\alpha_i$ is the variation of duty ratio.

With constant passive component parameters, transient response of $\mathbf{U}$ under variable I_{imp}^i are affine. Due to nonlinear relationship between I_{imp}^i and α_i , several feature parameters of voltage transient response would be nonlinear to α_i as well, including for instance peak value and ramping coefficient.

C. Ripple correlation

Similar to equivalent impulse current generated by duty ratio variation, pulse current due to converter switching nature can be separated into repeating impulse current as well. Regarding buck-boost converter network, injection current I_{sw}^i from node i and global current vector $\mathbf{I}_{sw}$ can be written as

$$I_{sw}^i(t) = \sum_{n=0}^{\infty} I_p^i \mathbf{1}(t - nT_i) - \sum_{n=0}^{\infty} I_p^i \mathbf{1}(t - nT_i - (1 - D_i)T_i) \quad (19)$$

Fig. 6: Current decomposition for ripple estimation

$$\mathbf{I}_{sw}(t) = \sum_{n=0}^{\infty} \mathbf{E}(t - n\mathbf{T}) \mathbf{I}_{imp} - \sum_{n=0}^{\infty} \mathbf{E}(t - n\mathbf{T} - (\mathbf{e} - \mathbf{D})\mathbf{T}) \mathbf{I}_{imp} \quad (20)$$

where

$$\begin{aligned} \mathbf{1}(t) &= \begin{cases} 1 & t \geq 0 \\ 0 & t < 0 \end{cases} \\ \mathbf{t} &= [t_1 \ \dots \ t_i \ \dots \ t_N]^T \\ \mathbf{T} &= [T_1 \ \dots \ T_i \ \dots \ T_N]^T \\ \mathbf{E}(\mathbf{t})[i, j] &= \begin{cases} \mathbf{1}(\mathbf{t}[i]) & i = j \\ 0 & i \neq j \end{cases} \\ \mathbf{I}_{imp} &= [I_{imp}^1 \ \dots \ I_{imp}^i \ \dots \ I_{imp}^N]^T \\ \mathbf{e}[i, j] &= \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases} \\ \mathbf{D}[i, j] &= \begin{cases} D_i & i = j \\ 0 & i \neq j \end{cases} \\ I_p^i &= \frac{I_{out}^i}{1 - D_i} \\ I_{out}^i &= \frac{U_i}{z_{ii}} - \sum_{E(i, j) \neq 0 \& i \neq j}^N \frac{U_j - U_i}{z_{ij}} \end{aligned} \quad (21)$$

With t_i representing nodal standard time, equal to global standard time with a constant switching signal's phase duration. Through Laplace transform and substituting $\mathbf{I}_{sw}(s)$ by $\mathbf{I}_{imp}(s)$ in (18), each node voltage ripples are able to be calculated. As grid component parameters are asymmetrical in most scenarios, peak-to-peak value of node voltage can be various under different average voltage distribution.

It is equivalent to use Fourier transformation or FFT algorithm to calculate voltage ripples. Through choosing switching

Fig. 7: Average model of Boost converter

frequency as fundamental frequency, injecting current vector can be decomposed as

$$I_{sw}^i(t) = \sum_{n=0}^{\infty} (I_{ai}^n \sin(n\omega t) + I_{bi}^n \cos(n\omega t)) \quad (22)$$

$$\mathbf{I}_{sw} = \sum_{n=0}^{\infty} (\mathbf{I}_{sin}^n + \mathbf{I}_{cos}^n) \quad (23)$$

where

$$\begin{aligned} \mathbf{I}_{sin}^n &= [\dots I_{ai}^n \sin(n\omega_i t - d_i) \dots I_{aN}^n \sin(n\omega_N t - d_N)]^T \\ \mathbf{I}_{cos}^n &= [\dots I_{bi}^n \cos(n\omega_i t - d_i) \dots I_{bN}^n \cos(n\omega_N t - d_N)]^T \\ \mathbf{I}_{sin}^n(s) &= [\dots I_{ai}^n \frac{n\omega_i}{s^2 + (n\omega_i)^2} e^{-\frac{d_i}{n\omega_i} s} \dots]^T \\ \mathbf{I}_{cos}^n(s) &= [\dots I_{bi}^n \frac{s}{s^2 + (n\omega_i)^2} - \frac{d_i}{n\omega_i} s \dots]^T \end{aligned} \quad (24)$$

with d_i being phase duration regarding universal timestamp.

Considering d_i can be calculated depending on selected universal and local timestamps, all pulse current can be shifted for symmetry so that I_{ai} is equal to 0. Nonzero I_{bi} and synthetic current vector $\mathbf{I}_{ft}$ can be derived as

$$I_{bi}^n = \frac{2I_p^i}{n\pi} \sin(n\pi(1 - D_i)) \quad (25)$$

$$\mathbf{I}_{ft} = \sum_{n=0}^{\infty} \mathbf{I}_{cos}^n \quad (26)$$

Through similar substitution of $\mathbf{I}_{ft}$ for $\mathbf{I}_{imp}$, voltage ripples would be derived as well.

D. Oscillation correlation

During transition period between two different stable status, oscillations are unavoidable and normally should be suppressed. While in an attack identification criteria, such oscillations benefit as it contains some information regarding global status. Regarding a Boost converter scenario, using average models of converters as shown in Fig. 7, network internal injection current vector $\mathbf{I}$ and voltage vector $\mathbf{U}$ follow:

$$\mathbf{U}_{in} - (\mathbf{e} - \mathbf{D})\mathbf{U} = \mathbf{L}\dot{\mathbf{I}} \quad (27)$$

$$(\mathbf{e} - \mathbf{D})\mathbf{I} - \mathbf{Y}\mathbf{U} = \mathbf{C}^{-1}\dot{\mathbf{U}} \quad (28)$$

with

$$\mathbf{U}_{in} = [U_{in}^1 \dots U_{in}^i \dots U_{in}^N]^T \quad (29)$$

$\mathbf{I}$ and its s-domain value can be derived as

$$\dot{\mathbf{I}} + \mathbf{C}\mathbf{Y}\dot{\mathbf{I}} + \mathbf{L}^{-1}\mathbf{C}(\mathbf{e} - \mathbf{D})^2\mathbf{I} = \mathbf{L}^{-1}\mathbf{C}\mathbf{Y}\mathbf{U}_{in} \quad (30)$$

$$s^2\mathbf{I} + s\mathbf{C}\mathbf{Y}\mathbf{I} + \mathbf{L}^{-1}\mathbf{C}(\mathbf{e} - \mathbf{D})^2\mathbf{I} = \mathbf{L}^{-1}\mathbf{C}\mathbf{Y}\mathbf{U}_{in} \quad (31)$$

It can be rewritten as (32). Both $\mathbf{A}$ and $\mathbf{B}$ are constant.

$$\mathbf{A}\mathbf{I} = \mathbf{B} \quad (32)$$

where

$$\begin{aligned} \mathbf{A}[i, j] &= \begin{cases} s^2 + sC_i \sum_{j=1}^N Y_{ij} + L_i C_i (1 - D_i)^2 & i = j \\ -sC_i Y_{ij} & i \neq j \end{cases} \\ \mathbf{B}[i] &= L_i^{-1} C_i \sum_{j=1}^N Y_{ij} U_{in}^j \end{aligned} \quad (33)$$

$\mathbf{A}$ has full rank, so (32) can be represented as

$$\mathbf{I} = \mathbf{A}^{-1}\mathbf{B} \quad (34)$$

with

$$\mathbf{A}^{-1}[i, j] = \frac{(-1)^{i+j} \mathbf{M}[i, i]}{\det(\mathbf{A})} \quad (35)$$

where $\mathbf{M}_{ij}$ denotes a minor of $\mathbf{A}$.

In order for further simplification, there exists a hypothesis in mandatory, who have been naturally satisfied in most large-scale DC distribution network:

- $|\sum_{j=1}^N Y_{ij}| \gg |Y_{ij}|$ if $i \leq j$

If Node 1 is selected, its injection current I_1 can be calculated as

$$\det(\mathbf{A}) \approx \prod_{i=1}^N \mathbf{A}[i, i] + o(s^{2N-2}) \quad (36)$$

$$\mathbf{M}[i, j] \approx \begin{cases} \prod_{i=1, i \neq j}^N \mathbf{A}[i, i] + o(s^{2N-2}) & i = j \\ O(s^{2N-4}) & i \neq j \end{cases} \quad (37)$$

$$\begin{aligned} I_1 &= \frac{\sum_{i=1}^N \mathbf{M}[i, j] B_i}{\det(\mathbf{A})} \approx \frac{B_1 (\prod_{i=2}^N \mathbf{A}[i, i] + o(s^{2N-2}))}{\prod_{i=1}^N \mathbf{A}[i, i] + o(s^{2N-2})} \\ &= \frac{B_1 s^{2N-2} + o(s^{2N-2})}{s^{2N} + s^{2N-1} \sum_{j=1}^N m_j + s^{2N-2} \sum_{i=1}^N q_i + o(s^{2N-2})} \\ &\approx \frac{B_1}{s^2 + s \sum_{j=1}^N m_j + \sum_{i=1}^N q_i} \end{aligned} \quad (38)$$

where

$$m_j = \sum_{i=1}^N C_i Y_{ij} \quad (39)$$

$$q_i = L_i C_i (1 - D_i)^2 + \sum_{j=1}^N m_i m_j$$

It is settled that $a = \sum_{j=1}^N m_j, b = \sum_{i=1}^N q_i$, then (38) can be converted through inverse Laplace transform, where $I_1(0)$ is

the initial value of I_1 . Obviously with a larger positive Δ , both its oscillation frequency and peak values would be higher. Moreover, there exist a positive correlation between Δ and b .

$$I_1 = \frac{e^{-\frac{at}{2}} \sin(\sqrt{\Delta}t)}{\sqrt{\Delta}} + I_1(0) \quad (40)$$

$$\Delta = b - \frac{a^2}{4}$$

Considering unstable and immeasurable nature of parasite components in most grids, through comparing various Δ in several scenarios, some current oscillation feature values can be sorted by estimation, for instance shooting value and first oscillation period.

V. EVENT-TRIGGERED ATTACK DETECTION AND IDENTIFICATION

Signal shielding can be easily detected by any relative agents. Considering large inertia designed in most systems, temporary power flow distortion caused by asynchronization under signal shielding can hardly influence global system stability considering BES. A coordinated attack with signal shielding and false message injection seems more efficient for attackers, since it can generate stealth unmatched power flow for a long period. The proposed detection flow chart is illustrated in Fig. 8.

An event trigger should be designed first based on attack detection, as shown in the blue block in Fig. 8, saving computation and communication resource in distributive network. When received neighbour data are estimated incompatible with its own data according to (41), detector is triggered and attacking pattern would be classified.

$$\hat{I}_{out}^i = Y_{ii}\hat{U}_i - \sum_{E(i,j) \neq 0 \& i \neq j}^N (\hat{U}_j - \hat{U}_i)Y_{ij} \quad (41)$$

where $\hat{I}_{out}^i$ is the estimate value of output current from node i , $\hat{U}_i$ is declared voltage level of node i . $E(i, j)$ is a 0/1 variable indicating whether node i and node j is linked.

The attack detection is implemented personally by the node whose detector is triggered, and its own sensors and neighbors should coordinate with him to avoid wrong judgment and further grievance procedures. Before commands sent out, the detector should broadcast its future action to avoid triggering other detectors, then start polling its neighbours to check whether examination period is available. Such polling mechanism should be designed and followed by all nodes, based on an universal communication protocol for instance IEC 61850 and scalable MAC Protocol (SC-MP)[25], [26]. Since communication protocol is not the main topic of this paper, further discussion on polling system is saved.

The only problem of such consensus is that an evil node would send coordination requests maliciously to its neighbor nodes, finally jamming action space of other nodes. Actually, trust mechanism for distributive network is still an open question[27], and in this paper, trust level on neighbors' cooperation request relies on action space redundancy, and limited request frequency is considered an effective solution,

Fig. 8: Attack detection flow chart

even attack responding speed would be influenced. Time-triggered attack detection and identification is also acceptable if no event has happened for a long period.

In accordance with detection flow chart in Fig. 8, as self sensor examination is always in advance of agent examination, rapid-response-required part is put afterward, violating original intentions of strategy choice. For industrial application, the order of examination should be exchanged, or let self sensor check be a routine before detection triggered. The procedure order in Fig. 8 is only designed for REG-integrated microgrid, where internal regulating capacity is enough and a quantity of nodes are naturally stochastic and unmanageable generation units, indicating that sensor attack in this network is more cheap and frequent.

If no attacker is identified in previous two procedures, node fault should be checked first. However, relay protection is commonly integrated and operates immediately when node fault happens. The step of node fault is illustrated by dashed line in Fig. 8, meaning that it would be dropped in most industrial application considering existence of relay protection. While it may be kept if some minor faults won't trigger relay protector and still needs to be paid attention, for instance surging current generated by EV charging while neglected by low-sampling-frequency sensors. If no attack or fault happen, the network parameter data Y and C should be calibrated based on impedance modeling methods[28].

A. Self sensor examination

Regular self sensor authentication is essential even attack detection has not been triggered, as trustworthy self signals are mandatory for future attacker identification. If the agent is verified to receive trustworthy self sensor data, neighbour

examination procedure will be prepared, otherwise the sensor would be distinguished as an instigator. A self sensor instigation is considered as a severe attack as it cannot be removed by node himself, and the node has to call for external help until the voltage sensor is rechecked or reinstalled by authorized system operator.

Commonly, active voltage adjustment will be adopted for self sensor examination, and it would also introduce short-term oscillations and raise communication cost due to duty of disclosure before application. While without detector triggered, neighbour nodes can be considered reliable temporarily. Through voltage ripple estimation, there is no necessity of extra action for sensor authentication. Considering a hypothesis in Section II-B, with a high switching frequency of semiconductor and similar higher voltage measuring frequency, no duty ratio can be measured directly in several switching periods. Since attacker are unable to predict the duty ratio variations, in order to ensure it could still be trusted in future stable CCM states, it has only choice to provide proportional data to its previous fake data simultaneously. The key idea for sensor examination based on this assumption, is to utilize the information gap of transition tendency and period.

1) *DCM examination*: As mentioned in Section IV-A, DCM will introduce nonlinear relationship between input and output voltage. It will directly help identify spurious scaled voltage data. It is equivalent to change self duty ratio or request others' voltage adjustment. However, in order to import DCM, the whole submodule has to suffer low output voltage, which may still be intolerable for self load. The other disadvantage of such method is that it only works in unidirectional converter, which limits its application region, especially for energy storage system.

2) *Ripple examination*: Through comparing estimated ripple magnitudes using received signals as illustrated in Section IV-C, nonlinear relationship between output voltage and ripple magnitudes would help identify whether these signals are deceptive. In most scenarios, active voltage adjustment can be even saved if original status can help verify sensor data. While such method proposes a high requirement on measurement equipment accuracy. Compared with other method, ripple estimation also requires a higher computation capability, so its deployment can be merely confined to important nodes.

B. Neighbour examination

If self measurement signals have been authenticated with triggered detector, evil neighbours should be identified afterwards. Active voltage variation would be used as well for evil neighbour classification if network impedance matrix is open data. With scheduled ramping or dropping voltage wave, the instigated agent would be identified.

The principle of evil member classification using voltage injection is explained as follows. In a stable network after some node voltage variation, for a specific node i , its output voltage variation can be calculated in (42), in order to verify the status of a specific neighbour node j . In order to survive, if a node request the attacking node to adjust voltage, the attacker has no choice but to raise or drop its output voltage

accordingly in honest, otherwise, unmatched current data will reveal the attacker after the network comes stable.

$$\Delta I_{out}^i = Y_{ij} \Delta U_j \quad (42)$$

1) *Impulse current response*: For transient analysis to classify the attacker, based on simplified circuits shown in Fig. 1(b), global transient state vectors including voltage vector $\mathbf{U}$ and current output vector $\mathbf{I}$ can be solved as mentioned in Section IV-B. Nonlinear relationship between $\Delta \mathbf{U}$ and $\Delta \mathbf{I}$ would expose the attacker. Even another attacker would mask the tested node through synchronized action, it will trigger other detectors and both of them will be distinguished through cross validation of all innocent nodes. Such method is serviceable for high power application due to high impulse current. Its fast response relies on a short sampling period, naturally meeting the response speed requirement in high power scenarios. Meanwhile, in low power scenarios, the impulse response can be easily overlapped by switching ripples.

2) *Ripple examination*: The ripple estimation for neighbour examination is similar to that for self examination mentioned in Section. V-A2.

3) *Oscillation examination*: As discussed in Section. IV-D, through comparing corresponding b , the order of feature values in various scenarios can be estimated for instance shooting value or first oscillation period. If the estimated order does not match measured one, the wrongly sorted one can reveal that the tested node in this scenario is the traitor.

If Sybil attack happens, such detection mechanism may fail as some evil agents can mask each other through stealth attack. Under such circumstance, voting system for all suspect nodes can perform better while a global ballot ticket collector should be picked. In this paper, this extreme scenario will be neglected as stealth attack is commonly difficult to implement especially under complicated transient behaviour of converters.

VI. VALIDATION AND DISCUSSION

The theoretical solution for attack detection to distinguish attack category has been illustrated. In order to verify the validity of proposed method, both simulation test on SIMULINK/PLECS and hardware test on dSpace platform have been implemented, separately in Buck-Boost and Boost scenarios. Detailed discussion were provided when comparing theoretical solutions with experimental data, and the efficacy of proposed method was proven.

A. Simulation verification

Regarding a simplified 4-node MVDC microgrid shown in Fig. 9a, buck-boost converters are employed as interfaces connecting inner system to neighbour nodes. The parameters of simulation system are listed in Tab. II.

1) *DCM for self examination*: Several parameters in self examination scene are listed in Tab. III, where all Buck-Boost converters employed are assumed unidirectional. If Node 2 is assumed being attacked, its output voltage equals 800V while its sensors would lie with a gap of 100V. In order to authenticate these messages and ensure future DCM, D_2

Fig. 9: Schematics of simulation and hardware testing DC network

TABLE II: Table of simulation system parameters

Parameter	Value	Meaning
f_{sw}	10kHz	Switching Frequency
R_{line}	2 Ω	Power line equivalent series resistance
L_{line}	5mH	Power line equivalent series inductance
R_{load}	64 Ω	Load resistance
V_{in}	800V	Subsystem input voltage
C	500 μ F	Subsystem output ground capacitance
L	0.2H	Inner inductance in converter

Fig. 10: Voltage wave in Node 2 for DCM examination

is adjusted to 0.4. Even there exists a small gap between estimated and simulated values due to MOSFET and diode loss, they are still assumed matched. Furthermore, according to Tab. IV and Fig. 10, such action would lead to an unavoidable difference between deceptive signals and estimated values, and self sensor attack can be detected eventually.

TABLE III: Table of DCM examination parameters

Parameter	Value	Meaning
D_i	0.5	Converter duty ratio
α	1.125	Amplifying ratio of self voltage sensor
ΔD_1	-0.1	Duty ratio variation for DCM

TABLE IV: Table of DCM estimation and simulation results

Parameter	Value
Real U_2	780.13V
Deceptive U_2	877.64V
Estimated U_2 with $V_{in} = 900V$	775.93V
Estimated U_2 with $V_{in} = 800V$	775.89V

2) *Impulse response for neighbourhood examination:* Bidirectional Buck-Boost converters are adopted in this testing scenario, where Node 2 was picked as an instigated agent to attack jgrid, who tried to steal energy from grid and tract it to a

Fig. 11: Voltage samples in Node 1 under impulse current

lower voltage level. Its neighbour Node 1 would send a voltage adjustment request after self sensor verification. Node 2 had no choice but to adjust voltage accordingly, while the mismatched output voltage data of Node 1 would reveal Node 2's guilty. The examination parameters are given in Tab. V, where Node 1 has detected there may exist a voltage gap of 266.7V between Node 2, if Node 2 is assumed as an traitor. so Node 2 is requested to raise its output voltage by 266.7V.

From the perspective of Node 1, whether Node 2 was cheating, it can generate theoretical solution to estimate its future voltage variation after relative nodes' action, as shown in orange lines in Fig. 11a. The mathematical solution of Node 1 voltage derivative could be derived as orange lines Fig. 11b show. Meanwhile, the relative simulation results of Node 1 output voltage in both scenarios are given in blue lines in Fig. 11a-11b. If a specific scenario has been assumed, the large divergence between theoretical solution and sampled data would help prove or reject the assumption. Detailed simulation results regarding output voltage waves of Node 1 are given in Fig. 12. Moreover, it can be concluded that the theoretical and simulation results highly matched for the same scenario.

TABLE V: Table of impulse examination parameters

Scenario	Parameter	Value
Node 2 is evil	Original duty ratio	0.4
	Updated duty ratio	0.5
	Original output voltage	533.3V
	Updated output voltage	800V
Node 2 is innocent	Original duty ratio	0.5
	Updated duty ratio	0.571
	Original output voltage	800V
	Updated output voltage	1066.7V

TABLE VI: Table of ripple results for self examination

Parameter	Value
Real ripple magnitude with $V_{in} = 800V$	1.427V
Real ripple magnitude with $V_{in} = 900V$	8.533V
Deceptive ripple magnitude	1.783V
Estimated ripple magnitude with $V_{in} = 800V$	1.249V

3) *Ripple estimation for both examination:* Regarding self examination, the attacking scenario is similar to that in Sec-

Fig. 12: Voltage wave in Node 1 under impulse current

Fig. 13: Voltage ripples in Node 2 for self examination

Fig. 14: Voltage ripples in Node 1 for neighbour examination

tion. VI-A1, while the voltage signals are scaled by 0.889, where its real output voltage is 900V and the sensor declares it as 800V. The estimated ripple magnitude and simulated one match well according to Tab. VI, and the gap between deceptive signals and estimated values is large enough for self sensor identification. The simulated voltage waves of Node 2 is illustrated in Fig. 13. Similarly, from the perspective of neighbour examination, under the same attack with that in Section. VI-A2, both Node 2 and Node 4 are requested to raise its voltage by 266.7V sequentially. The ripple magnitude gap is also large enough to distinguish as shown in Fig. 14 and Tab. VII.

TABLE VII: Table of ripple results for neighbour examination

Parameter	Value
Real ripple magnitude with Node 2 polled	1.394V
Real ripple magnitude with Node 4 polled	2.359V
Estimated ripple magnitude with Node 2 polled	1.249V
Estimated ripple magnitude with Node 4 polled	2.434V

B. Hardware verification

In hardware test part, boost-converter-based DC network is established according to Fig.9b and investigated as illustrated in Fig. 15. Due to power and measurement limit of such platform, impulse current response is too small to observe and ripple magnitude measured is inaccurate. Moreover, without

Fig. 15: Voltage oscillation in Node 1

Fig. 16: Detailed voltage wave in Node 2

exact knowledge of parasite inductance of connection lines, the estimated transients waves are difficult to match real ones. The loss of MOSFET and diode should be considered as well. That explains why only DCM and oscillation examination are adopted in this experiment. Actually, due to physical limits in real DC microgrid, not all attack identification methods are applicable. The basic parameters of such platform are listed in Table. VIII.

TABLE VIII: Table of hardware system parameters

Parameter	Value	Meaning
f_{sw}	10kHz	Switching Frequency
R_{line}	30.4 Ω	Power line equivalent series resistance
R_{load}	114 Ω	Load resistance
V_{in}	90V	Subsystem input voltage
C	1.1 mF	Subsystem output ground capacitance
L	1 mH	Inner inductance in converter

1) *DCM examination:* External voltage lifting for local DCM is implemented in this case. The system status parameters are listed in Tab. IX, where the attacking sensor lied that Node 2's inner voltage level is 100V. Through lifting its own output voltage, Node 2 is in DCM, whose voltage waves are measured and shown in Fig. 16. As shown in Tab. IX, he estimated voltage is close to measured one, eventually helping node 2 detect self sensor attack successfully.

TABLE IX: Table of theoretical and simulation results

Parameter	Value
Voltage signal amplifying ratio	1.11
Original duty ratio of Node 1	0.32
Original duty ratio of Node 2	0.09
Original duty ratio of Node 3	0.32
Updated duty ratio of Node 1	0.46
Estimated U_2 with $V_{in} = 80V$	93.0V
Estimated U_2 with $V_{in} = 100V$	93.5V
Measured U_2 with $V_{in} = 80V$	92.0V
Deceptive U_2	112.2V

Fig. 17: Injection current wave in Node 1

2) *Oscillation examination*: The attacking and action parameters are listed in Tab. X. Due to unknown parasite inductance in such system, oscillation examination is adopted. Considering symmetrical topology of this system, only $\sum_{i=1}^3 (1 - D_i)^2$ are calculated and compared. The scenario that Node 2 is evil owns a higher value of $\sum_{i=1}^3 (1 - D_i)^2$, which indicates that Δ would be also higher in this scenario.

TABLE X: Table of theoretical examination parameters

Scenario	Parameter	Value
Before action	original D_1	0.32
	original D_2	0.09
	original D_3	0.32
	original U_1	132.4V
	original U_2	98.9V
	original U_3	132.4V
Node 2 is evil	updated D_2	0.32
	updated U_2	132.4V
Node 2 is innocent	updated D_3	0.46
	updated U_3	166.7V

As discussed in Section IV-D, if Δ is positive, ΔT_{I1} and $|\Delta I_1|$ should be positive, then it can be derived that when Node 2 is evil, $\Delta T_{U1}, \Delta T_{I1}, |\Delta U_1|$ and $|\Delta I_1|$ should be larger as well. Otherwise these four parameters should be smaller under the circumstance that Node 2 is evil. In order to verify such conclusion, both simulation and hardware experiments are conducted. As illustrated in Fig. 17-18, through comparing specific indices, all comparisons match only theoretically estimated ones, especially $|\Delta I_1|$ is most different, and a higher $|\Delta I_1|$ under negative Δ indicates that Node 2 is innocent. The measurement data in various scenarios during hardware testing are illustrated in Fig. 19-20. Through selecting certain points and calculating corresponding parameters as shown in Tab. XI-XII. All index comparison results have met estimated ones, especially for $|\Delta U_1|$. The efficacy of proposed oscillation examination methods has been verified.

VII. CONCLUSION

This article has presented an event-triggered attack detection and identification for converter-based DC network. Through stable or transient wave analysis, neither instigated sensors nor agents can mask themselves. In response for attacks in various formats, four attack identification strategies have been

Fig. 18: Detailed voltage wave in Node 1

Fig. 19: Detailed voltage wave in Node 1

Fig. 20: Output voltage wave in Node 1

TABLE XI: Table of examination parameters

Scenario	Time(s)	Parameter	Value
Node 2 is evil	0.5544	U_1	116.367V
	0.5683	U_1	113.407V
	0.5508	I_1	1.355A
	0.5762	I_1	0.891A
	0.7218	U_1	116.398V
Node 2 is innocent	0.7438	U_1	106.113V
	0.7143	I_1	1.367A
	0.7489	I_1	0.793V

investigated and tested both by simulation and hardware tests. The matching between estimation, simulation and measurement values illustrates the efficacy of proposed methods.

For a DC network with specific parameters, voltage or current response under each identification strategy can be estimated in advance and the strategy with most obvious phenomenon is preferred. Through flexible strategy selection, the whole anti-attack system is robust in most scenarios. In

TABLE XII: Table of derived values for oscillation examination

Scenario	Parameter	Value
Node 2 is evil	ΔT_{U1}	13.9ms
	ΔT_{I1}	25.4ms
	ΔU_1	-2.960V
	ΔI_1	-0.440A
Node 2 is innocent	ΔT_{U1}	22.0ms
	ΔT_{I1}	34.6ms
	ΔU_1	-10.285V
	ΔI_1	-0.574A

future, more feature values contained in voltage or current waves would be extracted for attacker identification. Under model-free scenes, machine learning including neural network may be employed as well for faster response and higher adaptivity.

ACKNOWLEDGMENT

The authors would like to thank the PowerLab DK in DTU for hardware test support.

REFERENCES

- [1] P. Sanjeev, N. P. Padhy, and P. Agarwal, "Peak energy management using renewable integrated dc microgrid," *IEEE Transactions on Smart Grid*, vol. 9, no. 5, pp. 4906–4917, 2017.
- [2] A. T. Elsayed, A. A. Mohamed, and O. A. Mohammed, "Dc microgrids and distribution systems: An overview," *Electric power systems research*, vol. 119, pp. 407–417, 2015.
- [3] J. J. Justo, F. Mwasilu, J. Lee, and J.-W. Jung, "Ac-microgrids versus dc-microgrids with distributed energy resources: A review," *Renewable and sustainable energy reviews*, vol. 24, pp. 387–405, 2013.
- [4] N. Holtsmark, H. J. Bahirat, M. Molinas, B. A. Mork, and H. K. Hoidalén, "An all-dc offshore wind farm with series-connected turbines: An alternative to the classical parallel ac model?" *IEEE Transactions on industrial Electronics*, vol. 60, no. 6, pp. 2420–2428, 2012.
- [5] F. Perez, A. Iovine, G. Damm, L. Galai-Dol, and P. F. Ribeiro, "Stability analysis of a dc microgrid for a smart railway station integrating renewable sources," *IEEE Transactions on Control Systems Technology*, 2019.
- [6] N. Ertugrul and D. Abbott, "DC is the future," *Proceedings of the IEEE*, vol. 108, no. 5, pp. 615–624, 2020.
- [7] McKinsey. (2010). Transformation of Europe's power system until 2050, [Online]. Available: https://www.mckinsey.com/~media/mckinsey/dotcom/client_service/epng/pdfs/transformation_of_europes_power_system.ashx (visited on 10/17/2020).
- [8] H. A. P. Grids. (2020). Hitachi ABB Power Grids launches game-changing EV charging system for large scale e-Mobility, [Online]. Available: <https://www.hitachiabb-powergrids.com/news/global-news/press-releases/hitachi-abb-powergrids-launches-game-changing-ev-charging-syste> (visited on 07/15/2020).
- [9] J. Zhou, M. Shi, Y. Chen, X. Chen, J. Wen, and H. He, "A novel secondary optimal control for multiple battery energy storages in a dc microgrid," *IEEE Transactions on Smart Grid*, 2020.
- [10] J. Sun, W. Lin, M. Hong, and K. A. Loparo, "Voltage regulation of dc-microgrid with pv and battery," *IEEE Transactions on Smart Grid*, 2020.
- [11] T. Morstyn, A. V. Savkin, B. Hredzak, and V. G. Agelidis, "Multi-agent sliding mode control for state of charge balancing between battery energy storage systems distributed in a dc microgrid," *IEEE Transactions on smart grid*, vol. 9, no. 5, pp. 4735–4743, 2017.
- [12] I.-Y. L. Hsieh, M. S. Pan, Y.-M. Chiang, and W. H. Green, "Learning only buys you so much: Practical limits on battery price reduction," *Applied Energy*, vol. 239, pp. 218–224, 2019.
- [13] S. Tan, J. M. Guerrero, P. Xie, R. Han, and J. C. Vasquez, "Brief survey on attack detection methods for cyber-physical systems," *IEEE Systems Journal*, 2020.
- [14] S. Sridhar and M. Govindarasu, "Model-based attack detection and mitigation for automatic generation control," *IEEE Transactions on Smart Grid*, vol. 5, no. 2, pp. 580–591, 2014.
- [15] L.-Y. Lu, H. J. Liu, H. Zhu, and C.-C. Chu, "Intrusion detection in distributed frequency control of isolated microgrids," *IEEE Transactions on Smart Grid*, vol. 10, no. 6, pp. 6502–6515, 2019.
- [16] J. James, Y. Hou, and V. O. Li, "Online false data injection attack detection with wavelet transform and deep neural networks," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 7, pp. 3271–3280, 2018.
- [17] L. Liu, M. Esmalifalak, Q. Ding, V. A. Emesih, and Z. Han, "Detecting false data injection attacks on power grid by sparse optimization," *IEEE Transactions on Smart Grid*, vol. 5, no. 2, pp. 612–621, 2014.
- [18] O. A. Beg, L. V. Nguyen, T. T. Johnson, and A. Davoudi, "Signal temporal logic-based attack detection in dc microgrids," *IEEE Transactions on Smart Grid*, vol. 10, no. 4, pp. 3585–3595, 2018.
- [19] S. Sahoo, S. Mishra, J. C.-H. Peng, and T. Dragičević, "A stealth cyber-attack detection strategy for dc microgrids," *IEEE Transactions on Power Electronics*, vol. 34, no. 8, pp. 8162–8174, 2018.
- [20] A. J. Gallo, M. S. Turan, F. Boem, T. Parisini, and G. Ferrari-Trecate, "A distributed cyber-attack detection scheme with application to dc microgrids," *IEEE Transactions on Automatic Control*, vol. 65, no. 9, pp. 3800–3815, 2020.
- [21] L. Ding, Q.-L. Han, X. Ge, and X.-M. Zhang, "An overview of recent advances in event-triggered consensus of multiagent systems," *IEEE transactions on cybernetics*, vol. 48, no. 4, pp. 1110–1123, 2017.
- [22] B. Moussa, M. Debbabi, and C. Assi, "Security assessment of time synchronization mechanisms for the smart grid," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 1952–1973, 2016.
- [23] A. Geetha and N. Sreenath, "Byzantine attacks and its security measures in mobile adhoc networks," *Int'l Journal of Computing, Communications and Instrumentation Engineering (IJCCIE 2016)*, vol. 3, no. 1, pp. 42–47, 2016.
- [24] J. R. Douceur, "The sybil attack," in *International workshop on peer-to-peer systems*, Springer, 2002, pp. 251–260.
- [25] B. Ismaiel, M. Abolhasan, W. Ni, D. Smith, D. Franklin, and A. Jamalipour, "Analysis of effective capacity and throughput of polling-based device-to-device networks," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 9, pp. 8656–8666, 2018.
- [26] S. S. Hussain, T. S. Ustun, and A. Kalam, "A review of iec 62351 security mechanisms for iec 61850 message exchanges," *IEEE Transactions on Industrial Informatics*, 2019.
- [27] Y. Yu, K. Li, W. Zhou, and P. Li, "Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures," *Journal of Network and computer Applications*, vol. 35, no. 3, pp. 867–880, 2012.
- [28] T. Roinila and T. Messo, "Online grid-impedance measurement using ternary-sequence injection," *IEEE Transactions on Industry Applications*, vol. 54, no. 5, pp. 5097–5103, 2018.