A Novel Attack Identification Mechanism in IoT-Based Converter-Composed DC Grids

Gong, Sicheng; Dragičević, Tomislav; Mijatovic, Nenad; Zhang, Zhe

Published in:
IEEE Internet of Things Journal

Link to article, DOI:
10.1109/JIOT.2022.3220182

Publication date:
2023

Document Version
Peer reviewed version

A Novel Attack Identification Mechanism in IoT-Based Converter-Composed DC Grids

Sicheng Gong, *Student Member, IEEE*, Tomislav Dragičević, *Senior Member, IEEE*, Nenad Mijatovic, *Senior Member, IEEE*, and Zhe Zhang, *Senior Member, IEEE*

***Abstract*—This paper proposes a novel attack identification mechanism for internet-of-things-based (IoT-based) converter-composed DC grids, where each agent collects its own and neighbours' measurement data for output regulation to meet a preceding power-sharing consensus. Independent from model-free or average-model-based attack detection theories, this mechanism is mainly inspired by converter stitching behavior analysis. Correspondingly, when facing latent signal substitution or agent instigation attacks, through comparing estimated signals with received ones for signal source authentication, both self-sensors and neighbours will be inspected. Eventually, not only can such attacks be detected, but also will respective attack sources be identified. A simulation case of 4-agent 800V IoT-based DC grid on Simulink and a hardware case of 3-agent 90V IoT-based DC grid on dSpace testing platform were investigated. Experimental results revealed that the estimation ratio error kept lower than 3.9% and all attacks were successfully identified, verifying the effectiveness of the proposed mechanism.**

***Index Terms*—internet of things, attack identification, DC grid, DC/DC converter, wave analysis.**

I. Introduction

DUE to stochastic nature of renewable energy generation(REG) and charging behavior, DC interconnection is advantageous for a REG-integrated power system or EV charging infrastructure as its looser grid code [1]. Part of rectifiers can be saved and merely voltage magnitude is considered in a DC network, indicating higher operation reliability and resilience [2]–[5]. Reduced conversion loss also highlights the necessity of DC system deployment [6]. Therefore DC grid is assumed an economical and reliable scheme for REG integration or EV charging. The rapid emergence of DC grids proves its priority over conventional AC grids [7], [8]. Simultaneously, with communication device integration requested by smart grid services, the DC grid is considered as an IoT, where a power-sharing consensus is achieved and implemented correspondingly [9].

Nonetheless, without a redundant regulation capacity based on external compensation, power curtailment or load shedding, the global stability of IoT-based DC grid can still be fragile and easily threatened by frequent intrinsic power imbalances. In order to enhance grid resilience, there exists a widespread solution of battery energy storage (BES) employment, who plays an alternative role of external regulator [10], [11]. However, BES is commonly expensive and only designed for periodic power variations [12]. It is unpractical to compensate for long-term power imbalances considering its finite capacity. Precisely, under deliberately biased node voltage or accidental node faults, power imbalance in an IoT-based DC grid will exist continuously until relative nodes are removed actively.

Under such circumstance, rapid attack or fault detection is expected, and BES should be employed merely for short-term voltage support. Relay protection technology is industrially mature to detect faults, while it cannot realize attack detection considering possible data incredibility, which is a widespread issue in an IoT particularly [13]–[15]. The situation becomes more severe in a distributive network, due to a lack of central controller and instant measurement data sharing. Under such circumstance, any misguided action will exhaust grid regulation capacity rapidly, leading to grid distortions or even collapsing. Therefore, a distributed attack identification strategy should be designed, providing a credible reference for next-step action to ensure grid benefits and stability.

Grid attacks can be classified into two categories, including physical attacks and functional attacks [16]. The physical attack aims to knock out electricity grids using up available resources, while the functional one targets system misdirection to maximize attackers' profits, especially in a specific electricity market [17]. These two different attacks threaten grid security interests and economic benefits separately. Namely, functional attacks lead to distortions on power-sharing consensus generation, while physical ones aim to cause a different power flow distribution in real grids from the achieved power-sharing consensus. In this paper, the power-sharing consensus in an IoT-based DC grid is assumed robust against functional attacks. Physical attacks are mainly focused to explore corresponding strategies in the remainder of this paper.

A brief survey on attack detection for a general cyber-physical system has been conducted in [18], including central controller and distributive controller scenarios in general cyber-physical systems. Regarding IoT-based power systems, a model-based physical attack detection strategy for generation control has been proposed in [19], and intrusion detection for distributed frequency controllers in microgrids was investigated in [20]. Reference [21] utilizes Hilbert-Huang transform to derive an extended energy spectrum, realizing the detection of false data injection attacks. Eigenvalue analysis can be employed for attack detection as well [22]. Besides, several

This work was supported by NEON (New Energy and mobility Outlook for the Netherlands, with project number 17628), a cross-over project financed by NWO (the Dutch Research Council).

S. Gong is with the Department of Electrical Engineering, Eindhoven University of Technology, Eindhoven, 5612 AZ, Netherlands (email: s.gong@tue.nl).

T. Dragičević, N. Mijatovic, Z.Zhang are with the Department of Electrical Engineering, Technical University of Denmark, Lyngby, 2800, Denmark (email: tomdr@elektro.dtu.dk; nm@elektro.dtu.dk; zz@elektro.dtu.dk).

This article has been accepted for publication in IEEE Internet of Things Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2022.3220182

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 [23]–[25]. Whereas all detection methods above are intended for AC grids.

For an emerging IoT-based converter-dominated DC grid, the machine learning method has been valid for attack detection [15], [26], [27]. However, such model-free method proposes a huge demand of testing data in advance of model training. It also suffers a high computation burden and a short valid period, considering inevitably frequent network parameter variations caused by dynamic environment temperature [28]. Therefore, model-based detection methods are expected, which is analytical and adaptive to network parameter variations. In [29], a predetermined reachable status set is investigated as a reference to attack detection. However, such method fails to figure out the attacker and requires a large number of testing scenarios. Signal temporal logic formalism can be employed to detect attacks and evaluate relative impacts on system stability [30], while it also cannot identify the attack source and depends on predefined reliable signal predicates. Eigenvalue analysis and Hilbert-Huang Transform can be also utilized in DC grid scenario, while depending on self sensor data reliability [31], [32]. In [33], 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. The effectiveness of detection methods using certain reliable data can be harmed when the attacker blocks such data source. Cyber-attack detection schemes based on unknown input observers have been investigated in [34], [35], realizing attack detection using non-reliable measurement data. Meanwhile, these schemes are derived from converter average model, whose estimation accuracy will be influenced during grid transient status. Moreover, attack source identification is still missing in these works.

In summary, all model-based detection strategies above fail to bridge the gap between converter switching model and DC grid attack detection in the context of non-reliable measurement data. Besides, attack identification is more expected than mere attack detection, for preparation of future attack source removal. The comparison between previous literature and this paper has been given in Table I. The motivation of the present work in this paper is to address this challenge.

Data authentication not only ensures measurement data reliability, but also helps identify attackers as well. Accordingly, this paper proposes a novel attack detection and identification mechanism, inspired by an artificially introduced nonlinear relationship between switching duty ratio and converter output performance. Such mechanism aims at efficient attack detection and identification in most attacking scenarios, while only depending on untrustworthy measurement data. Through the proposed identification procedures, no malicious sensors or agents can hide, and a reconfigured network topology will remove those attackers to ensure grid stability. In summary, the main contributions of this paper are listed as below:

- Clarify two attack patterns who are intended to avoid being identified using existing model-based methods, including self-sensor instigation and neighbour instigation, which are able to bypass detection methods in [25]-[26], [28]-[32].
- Clarify analytical relationship between estimated and measured variables under two above attacks, thus figuring out corresponding attack identification indices.
- Exploit a novel attack identification mechanism in IoT-based converter-composed DC grids. Through artificially importing converter dynamics for authentication, instigated self-sensors and neighbours would be identified by comparison. The whole operation flow has no dependence on reliable data from self-sensors or neighbours.
- Validate the efficacy of the proposed attack identification mechanism by simulation and experimental tests.

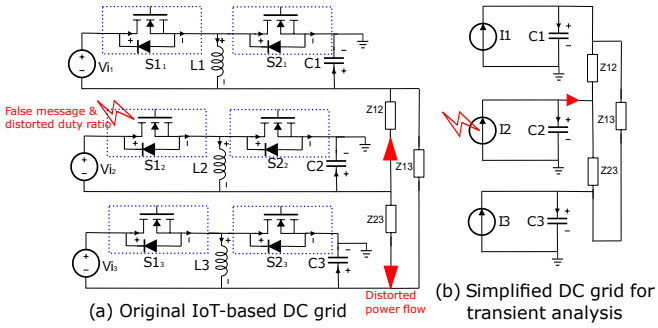


Fig. 1: IoT-based DC grid utilizing Buck-Boost converters

The rest of this paper is organized as follows. Section II represents general structure of an IoT-based converter-composed DC grid and corresponding attack categorization. Then IoT-based DC grid characteristics are analyzed in Section III, which provides theoretical foundation for attack detection mechanism discussed in Section IV. Simulation and hardware verification are implemented in Section V and a conclusion is provided in Section VI.

II. System Model

A. IoT-based DC Grid Model

The schematic of an IoT-based converter-composed DC grid is shown in Fig. 1a, and each converter is controlled by an independent agent. Its operation flow chart is illustrated in Fig. 2, where regular communication represented by blue links is mandatory to reach a power balancing consensus. Such coupling between power and communication networks make the whole DC grid as an IoT. For modeling simplification, it is assumed that the subsystem consists of a stable voltage source and a DC/DC converter, where the voltage source is considered an assemble of local generations and internal loads. The equivalent output power should keep regulated to follow the preceding consensus, otherwise the local stability would be claimed lost. MOSFETs and diodes are assumed ideal, so normally will the converter duty ratio determine its output voltage. Further discussion on converter topology flexibility has been given in Appendix A.

Switching signals are generated by local controllers. Once a stable power-sharing consensus is achieved, which contains

This article has been accepted for publication in IEEE Internet of Things Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2022.3220182

TABLE I: DC grid attack identification scheme comparison

Literature	Model-Based	Required Data	Converter Model	Attack Source Identification
[26], [27]	No	Reliable training data	-	**Yes**
[29]	**Yes**	Reliable reachable status sets	**Switching model**	No
[30]	**Yes**	Reliable predefined signal predicates	Average model	No
[31]	**Yes**	Reliable self sensor measurement data	**Switching model**	No
[32]	**Yes**	Reliable self sensor measurement data	Average model	No
[33]	**Yes**	Reliable neighbours' output current data	Average model	No
[34], [35]	**Yes**	**Non-reliable measurement data**	Average model	No
This paper	**Yes**	**Non-reliable measurement data**	**Switching model**	**Yes**

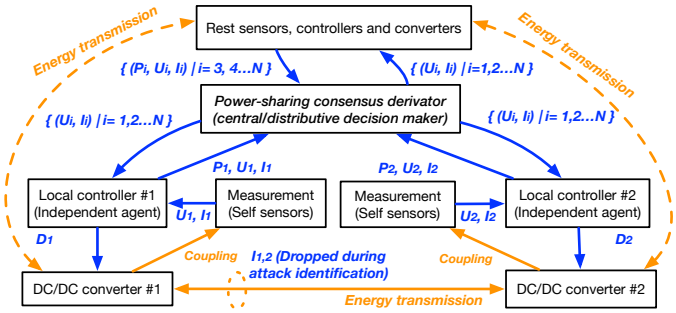


Fig. 2: IoT-based DC grid operation flow chart

the information of voltage distribution, the converter duty ratio should hold until receiving neighbours' authentication requests or following an updated consensus. More details about duty ratio adjustment conditions would be discussed later in Section IV. The DC power line adopted a Π-section model, hence relative terminal ground capacitance could be merged into nodal output ground capacitance. The line inductance is neglected for modelling simplification. In view of advanced modeling technology, relative parameters can be derived through active current injection from agents or specific functional sensors [36]. Since each agent can implement such measurement itself and cross-validation can be conducted during regular communication, the network admittance matrix is supposed to keep accessible and reliable even under attacks. There is no restriction on network topology, while every topology reconfiguration should notify all nodes in advance to ensure global information synchronization.

B. DC Grid Attack Model

As illustrated in Fig. 1a, the physical grid attack is intended to cause a divergence between perception and reality, revealed by distorted duty ratios and unexpected power flow. Physical grid attacks can be categorized into three patterns, including signal shielding, signal substitution and agent instigation.

1) Signal Shielding: Signal shielding attacks are intended to impose indirect malicious impacts on global stability. Under a long-term absence of measurement data and communication, the agent is highly potential to lose physical synchronization. Sensor destruction, cyber-link destruction and cyber-link jamming are typical attacking methods to shield signals. In communication protocol vulnerability analysis, the jamming attack is frequently discussed, for instance denial of service (DoS) and selective packet delay [37]. The influenced IoT-based DC grid operation flow chart is given by Fig. 24 in

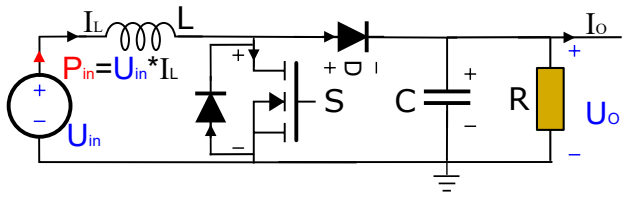


Fig. 3: Boost-converter-based subsystem schematic

Appendix B. Meanwhile, since cyber-link jamming may occur as well in normal scenarios, it should be tolerated in a short period.

2) Signal Substitution: Both sensor instigation and message substitution belong to signal substitution attacks, generating substituted signals to deceive all agents simultaneously. In case that a output voltage sensor was instigated to claim a below-actual value, the corresponding innocent agent would raise its own output voltage to follow the previous power-sharing consensus, injecting distorted power flow into its neighbours. In essence, signal substitution is considered a upgrade of signal shielding, as the front one can also realize communication and measurement blocking. The message substitution includes package manipulation and repetition, both of which are costly to implement due to mature communication authorization protocols. Meanwhile, combining with signal shielding, only a few cyber-links and sensors need to be focused, since relative agents have no choice but to rely on these links and sensors for communication and measurement. Such coordinated attacks would be more efficient compared to homogeneous attacks.

In order to inspect potentially shielded or substituted measurement signals in IoT-based DC girds, relative signals should be classified first as shown in Table II. The measurement sampling frequency is equal to or a few times over converter switching frequency, so it is unpractical to calculate the duty ratio simultaneously only based on the measurement data of a single sensor under this circumstance.

As illustrated in Fig. 3, considering subsystem injection power P_{in}, inductor current I_L, output current I_o can be estimated mutually, using given input voltage U_{in} and duty ratio D, only one sensor is mandatory. Once these four inter-dependent variables are manipulated simultaneously without violating their mutual relationship, the agent is considered blind, since there exists no trustworthy index to monitor P_{in}. If P_{in} is distorted, the subsystem internal power balance would be broken, leading to subsystem instability and even grid collapsing. Therefore, to avoid such dilemma, P_{in} is assumed constantly trustworthy to provide a reference to local stability,

This article has been accepted for publication in IEEE Internet of Things Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2022.3220182

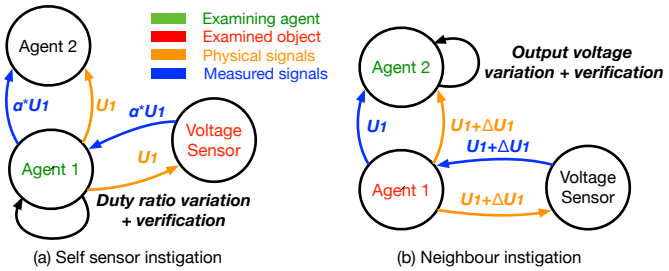


Fig. 4: Attack flow chart in IoT-based DC grids

and other two variable are considered auxiliary and assumed reliable once passing the mutual relationship check. In other words, unavailable signals monitoring I_L and I_o will impose no negative impacts on the proposed attack identification mechanism in this paper. Similarly, U_{in} and output voltage U_o can be estimated mutually.

TABLE II: Table of measurement signals in DC microgrids

Measurement	Trust level	Availability
Subsystem injection power	High	Yes
Inductor current / Output current	Medium	Flexible
Input voltage / Output voltage	Low	Yes
Neighbour output voltage	Low	Yes
Power line current	-	No

From the perspective of attackers, credible power line current sensors would help distinguish the source of malicious power injection quickly. Therefore grid attackers commonly pollute or block those data primarily to realize further attacks. If the polluted data are designed deceptive, an innocent agent can be easily slandered. So these signals would be put aside or assumed unavailable directly under attack identification. The trust levels and availability of all measurement signals are summarized in Table. II. A low trust level denotes relative measurement signals may be attacked and should be authenticated in advance of employment, and a high trust level distinguishes constantly trustworthy signals. Meanwhile, signals with a medium trust level are assumed reliable after checking with reliable P_{in}.

Since neighbour output voltage signals should be authenticated first by neighbours themselves, the signal substitution problem can be decomposed into independent self voltage sensor instigation problems accordingly. The affected IoT-based DC grid operation flow chart is given by Fig. 25 in Appendix B. For further illustration, the self-sensor instigation attack aims to manipulate output voltage measurement data thus misguiding the agent. Considering each local controller is able to vary its duty ratio actively, as illustrated in Fig. 4a, instigated self-sensors have to apply a constant amplifying ratio α to original measurement data U_1 for masking.

3) Agent Instigation: Under agent instigation attacks, those instigated agents will generate and distribute deceptive information actively, indicating a mismatching between its physical behavior and declaration from beginning to end. Compared to signal substitution attack, at least one agent has noticed deceptive signals initially before they have been broadcast. For classification, Byzantine attack and Sybil attack are distinguished from the ratio of instigated agents [38], [39]. Instead of instigating several nodes in Byzantine attack, Sybil attack indicates a high penetration ratio of traitors, eventually able to influence the preceding power-sharing consensus and slander innocent agents directly. Since Sybil attacks are commonly too expensive to implement, it would be not further investigated in this paper. The influenced DC microgrid operation flow chart under such attacks is given by Fig. 26 in Appendix B.

For a specific agent, the agent instigation attack is implemented by its neighbours, who manipulate and broadcast their own output voltage measurement data to provoke its incorrect actions. For In an IoT-based DC grid, an instigated agent would apply a constant voltage bias ΔU_1 to its claimed output voltage U_1, as illustrated in Fig. 4b. If those innocent neighbours request it to raise its output voltage, it must follow to avoid exposing itself. With a claimed underestimated voltage level, its neighbours will decrease their output voltage similarly according to the preceding power-sharing consensus. Afterwards, due to its actual high output voltage, excessive power will flow into those neighbours, finally destabilizing them and triggering their internal relay protectors.

In summary, self-sensor instigation and neighbour instigation are classical attacking patterns, both of which would be further discussed separately to exploit corresponding detection and identification strategies. No matter whether power line current signals are physically available or not, they will be ignored to avoid potential misjudgement.

III. Characteristic of IoT-based DC grids

After attack classification has been introduced, network characteristics should be analyzed as well for preparation of physical security strategy exploitation. Self sensor instigation attack is difficult to detect for an islanded agent, as linearly scaled measurement signals are immune to duty ratio variations, so the converter can be completely manipulated through deceptive voltage signal feedback. Whereas in an IoT-based DC grid, due to nonlinear properties imported from neighbouring converters, malicious signals are hard to mask themselves only by a linearization policy.

It is essential to figure out IoT-based DC grid characteristics with determined network parameters, which helps quantify a nonlinear relationship between some specific estimated and measured variables, providing a theoretical foundation of proposed strategies. Therefore, in this section, such nonlinear relationship would be imported through specific actions for preparation of future identification.

A. Discontinuous Current Mode (DCM)

A converter with fixed duty ratio D and input voltage U_{in} in continuous current mode (CCM) can be considered as a constant voltage source. Regarding a Boost converter, as illustrated in Fig. 5, its expected output voltage U_o can be derived directly. While for an unidirectional DC/DC converters, discontinuous inductor current is probable, especially considering a large voltage gap between two connected converters. With

This article has been accepted for publication in IEEE Internet of Things Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2022.3220182

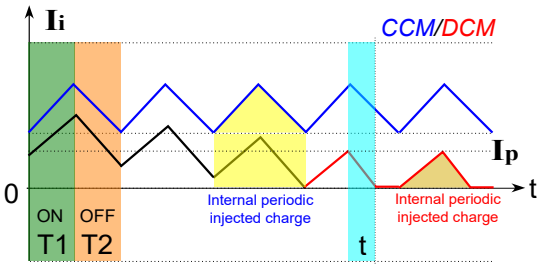


Fig. 5: Current profile of inductor in Boost converter

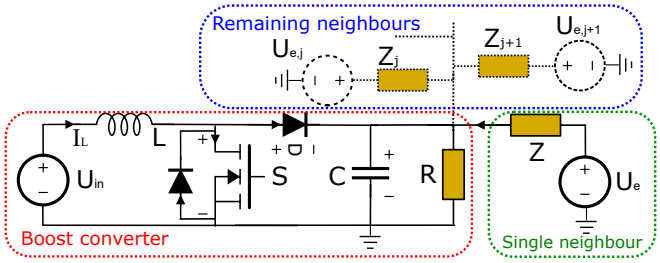


Fig. 6: Simplified DC grid using Boost converters

a low output voltage, its neighbours may force it to reduce output current and even work in DCM. A Boost converter in DCM with a single neighbour has been shown in Fig. 6, whose output voltage would be calculated based on power balancing rule (1) and sectional voltage-second balancing principle (2). U_e, Z are external voltage and connection line resistance. T denotes the switching period. t is the diode conducting period.

$$\underbrace{\frac{U_e - U_o}{Z} U_o T}_{\text{external injection}} + \underbrace{\frac{I_p}{2}(t + DT)U_{in}}_{\text{internal provision}} = \underbrace{\frac{U_o^2}{R} T}_{\text{load consumption}} \tag{1}$$

$$(U_o - U_i) \cdot t = U_i \cdot D \cdot T \tag{2}$$

Equation (1) and (2) can be combined as

$$U_o^2(\frac{1}{R} + \frac{1}{Z}) - U_o(\frac{U_{in}}{R} + \frac{U_{in} + U_e}{Z}) + (\frac{U_e U_{in}}{Z} - \frac{I_p U_{in} D}{2}) = 0$$
$$I_p = \frac{U_{in}}{L} DT \tag{3}$$

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

In order to derive a nontrivial U_o, it proposes

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

DCM constrain (5) should be checked as well after relative solutions $U_{o(1)}, U_{o(2)}$ are calculated.

$$t < (1 - D)T \tag{5}$$

Both $U_{o(1)}$ and $U_{o(2)}$ are stable solutions to U_o if they are real and meet (5). In real applications, the final stable value of U_o depends on converter initial status.

In an IoT-based DC grid case, a DCM converter may own more connections and its neighbours can be modeled as illustrated in the blue part of Fig. 6. Therefore (1) should be rewritten as

$$\sum_{j=1}^{J} \frac{U_{e,j} - U_o}{Z_j} U_o T + \frac{I_p}{2}(t + DT)U_{in} = \frac{U_o^2}{R} T \tag{6}$$

with J being the number of neighbouring agents.

Accordingly U_o becomes hard to calculate directly since agents' working status are mutually influenced. Considering potential DCM, it is irrational to simplify each neighbouring agent as a static voltage source. Intended for a stable solution, referring to Gaussian-Seidel method, an iterative algorithm is proposed to derive network voltage distribution as shown in Algorithm 1.

Algorithm 1: DCM voltage derivation

Result: $U_{o,1} \cdots U_{o,n}$
Initialize $U_{o,1}^{(0)} \cdots U_{o,N}^{(0)}$ as all converters are in CCM;
$i \leftarrow 0$, ϵ is error tolerance and m is iteration constraint;
$n \in \{1, 2\}$, $q \in \{1, 2, \cdots, J+1\}$;
while $\sum_{j=1}^{J+1} |U_{o,j}^{(i)} - U_{o,j}^{(i-1)}| \leq \epsilon$ *and* $i \leq m$ **do**
  $k \leftarrow 1$;
  while $k \leq J + 1$ **do**
    $\Omega \leftarrow \{U_{e,1}^{(i)} \cdots U_{e,J+1}^{(i)}\}$;
    $\Omega \leftarrow \Omega - \{U_{e,k}^{(i)}\}$;
    Solve U_o in (6) using Ω as $\{U_{e,1} \cdots U_{e,J}\}$;
    if $U_{o(1)}$ *or* $U_{o(2)}$ *is nontrivial* **then**
      Record nontrival solutions for callback;
      $U_{e,k}^{(i+1)} \leftarrow U_{o(n)}$, if $U_{o(n)}$ is nontrivial;
      Mark $U_{o(n)}$ as used for $U_{e,k}^{(i+1)}$;
    else
      if *unused nontrivial* $U_{e,q}^{(p)}$ $(p \leq i)$ *exists* **then**
        Recall unused nontrivial solutions;
        Update $U_{e,q}^{(p)}$, $i \leftarrow p$;
      else
        No DCM with such duty ratio;
        Break;
      end
    end
    $k \leftarrow k + 1$;
  end
  $i \leftarrow i + 1$;
end

B. Impulse Current Injection

Grid voltage vector $\mathbf{U}$ and current output vector $\mathbf{I}$ are coupled as $\mathbf{I} = \mathbf{YU}$ according to (7). Each agent can be simplified as a dynamic impulse current source as shown in Fig. 1(b). In a steady state, output average current I_{out}^i and converter inductor current I_{cov}^i in agent i keep constant. Intended to identify potential attacks, duty ratio variation is imported artificially and relative status variables would be observed. In such transition period, $\mathbf{I}$ can be decomposed into two parts in such a linear system, including the steady one and the transient one. y_{ij} is the admittance of power line between node i and node j. $\mathbf{Y}$ denotes the admittance matrix. N denotes the grid node number.

This article has been accepted for publication in IEEE Internet of Things Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2022.3220182

$$Y_{ij} = \begin{cases} -y_{ij} & i \neq j \\ \sum_{k=1}^{n} y_{ik} & i = j \end{cases}, \quad y_{ij} = \begin{cases} \frac{1}{z_{ij}} & E(i,j) \neq 0 \\ 0 & E(i,j) = 0 \end{cases} \tag{7}$$
$$\mathbf{U} = \begin{bmatrix} U_1 & U_2 & \dots & U_N \end{bmatrix}^T, \quad \mathbf{I} = \begin{bmatrix} I_1 & I_2 & \dots & I_N \end{bmatrix}^T$$

Regarding the transient part, I^i_{cov} is assumed quasi-constant in first several switching periods after duty ratio adjustment. Equation (8) can be derived in a Boost converter case. $\Delta\alpha_i$ denotes the variation of duty ratio. I^i_{imp} is the changing part of injection current caused by $\Delta\alpha_i$, and it is defined as an average value. With same grid parameters, the transient part of $\mathbf{U}$ is affine to I^i_{imp}. Due to a nonlinear relationship between I^i_{imp} and α_i, several feature parameters of transient voltage response would be also nonlinear to α_i, including peak value and its ramping coefficient.

$$\begin{aligned} \mathbf{I}_{imp} &= \begin{bmatrix} 0 & \dots & I^i_{imp} & \dots & 0 \end{bmatrix}^T \\ I^i_{imp} &= \Delta\alpha_i \cdot I^i_{cov} = -\Delta\alpha_i \cdot \frac{I^i_{out}}{1-\alpha_i} \\ \mathbf{CU}(s) &= \frac{\mathbf{I}_{imp}(s) - \mathbf{I}(s)}{s}, \quad \mathbf{C}[i,j] = \begin{cases} C_i & i = j \\ 0 & i \neq j \end{cases} \end{aligned} \tag{8}$$

C. Ripple Correlation

The injection current keeps in a pulsing shape. As shown in Fig. 7, instead of employing average value in Section III-B, injection current wave I^i_{sw} from agent i and global current wave vector $\mathbf{I}_{sw}$ can be decomposed into a series of positive and negative step functions as (9). All matrices and vectors in (9) are in size of $N \times N$ and $N \times 1$ respectively.

Through Laplace transform and substituting $\mathbf{I}_{sw}(s)$ by $\mathbf{I}_{imp}(s)$ in (8), voltage ripple distribution are able to be calculated. As grid parameters are asymmetrical in most scenarios, by taking peak-to-peak value of U_i as an index, it will vary differently even those two neighbours takes the same action separately. There would exist an nonlinear relationship between output voltage variation and ripple magnitude based on such estimation mechanism, which contributes to future attack identification.

$$\begin{aligned} &\mathbf{I}_{sw}(\mathbf{t}) = \sum_{n=0}^{\infty} \mathbf{E}(\mathbf{t} - n\mathbf{T})\mathbf{I}_p - \sum_{n=0}^{\infty} \mathbf{E}(\mathbf{t} - n\mathbf{T} - (\mathbf{e}-\mathbf{D})\mathbf{T})\mathbf{I}_p \\ &\mathbf{t} = \begin{bmatrix} t_1 & t_2 & \dots & t_N \end{bmatrix}^T, \quad \mathbf{T} = \begin{bmatrix} T_1 & T_2 & \dots & T_N \end{bmatrix}^T \\ &\mathbf{E}(\mathbf{t})[i,j] = \begin{cases} \mathbf{1}(\mathbf{t}[i]) & i = j \\ 0 & i \neq j \end{cases}, \quad \mathbf{1}(t) = \begin{cases} 1 & t \geq 0 \\ 0 & t < 0 \end{cases} \\ &\mathbf{I}_p = \begin{bmatrix} I^1_p & I^2_p & \dots & I^N_p \end{bmatrix}^T \\ &\mathbf{e}[i,j] = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}, \quad \mathbf{D}[i,j] = \begin{cases} D_i & i = j \\ 0 & i \neq j \end{cases} \\ &I^i_p = \frac{I^i_{out}}{1-D_i}, \quad I^i_{out} = \frac{U_i}{z_{ii}} - \sum_{E(i,j)\neq 0 \& i \neq j}^{N} \frac{U_j - U_i}{z_{ij}} \end{aligned} \tag{9}$$

where t_i represents synchronized time of agent i, equal to global standard time plus a constant switching phase delay

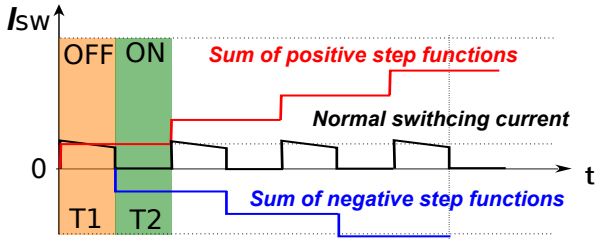


Fig. 7: Current decomposition for ripple estimation

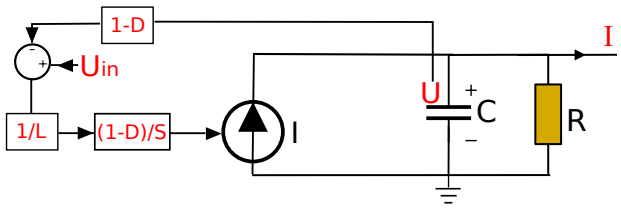


Fig. 8: Average model of Boost converter

duration. T_i is the switching period and I^i_p is the peak value of injection current.

D. Oscillation Correlation

In a 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 essential information regarding global status. Regarding a Boost converter scenario, using current-source model as shown in Fig. 8, grid injection current vector $\mathbf{I}$ and voltage vector $\mathbf{U}$ follow:

$$\begin{aligned} \mathbf{U}_{in} - (\mathbf{e}-\mathbf{D})\mathbf{U} &= \mathbf{L}\dot{\mathbf{I}} \\ (\mathbf{e}-\mathbf{D})\mathbf{I} - \mathbf{YU} &= \mathbf{C}\dot{\mathbf{U}} \end{aligned} \tag{10}$$

with

$$\mathbf{U}_{in} = \begin{bmatrix} U^1_{in} & \dots & U^i_{in} & \dots & U^N_{in} \end{bmatrix}^T \tag{11}$$

where U^i_{in} denotes the internal voltage of node i.

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

$$\begin{aligned} \ddot{\mathbf{I}} + \mathbf{C}^{-1}\mathbf{Y}\dot{\mathbf{I}} + (\mathbf{LC})^{-1}(\mathbf{e}-\mathbf{D})^2\mathbf{I} &= (\mathbf{LC})^{-1}\mathbf{YU}_{in} \\ s^2\mathbf{I} + s\mathbf{C}^{-1}\mathbf{YI} + (\mathbf{LC})^{-1}(\mathbf{e}-\mathbf{D})^2\mathbf{I} &= (\mathbf{LC})^{-1}\mathbf{YU}_{in} \end{aligned} \tag{12}$$

where $\mathbf{C}$ and $\mathbf{L}$ are diagonal matrices of nodal output capacitance C_i and internal inductance L_i. The definition of $\mathbf{e}$ and $\mathbf{D}$ inherits from (9).

$s-$domain equation in (12) can be reorganized as (13), with both $\mathbf{A}$ and $\mathbf{B}$ being constant $N \times N$ matrices in a determined DC microgrid.

$$\mathbf{AI} = \mathbf{B} \tag{13}$$

where

$$\begin{aligned} \mathbf{A}[i,j] &= \begin{cases} s^2 + sC_i^{-1}\sum_{k=1}^{N} Y_{ik} + (L_iC_i)^{-1}(1-D_i)^2 & i = j \\ -sC_i^{-1}Y_{ij} & i \neq j \end{cases} \\ \mathbf{B}[i] &= (L_iC_i)^{-1}\sum_{j=1}^{N} Y_{ij}U^j_{in} \end{aligned} \tag{14}$$

This article has been accepted for publication in IEEE Internet of Things Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2022.3220182

$\mathbf{A}$ owns full rank, so (13) can be represented as

$$\mathbf{I} = \mathbf{A}^{-1}\mathbf{B}, \quad \mathbf{A}^{-1}[i,j] \quad = \frac{(-1)^{i+j}\mathbf{M}[i,j]}{\det(\mathbf{A})} \tag{15}$$

where $\mathbf{M}[i,j]$ denotes a minor of $\mathbf{A}$.

Intended for further simplification, a certain hypothesis is mandatory as below:

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

$|\sum_{k=1}^{N} Y_{ik}|$ is equal to the absolute reciprocal of output ground resistance in node i. If the ground resistance is much lower than power line resistance, the hypothesis is satisfied naturally. Actually, such scenario frequently happen when subsystem internal energy consumption is mainly supported by self supply. Once node 1 is selected, since only oscillation part is extracted, its injection current $\mathbf{I}[1]$ can be approximated according to such hypothesis as given in (16). $o(\cdot)$ or $O(\cdot)$ denotes a lower or same order of error items compared to its input polynomial.

$$\begin{aligned} \det(\mathbf{A}) &\approx \prod_{i=1}^{N} \mathbf{A}[i,i] + o(s^{2N-2}) \\ \mathbf{M}[i,j] &\approx \begin{cases} \prod_{i=1, i\neq j}^{N} \mathbf{A}[i,i] + o(s^{2N-2}) & i = j \\ O(s^{2N-4}) & i \neq j \end{cases} \end{aligned} \tag{16}$$

Hence $\mathbf{I}[1]$ can be derived as

$$\begin{aligned} \mathbf{I}[1] &= \frac{\sum_{i=1}^{N} \mathbf{M}[i,j]\mathbf{B}[i]}{\det(\mathbf{A})} \approx \frac{\mathbf{B}[1](\prod_{i=2}^{N} \mathbf{A}[i,i] + o(s^{2N-2}))}{\prod_{i=1}^{N} \mathbf{A}[i,i] + o(s^{2N-2})} \\ &= \frac{\mathbf{B}[1]s^{2N-2} + o(s^{2N-2})}{s^{2N} + s^{2N-1}\sum_{j=1}^{N} m_j + s^{2N-2}\sum_{i=1}^{N} q_i + o(s^{2N-2})} \\ &\approx \frac{\mathbf{B}[1]}{s^2 + s\sum_{j=1}^{N} m_j + \sum_{i=1}^{N} q_i}, \quad m_j = \sum_{i=1}^{N} C_i^{-1} Y_{ij}, \\ q_i &= (L_i C_i)^{-1}(1 - D_i)^2 + \sum_{j=1}^{N} m_i m_j \end{aligned} \tag{17}$$

It is settled that $a = \sum_{j=1}^{N} m_j, b = \sum_{i=1}^{N} q_i$, then (17) can be converted into (18) through inverse Laplace transform, where $I_1(0)$ is the initial value of I_1. Obviously with a larger positive Δ, both its first oscillation period and peak values would be higher. Simultaneously, there exist a positive correlation between Δ and b.

$$I_1 = B_1 \cdot \frac{e^{-\frac{at}{2}} \sin(\sqrt{\Delta}t)}{\sqrt{\Delta}} + I_1(0), \quad \Delta \quad = b - \frac{a^2}{4} \tag{18}$$

Considering unstable and immeasurable nature of parasite components in most industrial microgrids, only various Δ in several scenarios need to be compared. Some oscillation feature values, for instance shooting current value and first oscillation period, can be sorted by estimation under a specific assumption that the tested agent is evil or innocent. Additionally, U_1 would share similar properties as derived likewise. Regarding a Buck-Boost converter scenario, $\mathbf{B}[i]$ should be considered as further discussed in Appendix C.

Those index values measured in different testing scenarios would be sorted as a sequence $\mathbf{S}$. The assumption whose estimation order $\hat{\mathbf{S}}$ is equal to $\mathbf{S}$ would be accepted, and those examined agents' identities can be determined. Moreover, for a symmetrical IoT-based DC grid composed of Boost converters, only duty ratio allocation influences Δ, indicating that exact system component parameters can be saved for identification.

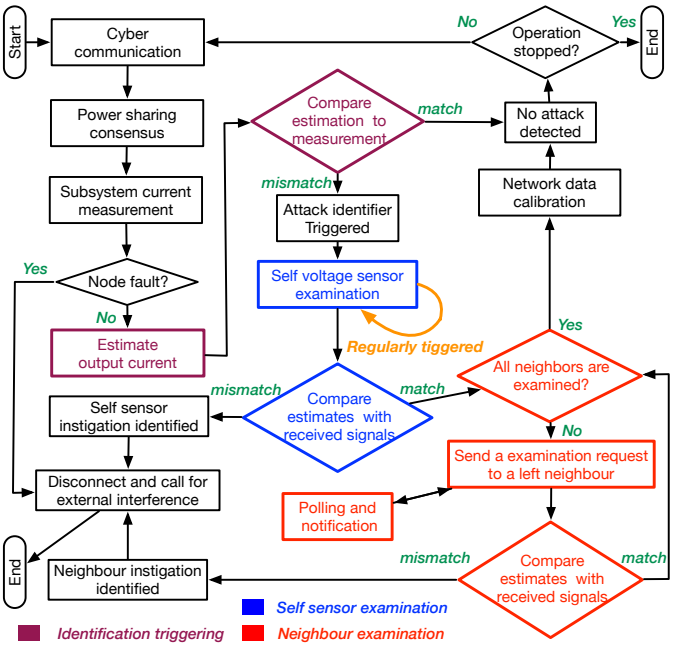


Fig. 9: Attack detection and identification flow chart

IV. Attack Detection and Identification

There is no detection strategy needed for an independent agent against signal shielding, as signal shielding can be directly detected and identified. Therefore only false date injection attacks would be discussed to investigate relative identification strategies in this paper, which include self-sensor instigation and neighbour instigation.

The attack detection and identification flow chart is proposed as given in Fig. 9. Theoretically, the performance of such algorithm depends on the accuracy of estimation index in each examination procedure, which is derived from known and reliable model parameters. In advance of attack detection, relay protection operates first to check grid faults. Without any fault detected by relay protectors, an event trigger is applied based on attack detection to save computation and communication resource before the decision of attack identification [40]. When received neighbour data are estimated incompatible with its own data according to (19), the attack identifier is triggered and attacking pattern would be classified. Designed for possible erroneous judgement in extreme scenarios, a time-triggered mechanism can be introduced to boost network immunity.

This article has been accepted for publication in IEEE Internet of Things Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2022.3220182

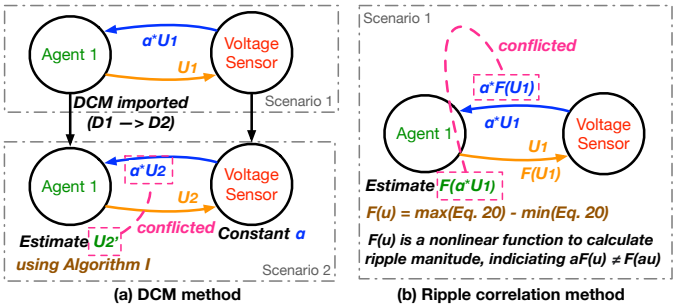


Fig. 10: Schematics of self-sensor examination

$$\hat{I}^i_{out} = Y_{ii}\hat{U}_i - \sum_{E(i,j)\neq 0 \& i\neq j}^{N} (\hat{U}_j - \hat{U}_i)Y_{ij} \tag{19}$$

where $\hat{I}^i_{out}$ 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 identification is separated into two parts, including self voltage sensor examination and neighbour examination. The identification procedures are implemented individually by the agent whose identifier is triggered, and its self-sensors and neighbors should coordinate to avoid potential misjudgment. The examining agent should broadcast its commands to avoid triggering other identifiers, and then start polling its neighbours to check whether examination period is available. Such polling mechanism should be designed and followed by all agents, referring to an universal communication protocol for instance IEC 61850 and Scalable MAC Protocol [41], [42].The disadvantage of such consensus is that an evil node may send requests maliciously to jam global action space. Trust mechanism designing in a distributive network is an open question, and trust on a certain cooperation request relies on action space redundancy [43]. A limited request frequency is considered an effective solution, even attack responding speed would be influenced.

In accordance with identification procedures in Fig 9, self-sensor examination is in advance of agent examination, since neighbour examination procedure can be prepared only based on trustworthy self signals. Moreover, with regularly triggered self-sensor examination, self-sensor examination can be skipped to accelerate identification. If no attack or fault is detected in final, network parameters Y and C should be calibrated based on impedance modeling methods [36]. Moreover, there is no restrictions on the converter controller type. If the agent utilizes a close-loop controller, relevant controller information must be broadcast to ensure its predictive switching behaviors, so that the attack identification flow chart keeps feasible. In this paper, all converter controllers are set open-loop for simplification, which will still not influence the validity of the proposed attack identification mechanism.

A. Self-Sensor Examination

Considering a hypothesis in Section II-B2, with a high switching frequency of semiconductor and similar higher

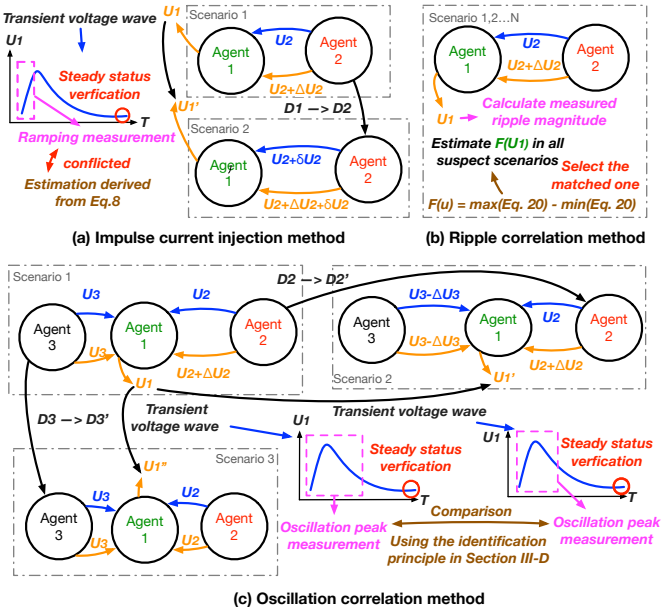


Fig. 11: Schematics of neighbour examination

voltage measuring frequency, no duty ratio can be measured directly in several switching periods. Since attacker are unable to predict the duty ratio variations, it has to provide proportional data constantly as shown in Fig. 9a.

1) DCM Examination: As mentioned in Section III-A, DCM will introduce a nonlinear relationship between input and output voltage. It will directly help distinguish spuriously scaled voltage data. A detailed illustration to DCM test for self-sensor examination is given in Fig. 10a, where a conflict between estimation and reception will expose the evil sensor.

2) Ripple Examination: Through comparing estimated ripple magnitudes using received signals as illustrated in Section III-C, a nonlinear relationship between output voltage and ripple magnitudes would help identify whether these signals are deceptive. If ripple magnitude is selected as the index, the ripple function should be calculated in advance according to (20), where a detailed definition of $\mathbf{I}_{sw}(t)$ can be founded in (9). As illustrated in Fig. 10b, the ripple magnitude function is nonlinear to self output voltage so that attack identification can be realized. In most scenarios, active voltage adjustment can be even saved if original status can help verify sensor data.

$$U_i(t) = \mathbf{I}^T_{sw}(t)\mathbf{Y}^{-1}\mathbf{e}_i \tag{20}$$

where

$$\mathbf{e}_i = \begin{bmatrix} 0 & \cdots & \underbrace{1}_{i\text{-th element}} & \cdots & 0 \end{bmatrix}^T \tag{21}$$

B. Neighbour Examination

Once self measurement signals have been authenticated and no evil sensor is recognized, evil neighbours should be identified. With scheduled active voltage adjustment, the instigated neighbour would be identified by its innocent neighbours only based on their own verified voltage measurement signals. As motioned in Section II-B3, the evil agent has no choice but

to adjust its output voltage according to received commands for attack masking, otherwise unmatched current data from the examining agent will expose the attacker. Even another attacker would mask the tested node through synchronized action, it will trigger other identifiers and both of them will be distinguished through cross validation of all innocent nodes. The key idea for neighbour examination is to restrict the action space of evil agents who has at least two neighbours where half of them are innocent. Such hypothesis is based on the definition of "Byzantine Attack".

1) Impulse Current Injection: During the transition period under active voltage adjustment, based on simplified circuits shown in Fig. 1b, global transient state vectors including voltage vector $\mathbf{U}$ and current output vector $\mathbf{I}$ can be solved as mentioned in Section III-B. A nonlinear relationship between $\Delta\mathbf{U}$ and $\Delta\mathbf{I}$ would help identify the potential attacker as illustrated in Fig. 11a. Such method is naturally serviceable for high power application due to high equivalent impulse current. Comparatively, the impulse response can be easily overlapped by switching ripples in low power scenarios.

Neighbour examination speed using this scheme is accelerated as well since it only uses a few sampling points at the start of voltage variation. If the received signals fail to match the estimated ones, the evil neighbour can be detected directly. Meanwhile, without attacker detected in the beginning, steady status verification is still mandatory to ensure that relevant agents have acted as expected.

2) Ripple Examination: The ripple estimation for neighbour examination is similar to that for self examination mentioned in Section IV-A2, while it is set event-triggered. A detailed examination schematic has been given in Fig. 11b.

3) Oscillation Examination: As discussed in Section. III-D, through comparing corresponding Δ and $\mathbf{B}[i]$, the order of feature values in various scenarios, for instance shooting value or first oscillation period, can be estimated under a specific assumption. If the estimated order $\hat{\mathbf{S}}$ mismatch $\mathbf{S}$, the previous hypothesis would be rejected. Another hypothesis would be proposed and examined continuously until $\hat{\mathbf{S}} = \mathbf{S}$.

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.

V. Validation and Discussion

In order to verify proposed methods in Section IV, both simulation test on SIMULINK and hardware test on dSpace platform have been implemented, separately in Buck-Boost and Boost converter scenarios. Detailed discussion was provided when comparing theoretical solutions with experimental data, eventually proving the efficacy of proposed methods.

A. Simulation Verification

Regarding a 4-node IoT-based DC grid whose topology is given in Fig. 12a, Buck-Boost converters are employed.

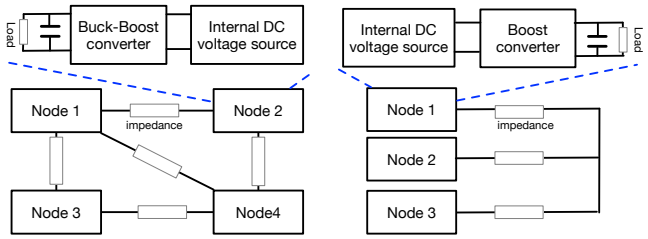


Fig. 12: Simulation and hardware testing IoT-based DC grids

TABLE III: Table of simulation system parameters

Parameter	Value	Meaning
f_{sw}/R_{load}	10 kHz / 64 Ω	Switching frequency / Load resistance
R_{line}/L_{line}	2 Ω / 5 mH	Line series resistance / inductance
V_{in}/C	800 V / 0.5 mF	Input voltage / Output capacitance
R_{mos}/R_{dio}	0.2 Ω / 0.2 Ω	Switcher / Diode conducting resistance
L	0.2 H	Inner inductance of converter

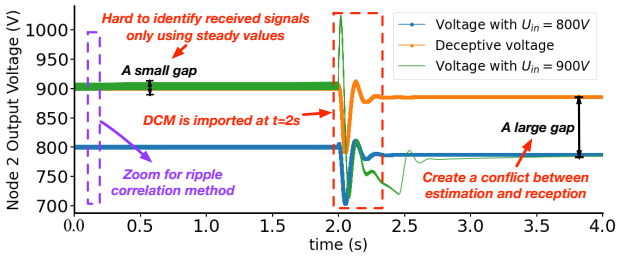


Fig. 13: Voltage waves in Node 2 for DCM examination

Relevant parameters of simulation system are listed in Table III. The sampling frequency is variable between 10 kHz to 100 kHz.

1) Self Sensor Examination: As mentioned in Section IV-A, self sensor examination can be implemented based on DCM method or ripple correlation method. Node 2 is assumed being attacked in this case. Even that its ideal output voltage equals 800V under a duty ratio of 0.5, its own sensor would declare it 900 V with a constant amplifying ratio of 1.125. Under this circumstance, if the voltage sensor is assumed innocent, the internal voltage would be derived as 900 V, otherwise it would be equal to 800 V. With the proposed attack detection and identification framework, due to inequality of (19), such deception would trigger Node 2's own attack identifier.

a) DCM: All Buck-Boost converters employed are assumed unidirectional when applying the DCM method. D_2 is adjusted to 0.4 to import DCM. Through running Algorithm 1 and importing DCM, estimated and received output voltage waves are recorded in Fig. 13. As illustrated in Table IV, such action would lead to an obvious difference between deceptive signals and estimated values, which can be received from sensors and derived by Algorithm 1 separately. Accordingly self sensor attack is detected and the instigated sensor is identified. In this case, the voltage gap is up to 101.43 V, accounting over 10% of standard voltage.

b) Ripple Correlation: Without active voltage adjustment, using a zoomed region in Fig. 13, ripple correlation

This article has been accepted for publication in IEEE Internet of Things Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2022.3220182

TABLE IV: Table of DCM estimation and simulation results

Parameter	Value
Original U_2 with U_{in} = 800 V/900 V	801.15 V / 886.23 V
Original / Updated deceptive U_2	901.30 V / 886.23 V
Updated U_2 with U_{in} = 800 V/900 V	910.57 V / 784.80 V

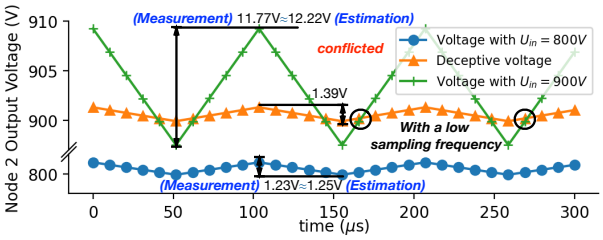


Fig. 14: Voltage ripples in Node 2 for ripple examination

method can be applied for self sensor examination as illustrated in Fig. 14. If the sensor is instigated, the voltage ripple magnitude from reception is 1.39 V while that from estimation is up to 11.10 V. Such an obvious conflict will help identify the instigated voltage sensor. According to simulated values from Fig. 14 and estimated values from Fig. 10b, both the estimation ratio errors are lower than 3.9%. The accuracy of ripple correlation estimation has been verified in this case.

A sampling frequency of 100 kHz is selected during ripple magnitude estimation. Instead, with a low sampling frequency of 10 kHz, the ripple magnitude is difficult to calculate as shown in black circles at Fig. 14. Even with a high sampling frequency, the expected ripple magnitude accuracy can only account less than 0.02% of standard voltage range. The ripple correlation method for self sensor examination may save active voltage adjustment, while it sets a high requirement on sampling frequency and measurement accuracy.

2) Neighbourhood Examination: Agent 2 was picked as an instigated agent, who tried to steal energy and adopted a constant negative output voltage bias. According to Fig. 9, with self sensor authenticated, Neighbour 1 would send a voltage adjustment request afterwards. Agent 2 had no choice but to adjust voltage accordingly, while the mismatched output voltage data of Agent 1 would reveal Agent 2's guilty. The examination parameters are given in Table V. Agent 1 has detected there may exist a voltage bias of -266.7 V from Agent 2 if it is assumed an traitor. Accordingly Agent 2 is requested to raise its voltage by 266.7 V. Simulated output voltage waves in various scenarios are plotted in Fig. 15.

TABLE V: Table of neighbour examination parameters

Scenario	Reality	Parameter	Value
1	Agent 2 is evil	Original D_2 / U_2	0.4 / 533.3 V
		Updated D_2 / U_2	0.5 / 800 V
		D_4 / U_4	0.5 / 800 V
2	Agent 2 is innocent	Original D_2 / U_2	0.5 / 800 V
		Updated D_2 / U_2	0.571 / 1066.7 V
		D_4 / U_4	0.4 / 533.3 V

a) Impulse Current Injection: As Agent 2 raised voltage accordingly, relative voltage measurement data were recorded

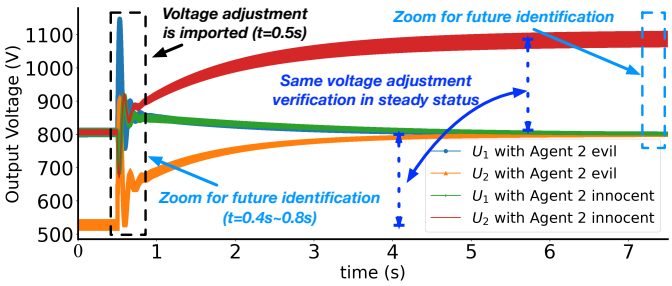


Fig. 15: Voltage waves in various scenarios

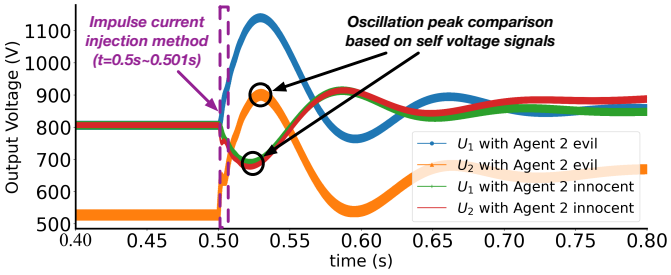
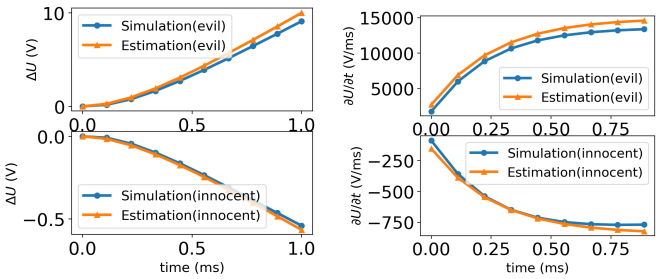


Fig. 16: Zoomed voltage waves in various scenarios



(a) (b)

Fig. 17: Indices derived by Agent 1 in various scenarios

and plotted in Fig. 16. In impulse current injection method, only the first millisecond measurement data after voltage adjustment would be utilized for identification. The sampling frequency can be as low as 10 kHz. Derivative of output voltage can be calculated to distinguish voltage ramping tendencies during the transition period. Both values under various circumstances have been given as blue lines in Fig. 17.

Whether Agent 2 was cheating, Agent 1 would estimate its future voltage variation after relative nodes' action as shown in orange lines in Fig. 17a. The mathematical solution of Agent 1 voltage derivative in various scenarios could be calculated accordingly as shown by orange lines in Fig. 17b. It can be concluded that the theoretical and simulation results in the same scenario matched well, indicating a high identification accuracy]. A large divergence between indices in various scenarios verified the efficacy of such method.

b) Ripple Correlation: Through zooming the last 300 μs in Fig. 15, Fig. 18 illustrates voltage ripples in various scenarios. There exists a gap of ripple magnitude under various assumptions, especially using U_2 as an identification index. The estimated values derived according to Section III-C also

This article has been accepted for publication in IEEE Internet of Things Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2022.3220182

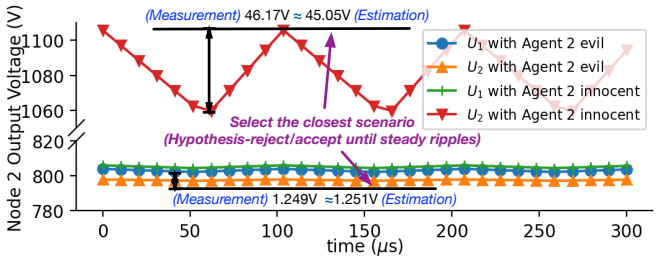


Fig. 18: Voltage ripples for neighbour examination

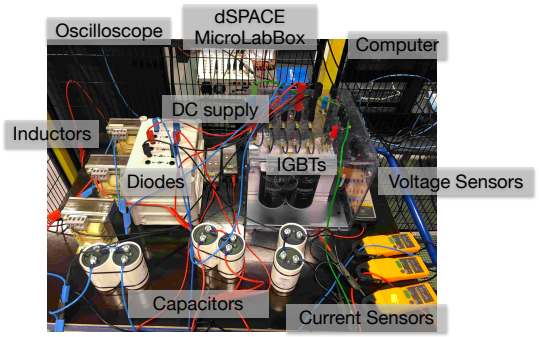


Fig. 19: IGBT-based hardware testing platform

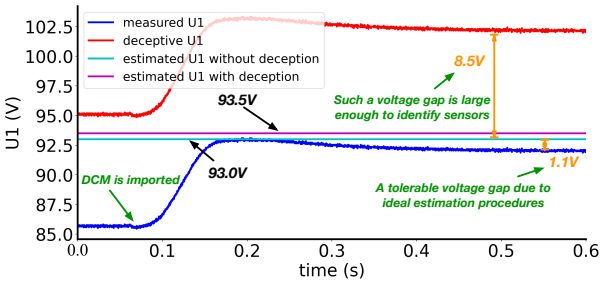


Fig. 20: Voltage waves during self sensor examination

match the simulated ones well, where both the estimation ratio errors are lower than 2.4%, indicating the reliability of ripple correlation method. Meanwhile, the requirement of a high sampling frequency and accuracy limits its application.

c) Oscillation Correlation: According to Section III-D and Appendix C, only $\mathbf{B}[i]$ and Δ should be focused, both of which rely on duty ratio distribution. In Fig. 16, A hypothesis that Agent 2 is evil in Scenario 1 was proposed. Under such hypothesis, B_2 in Scenario 1 will be larger than that in Scenario 2, as this B_2 is linear to injection current from Agent 2 in a twin grid whose voltage distribution is changed to **DU**. Since Δ in Scenario 1 is also larger than that in Scenario 2, oscillation peak magnitude of U_2 in Scenario 1 is estimated larger than that in Scenario 2 correspondingly. Such order match the simulated result, so the hypothesis is accepted and Agent 2 is identified evil in Scenario 1.

3) Summary: In summary, in such simulation case, only depending on non-reliable measurement data, all proposed attack identification strategies have been verified. Meanwhile, attack detection methods in previous literature listed in Table I would fail to identify attack signal sources, as all these methods still mainly focus on attack detection and skip the procedure of authentication.

B. Hardware Verification

In hardware test part, a Boost-converter-composed DC microgrid is established according to Fig.12b and investigated as illustrated in Fig. 19. The basic parameters of such platform are listed in Table VI. Due to power and measurement limit of such platform, impulse current response is too small to observe and accurate ripple magnitude measurement is unachieved. That explains why only DCM and oscillation examination are adopted in this experiment. Actually, due to physical limits in real DC microgrids, not all attack identification methods are applicable in a specific scenario.

TABLE VI: Table of hardware system parameters

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

1) DCM Examination: External voltage lifting for self DCM introduction is implemented in this case. The system status parameters are listed in Table VII, where the attacking sensor lied that Agent 2's inner voltage level is $100V$. With Agent 1 lifting its own output voltage, Agent 2 is in DCM. Relative voltage waves are measured and plotted in Fig. 20. As shown in Table VII, a large voltage gap exist between deceptive signals and estimated signals, eventually helping Agent 2 identify its own voltage sensor. Moreover, the estimated voltage is close to the corresponding measured one, where the estimating ratio error is only 1.2%, avoiding misjudging innocent sensors.

TABLE VII: Table of estimation and simulation results

Parameter	Value
Voltage signal amplifying ratio	1.11
Original duty ratio of Agent 1 / 2 / 3	0.32 / 0.09 / 0.32
Updated duty ratio of Agent 1	0.46
Estimated U_2 with $V_{in} = 80$ V / 100 V	93.0 V / 93.5 V
Measured/Deceptive U_2 with $V_{in} = 80$ V	91.9 V / 112.0 V

2) Oscillation Examination: The neighbour attack and action parameters are listed in Table VIII. Due to unknown parasite inductance in such system, oscillation correlation method is adopted for neighbour examination. Considering symmetrical topology of this system, only the sum of $(1-D_i)^2$ are calculated and compared. The scenario that Node 2 is evil owns a higher sum of $(1 - D_i)^2$, accordingly indicating a higher Δ .

As discussed in Section III-D, if Δ is positive, ΔT_{I1} and $|\Delta I_1|$ should be positive, then it can be derived that under a assumption that Agent 2 is evil, ΔT_{U1},ΔT_{I1},$|\Delta U_1|$ and $|\Delta I_1|$ in Scenario 1 should be larger those in Scenario 2. Through comparing specific indices, all comparisons match only theoretically estimated ones, especially $|\Delta I_1|$ is most

This article has been accepted for publication in IEEE Internet of Things Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2022.3220182

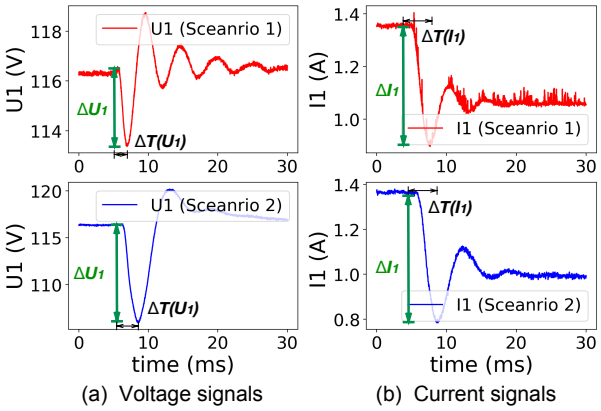


Fig. 21: Measurement data during neighbour examination

TABLE VIII: Table of theoretical examination parameters

Assumption	Parameter	Value
Before action	original D_1 / D_2 / D_3 original U_1 /U_2 /U_3 (V)	0.32 / 0.09 / 0.32 132.4 / 98.9 / 132.4
Evil agent 2 (#1)	updated D_2 / U_2	0.32 / 132.4 V
Innocent agent 2 (#2)	updated D_3 / U_3	0.46 / 166.7 V

different, and a higher $|\Delta I_1|$ under negative Δ indicates that Agent 2 is innocent. The measurement data in various scenarios during hardware testing are illustrated in Fig. 21.

During hardware testing, the action starting timestamp cannot be clarified, so certain points should be selected and processed to calculate corresponding parameters as shown in Table IX. All index comparison results have met the estimated ones based on an assumption that Agent 2 is evil. While such selection can be tricky considering fluctuating measurement signals. Hence in this scenario, it is recommended to adopt the oscillation peak magnitude as an index for comparison. The derived identification results especially based on $|\Delta U_1|$ still consist with the facts. The efficacy of proposed oscillation examination methods has been verified.

TABLE IX: Table of measurement data and indices

Scenario	Parameter	Value
#1 Assume Agent 2 is evil Action starts at t=5.1 ms	U_1 I_1 ΔT_{I1} / ΔT_{I1} ΔU_1 / ΔI_1	116.306 V→113.407 V 1.346A→0.913A 1.7ms / 2.8ms -2.899 V / -0.433 A
#2 Assume Agent 2 is innocent Action starts at t=6.0 ms	U_1 I_1 ΔT_{I1} / ΔT_{I1} ΔU_1 / ΔI_1	116.398 V→106.662 V 1.343 A→0.787 A 3.0 ms / 2.8 ms -9.736 V / -0.556 A

3) Summary: In summary, both DCM examination and oscillation examination have been verified in this experimental testing case, even on the basis of the limited sampling frequency and accuracy. Comparatively, identification methods in previous literature listed in Table I still fail to realize attack identification, as no authentication procedure is considered.

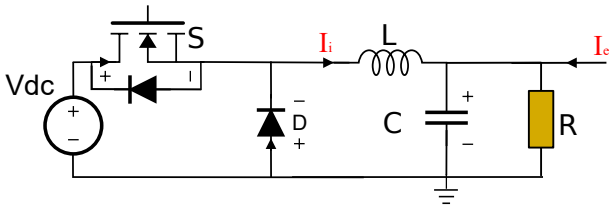


Fig. 22: Schematic of unidirectional Buck converter

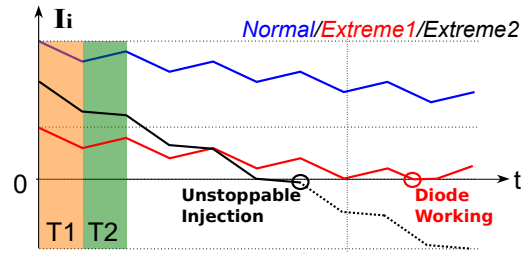


Fig. 23: Current profile of inductor in Buck converter

VI. Conclusion

This article has presented a novel attack detection and identification mechanism for IoT-based converter-composed DC grids. 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 investigated and tested by both simulation and hardware experiments. The low estimation ratio error keeps lower than 3.9% according to the validation works in this paper. The success in attacker recognition under various attacking patterns illustrates the efficacy of proposed methods. For an IoT-based DC grid with determined parameters, voltage or current response under each identification strategy can be estimated in advance, hence the strategy with the most distinguished evidence is preferred. Through flexible strategy selection, the whole attack identification system is robust and efficient in all testing scenarios.

In future, more feature values calculated from measurable data in IoT-based DC grids would be exploited, intended to extend the bank of attack identification indices. Moreover, the proposed mechanism can be integrated into an connection authorization protocol in IoT-based power systems, where communicators between REGs and EV chargers are in demands to support smart grid services.

Appendix A
Converter Topology Flexibility in DC Microgrids

Regarding the topology of DC/DC converters, a conventional unidirectional Buck converter is not recommended. As illustrated in Fig. 22, when the external injection current I_e raises, I_i flowing in inductor L will drop. In normal scenariosI_i keeps positive, while it would become negative in extreme scenarios as shown in Fig. 23. Unfortunately, if I_e is large enough to push capacitor voltage higher than input voltage V_{dc} transiently, there would exist unstoppable inverse I_i, eventually leading to continuous current injection even the switcher turns off.

This article has been accepted for publication in IEEE Internet of Things Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2022.3220182

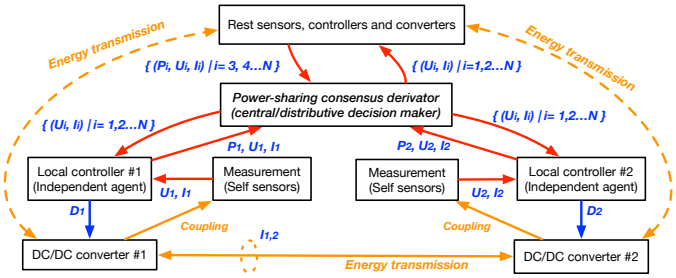


Fig. 24: Flow chart under signal shielding attack

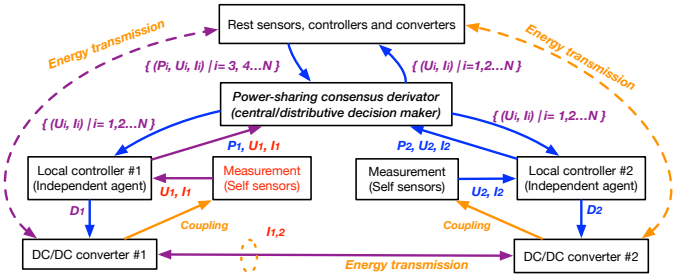


Fig. 25: Flow chart under signal substitution attack

Intended to ensure a controllable subsystem, the switcher should be selected unidirectional itself or be in series with a diode. Instead, unidirectional Boost and Buck-Boost converters are robust against shooting injection current. Bidirectional DC/DC converters are flexible with these three typologies to avoid uncontrollable current injection. The selection between unidirectional and bidirectional converters depends on the budget and specific demands, particularly considering bidirectional converters will disable part of detection methods.

APPENDIX B
INFLUENCED DC MICROGRID OPERATION FLOW CHARTS

The influenced DC microgrid operation flow charts under different attacking patterns are given in Fig. 24-26. Different colours are adopted to indicate various status of the same component, which are further illustrated in Table X.

TABLE X: Table of colour indications

Object	Colour	Meaning
Links	Blue	Healthy cyber-links
	Orange	Healthy physical connections
	Red	Distorted cyber-links / physical connections
	Purple	Cyber-links containing distorted messages
Signals	Blue	Innocent signals
	Red	Arbitrarily modified signals
	Purple	Indirectly distorted signals

APPENDIX C
OSCILLATION CORRELATION IN BUCK-BOOST SCENARIOS

The grid injection current vector $\mathbf{I}$ and voltage vector $\mathbf{U}$ in a Buck-Boost scenario follow:

$$\mathbf{D}\mathbf{U}_{in} - (\mathbf{e} - \mathbf{D})\mathbf{U} = \mathbf{L}\dot{\mathbf{I}} \tag{22}$$

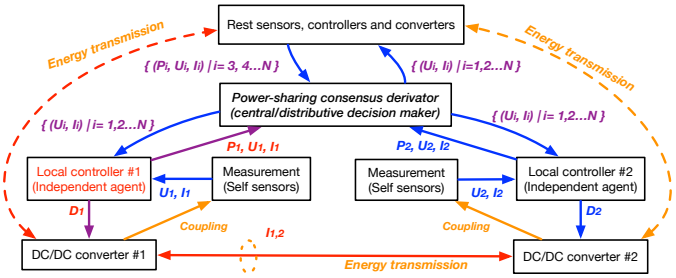


Fig. 26: Flow chart under agent instigation attack

Accordingly $\mathbf{U}_{in}$ and B_1 in Section III-D are updated as

$$\begin{aligned} &\mathbf{D}\mathbf{U}_{in} \longrightarrow \mathbf{U}_{in} \\ &B_1 = (L_1 C_1)^{-1} \sum_{j=1}^{N} Y_{1j} D_j U_{in}^j \end{aligned} \tag{23}$$

According to (18), it can be derived that both Δ and B_1 would influence oscillation feature variables. Specially, both Δ and B_1 own a positive relationship with oscillation peak value.

REFERENCES

[1] A. Makkieh, G. Burt, R. Pena Alzola, *et al.*, *DC Networks on the Distribution Level – New Trend or Vision?* (DC Distribution Networks), English. CIRED, Sep. 2021.

[2] A. Ginart and B. Sharifipour, "High penetration of electric vehicles could change the residential power system: Public dc fast chargers will not be enough.," *IEEE Electrific. Mag.*, vol. 9, no. 2, pp. 34–42, 2021.

[3] P. Sanjeev, N. P. Padhy, and P. Agarwal, "Peak energy management using renewable integrated dc microgrid," *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 4906–4917, 2017.

[4] 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.

[5] L. Sun, W. Huang, R. Li, *et al.*, "Capacity and volume balance of buffering converters for the marine pulsed power system," *IEEE Trans. Ind. Electron.*, 2022.

[6] F. Perez, A. Iovine, G. Damm, *et al.*, "Stability analysis of a dc microgrid for a smart railway station integrating renewable sources," *IEEE Trans. Control Syst. Technol.*, 2019.

[7] N. Ertugrul and D. Abbott, "DC is the future," *Proc. IEEE*, vol. 108, no. 5, pp. 615–624, 2020.

[8] McKinsey. " Transformation of Europe's power system until 2050." (2010), [Online]. Available: https://www.mckinsey.com/~/media/mckinsey/dotcom/client_service/epng/pdfs/transformation_of_europes_power_system.ashx.

[9] M. Neaimeh and P. B. Andersen, "Mind the gap-open communication protocols for vehicle grid integration," *Energy Informatics*, vol. 3, no. 1, pp. 1–17, 2020.

[10] J. Zhou, M. Shi, Y. Chen, *et al.*, "A novel secondary optimal control for multiple battery energy storages in a dc microgrid," *IEEE Trans. Smart Grid*, 2020.

[11] J. Sun, W. Lin, M. Hong, and K. A. Loparo, "Voltage regulation of dc-microgrid with pv and battery," *IEEE Trans. Smart Grid*, 2020.

[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. Sarangi, B. K. Sahu, and P. K. Rout, "A comprehensive review of distribution generation integrated dc microgrid protection: Issues, strategies, and future direction," *International Journal of Energy Research*, vol. 45, no. 4, pp. 5006–5031, 2021.

[14] L. Xing, "Reliability in internet of things: Current status and future perspectives," *IEEE Internet Things J.*, vol. 7, no. 8, pp. 6704–6721, 2020.

[15] M. Farhoumandi, Q. Zhou, and M. Shahidehpour, "A review of machine learning applications in iot-integrated modern power systems," *The Electricity Journal*, vol. 34, no. 1, p. 106 879, 2021.

[16] H. Zhang, B. Liu, and H. Wu, "Smart grid cyber-physical attack and defense: A review," *IEEE Access*, vol. 9, pp. 29 641–29 659, 2021.

[17] H. Xu, Y. Lin, X. Zhang, and F. Wang, "Power system parameter attack for financial profits in electricity markets," *IEEE Trans. Smart Grid*, vol. 11, no. 4, pp. 3438–3446, 2020.

[18] S. Tan, J. M. Guerrero, P. Xie, *et al.*, "Brief survey on attack detection methods for cyber-physical systems," *IEEE Syst. J.*, 2020.

[19] S. Sridhar and M. Govindarasu, "Model-based attack detection and mitigation for automatic generation control," *IEEE Trans. Smart Grid*, vol. 5, no. 2, pp. 580–591, 2014.

[20] L.-Y. Lu, H. J. Liu, H. Zhu, and C.-C. Chu, "Intrusion detection in distributed frequency control of isolated microgrids," *IEEE Trans. Smart Grid*, vol. 10, no. 6, pp. 6502–6515, 2019.

[21] M. Dehghani, M. Ghiasi, T. Niknam, *et al.*, "False data injection attack detection based on hilbert-huang transform in ac smart islands," *IEEE Access*, vol. 8, pp. 179 002–179 017, 2020.

[22] E. Drayer and T. Routtenberg, "Detection of false data injection attacks in smart grids based on graph signal processing," *IEEE Syst. J.*, vol. 14, no. 2, pp. 1886–1896, 2019.

[23] L. Liu, M. Esmalifalak, Q. Ding, *et al.*, "Detecting false data injection attacks on power grid by sparse optimization," *IEEE Trans. Smart Grid*, vol. 5, no. 2, pp. 612–621, 2014.

[24] J. James, Y. Hou, and V. O. Li, "Online false data injection attack detection with wavelet transform and deep neural networks," *IEEE Trans. Ind. Informat.*, vol. 14, no. 7, pp. 3271–3280, 2018.

[25] R. Jiao, G. Xun, X. Liu, and G. Yan, "A new ac false data injection attack method without network information," *IEEE Trans. Smart Grid*, vol. 12, no. 6, pp. 5280–5289, 2021.

[26] M. R. Habibi, H. R. Baghaee, T. Dragicevic, F. Blaabjerg, *et al.*, "Detection of false data injection cyber-attacks in dc microgrids based on recurrent neural networks," *IEEE J. Emerg. Sel. Top. Power Electron*, 2020.

[27] M. R. Habibi, H. R. Baghaee, F. Blaabjerg, and T. Dragicevic, "Secure mpc/ann-based false data injection cyber-attack detection and mitigation in dc microgrids," *IEEE Syst. J.*, 2021.

[28] R. S. Singh, S. Cobben, and V. Ćuk, "Pmu-based cable temperature monitoring and thermal assessment for dynamic line rating," *IEEE Trans. Power Del*, vol. 36, no. 3, pp. 1859–1868, 2020.

[29] O. A. Beg, T. T. Johnson, and A. Davoudi, "Detection of false-data injection attacks in cyber-physical dc microgrids," *IEEE Trans. Ind. Informat.*, vol. 13, no. 5, pp. 2693–2703, 2017.

[30] O. A. Beg, L. V. Nguyen, T. T. Johnson, and A. Davoudi, "Signal temporal logic-based attack detection in dc microgrids," *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 3585–3595, 2018.

[31] M. Ghiasi, M. Dehghani, T. Niknam, *et al.*, "Cyber-attack detection and cyber-security enhancement in smart dc-microgrid based on blockchain technology and hilbert huang transform," *IEEE Access*, vol. 9, pp. 29 429–29 440, 2021.

[32] S. Tan, P. Xie, J. M. Guerrero, *et al.*, "Attack detection design for dc microgrid using eigenvalue assignment approach," *Energy Reports*, vol. 7, pp. 469–476, 2021.

[33] S. Sahoo, S. Mishra, J. C.-H. Peng, and T. Dragičević, "A stealth cyber-attack detection strategy for dc microgrids," *IEEE Trans. Ind. Electron.*, vol. 34, no. 8, pp. 8162–8174, 2018.

[34] A. J. Gallo, M. S. Turan, F. Boem, *et al.*, "A distributed cyber-attack detection scheme with application to dc microgrids," *IEEE Trans. Automat. Contr.*, vol. 65, no. 9, pp. 3800–3815, 2020.

[35] M. Liu, C. Zhao, Z. Zhang, *et al.*, "Converter-based moving target defense against deception attacks in dc microgrids," *IEEE Trans. Smart Grid*, 2021.

[36] T. Roinila and T. Messo, "Online grid-impedance measurement using ternary-sequence injection," *IEEE Trans. Ind. Appl.*, vol. 54, no. 5, pp. 5097–5103, 2018.

[37] B. Moussa, M. Debbabi, and C. Assi, "Security assessment of time synchronization mechanisms for the smart grid," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 1952–1973, 2016.

[38] 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.

[39] J. R. Douceur, "The sybil attack," in *International workshop on peer-to-peer systems*, Springer, 2002, pp. 251–260.

[40] L. Ding, Q.-L. Han, X. Ge, and X.-M. Zhang, "An overview of recent advances in event-triggered consensus of multiagent systems," *IEEE Trans. Cybern.*, vol. 48, no. 4, pp. 1110–1123, 2017.

[41] B. Ismaiel, M. Abolhasan, W. Ni, *et al.*, "Analysis of effective capacity and throughput of polling-based device-to-device networks," *IEEE Trans. Veh. Technol.*, vol. 67, no. 9, pp. 8656–8666, 2018.

[42] S. S. Hussain, T. S. Ustun, and A. Kalam, "A review of iec 62351 security mechanisms for iec 61850 message exchanges," *IEEE Trans. Ind. Informat.*, 2019.

[43] 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.