Electric Power Systems Research 214 (2023) 108888

Contents lists available at ScienceDirect

Electric Power Systems Research

journal homepage: www.elsevier.com/locate/epsr

Secondary frequency control strategy considering DoS attacks for MTDC system☆

Yunning Zhang [a], Le Wei [a], Wenlong Fu [a,b,*], Xi Chen [a], Songlin Hu [c]

[a] School of Electrical and New Energy, China Three Gorges University, Yichang 443002, Hubei Province, China
[b] Hubei Provincial Key Laboratory for Operation and Control of Cascaded Hydropower Station, China Three Gorges University, Yichang 443002, Hubei Province, China
[c] Institute of Advanced Technology for Carbon Neutrality, Nanjing University of Posts and Telecommunications, Nanjing 210003, Jiangsu Province, China

ARTICLE INFO

Keywords:
MTDC systems
Secondary frequency control
Cyber security
Denial of service attacks

ABSTRACT

The utilization of communication networks brings benefits to frequency support strategies for multi-terminal high voltage direct current (MTDC) systems, yet leads to the systems facing cyber security risks. In particular, the denial of service (DoS) attacks will cause loss of measured signals and make the MTDC system unstable. This paper is concerned with the secondary frequency control problem defending DoS attacks in MTDC systems. Focusing on energy-limited and periodic DoS attacks, a Bernoulli process model is firstly adopted, and the control objective considering DoS attacks is built. Thereafter a switching scheme of the attacked station from droop control to secondary frequency regulation is devised for frequency support of MTDC systems. Two strategies respectively using the reference value and the data of the previous time interval are then proposed to compensate for the lost data due to DoS attacks. Four scenarios are simulated on a four-terminal MTDC system to verify the effectiveness of the two proposed solutions. The results show that, if the system is in equilibrium states during DoS attacks, both of the two proposed strategies are effective. Whereas the solution using the data of the previous time interval has better performances in the subsequent regulation process after load disturbance.

1. Introduction

The control of MTDC systems is a essential technology to ensure the stable operation of the systems. At present, many scholars have conducted researches on the crucial issues of MTDC systems such as DC voltage control, power distribution and frequency support, etc [1–4]. As new energy sources and microgrids continue to be connected into power systems, the application of MTDC systems to provide frequency support for AC systems has become a research focus. Ref. [5] proposed a droop control method with additional frequency regulation not requiring inter-station communication. Refs. [6,7] proposed adaptive frequency droop control methods, which improve the transient response of DC voltage and frequency by adaptive adjusting the droop coefficient. In order to improve the frequency stability and reduce the amount of rotation reserve required, a supplementary frequency control on the basis of droop control was proposed in Ref. [8]. Some researches adopted virtual synchronous generator inertia control strategies in MTDC systems, and used the virtual inertia response to provide frequency support for AC system [9,10].

With the application of supervisory control and data acquisition systems, wide area measurement systems, and energy management systems in modern power systems, the formed cyber physical system (CPS) [11,12] provides more benefits in data and communication for control design. For example, distributed consistency control structures for AC interconnection systems requiring inter-station communication have been developed and extended to MTDC systems [13,14]. However, the widely application of communication network brings some disadvantages to the operation of the physical facilities of the power system, even if secure networks are used for communication and transmission. For instance, it may bring some risks of cyber attack. The cyber attack on the Ukrainian power grids is a typical example of CPS attacks on the power grid in recent years [15]. Nevertheless, the above-mentioned control methods for MTDC systems continuously improve the control range and control accuracy yet rarely consider cyber attack factors. Furthermore, the cyber security risk is increasing to a certain extent with the communication networks application. Therefore, considering cyber attacks in the design of MTDC systems control is necessary.

☆ This work was supported in part by the National Natural Science Foundation of China under Grant 62173187.
* Corresponding author at: School of Electrical and New Energy, China Three Gorges University, Yichang 443002, Hubei Province, China.
E-mail address: ctgu_fuwenlong@126.com (W. Fu).

https://doi.org/10.1016/j.epsr.2022.108888
Received 15 February 2022; Received in revised form 17 September 2022; Accepted 9 October 2022
Available online 19 October 2022

Cyber attacks include false data injection (FDI) attacks, time delay (TD) attacks and denial-of-service (DoS) attacks [16]. Compared to other attack methods, DoS attacks are simpler and more destructive in CPS. The purpose of DoS attacks is to block communication between various components of the system and cause data packet loss. Therefore, most researchers model DoS attacks as packet loss in the control problem, and consider the energy limited characterizing of DoS attacks in previous researches [17,18].

In control design of against DoS attacks, researchers have considered some control methods such as optimal control [19,20], event triggering [21–23], game theory [24], etc. Most of the above control strategies for DoS attacks are based on known and reduced dimensionality linearized state space model to design compensate strategies. As for large-scale power systems such as the MTDC system, due to the complexity of the system and the randomness of DoS attacks, it is difficult to predict all the state quantities and compensate for lost data. Therefore, when a DoS attack causes data packet loss in a complex system, a control strategy not requiring complete state information of the system and performs data compensation on the receiving side of the controller can be considered.

The main contributions of this paper are as follows:

1. In order to restore the frequency of MTDC systems to a range that can be operated for a long time and reduce the complexity of secondary controller as much as possible, a switching control mechanism is devised. When the connected AC system emerges load disturbance, the outer controller of VSC station switches to secondary frequency control from droop control.
2. The impact of DoS attacks on the measurement signal transmission channel from sensors to controllers of MTDC systems is considered. An energy-limited, periodic DoS attacks is modeled, which can cause the controllers of MTDC systems to fail to receive frequency, active power, reactive power, and DC voltage measurement data.
3. Two compensation strategies are proposed. The two strategies respectively use the reference value and the data of the previous time interval to compensate for the lost data. These control strategies do not demand to know the linearization model of the system in advance, but only require temporary data storage at the signal receiving end. The simulation results verify the effectiveness of the two proposed solutions against DoS attacks under load disturbance.
4. The influence of different attack time intervals on the system control performance is studied. It shows that the control consequent is still effective when the attack time interval increases.

The rest of this article is arranged as follows:

Section 2 introduces the related content of traditional frequency droop control of MTDC systems and the modeling of DoS attack. The frequency regulation strategies of MTDC systems against DoS attacks are presented in Section 3. Some simulation cases using MATLAB/SIMULINK are shown in Section 4. Finally, the conclusions are drawn in Section 5.

2. Traditional frequency droop control of MTDC systems and the modeling of DoS attacks

2.1. VSC-MTDC systems control structure

An example of VSC-MTDC system structure with the double closed-loop controller under the dq rotating coordinate system are shown in Fig. 1. AC power grids AC1∼4 are connected to the DC network through VSC1∼4 stations, respectively. P1∼4 denote the output power of the VSC stations, and the direction of injection into DC network is defined as positive.

Through measurement and calculation, essential measurement signals such as frequency, active power, DC voltage and reactive power are

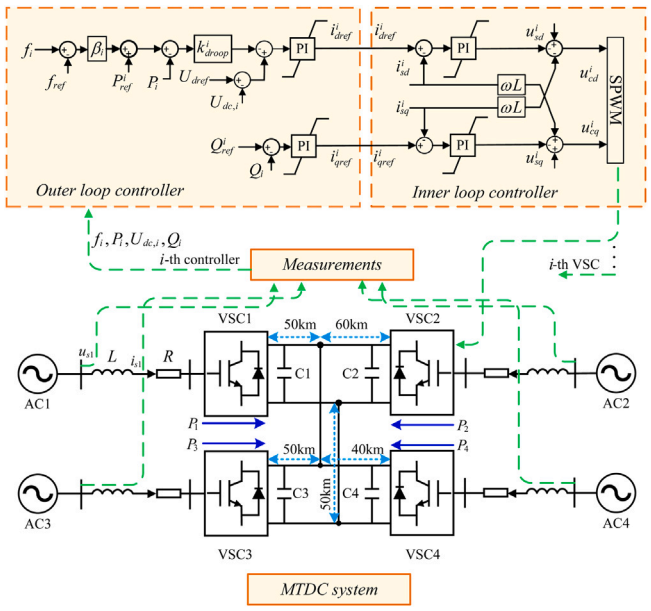

Fig. 1. Example of VSC-MTDC system structure.

transmitted to the outer loop controller of each converter station. The outer loop controller generates the current reference values i_{dref} and i_{qref} for the inner loop controller. Then, the inner loop controller generates an AC voltage signal through comparison and calculation, and controller finally controls the VSC through a PWM pulse trigger [1].

Mathematical model of the VSC in the two-phase rotating dq frame is as follows:

$$\begin{cases} L\frac{di_{sd}}{dt} = -Ri_{sd} + \omega Li_{sq} + u_{sd} - u_{cd} \\ L\frac{di_{sq}}{dt} = -Ri_{sq} - \omega Li_{sd} + u_{sq} - u_{cq} \end{cases} \tag{1}$$

where u_{sd}, u_{sq}, u_{cd}, u_{cq}, i_{sd}, i_{sq} are the d-axis and q-axis components of AC voltage at AC power grid side, AC voltage at the converter side and AC current, respectively. L and C are the equivalent resistance and equivalent inductance on AC side, respectively; ω is the synchronous rotational angular velocity of the grid voltage vector. The d-axis of the dq axis coincides with phase A of the three-phase voltage, the decoupling control of P (active power) and Q (reactive power) can be realized by controlling i_{sd} and i_{sq}. (1) is usually used to design inner controller of VSC.

Droop control is one of the main control methods of VSC-MTDC which is used in the outer loop controller. The traditional frequency droop controller of the ith VSC station is as follows:

$$\begin{cases} i^i_{dref} = \left(k^{drp}_p + k^{drp}_i/s\right)\left[\left(U^i_{dref} - U_{dc,i}\right)\right. \\ \qquad \left. -k^i_{droop}(P^i_{ref} + \beta_i(f_i - f_{ref}) - P_i)\right] \\ i^i_{qref} = \left(k^Q_p + k^Q_i/s\right)\left(Q^i_{ref} - Q_i\right) \end{cases} \tag{2}$$

where f_i, P_i, $U_{dc,i}$, Q_i are the measured values; f_{ref}, P^i_{ref}, U^i_{dref}, Q^i_{ref} are the reference values; k^{drp}_p, k^{drp}_i, k^Q_p, k^Q_i are the active and reactive PI controller parameters respectively; k^i_{droop} and β_i are the voltage droop coefficient and frequency droop coefficient, respectively.

2.2. DoS attack model

In some researches, DoS attacks have been modeled as periodic [17,18,25,26]. Due to energy limitations, periodic DoS attacks need to dormant for an interval of time after an attack to store energy to launch the next attacks. Owing to DoS attacks need few prior Information

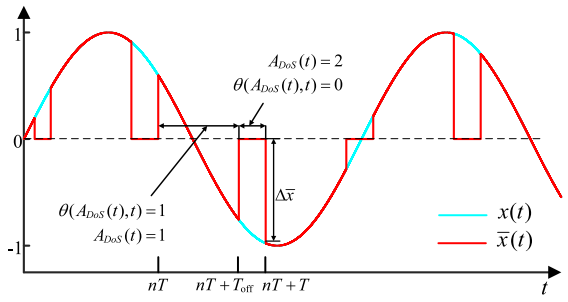

Fig. 2. The conceptual diagram of the measured signal which is assumed as sinusoidal signal being attacked.

of target, periodic attacks model is simple and efficient for design for attacker. Therefore, this paper adopts periodic DoS attacks for modeling and control analysis and considers the statistical properties of information transfer.

Assuming that the DoS attacks period is $t \in [nT, nT+T)$, define $A_{DoS}(t) \in \{1,2\}$ to indicate different time interval in the attack period [27]:

$$A_{DoS}(t)=\begin{cases} 1, t\in\left[nT, nT+T_{off}\right) \\ 2, t\in\left[nT+T_{off}, nT+T\right) \end{cases} \tag{3}$$

where $A_{DoS}(t)=1$ denotes the dormant phase when no interference signals affect the communication. $A_{DoS}(t)=2$ denotes the attack phase when interference signal access causes communication congestion, where the constant T_{off} represents the interval of dormant in a period.

We characterize the switching signal $\theta\left(A_{DoS}(t),t\right) \in \{0,1\}$ as the event that whether the communication packet transmission is successful or not

$$\theta\left(A_{DoS}(t),t\right)=\begin{cases} 0, \text{ Transmission failure} \\ 1, \text{ Transmission success} \end{cases} \tag{4}$$

Assuming that the successful transmission rate of data packets during the dormant phase and the attack phase obeys the Bernoulli probability distribution

$$\begin{cases} P\left[\theta\left(A_{DoS}(t),t\right)=1\right]=\rho_t \\ P\left[\theta\left(A_{DoS}(t),t\right)=0\right]=1-\rho_t \end{cases} \tag{5}$$

where ρ_t is the probability of successful transmission.

When a DoS attack occurs on the system measurement signal transmission channel, packet loss can make the measurement value become zero [28]. Assuming that the actual measurement signal is $x(t)$ and the signal received by the controller under DoS attacks without compensation is $\bar{x}(t)$

$$\bar{x}(t)=\begin{cases} x(t), \theta\left(A_{DoS}(t),t\right)=1 \\ 0, \theta\left(A_{DoS}(t),t\right)=0 \end{cases} \tag{6}$$

In order to visualize the impact of the modeled DoS attack on signal transmission, the conceptual diagram of the measured signal which is assumed as sinusoidal signal being attacked is shown in Fig. 2. For MTDC systems, frequency, active power, DC voltage and reactive power are the most important measured signals and attack targets for DoS attacks. The measured signals of the ith converter station is expressed as $x_i=\left[\begin{array}{cccc} f_i & P_i & U_{dc,i} & Q_i \end{array}\right]^{\mathrm{T}}$ in this paper. The error between the measured signal data and the actual data caused by the DoS attack is supposed to be the attack error $\Delta\bar{x}$. It is easy to know from (6) and Fig. 2 that $\Delta\bar{x}$ is equal to the actual measured value. Then, when the

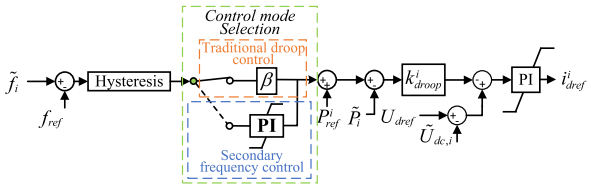

Fig. 3. Secondary frequency control structure with hysteresis.

ith converter station suffering the DoS attacks, (2) becomes:

$$\begin{cases} i^i_{dref}=\left(k^{drp}_p+k^{drp}_i/s\right)\left[\left(U^i_{dref}-\bar{U}_{dc,i}\right)\right. \\ \qquad \left.-k^i_{droop}(P^i_{ref}+\beta_i(\bar{f}_i-f_{ref})-\bar{P}_i)\right] \\ i^i_{qref}=\left(k^Q_p+k^Q_i/s\right)\left(Q^i_{ref}-\bar{Q}_i\right) \end{cases} \tag{7}$$

From (6) and (7), it can be seen that periodic DoS attacks will cause data packet loss and affect the balance of the MTDC system. The attacks test of this DoS model will be shown in Section 4.

Combined with the content of this section, the control objective of this paper is to eliminate the negative effects of DoS attacks and ensure that the frequency regulation ability of the MTDC system is not affected.

3. Frequency control strategies considering DoS attacks

In order to avoid frequent actions of the controller, hysteresis control is added based on the traditional frequency droop control. The upper and lower limits of the control frequency are set to 50.1 Hz and 49.9 Hz, respectively.

When the AC system load changes, the system can achieve active power balance relying on the frequency regulation effect of the generator set, the power frequency characteristics of the load and the frequency droop control. However, the droop control cannot restore the frequency to a range that allows the system to operate for a long time. Therefore, a proportional–integral (PI) controller can be used for secondary frequency regulation. When the controller of converter station detects the load change of the connected AC system, the outer loop controller will switch to secondary frequency regulation control. The secondary frequency regulation control structure with hysteresis is shown in Fig. 3.

In the converter station connected to the AC system where the load changes, the outer loop controller is given by:

$$\begin{cases} i^i_{dref}=\left(k^{drp}_p+k^{drp}_i/s\right)\left[\left(U^i_{dref}-U_{dc,i}\right)\right. \\ \qquad \left.-k^i_{droop}(P^i_{ref}+(f_i-f_{ref})\left(k^f_p+k^f_i/s\right)-P_i)\right] \\ i^i_{qref}=\left(k^Q_p+k^Q_i/s\right)\left(Q^i_{ref}-Q_i\right) \end{cases} \tag{8}$$

where k^f_p and k^f_i are the secondary frequency regulation parameters.

Although (8) can achieve the secondary frequency regulation, it still cannot deal with DoS attacks. When the MTDC system suffers a DoS attack, the outer loop output of the controller using the secondary control is as follows:

$$\begin{cases} i^i_{dref}=\left(k^{drp}_p+k^{drp}_i/s\right)\left[\left(U^i_{dref}-\bar{U}_{dc,i}\right)\right. \\ \qquad \left.-k^i_{droop}(P^i_{ref}+(\bar{f}_i-f_{ref})\left(k^f_p+k^f_i/s\right)-\bar{P}_i)\right] \\ i^i_{qref}=\left(k^Q_p+k^Q_i/s\right)\left(Q^i_{ref}-\bar{Q}_i\right) \end{cases} \tag{9}$$

A control strategy is necessary to compensate for the lost data packets after the data packet loss is detected. Some network analysis tools (such as wireless network Airo peek, Ethernet Ethereal, etc.) can be used to capture data packets and then analyze whether the data

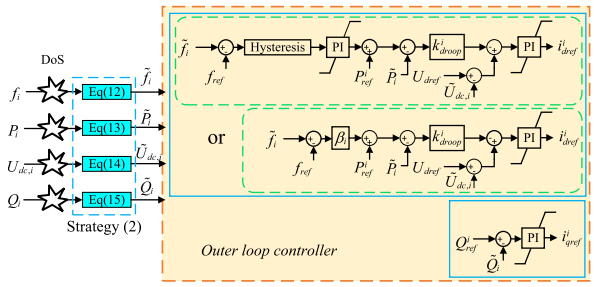

Fig. 4. Secondary frequency regulation Strategy (2) of VSC considering DoS Attack (Strategy (1) is similar.).

packets are normal or lost according to the type identification, sequence number, and timestamp of the data packet [29].

It needs to be noted that the dimension of state space model of typical 4-terminal MTDC system is 56 × 56 [30]. This value will get higher and higher as the scale of the MTDC system continues to expand. Due to the complexity of MTDC systems, it is difficult to predict all the state quantities and compensate for lost data. The proposed compensation strategy should use local information to reduce communication and should be as simple as possible. The reference value data can be used to compensate for packet loss data. The signal state received by the controller is:

$$\tilde{x}_i(t) = \theta\left(A_{DoS}(t),t\right) x_i(t) + \left(1-\theta\left(A_{DoS}(t),t\right)\right) x^i_{ref} \tag{10}$$

In order to cope with scenarios where the operating conditions of the system change, the data from the closest time interval to the time of the attack can be adopted to compensate:

$$\tilde{x}_i(t) = \theta\left(A_{DoS}(t),t\right) x_i(t) + \left(1-\theta\left(A_{\mathrm{DoS}}\ (t),t\right)\right) x_i(t-\Delta T) \tag{11}$$

where $\Delta T = T - T_{off}$ is the attack time interval. For the convenience of the following description, let (10) be Strategy (1) and (11) be Strategy (2) respectively.

The control strategy structure is shown in Fig. 4 when Strategy (2) is applied. The status of each measurement signal received by the controller is as follows:

$$\begin{aligned}\tilde{f}_i(t) &= \theta\left(A_{DoS}(t),t\right) f_i(t) \\ &+ \left(1-\theta\left(A_{DoS}(t),t\right)\right) f_i(t-\Delta T)\end{aligned} \tag{12}$$

$$\begin{aligned}\tilde{P}_i(t) &= \theta\left(A_{DoS}(t),t\right) P_i(t) \\ &+ \left(1-\theta\left(A_{DoS}(t),t\right)\right) P_i(t-\Delta T)\end{aligned} \tag{13}$$

$$\begin{aligned}\tilde{U}_{dc,i}(t) &= \theta\left(A_{DoS}(t),t\right) U_{dc,i}(t) \\ &+ \left(1-\theta\left(A_{DoS}(t),t\right)\right) U_{dc,i}(t-\Delta T)\end{aligned} \tag{14}$$

$$\begin{aligned}\tilde{Q}_i(t) &= \theta\left(A_{DoS}(t),t\right) Q_i(t) \\ &+ \left(1-\theta\left(A_{DoS}(t),t\right)\right) Q_i(t-\Delta T)\end{aligned} \tag{15}$$

4. Simulation cases

In order to verify the effectiveness of the proposed strategies, four scenarios are considered in this section.

The four-terminal MTDC system as shown in Fig. 1 has a rated power of 200 MW, a rated AC voltage of 230 kV, a rated DC voltage of 100 kV and a rated frequency of 50 Hz. The per-unit value model is adopted for the control system. The load of AC1∼AC4 system are 100 MW, 250 MW, 100 MW and 250 MW respectively. The system simulation parameters are given by Appendix Table A.1. The simulation experiments are carried out in MATLAB/SIMULINK.

4.1. Scenario 1: Research on frequency regulation strategies under load disturbance

Scenario 1 is set up to verify the effectiveness of the proposed secondary frequency control method. The load of AC system connected to VSC3 increases by 50 MW at 35 s (the load change rate is 7.14% of the total load, also 50% of connected AC system load). When the controller of converter station detects the load change of connected AC system, the frequency regulation strategies of the outer loop controller used are traditional control strategy of (2) and the secondary frequency control strategy of (8), respectively. The system response comparisons of different control methods are shown in Fig. 5 .

It is worth noting that the frequency range that the AC system can operate for a long time is 49.8 Hz to 50.2 Hz. From Fig. 5(a), the frequency of AC3 drops to 49.6 Hz, but the frequency of other AC systems changes a little while using traditional control. That is, other AC power grids do not provide enough frequency support to AC3 through the MTDC system. In Fig. 5(a), the frequencies of AC1∼4 are 49.83 Hz, 49.9 Hz, 49.83 Hz and 49.83 Hz respectively under the action of secondary frequency regulation. The AC system without load changes has more frequency drops than AC3 because other AC systems provide frequency support for AC3. In brief, the frequency of all AC systems can be maintained within a safe operating range under the proposed secondary frequency regulation.

Fig. 5(b) shows that the secondary frequency control has a stronger power distribution effect. Due to the drooping characteristics, it needs to sacrifice 6% of DC voltage deviation of the secondary frequency control for the balance of controller output in Fig. 5(c). Fig. 5(d) indicate the reactive power under the secondary frequency regulation control can be stabilized after short adjustment.

It is worth noting that only one VSC station which is connected to the AC power grid with changing load switches to the secondary frequency regulation strategy as (8) in order to avoid power fluctuations. Other VSC stations still utilize the frequency regulation strategy as (2).

4.2. Scenario 2: The proposed DoS model attacks test on the MTDC system

The objective of this scenario is to study the impact of DoS attacks on MTDC systems. Set the work period T of DoS attacks model as 2 s, the dormant time interval T_{off} as 1.8 s, the attack time interval ΔT as 0.2 s. The probability of successful signal transmission during attack ρ_t is 0.05. The attack duration is $t \in [30, 50]$. In this section, we assume the targets of attacker are the transmission channel of frequency, active power, DC voltage, and reactive power measurement signals of VSC2.

Waves of VSC2 measured signals under DoS attacks without compensation strategy are shown in Fig. 6(a) and Fig. 6(b). It can be seen from Fig. 6 that the states of each measured signal received by the controller has become zero at the moment of DoS attack instead of the actual measurement state quantity by (6). The consequence of data losing is causing the controller to make a wrong response, output the wrong control signal and seriously affect the subsequent control process.

Fig. 7 illustrates the system responses under DoS attack without compensation strategy. Fig. 6 and Fig. 7 indicate that although only one converter station has suffered DoS attacks, the state of others has changed and eventually led to system instability as a result. The frequency, power, and voltage fluctuations caused by the system during the attack will cause irreversible damage to many electrical equipment. Therefore, it is extremely necessary to consider DoS attacks in the design of MTDC systems control.

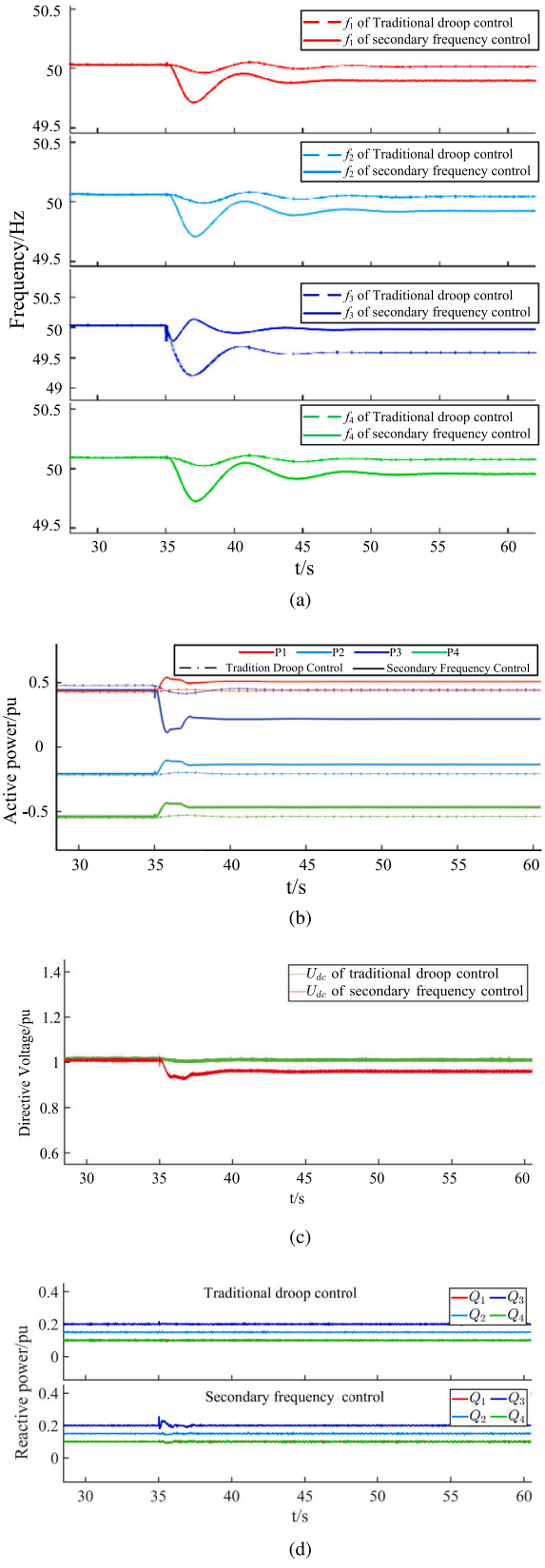

Fig. 5. The system response comparisons of different control methods (a)Frequency. (b) Active power. (c) DC voltage. (d) Reactive power.

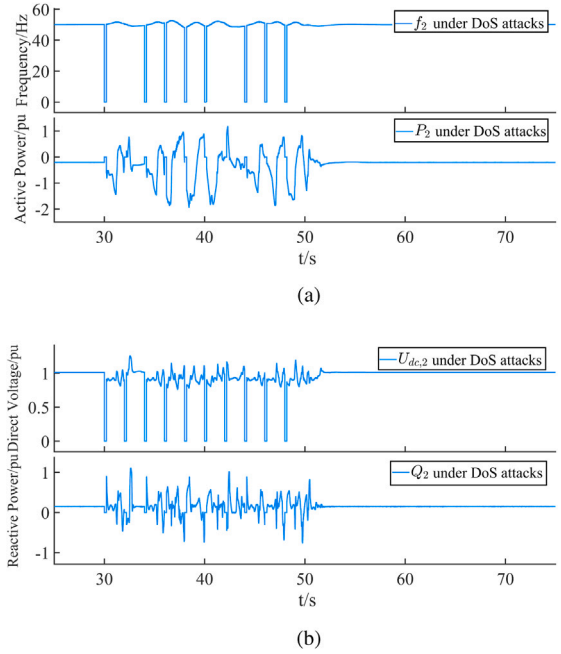

Fig. 6. Status of VSC2 measurement signals under DoS attack without compensation strategy. (a) Frequency, active power. (b) DC voltage, reactive power.

4.3. Scenario 3: The MTDC system suffers DoS attacks with proposed compensation strategies

To comprehensively compare the performance of the proposed strategies, we set the attack duration as $t \in [30, 60]$ and the load of AC system connected to converter station 3 increases by 50MW at 35 s. The other settings refer to *Scenario* 2. When under a DoS attack, the controller of VSC2 applies Strategy (1) and Strategy (2), respectively.

Fig. 8 shows the states of VSC2 measurement signals under DoS attack with Strategy (1) and Strategy (2). Fig. 8 indicates that the attack duration includes the operating phase of steady-state, system frequency regulation phase and new steady state phase after the regulation is completed. When the system is under DoS attacks during the steady-state operation phase, the reference value data selected by Strategy (1) and the latest data taken by Strategy (2) are close to the steady-state actual value. Therefore, the data packet loss caused by the DoS attack both can be compensated by the proposed strategies during the operating phase of steady-state. However, in the system frequency regulation time period and the new steady state phase after the regulation is completed, the reference value data obtained by Strategy (1) will not change with the change of the system load. The compensation data by Strategy (1) becomes a new disturbance which will affect the system frequency restoring. The data at the latest time taken by Strategy (2) is closer to the actual measured value data, and has almost no effect on the system frequency regulation process. In the new steady-state time interval after the regulation is completed, the latest time data taken by Strategy (2) can also follow the new steady-state measurement data of the system.

The system frequency responses under the DoS attack with Strategy (1) and Strategy (2) are illustrated in Fig. 9(a) and Fig. 9(b), respectively. As can be seen from Fig. 9, owing to the secondary frequency regulation control and the hysteresis, the frequency of AC3 with a sudden increase in load is restored to 49.9 Hz. Compared with Strategy (1), Strategy (2) is more effective in dealing with DoS attacks, and the frequency waveform is more smooth.

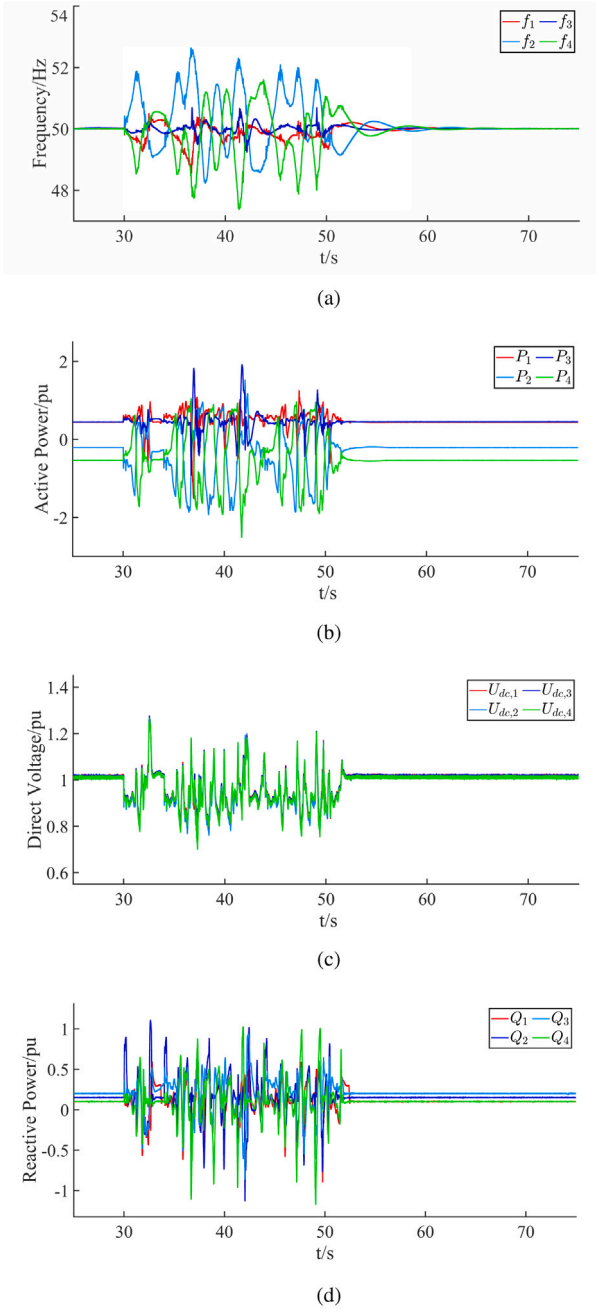

Fig. 7. The system responses under DoS attack without compensation strategy. (a) Frequency. (b) Active power. (c) DC voltage. (d) Reactive power.

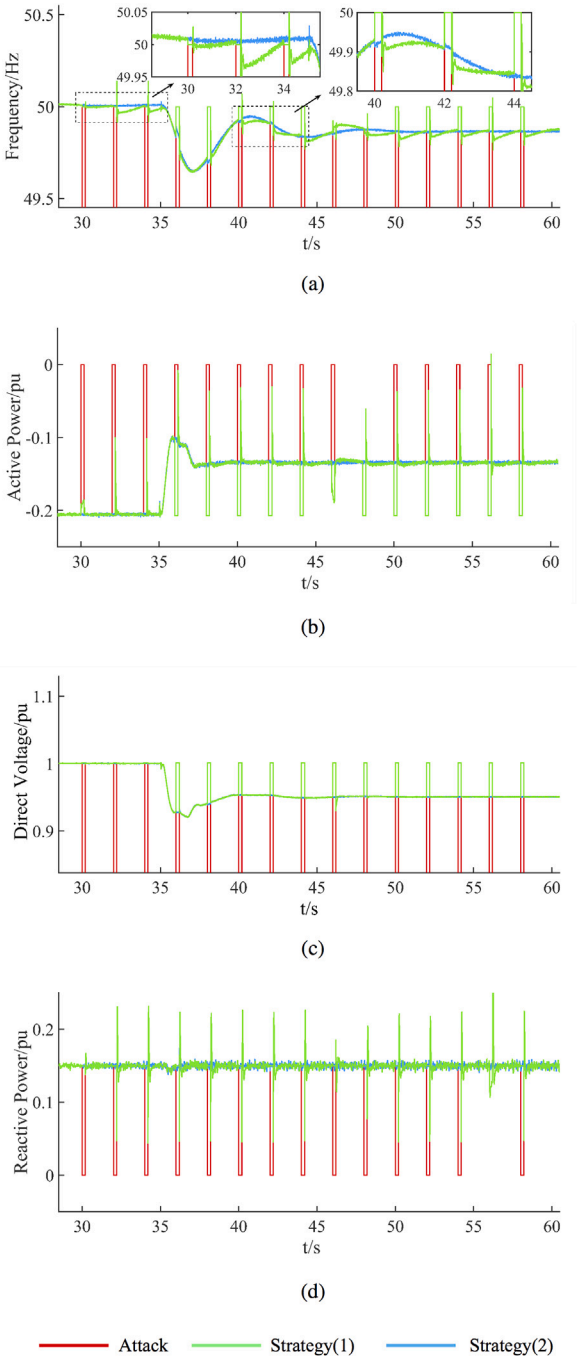

Fig. 8. The states of VSC2 measurement signals under DoS attack with compensation strategies. (a) Frequency. (b) DC voltage. (c) active power. (d) reactive power.

4.4. Scenario 4: The impact of the attack time interval changes

In order to study the assumptions mentioned in Section 2, take the frequency compensation signal as shown in Fig. 10 as an example. When ΔT is 0.2 s, the maximum compensation error Δx_{MAX} is 0.06 Hz in the figure. The frequency after compensation is 49.83 Hz, the actual frequency is 49.77 Hz, and the percentage error is 0.1206%. Therefore, the compensation error of this strategy can be ignored in engineering.

Moreover, it can be seen that the compensation error Δx is positively related to ΔT. The larger ΔT is, the larger Δx may increase, and the compensation effect may be worse. In order to study the impact of ΔT increase on the system, it is necessary to simulate the scenario changing parameters of the DoS attack model.

In the scenario, the set of ΔT is changed from 0.2 s to 0.4 s. Due to the energy limited characterizing of the DoS attack, set the attack model's working period T=4 s and dormant time T_{off}=3.6 s, and the other settings refer to *Scenario* 3.

The frequency signal after compensation is illustrated in Fig. 11, and the system frequency is illustrated in Fig. 12. The comparison diagram of the state quantity and the actual frequency waveform after the frequency signal compensation of the attacked converter station at ΔT=0.2 s and ΔT=0.4 s is illustrated in Fig. 13.

It can be seen from Fig. 11 that when ΔT is 0.4 s, the maximum compensation error is 0.13 Hz. The compensation data is 49.83 Hz, the actual data is 49.70 Hz, and the percentage error is 0.2616%, which

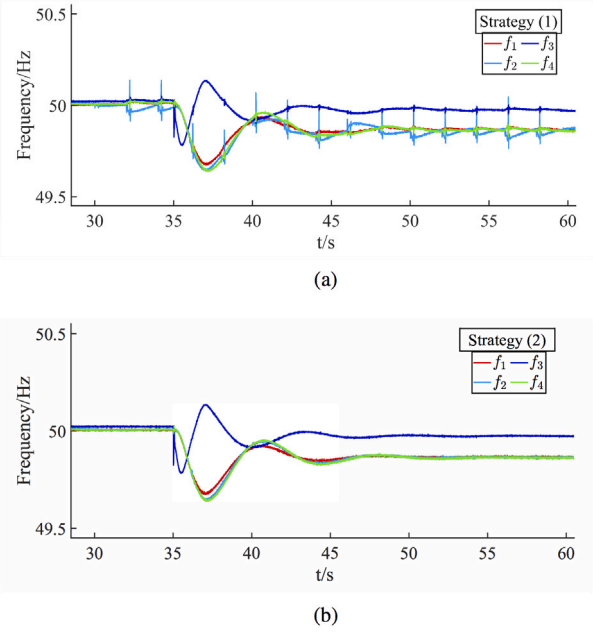

Fig. 9. The system frequency responses under the DoS attack with compensation strategy. (a) Strategy (1). (b) Strategy (2).

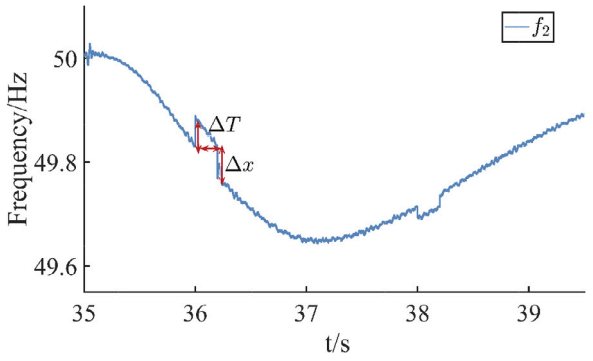

Fig. 10. The compensated state of the frequency signal for Strategy (2).

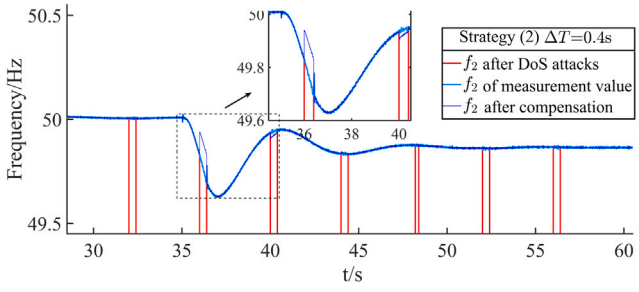

Fig. 11. Frequency signal compensation of ΔT=0.4 s.

slightly increases when ΔT is 0.2 s. However the percentage error is still very small and can still be ignored.

As illustrated in Fig. 12, although ΔT increases, the control system can still complete the frequency regulation work. The frequency of all AC systems can be stabilized in the range that can work for a long time.

Fig. 13 shows that when ΔT=0.2 s and ΔT=0.4 s, the state of frequency after compensation of the attacked VSC station both have little influence on the control process, and the deviations of the actual frequency are small. Furthermore, the system state will not be affected

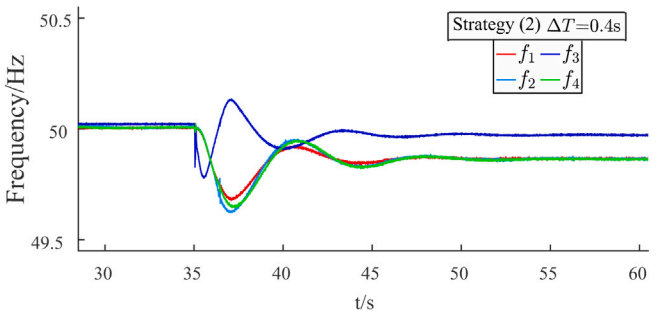

Fig. 12. The system frequency of ΔT=0.4 s.

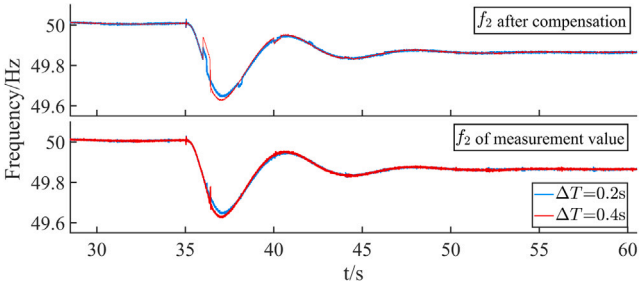

Fig. 13. The comparison diagram of the state of frequency after compensation and the actual frequency waveform of the attacked converter station when ΔT=0.2 s and ΔT=0.4 s.

by ΔT changes on the system steady-state operation period and the new steady-state period.

5. Conclusion

This paper reveals the necessity of MTDC systems to defend DoS attacks. Then, for ensuring MTDC systems remain stable when subjected to DoS attacks, two compensation strategies based on secondary frequency regulation control are proposed. The compensation strategy which uses the reference value can be utilized when the system is in operating phase of steady-state. The other compensation strategy which uses the data of the previous time interval has a better performance in the operating state when the system changes. Furthermore, it is verified that these control strategies can effectively defend DoS attacks and realize the secondary frequency regulation. In the future works, the aperiodic attack model and the impact of the model parameters changes on the control strategy needs to be further studied, and the impact of different attacks on the system needs to be also considered.

CRediT authorship contribution statement

Yunning Zhang: Conceptualization, Methodology, Writing – reviewing and editing. **Le Wei:** Software, Validation, Data curation, Writing – original draft. **Wenlong Fu:** Investigation, Writing – reviewing and editing. **Xi Chen:** Supervision. **Songlin Hu:** Project administration.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

The authors are unable or have chosen not to specify which data has been used.

Table A.1
Simulation parameters.

Parameter and Symbol	Value
AC Side Equivalent Resistance R/Ω	0.2
AC Side Equivalent Inductance L/H	0.001
DC Side Capacitance C/uF	250
DC transmission line Resistance R_{line} / $(\Omega\ \text{km}^{-1})$	0.0139
DC transmission line Inductance L_{line} / $(\text{H}\ \text{km}^{-1})$	0.159×10^{-3}
DC transmission line Capacitance C_{line} / $(\text{F}\ \text{km}^{-1})$	0.237×10^{-6}
Outer Controller k_p^{drp}, k_i^{drp}, k_p^{Q}, k_i^{Q}	10, 400, 10, 400
Secondary Controller k_p^{f} and k_i^{f}	10, 100
Voltage Droop Coefficient k_{droop}^{i} $i = 1, 2, 3, 4$	0.12, 0.08, 0.08, 0.1
Frequency Droop Coefficient β_i $i = 1, 2, 3, 4$	0.12, 0.08, 0.08, 0.1
Frequency Reference Value f_{ref}/Hz	50
Active Power Reference Value P_{ref}^{i}/pu	0.465, −0.187, 0.5, −0.53
DC Voltage Reference Value U_{dref}/pu	1
Reactive Power Reference Value Q_{ref}^{i}/pu	0.1, 0.15, 0.2, 0.1

Appendix

See Table A.1.

References

[1] Q. Zhang, et al., Primary frequency support through North American continental HVDC interconnections with VSC-MTDC systems, IEEE Trans. Power Syst. 36 (2021) 806–817.

[2] A. Chakrabortty, A.A. Milani, M.T.A. Khan, I. Husain, Equilibrium point analysis and power sharing methods for distribution systems driven by solid-state transformers, IEEE Trans. Power Syst. 33 (2018) 1473–1483.

[3] M.S.E. Moursi, A. Kirakosyan, E.F. El-Saadany, K. Al Hosani, DC voltage regulation and frequency support in pilot voltage droop-controlled multiterminal HVdc systems, IEEE Trans. Power Deliv. 33 (2018) 1153–1164.

[4] R. Zhan, Y. Li, Y. Tang, Z. Li, Z. Wei, X.P. Zhang, Frequency support control method for interconnected power systems using VSC-MTDC, IEEE Trans. Power Syst. 36 (2021) 2304–2313.

[5] M. Guan, et al., The frequency regulation scheme of interconnected grids with VSC-HVDC links, IEEE Trans. Power Syst. 32 (2017) 864–872.

[6] Y. Cao, U. Hager, W. Wang, Y. Li, C. Rehtanz, Adaptive droop control of VSC-MTDC system for frequency support and power sharing, IEEE Trans. Power Syst. 33 (2018) 1264–1274.

[7] J. Ostergaard, Y. Li, Z. Xu, D.J. Hill, Coordinated control strategies for offshore wind farm integration via VSC-HVDC for system frequency support, IEEE Trans. Energy Convers. 32 (2017) 843–856.

[8] A.E. Leon, Short-term frequency regulation and inertia emulation using an MMC-based MTDC system, IEEE Trans. Power Syst. 33 (2018) 2854–2863.

[9] Y. Cao, et al., A virtual synchronous generator control strategy for VSC-MTDC systems, IEEE Trans. Energy Convers. 33 (2018) 750–761.

[10] Y. Cao, H. Zhu, C. Rehtanz, C. Li, Y. Li, U. Hager, Virtual synchronous generator control for damping DC-side resonance of VSC-MTDC system, IEEE J. Emerg. Sel. Top. Power Electron. 6 (2018) 1054–1064.

[11] Q. Mou, H. Ye, K. Liu, Y. Liu, Modeling and formulation of delayed cyber-physical power system for small-signal stability analysis and control, IEEE Trans. Power Syst. 34 (2019) 2419–2432.

[12] Z. Wang, L. Xu, Q. Guo, H. Sun, Modeling of time-delayed distributed cyber-physical power systems for small-signal stability analysis, IEEE Trans. Smart Grid 12 (2021) 3425–3437.

[13] Y. Xu, Z. Wang, J. He, F. Zhang, Distributed control of VSC-MTDC systems considering tradeoff between voltage regulation and power sharing, IEEE Trans. Power Syst. 35 (2020) 1812–1821.

[14] Y. Gao, Q. Ai, Distributed multi-agent control for combined AC/DC grids with wind power plant clusters, IET Gener. Transm. Distrib. 12 (2018) 670–677.

[15] J. Zhao, F. Luo, G. Liang, S.R. Weller, Z.Y. Dong, The 2015 Ukraine blackout: Implications for false data injection attacks, IEEE Trans. Power Syst. 32 (2017) 3317–3318.

[16] D. Kundur, A.A. Jahromi, A. Kemmeugne, A. Haddadi, Cyber-physical attacks targeting communication-assisted protection schemes, IEEE Trans. Power Syst. 35 (2020) 440–450.

[17] L. Shi, H. Zhang, P. Cheng, J. Chen, Optimal denial-of-service attack scheduling with energy constraint, IEEE Trans. Automat. Control 60 (2015) 3023–3028.

[18] T. Li, S. Lai, B. Chen, L. Yu, Packet-based state feedback control under DoS attacks in cyber-physical systems, IEEE Trans. Circuits Syst. II, Exp. Briefs 66 (2019) 1421–1425.

[19] L. Shi, H. Zhang, P. Cheng, J. Chen, Optimal DoS attack scheduling in wireless networked control system, IEEE Trans. Control Syst. Technol. 24 (2016) 843–852.

[20] H. Peng, X. Cao, Y. Sun, et al., Energy efficient jamming attack schedule against remote state estimation in wireless cyber-physical systems, 272, 2018, pp. 571–583,

[21] C. De Persis, V.S. Dolk, P. Tesi, W.P.M.H. Heemels, Event-triggered control systems under denial-of-service attacks, IEEE Trans. Control Netw. Syst. 4 (2017) 93–105.

[22] Pietro Tesi, S. Feng, Resilient control under denial-of-service: Robust design, Automatica 79 (2017) 42–51.

[23] A. Lu, G. Yang, Input-to-state stabilizing control for cyber-physical systems with multiple transmission channels under denial of service, IEEE Trans. Automat. Control 63 (2018) 1813–1820.

[24] P. Cheng, J. Chen, Y. Li, L. Shi, D.E. Quevedo, Jamming attacks on remote state estimation in cyber-physical systems: A game-theoretic approach, IEEE Trans. Automat. Control 60 (2015) 2831–2836.

[25] S. Biswas, B. Niemoczynski, J. Kollmer, Stability of discrete-time networked control systems under denial of service attacks, Proc. Resilience Week (2016) 119–124.

[26] V. Gupta, G.K. Befekadu, P.J. Antsaklis, Risk-sensitive control under Markov modulated denial-of-service (DoS) attack strategies, IEEE Trans. Automat. Control 60 (2015) 3299–3304.

[27] Y. Zhu, W.X. Zheng, Observer-based control for cyber-physical systems with periodic dos attacks via a cyclic switching strategy, IEEE Trans. Automat. Control 65 (2020) 3714–3721.

[28] G.K. Venayagamoorthy, X. Zhong, I. Jayawardene, R. Brooks, Denial of service attack on tie-line bias control in a power system with PV plant, IEEE Trans. Emerg. Top. Comput. Intell. 1 (2017) 375–390.

[29] M. Kassouf, M. Debbabi, B. Moussa, A. Al-Barakati, C. Assi, Exploiting the vulnerability of relative data alignment in phasor data concentrators to time synchronization attacks, IEEE Trans. Smart Grid 11 (2020) 2541–2551.

[30] Olimpo Anaya-Lara, Giddani O. Kalcon, Grain P. Adam, Small-signal stability analysis of multi-terminal VSC-based dc transmission systems, IEEE Trans. Power Syst. 27 (2012).