APPENDIX I
THE EFFECT OF SEQUENCES OF ATTACK EVENTS ON FAILURE EVOLUTION

In the N$-k$ cascading failure scenario, the propagation trajectory and failure consequence are almost determined once the initial failure occurs. However, when lines in the combination fail in a different order, the propagation trajectory and consequences of the cascading failure may be totally different. The example is shown in Fig.6.

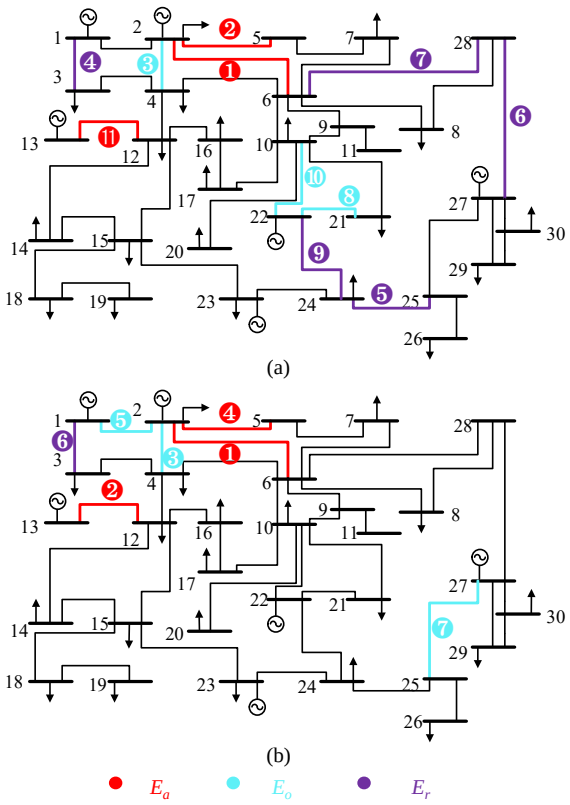

Fig. 6. The effect of failure sequences on failure propagation.

In both Fig.6(a) and Fig.6(b), the colored numbers above the line represent the failure order and the type of failure. The attack event aims at the same line combination including $\{(2,6),(2,5),(12,13)\}$. As shown in Fig.6(a), lines fail in the order of $(2,6)\rightarrow(2,5)\rightarrow(12,13)$. Three lines fail due to E_o and five lines fail due to E_r after the failure propagation. As a result, 144MW of the load is lost and the original system is splitting. However, the propagation process is totally changed when lines fail in the order of $(2,6)\rightarrow(12,13)\rightarrow(2,5)$ The failure does not cause any load shedding or system splitting. The interaction between the attack event and failure propagation increases the uncertainty of the failure consequence. Therefore, identifying vulnerable sequences precisely is important to mitigate this threat.

APPENDIX II
THE PSEUDOCODE AND DETAIL DESCRIPTION

A delineation of the precise procedural steps is provided in Algorithm 2.

Algorithm 2 The VSIM

Input: cascading failure model H
policy network Q_p^{Ω}
target network Q_t^{Ω}
number of episode M
length of vulnerable sequences k
replay buffer D
number of candidate lines n_c
Output: vulnerable sequences set υ
Phase 1. Model training
for episode=1, …, M
for $t=1,\ldots,k-1$
$a_t \leftarrow \varepsilon$-greedy$(s_{t-1})$
$r_t, s_{t+1} \leftarrow H(a_t)$
$D \leftarrow (s_t, a_t, r_t, s_{t+1})$
sample minibatch $(s_t, a_t, r_t, s_{t+1}) \leftarrow D$
update Q_p^{Ω} by minimizing:
$(Q_p^{\Omega}(s_i,a_i) - (r_i + Q_t^{\Omega}(s_{i+1}, \Omega(s_i+1))))^2$
set $Q_t^{\Omega} \leftarrow Q_p^{\Omega}$ for every c steps
end
end
Phase2. Vulnerable sequences identification
for each line k
$a_0 \leftarrow$ line l fails
$s_0 \leftarrow H$
for $i=1,\ldots,k-1$
$a_i = \underset{a_i \in A | a_i \neq a_j, j=0,\ldots,i-1}{\arg\max} Q_p^{\Omega}(s_{i-1}, a_i)$
$s_i \leftarrow H(s_{i-1}, a_i)$
end
$\upsilon' = (I(a_0), \ldots, I(a_{k-1}))$
if $|H_{\upsilon'}| > \gamma \sum_i p_L^i$
$\upsilon \rightarrow \upsilon'$
end
end

In the training phase of VSIM, the state characterization s_t of the system is formulated by integrating physical and topological eigenvectors. The action a_t is determined through epsilon-greedy exploration. Subsequently, the hybrid system model is employed to conduct simulation, yielding the reward r_t and the succeeding state s_{t+1}. And the tuple (s_t, a_t, r_t, s_{t+1}) is stored in the replay buffer D. Through random batch sampling from D, the parameters of the policy network can be updated by achieving regression between $Q_p^{\Omega}(s_i, a_i)$ and $r_i + Q_t^{\Omega}(s_{i+1}, \Omega(s_{i+1}))$. Finally, the parameters of the target network are synchronized with those of the policy network after Q_p^{Ω} has been updated for several times. In the identification phase, solely the policy network is involved in making step-by-step decisions. At each decision point, the optimal action a_t is determined via Q_p^{Ω}, thus facilitating the identification of vulnerable sequences. Moreover, for practical purposes aimed at obtaining a broader set of vulnerable sequences, it is not strictly necessary to select a_t corresponding to the maximum $Q_p^{\Omega}(s_t, a_t)$. It can be relaxed and select the top n corresponding $a_i, i=1,\ldots,n$ to obtain more vulnerable sequences. And such a relaxed version of this algorithm is employed in the Section

V-B.

Besides, there are two points worth to be mentioned. The first is the design of physical and topological eigenvectors. In order to reduce the difficulty of network training, it is necessary to characterize the system state with a low-dimensional eigenvector. The physical eigenvector $\boldsymbol{e_P}$ designed as a column vector can be formulated as

$$\boldsymbol{e_P} = (\frac{pf_1}{c_1}, \frac{pf_2}{c_2}, \ldots, \frac{pf_{n_l}}{c_{n_l}}) \tag{24}$$

where pf_i denotes the power flow of line i, c_i denotes the transmission capacity of line i, n_l denotes the number of lines. The physical eigenvector serves as a representation of the load level associated with each transmission line within the power grid. Moreover, it encapsulates various physical attributes inherent to the power grid, including line parameters, node loads, etc. And the topological eigenvector $\boldsymbol{e_T}$ is also a column vector extracted from adjacency matrix through the algorithm discussed in the Section IV-C. By integrating both $\boldsymbol{e_P}$ and $\boldsymbol{e_T}$, the eigenvector inputted to VSIM $\boldsymbol{e_I}$ can be represented as

$$\boldsymbol{e_I} = (\boldsymbol{e_P}^T, \boldsymbol{e_T}^T)^T \tag{25}$$

where $\boldsymbol{e_I}$ is still a column vector. Besides, if $|\boldsymbol{e_P}| = n_p$ and $|\boldsymbol{e_T}| = n_t$, then we have $|\boldsymbol{e_I}| = n_p + n_t$.

Secondly, the load shedding (LS) after the failure propagation is set to the reward in an epoch. The delayed reward is used to enable the policy network to make decisions that more focuses on the future benefits rather than immediate benefits:

$$r_1 = 0, r_2 = 0, \ldots, r_n = \mathrm{LS} \tag{26}$$

where r_i represents the reward of ith action. Although, the reward for most actions in an epoch is zero, every step of action is valuable due to the cumulative actions of each step ultimately leading to the significant load shedding.

Appendix III
Proof of the upper bound of the TFEA

In the proposed algorithm, since the maximum eigenvalue of the adjacency matrix $\mathbf{A}$ is integrated, the upper bound of the objective function can be determined as

$$||\mathbf{A} - \mathbf{A}'||_2 \leq 2\lambda_{max} \tag{27}$$

To prove this inequality, some properties of matrix norm need to be addressed firstly, including non-negativity, homogeneity, and triangle inequality shown as

$$||\mathbf{A}|| \geq 0, \text{iff } \mathbf{A} = \mathbf{0}, ||\mathbf{A}|| = 0 \tag{28}$$

$$||\lambda\mathbf{A}|| = |\lambda|||\mathbf{A}|| \tag{29}$$

$$||\mathbf{A} + \mathbf{B}|| \leq ||\mathbf{A}|| + ||\mathbf{B}|| \tag{30}$$

Besides, it is important to know that 2-norm of the real symmetric matrix is its maximum eigenvalue. Then the inequality (27) can be derived as

$$\begin{aligned} &||\mathbf{A} - \mathbf{A}'||_2 \\ =&||\mathbf{A} + (-\mathbf{A}')||_2 \\ \leq&||\mathbf{A}||_2 + ||\mathbf{A}'||_2 \\ \leq&2\lambda_{max} \end{aligned} \tag{31}$$

where the first inequality sign holds due to the equation (29) and (30). The effectiveness of the proposed embedding algorithm can be validated theoretically by the above discussion. Moreover, to better illustrate the idea of the embedding algorithm, some discussions are conducted by presenting some visualizations shown in Fig.7.

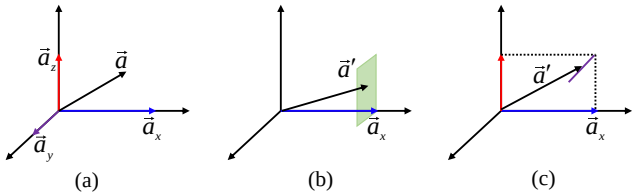

Fig. 7. Visualizations of topological feature embedding algorithm.

As shown in Fig.7, the vector is used to analogize matrix for visual presentation due to a lot of similarities. For example, the vector $\vec{a}$ can be represented by $\vec{a}_x + \vec{a}_y + \vec{a}_z$ in Fig.7(a). The adjacency matrix $\mathbf{A}$ can also be represented by n components as $(\lambda_1\mathbf{u}_1, \lambda_2\mathbf{u}_2, \ldots, \lambda_n\mathbf{u}_n)$. The $|\vec{a}_x|$ is similar to the λ_1, and $\vec{a}_x$ is similar to $\mathbf{u}_1$. When $\vec{a}_x$ is known, possible trajectories of $\vec{a}_x$' lie in the green square plane shown in Fig.7(). In other words, the known $\vec{a}_x$ can effectively reduce the $\|\vec{a} - \vec{a}'\|$ because $\vec{a}_x$ contains the main component information in $\vec{a}$. And when $\vec{a}_x$ and $\vec{a}_z$ are known, the $\|\vec{a} - \vec{a}'\|$ will be smaller. As a price, the number of dimensions of the known information is increased.

Appendix IV
Numerical comparison of distribution similarity

To numerically compare the similarities of the data distributions of sequential and N$-k$ cascading failure to the historical data, Kullback-Leible (KL) divergence and mean-square error (MSE) are used to achieve accurate comparison shown as

$$KL(P||Q) = \sum P(x) \log \frac{P(x)}{Q(x)} \tag{32}$$

$$MSE(m,n) = \frac{1}{N}\sum_{i}^{N} m(i) - n(i) \tag{33}$$

where $P(x)$ is the real distribution of random variable x, $Q(x)$ is the approximate distribution of random variable x, m and n are the two distribution of percentage of load shedding under different failure model. N is the number of elements in m or n. The results are shown in Table I.

As shown in Table I, both KL divergence and MSE are smaller under sequential cascading failure than under N$-k$ cascading failure. Therefore, the sequential cascading failure is more similar to the actual scenario and is better at characterizing the real failure.

TABLE I
THE SIMILARITIES OF DISTRIBUTION OF LOAD SHEDDING UNDER DIFFERENT SCENARIOS

Scenario	KL divergence	MSE
sequential cascading failure	**0.0254**	**0.0388**
N$-k$ cascading failure	0.2649	0.5092

APPENDIX V
NUMERICAL EXPERIMENTS ON VALIDATING THE EFFICIENCY OF VSIM AND INFLUENCE OF β

And then, some comparative experiments are conducted to validate the efficiency of the proposed VSIM. An indicator that the average simulation time required to identify single vulnerable sequence is formulated to compare the efficiency of different algorithms. The experiments are conducted on a workstation equipped with an AMD Ryzen 7 5800H CPU and 16GB of RAM, operating on Python 3.8. The corresponding results are presented in Table II.

TABLE II
COMPARISON OF IDENTIFICATION EFFICIENCY AMONG DIFFERENT METHODS

Case	Average time required for identifying single vulnerable sequence				
	VSIM	RS	IM1	IM2	GP
30-bus	**20.8s**	102.29s	11.59s	103.32s	103.78s
200-bus	**373.44s**	103,816.75s	1,043.38s	/	2,076.34s

[a] The symbol / represents no fragile sequence is identified, therefore the average time cannot be calculated.

As depicted in Table II, two important conclusions can be drawn and merit highlighting. Firstly, the superior efficiency of the proposed VSIM is validated within both IEEE 30-bus and 200-bus systems. The excellent performance can be attributed to the low time complexity of the proposed algorithm and its capability to make dynamic decisions based on changes in the system's state, thereby identifying more vulnerable sequences within a limited number of simulations. Secondly, the efficiency of IM1, IM2 and GP is found to be unsatisfactory, as they exhibit inferior performance compared to RS in some scenarios. Both IM1 and IM2 overlook the dynamic evolution of the system, and the simple indicator may introduce incorrect information during the identification process. Furthermore, the deficiency of GP arises from its exclusive focus on pursuing local optima for short-term benefits.

Besides, the effect of threshold β on vulnerable sequence identification is explored through numerical experiments. We counted the distribution of the number of vulnerable sequences identified by VSIM set with different values of β. And β ranges from 5% to 25%. The results are shown in Fig.8.

The experimental results in Fig.8 can be summarized from three aspects as below. Firstly, more vulnerable sequences are identified as the threshold β increases. However, an increase in the threshold also means more time consumption for identification. Therefore, it is important to make a trade-off

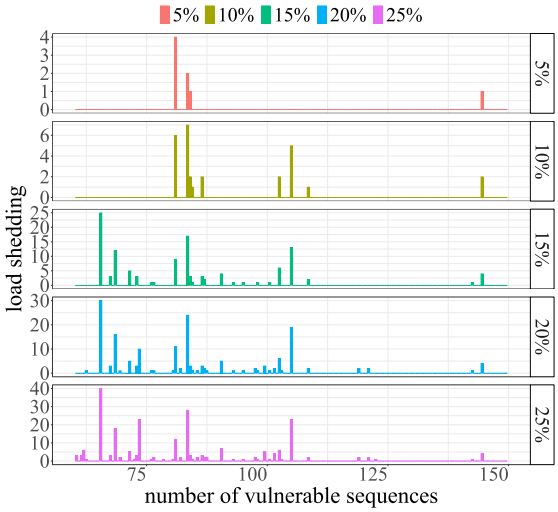

Fig. 8. The analysis of the effect of threshold on vulnerable sequence identification on IEEE 30-bus system.

between identification quantity and efficiency. Secondly, when the threshold β exceeds 15%, the distribution of load shedding caused by the identified vulnerable sequences is essentially the same. And it can provide an approximate picture of the threat of the vulnerable set in the system. Thirdly, the number of identified vulnerable sequences that can cause the most load shedding does not increase significantly with the increase of β. Combined with the exhaustive search results, the number of vulnerable sequences mentioned above is small, and most of them can be identified when the threshold is small. It reflects the effectiveness of the proposed VSIM.

APPENDIX VI
ABLATION AND COMPARATIVE EXPERIMENTS ON TFEA

In Section IV-C, the theoretical effectiveness of the proposed topological features embedding method is analyzed. In order to validate its practical performance, the ablation experiments are conducted. Additionally, the DeepWalk (DW) method [40], which combines the RandomWalk and skip-gram is used for comparison to demonstrate the effectiveness of the proposed VSIM. It is important to note that the proposed TFEA aims to improve the performance of identifying vulnerable sequences of cascading failures within transmission network scenarios. Therefore, the experiments are all conducted in transmission network and the experimental results are shown in Fig.9.

As depicted in Fig.9, the results of the ablation experiments indicate that the integration of topological features via both the TFEA and DW enhances both the quality and quantity of vulnerable sequence identification. The incorporation of topological features allows for a more comprehensive characterization of the system's state changes resulting from failure propagation, thereby facilitating the identification of more vulnerable sequences capable of inducing greater load shedding. Furthermore, the proposed TFEA exhibits a more pronounced enhancement in identification performance, attributed to its theoretical performance guarantee.

It is essential to highlight that the proposed TFEA is designed to enhance the performance of identifying vulnerable

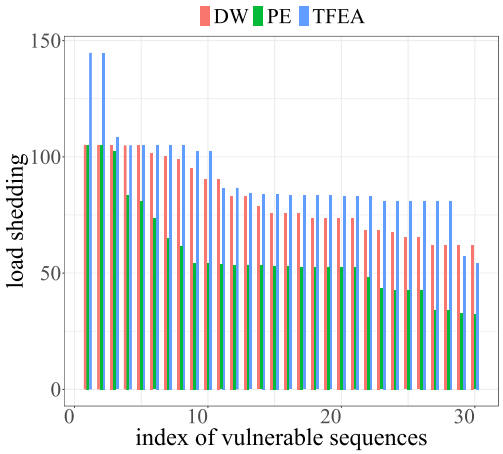

Fig. 9. The results of ablation and comparative experiments.

sequences of cascading failures within transmission network scenarios. Therefore, the experiments are specifically conducted within transmission network. Moreover, in other forms of grids, such as distribution grids and microgrids, there is a potential security threat of cascading failures due to their networked nature as well as the transmission grid. However, distinct physical responses and focus of attention exist within each grid type during the evolution of failures. For example, in the transmission grid, emphasis is placed on maintaining the supply of system loads, whereas in the distribution grid, greater attention is directed toward the voltage levels of nodes. Hence, it is imperative to allocate additional efforts towards exploring topological feature embedding methods tailored to different grid architectures, thereby optimizing the utility of topological features for future applications.