

Research Article

Open Access



# VNN-DM: a vector neural network-based detection model for time synchronization attacks in park-level energy internet

Jiacheng Yang<sup>1</sup>, Fanrong Shi<sup>1</sup>, Yunlong Li<sup>1</sup>, Zhihang Zhao<sup>1</sup>, Qiushi Cui<sup>2</sup>

<sup>1</sup>School of Information Engineering, Southwest University of Science and Technology, Mianyang 621010, Sichuan, China.

<sup>2</sup>School of Electrical Engineering, Chongqing University, Chongqing 400044, China.

**Correspondence to:** Dr. Fanrong Shi, School of Information Engineering, Southwest University of Science and Technology, No.59, Middle Section of Qinglong Avenue, Fucheng District, Mianyang 621010, China. E-mail: sfr\_swust@swust.edu.cn

**How to cite this article:** Yang J, Shi F, Li Y, Zhao Z, Cui Q. VNN-DM: a vector neural network-based detection model for time synchronization attacks in park-level energy internet. *Intell Robot* 2024;4(4):406-21. <http://dx.doi.org/10.20517/ir.2024.24>

**Received:** 15 Oct 2024 **First Decision:** 6 Nov 2024 **Revised:** 17 Nov 2024 **Accepted:** 21 Nov 2024 **Published:** 29 Nov 2024

**Academic Editor:** Simon Yang **Copy Editor:** Pei-Yun Wang **Production Editor:** Pei-Yun Wang

## Abstract

Micro phasor measurement units ( $\mu$ PMUs) provide high-precision voltage and current phasor data, allowing real-time state estimation and fault detection, which are critical for the stability and reliability of modern power systems. However, their reliance on accurate time synchronization makes them vulnerable to time synchronization attacks (TSAs), which can disrupt grid monitoring and control by corrupting  $\mu$ PMU data. Addressing these vulnerabilities is essential to ensure the secure and resilient operation of smart grids and energy internet technologies. To address these challenges, intelligent detection methods are essential. Therefore, this paper proposes a  $\mu$ PMU measurement data TSA detection model based on vector neural networks (VNNs). This model initially employs a vector neural network to process raw data, effectively extracting and analyzing temporal features. During the same time, a capsule network is employed to classify these temporal features. On this basis, a reconstruction network is used to verify the representational capacity of the model. Simulations based on  $\mu$ PMU measurement data demonstrate that the model exhibits excellent detection capacity in various performance metrics, underscoring its precision and robustness.

**Keywords:** Time synchronization attack, vector neural networks,  $\mu$ PMUs, park-level energy internet, attack detection



© The Author(s) 2024. **Open Access** This article is licensed under a Creative Commons Attribution 4.0 International License (<https://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, sharing, adaptation, distribution and reproduction in any medium or format, for any purpose, even commercially, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made.



## 1. INTRODUCTION

The rapid development of the energy internet in industrial parks is transforming the operational model of traditional power systems. State estimation, as a key link in ensuring the stability and security of power systems, has emerged as a key research focus<sup>[1]</sup>. The application of phasor measurement units (PMUs) in state estimation has significantly enhanced their efficiency and accuracy. PMUs are widely used in smart grids to enhance or replace traditional sensors in supervisory control and data acquisition (SCADA) systems<sup>[2]</sup>. Compared to traditional sensors, PMUs have higher sampling rates, significantly enhancing the real-time performance of wide-area measurement systems<sup>[3]</sup>. Micro PMUs ( $\mu$ PMUs) offer even higher sampling rates, finer measurement accuracy, and more flexible deployment, demonstrating distinct advantages in broader power grid monitoring applications<sup>[4]</sup>. However, accurate time synchronization is critical for  $\mu$ PMUs to capture precise state data from the power grid.

Accurate time synchronization serves as a cornerstone for effective power grid monitoring, enabling precise coordination and data reliability<sup>[5]</sup>. It ensures that each  $\mu$ PMU device can collect data under the same time reference, allowing precise monitoring of the state of the grid.  $\mu$ PMUs can accurately capture the voltage and current phasor information of the grid, providing real-time monitoring of grid operations, thus enhancing the stability and reliability of the power system<sup>[6,7]</sup>. However, with the continued advancement of information technology, grid time synchronization technologies face new challenges<sup>[8]</sup>, one of which is the time synchronization attack (TSA).

TSA is a malicious behavior that disrupts time synchronization in the power grid by tampering with time signals. This type of attack exploits system vulnerabilities, using techniques such as injecting false time signals or interfering with the transmission of time signals<sup>[9,10]</sup>, causing  $\mu$ PMUs to receive incorrect time signals. To effectively mitigate these threats, the implementation of intelligent detection technologies is essential. Recent advances in robust consensus mechanisms have shown that resilient consensus can be achieved in multihop communication with path-dependent delays, even within random dynamic networks under mobile malicious attacks<sup>[11,12]</sup>. These studies provide essential theoretical support for building robust frameworks capable of detecting TSA in complex networked environments. Such technologies employ sophisticated algorithms to continuously monitor synchronization data in real time, facilitating automatic identification of anomalies indicative of TSA<sup>[13]</sup>. This proactive approach facilitates early warnings, enhancing system resilience and robustness against potential attacks. As a result,  $\mu$ PMUs can report incorrect voltage or current phasor data, leading to misjudgments about the state of the grid at the control center, and potentially resulting in operational scheduling errors. Moreover, during long-term grid operation, repeated errors may lead to the accumulation of synchronization data discrepancies<sup>[14]</sup>, potentially triggering more severe grid safety incidents. Detecting and preventing TSAs and ensuring the authenticity of grid monitoring data have become urgent issues that need to be addressed.

Scholars from various regions have conducted relevant research on attack detection. Existing detection models can be categorized into fully supervised learning models<sup>[15–17]</sup>, semi-supervised learning models<sup>[18–20]</sup>, and unsupervised learning models<sup>[21,22]</sup> based on their learning approaches. Fully supervised learning models rely on large amounts of labeled data, using known attacks and normal behavior to train the model for classification. Semi-supervised learning models combine a small amount of labeled data with a large amount of unlabeled data, improving detection performance through pseudo-labeling or other techniques. Unsupervised learning models, on the other hand, do not require labeled data; they rely on the intrinsic structure or patterns in the data to identify potential anomalies and attack behaviors.

While fully supervised models are dependent on a substantial quantity of high-quality labeled data, in the context of TSA issues within park-level energy internet environments involving  $\mu$ PMU measurement data, it is often difficult to obtain a large volume of labeled data. Although unsupervised learning models do not

require labeled data, they are generally incapable of precise classification or prediction and are commonly used to detect distributed denial of service (DDoS) attacks<sup>[23]</sup>. Semi-supervised learning models can be effectively trained with a small amount of labeled data and a large amount of unlabeled data; however, these models are often complex in structure, accompanied by high computational costs and unstable training processes. Against this backdrop, the vector neural network (VNN) has emerged as an advanced model offering greater flexibility. VNNs possess strong adaptability and can be tailored to various supervised learning modes based on actual application needs. In wide-area power grids, VNNs have demonstrated the capability to detect attacks<sup>[24]</sup>, thereby enhancing the security and stability of the system.

Therefore, this paper analyzes the application of  $\mu$ PMUs in park-level energy internet systems, the principles of TSAs, and their impact on grid monitoring. To address the TSA issue, a VNN-based detection model (VNN-DM) is proposed. The model incorporates the design concepts of both VNNs and convolutional neural networks (CNNs), enabling the analysis of features in data collected by  $\mu$ PMUs, and achieving detection of TSA data in smart grids. VNNs offer considerable flexibility, adapting to various supervised learning modes based on actual usage scenarios, and possess the ability to recognize complex patterns and attack behaviors. In complex attack scenarios, they exhibit high accuracy and robustness. The contributions of this paper are as follows:

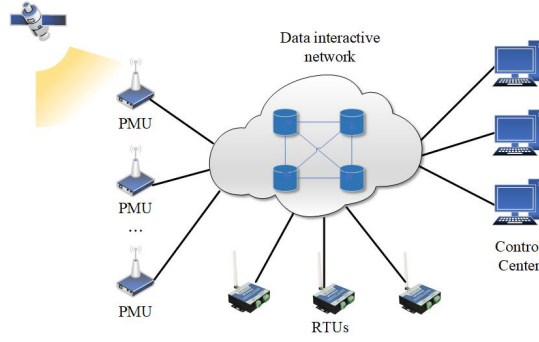
1. Clarification of the characteristics of  $\mu$ PMU measurement data under TSA: This paper conducts an in-depth study of the impact of TSAs on  $\mu$ PMU data, revealing how attacks manipulate time signals to cause deviations in power grid state estimation. This provides a theoretical foundation for the design of effective detection methods.
2. Proposal of a TSA detection model based on VNNs (VNN-DM): Building on the VNN architecture, this paper introduces convolutional layers for multi-scale temporal feature extraction and enhances the feature classification capability of capsule networks by optimizing the dynamic routing mechanism. The VNN-DM model achieves precise analysis of power grid states and attack detection in response to TSA issues in park-level energy internet, offering strong detection accuracy and robustness.

The remainder of the paper is structured as follows: Chapter 2 explores the application of  $\mu$ PMU in power grids and the threat of TSAs to grid security. Chapter 3 introduces the improved VNN-DM model for detecting TSAs in  $\mu$ PMU measurement data within park-level energy internet. Chapter 3 validates the performance of the VNN-DM model through simulation experiments, demonstrating its advantages in detection accuracy and robustness. Finally, Chapter 4 concludes the research findings and proposes directions for future work.

## 2. TSA IN PARK-LEVEL ENERGY INTERNET

In the park-level energy internet,  $\mu$ PMUs, with their high sampling rate and fine measurement accuracy, have become key components in power system state estimation. The measurement data from  $\mu$ PMUs is transmitted through the power communication network to the control center, where it is analyzed to estimate the current state of the power system, detect potential faults, and send control signals back to remote terminal units (RTUs) to execute corresponding operations. This ensures the reliability of the system, as illustrated in [Figure 1](#). The accuracy of  $\mu$ PMU data is crucial for the precision of state estimation and forms the foundation for the stable operation of power systems.

However, TSA poses a real threat to the accuracy of  $\mu$ PMU data. As shown in [Figure 1](#), TSA attackers can send GPS spoofing signals around the target  $\mu$ PMU without needing to infiltrate the monitoring system or physically access the  $\mu$ PMU. By tampering with the time synchronization signals, TSA causes measurement data with incorrect timestamps to be transmitted to the control center, leading to errors in the system state estimation. These erroneous data may bypass simple algorithmic detection and affect the operational scheduling of the power system. While some data processing programs can handle measurement errors, most of them only



**Figure 1.** PMU measurement in smart grids. PMU: Phasor measurement unit.

account for errors caused by noise or data packet loss. Since TSA can introduce time deviations that easily bypass basic defense mechanisms such as smoothing filters and bad data detection (BDD), investigating the impact of TSA on  $\mu$ PMU data collection and ensuring the reliability of grid monitoring data has become a pressing issue that needs to be addressed.

### 2.1. Principle of system state estimation

In the power system network,  $\mu$ PMUs are strategically distributed across the buses, providing detailed measurements of system dynamics.  $\mu$ PMUs capture both the complex voltage of the bus and the complex currents flowing through all transmission lines connected to it, enabling precise monitoring of power flow dynamics. Considering a local network, suppose there are  $N_b$  buses, connected by  $N_l$  transmission lines. The number of transmission lines connected to bus  $n$  is  $L_n$ . The set of other buses connected to bus  $n$  is denoted as  $B_n$ . The  $\mu$ PMU measurement vector is  $Z = [z_1, \dots, z_{N_b}] \in R^{N_b}$ . The bus voltage vector for all bus-es is denoted as  $V_n = [v_{nr}, v_{nj}] \in R^{N_b \times 2}, n = 1, \dots, N_b$ , where  $v_{nr}$  and  $v_{nj}$  represent the real and imaginary parts of  $V_n$ , respectively. Similarly, for the branch connected to bus  $n$ , the complex current vector of the bus transmission line can be expressed as  $I_n = [I_{nk} | (i_{nk,r}, i_{nk,j})] \in R^{N_b \times L_n \times 2}, n = 1, \dots, L_n$ , where  $i_{nk,r}$  and  $i_{nk,j}$  represent the real and imaginary parts of the complex current  $I_{nk}$  of the transmission line  $k$  and bus  $n$ . The measurement vector is:

$$z_n = \begin{bmatrix} v_{nr} \\ v_{ni} \\ \{i_{nk,r}\} \\ \{i_{nk,j}\} \end{bmatrix} = \begin{bmatrix} |V_n| \cos \theta_n \\ |V_n| \sin \theta_n \\ |I_{nk}| \cos \theta_{nk} \\ |I_{nk}| \sin \theta_{nk} \end{bmatrix} \quad (1)$$

Where  $\theta_k$  and  $\theta_n$  are the corresponding phase angles of the voltage and current. In the classical state estimation problem, the relationship between the  $\mu$ PMU measurements and the system state vector is established as follows:

$$Z = h(X) + e \quad (2)$$

where  $h(X)$  represents the measurement function of the system state vector  $X = [x_1, \dots, x_m]^T \in R^m$ ;  $e = [e_1, \dots, e_{N_b}]$  represents the random measurement errors introduced during the measurement process. These errors follow a Gaussian distribution  $e \sim N(0, \sigma^2)$ , and the covariance matrix  $R$  is denoted as  $R = \text{diag}[\sigma_1^2, \dots, \sigma_{N_b}^2]$ . During the state estimation process using  $\mu$ PMUs, to improve the accuracy of the estimation, the weighted least

squares (WLS) method is commonly employed to adjust the weight of the measurement values. The measurement residual is defined as  $r = Z - h(X)$ . To quantify the deviation between the measured value and the estimated value, the objective function  $Y_{WLS}$  is expressed as the weighted sum of squared residuals:

$$Y_{WLS} = (Z - h(X))^T R^{-1} (Z - h(X)) \quad (3)$$

To obtain the optimal state estimation, it is necessary to minimize the objective function  $Y_{WLS}$ . Therefore, the new objective function can be written as:

$$\min Y_{WLS} = (Z - h(X))^T R^{-1} (Z - h(X)) \quad (4)$$

Assume the initial state estimate is  $x^{(t)}$ , such that  $h(X)$  is linear around the initial estimate. By performing a Taylor series expansion of  $h(X)$  at  $x^{(t)}$  we obtain:

$$h(X) = h(x^{(0)}) + H(x^{(0)}) \Delta x + \frac{1}{2} H'(x^{(0)}) (\Delta x)^2 + \dots + \frac{1}{n!} H^{(n)}(x^{(t)}) (\Delta x)^n \quad (5)$$

Where  $J(\cdot)$  is the Jacobian matrix of  $h(\cdot)$ .

$$J(\cdot) = \frac{\partial h(X)}{\partial x} \quad (6)$$

Substituting the higher-order terms and applying the formula and let  $\tilde{r}_t = Z - h(x^{(t)})$ :

$$Y_{WLS} = (\tilde{r}_t - J(x^{(t)}) \Delta x)^T R^{-1} (\tilde{r}_t - J(x^{(t)}) \Delta x) \quad (7)$$

To obtain the optimal objective function, set  $\frac{\partial Y_{WLS}}{\partial \Delta x} = 0$  and solve for the estimate of  $\Delta \hat{x}$ :

$$\Delta \hat{x} = \left( J^T(x^{(t)}) R^{-1} J(x^{(t)}) \right)^{(-1)} J^T(x^{(t)}) R^{-1} \tilde{r}_t \quad (8)$$

Thus, the state estimate vector is iteratively updated according to the iterative formula:

$$\begin{cases} \Delta \hat{x} = \left( J^T(x^{(t)}) R^{-1} J(x^{(t)}) \right)^{(-1)} J^T(x^{(t)}) R^{-1} \tilde{r}_t \\ x^{(t+1)} = x^{(t)} + \Delta \hat{x}^t \end{cases} \quad (9)$$

When  $\Delta \hat{x}$  satisfies the convergence condition  $\Delta \hat{x} \leq \varepsilon$ , the iteration stops. The state estimate  $\Delta \hat{x}$  is obtained. The final value of the state estimate is:

$$\hat{x} = \left( J^T R^{-1} J \right)^{-1} J^T R^{-1} z_t \quad (10)$$

**Table 1. Phase angle error caused by TSA**

Reference	Phase-angle error (degrees)
Jiang et al. [27]	52
Zhang et al. [26]	±60
Shepard et al. [28]	72

TSA: Time synchronization attack.

In system state estimation, the largest normalized residual (LNR) method is used for anomaly detection. This method normalizes the residuals of each measurement and then compares the maximum normalized residual to a predefined threshold. Specifically, if the LNR is below the threshold  $\tau$ , it indicates that the measurement does not contain significant bad data and can be accepted for further analysis and processing. Otherwise, the measurement is considered abnormal, potentially containing erroneous data, and requires further inspection and handling. This method effectively improves the reliability of data quality and enhances the overall stability of the system.

## 2.2. TSA attack model

During a TSA, the attacker sends spoofed GPS signals, introducing incorrect time synchronization in  $\mu$ PMU measurements. This disrupts the phase angles of synchronized data, causing a mismatch between measured and actual phase values [25]. Assume that the attack occurs on bus  $k$ . The power system operates at a frequency  $f$  of 60 Hz. The attack induces a clock shift  $\Delta t_k$  [26], causing the  $\mu$ PMU's phase angle to change, leading to a phase angle deviation  $\Delta\theta_k^{err}$ :

$$\Delta\theta_k^{err} = 2\pi f \Delta t_k \quad (11)$$

Table 1 presents the phase angle deviation errors caused by TSA. The phase angle deviation of the affected bus  $z_{t_k}^{err}$  can be expressed as:

$$z_{t_k}^{err} = z_{t_k} \exp(j\Delta\theta_k^{err}) \quad (12)$$

Through analysis, the relationship between the measurement vector under TSA and the normal measurement vector can be derived. The phase angle deviation  $\Delta\theta_k^{err}$  falls within the interval  $[0, 2\pi]$  or  $[-\pi, \pi]$ , depending on the specific conditions. To further describe the measurement vector under TSA for all buses, the measurement vector is:

$$A_{attack} = \text{diag}\left(E_1, \dots, E_{k_1} \cdot e^{j\Delta\theta_{t_{k_1}}^{err}}, \dots, E_{k_n} \cdot e^{j\Delta\theta_{t_{k_n}}^{err}}, \dots, E_{N_b}\right) \quad (13)$$

Where  $E_n$  ( $n = 1, \dots, N_b$ ) is a diagonal matrix.  $E_{k_1}, \dots, E_{k_n}$  represent the  $\mu$ PMUs affected by TSA. The measurement vector for each affected bus can be expressed as:

$$z_{t_k}^{err} = A_{attack} \cdot z_t \quad (14)$$

The residual error vector is:

$$\|r^{err}\| = \|z_{t_k}^{err} - J\hat{x}\| = A_{attack} \cdot z_t - J(J^T R^{-1} J)^{-1} J^T R^{-1} \cdot z_t \quad (15)$$

An adversary can exploit the attack matrix  $A_{attack}$ , which satisfies condition  $\|r^{err}\| \leq \tau$ . This can allow the attack to bypass basic detection mechanisms such as BDD. A TSA attack enables an attacker to inject falsified phase measurement data, causing the system to incorrectly assume that its state estimation is accurate. This erroneous state estimation may lead to failures in power dispatch and control decisions, further triggering a chain reaction that affects the efficiency and safety of power generation and transmission. Experimental studies [29] have shown that TSA can evade BDD detection by subtly adjusting the PMU timing, thus masking timing discrepancies within acceptable limits of detection mechanisms such as the  $\chi^2$  test. These adjustments, while seemingly minor, allow timing errors to accumulate undetected over time, exacerbating system vulnerabilities. The growing dependency on synchronized measurement data in modern power grids magnifies the risks posed by such attacks. Therefore, effectively detecting TSA attacks is crucial to ensuring the secure operation of the power system.

### 3. TSA DETECTION MODEL

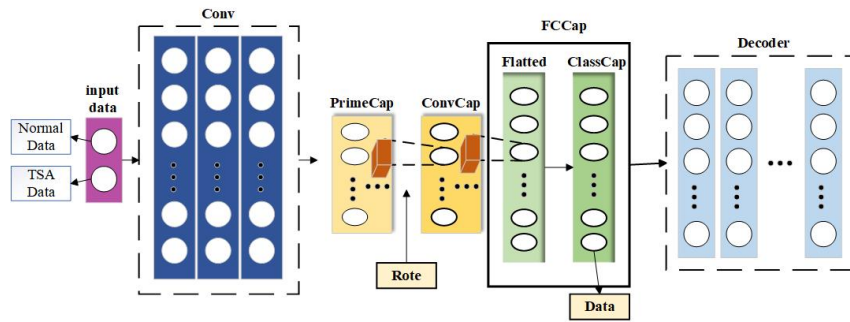
VNNs are a type of neural network model specifically designed to process vector data. They comprise vector neurons (capsules) that use vector outputs instead of traditional scalar-based feature detectors [30,31]. Each vector neuron retains instantiation parameters and uses a dynamic routing mechanism to transmit data to the next layer, while preserving the direction, posture, and spatial information of the target features. Compared to traditional neural networks, VNNs are better at capturing temporal information and geometric relationships in input data. In  $\mu$ PMU measurements, the physical information of magnitude and phase angle are closely related, and the use of VNNs can preserve these relationships, allowing for more accurate detection of phase angle shifts caused by TSA. To address the TSA problem in the park-level energy internet environment, this paper introduces a multi-layer CNN for multi-scale temporal feature extraction and optimizes the dynamic routing mechanism of VNNs to better capture the geometric relationships and feature variations in temporal data. Additionally, a multi-layer perceptron (MLP) is integrated to reconstruct the classification results, enhancing the model's robustness and detection accuracy in complex attack scenarios. The structure of the VNN-DM model is shown in Figure 2. The model consists of a convolutional Layer, a primary capsule layer (PrimeCap), a convolutional capsule layer (ConvCap), a fully connected capsule layer (FCCap), and a decoder. During the feature extraction phase, a multi-layer convolutional structure with different kernel sizes is used to extract multi-scale temporal features. The dynamic routing mechanism enhances the feature classification capabilities of the capsule network, ensuring the model effectively adapts to feature variations in data under different attack modes. Finally, the MLP reconstructs the feature classification results, improving the model's robustness and detection accuracy in complex attack scenarios within localized networks.

#### 3.1. Dynamic routing between vector neurons

Dynamic routing establishes a non-linear mapping through an iterative process, enabling more adaptive and hierarchical information flow between network layers. In this process, the data from each lower-level capsule (sub-capsule) is passed to the appropriate higher-level capsule (parent capsule) in the next layer. Dynamic routing adaptively modulates the connection strength between sub-capsules and parent capsules, leveraging the output of the sub-capsules, thereby increasing or decreasing these connections. Let the data in the sub-capsule be denoted as  $z_n$ . The relationship between sub-capsule  $n$  and parent capsule  $k$  can be expressed as:

$$\hat{z}_{k|n} = \omega_{nk} z_n + b_{k|n} \quad (16)$$





**Figure 2.** Structure of TSA detection model. TSA: Time synchronization attack.

Where each sub-component of the data encapsulated in the capsule is subjected to positional encoding. This ensures that the prediction includes the correlation between the input data's amplitude and positional phase. In other words, the prediction captures the correlation between the amplitude and phase of the actual input data. Using the measured value as an example, the corresponding peak value in the complex wave is simplified, and the positional encoding data is expressed. The predictive measurement after encoding is given by:

$$\begin{cases} \hat{z}_{k|nr} = \omega_{nk_r} \times z_{nr} + b_{k|nr} \\ \hat{z}_{k|nj} = \omega_{nk_j} \times z_{nj} + b_{k|nj} \end{cases} \quad (17)$$

$$\hat{z}_{k|n} = [\hat{z}_{k|nr}, \hat{z}_{k|nj}]^T \quad (18)$$

Where  $\hat{z}_{k|n}$  is the contribution of the child capsule  $z_n$  to the father capsule  $v_k$ . Assuming that a child capsule provides input, based on dynamic routing, the contribution from the latent parent capsule is derived as follows:

$$z_k = \sum c_{nk} \hat{z}_{k|n}, n \in \{1, \dots, i\} \quad (19)$$

$$v_k = g(z_k) = squish(z_k) = \frac{\|z_k\|}{1 + \|z_k\|^2} \cdot \frac{z_k}{\|z_k\|} \quad (20)$$

Where  $g(z_k)$  is a non-linear activation function. The iterative update of the selection coefficient  $c_{nk}$  uses the *SoftMax* function, expressed as:

$$c_{nk} = SoftMax(b_{k|n}) \quad (21)$$

The parent capsule  $v_k$  is the result of a non-linear compression and normalization of the weighted sum of predicted vectors, and the existence probability of the parent capsule is expressed as  $\|v_k\|_2$ . The parent capsule's prediction is regularized using dynamic routing with iterative weighted averaging and non-linear compression. The iterative value of  $b_{k|n}$  is updated as:

$$b_{k|n} = b_{k|n} + \hat{z}_{k|n} \cdot v_k \quad (22)$$



In the initial stage, the prediction weights  $b_{k|n}$  are set to 0. The flow chart of complex dynamic routing is shown in Algorithm 1. The dynamic routing mechanism trains parameters by predicting vectors and obtains capsule output.

---

**Algorithm 1** Routing Process for Capsules
 

---

```

1: Begin
2: Initialize the routing coefficients between capsule  $i$  in layer  $l$  and capsule  $k$  in layer  $l + 1$ .
3: Compute the prediction vectors.
4: for all capsules  $n$  in layer  $l$  do
5:     Calculate the SoftMax values.
6: end for
7: Accumulate the prediction vectors for all capsules in layer  $l + 1$ .
8: Apply the squash function for all capsules in layer  $l + 1$ .
9: for  $n$  iterations do
10:    Update the routing coefficients for all capsules  $i$  in layer  $l$  and capsules  $k$  in layer  $l + 1$ .
11: end for
12: Return the final routing vector.
13: End
  
```

---

This dynamic routing process can be likened to a reinforcement learning mechanism. The process ensures each layer's input is recalculated based on the forward propagation strategy. During network training, the optimization strategy relies on a margin loss function, defined as:

$$L_c = T_c \cdot \max(0, m^+ - \|v_k\|)^2 + \lambda (1 - T_c) \cdot \max(0, m^- - \|v_k\|)^2 \quad (23)$$

Here,  $T_c$  is the target output for class  $c$  and  $T_c$ . If the target is the correct class,  $T_c=1$ ; otherwise,  $T_c=0$ .  $m^+$  is the upper margin (typically set to 0.9) and  $m^-$  is the lower margin (typically set to 0.1). A regularization weight  $\lambda$  is applied to the total loss.  $v_k$  is the output vector. The weight update for the layers during back-propagation is given by:

$$\delta^L = \nabla_{v_k} L_c \odot \sigma'(\hat{z}'_{k|n}) \quad (24)$$

Where  $\nabla_{v_k}$  denotes the gradient of the loss function with respect to  $v_k$ .  $\sigma'(\cdot)$  represents the derivative of the activation function. The error in back-propagation is calculated layer by layer, with the error in back-propagation being:

$$\delta^l = \left( (\omega^{l+1})^T \delta^{l+1} \right) \odot \sigma'(\hat{z}'_{k|n}) \quad (25)$$

Where  $\omega^{l+1}$  is the transpose of the weight matrix in layer  $l + 1$ . After updating the weights and biases layer by layer using the gradient descent method, the model returns the updated weight matrix  $\omega^l$ . The reset method is defined as:

$$\omega^l = \omega^l - \frac{\eta}{m} \sum \delta^l (z_n^l)^T \quad (26)$$

Where  $\eta$  is the learning rate, and the learning rate and  $m$  is the sample size.

### 3.2. TSA detection model

The overall structure of the VNN-DM model consists of two components: an encoder and a decoder. The encoder is primarily responsible for data extraction and representation, while the decoder enhances the model's representational capacity. This section provides a detailed explanation of the detection model's structure.

#### 3.2.1 Encoder

The encoder consists of Conv, PrimCap, ConvCap, and FCCap layers. Multiple convolutional layers are employed to extract features from the input data. When the measured data is fed into the convolutional layers, the local feature detectors are activated by the rectified linear unit (ReLU) to capture the underlying features of the data:

$$z_i = \text{ReLU} \left( \sum_n^i \omega_i \cdot x_i + b_i \right) \quad (27)$$

Here,  $\omega_i$  represents the weight matrix of the feature map in the  $i$ -th capsule. For the fully connected capsule, the input is two-dimensional, and the positional relationship between the data is retained, making it crucial in ensuring the effective use of capsule networks for feature extraction.

The initial capsule feature vector is a high-dimensional compressed data vector combined with multiple parameters based on actual input data, maintaining the correlation between the amplitude and positional phase. The relevant equation is:

$$v_j^l = g \left( \sum_j^n c_{ij} \cdot (\omega_{ij} \cdot z_i + b_{ij}) \right) \quad (28)$$

Where  $c_{ij}$  is the coefficient calculated by the machine during dynamic routing. A fully connected capsule network will predict the output of each capsule layer differently, requiring different weight matrices  $M_l$ , to normalize the prediction result of each capsule using the matmul function:

Due to the dimensional differences between the fully connected capsule layer and the convolutional capsule layer, a pose matrix  $M_l$  is required. This matrix is composed of the direction cosines of two different sets of orthonormal basis vectors:

$$z_j = \text{matmul} \left( v_j^l \cdot M_l \right) \quad (29)$$

Here,  $\text{matmul}(\cdot)$  represents the matrix product between the prediction matrix and the corresponding matrix in the capsule layers. Each  $v_j = g(z_j)$  represents a class, while  $a = \|v_j\|_2$  denotes the probability of belonging to that class. This allows for determining whether the measured values are normal or influenced by a TSA attack.

### 3.2.2 Decoder

The decoder adopts a MLP structure. It is designed to reconstruct the input feature vector from the latent space representation  $x$  produced by the encoder. This component is critical to the model's reconstruction ability, with the primary objective of enhancing the model's robustness and representational power through the reconstruction process, thus improving performance in anomaly detection tasks within time series data, particularly in the context of TSA attacks. The decoder comprises several fully connected layers, which progressively expand the dimensionality of the latent space, ultimately outputting the reconstructed data  $\hat{x}$  with the same shape as the original input  $x$ . The calculation of the latent representation received by the decoder from the encoder is given by:

$$h = f_{en}(x) \quad (30)$$

Where  $f_{en}$  represents the latent space of the decode and  $x$  is the original input data. The decoder extracts the essential features of the input data and maps it to the latent space using:

$$h_1 = \text{ReLU}(W_1 h + b_1) \quad (31)$$

Where  $W$  is the weight matrix and  $b$  is the bias term. This ReLU activation function enhances the non-linear feature extraction capability of the decoder, allowing the latent space to enter the higher-dimensional feature space through multiple layers. If the capsule is used for TSA detection, the network computes the reconstruction error using the sigmoid function to ensure the output matches the original input data, defined as:

$$\hat{x} = \text{sigmoid}(W_n h_{n-1} + b_n) \quad (32)$$

To balance the reconstruction error, the mean squared error (MSE) is used as the loss function  $\rho$ , and this error evaluates the difference between the original input data features and the output of the decoder:

$$\rho = \|x - \hat{x}\|^2 \quad (33)$$

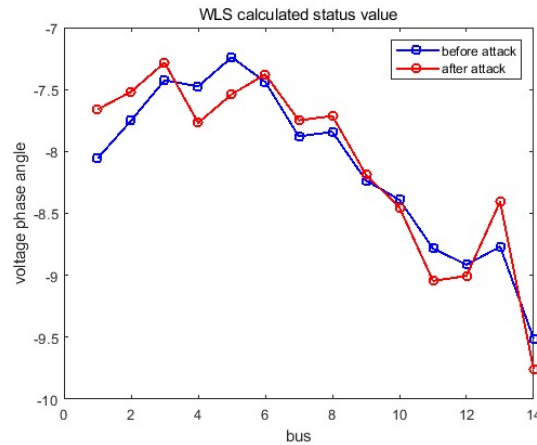
By minimizing the error, the model can accurately reconstruct the input data, ensuring that the capsule network retains the feature extraction and representational power necessary for TSA detection tasks.

## 4. RESULTS

To simulate the basic equipment and scenarios of a regional energy internet and verify the effectiveness of the detection model, this paper generates a simulation dataset based on the IEEE 14-bus standard network, incorporating the fundamental characteristics of a regional energy internet. The IEEE 14-bus network is a widely used and standardized test system that provides representative operational scenarios for power systems within energy internet frameworks. The network includes key components such as generators, transformers, and load nodes, effectively reflecting the complexity of multi-node, multi-device coordinated operation in a regional energy internet. Using the standard topology and parameter settings provided by the Matpower toolbox, this paper simulates measurement data samples under real-world conditions. To better represent the measurement errors found in actual data, the signal-to-noise ratio (SNR) of the simulation dataset is set to 20

**Table 2. Training data set**

Data type	Training data	Test data
Measure data	12000	3000
Attack data	12000	3000

**Figure 3.** State estimation with or without attack.

dB, thereby simulating measurement data with random noise. Additionally, to evaluate the performance of the detection model under malicious attacks, this paper introduces a TSA at one of the nodes in the IEEE 14-bus network, simulating the power system state of a regional energy internet under such attacks. This process generates power data samples for both normal and attack scenarios. The simulation dataset is shown in Table 2.

#### 4.1. The impact of TSA attacks on energy internet systems

To analyze the impact of TSA attacks on park-level energy internet, this paper designs a system state estimation simulation scenario based on the IEEE 14-bus standard network. The system state estimation method follows the approach outlined in Chapter 2. During the state estimation process, this paper simulates an attacker's TSA on the system, with the attack set at Node 4. The WLS calculation values under both attack and non-attack conditions are shown in Figure 3.

The experimental results demonstrate that significant deviations in voltage phase angles occurred at multiple nodes before and after the attack, with the attack on Node 4 also causing deviations at other nodes. This is because the power system is a complex network where the state of each node depends not only on its own attributes but also on the states of the nodes it is connected to. When Node 4 is attacked, its voltage phase angle is tampered with or disturbed, altering the power flow and phase angle distribution between this node and its neighboring nodes, which in turn causes changes in the states of other nodes. The TSA attack directly influences the time synchronization of measurement devices, leading to phase angle shifts in state estimation. Distortion in state estimation can result in incorrect power flow control and dispatch, thereby affecting the normal operation and energy distribution of the system. This has significant implications for the reliability and security of the regional energy internet system.

#### 4.2. Model performance evaluation

To evaluate the performance of the proposed model, this paper introduces the Confusion Matrix to quantify the gap between predicted results and actual outcomes. The Confusion Matrix is a method for visualizing computational results, and its structure is shown in Table 3. From this matrix, four key parameters can be derived: true positive (TP), true negative (TN), false positive (FP), and false negative (FN). Using these parameters,

Table 3. Confusion matrix

	Actual value (positive)	Actual value (negative)
Predicted value (positive)	TP	FP
Predicted value (negative)	FN	TN

TP: True positive; FP: false positive; FN: false negative; TN: true negative.

Table 4. Model rating index

Model	Accuracy	Precision	Recall	F1-score
1-layer convolutional model	0.5493	0.5591	0.4667	0.5087
Model from ref. [20]	0.8747	0.8482	0.9127	0.8793
VNN-DM	0.8950	0.8741	0.9207	0.8968
MLP	0.8153	0.7986	0.8433	0.8204
SVM	0.7740	0.7553	0.8107	0.7820
KNN	0.6487	0.6345	0.7013	0.6662

VNN-DM: Vector neural network-based detection model; MLP: multi-layer perceptron; SVM: support vector machine; KNN: K-nearest neighbor.

several evaluation metrics can be calculated, including accuracy, precision, recall, and F1-score, as well as the receiver operating characteristic (ROC) curve and the area under the curve (AUC), to quantify the model's performance. These metrics are defined as follows:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (34)$$

$$Precision = \frac{TP}{TP + FP} \quad (35)$$

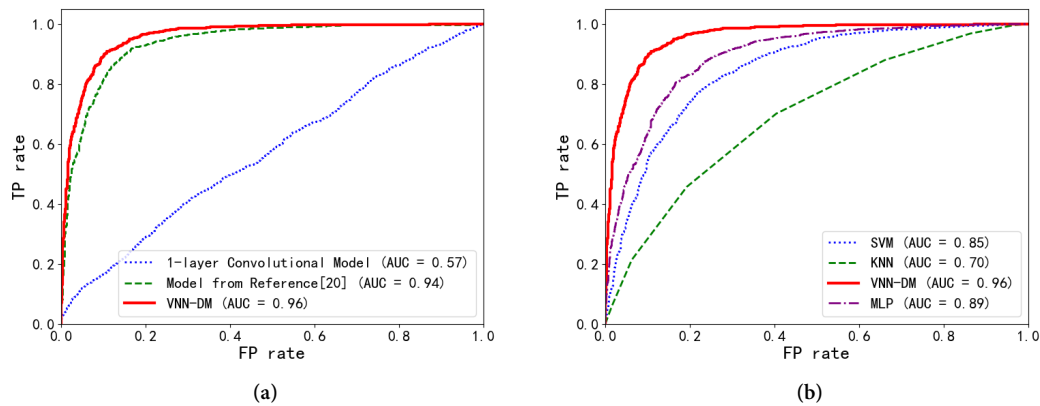
$$Recall = \frac{TP}{TP + FN} \quad (36)$$

$$F1\text{-measure} = \frac{2 \times Precision \times Recall}{Precision + Recall} \quad (37)$$

Accuracy reflects the overall correctness of the model's predictions. Precision evaluates the proportion of correctly predicted positive samples among all samples predicted as positive. Recall measures the model's ability to correctly identify positive samples among all actual positive samples. The F1-score is used to assess the model's performance on imbalanced datasets and is the harmonic mean of Precision and Recall.

To validate the effectiveness of the VNN-DM detection model in TSA detection tasks, two sets of experiments were designed to compare the performance of different models on the same test dataset. The first set of experiments analyzed the detection capability differences between a single-layer convolutional model, the reference model, and the proposed VNN-DM model, aiming to verify the performance improvements in feature extraction and classification achieved by combining a multi-layer convolutional network structure with a capsule network. The second set of experiments compared traditional machine learning models, including support vector machine (SVM), K-nearest neighbor (KNN), and MLP, to further assess the performance improvements of the VNN-DM model over traditional models. The evaluation metrics for all models in both sets of experiments are shown in Table 4.

Additionally, to further highlight the classification performance of the models, ROC curves were plotted for both sets of experiments. The ROC curve illustrates the model's discriminative ability by displaying the relationship between the true positive rate (TPR) and the false positive rate (FPR). To quantify the overall perfor-



**Figure 4.** ROC curves and AUC values corresponding to different models. (A) First set of experiment; (B) Second set of experiment. ROC: Receiver operating characteristic; AUC: area under the curve.

mance of the ROC curve, the AUC was calculated, with values closer to 1 indicating better model performance. Figure 4 presents the ROC curves for the different models, with Figure 4A showing the ROC curve and AUC values for the first experiment, and Figure 4B for the second experiment.

An analysis of the ROC curves and the experimental results in Table 4 clearly demonstrates significant performance differences among the models in the TSA detection task. In the first set of experiments, the single-layer convolutional model performed poorly across all metrics, indicating clear deficiencies in feature extraction and classification, making it difficult to handle data with complex temporal features. In contrast, the reference model showed considerable improvement, but still suffered from a certain degree of false positives and false negatives, indicating that the detection performance was not optimal. The proposed VNN-DM model, utilizing a multi-layer convolutional structure, outperformed the other models in terms of accuracy, precision, and recall. As shown by the ROC curve in Figure 4A, the AUC value of the VNN-DM model is 0.96, higher than the 0.57 of the single-layer convolutional model and the 0.94 of the reference model. This demonstrates that the VNN-DM model can more effectively differentiate between normal data and attack data, particularly when dealing with complex multi-node joint attacks and small phase disturbances, exhibiting higher detection accuracy and robustness.

In the second set of experiments, the VNN-DM model achieved an F1-score of 0.8968, significantly higher than the SVM model's 0.7820 and the KNN model's 0.6662, indicating that the VNN-DM model is more effective at extracting data features when handling complex temporal features and multi-node attacks, thus exhibiting greater classification ability and robustness. The MLP model performed well on some metrics, but its F1-score of 0.8204 was still lower than that of the VNN-DM model. The analysis of the ROC curve in Figure 4B shows that the ROC curve of the VNN-DM model is closer to the upper left corner, with an AUC value of 0.96, significantly outperforming other traditional models. This indicates that the VNN-DM model maintains high classification accuracy and low false-positive and false-negative rates when addressing the problem of TSAs in the Park-Level Energy Internet. Therefore, through the combination of a multi-layer convolutional structure and a dynamic routing mechanism, the VNN-DM model further enhances its ability to extract and classify multi-scale temporal features, making it more adaptable to various complex attack types in the Park-Level Energy Internet environment, thus establishing it as a more robust TSA detection model.

## 5. CONCLUSIONS

We address the challenge of TSA in the park-level energy internet by proposing the VNN-DM model, an innovative detection framework that combines VNNs with CNN, specifically tailored for  $\mu$ PMU-based TSA detection. Experimental results validate that VNN-DM achieves high accuracy and robustness, outperforming benchmark models, and thus advancing the current state-of-the-art in TSA detection. Through comprehensive analysis of  $\mu$ PMU data, we demonstrate the practical applicability of the model to maintaining reliable state estimation under TSA conditions, effectively mitigating a critical vulnerability in the Energy Internet. The unique architecture of VNN-DM, integrating vector processing and capsule networks, enables precise extraction of multi-scale temporal features, representing a significant methodological advancement over traditional approaches. Future efforts will focus on deploying the model on edge devices, thereby extending its applicability to more diverse and complex real-world scenarios. VNN-DM thus offers a deployable solution for bolstering grid resilience against TSA, contributing to the secure evolution of smart grid infrastructure and setting a new benchmark within this field.

## DECLARATIONS

### Authors' contributions

Implemented the methodologies presented and wrote the paper: Yang J

Developed the idea of the proposed framework: Shi F

Responsible for data collection and technical support: Li Y, Zhao Z

Managed and supervised the research project: Cui Q

All authors have revised the text and agreed to the published version of the manuscript.

### Availability of data and materials

Not applicable.

### Financial support and sponsorship

The work is supported by the National Natural Science Foundation of China (No. U23A20651)

### Conflicts of interest

All authors declared that there are no conflicts of interest.

### Ethical approval and consent to participate

Not applicable.

### Consent for publication

Not applicable.

### Copyright

© The Author(s) 2024.

## REFERENCES

1. Wu Z, Mao L, Li K, He S. Power distribution network state assessment technology based on unified computing resource pool. In: 2022 7th Asia Conference on Power and Electrical Engineering (ACPEE); 2022 Apr 15-17; Hangzhou, China. IEEE; 2022. pp. 931–7. [DOI](#)
2. Phadke AG, Bi T. Phasor measurement units, WAMS, and their applications in protection and control of power systems. *J Mod Power Syst Clean Energy* 2018;6:619–9. [DOI](#)
3. Sexauer J, Javanbakht P, Mohagheghi S. Phasor measurement units for the distribution grid: Necessity and benefits. In: 2013 IEEE PES innovative smart grid technologies conference (ISGT); 2013 Feb 24-27; Washington, USA. IEEE; 2013. p. 1–6. [DOI](#)
4. Xue AC, Xu FY, You HY, Xu J, Martin KE, Bi T. Robust parameter identification of distribution line based on micro PMU. *Electr Power Autom Equip* 2019;39:1–7. [DOI](#)



5. Zhao T, Li Z, Zou B, He Z, Ren S. Wide-area time synchronization method for mutual preparation of satellite clock and network clock. *Automat Electr Power Syst* 2017;41:202–7. DOI
6. Xu J, Wu Z, Hu Q, et al. Interval state estimation for active distribution networks considering uncertainties of multiple types of DGs and loads. *Proc CSEE* 2018;38:3255–66. DOI
7. Tian S, Li K, Wei S, Fu Y, Li Z, Liu S. Security situation awareness approach for distribution network based on synchronous phasor measurement unit. *Proc CSEE* 2021;41:617–31. DOI
8. Qian B, Cai Z, Xiao Y, et al. Review on time synchronization attack in power system. *Power Syst Technol* 2020;44:4035–45. DOI
9. Zhao X, Liu G, Li L. Importance-driven denial-of-service attack strategy design against remote state estimation in multi-agent intelligent power systems. *Intell Robot* 2024;4:244–55. DOI
10. Bi T, Guo J, Xu K, Zhang L, Yang Q. The impact of time synchronization deviation on the performance of synchrophasor measurements and wide area damping control. *IEEE Trans Smart Grid* 2017;8:1545–52. DOI
11. Shang Y. Resilient vector consensus over random dynamic networks under mobile malicious attacks. *Comput J* 2023;67:1076–86. DOI
12. Shang Y. Resilient consensus in continuous-time networks with  $\ell$ -hop communication and time delay. *Syst Control Lett* 2023;175:105509. DOI
13. Zeng H, Ye Z, Zhang D, Lu Q. Robust distributed model predictive control of connected vehicle platoon against DoS attacks. *Intell Robot* 2023;3:288–305. DOI
14. Xue A, Xu F, Martin KE, Xu J, You H, Bi T. Linear approximations for the influence of phasor angle difference errors on line parameter calculation. *IEEE Trans Power Syst* 2019;34:3455–64. DOI
15. Saraswat D, Bhattacharya P, Zuhair M, Verma A, Kumar A. AnSMart: a SVM-based anomaly detection scheme via system profiling in smart grids. In: 2021 2nd International Conference on Intelligent Engineering and Management (ICIEEM); 2021 Apr 28–30; London, UK. IEEE; 2021. pp. 417–22. DOI
16. Niu X, Li J, Sun J, Tomsovic K. Dynamic detection of false data injection attack in smart grid using deep learning. In: 2019 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT); 2019 Feb 18–21; Washington, USA. IEEE; 2019. pp. 1–6. DOI
17. Jeyaselvi M, Sathya M, Suchitra S, Ibrahim SJA, Chakravarthy NSK. SVM-based cloning and jamming attack detection in IoT sensor networks. In: Goar V, Kuri M, Kumar R, Senjyu T, editors. Advances in information communication technology and computing: proceedings of AICTC 2021. Springer; 2022. pp. 461–71. DOI
18. Zou Z. Research on detection and defense in smart grid GPS spoofing attack. 2022. DOI
19. Zhang Y, Wang J, Chen B. Detecting false data injection attacks in smart grids: a semi-supervised deep learning approach. *IEEE Trans Smart Grid* 2020;12:623–34. DOI
20. Tan Q. GAN-based adversarial attack and defense on time series classification. 2023. DOI
21. Hoang TM, Nguyen NM, Duong TQ. Detection of eavesdropping attack in UAV-aided wireless systems: Unsupervised learning with one-class SVM and k-means clustering. *IEEE Wireless Commun Lett* 2019;9:139–42. DOI
22. Ma Z, Ma H, Gao X, et al. An improved DDoS attack detection model based on unsupervised learning in smart grid. In: Xiong J, Wu S, Peng C, Tian Y, editors. International Conference on Mobile Multimedia Communications. Springer; 2021. pp. 550–62. DOI
23. Zheng C, Wang H, Liu R. A review of research on DDoS attack detection in SDNs. *Comput Eng Appl* 2024;1–20. Available from: <https://link.cnki.net/urlid/11.2127.TP.20240814.1351.006>. [Last accessed on 25 Nov 2024]
24. Huang R, Li Y. False phasor data detection under time synchronization attacks: a neural network approach. *IEEE Trans Smart Grid* 2022;13:4828–36. DOI
25. Akkaya I, Lee EA, Derler P. Model-based evaluation of GPS spoofing attacks on power grid sensors. In: 2013 Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSPCES); 2013 May 20; Berkeley, USA. IEEE; 2013. p. 1–6. DOI
26. Zhang Z, Gong S, Dimitrovski AD, Li H. Time synchronization attack in smart grid: impact and analysis. *IEEE Trans Smart Grid* 2013;4:87–98. DOI
27. Jiang X, Zhang J, Harding BJ, Makela JJ, Dominguez-García AD. Spoofing GPS receiver clock offset of phasor measurement units. *IEEE Trans Power Syst* 2013;28:3253–62. DOI
28. Shepard DP, Humphreys TE, Fansler AA. Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks. *Int J Crit Infrastruct Prot* 2012;5:146–53. DOI
29. Shereen E, Delcourt M, Barreto S, Dán G, Le Boudec JY, Paolone M. Feasibility of time-synchronization attacks against PMU-based state estimation. *IEEE Trans Instrum Meas* 2020;69:3412–27. DOI
30. Hinton GE, Krizhevsky A, Wang SD. Transforming auto-encoders. In: Artificial Neural Networks and Machine Learning - ICANN 2011: 21st International Conference on Artificial Neural Networks. Springer; 2011. pp. 44–51. DOI
31. Sabour S, Frosst N, Hinton GE. Dynamic routing between capsules. In: Proceedings of the 31st International Conference on Neural Information Processing Systems. 2017. pp. 3859–69. DOI