A Communication Network Robustness Estimation Method Based on an Improved ELM

Guo-Yi WEN¹,², Ning HUANG¹,* and Wei-Qiang WU³

¹School of Reliability and Systems Engineering, Beihang University, Xue Yuan Road No. 37, HaiDian District, Beijing, China, 100083
²Department of Aeronautic Electronics, The First Aeronautic Institute of Air Force, Shihe District, Xinyang, China, 464000
³China Huarong Asset Management Co., Ltd. Postdoctoral Research Station, No. 8 Financial Street, Xicheng District, Beijing, China, 100033

Email: wenguoyi@buaa.edu.cn, hn@buaa.edu.cn, wuweiqiang@chamc.com.cn.

Keywords: Estimation, Robustness, Fault-tolerant strategy, ELM, Communication network.

Abstract. The communication network robustness is becoming increasingly important because of its wider applications on higher reliability requirement systems, such as UAV, CBTC, etc. But communication network robustness estimation is becoming more difficult due to related various factors such as attacks, EMI, errors, mobility, fault-tolerant strategies, etc. With the purpose of estimating the robustness of communication network, most existing network robustness estimation researches mainly focus on failures in network physical layer and take complex network methods to estimate network robustness; recently, others have used Monte Carlo method to consider nodes mobility and several researches have summed up whole factors with weights to estimate the network robustness by AHP methods. Though these methods have largely been exploited to estimate the robustness of networks approximately, there is still no proper method to estimate the robustness of real communication network with consideration of nonlinear relationships among multiple factors. In this study, firstly, a double-layer network robustness model has been constructed; secondly, in order to take more robustness related factors into consideration, we have constructed a simulation platform based on NS-3; finally, we have proposed a novel robustness estimation method based on improved ELM (extreme learning machine), which is powerful to estimate the nonlinear relationships. The novel robustness estimation method has been formed by four steps: simulation and data collection, improved EML, model training, and estimation. In the end, contrast analyzes have been made to illustrate three facts: (1) fault-tolerant strategies can improve the robustness obviously; (2) our double-layer network robustness model is better than the previous model; (3) the improved ELM has a better cross-validation accuracy which is above 95%.

Introduction

The robustness of network is of great importance especially when it is under targeted attacks or stochastic failures and has attracted increasing attention in various fields, such as communication network[1, 2], biology[3, 4] and other common network[5, 6]. In order to improve the robustness of network, fault-tolerant strategies are employed to struggle against the attacks in both the physical and logical layers of the communication network[7, 8]. The analysis and estimation of robustness can avoid suffering, lower the risk, and help to improve the reliability[9, 10].

Based on the complex network theories and methods, most studies of robustness estimation over the last decade have focused on the analysis of the physical layer of network[5, 10-16]. Earlier researches regarding the robustness of network have mainly focused on network topology, such as, the node failures when being suffered from targeted attacks or random failures. Paolo et al.[11] studied the robustness to resist attacked failures and simulated the robustness under the breakdown of group nodes. Gallos et al.[12] studied the tolerance and topology of random scale-free networks between attacks and defences strategies that depend on the degree k of the nodes. Later,
random graph theory and percolation theory were taken to estimate the robustness of network[17, 18]. Zhao et al.[17] derived a sharp zero-one law for k-robustness in a random graph model. Scuola et al.[18] used a percolation dynamics analytical method to estimate the robustness on a modular network and the percolation criticality value is proposed.

Further researches have taken some new methods to estimate the robustness of the network with considerations of dynamics networks over time, such as under different attacking strategies. Salvato et al.[19] used temporal robustness metric to estimate the robustness of temporal random network. Morohosiet al.[20] used Monte Carlo method to estimate the robustness of network. Motter et al.[21] used Load-Capacity Model and studied the robustness of network under targeted attacks or random failures.

Based on the AHP (Analytic Hierarchy Process) method, researches estimated the robustness of a network and consider multiple layers[22, 23]. Ren[23] assumed that the robustness of the IoT (Internet of Things) should include three layers, which were the perception layer, transport layer, and application layer. Li[22] conducted a robustness index system, which included several layers and plenty of related factors, and estimated the robustness of service-oriented manufacturing information system.

According to the related researches, robustness estimation is increasingly coming towards the real system. Now more and more networks begin to apply fault-tolerant strategies to improve the robustness of network. The estimation of a network robustness, which employed fault-tolerant strategies, is more realistic and badly needed, especially when networks have high reliability demands. To the best of our knowledge, we find little relative robustness estimation study which considers multi-factors on both the physical layers and logical layers and estimates the robustness from the double layers, especially for communication network.

The aim of our study is to propose a robustness estimation method, which is suitable for networks with multiple nonlinear impacting factors. First of all, a network robustness model, which can cover the physical layers and logical layers with multiple nonlinear impacting factors, has been constructed; secondly, run and simulate the network robustness model and calculate the robust parameters of physical layers, logical layers and the whole system; finally, because the nonlinear relationships among the factors relative to the network robustness are various, the ELM is adopted to estimate the network robustness by the machine learning on the big data derived from the simulation. And in order to improve generalization characters, we give the improved ELM method.

**Network Robustness Model**

To estimate the network robustness, a network robustness model, considered the network structure and fault-tolerant strategies, should be constructed. The communication network can be divided into several different layers, such as, the seven layers, the five layers and others. Here the two layers division, which includes the physical layer and logical layer, is adopted. Because of attacks, error, and mobility, the physical structure of a network varies with time. To achieve a successful communication, the routing table produced by the routing protocol on the logical layer which is based on the physical layer, also varies with time[24]. So a network model, which is spatio-temporal dynamics, should be constructed firstly.

**Spatio-temporal Dynamics Network Model**

In order to describe the temporal and spatial dynamic characteristics and apply fault-tolerant strategies on both the logical layer and the physical layer, a model is proposed as shown in figure 1.

The spatio-temporal dynamic network model is composed of two parts: a physical layer constructed by physical connections, and a logical layer constructed by protocols such as routing. The physical layer changes with the mobility, radiation range of nodes, targeted attacks, random errors, and et al. Correspondingly, the routing table, transition path, time delay and others parameters on the logical layer, varies with the physical layer to keep a successful communication.

The spatio-temporal dynamic network model can be described in the following two layers.
1. Physical layer description. In the graph theory, network $G$, having $N$ vertices and $M$ edges, can be described as $P(u,v) = \beta e^{-\frac{d(u,v)}{\alpha}}$. So as to describe the communication network, the paths are directed. If $u \in V, v \in V$, $\beta, \alpha \in (0,1]$ means the directed path from node $u$ to node $v$ and the ensemble $E = \{e(u,v) | u \in V, v \in V\}$. The number of nodes and edges in the network can be described respectively as $|V|$ and $|E|$. The function $W(e(u,v))$ is the weight of the edge $e(u,v)$, which is positive real arithmetic value and if this value is 0, there is no edge between node $u$ and node $v$.

2. Logical layer description. In the logical layer, it is important to find the best directed path to deliver data packages. Let’s define $path(u,v)$ as a certain path from the node $u$ to node $v$, which successively pass through node $u, node v_1, node v_2, ..., node v_n$, to node $v$. The ensemble $Path(u,v)$ concludes all the paths from the node $u$ to node $v$. The function $f(path(u,v))$ can evaluate the $path(u,v)$, And the best directed path from the node $u$ to node $v$ can be expressed by $path^*(u,v)$, which can be found by $f(path(u,v))$ and satisfy the equation $f(path^*(u,v)) \leq f(path(u,v))$.

Robustness Model with Fault-tolerant Strategies

Be similar to the spatio-temporal dynamic network model, it is also needed to describe the robustness of double layers and fault-tolerant strategies.

1. Physical layer robustness with fault-tolerant strategies. Plenty of research studied the network robustness of the physical layer and many parameters can reflect fault-tolerant strategies. The flow robustness, which is defined as the fraction of node pairs that remain connected after a number of deletions [25], is chosen as the network robustness of the physical layer. Here we use $R_{ps}$ to represent the network robustness of the physical layer, and then

$$R_{ps} = \frac{\sum_{i=1}^{k} n_i \cdot (1 - n_i)}{N \cdot (1 - N)}$$

(1)

Where $n_i$ is the number of nodes in the giant component $i$. And $N$ is the number of nodes in the whole network.

2. Logical layer robustness with Fault-tolerant strategies. The robustness of the logical layer is to maintain an effective logical path with fault-tolerant strategies especial when the network is under attacks or errors and the previous path has destroyed. And a parameter, which reflects the diversity of the paths between a given node-pair, is the $EPD$ (effective paths diversity)[26], and here we use the $EPD$ as our model.

$$EPD = 1 - e^{-\lambda k_{pd}}$$

(2)

Where $\lambda$ is an experimentally determined constant, and the $k_{pd}$ is a value of the added diversity of the paths defined as
\[ k_{pd} = \sum_{i=1}^{k} D_{min}(P_i) \] (3)

Where \( D_{min}(P_i) \) is the minimum diversity of the path \( I \) when evaluated against each member of the set of previously selected paths.

**Robustness Estimation Method**

The related factors, which influence the network robustness, are complex and have the nonlinear relationships. In order to take the related factors into consideration, we constructed a simulation platform based on NS-3 to finish the simulation and data collection. The traditional methods based on the models are impossible to analyze the nonlinear relationship. To estimate the network robustness, the extreme learning machine, abbreviated to ELM, is adapted. Because the ELM has the lower generalization character, we improved the ELM by adding a different function to the function of hidden node and the generalization character is raised obviously. And then a robustness estimation method, based on the improved ELM, is finished by following four steps. As can be shown in Fig. 2.

1. **Simulation and Data Collection.** The above network robustness models, give us the parameters, such as \( R_m, EPD \), that represent the robustness of the physical and logical layer. In order to obtain these values in different situation, we should simulate the packages delivering process of network and choose the package delivering ratio, abbreviated to \( PDR \), which is a reliability parameter, to the whole communication network robustness. And we choose the Waxman model [27] to construct a network graph to simulate the communication network. In order to add different routing protocols, the NS3 is adapted because of its extensibility and openness.

2. **Improved ELM.** Here the ELM, is adapted to analyze the nonlinear relationship between the inputs \( R_m, EPD \) and the output \( PDR \). The nonlinear relationship, which has multi-parameter inputs, other environmental influence factors and all these inputs and factors are coupling with each other, can be described as the following dynamic equation [28].

\[ \frac{dx}{dt} = F(x) + \sum_{j=1}^{N} A_j G(x, x_j) \] (4)

Where the \( x_i \) is an element in the vector \( \vec{x} \). The \( F(x) \) and \( G(x, x_j) \) represent the dynamical laws that govern the system’s components. \( A_j \) is the weighed connectivity matrix. In the ELM, the equation to estimate the robustness can be written as follows.

\[ F(x) = H \beta = \sum_{i=1}^{k} \beta_i f(a_i x + b_i) \] (5)

\[ \min \left[ O - \|H \beta - T\| \right] \]

![Figure 2. Steps of robustness estimation method.](image)

Figure 2. Steps of robustness estimation method.
Where

\[ H(a_1, a_2, \ldots, a_L, b_1, b_2, \ldots, b_L, x_1, x_2, \ldots, x_L) = \begin{bmatrix} f(a_1 x_1 + b_1) & f(a_1 x_1 + b_1) \\ \vdots & \vdots \\ f(a_L x_L + b_L) & f(a_L x_L + b_L) \end{bmatrix} \] (6)

Usually the vector \( \beta \) is an unknown vector, which can be obtained by the training samples. But there always exists an error \( O \) between the target \( T \) and the estimation result \( H\beta \) as follows.

\[ O = \| H\beta - T \| \] (7)

In order to get a minimum error \( O \), we add \( g(a_i x_i + b_i) \) to the hidden layers to solve the generation problem. Here the \( f(a_i x_i + b_i) \) and the \( g(a_i x_i + b_i) \) replace by.

\[ \varphi(a_i, b_i, x_i) = \alpha \cdot f(a_i, b_i, x_i) + (1 - \alpha) g(a_i, b_i, x_i) \] (8)

Where \( \alpha \) is the proportion of \( f(x) \) and \( g(x) \). And these two functions must be continuously differentiable function. And two typical continuously differentiable functions chosen are the sigmoid function \( f(x) \) and radial basis function \( g(x) \). So

\[ f(x) = \frac{1}{1 + e^{-x}} \] (9)

\[ g(x) = e^{-x} \] (10)

And the structure diagram of improved ELM model is shown in the Fig.3.

Figure 3. Structure diagram of improved ELM model.

2. ELM Model Training. The model training is the process of machine learning to obtain the weighed vector \( \beta \). Let us suppose the error equal to 0. So

\[ H\beta = T \] (11)

Then

\[ \beta = H^{-1}T \] (12)
But generally, \( H \) is not invertible matrix because the number of hidden layers is less than the sample number. In that case, the Moore-Penrose generalized inverse matrix \( H^+ \) is adapted to replace \( H^{-1} \).

3. Network Robustness Estimation. If the upper tasks are finished completely, we can use the Eq.5 to realize the network robustness estimation just by inputting the vector \( x \). You can give different kinds of input data, which vary with different rules to get certain laws in different situations. And in order to test the estimation accuracy, the data can be divided into training set and testing set randomly.

Case Analysis and Method Verification

Here we construct a tactical internet, belonging to the communication network, with the following settings in the Table 1.

<table>
<thead>
<tr>
<th>Attributes</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>topology</td>
<td>Waxman model</td>
</tr>
<tr>
<td>Map Size</td>
<td>3000m*3000m</td>
</tr>
<tr>
<td>Node Scale</td>
<td>1000</td>
</tr>
<tr>
<td>Node Communication Radius</td>
<td>50m</td>
</tr>
<tr>
<td>Time Steps</td>
<td>1000</td>
</tr>
<tr>
<td>Movement mode</td>
<td>Random Walk</td>
</tr>
<tr>
<td>Node failure mode</td>
<td>Random Failure</td>
</tr>
<tr>
<td>Protocol</td>
<td>AODV/DSR</td>
</tr>
</tbody>
</table>

Waxman model can be realized by INET module in NS3. If \( \beta, \alpha \in (0,1) \) are given, the network topology will be generated and probability of the edge between node \( u \) and node \( v \) is given by based on the following equation.

\[
P(u,v) = \beta e^{-\frac{d(u,v)}{L\alpha}}
\] (13)

Where \( \beta, \alpha \in (0,1) \), and \( d(u,v) \) is the distance from node \( u \) to \( v \), \( L \) is the maximum distance between two nodes.

Table 2. The robustness of physical layer.

<table>
<thead>
<tr>
<th>Failed nodes</th>
<th>( \alpha=0.5 ), ( \beta=0.8 )</th>
<th>( \alpha=0.8 ), ( \beta=0.5 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.784</td>
<td>0.535</td>
</tr>
<tr>
<td>40</td>
<td>0.524</td>
<td>0.346</td>
</tr>
<tr>
<td>80</td>
<td>0.284</td>
<td>0.214</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

The table 2 gives the \( R_p \) under certain parameters and failed nodes with same logical layer settings.

Table 3. The robustness under different failed nodes.

<table>
<thead>
<tr>
<th>Failed nodes</th>
<th>( R_p )</th>
<th>EPD</th>
<th>PDR</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.783784</td>
<td>0.591592</td>
<td>0.546547</td>
</tr>
<tr>
<td>2</td>
<td>0.793587</td>
<td>0.601202</td>
<td>0.55511</td>
</tr>
<tr>
<td>3</td>
<td>0.807422</td>
<td>0.605817</td>
<td>0.561685</td>
</tr>
</tbody>
</table>
Failed nodes | $R_p$ | EPD | PDR \\
--- | --- | --- | --- \\
4 | 0.791165 | 0.581325 | 0.558233 \\
5 | 0.78794 | 0.59598 | 0.552764 \\
6 | 0.795775 | 0.586519 | 0.54829 \\
7 | 0.791541 | 0.599194 | 0.562941 \\
... | ... | ... | ... \\
1000 | 0 | 0 | 0 \\

And the Table 3 gives the $R_p$, EPD, and PDR, which vary with the number of failed nodes, with AODV and $\beta=\alpha=0.5$.

As shown in Fig.4, there is much difference of robustness when AODV protocol and DSR protocol are used respectively, and the robustness of communication network with AODV protocol is better because fault-tolerant strategies are employed in AODV protocol. It is obvious that fault-tolerant strategies can improve the robustness of communication network.

To verify the effectiveness of this model, we give the contrast figure, Fig.5. It is obvious the proposed model can predict the robust value with higher estimation accuracy than others because the proposed spatio-temporal dynamic network model is better than the previous. And the improved ELM method is also better, which can be seen by contrasting the Fig.6 and Fig.7.

Figure 4. Robustness of AODV and DSR under different failure nodes.
Figure 5. Contrast among the estimation effect based on different ways.

Figure 6. Robustness of real and estimation value in improved EML.
Figure 7. Robustness of real and estimation value in EML.
As shown in Fig.6, the red real robustness value and the yellow estimation value are very close; the average accuracy is 95.32%. In Fig.7, there are some big errors between the red real robustness value and the yellow estimation value at the node number of around 600 if the EML is not improved, and the average accuracy is 92.41%, which is lower than results from the improved EML. So the improved ELM method, which is powerful to estimate the nonlinear relationship, can be proved.

Conclusions
Both simulations and analytical results reveal that there are plenty of related factors, which have obvious influence on the network robustness. For example, with different network protocols, the robustness is different, and here the AODV is a better choice. It is obvious our proposed double-layer robustness model is better than others, which can be seen in the Fig.5; the platform gives a flexible way to estimate the robustness of a complex communication network with different factors, such as fault-tolerant strategies; the proposed improved EML method is successful to estimate the network robustness and also powerful to estimate other nonlinear relationships. We improve the ELM by adding a different function to the functions of hidden nodes and the generalization character is raised obviously.

References


