Life Cycle and Intrusion Tolerance Optimization Topology Models for Wireless Sensor Networks

https://doi.org/10.3991/ijoe.v14i05.8643

Jinhui Lei(✉), Xiyan Tian, Zhixia Zhang
Henan Institute of Science and Technology, Xinxiang, China
32745994@qq.com

Abstract—Wireless sensor networks have such disadvantages as upper limit of node energy and poor intrusion tolerance, etc. In light of these disadvantages, by analyzing such key parameters as residual energy, load, node degree, this paper proposes a wireless sensor network (WSN) life-cycle model, which fully considers node energy consumption and load fault tolerance, and a scale-free intrusion tolerance and targeted attacks optimization topology model. Then it verifies their feasibility through simulation test. The results show that the WSN life cycle model takes into account the impacts of residual energy and load capacity on the life cycle and fault tolerance of the system and improves the connectivity probability of high energy consumption nodes and small load nodes, leading to more uniform energy consumption of the wireless sensor network. Through the load adjustment coefficient, the life cycle of the network model is significantly increased. The simulation results show that the fault tolerance and survival time of the proposed model are both improved to some extent compared with those of other models. The proposed scale-free intrusion tolerance and targeted attacks optimization topology model optimizes the power exponent of the network using the structure entropy, and the established scale-free topology structure can make the model more tolerant to intrusion. The simulation results show that the intrusion tolerance of the algorithm proposed in this paper is 2.5 times that of the traditional network model, and the average life cycle is also significantly increased compared to those of other models.

Keywords—Wireless sensor networks; Network topology; Intrusion tolerance; Life cycle; Energy; Node failure

1 Introduction

At present, wireless sensor network is mainly used for communication and data transmission in special environments. However, energy exhaustion and communication transmission failure often occur to network nodes in harsh environments, paralyzing the entire network. Therefore, how to ensure the normal operation of network nodes and improve the network topology and fault tolerance in extreme situations are the key issues and challenges in current research [1-7].

The fault tolerance mechanisms for wireless sensor networks mainly include two kinds - static and dynamic fault-tolerance. When a traditional network model fails at a single node, its load will be transferred to an adjacent node, so that the adjacent node will be overloaded, causing a wide range of node failure and eventually paralyze the whole network [8-10]. The redundancy mechanism, scale-free topology mechanism, energy perception mechanism and fitness and local world mechanism are commonly used to strengthen the topological capabilities of network systems [11-16]. However, these models all have different limitations in practice.

In view of the disadvantages of wireless sensor networks, such as the upper limit of node energy and poor intrusion tolerance, etc., by analyzing such key parameters as residual energy, load, node degree, this paper proposes a WSN life-cycle model, which fully considers node energy consumption and load fault tolerance, and a scale-free intrusion tolerance and targeted attacks optimization topology model, respectively. This paper also verifies their feasibility through simulation test.

2 WSNs Lifecycle Modeling and Reliability Verification

2.1 Related knowledge and network node modeling

The life cycle of a wireless sensor network is the length of time from the point when the nodes are filled with energy to the point when the energy is all used up. It is mainly affected by residual energy and node load, $L_i(t)$. The latter is expressed as:

$$L_i\left(t\right) = L + k_i^{\alpha} L\left(\alpha \geq 0\right) \tag{1}$$

where, *Ki* represents the node degree, and L is the transmission of data traffic. If the communication radius of a single node is R_i, the data accepted and transmitted by the node for a period of time will be k_i^{α} and $L_i(t)$. From Formula (1), it can be seen that $E_i\,(t)$, i.e. the energy consumed by the node in this period of time, is expressed as follows:

$$E_i\left(t\right) = E_{elec} k_i^{\alpha} L + \left(E_{elec} + \varepsilon_{amp} R_i^2\right) L_i\left(t\right) = \left(2E_{elec} + \varepsilon_{amp} R_i^2\right) L_i\left(t\right) - E_{elec} L \tag{2}$$

where, E_{elec} is energy consumption by data transmission after fusion; and ε_{amp} is energy consumption coefficient. Through comparison of Formulas (1) and (2), it can be seen that $E_i(t)$ is proportional to $L_i(t)$. The following formula can be obtained by combining these two formulas:

$$E_i\left(t\right) = aL\left(1 + k_i^{\alpha}\right) + b \tag{3}$$

As can be seen from Formula (3), the more energy a node consumes, the more likely it is to fail. The node life cycle can be expressed as:

$$\tau_{node} = \frac{E_i}{E_i(t)} = \frac{E_i}{aL\left(1+k_i^{\alpha}\right)+b} \tag{4}$$

The shortest life cycle of a wireless network sensor can be expressed as:

$$\tau_{net} = \min\left(\tau_{node}\right) \tag{5}$$

The relationship between $n_{i,}$ - the number of nodes existing in a certain communication monitoring neighborhood of wireless sensor and R$_i$, - the corresponding communication distance is expressed as

$$n_i = N\iint_{G_i} g(x,y)\,dxdy = N\frac{\pi R_i^2}{A} \tag{6}$$

The maximum load data for a single node in the process of data transmission is:

$$L_{\max}(t) = L + k_{\max}^{\alpha}L \le L + \left(N\pi R_{\max}^2/A\right)^{\alpha}L \tag{7}$$

The larger the L_{max}(t) of a node is, the faster the node will consume energy, and E_{max}(t) - the maximum energy consumption of a node will be:

$$E_{\max}(t) = aL_{\max}(t) + b \le a\left[L + \left(N\pi R_{\max}^2/A\right)^{\alpha}L\right]+b \tag{8}$$

The shortest node life cycle can be converted into:

$$\tau_{net} = \frac{E_i}{a\left[L + \left(N\pi R_{\max}^2/A\right)^{\alpha}L\right]+b} \tag{9}$$

According to Formulas (5)-(9), the life cycle of a wireless sensor network is mainly controlled by *Ei*, the residual energy, and α, the load coefficient. The higher *Ei* is, the longer the life cycle will be; and the greater α is, the shorter the life cycle will be. In the actual modeling, we should take full advantage of the characteristics of α to construct a reasonable network topology.

2.2 LCEL model and its dynamic characteristics

According to the theoretical analysis in the previous section, this paper proposes a WSN life cycle model (LCEL) considering node energy consumption and load fault tolerance. The node communication in a WSN is constrained, so when a new node is linked, the fitness of the new node is constructed using the priority link model:

$$\prod_{\Lambda}\left(k_i\right)=\frac{\eta_i k_i}{\sum_{j\in\Lambda}\eta_j k_j} \tag{10}$$

where, η_i is the fitness function. During data transmission, a new node is added in each iteration, together with several edges extending outward from the node. The new node selectively links the other nodes within the transmission range, and the probability of the link is as follows:

$$\prod_{\Lambda}\left(k_i\right)=\frac{\eta_i k_i}{\sum_{j\in\Lambda}\eta_j k_j}=\frac{E_i k_i^{1-\alpha}}{\sum_{j\in\Lambda}E_j k_j^{1-\alpha}} \tag{11}$$

When α=0, the energy consumption of the model will decrease. When α>0, the weight of fertility and node degree can be adjusted to optimize the topology performance of the wireless sensor network.

According to the continuum theory, the node degree is continuously changing. Based on the preferred growth of the above node, the variation of the node degree can be obtained as follows:

$$\frac{\partial k_i}{\partial t}=m\prod_{\Lambda}\left(k_i\right)=m\frac{E_i k_i^{1-\alpha}}{\sum_{j\in\Lambda}E_j k_j^{1-\alpha}} \tag{12}$$

Through a series of transformations, the above formula can be simplified as:

$$\prod_{\Lambda}\left(k_i\right)=\frac{E_i k_i^{1-\alpha}}{E_\xi\sum_{j\in\Lambda}k_j^{1-\alpha}} \tag{13}$$

If the new node is added into the system network at time t, then the radius of the network will be R_t, the initial radius R_0, and the communication radius of the new node R_n at this point. The probability of adjacent node set of the new node can be expressed as:

$$\frac{\partial p\left(k_i\left(t\right)<k\right)}{\partial k}=\frac{\partial\left(1-p\left(t_i\le te^{\frac{m^\alpha-k^\alpha}{f\left(E_i,E_\xi\right)2^{\alpha-1}\alpha m^\alpha}}\right)\right)}{\partial k}=\frac{1}{f\left(E_i,E_\xi\right)2^{\alpha-1}m}\left(\frac{k}{m}\right)^{-(1-\alpha)}\times e^{\frac{m^\alpha-k^\alpha}{f\left(E_i,E_\xi\right)2^{\alpha-1}\alpha m^\alpha}} \tag{14}$$

In other words, when the growth of the wireless sensor network is known, the topology distribution mainly has something to do with fertility and load adjustment coefficient.

2.3 Simulation test verification

The proposed algorithm is compared with the traditional topology fault-tolerance algorithms - EAEM and BA algorithms, in order to verify its feasibility and superiority in terms of WSN fault tolerant topology and life cycle. The three algorithms all use the same network size to reduce the impacts of load and residual energy on the calculation results. The energy within the network system is initialized to enable each node to carry out 5,000 data transmissions, and the results of 100 tests are averaged as the final result.

Figure 1 shows the relationship between the node degree k and the system residual energy under the EAEM, BA and LCEL topology models. As can be seen from the figure, the distribution probabilities of the nodes with higher node degrees in the EAEM algorithm and the proposed algorithm are smaller, while the distribution probabilities of the nodes with lower node degrees are greater. The algorithm proposed in this paper achieves even more uniform distribution of node degrees and load, thus reducing the energy consumption of the nodes. At the same time, under these two models, the greater the K is, the greater the corresponding *Ei* will be. On the other hand, the BA algorithm shows the irregular oscillation feature of residual energy, because the proposed algorithm and the EAEM algorithm have fully considered the impact of residual energy of nodes on the algorithm, and preferentially link the nodes with greater *Ei* during data transmission. On the whole, the residual energy of the proposed algorithm is the largest at different node degrees, and its energy consumption is relatively small in the data transmission process, because it has considered the mutual coupling effect of *Ei* and load. The above analysis proves the superiority of the proposed model in the evolution of WSN topology.

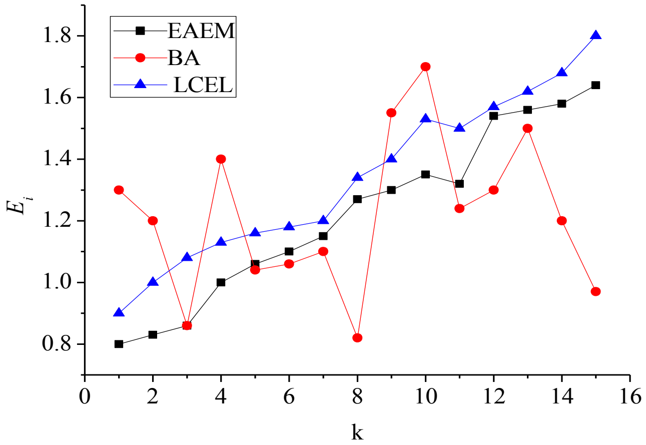

Fig. 1. Relation curve between k and E_i under different WSN topology models

Figure 2 shows the fault-tolerance performances of the proposed algorithm (α = 0.5 and α = 0.89) and EAEM and EBFL models in the simulation of random node failure. In the test, all the nodes in each iteration exchange data with their adjacent nodes, and then a node is selected for removal, and the number of nodes in the largest connected area in the system is calculated.

It can be seen from the figure that all the three models have high fault tolerance when nodes fail, and comparatively, the proposed algorithm (α = 0.89) has the best fault tolerance performance, which is because the proportion of nodes with high node degrees is far less than that of nodes with low node degrees in the network topology of the model, and accordingly, the failed nodes are usually those with lower node degrees, which have little impact on the overall data transmission of the system. However, the proposed algorithm can use the energy load more evenly, owing to its comprehensive consideration of energy and load factors.

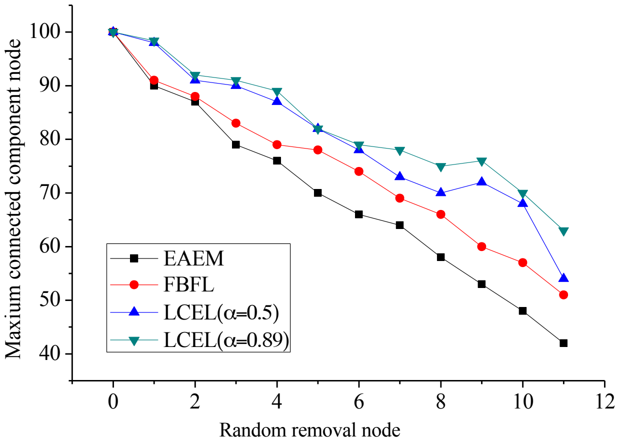

Fig. 2. The relation curve of fault-tolerance ability with different WSNs topology model

3 Modeling and Verification of WSN Intrusion Tolerance Index

The previous section introduces the optimization model for extending the life cycle and improving fault tolerance of WSN. However, in actual WSN operation, it is also often exposed to targeted attacks and scale-free intrusion tolerance attacks, which cannot be solved by the traditional wireless sensor topology model. Therefore, it is of great significance to work out a topology model strongly against targeted attacks and intrusion tolerance attacks.

3.1 Analysis on the SITT evolution model and its characteristics

Aiming at the targeted attacks and scale-free intrusion tolerance attacks in the network environment, this paper proposes an scale free intrusion tolerance and targeted attacks optimization topology model for WSN, which is an improvement made according to the scale-free theory of the classical topological BA model and calculates the degree distribution in the network area with the continuum theory. The average number μ(t) of nodes within time t is:

$$\mu(t) = E\left[N(t)\right] = \zeta t \tag{15}$$

N(t) is the node arrival process, and M(t) is the total number of nodes in the network system at time t.

$$M(t) = \int_0^t r(\zeta t)^\theta \zeta \mathrm{d}t = r\zeta^{\theta+1}\frac{t^{\theta+1}}{\theta+1} \tag{16}$$

According to the continuum theory, the node degree $k_{ij}(t)$ can be expressed as follows:

$$\frac{\mathrm{d}k_{ij}}{\mathrm{d}t} = mr(\zeta t)^\theta \zeta \prod(k_{ij}) \tag{17}$$

Combining Formulas (15)-(17), we have:

$$\frac{\mathrm{d}k_{ij}}{\mathrm{d}t} = \frac{1}{t}m\left[\beta_1(\theta+1)\frac{E_{ij}}{\langle E\rangle_t} + \beta_2(\theta+1)\frac{k_{ij}}{\langle k\rangle_t}\right] \tag{18}$$

By transforming the above formula based on the component variable method, we have:

$$k_{ij}(t) = C_1\frac{2}{\beta_2(\theta+1)}t^{\frac{\beta_2(\theta+1)}{2}} - 2mf(E)\frac{\beta_1}{\beta_2} \tag{19}$$

After a series of transformations, the degree distribution function of the SITT model is obtained as follows:

$$p(k) = \lim_{t\to\infty}\frac{1}{E\left[N(t)\right]}\sum_{i'=1}^{\infty}\frac{1}{r\left[N(t)\right]^\theta}\times\sum_{j'=1}^{r[N(t)]^\theta}p\left(k_{ij}(t)=k\right) = \frac{2}{\beta_2(\theta+1)}\frac{(m+2h)^{\frac{2}{\beta_2(\theta+1)}}}{(k+2mh)^{\frac{2}{\beta_2(\theta+1)}+1}} \tag{20}$$

As can be seen from the above formula, the power distribution of the degree distribution function can ultimately achieve a good model fault tolerance by adjusting θ and β to make the function value change within the specified range.

The network structure entropy is used to evaluate the performance of the network system against intrusion tolerance attacks, and the scale-free network degree function can be expressed as:

$$f\left(a\right)=\left(\frac{\lambda-1}{NC}\right)^{-\frac{1}{\lambda\text{-}1}}\times\left[a+\frac{\left(N^{-\lambda+2}C\right)}{\lambda-1}\right]^{-\frac{1}{\lambda-1}} \tag{21}$$

λ is the power exponent; N is the total number of nodes; a is the node number; C is the scale coefficient, whose expression is

$$\int_{k_{\min}}^{+\infty}p\left(k\right)\mathrm{d}k=\int_{k_{\min}}^{+\infty}Ck^{-\lambda}\mathrm{d}k=1 \tag{22}$$

When λ<2, the network can be called a scale-free network, where the network topology will become abnormal and its capability will be very poor against intrusion tolerance attacks. Therefore, this paper only considers the definition of the structure entropy F when λ> 2:

$$F=-\frac{\int_{1}^{N}f\left(a\right)\ln f\left(a\right)\mathrm{d}a}{\int_{1}^{N}f\left(a\right)\mathrm{d}a}+\ln\left(\int_{1}^{N}f\left(a\right)\mathrm{d}a\right) \tag{23}$$

Formula (23) is the relation function of the structure entropy and λ and N. When λ and N are known, Formula (23) can be used to verify the capability of the established model against intrusion tolerance attacks. The greater F is, the better the performance against intrusion tolerance attacks will be and the more uniform the network topology will be, and the vice versa.

3.2 Simulation verification

According to the calculation, the maximum value of the structure entropy can be obtained when λ=3.5. Two sets of test parameters are taken: λ_1=3.5, θ=0.6, β_1=0.43, β_2=0.55; λ_1=3.5, θ=1.8, β_1=0.74, β_2=0.26. The two experimental models are compared with the traditional EAEM model and the BA model to verify the effect of the algorithm on the performance of the network against intrusion tolerance attacks.

Figure 3 verifies the fault tolerance ability of the proposed algorithm. Like in the algorithm in the previous section, a node is randomly removed in the computation of each iteration. As can be seen, all the 3 algorithms have strong capabilities against intrusion tolerance attacks, because most of the nodes in the network system are those with low node degrees, and accordingly, most of the failed nodes are also of lower node degrees, which have less impact on the network connectivity.

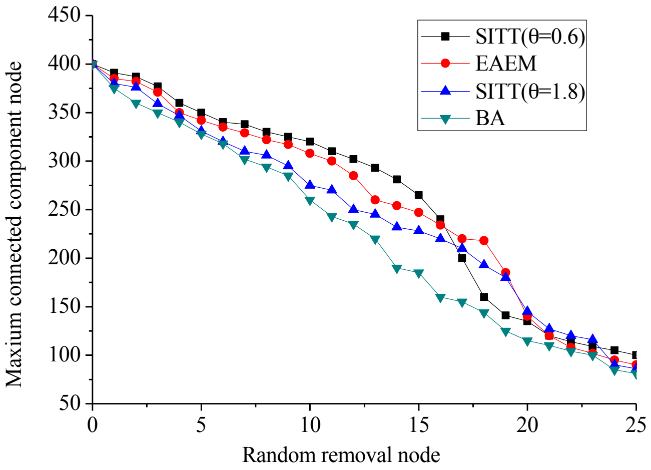

Fig. 3. Relation curve of the fault-tolerance ability

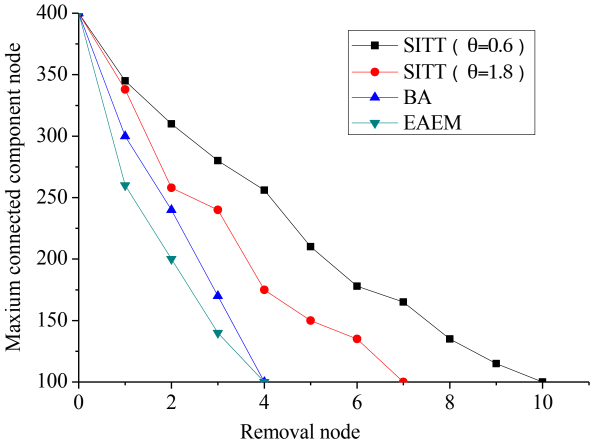

Fig. 4. Relation curve of intrusion tolerance under different WSN topology models

Figure 4 shows the comparison of the intrusion tolerances of the 3 models. It obtains the relation between the number of deleted nodes and the number of nodes in the largest connected area in the network by preferentially deleting nodes with higher node degrees. As can be seen, the intrusion tolerance of the SITT algorithm is the best when parameter θ=0.6. Only when the number of the failed nodes reaches 10 does the network meet the collapse criterion. When the parameter θ=1.8, it can only tolerate the deletion of 7 nodes at most. The parameter θ is an important index of the proposed algorithm. With the increase of θ, the number of nodes will also increase and the imbalance in the network system will become greater. Therefore, when the parameter θ=1.8, the intrusion tolerance of the network is weaker than that when θ=0.6. Both the BA model and the EAEM model can only tolerate the removal of 4 nodes, and the intrusion tolerance of the proposed algorithm is 2.5 times that of these two algorithms.

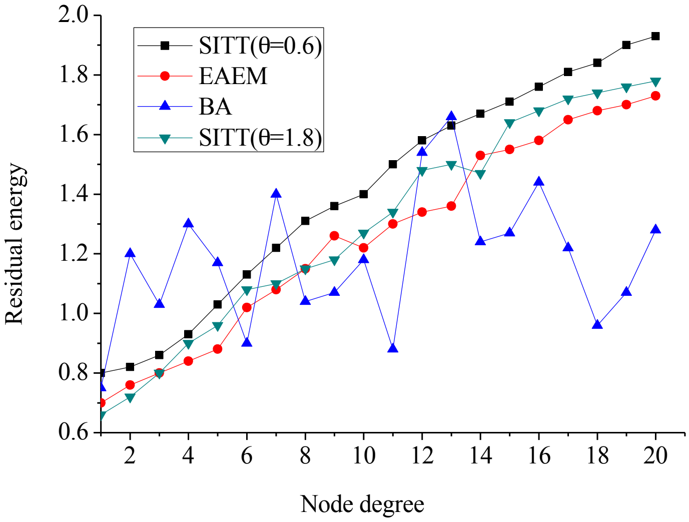

Fig. 5. Relation curve between node degree and residual energy

Due to some of its features, the WSN has certain constraint on the node energy of the WSN, so increasing the node energy intensity and extending its life cycle would be another important indicator to evaluate the model. Figure 5 compares the node residual energy under the three algorithms at different node degrees. Figure 6 shows the relationship between the proportion of failed nodes and the life cycle of the network system under the three models. After each iteration, the energy data are exchanged between any node and its adjacent nodes. It can be seen from the figure that under the EAEM model and the proposed model, the higher the node degree is, the higher the residual energy will be, making the energy consumption by the wireless sensor network more reasonable, while under the BA model, there is no significant correlation between the proportion of failed nodes and the residual energy. The life cycles of the WSN under the proposed model at two different θ values are obviously longer than those of the EAEM and BA models. Specifically, when θ=0.6, the average life cycle is about 12.5% longer than that under the EAEM model and about 17.9% longer than that under the BA model. This is because when the number of failed nodes increases, the SITT model considers the effects of topology parameters on the life cycle and topology structure, making it much advantageous in intrusion tolerance and extension of node life cycle.

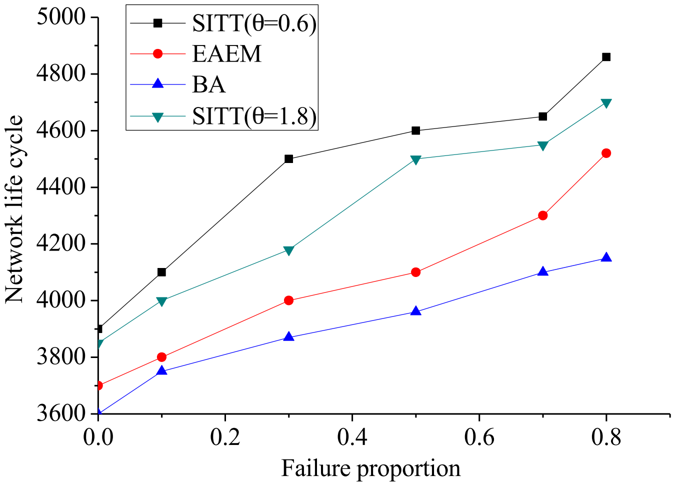

Fig. 6. Relation curve of network life cycle under different WSN topology models

4 Conclusions

In view of the disadvantages of the wireless sensor networks, such as upper limit of node energy and poor intrusion tolerance, etc., this paper proposes a wireless sensor network (WSN) life-cycle model, which fully considers node energy consumption and load fault tolerance, and a scale-free intrusion tolerance and targeted attacks optimization topology model. Then it verifies their feasibility through simulation test. The conclusions are as follows:

1. The WSN life cycle model takes into account the impacts of residual energy and load capacity on the life cycle and fault tolerance of the system and improves the connectivity probability of high energy consumption nodes and small load nodes, leading to more uniform energy consumption of the wireless sensor network. Through the load adjustment coefficient, the life cycle of the network model is significantly increased. The simulation results show that the fault tolerance and survival time of the proposed model are both improved to some extent compared with those of other models.
2. The proposed scale-free intrusion tolerance and targeted attacks optimization topology model optimizes the power exponent of the network using the structure entropy, and the established scale-free topology structure can make the model more tolerant to intrusion. The simulation results show that the intrusion tolerance of the proposed algorithm is 2.5 times that of the traditional network model, and the average life cycle is also significantly increased compared to those of other models.

5 References

[1] Li, Z.J. (2017). Application of neural network technology in machining error recovery, Journal of Manufacturing Engineering, 15(3), 6-11.

[2] Zhu, H., Luo, H., Peng, H., Li, L., Luo, Q. (2009). Complex networks-based energy-efficient evolution model for wireless sensor networks. Chaos Solitons & Fractals, 41(4), 1828-1835. https://doi.org/10.1016/j.chaos.2008.07.032

[3] Zheng, G., Liu, Q. (2012). Scale-free topology evolution for wireless sensor networks ⍰. Computers & Electrical Engineering, 38(3), 643-651. https://doi.org/10.1016/j.compeleceng.2013.01.009

[4] Wang, J., Rong, L., Zhang, L., Zhang, Z. (2008). Attack vulnerability of scale-free networks due to cascading failures. Physica A Statistical Mechanics & Its Applications, 387(26), 6671-6678. https://doi.org/10.1016/j.physa.2008.08.037

[5] Gonçalves, C.P. (2017). Quantum neural machine learning: backpropagation and dynamics, NeuroQuantology, 15(1), 22-41. https://doi.org/10.14704/nq.2017.15.1.1008

[6] Fichera, A., Frasca, M., Volpe, R. (2016). On energy distribution in cities: a model based on complex networks, International Journal of Heat and Technology, 34(4), 611-615. https://doi.org/10.18280/ijht.340409

[7] Kashyap, A., Khuller, S., Shayman, M. (2008). Relay placement for higher order connectivity in wireless sensor networks. Proceedings - IEEE INFOCOM, 15(1), 1-12. https://doi.org/10.1109/INFOCOM.2006.273

[8] Ma, J., Jiang, Q.T., Zhang, X. W., Wei, L., Chen, G.Y., Qi, P.F. (2014). Effect of lipids on starch determination through various methods.Pakistan Journal of Agricultural Sciences, 51(3), 749-755.

[9] Boccaletti, S., Latora, V., Moreno, Y., Chavez, M., Hwang, D.U. (2006). Complex networks: structure and dynamics. Physics Reports, 424(4), 175-308. https://doi.org/10.1016/j.physrep.2005.10.009

[10] Crucitti, P., Latora, V., Marchiori, M. (2004). Model for cascading failures in complex networks. Physical Review E Statistical Nonlinear & Soft Matter Physics, 69(4 Pt 2), 45-104. https://doi.org/10.1103/PhysRevE.69.045104

[11] Motter, A.E. (2004). Cascade control and defense in complex networks. Physical Review Letters, 93(9), 098701. https://doi.org/10.1103/PhysRevLett.93.098701

[12] Albert, R., Barabasi, A.L. (2000). Dynamics of complex systems: scaling laws for the period of boolean networks. Physical Review Letters,84(24), 56-60. https://doi.org/10.1103/PhysRevLett.84.5660

[13] Li, N., Hui, X.H. (2016). Study on topology constraint design under complex mechanical system of topological structure, Academic Journal of Manufacturing Engineering, 14(2), 28-32.

[14] Carreras, B.A., Lynch, V.E., Dobson, I., Newman, D.E. (2004). Complex dynamics of blackouts in power transmission systems. Chaos, 14(3), 643. https://doi.org/10.1063/1.1781391

[15] Djedai, H., Mdouki, R., Mansouri, Z., Aouissi, M. (2017). Numerical investigation of three-dimensional separation control in an axial compressor cascade, International Journal of Heat and Technology, 35(1), 657-662. https://doi.org/10.18280/ijht.350325

[16] Dou, B.L., Wang, X.G., Zhang, S.Y. (2010). Robustness of networks against cascading failures. Physica A Statistical Mechanics & Its Applications, 389(11), 2310-2317. https://doi.org/10.1103/PhysRevE.77.056103

6 Authors

Lei Jinhui received the B.S. degree in electronic information engineering and the M.S. degrees in communication and information system from Zhengzhou University in 2003 and 2011, respectively. He is currently a Lecturer with the School of Information Engineering, Henan Institute of Science and Technology, Xinxiang, China. His research interests include Internet of Things, embedded systems, and wireless sensor networks.

Tian Xiyan received the B.S. degree in applied electronic technology from Henan Normal University in 2002, and the M.S. degrees in communication and information system from Zhengzhou University in 2012. She is currently a Lecturer with the School of Mechanical and Electrical Engineering, Henan Institute of Science and Technology, Xinxiang, China. Her research interests include mobile communication network, wireless communication and electromagnetic compatibility, and cyber-physical systems.

Zhang Zhixia, female, Lecturer. She graduated from Henan Institute of Science and Technology in September 2005, winning a bachelor’s degree in information engineering. In 2009 she graduated from Electronic Information College of Northwestern Polytechnical University, majoring in the signal and information processing, and received a master's degree. In July 2009 she came to Henan Institute of Science and Technology and worked in the College of Information Engineering. Her main research direction is the processing of intelligent signal and image.

Article submitted 30 March 2018. Final acceptance 05 May 2018. Final version published as submitted by the authors.