Acta Technica *62* (2017), No. 6B, 605–622 © 2017 Institute of Thermomechanics CAS, v.v.i.

Adaptive neural network tracking and controlling network attack node in WSN

Wei Wang[1], Zhilai Zhang[1], Zhihui Wang[1]

Abstract. At the time of formulating network attack strategy, information of target network is uncertain and the attacker lacks comprehensive, reliable and real-time attack basis, which makes it difficult to achieve attack effect. Hence, a scientific complex network attack method is proposed. The attackers' income, loss, cost and encountered risk in network attack are analyzed and index system is established to comprehensively evaluate attack effect of network node with dynamic Bayesian network and overcome defects of static evaluation for target node by traditional evaluation method of node significance by relying on single index of network topology. Simulation experiment shows that such method combines more node relationship and observation relationship at the time of attack, avoids the gap between actual attack effect and theoretical expectation when attack is implemented by relying on static evaluation. In the meanwhile, it is more accurate in attack precision and of high attack efficiency.

Key words. Network attack, Neural network, Prediction, Network control, Network node, Node.

1. Introduction

Situation awareness system, monitoring and controlling system, information hinge center and various force units in network space information are composed of highly connected complex network. If network system of the opponent is firstly attacked in information countermeasure, the opponent's information defense system can be directly destroyed or disintegrated. With continuous development of information technology, complex network is more and more widely applied in military and economic fields and organization structure of network application is of more collaboration. Application level tends to develop towards multiple directions and network attack behavior is of more uncertainty. Attack strategy tends to be complex and diversified. How to use limited force to conduct attack of the most value for many nodes in target

[1]College of Information Engineering, Handan University, Handan, China

network relates to degree of attack efficiency. To formulate network attack strategy, effect of network attack effect shall be evaluated precisely to form consensus. Howe to make qualitative and quantitative evaluation for effect of network attack under complex network environment and check validity of attack behavior and safety of network system have become research hotspots of related fields.

2. Establishment of evaluation index system for network node and theoretical basis

2.1. Establishment of index system

(1) Attack income based on local attribute of network

Attack income refers to effect achieved by expected action before network attack. During network attack, it mainly refers to the influence on the opponent's network after attacked network node is paralyzed, significance of node subject to intentional attack in the opponent's network and possible impact on the global situation after being attacked and paralyzed. Hence, attack strategy is determined thereby[4, 5, 6].

Significance index of local attribute for node network is easy to be quantified and attribute information of adjacent nodes is considered only. It is applicable to analyze significance of local network node in large-scale network.

Definition 1 Node degree

Degree of node i in the network is defined as number of adjacent nodes, expressed as follows:

$$K(i) = \sum_{j \in G} a_{ij} \,, \tag{1}$$

$a_{ij} = 1$ indicates direct connection beteween nodes $i, j (i \neq j)$. Otherwise, $a_{ij} = 0$. The attribute reflects the extent to that single node influences functional characteristics of other nodes in local network. In the meanwhile, the significance of node in the network not only depends on its own attribute information, degree of adjacent node also has certain influence on its significance. Based on adjacent node information and clustering coefficient, node significance can be defined as $L(i)$, specifically as follows:

$$L(i) = \sum_{j \in \Gamma(i)} \sum_{u \in \Gamma(j)} N(u) \,. \tag{2}$$

$\Gamma(i)$ indicates adjacent node set of node i, $\Gamma(j)$ is set of node and the nearest neighboring node of j. $N(u)$ is sum of number of the nearest neighboring nodes of node u and number of adjacent nodes.

Definition 2 Approximation centrality

Node approximation indicates reciprocal of the sum of the shortest path distances between node i and other nodes in the network. If d_{ij} is the shortest distance between

node i and j, its expression is

$$CC_i = N/\sum_{j=1}^{N} d_{ij}\,. \tag{3}$$

The bigger value of node approximation centrality is, the higher degree in the position of network center will be and the more important the node will be.

Definition 3 Betweenness centrality

If $g_{jk}(i)$ indicates number of the shortest paths between node j and node k via node i and g_{jk} indicates number of the shortest paths between node j and node k. Then the expression of betweenness centrality is:

$$BC_i = \sum_{i\neq j\neq k\in V} \frac{g_{jk}(i)}{g_{jk}}\,. \tag{4}$$

If a node is the only route for communication among other nodes in the network, its status is more important and its influence on network communication is greater.

Definition 4 Cluster coefficient

Connection degree of all nodes connected with one node in the network can be defined as node cluster coefficent and network cluster coefficient.

Definition of node cluster coefficient is expressed with coefficient C_i as follows:

$$C_i = \frac{2e_i}{u_i(u_i-1)}\,. \tag{5}$$

u_i is quantity of nodes connected with node i and e_i is quantity of possible sides among nodes connected with the node.

Network cluster coefficient is defined as average value of all node cluster coefficients in the network, expressed as follows:

$$C = \frac{1}{N}\sum_{i=1}^{N} C_i\,. \tag{6}$$

Connection closeness among nodes in the network is in direct proportion to network cluster coefficient. When the coefficient value is 1, the network is a complete graph and there is side to connect any nodes; if the coefficient is 0, it shows that nodes in the network are all isolated nodes and there is no side among nodes.

In addition, after comprehensively considering number of adjacent nodes and association degree, a method based on information of adjacent node and cluster coefficient can be used to more objectively judge node significance, specifically defined as follows:

$$P(i) = \frac{fi}{\sqrt{\sum_{j=1}^{N} f_i^2}} + \frac{g_i}{\sqrt{\sum_{j=1}^{N} g_i^2}}\,. \tag{7}$$

Where, f_i is sum of degrees of node i and adjacent node $f_i = k(i) + \sum_{u \in \Gamma(i)} k(u)$ and $k(u)$ is degree of node u. g_i is expressed as follows:

$$g_i = \frac{\max\limits_{j=1}^{N} \left\{ \frac{c_j}{f_j} \right\} - \frac{c_i}{f_i}}{\max\limits_{j=1}^{N} \left\{ \frac{c_j}{f_j} \right\} - \min\limits_{j=1}^{N} \left\{ \frac{c_j}{f_j} \right\}} . \tag{8}$$

Where c_i is node cluster coefficient.

(2) Attack income based on global attribute of network

Definition 5 Feature vector

When degree index is used to evaluate node significance, adjacent nodes are all deemed to be equally significant. Such consideration is unrealistic. Nodes are unequal. When significance of the node is judged, influence of adjacent nodes shall be considered as well. If a node is drastically influenced by adjacent nodes, significance of the node may be very high. If it is slightly influenced by adjacent nodes, even the node has many neighboring nodes, it may not be insignificant. Such condition is deemed as feedback for significance of adjacent node.

Feature vector is used in the Thesis to measure the characteristics of node, namely feature vector of maximum feature value corresponding to adjacent matrix of network, specifically defined as follows:

$$C_e(i) = \lambda^{-1} \sum_{j=1}^{N} a_{ij} \varepsilon_j . \tag{9}$$

Where λ is maximum feature value of adjacent matrix and $\varepsilon = (\varepsilon_1, \varepsilon_2 ... \varepsilon_n)^T$ is feature vector of maximum feature value corresponding to adjacent matrix. Reputation of single node in the network can be deemed as linear combination of reputation of other nodes to obtain a linear equation set. Feature vector corresponding to maximum feature value of equation set can be used to measure significance of all nodes.

Definition 6 Closeness

Closeness can be used to measure the capacity of nodes in the network imposing influence on other nodes. Stronger closeness of node indicates that the node is more significant for functional relation of network system and it is at more central position in network topology structure, defined as follows:

$$V(i) = \frac{N-1}{\sum\limits_{j=1}^{N} d_{ij}} . \tag{10}$$

Where d_{ij} is the shortest distance between nodes i, j and closeness index depends on network topology structure to a great degree. Time complexity at the time of calculation shall be considered.

(3) Significance for network node of complex load based on invalid cascade

Significance evaluation for network node is mainly considered from static per-

spective in the first two sections. In reality, most networks are equipped with load. It may be concrete or abstract[7, 8, 12, 13]. Its distribution can be decided by many factors. Network topology structure is one of main factors and load decided by topology structure can be defined as "structure load". When it is impossible to judge specific physical load in the network, "structure load" can be used to evaluate invulnerability of complex network and node significance. Here number of the shortest path L_i is used to measure load size. Namely, it is held that the more the shortest path passing node is, the higher of load on the node will be[8], specifically defined as follows:

$$L_i = \frac{\sum\limits_{i \neq j} \frac{s_{ij}(k)}{s_{ij}}}{n(n-1)}. \tag{11}$$

Where s_{ij} is number of all shortest paths between nodes i, j and $s_{ij}(k)$ is number of the shortest paths between i, j via node k.

(4) Attack loss

Attack loss is resource consumption used by attack acion. In network attack, various attack means (equipment) have resource costs subject to performance evaluation and these resource costs can be extracted as corresponding indexes. It mainly refers to one's own computer resource loss when trojan, virus and others are used for attacking. Measurable indexes include bwndwidth, CPU, RAM occupation quantity and attack time.

CPU ocupancy rate is expressed as follows:

$$\bar{R}_{cpu} = \frac{\sum\limits_{i=1}^{n} R^t_{i_{cpu}} - R^0_{i_{cpu}}}{n}. \tag{12}$$

$\bar{R}_{cpu}$ is average value of CPU occupancy rate of host group attacking after network attack and $R^t_{i_{cpu}}$, $R^0_{i_{cpu}}$ are respectively CPU occupancy rates of single attack terminal after and before network attack; similarly, expressions for occupancy rate of RAM and bandwidth are shown in Equation (7) and Equation (8):

Occupancy rate of RAM:

$$\bar{R}_{mem} = \frac{\sum\limits_{i=1}^{n} R^t_{i_{mem}} - R^0_{i_{mem}}}{n}. \tag{13}$$

Occupancy rate of bandwidth:

$$\bar{R}_{band} = \frac{\sum\limits_{i=1}^{n} R^t_{i_{band}} - R^0_{i_{band}}}{n}. \tag{14}$$

(5) Attack cost

Traditional selective attack strategies of complex network mostly do not consider cost factor at the time of attack. Under such precondition, attack cost is not deemed as considerations to remove nodes or sides in the network. As per such condition,

network appears very weak when scale-free network is attacked selectively. However, in reality, scale-free network can present robustness inconsistent with assumptions when it is attacked. Therefore, to comprehensively measure attack strategy, cost factor shall be considered[9, 11].

Network G containing N nodes and E sides can be defined as set $G = (N, E)$. When network G is attacked once, M nodes shall be removed. Then $U(M)$ is taken as attack cost, defined as follows:

$$U(M) = \sum_{i \subset \Gamma(M)}^{H(i)} . \tag{15}$$

$H(i)$ is defined as function regarding degree x of node , defined as $H(i) = x$. At this time, cost spent to remove degree x of node under the same attack strategy is x. Therefore, node with larger node degree requires greater attack cost. In reality, attack cost of attack action has upper limit, indicates cost $U(N)$ spent to remove all nodes N in the network G. To facilitate quantization, $U(M)$ is expressed as the following through normalization processing:

$$\overline{U}(M) = \frac{U(M)}{U(N)} . \tag{16}$$

(6) Attack risk degree

Single loophole is quantified with risk ratio $P(V_i)$ and decided by popularity P_x, easiness P_y and influence P_z of the loophole, $P(V) = P_x * P_y * P_z$. Attack formed by multi-stage attack of attacker is composed of N loopholes. The attack can be realized when attack conditions of M loopholes are satisfied, namely $V = V_1 \wedge V_2 \wedge V_3 \wedge ... \wedge V_m$. So attack risk degree can be defined as the following:

$$R\,(A) = P(V)_1 \wedge (V)_2 \wedge (V_3) \wedge ... \wedge (V_m)\,. \tag{17}$$

(7) Attack effect of target network

Change of structure function before and after attack of target network reflects change of its operation efficiency. It can reflect effect of single attack. Here maximum connected subgraph O(M) after network attack is used to quantify network efficiency[1314, 15]. Network efficiency is provided with normalization processing and expressed with $E(M)$ as follows:

$$E(M) = \frac{\mathrm{O(M)}}{|N|} . \tag{18}$$

In above equation, $|N|$ indicates total number of nodes contained in the network. As per above definition, to calculate attack effect of target network under specific attack strategy, paid attack cost and attack loss shall be comprehensively considered and attack income and loss, cost-efficiency ratio shall be effectively controlled. If inverse relation among cost, loss and network efficiency is more obvious, the attack strategy will be more effective. On the contrary, attack strategy of lower validity.

2.2. Determination of index weight

(1) Determination of weight for criterion level

When weights of attack loss, attack income and attack risk at criterion level are determined, they shall be set up as per actual attack demand. If attack is made at no cost, weight of attack income shall be increased; under the condition of preserving one's own force, weight of attack loss shall be increased.

(2) Determination of weight for index level

When weights for all factors at index level are determined, analytic hierarchy process can be determined, with steps as follows

Step 1 Build two-two judgment matrix. 9-scale method is adopted to score and quantify all indexes at the same level and judgment matrix A is established.

Step 2 Calculate feature vector and maximum feature value. Normalize all column vectors in judgment matrix to obtain $B = (b_{ij})_{m\times n}$

$$b_{ij} = a_{ij} \Big/ \sum_{k=1}^{n} a_{kj} \qquad (i, j = 1, 2, ..., n)\,. \tag{19}$$

Arithmetic average value for elements of row vector of B is:

$$w_i = \frac{1}{n} \sum_{j=1}^{n} b_{ij}, \quad i, j = 1, 2, ..., n)\,. \tag{20}$$

Calculate maximum feature value

$$\lambda_{\max} = \frac{1}{n} \sum_{i=1}^{n} \frac{(A\omega)_i}{\omega_i}\,. \tag{21}$$

Step 3 Check matrix consistency

Calculate consistency index

$$C.I = \frac{\lambda_{\max} - n}{n-1}\,. \tag{22}$$

Calculate consistent $R.I$(as shown in Table 1)

Table 1. Consistency **R.I**

Order	1	2	3	4	5	6	7	8	9
R.I	0	0	0.58	0.90	1.12	1.24	1.32	1.41	1.45

Calculate consistency proportion:

$$C.R = \frac{C.I}{R.I}\,. \tag{23}$$

When $C.R < 0.1$, it is considered that judgment matrix A has satisfactory con-

sistency; on the contrary, when $C.R \geq 0.1$, it is considered that judgment matrix A has no satisfactory consistency and needs to be revised.

3. Evaluation method for attack effect of network node based on fuzzy, discrete and dynamic Bayesian network

3.1. Theoretical basis for evaluation of dynamic Bayesian network

As for discrete static Bayesian network with n hidden nodes and m observation nodes, the inference principle can be reflected as mathematical process of Equation (23) as per condition independence characteristics.

$$p(x_1,x_2,...,x_n\,|y_1,y_2,...,y_m\,) = \frac{\prod\limits_j p(y_j\,|p_a(Y_j)) \prod\limits_i p(x_i\,|p_a(X_i))}{\sum\limits_{x_1,x_2,...,x_n} \prod\limits_j p\,(y_j\,|p_a(Y_j)\,) \prod\limits_i p\,(x_i\,|p_a(X_i)\,)} \quad i \in [1,n]\,, j \in [1,m] \tag{24}$$

Where, x_i is a state value of X_i and $p_a(Y_j)$ indicates father node set of Y_j. $x_{11},...,x_{1n},...,x_{T1},...,x_{Tn}$ indicates a composite state of hidden variables. Distribution for composite state of observation variables can be determined through above equation.

Discrete static Bayesian network forms discrete dynamic Bayesian network of T time slices. At this time, observation value only has one composite state. So distribution of hidden variables under observation values is:

$$p(x_{11},...,x_{1n},...,x_{T1},...,x_{Tn}\,|Y_{11},Y_{12},...,Y_{1m}\,,...,Y_{T1},Y_{T2},Y_{Tm}) = \frac{\prod\limits_{i,j} p(y_{ij}\,|pa(Y_{ij})) \prod\limits_{i,k} p(x_{ik}\,|pa(X_{ik}))}{\sum\limits_{x_{11},x_{21},...,x_{T1}...x_{Tn}} \prod\limits_{i,j} p\,(y_{ij}\,|pa(Y_{ij})\,) \prod\limits_{i,k} p\,(x_{ik}\,|pa(X_{ik})\,)}$$

In above equation, x_i is a state value of X_i and subscript i indicates time slice. Subscript j indicates observation node j. y_{ij} is observation value of variable Y_{ij} and $p_a(Y_{ij})$ is parent node set of y_{ij}. $x_{11},...,x_{1n},...,x_{T1},...,x_{Tn}$ and $Y_{11},Y_{12},...,Y_{1m},...,Y_{T1},Y_{T2},Y_{Tm}$ respectively indicate a state combination of hidden nodes and observation nodes.

When there are few hidden nodes and observation nodes in the network or node coupling is strong, with fewer network structure layer and time slices considered, all time slices of DBN can be deemed as a static Bayesian network. When nodes gradually increase or node coupling is enhanced, DBN composed of T time slices can be obtained in time domain. After fuzzy processing of discrete Bayesian network, observation values are not unique and probability of each state combination is not 1. Then posterior general distribution for combination state of hidden variable is

calculated and general weighting is conducted finally. Therefore, inference process of fuzzy dynamic Bayesian network is shown as follows:

$$p(x_{11},...,x_{1n},...,x_{T1},...,x_{Tn}\,|Y_{11o},Y_{12o},...,Y_{1mo}\,,...,Y_{T1o},Y_{T2o},Y_{Tmo}) = \sum_{y_{11}y_{12}...y_{Tm}} \frac{\prod_{i,j} p(y_{ij}\,|p_a(Y_{ij}))\prod_{i,k} p(x_{ik}\,|p_a(X_{ik}))\prod_{i,j} p(Y_{ijo}=y_{ijo})}{\sum_{x_{11},x_{21},...,x_{T1}...x_{Tn}}\prod_{i,j} p\left(y_{ij}\,|p_a(Y_{ij})\right)\prod_{i,k} p\left(x_{ik}\,|p_a(X_{ik})\right)} \quad (25)$$
$$i \in [1,T]\,, j \in [1,m]\,, K \in [1,n]$$

In above equation, x_{ij} is a state value of X_{ij}; i is time slice i in time sequence; j indicates observation node; y_{ij} indicates observation value of variable Y_{ij} in time slice i; $p_a(Y_{ij})$ is parent node set of y_{ij}; Y_{ijo} is observation state of observation node j in time slice i; $p(Y_{ijo} = y_{ijo})$ represents membership of continuous observation value of Y_{ij} belonging to state y_{ij}.

3.2. Establishment of dynamic Bayesian evaluation network

Situation states of index at criterion level and attack effect at target level are classified as per key parameter threshold of index element. After states at all levels are normalized by next level of indexes, division is made as per values obtained after adding weights. Multiple time slices are selected to repeat the process to obtain value range. They are divided to different thresholds to build fuzzy set $E_A =$ (high efficiency, medium efficiency and low efficiency), $E_{m_1} =$ (high income, medium income and low income), $E_{m_2} =$ (high loss, medium loss and low loss); $E_{m_3} =$ (high risk, medium risk and low risk) $E_{m_4} =$ (high cost, medium cost and low cost).

4. Example analysis

In certain network attack action, "kite network" designed by Krackhardt is taken as an example, as shown in Fig. 2. Table 2 is attack income index for local attribute of all nodes before attack to attack global attribute index and number of the shortest path. From calculation of attack income index, it can be known that node 7 is major attack target in the network. Attack risk degree is calculated after feeding back loophole scanning of network sensor during the attack. In combination with evaluation of attack loss, attack efficiency probability is evaluated with attack effect of node 7 in 10 different moments as an example.

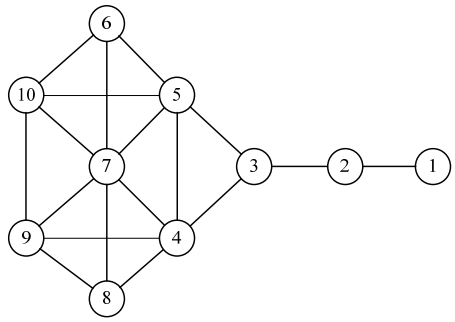


Fig. 1. Kite network

Table 2. Data calculation result at index level of attack income based on local attribute of network

Node	Node degree	Proximity centrality	Betweenness centrality	Cluster coefficient
1	1	1.23	0.3347	1
2	2	0.5726	0.4762	1
3	3	0.4944	0.6731	1
4	5	0.4703	0.7143	0.5
5	5	0.4703	0.7143	0.5
6	3	0.7051	0.5655	1
7	6	0.4742	0.6762	0.4
8	3	0.7053	0.5563	1
9	4	0.5782	0.5891	0.66
10	4	0.5782	0.5891	0.66

4.1. Determination of weight

Estimated weighted value of effect of target level at index level is calculated according to level recombination principle. As per statistics of previous attack, weights of attack income, attack loss, attack cost and attack risk at criterion level are initialized as $\omega_m^t = (0.35,\ 0.25,\ 0.2,\ 0.2)$ (dynamically adjusting weight ratio after obtaining effect data). Two-two comparison method is applied and weights of all indexes for attack income at index level are $\omega_{q_1-q_7}^n = (0.137,\ 0.157,\ 0.125,\ 0.173,\ 0.116,\ 0.093,\ 0.109)$; weights of all indexes for attack loss are $\omega_{q_8-q_{11}}^n = (0.25,\ 0.35,\ 0.25,\ 0.15)$ and weights of all indexes for attack risk are $\omega_{q_{13}-q_{19}}^n = (0.126,\ 0.131,\ 0.158,\ 0.139,\ 0.137,\ 0.157,\ 0.162)$.

Hence, weight of index level relative to the highest level is:

$$\begin{aligned}\omega_{q_1-q_7}^t &= \omega_m^t(1) \times \omega_n^m \times \omega_{q_1-q_7}^n \\ &= 0.35 \times 1 \times (0.137, 0.157, 0.125, 0.173, 0.116, 0.093, 0.109)\,,\end{aligned}$$

$$\omega_{q_8-q_{11}}^t = \omega_m^t(2) \times \omega_n^m \times \omega_{q_8-q_{11}}^n = 0.25 \times (0.25, 0.35, 0.25, 0.15)$$

$$\begin{aligned}\omega_{q_{13}-q_{19}}^t &= \omega_m^t(3) \times \omega_o^m(1) \times \omega_{q_{13}-q_{19}}^o \\ &= 0.2 \times (0.126, 0.131, 0.158, 0.139, 0.137, 0.157, 0.162)\,.\end{aligned}$$

4.2. Evaluation

After evaluation matrix is determined, corresponding matlab algorithm can be used to attribute values of all indexes with indexes $q_1 \sim q_7$ to compose decision-making matrix $X = (x_{ij})_{N\times M}$. Weighted normal matrix is calculated as per weight value obtained by use of AHP method and decision-making matrix R after standardization of matrix X.

$$Y = \begin{pmatrix} 0.0142 & 0.0772 & 0.1003 & 0 & 0.0733 & 0.1243 & 0.0548 \\ 0.0274 & 0.1752 & 0.1381 & 0.2861 & 0.1251 & 0.0343 & 0.2164 \\ 0.0428 & 0.1967 & 0.1937 & 0.4994 & 0.2273 & 0.0343 & 0.1790 \\ 0.0721 & 0.2074 & 0.1613 & 0.2974 & 0.1221 & 0.2343 & 0.1922 \\ 0.0721 & 0.2074 & 0.1937 & 0.2974 & 0.0302 & 0.1313 & 0.2021 \\ 0.0428 & 0.1383 & 0.1613 & 0 & 0.1653 & 0.1543 & 0.1833 \\ 0.0859 & 0.2053 & 0.1925 & 0.1303 & 0.1473 & 0.2279 & 0.0302 \\ 0.0428 & 0.1382 & 0.1613 & 0 & 0.1093 & 0.0343 & 0.2341 \\ 0.0571 & 0.1682 & 0.1703 & 0.0293 & 0.2253 & 0.1827 & 0.0951 \\ 0.0571 & 0.1682 & 0.1703 & 0.0293 & 0.1043 & 0.2037 & 0.2217 \end{pmatrix}.$$

Loopholes of all nodes in the network are analyzed and selected attack tool set is determined to be $\{p_1, p_2, ...p_n\}$. Each attack p_i has resource consumption evaluated by the system $C_i(q_8, q_9, q_{10}, q_{11})$, then index $q_8 \sim q_{11}$ is total cost of resource consumption $C = \sum_{i=1}^{n} C_i$; indexes $q_{12} \sim q_{17}$ can be evaluated through protection capacity of attack system; as for index q_{18}, loophole risk ratio $P(V_i)$ is calculated through node loophole analysis and risk degree $R(A)$ is solved.

4.3. Setup of model parameters

Attack effect of target node is inferred from three index states, attack income, attack risk and attack loss of network node and condition and state transfer probability are shown in Table 3 and Table 4. Joint tree inference engine of MATLAB BNT tool cabinet is selected to infer the model[4]. Suppose attack moments are continuous and continuous observation is conducted at 9 moments, observation values are set up according to data obtained in different moments. All initial data in Table 3 and Table 5 are input to the model.

Fig. 4 shows distribution for probability of attack effect from the first attack to the tenth attack. It can be known that from the first attack to the fourth attack, with attack strategy formulated on the basis of known network topology structure, at the time of implementing attack, information fed back from loophole, attack cost and attack loss is incomplete and attack effect is low. After continuously adjusting attack strategy and conducting the eighth attack, attack effect is improved significantly and gradually increases to the tenth to reach the peak value. Finally, it is calculated that probability average value with the 10th high attack effect for the node is 0.65. Similarly, it is calculated for the remaining 9 nodes with the method to obtain

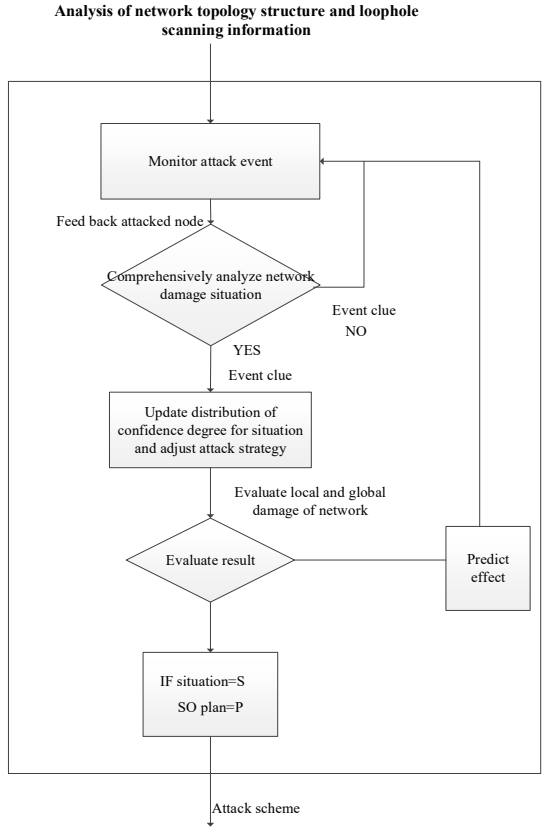


Fig. 2. Decision-making steps of network attack scheme

probability average value with high attack effect as follows:

$$\bar{P}_1 = 0.47, \bar{P}_2 = 0.52\bar{P}_3 = 0.33\bar{P}_4 = 0.52\bar{P}_5 = 0.63\bar{P}_6 = 0.39\bar{P}_7 = 0.65,$$
$$\bar{P}_8 = 0.42\bar{P}_9 = 0.38\bar{P}_{10} = 0.36.$$

Table 3. Conditional transfer probability for index at node criterion level

A	P(m1/A) High medium low	P(m2/A) High medium low	P(m3/A) Strong general weak	P(m3/A) Strong general weak
High	0.4 0.3 0.3	0.6 0.2 0.2	0.3 0.5 0.2	0.2 0.5 0.3
Medium	0.5 0.3 0.2	0.5 0.3 0.2	0.4 0.4 0.2	0.7 0.1 0.2
Low	0.1 0.2 0.7	0.1 0.3 0.6	0.1 0.4 0.5	0.2 0.5 0.3

Table 4. State transfer probability of node attack effect

A(T+1)	High (T+1)	Medium (T+1)	Low (T+1)
A(T)			
High (T)	0.6	0.2	0.2
Medium (T)	0.3	0.4	0.6
Low (T)	0.1	0.4	0.2

Table 5. State observation values for index probability at node criterion level

	m1	m2	m3	m3
T0	(0.6, 0.1, 0.3)	(0.1, 0.1, 0.8)	(0.4, 0.2, 0.4)	(0.2, 0.5, 0.3)
T1	(0.1, 0.1, 0.8)	(0.2, 0.3, 0.5)	(0.5, 0.2, 0.3)	(0.1, 0.3, 0.6)
T2	(0.1, 0.2, 0.7)	(0.3, 0.4, 0.2)	(0.5, 0.3, 0.2)	(0.4, 0.3, 0.3)
T3	(0.1, 0.2, 0.7)	(0.4, 0.4, 0.2)	(0.6, 0.3, 0.1)	(0.2, 0.3, 0.5)
T4	(0.1, 0.3, 0.6)	(0.5, 0, 0.5)	(0.6, 0.2, 0.2)	(0, 0.2, 0.8)
T5	(0.3, 0.6, 0.1)	(0.6, 0.4, 0)	(0.6, 0.3, 0.1)	(0.3, 0.3, 0.4)
T6	(0.6, 0.3, 0.1)	(0.7, 0.2, 0.1)	(0.8, 0.1, 0.1)	(0.8, 0.1, 0)
T7	(0.7, 0.2, 0.1)	(0.8, 0.1, 0.1)	(0.7, 0.2, 0.1)	(0.6, 0.2, 0.2)
T8	(0.8, 0.1, 0.1)	(0.9, 0.1, 0)	(0.8, 0.1, 0.1)	(0.3, 0.2, 0.5)

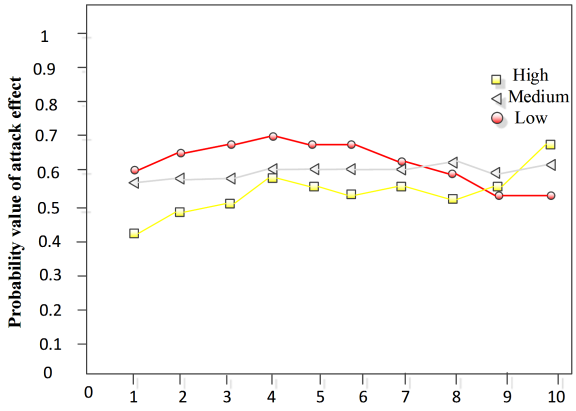


Fig. 3. Probability distribution for high, medium and low time of different attack effects of node 3

4.4. Analysis of method efficiency

To further describe method validity, INET3.0 is used under experiment to select node topology graph of some information hinges in "backbone network for all-American information superhighway" (data publicized in 2007) for simulation attack.

It is defined that as for network $G_o = (94, 239)$, node deletion method, betweenness method and method in the Thesis are respectively adopted for experiment. Fig. 4 is distribution for node significance of all information hinges calculated with three methods. Attack strategy is formulated according to data calculated as per significance for simulation attack. Fig. 5, Fig. 6 and Fig. 7 are comparisons of network node distribution before and after attacking with node deletion method, betweenness method and method in the Thesis adopted. After attack, the network can be respectively redefined as $G_1 = (77, 157), G_2 = (69, 141), G_3 = (57, 127)$. Based on 3 methods, after attacking G_o for fifty times, the network efficiency is calculated and summarized, as shown in Fig. 4.

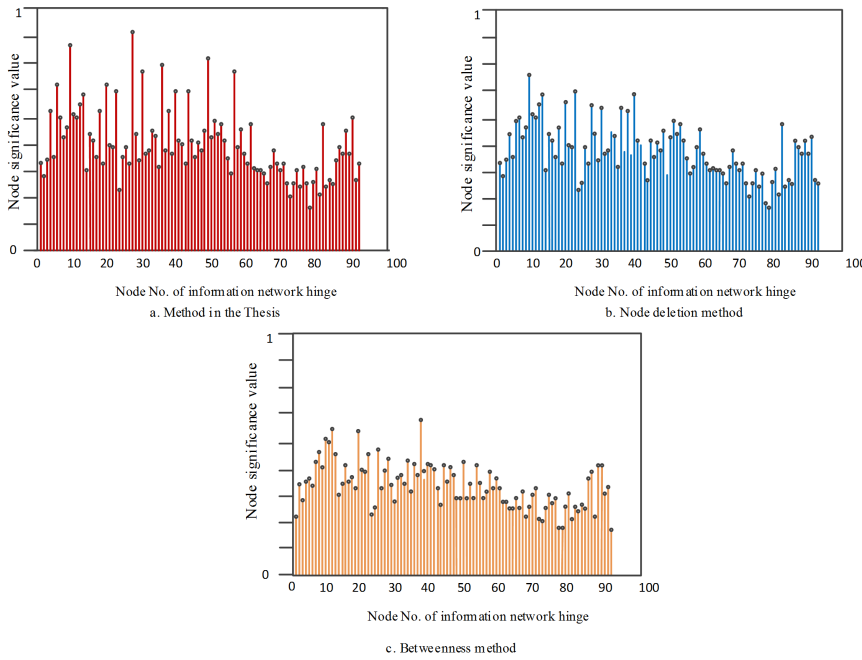
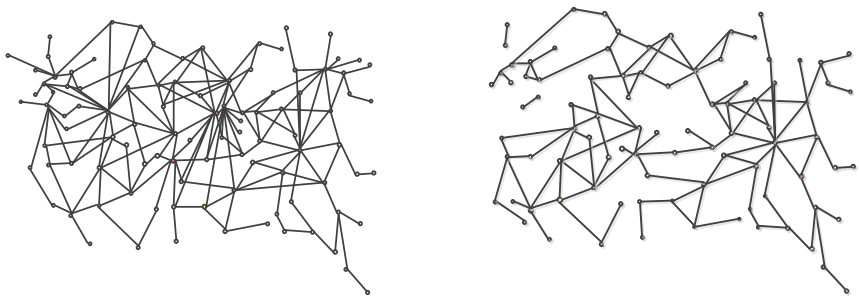
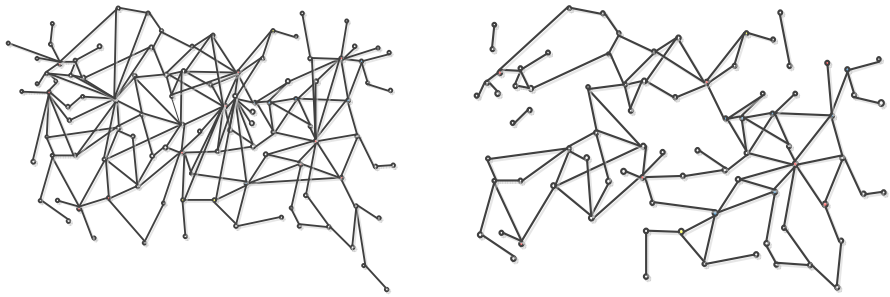


Fig. 4. Distribution for node significance in three methods

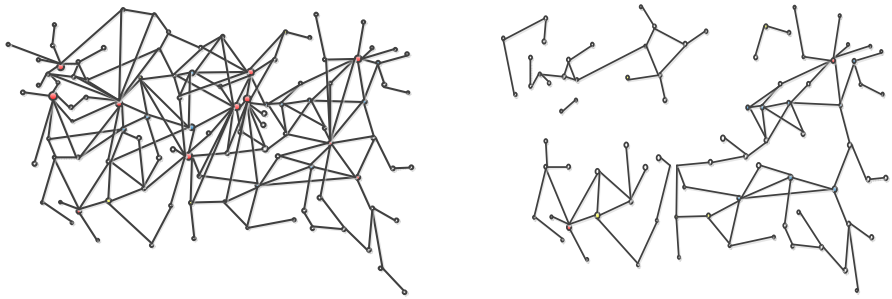
It can be seen from Fig. 5, Fig. 6 and Fig. 7 that effects for implementing attack after estimating significance of network nodes with typical betweenness method and node deletion method in simulation experiment differ slightly. Attack of target network with method in the Thesis has obvious advantage in efficiency. As for complex network with the same topology structure, when selective attack is implemented, effect produced by attack and expectation shall be fit in each attack[16, 17], and attack strategy shall be dynamically adjusted to transfer weight to nodes of maximum connected subgraph which will directly influence function of the whole network system after removal and filter those nodes of maximum connected subgraph without influence on network function. Finally, random network with different scales (ER model, connection probability p = 0.35) is provided with attack probability analysis under the same experiment environment. Time index is selected for evaluation. It



a. Connected distribution graph of network nodes before attacking with betweenness method
b. Connected distribution graph of network nodes after attacking with betweenness method



c. Connected distribution graph of network nodes before attacking with node deletion method
d. Connected distribution graph of network nodes after attacking with node deletion method



e. Connected distribution graph of network nodes before attacking with method in the thesis
f. Connected distribution graph of network nodes after attacking with method in the thesis

Fig. 5. Comparisons before and after attacking target network with three methods

can be seen from Fig. 7 that when network scale increases continuously and complexity of topology structure rises continuously, with gradual increasing of nodes, method in the Thesis is relatively stable in time consumption and is superior to other two algorithms after network scale reaches certain degree[19].

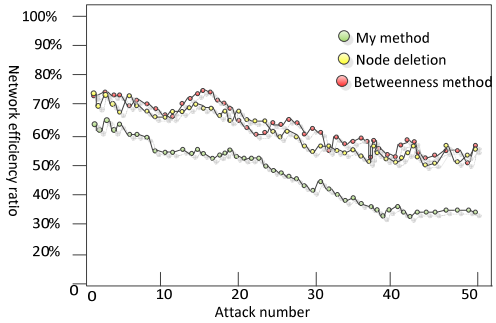


Fig. 6. Network efficiency comparison after attacking target network for 50 times with three methods

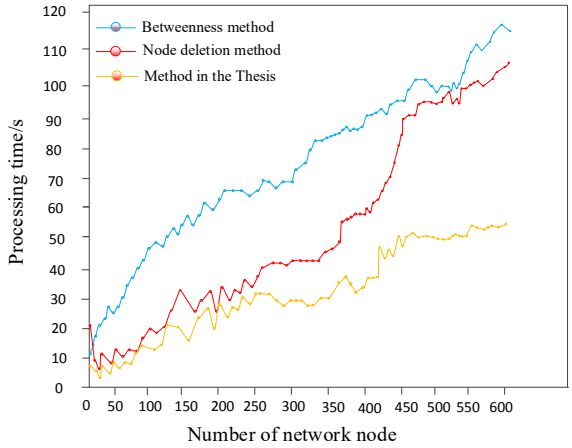


Fig. 7. Efficiency comparison after attacking target network with three methods

5. Conclusion

When attack strategy is formulated, structure, defense deployment and important nodes of network to be attacked are unknown and uncontrollable and index data used to evaluate attack effect are always not comprehensive. If static means are used to evaluate target network, it is strongly passive and there is always gap between expected effect. Through comprehensively analyzing all factors of network attack with dynamic Bayesian network, evaluation index system is established to apply dynamic Bayesian network method to dynamically evaluate network attack effect. In consideration of global and local effect after network nodes are attacked, attack cost and loss are taken as consideration factor for decision-making basis at the time of attack and new attack method is proposed to provide more scientific, autonomous and controllable aid decision-making means at the time of formulating network attack scheme and implementing attack action and drastically improve

attack of complex network attack. However, whether superiority embodied by this method under experiment environment is applicable to other network attack with more complex structure and highly intelligentized defense strategy.

References

[1] Sun F, Shayman M: (2007) *Prolonging Network Lifetime via Partially Controlled Node Deployment and Adaptive Data Propagation in WSN*[C]// Information Sciences and Systems, 2007. Ciss '07. Conference on. DBLP, 2007:226-231.

[2] Lu P, Zhang G W, Yang F C: (2014) *Node Capture Attack Detection in Dynamic WSNs Based on New Node Tracking*[J]. Advanced Materials Research, 945-949:2372-2379.

[3] Jie Z, Guo Y, Lingyan H U: (2012) *Detection and control of the node capture attack in WSN*[J]. Journal of Xidian University, 39(1):185-190.

[4] Lin C, Wu G: (2013) *Enhancing the attacking efficiency of the node capture attack in WSN: a matrix approach*[J]. The Journal of Supercomputing, 66(2):989-1007.

[5] Upadhyay R, Khan S, Tripathi H, et al.: (2015) *Detection and prevention of DDOS attack in WSN for AODV and DSR using battery drain*[C]// International Conference on Computing and Network Communications. IEEE, 2015:446-451.

[6] Liu L, Manli E: (2010) *Improve the positioning accuracy for wireless sensor nodes based on TFDA and TFOA using data fusion*[C]// IEEE International Conference on Networking, Sensing and Control, Icnsc 2010, Chicago, Il, Usa, 10-12 April. DBLP, 2010:32-37.

[7] Hsu C F: (2013) *A self-evolving functional-linked wavelet neural network for control applications*[J]. Applied Soft Computing, 13(11):4392-4402.

[8] Niu H, Jagannathan S: (2016) *Neural network-based attack detection in nonlinear networked control systems*[C]// International Joint Conference on Neural Networks. 2016:4249-4254.

[9] Akpan V A, Hassapis G D: (2010) *Adaptive recurrent neural network training algorithm for nonlinear model identification using supervised learning*[C]// American Control Conference. 2010:4937-4942.

[10] Li M, Koutsopoulos I, Poovendran R: (2010) *Optimal Jamming Attack Strategies and Network Defense Policies in Wireless Sensor Networks*[J]. IEEE Transactions on Mobile Computing, 9(8):1119-1133.

[11] Manoonpong P, Pasemann F, Wörgötter F: (2008) *Sensor-driven neural control for omnidirectional locomotion and versatile reactive behaviors of walking machines*[J]. Robotics & Autonomous Systems, 56(3):265-288.

[12] Xu B, Shi Z, Yang C, et al.: (2013) *Neural control of hypersonic flight vehicle model via time-scale decomposition with throttle setting constraint*[J]. Nonlinear Dynamics, 73(3):1849-1861.

[13] Dahlem M A, Schneider F M, Panchuk A, et al.: (2007) *Control of sub-excitable waves in neural networks by nonlocal coupling*[J]. Physics, 5517:1061-1069.

[14] Li M, Koutsopoulos I, Poovendran R: (2010) *Optimal Jamming Attack Strategies and Network Defense Policies in Wireless Sensor Networks*[J]. IEEE Transactions on Mobile Computing, 9(8):1119-1133.

[15] Xu B, Shi Z, Yang C, et al.: (2013) *Neural control of hypersonic flight vehicle model via time-scale decomposition with throttle setting constraint*[J]. Nonlinear Dynamics, 73(3):1849-1861.

Received May 7, 2017