INTERNATIONAL JOURNAL OF CIRCUITS, SYSTEMS AND SIGNAL PROCESSING
DOI: 10.46300/9106.2020.14.86 Volume 14, 2020

An Algorithm of Tracking and Controlling Network Attack Node based on Adaptive Neural Networks

Wei Wang
College of Information Engineering, Handan University, Handan，056005, China

Received: August 6, 2020. Revised: September 21, 2020, Accepted: October 12, 2020.
Published: October 21, 2020.

Abstract—In order to obtain certain and comprehensive information for formulating network attack strategy, a complex network attack method is proposed in this paper. The attackers' income, loss, cost and encountered risk in network attack are analyzed and index system is established to evaluate attack effect of network node with dynamic Bayesian network. This method can overcome defects of static evaluation which is relied on single index of network topology. Simulation experiment shows that this method combines more nodes and observation during the attack. It can avoid 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.

Keywords—Network attack, Neural network, Prediction, Network node.

I. Introduction

Situation awareness system, monitoring and controlling system, information hinge center and various force units in network are composed of highly connected network. If the 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. Application level tends to develop towards multiple directions. The attack behaviors in the network are more uncertain. So attack strategy tends to be complex and diversified. How to use limited force to conduct attack of the most value relates to degree of attack efficiency.

The mature and popular algorithms mainly include node deletion method and betweenness method. Node deletion method: the importance is defined by the degree of network connectivity destruction after the node is deleted, that is, "destructiveness is equivalent to importance". The more destructive the network is, the more important the node is. The defect of this method is the destructiveness of the network after deleting the key equivalent nodes of the nodes, and the research of the index destroys the integrity of the network[1].Betweenness method: the betweenness describes the information control ability of nodes to other nodes in the network[2]. By introducing the network nodes, the centrality of nodes is determined, and the central nodes are deleted iteratively to decompose the network. The advantage is that the network can be decomposed quickly. Both approaches are based on their algorithms judging the importance of nodes, but they fail to solve the problem of efficiency, that is, how to use limited power to carry out the most valuable attacks on many nodes in the target network. In order to formulate the strategy of network attack, it is necessary to accurately evaluate the effect of network attack and reach a consensus. However, how to evaluate the effectiveness of network attacks in complex network environment qualitatively and quantitatively, check the effectiveness of attacks and the security of network systems, has become a research hotspot in related fields.

The way of adaptive neural network is the current comprehensive research method, which not only considers the benefit, but also considers the effect of efficiency and cost comprehensively, making the whole behavior more cost-effective. Its model is that a typical adaptive neural network is divided into an input layer and a competition layer. The input layer is responsible for receiving the external information and transmitting the information to the competition layer. The competition layer is responsible for comparing and analyzing the patterns to find out that the rules and be classified correctly. The establishment of Bayesian evaluation network model for analysis and judgment is the core of this paper.

II. Establish of Evaluation Index System

A. Establishment of Index System

(1) Attack income based on local attribute of network

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

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

Node degree i is defined as number of adjacent nodes, expressed as follows

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

$a_{ij}=1$ means direct-connection between nodes $i, j(i\neq j)$. Otherwise, $a_{ij}=0$. This property reflects the extent to which a single node affects the functional characteristics of other nodes in the local network. Meanwhile, the significance of node in the network, not only depends on its own attribute information, but also influenced by the degree of adjacent node. Based on adjacent node information and clustering coefficient, the importance of node can be defined as $L(i)$, specifically as follows[3]

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

Γ(i) means a set of node that adjacent node i, Γ(j) is node j and a set of node that adjacent node j . N(u) is sum of the nearest neighboring nodes' number .

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. The d_{ij} is the shortest distance between node *i* and *j*. Its expression is [3]

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

The bigger value of node approximation centrality is, 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 to others , its status is more important and its communication influence is greater.

Definition 4. Clustering coefficient

In the network, connection degree of all nodes connected with one node, is defined as clustering coefficient and network cluster coefficient.

Definition of node clustering coefficient is expressed with coefficient Ci as follows

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

u_i is quantity of nodes connected with node i. e_i is quantity of possible-sides among nodes[8].

Network clustering coefficient is defined as average value of all node cluster coefficients in the network. The definition is as follows

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

Connection closeness among nodes is in direct proportion to clustering 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[6].

In addition, after considering number of adjacent nodes and association degree comprehensively, a method can be used to judge node significance more objectively based on information of adjacent node and clustering coefficient. The definition is as follows

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

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

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

c_i is clustering coefficient of the node.

(2) Attack income is based on global attribute of network

Definition 5. Feature vector

When degree index is used to evaluate node significance, adjacent nodes are deemed to be equally significant. Such consideration is unrealistic. When significance of the node is judged, influence of adjacent nodes should be considered as

well. If it is slightly influenced by adjacent nodes, it may be not insignificant. Such condition is deemed as feedback for significance of adjacent node[7].

Feature vector is used to measure the characteristics of node in this paper. The definition is as follows

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

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

Definition 6. Closeness

Closeness can be used to measure the capacity of nodes imposing influence on other nodes in the network. The more intimate the nodes are, the more important the functional relationship of the network system is, and the more central the node is in the network topology. It is defined as follows

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

d_{ij} is the shortest distance between nodes i, j.Closeness index depends on topology structure of the network. Time complexity shall be considered in the time-calculation.

(3) Implications of complex loads for network nodes based on invalid cascade

Significance evaluation about network node is mainly considered from static perspective in the first two sections. In reality, most networks are equipped with load. It may be concrete or abstract. Its distribution can be decided by many factors. Network topology structure is one of main factors. The load is decided by topology structure. So it 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. The number of the shortest path L_1 is used to measure the size of the load. Generally, The more nodes the shortest path passes through, the higher the load on the node [10].Its definition is as follows

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

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 *k*.

(4) Attack loss

Attack loss is resource consumption used in attack action. Various attack (equipment) have resource costs which can be extracted as corresponding indexes. It mainly refers to own computer resource loss when troy, virus and others are used for attacking. Measurable indexes include bandwidth, CPU, RAM occupation quantity and attack time.

CPU occupancy rate is expressed as follows

$$\overline{R}_{cpu} = \frac{\sum_{i=1}^{n} R_{i_{cpu}}^{t} - R_{i_{cpu}}^{0}}{n} \tag{12}$$

$\overline{R}_{cpu}$ is average value of CPU occupancy rate of host group attacking after network attack. $R_{i_{cpu}}^{t}$, $R_{i_{cpu}}^{0}$ are respectively CPU occupancy rates of single attack terminal after and before network attack.Expressions for occupancy rate of RAM and bandwidth are shown in Equation (7) and Equation (8).

Occupancy rate of RAM is

$$\overline{R}_{mem} = \frac{\sum_{i=1}^{n} R_{i_{mem}}^{t} - R_{i_{mem}}^{0}}{n} \tag{13}$$

Occupancy rate of bandwidth is

$$\overline{R}_{band} = \frac{\sum_{i=1}^{n} R_{i_{band}}^{t} - R_{i_{band}}^{0}}{n} \tag{14}$$

(5) Attack cost

Traditional selective attack strategies of complex network mostly do not consider cost factor when attack. Under such precondition, attack cost is not deemed as considerations to remove nodes or sides in the network. As such condition, network appears very weak when scale-free network is attacked selectively. However, in reality, scale-free network can present inconsistent with assumptions about robustness when attacked. Therefore, if you want to measure attack strategy comprehensively, the cost factor should be considered[9, 11].

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

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

H(*i*) is defined as function about node degree x , defined as *H*(*i*) = *x*. At this point, the cost of removing node degree X under the same attack strategy is X. Therefore, nodes with larger node degree need larger attack cost. In fact, the attack cost of the attack action has an upper limit, which is U (N) of the cost of removing all nodes N in the network G. For the convenience of quantization, U (M) is represented by normalization as follows

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

(6) Attack risk degree

Single vulnerability is quantified with risk ratio $P(V_i)$ and decided by popularity P_x , easiness P_y and influence P_z of the vulnerability, $P(V) = P_x * P_y * P_z$. Attack formed by multi-stage attack of attacker is composed of N vulnerabilities. Attack can be realized when attack conditions of M

vulnerabilities are satisfied, $V = V_1 \Lambda V_2 \Lambda V_3 \Lambda ... \Lambda V_m$. So attack risk degree can be defined as the following

$$R(A) = P(V_1) \Lambda (V_2) \Lambda (V_3) \Lambda ... \Lambda (V_m) \quad (17)$$

(7) Attack effect of target network

Structure function will change before and after attack . It reflects operation efficiency of network. It can reflect effect of single attack. We use to quantify network efficiency by attack maximum connected subgraph O(M). Network efficiency is provided with normalization processing and expressed with E(M) as follows

$$E(M) = \frac{O(M)}{|N|} \quad (18)$$

In above equation, $|N|$ is total number of nodes contained in the network. When we calculate attack effect, we should consider cost and loss comprehensively. Attack income, loss, and cost-efficiency ratio shall be controlled effectively. The more obvious cost-loss relation is, the more effective attack strategy is.

B. Determination of Index Weight

(1) Determination of weight of criterion level

When weights of attack loss, attack income and attack risk at criterion level are determined, we can set up attack demand in actual .If attack is no cost, the weight of attack income shall be increased.

(2) Determination of weight of 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. we score and quantify all indexes by 9-scale method at the same level ,then we can set up judgment matrix A .

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

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

Arithmetic average value for elements of row vector of B is

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

Calculate maximum feature value

$$\lambda_{\max} = \frac{1}{n} \sum_{i=1}^{n} \frac{(Aw)_i}{w_i} \quad (21)$$

Step 3 Check matrix consistency

Calculate consistency index

$$C.I = \frac{\lambda_{\max} - n}{n-1} \quad (22)$$

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	0.9	1.12	1.24	1.32	1.41	1.45

Calculate consistency proportion

$$C.R = C.I / R.I . \quad (23)$$

When C.R < 0.1, it is considered that judgment matrix A's consistency is satisfactory; on the contrary, when C.R ≥ 0.1, it is has no satisfactory consistency .It needs to be revised.

III. Evaluation Method for Attack Effect of Network Node Based

A. Theoretical basis for evaluation of dynamic Bayesian network.

To discrete static Bayesian network with N hidden nodes and M observation nodes, the principle can be reflected as mathematical process of Equation(23), under condition independence characteristic .

$$p(x_1, x_2, ..., x_n \mid y_1, y_2, ..., y_m) = \frac{\prod_j p(y_j \mid p_a(Y_j)) \prod_i p(x_i \mid p_a(X_i))}{\sum_{x_1, x_2, ..., x_n} \prod_j p(y_j \mid p_a(Y_j)) \prod_i p(x_i \mid p_a(X_i))} \quad (24)$$
$$i \in [1, n],\ j \in [1, m]$$

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. Through above equation, Distribution for composite state of observation variables can be determined. Discrete static Bayesian network forms discrete dynamic Bayesian network of T time slices. At this time, observation value has one composite state only. So distribution of hidden variables under observation values is:

$$p(x_{11},...,x_{1n},...,x_{T1},...,x_{Tn} \mid Y_{11}, Y_{12},..., Y_{1m},..., Y_{T1}, Y_{T2}, Y_{Tm}) = \frac{\prod_{i,j} p(y_{ij} \mid p_a(Y_{ij})) \prod_{i,k} p(x_{ik} \mid p_a(X_{ik}))}{\sum_{x_{11}, x_{21}, ..., x_{T1} ... x_{Tn}} \prod_{i,j} p(y_{ij} \mid p_a(Y_{ij})) \prod_{i,k} p(x_{ik} \mid p_a(X_{ik}))}$$

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} . $x_{11},...,x_{1n},...,x_{T1},...,x_{Tn}$, $Y_{11}, Y_{12},..., Y_{1m},..., Y_{T1}, Y_{T2}, Y_{Tm}$, and 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[3]. After the fuzzy processing, the observed values are not unique, and the probability of each state combination is not 1. The main reason is that the bayesian network needs to be discretized to meet the needs of digitization of computer modeling, and the degree of discretization is that the number of state combinations determines the observation probability and. When the degree of discretization tends to infinity, that is, the continuous integral, the probability of all state combinations is 1.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

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

In above equation, x_{ij} is a state value of X_{ij} j ; *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} .

B. 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. States at all levels are normalized by next level of indexes. Multiple time slices are selected to repeat the process to obtain value range. They are divided to different thresholds in order to build fuzzy set EA = (high efficiency, medium efficiency and low efficiency), Em1 = (high income, medium income and low income), Em2 = (high loss, medium loss and low loss); Em3 = (high risk, medium risk and low risk) Em4 = (high cost, medium cost and low cost).

IV. EXAMPLE ANALYSIS

"kite network" designed by Krackhardt is taken as an example, as shown in Fig. 1.

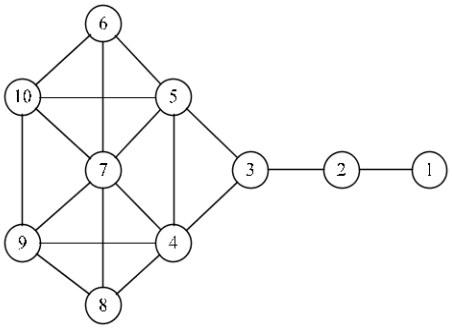


Fig. 1 Kite network

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.	0.4	1
3	3	0.	0.6	1
4	5	0.	0.7	0.
5	5	0.	0.7	0.
6	3	0.	0.5	1
7	6	0.	0.6	0.
8	3	0.	0.5	1
9	4	0.	0.5	0.66
10	4	0.5782	0.5891	0.66

Table 2 is attack income index .It is local attribute of all nodes before attack. It include attack global attribute index and the shortest path number. 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。 the feeding back come from network sensor vulnerability scanning of during the attack. In combination with evaluation of attack loss , we use attack effect of node 7 in 10 different moments as example, attack efficiency probability can be evaluated .

A. Determination of Weight

By statistics of previous attack, weights of attack income, attack loss, attack cost and attack risk at criterion level, are initialized as w_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 w_{q1-q7}^n = (0.137, 0.157, 0.125, 0.173, 0.116, 0.093, 0.109); weights of all indexes for attack loss are w_{q8-q11}^n = (0.25, 0.35, 0.25, 0.15) and weights of all indexes for attack risk are $w_{q13-q19}^n$ = (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:

$$w_{q1-q7}^t = w_m^t(1)\times w_n^m \times w_{q1-q7}^n$$
$$= 0.35\times 1\times (0.137, 0.157, 0.125, 0.173, 0.116, 0.093, 0.109),$$
$$w_{q8-q11}^t = w_m^t(2)\times w_n^m \times w_{q8-q11}^n$$

$= 0.25\times (0.25, 0.35, 0.25, 0.15)$

$w^t_{q13-q19} = w^t_m(3)\times w^m_o(1)\times w^o_{q13-q19}$

$= 0.2\times (0.126, 0.131, 0.158, 0.139, 0.137, 0.157, 0.162)$.

B. Evaluation

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

$$Y = \begin{pmatrix} 0.0142 & 0.0772 & 0.1003 & 0 & 0.0733 & 0.1243 & 0.0548 \\ 0.0274 & 0.1752 & 0.1381 & 0.2861 & 0.1251 & 0.0343 & 0.2164 \\ 0.0428 & 0.1967 & 0.1937 & 0.4994 & 0.2273 & 0.0343 & 0.1790 \\ 0.0721 & 0.2071 & 0.1613 & 0.2974 & 0.1221 & 0.2343 & 0.1922 \\ 0.0721 & 0.2071 & 0.1937 & 0.2974 & 0.0302 & 0.1313 & 0.2021 \\ 0.0428 & 0.1383 & 0.1613 & 0 & 0.1653 & 0.1543 & 0.1833 \\ 0.0859 & 0.2053 & 0.1925 & 0.1303 & 0.1473 & 0.2279 & 0.0302 \\ 0.0428 & 0.1382 & 0.1613 & 0 & 0.1093 & 0.0343 & 0.2341 \\ 0.0571 & 0.1682 & 0.1703 & 0.0293 & 0.2253 & 0.1827 & 0.0951 \\ 0.0571 & 0.1682 & 0.1703 & 0.0293 & 0.1043 & 0.2037 & 0.2217 \end{pmatrix}$$

vulnerabilities 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 -q_{11} is total cost of resource consumption $C = \sum_{i=1}^{n} C_i$; indexes q_{13} -q_{18} can be evaluated through protection capacity of attack system; as for index q_{18}, vulnerability risk ratio $P(V_i)$ is calculated through node loophole analysis and risk degree $R(A)$ is solved.

C. Setup of Model Parameters

IT is decision-making steps of network attack scheme.It is shown in Fig 2. The attack effect is inferred from three index states: attack income, attack risk and attack loss of network node. The condition and state transfer probability are shown in Table 3 and Table 4. The neural network can be self optimized through the feedback and the calculation of the bayesian network model. It can balance some parameters ,such as the income cost, attack damage and attacked earnings, and get the most cost-effective attack nodes. At the same time ,it can set attack number of times,attack frequency and attack efficiency to control termination. For example, when average probability of the effect of the attack node is greater than 0.65, the attack stops.

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	$P(m4/A)$ 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) / A(T)	High(T+1)	Medium(T+1)	Low(T+1)
High (T)	0.6	0.2	0.2
Medium(T)	0.3	0.4	0.6
Low(T)	0.1	0.4	0.2

We select tree inference engine and infer the model in MATLAB BNT tool cabinet[4] . Suppose attack moments are continuous . Continuous observation is conducted at 9 moments. We can set up observation values according to data obtained in different moments. All initial data in Table 3 and Table 5 are input to the model.

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

	m1	m2	m3	m4
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)

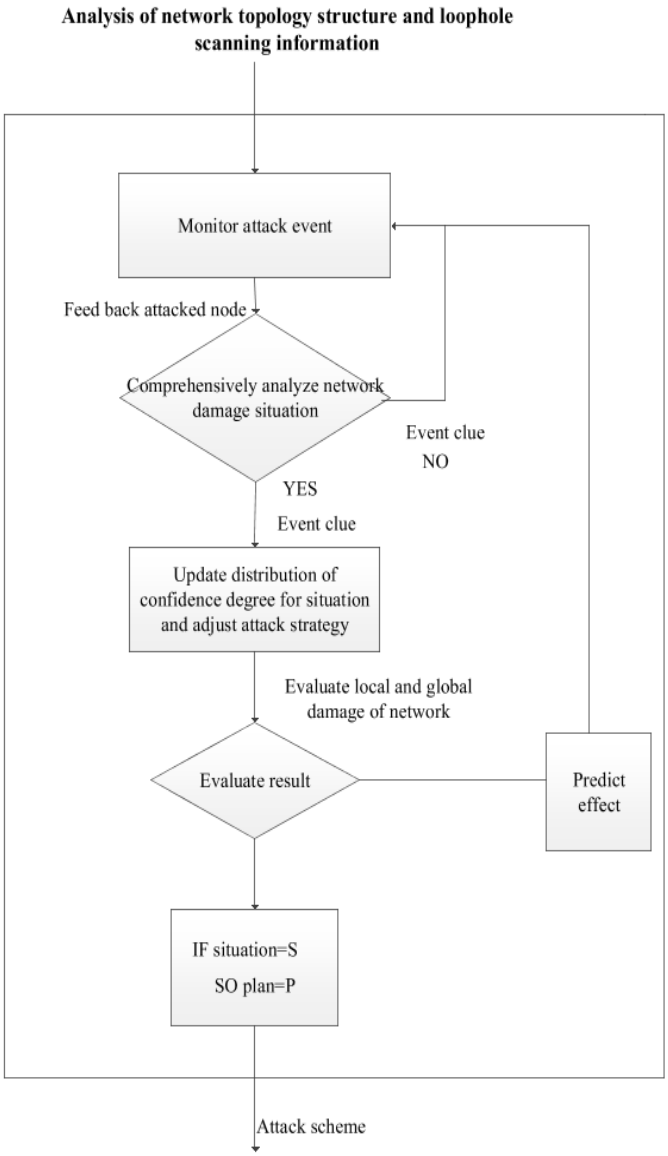


Fig. 2. Decision-making steps of network attack scheme

Fig. 3 shows distribution for probability of attack effect from the first attack to the tenth attack.

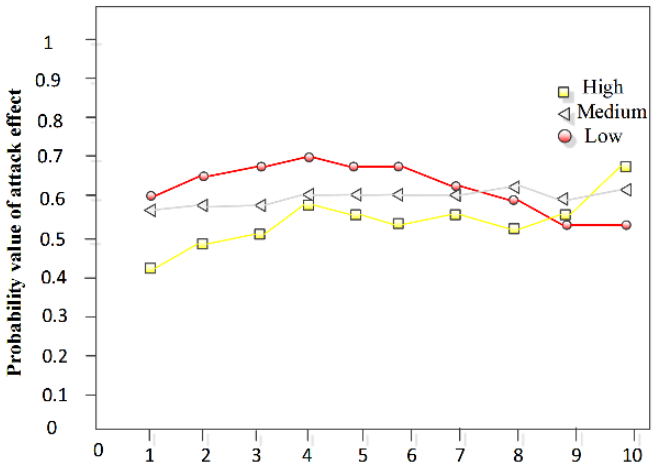


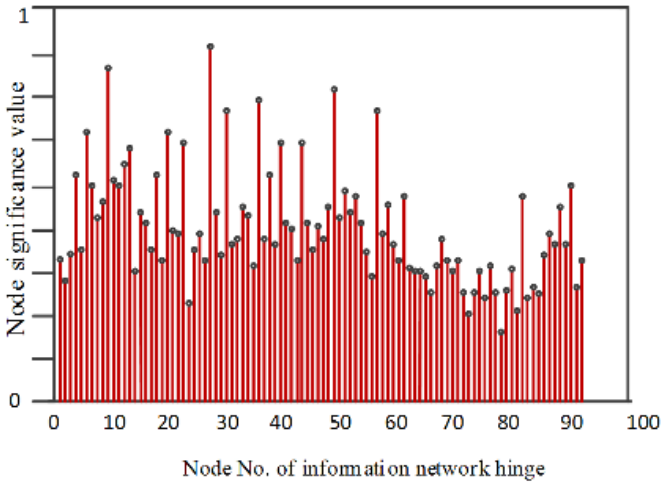
Fig. 3. Probability distribution for high, medium and low time of different attack effects of node 3

Figure 4 shows the probability distribution of attack effects from the first attack to the tenth attack. It can be seen that, from the first attack to the fourth attack, the attack strategy is formulated based on the known network topology. When the attack is carried out, the vulnerability feedback information, attack cost and attack loss are incomplete, and the attack effect is very low. After constant adjustment of attack strategy the attack effect was significantly improved and gradually increased to the peak value of the tenth attack. Finally, the average probability of the tenth highest attack effect on this node is 0.65. Similarly, this method was used to calculate the remaining 9 nodes, and the average probability of high attack effect was obtained as follows

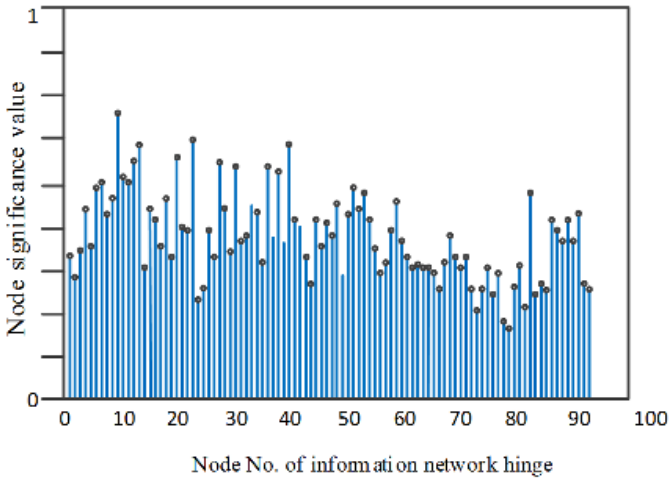
$\overline{P}_1 = 0.47,\ \overline{P}_2 = 0.52\ \overline{P}_3 = 0.33\ \overline{P}_4 = 0.52\ \overline{P}_5 = 0.63\ \overline{P}_6 = 0.39\ \overline{P}_7 = 0.65,\ \overline{P}_8 = 0.42\ \overline{P}_9 = 0.38\ \overline{P}_{10} = 0.36.$

D. Analysis of Method Efficiency

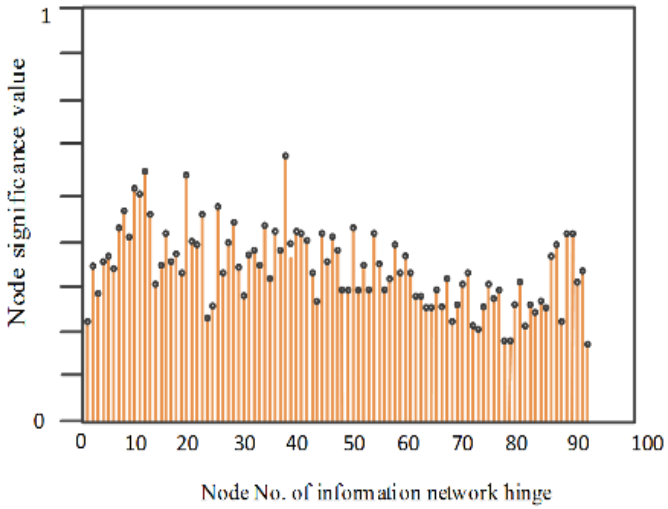
We simulated the attack in "backbone network for all-American information superhighway" (data publicized in 2007) by INET3.0.We define a network G_0 = (94, 239).Node deletion method, betweenness method and method in the thesis are respectively adopted for experiment. The network Go = (94,239) means that the network has 94 nodes and 239 inter-node links. Fig. 4 is distribution for node significance of all information hinges calculated with three methods. Attack strategy is formulated according to data calculated significance.The strategy is for simulation attack. Fig. 5, Fig. 6 and Fig. 7 are comparisons of network node distribution before and after attacking with node deletion method, between-ness 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_0 for fifty times, the network efficiency is calculated and summarized, as shown in Fig. 4. After comparing three pictures we can see that its attack node and order are obviously different, and attack effect is also different by choosing different method, using different attack algorithm. The method in this paper has the best effect.It can remain 57 nodes and 127 Internode links. Residual rate of nodes is 60.64%, and residual rate of links is 53.14%.The network is clearly dispersed.



a)Method in the Thesis

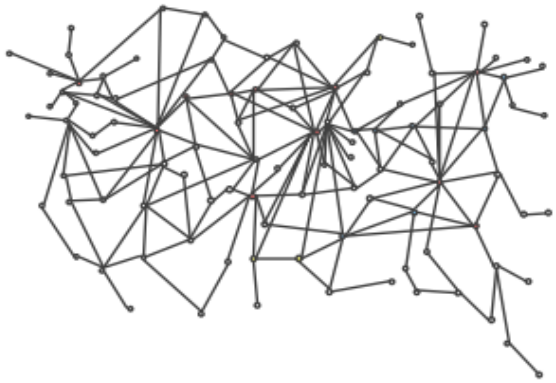


b)Node deletion method

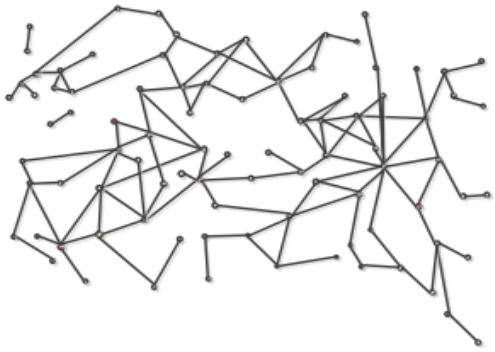


c)Beteenness method

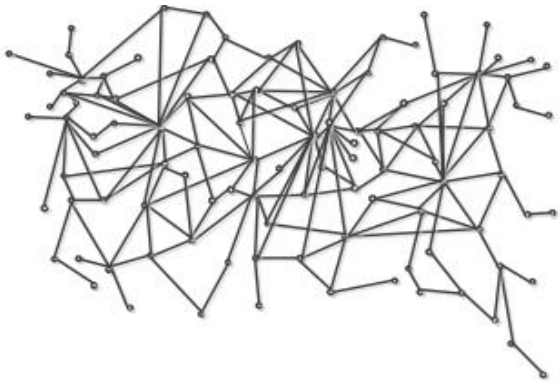
Fig. 4. Distribution for node significance in three methods



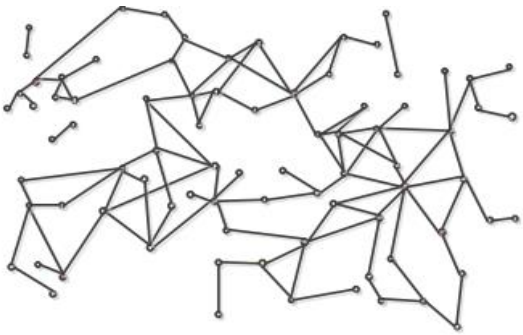
a. Connected distribution graph of network nodes before attacking with betweenness method



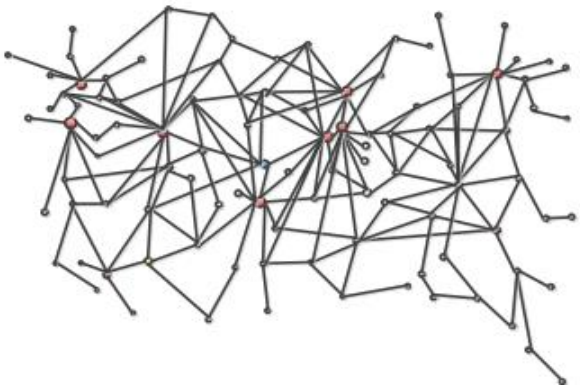
b. Connected distribution graph of network nodes after attacking with betweenness method



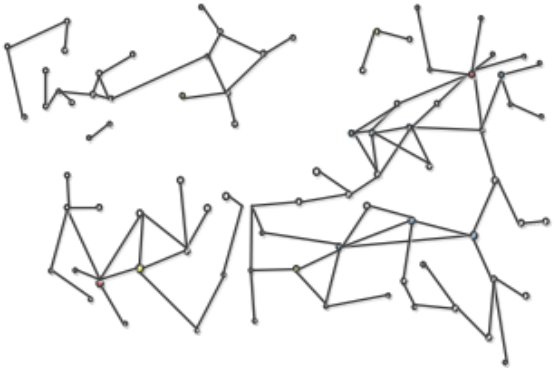
c. Connected distribution graph of network nodes before attacking with node deletion method



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

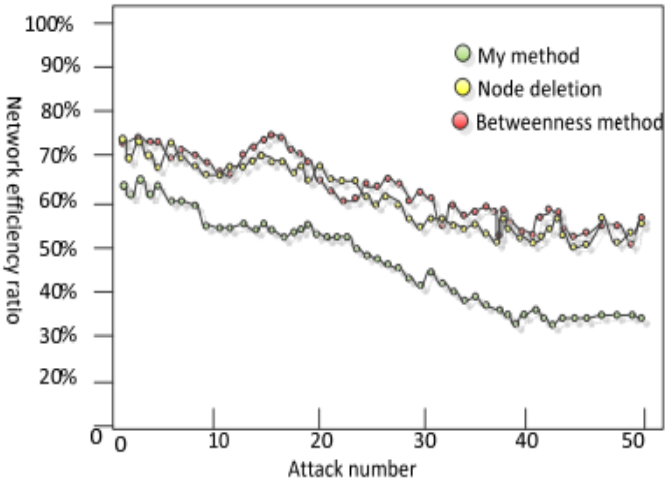


Fig. 6. Network efficiency comparison after attacking target network for 50 times with three methods

It can be seen in Fig. 5, Fig. 6 and Fig. 7 that effects of attack differ slightly after estimating significance of network nodes with typical betweenness method and node deletion method in simulation experiment. The method in the paper has obvious advantage in efficiency.When selective attack is implemented in complex network with the same topology structure, , effect produced by attack and expectation shall be fit in each attack 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 removing these nodes. 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.

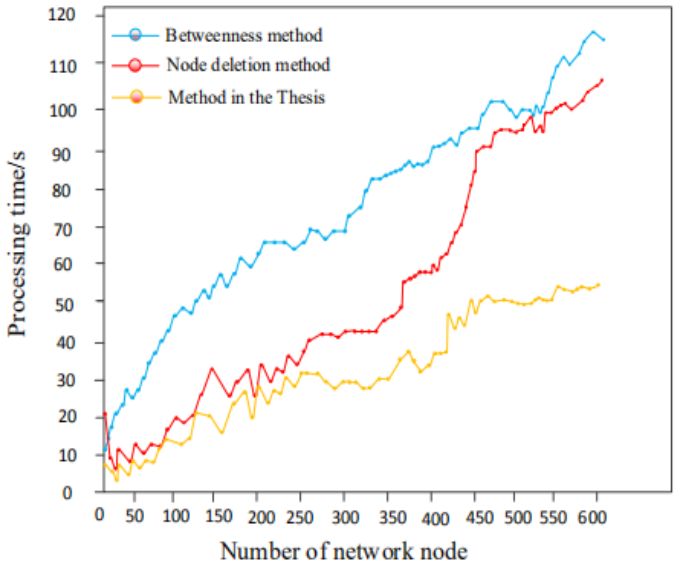


Fig. 7. Efficiency comparison after attacking target network with three methods

It can be seen in Fig. 7 that complexity of topology structure rises continuously when network scale increases continuously. The method in this paper is relatively stable in time consumption. It is superior to other two algorithms after reaching certain degree in network scale.

V. Conclusion

When attack strategy is formulated, structure, defense deployment and important nodes of network to be attacked are unknown and uncontrollable.Index data used to evaluate attack effect are always not comprehensive. If static methods are used to evaluate target network, it is strongly passive and there is always gap between expected effect. The attack effect is evaluated dynamically by analyzing all factors of network attack with dynamic Bayesian network. After considering the impact, costs and losses of the attack, a new attack method is proposed which can develop attack strategies and carry out attacks.

At the same time, the method in this paper is still has limitations. We need a lot of experimental data to give the value for Bayesian network. And the experimental data come from summary of experiences, such as Conditional transfer probability for index at node criterion level,State transfer probability of node attack effect, etc.They all need the support of the corresponding database.

References

[1]Pengfei Li,Yingke Lei. “Identification of Key nodes in Ad Hoc Network by Fusion Delete Method ”,Journal of Chinese Computer Systems,2017,pp.1198-1202.

[2] Lukas Pavlik, “Modeling the Impact of Selected Cyber Threats on the Organization's Parameters in the Framework of Cyber Risk Insurance”, WSEAS Transactions on Business and Economics, 2018,pp. 522-528, Volume 15.

[3] Pu Zaiyi. "Network security situation analysis based on a dynamic Bayesian network and phase space reconstruction", The Journal of Supercomputing, 2018 .

[4]Yifan Liu, Jianqiang Yi, Ruyi Yuan, Zhiqiang Pu. "Adaptive Type-2 Fuzzy Control for Flexible Air-breathing Hypersonic Vehicles with Measurement Noises", 2018 Annual American Control Conference (ACC), 2018.

[5]UPADHYAY R, Khan S, TRIPATHI H,ET AL, “Detection and prevention of DDOS attack in WSN for AODV and DSR using battery drain”, International Conference on Computing and Network Communications. IEEE, 2015, pp.446-451.

[6]Xiaocui Yang,Rutao Liu,Shao Xu. “Comparison of Application of Neural Network Algorithm in Computer Security Evaluation”, Computer Programming Skills & Maintenance,2016,pp.89-90

[7]Yiyou Xie,Gang Du,Yanyun Zhu,Chen Zhang.“Similar Image Retrieval Based on Neural Networks”, Telecommunication science,2020.

[8]Diego Espitia,Hernan Larralde. “Universal and non-universal text statistics: Clustering coefficient for language identification”,Physica A:Statistical Mechanics and its Applications,2020,Volume 553.

[9]Aneta Zemánková,Artificial Intelligence and Blockchain in Audit and Accounting: Literature Review, WSEAS Transactions on Business and Economics, 2019,pp. 568-581, Volume 16.

[10]Niu H, Jagannathan S, “Neural network-based attack detection in nonlinear networked control systems”, International Joint Conference on Neural Networks, 2016, pp.4249-4254.

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

[12]Djillali Bouagada, Samuel Melchior, Paul Van Dooren. “Calculating the H ∞ norm of a fractional system given in state-space form[J] Applied Mathematics Letters, 2018, pp.79