

基于多属性决策的复杂网络节点攻击研究

王劲松, 李宗育, 徐晏琦
(解放军信息工程大学, 郑州 450001)

摘要: 在复杂网络攻击中, 指挥决策者在制定攻击方案时缺乏可靠依据, 实施行动时难以达到任务目标效果, 针对这种情况提出了一种科学的复杂网络节点攻击效果评估方法。通过对网络攻击中攻击方收益、攻击方损耗、攻击方遇到的风险进行分析, 建立了相应的指标体系; 利用 TOPSIS 方法对网络中节点的攻击效果进行综合评估和排序, 有效克服了传统节点选取方法中依靠网络拓扑单一指标(如介数、度中心性)进行评价的片面性, 为制定网络攻击方案提供了科学依据。

关键词: 网络攻击; 多属性决策; 复杂网络; 综合评估

中图分类号: E27 **文献标志码:** A **文章编号:** 1671-637X(2016)04-0042-06

Complex Network Node Attacking Based on Multi-attribute Decision Making

WANG Jin-song, LI Zong-yu, XU Yan-qi
(The PLA Information Engineering University, Zhengzhou 450001, China)

Abstract: In complex network attacks, the lack of a reliable evidence for decision-makers in attack planning makes it difficult to achieve mission objectives in action. A scientific method for evaluating the complex network node attacking effect is presented. By analyzing the income, loss, and risks of the attacker, we established the corresponding index systems. TOPSIS method was used for making comprehensive assessment and sorting to the attacking effect of the nodes in the network. It can overcome the one-sidedness shortcoming of the traditional node selection method, i. e., relying on a single indicator of network topology. The study supplies a scientific basis for scheme making in network attacking.

Key words: network attack; multiple attribute decision making; complex network; comprehensive assessment

0 引言

信息化战场的态势感知系统、指挥控制系统、火力平台及各类作战单元由高度联结复杂网络所构成, 它是组成作战体系的关键, 在打击敌方信息系统时, 首先对其网络进行攻击, 能够直接破坏或瓦解敌方作战体系。然而信息化战场网络互联程度高、战场环境特殊、不确定性强、网络中节点众多、各节点价值迥异, 怎样使用有限的力量对其众多节点中最具价值的节点进行攻击, 直接关系到攻击效能的高低。例如在分布式拒绝服务攻击中(DDos), 选用的傀儡机或攻击目标节点不同, 攻击的效果也会不同。因此, 在攻击前必须对网络节点的攻击效果进行全面评估, 根据任务需求选择

不同节点作为傀儡机或攻击目标。

国外学者在该领域进行了一些研究, TSEN F P 和 SUNG T Y 提出了基于最小生成树准则来评价链路重要性的算法, 其思想是基于最小生成树定理, 当子网的生成树数目发生变化时, 变化越大则说明该链路越重要, 国内学者胡爱群、王勇等人以此为基础从网络的节点角度出发, 提出了基于最小生成树准则的节点删除法, 来判定网络各节点的重要性, 此外, 利用节点的某个属性计算其重要度是一种比较常用的评估方法, 以上传统方法在评价网络节点重要性时, 具有一定的精度, 但也存在一定缺陷, 对于节点删除法, 如果出现多个节点被删除使得网络不联通, 那么这些节点重要性为一致的, 这样未考虑相邻节点影响, 评估结果就不精确, 而对节点单一属性计算重要度又忽略了在复杂网络中节点的综合指标性质, 评估结果不全面^[1]。此外, 单纯考虑节点重要度选择攻击节点, 而忽略攻击付出的代价和攻击遭遇的风险等因素, 评估结果也会不

收稿日期: 2015-04-02

修回日期: 2015-11-25

基金项目: 信息化战场信息安全保障体系研究(13QJ003-22)

作者简介: 王劲松(1965—), 男, 河南确山人, 博士, 教授, 硕导, 研究方向为指挥决策支持技术及智能算法。

够客观。为此,本文在全面分析影响节点攻击效果的多属性指标因素的基础上,采用逼近理想解排序法(TOPSIS)^[2],对各节点攻击效果进行评估与排序,为攻击节点的选取提供依据,提高网络攻击效率。

1 网络节点评估指标体系的构建

大量的实战决策案例证明,导致网络攻击行动效果不佳的原因往往在于事前评估时所采用的评选指标不当,亦或根本没有明确的指标,攻击时存在盲目性^[3]。因此,对战场复杂网络中节点的攻击效果进行客观评价,建立合理完备的评估指标体系是进行综合评估的基础,这里按照构建指标体系的一般原则,综合考虑分析的各类影响因素,构建出评估指标体系,根据实际需求赋予指标权重。

1.1 建立指标体系

对于信息作战行动来说,实现任务目标的效果是衡量行动成功与否的首要指标,其次为使用的作战力量所付出的代价,最后,应当考虑行动中源于军事行动条件的不确定性导致可能出现的风险,其决定了攻击行动实施效果的不确定性^[4]。结合网络攻击行动特点,本文从攻击收益、攻击损耗和攻击风险3个评价准则出发,建立指标体系,如图1所示。

1) 攻击收益。

攻击收益指网络攻击行动收到的效果。在网络攻击过程中主要指被攻击的网络节点瘫痪后,会对敌方网络造成多大的影响,即攻击节点在敌方网络中的重要度。根据复杂网络理论,可以衡量网络中节点重要度的指标包括度中心性、接近中心性、介数中心性、结构洞等指标,各指标定义如下。

定义1 度中心性(degree centrality)。

与节点*i*相连边数同网络中与节点*i*可能相连的最大边数之比,表达式为

$$DG_i = k_i / (N - 1) \quad (1)$$

式中, k_i 为与节点*i*相连的边数。度中心性能够反映一个节点与其余节点的直接通信能力,其值越大通信能力越强。

定义2 接近中心性(closeness centrality)。

节点*i*与网络中其余节点的最短路径距离之和的倒数,若 d_{ij} 为节点*i*到节点*j*的最短距离,则其表达式为

$$CC_i = N / \sum_{j=1}^N d_{ij} \quad (2)$$

节点接近中心性值越大,其居于网络中心位置的程度越大,该节点就越重要。

定义3 介数中心性(betweenness centrality)。

若 $g_{jk}(i)$ 表示节点*j*和节点*k*之间经过节点*i*的最

短路径的条数, g_{jk} 表示节点*j*和节点*k*之间所有最短路径条数,则介数中心性表达式为

$$BC_i = \sum_{i \neq j \neq k \in V} \frac{g_{jk}(i)}{g_{jk}} \quad (3)$$

介数中心性定义认为,如果一个节点为网络中其余节点通信的必经之路,则其地位越重要,其对网络通信的影响力越大^[5]。

定义4 结构洞(structural holes)。

结构洞指网络中两个节点之间不存在直接连接或间接的冗余关系。Burt提出了计算结构洞的网络约束系数对网络闭合性和结构洞进行测度,其表达式为

$$C_i = \sum_j (p_{ij} + \sum_{q \neq i \neq j} p_{iq} p_{qj})^2 \quad (4)$$

式中: C_i 为网络约束系数; q 为节点*i*和节点*j*的间接连接节点; p_{ij} 为节点*i*花费在节点*j*上的时间(精力)占其总时间(精力)的比例。网络约束系数越小,结构洞的程度越大,节点的位置越重要。

2) 攻击损耗。

攻击损耗指攻击行动付出的代价。在网络攻击过程中主要指使用木马、病毒等攻击时,己方的计算机资源耗损量,可以衡量的指标包括带宽、CPU、内存的占用量以及进行攻击的时间。网络攻击中,每种攻击工具(装备)都拥有各自经过性能评估的资源代价^[6],而这些资源代价可以提取作为相应的指标。

3) 攻击风险。

攻击风险指攻击行动中因情况变化,导致方案实施效果与预期效果存在落差。网络攻击中的主要风险在于攻击过程中敌方系统防护度和被敌方发现后敌方自身漏洞的修复难度。敌方防护能力主要包括操作系统安全、防火墙、入侵检测、路由器安全、交换机安全。敌方节点漏洞修复难易度指标表现为敌方节点漏洞修复时间长短^[7]。

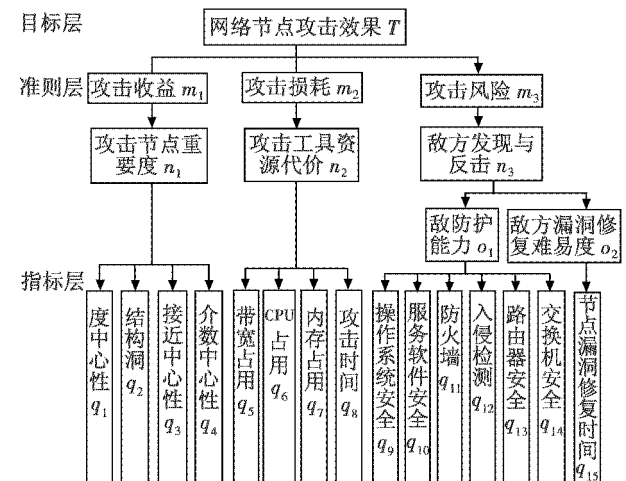


图1 网络节点攻击效果指标体系

Fig. 1 The index system of network node attacking effect

1.2 指标权重的确定

1) 准则层权重的确定。

确定准则层攻击损耗、攻击收益、攻击风险的权重时,须根据实际作战需求进行设置。如在不惜代价进行攻击时,要提高攻击收益权重;在保全自身力量的情况下,要提高攻击损耗权重^[8]。在操作时,可采用专家打分法,根据实际作战需求确定。

2) 指标层权重的确定。

确定指标层各因素权重时,可使用层次分析法(Analytic Hierarchy Process, AHP)确定,步骤如下。

① 构造两两判断矩阵。采用9标度法,对同一层次各指标打分量化,建立判断矩阵A。

② 计算特征向量及最大特征值。将判断矩阵的每一列向量归一化,得到 $B = (b_{ij})_{m \times n}$

$$b_{ij} = a_{ij} / \sum_{k=1}^n a_{ik} \quad i = 1, 2, \dots, n; j = 1, 2, \dots, n \quad (5)$$

B的行向量的元素算术平均值为

$$\omega_i = \frac{1}{n} \sum_{j=1}^n b_{ij} \quad i = 1, 2, \dots, n; j = 1, 2, \dots, n \quad (6)$$

计算最大特征值

$$\lambda_{\max} = \frac{1}{n} \sum_{i=1}^n \frac{(A\omega)_i}{\omega_i} \quad (7)$$

③ 检验矩阵一致性。

计算一致性指标

$$C.I = \frac{\lambda_{\max} - n}{n - 1} \quad (8)$$

利用一致性R.I(如表1所示)。

表1 一致性R.I

Table 1 R.I consistency

阶数	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

计算一致性比例

$$C.R = \frac{C.I}{R.I} \quad (9)$$

当 $C.R < 0.1$ 时,认为判断矩阵A有满意一致性;当 $C.R \geq 0.1$ 时,认为判断矩阵不具有满意一致性,需要进行修正。

2 基于TOPSIS的网络节点攻击效果评价方法

基于TOPSIS的网络节点攻击效能评估方法,其思想是将每个节点看作一个方案,将节点的各个指标看作方案的各个属性,则评价节点攻击效果就转化为对各个方案进行评估排序的多属性决策问题^[9]。

若战场复杂网络中的节点数为 m ,则节点集为 $V =$

$\{V_1, V_2, \dots, V_m\}$,每个节点的评价指标为 n 个,则节点的指标集 $q = \{q_1, q_2, q_3, \dots, q_n\}$ 。节点 V_i 在指标 q_i 下的评价值为 $x_i(j), i = 1, 2, \dots, m; j = 1, 2, \dots, n$,则建立评估矩阵 $X[x_i(j)]_{m \times n}$ 的步骤如下所述。

1) 利用向量归一化方法对评估矩阵作标准化处理,得到标准化矩阵 $Y[y_i(j)]_{m \times n}$,式中

$$y_i(j) = x_i(j) \left(\sum_{i=1}^m [x_i(j)]^2 \right)^{-1/2} \quad (10)$$

2) 计算加权标准化判断矩阵

$$U = [u_i(j)]_{m \times n} = [\omega_j y_i(j)]_{m \times n} \quad (11)$$

式中, ω_j 为指标 q_j 的权重。

3) 确定理想解和负理想解。

确定理想解为

$$U_0^+ = \{ \max_{i \leq 1 \leq m} u_i(j) \mid j \in J^+, \min_{i \leq 1 \leq m} u_i(j) \mid j \in J^- \} = (u_0^+(1), u_0^+(2), \dots, u_0^+(j), \dots, u_0^+(n)) \quad (12)$$

确定负理想解为

$$U_0^- = \{ \min_{i \leq 1 \leq m} u_i(j) \mid j \in J^+, \max_{i \leq 1 \leq m} u_i(j) \mid j \in J^- \} = (u_0^-(1), u_0^-(2), \dots, u_0^-(j), \dots, u_0^-(n)) \quad (13)$$

式中: J^+ 为效益型指标集合; J^- 为成本性指标集合。

4) 计算各节点评估值到理想解和负理想解的灰色关联度。节点 V_i 评估值与理想解和负理想解关于指标 T_i 的灰色关联系数分别为

$$e_{ij}^+ = \frac{\min_i \min_j |u_0^+(j) - u_i(j)| + \rho \max_i \max_j |u_0^+(j) - u_i(j)|}{|u_0^+(j) - u_i(j)| + \rho \max_i \max_j |u_0^+(j) - u_i(j)|} \quad (14)$$

$$e_{ij}^- = \frac{\min_i \min_j |u_0^-(j) - u_i(j)| + \rho \max_i \max_j |u_0^-(j) - u_i(j)|}{|u_0^-(j) - u_i(j)| + \rho \max_i \max_j |u_0^-(j) - u_i(j)|} \quad (15)$$

式(14)和(15)中, ρ 为关联系数, $0 \leq \rho \leq 1$,通常取0.5。

理想解与节点 V_i 的灰色关联度为

$$E_i^+ = \frac{1}{n} \sum_{j=1}^n e_{ij}^+ \quad i = 1, 2, \dots, m \quad (16)$$

$$E_i^- = \frac{1}{n} \sum_{j=1}^n e_{ij}^- \quad i = 1, 2, \dots, m \quad (17)$$

5) 计算理想解贴近度。取节点 i 与理想解和负理想解的比值 $T_i = E_i^+ / (E_i^+ + E_i^-)$ 作为贴近度^[10]。 E 越大,表明节点评估解与理想解和负理想解的相关程度比越大,即节点靠近理想解而远离负理想解,所以 E 越大表明节点攻击效果越好。

3 实例分析

某网络攻击行动中,对形如图2的“风筝网络”进行攻击,经过侦察可知各节点漏洞情况,现需对攻击节点效能进行评估,以选择最优攻击节点。

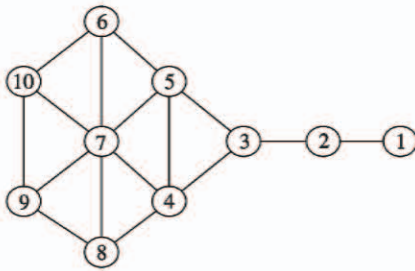


图2 风筝网络

Fig. 2 The kite network

3.1 确定权重

根据专家打分情况,确定准则层攻击收益、攻击损耗、攻击风险的权重为 $\omega_m^i = (0.7, 0.15, 0.15)$ 。运用两两对比法,敌方发现与反击各指标为 $\omega_o^n = (0.652, 0.348)$ 。指标层中攻击收益各指标权重为 $\omega_{q(1-4)}^n = (0.086, 0.207, 0.307, 0.499)$,攻击损耗各指标权重为 $\omega_{q(5-8)}^n = (0.25, 0.35, 0.25, 0.15)$,我方防护能力各指标权重为 $\omega_{q(9-14)}^o = (0.126, 0.231, 0.258, 0.115, 0.113, 0.157)^{[11]}$ 。

因此,指标层相对于最高层的权重为: $\omega_m^i(1) \times \omega_n^m \times \omega_{q(1-4)}^n = (0.0602, 0.1449, 0.2149, 0.2800)$;

$\omega_{q(5-8)}^i = \omega_m^i(2) \times \omega_n^m \times \omega_{q(5-8)}^n = (0.0375, 0.0525, 0.0375, 0.0225)$; $\omega_{q(9-14)}^i = \omega_m^i(3) \times \omega_o^n(1) \times \omega_{q(5-8)}^o = (0.0123, 0.0226, 0.0252, 0.0112, 0.0111, 0.0154)$; $\omega_{q15}^i = \omega_m^i(3) \times \omega_o^n(2) \times \omega_{q15}^o = 0.15 \times 0.348 \times 1 = 0.0522$ 。因此 $\omega_q^i = (\omega_{q(1-4)}^i, \omega_{q(5-8)}^i, \omega_{q(9-14)}^i, \omega_{q15}^i) = (0.0602, 0.1449, 0.2149, 0.2800, 0.0375, 0.0525, 0.0375, 0.0225, 0.0123, 0.0226, 0.0252, 0.0112, 0.0111, 0.0154, 0.0522)$ 。

3.2 进行评估

1) 确定评估矩阵。

指标 $q_1 \sim q_4$ 可利用相应的 Matlab 算法计算得出;对网络中各节点的漏洞进行分析,确定选用的攻击工具集合为 $\{P_1, P_2, \dots, P_n\}$, 每种攻击 P_i 都有经过系统测评的资源消耗代价 $C_i(q_5, q_6, q_7, q_8)$, 则指标 $q_5 \sim q_8$ 即为资源消耗的总代价 $C = \sum_{i=1}^n C_i^{[12]}$; 指标 $q_9 \sim q_{14}$ 可通过我方攻击系统防护能力评估得到; 指标 q_{15} 可通过对节点漏洞分析得到。

通过搭建模拟系统,构造“风筝网络”拓扑环境,根据实际情况采集各指标数据如表2所示。

表2 各指标采集数据
Table 2 Index data

ID	q_1	q_2	q_3	q_4	q_5	q_6	q_7	q_8	q_9	q_{10}	q_{11}	q_{12}	q_{13}	q_{14}	q_{15}
1	0.1111	1.25	0.3448	0	0.28	0.55	0.13	15	65	88	66	54	63	45	63
2	0.2222	0.5556	0.4762	16	0.35	0.41	0.08	18	75	65	42	59	52	55	56
3	0.3333	0.4944	0.6667	28	0.24	0.47	0.09	10	66	58	49	65	68	71	47
4	0.5556	0.4701	0.7143	16.67	0.29	0.53	0.12	12	68	45	75	36	91	41	45
5	0.5556	0.4701	0.7143	16.67	0.35	0.56	0.11	13	43	89	63	69	57	54	42
6	0.3333	0.7059	0.5556	0	0.33	0.43	0.08	22	62	63	87	78	84	74	74
7	0.6667	0.4746	0.6667	7.33	0.31	0.33	0.05	32	54	65	78	87	75	44	36
8	0.3333	0.7059	0.5556	0	0.27	0.31	0.16	26	26	38	25	81	54	73	87
9	0.4444	0.5783	0.5882	1.67	0.26	0.29	0.06	16	58	45	61	76	87	82	78
10	0.4444	0.5783	0.5882	1.67	0.23	0.36	0.07	11	35	63	86	62	63	67	58

不同指标取值范围相差巨大,各指标物理意义和计量单位不同,所以需要原始数据进行归一化去量

纲处理^[13],得到标准化矩阵

$$X[x_i(j)]_{m \times n} =$$

0.082	0.593	0.183	0	0.301	0.4	0.409	0.253	0.359	0.435	0.316	0.25	0.282	0.229	0.328
0.163	0.263	0.252	0.393	0.377	0.298	0.252	0.303	0.415	0.321	0.201	0.274	0.233	0.28	0.292
0.245	0.234	0.353	0.688	0.258	0.342	0.283	0.168	0.365	0.287	0.235	0.301	0.304	0.361	0.245
0.408	0.223	0.378	0.41	0.312	0.386	0.378	0.202	0.376	0.222	0.36	0.167	0.407	0.209	0.234
0.408	0.223	0.378	0.41	0.377	0.407	0.346	0.219	0.238	0.44	0.302	0.32	0.255	0.275	0.219
0.245	0.335	0.294	0	0.355	0.313	0.252	0.371	0.343	0.311	0.417	0.362	0.376	0.376	0.385
0.49	0.225	0.353	0.18	0.334	0.24	0.157	0.539	0.299	0.321	0.374	0.403	0.336	0.224	0.187
0.245	0.335	0.294	0	0.291	0.226	0.504	0.438	0.144	0.188	0.12	0.376	0.242	0.371	0.453
0.327	0.274	0.312	0.041	0.28	0.211	0.189	0.27	0.321	0.222	0.292	0.352	0.389	0.147	0.406
0.327	0.274	0.312	0.041	0.248	0.262	0.22	0.185	0.194	0.311	0.412	0.287	0.282	0.341	0.302

对标准化矩阵进行加权,得到加权标准化判断矩阵

$$Y[y_i(j)]_{m \times n} =$$

0.005	0.086	0.039	0	0.011	0.021	0.015	0.006	0.004	0.01	0.008	0.003	0.003	0.004	0.017
0.01	0.038	0.054	0.11	0.014	0.016	0.009	0.007	0.005	0.007	0.005	0.003	0.003	0.004	0.015
0.015	0.034	0.076	0.193	0.010	0.018	0.011	0.004	0.004	0.006	0.006	0.003	0.003	0.006	0.013
0.025	0.032	0.081	0.115	0.012	0.020	0.014	0.005	0.005	0.005	0.009	0.002	0.005	0.003	0.012
0.025	0.032	0.081	0.115	0.014	0.021	0.013	0.005	0.003	0.010	0.008	0.004	0.003	0.004	0.011
0.015	0.048	0.063	0	0.013	0.016	0.009	0.008	0.004	0.007	0.011	0.004	0.004	0.006	0.020
0.029	0.033	0.076	0.050	0.013	0.013	0.006	0.012	0.004	0.007	0.009	0.005	0.004	0.003	0.010
0.015	0.048	0.063	0	0.011	0.012	0.019	0.010	0.002	0.004	0.003	0.004	0.003	0.006	0.024
0.020	0.040	0.067	0.011	0.010	0.011	0.007	0.006	0.004	0.005	0.007	0.004	0.004	0.006	0.021
0.020	0.040	0.067	0.011	0.009	0.014	0.008	0.004	0.002	0.007	0.010	0.003	0.003	0.005	0.016

其中, q_1, q_3, q_4, q_{15} 为效益型指标, 其余为成本型指标, 因此理想解为: $U_0^+ = (0.029, 0.032, 0.081, 0.193, 0.009, 0.011, 0.006, 0.004, 0.002, 0.004, 0.003, 0.003, 0.003, 0.003, 0.024)$; 负理想解为: $U_0^- = (0.005, 0.086,$

$0.039, 0, 0.014, 0.021, 0.019, 0.012, 0.005, 0.01, 0.011, 0.005, 0.005, 0.006, 0.010)$ 。

经过计算, 每个节点评估值到正理想方案和负理想方案距离以及贴近度见表3。

表3 贴近度计算结果

Table 3 Calculation results of close degree

ID	1	2	3	4	5	6	7	8	9	10
E_i^+	0.206 840 716	0.121 421	0.021 384	0.080 574	0.080 915	0.518 054	0.143 835	0.195 585	0.182 6	0.182 862
E_i^-	0.011 630 635	0.121 421	0.203 759	0.135 487	0.135 405	0.482 094	0.087 299	0.049 867	0.061 02	0.059 809
$E_i^+ + E_i^-$	0.218 471 35	0.242 842	0.225 143	0.216 061	0.216 32	1.000 148	0.231 133	0.245 453	0.243 619	0.242 671
E_i	0.532 364 3	0.5	0.905 02	0.627 076	0.625 948	0.482 023	0.377 699	0.203 164	0.250 471	0.246 46

由表可见, 按照贴近度, 各点攻击效果排序为: $T_3 > T_5 > T_4 > T_2 > T_6 > T_7 > T_9 > T_{10} > T_8 > T_1$ 。

因而, 可以按上述顺序选择攻击节点。从图2来看, 节点3位于网络中信息控制能力最大的位置, 对节点3的破坏将导致整个网络不再连通, 所以对其进行攻击的效果最大; 节点4, 5在网络中结构位置一样, 所以攻击效果相同, 对这两个节点的破坏会导致网络中节点间的通信距离增大, 因而重要性次之; 节点2是介数值较大的节点, 破坏节点2会导致节点1与网络断开, 其重要性次于节点4和5; 节点7度数最大, 但对其进行破坏仅使得网络的通信冗余度变少, 对整个网络的通信能力未造成影响; 节点9和节点10, 节点6和节点8, 在网络中的结构位置相同, 这些节点受到破坏并没有对网络的连通造成影响, 所以对其攻击的效能更为靠后。

3.3 算法效率分析

为进一步说明本文算法的有效性, 对图3中ARPA网络拓扑结构 (ARPA拓扑是目前分析网络节点重要程度时广泛使用的干线网络拓扑)^[14] 分别运用本文算法、节点删除法和介数法进行分析。

节点删除法是根据节点为网络提供的最短可用路由功能及移除节点后网络生成数目的变化判断其重要程度, 从表4中可以看出, 这种算法对各节点重要度区分不够明显。介数法根据节点介数值大小判断其重要度, 不够全面, 这种算法下节点 $V_7, V_8, V_9, V_{10}, V_{11}$ 的重要程度一致, V_{20} 与 V_{21} 重要度一致, 没有区分开。使用

本文算法在精度上更加准确, 同时区分度更高。

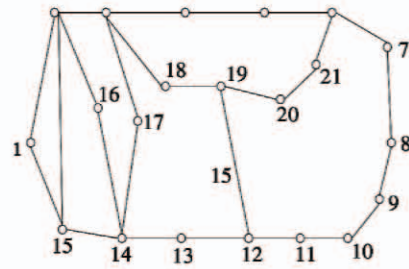


图3 ARPA网络

Fig.3 ARPA network

表4 节点重要度计算结果对比

Table 4 Calculation result of node important degree

节点	介数法	节点删除法	本文算法
V_1	0.034 522	0.626 223	0.372 165
V_2	0.175 932	0.972 121	0.954 082
V_3	0.452 641	0.993 037	0.933 236
V_4	0.294 827	0.838 727	0.391 127
V_5	0.267 923	0.838 751	0.348 632
V_6	0.349 413	0.983 613	0.372 138
V_7	0.189 952	0.879 737	0.234 082
V_8	0.142 861	0.879 737	0.203 164
V_9	0.139 826	0.879 737	0.172 295
V_{10}	0.192 214	0.879 737	0.153 729
V_{11}	0.268 311	0.879 737	0.327 108
V_{12}	0.438 326	0.978 028	0.532 077
V_{13}	0.245 613	0.805 152	0.551 392
V_{14}	0.252 521	0.986 470	0.872 437
V_{15}	0.101 879	0.878 718	0.913 236
V_{16}	0.070 832	0.663 938	0.734 133

续表

节点	介数法	节点删除法	本文算法
V_{17}	0.143 057	0.697 716	0.831 624
V_{18}	0.238 371	0.770 123	0.692 519
V_{19}	0.365 092	0.967 137	0.582 364
V_{20}	0.173 484	0.827 953	0.337 591
V_{21}	0.162 753	0.827 953	0.270 452

最后在 Intel Atom Z3560 微机上使用 Matlab 程序对规模不同的随机网络(ER 模型,连接概率 $p = 0.35$)进行节点重要度评估,从图 4 可以看出,网络规模越大,节点越多时,本文算法明显优于其他两种算法,对节点数目为 500 的网络进行评估仅需要 24 s。

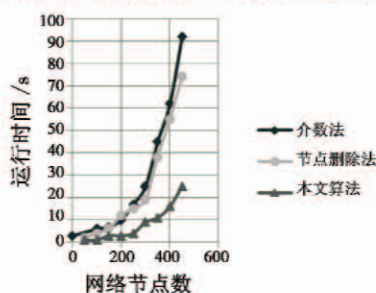


图 4 3 种算法效率对比

Fig. 4 Efficiency contrast of the three kinds of algorithms

4 结束语

在网络攻击行动中,对攻击节点的选取不仅要考虑其在战场网络拓扑中的重要度,更要考虑攻击中我方力量的消耗程度以及敌方针对攻击行动做出的抗击行动。本文通过对战场复杂网络中各种因素综合分析,建立评估指标体系,运用 TOPSIS 方法,对各节点攻击效果进行评估排序,为指挥决策者在制定网络攻击方案和实施攻击行动时提供了更加科学、自主、可控的辅助决策手段,能够较大提高信息作战中网络攻击的效果。

参考文献

[1] 章丽娟,王清贤. 网络攻击方案评估系统设计与仿真[J]. 计算机工程与设计, 2012, 33(5): 1746-1751. (ZHANG L J, WANG Q X. Network attack scenarios evaluation system design and simulation[J]. Computer Engineering and Design, 2012, 33(5): 1746-1751.)

[2] 许峰,毛钢,秦臻. 复杂网络特征量度及典型网络模型分析[J]. 通信技术, 2010, 43(9): 112-114. (XU F, MAO G, QIN Z. Analysis of characteristic measurement and typical network models in complex network[J]. Communications Technology, 2010, 43(9): 112-114.)

[3] 罗高健,郭建蓬. 通信网节点集攻击效能评估[J]. 舰船电子工程, 2012, 32(7): 65-67. (LUO G J, GUO J P. Efficiency evaluation of communication network's nodes attacks[J]. Ship Electronic Engineering, 2012, 32(7): 65-67.)

[4] 周璇,张凤鸣,李克武,等. 利用重要度评价矩阵确定复杂网络关键节点[J]. 物理学报, 2012, 61(5): 050201-050206. (ZHOU X, ZHANG F M, LI K W, et al. Efficiency key importance evaluation matrix is used to determine the complex network nodes[J]. Acta Phys. Sin, 2012, 61(5): 050201-050206.)

[5] 张益. 一种定量评估复杂网络节点重要度的算法[J]. 计算机工程, 2011, 37(20): 87-89. (ZHANG Y. Quantitative evaluation algorithm for node importance of complex networks[J]. Computer Engineering, 2011, 37(20): 87-89.)

[6] 陈静,孙林夫. 复杂网络中节点重要度评估[J]. 西南交通大学学报, 2009, 44(3): 426-429. (CHEN J, SUN L F. Evaluation of node importance in complex networks[J]. Journal of Southwest Jiaotong University, 2009, 44(3): 426-429.)

[7] 张喜平,李永树,刘刚,等. 节点重要度贡献的复杂网络节点重要度评估方法[J]. 复杂系统与复杂性科学, 2014, 11(3): 26-32. (ZHANG X P, LI Y S, LIU G, et al. Evaluation method of importance for nodes in complex networks based on importance contribution[J]. Complex Systems and Complexity Science, 2014, 11(3): 26-32.)

[8] 赫南,李德毅,淦文燕,等. 复杂网络中重要性节点发掘综述[J]. 计算机科学, 2007, 34(12): 1-4. (HE N, LI D Y, GAN W Y, et al. Mining vital nodes in complex networks[J]. Computer Science, 2007, 34(12): 1-4.)

[9] 刘建国,任卓明,郭强,等. 复杂网络中节点重要性排序的研究进展[J]. 物理学报, 2013, 62(17): 178901-178909. (LIU J G, REN Z M, GUO Q, et al. Node importance ranking of complex networks[J]. Acta Phys. Sin, 2013, 62(17): 178901-178909.)

[10] 刘建香. 复杂网络及其在国内研究进展的综述[J]. 系统科学学报, 2009, 17(4): 31-36. (LIU J X. Complex network and review of domestic research[J]. Journal of Systems Science, 2009, 17(4): 31-36.)

[11] HOU B N, YAO Y P, LIAO D S. Identifying all-around nodes for spreading dynamics in complex networks[J]. Physica A Statistical Mechanics & Its Applications, 2012, 391(15): 4012-4017.

[12] 李茂林,龙建国,刘伟涛. 信息化条件下作战体系节点重要性指标的选择[J]. 火力与指挥控制, 2011, 36(8): 119-122. (LI M L, LONG J G, LIU W T. Choice of importance index for nodes of operational system of systems under the informationized condition[J]. Fire Control & Command Control, 2011, 36(8): 119-122.)

[13] HARDY G, LUCET C, LIMNIOS N. K-Terminal network reliability measures with binary decision diagrams[J]. IEEE Transactions on Reliability, 2007, 56(3): 506-515.

[14] MISHRA R, CHATURVEDI S K. A cutsets-based unified framework to evaluate network reliability measures[J]. IEEE Transaction on Reliability, 2009, 58(4): 658-666.