控制与决策
Control and Decision

一种面向网络连通性的关键网络元素脆弱性分析方法

刘树美， 于尧， 郭磊

引用本文:
刘树美, 于尧, 郭磊. 一种面向网络连通性的关键网络元素脆弱性分析方法[J]. 控制与决策, 2020, 35(6): 1421−1426.

在线阅读 View online: https://doi.org/10.13195/j.kzyjc.2018.1280

文章编号: 1001-0920(2020)06-1421-06 DOI: 10.13195/j.kzyjc.2018.1280

一种面向网络连通性的关键网络元素脆弱性分析方法

刘树美, 于 尧†, 郭 磊

(东北大学 计算机科学与工程学院，沈阳 110169)

摘 要: 准确评估网络系统脆弱性对于网络安全规划和风险管理至关重要. 现有网络脆弱性分析方法大多利用单一特性识别脆弱元素,随着网络系统复杂化进程加快,多元化的脆弱性识别显得尤为重要. 从攻击者的角度出发,提出一种面向网络连通性的关键元素脆弱性分析方法,识别网络中具有多重重要身份且破坏代价小的网络元素,利用局部分析措施确定网络关键元素并将网络连通性作为脆弱性衡量指标,以识别出关键元素中可致使网络连通性特定降级的最小代价集合. 仿真结果表明,所提出方案对脆弱元素的定位更加准确,可为网络安全防护措施的制定提供有效且可靠的参考.

关键词: 网络安全；网络脆弱性分析；连通性；关键元素；破坏代价

中图分类号: TN918 **文献标志码:** A

A vulnerability analysis method for critical elements based on network connectivity

LIU Shu-mei, YU Yao†, GUO Lei

(College of Computer Science and Engineering，Northeastern University，Shenyang 110169，China)

Abstract: Accurately assessing the vulnerability of network systems is vital for network security planning and risk management. Existing network vulnerability analysis methods mostly focus on identifying vulnerable elements with a single feature. With the quickening of network system complexity process, the diversified vulnerability identification is particularly important. This paper innovatively proposes a vulnerability analysis method for critical elements based on network connectivity from the perspective of attackers, identifying network elements with multiple important identities and low-disruption-cost. Critical elements are identified by using local analysis measures, network connectivity is used as the measure of vulnerability to identify the minimum-cost set of critical elements that can cause a particular degradation of network connectivity. The simulation results show that the proposed scheme is more accurate in locating vulnerable elements and can provide an effective and reliable reference for the development of protection measures.

Keywords: network security；network vulnerability analysis；connectivity；critical element；disruption cost

0 引 言

从自然灾害到恶意攻击的破坏性事件将严重损害网络正常运转和提供正常服务的能力,尤其是诸如电网或公路系统[1]等基础设施的故障事件,会对网络系统造成极其严重的毁坏结果,甚至可能导致全网的瘫痪[2-3]. 因此,全面评估网络中的安全薄弱点并识别出可能出现的最具破坏性的攻击事件,对于相应安全措施的制定以及全网服务质量的保障至关重要[4],这也使得网络脆弱性分析领域成为学者们近几年研究的热点.

国内外研究学者利用图论知识,已对网络脆弱性分析作过大量的研究. 最初的研究手段将脆弱元素定义为网络中的局部关键元素[5-7],比如,利用度中心性识别具有一定控制作用的“大流量”节点[5];利用介数中心性识别在网络通信或传输过程中可起到“传输桥梁”作用的节点或链路等[6]. 然而,这些分析手段都属于局部分析措施,无法反映出这些元素在网络全局中的作用,更无法体现其在网络整体连通性中的重要程度.

众所周知,网络连通性是保证网络系统正常运转的最基本前提条件[8]. 为了在整体连通功能上提高网络的鲁棒性,研究学者们从网络连通性的角度出发并制定相应的分析措施,目的是识别在网络整体连通角度占据重要位置的节点或链路[9-12].

收稿日期: 2018-09-19；**修回日期:** 2019-01-07.

基金项目: 国家自然科学基金项目(61771120)；中央高校基本科研业务费项目(N171602002, N181613003).

责任编委: 林崇.

†通讯作者. E-mail: yuyao@mail.neu.edu.cn.

文献[9-11]将网络元素脆弱性分析作为一种优化问题. 文献[9-10]识别可导致网络全局成对连接特定降级的最小节点或链路集合. 文献[11]提出了一种自适应分析算法分析动态网络中的脆弱节点和脆弱链路. 文献[12]利用谱方法分析传输网络中的瓶颈路段. 虽然这些研究从网络全局连通性进行分析,然而却将节点脆弱性和链路脆弱性分开考虑,忽略了攻击者针对节点和链路的联合攻击场景. 针对这一研究空白,文献[13]面向联合攻击场景提出了相应的脆弱性分析方案,并引入攻击代价问题来定位攻击者最可能发起的攻击事件.

然而,以上研究都侧重于利用单一特性去识别对应特征下的脆弱元素,忽略了具有多重重要身份元素的失效可能对网络造成的破坏,同时也忽视了攻击者的针对性攻击可导致的巨大损失.

随着当今网络复杂化进程的加快,为了应对更加多元化的网络环境,脆弱元素的多重定位与分析是网络优化与鲁棒性设计的基础. 因此,针对现有研究中对联合攻击场景研究较少及对脆弱元素定位不够全面的现状,本文针对联合攻击场景提出一种面向网络连通性的关键网络元素脆弱性分析方法(aulnerability analysis hod for critical elements based on network connectivity, NLC-C),以解决现有脆弱性分析方法脆弱元素定位单一的问题与脆弱程度量化不全面问题.

本文所提出NLC-C方案的目标为识别关键节点和链路集合中可对网络整体连通性造成特定破坏且破坏代价最小的一组元素,这样的网络元素因具有多重重要身份,且破坏代价小或需破坏元素个数少而极易成为攻击者的目标,因此对其进行识别定位与脆弱程度衡量,可为网络优化与结构鲁棒性设计措施提供可靠的参考.

1 面向网络连通性的关键元素脆弱性分析

1.1 模型与定义

为了方便分析,本文将一般网络模型抽象为$G=(V,E)$,将真实网络中的节点连接关系映射到模型图中,其中$V=v_1,v_2,\dots,v_n$指网络图中所有节点的集合,$E=e_1,e_2,\dots,e_m$表示所有链路的集合,用n和m分别表示节点和链路总数.

值得指出的是,网络模型图分为有向图和无向图. 在有向图中,网络元素之间的通信或传输只能按照规定的方向进行. 本文分析考虑的是更加普适的无向网络图,无向图可以看作每条链路都有两个方向的有向图,在现实场景中的应用更加广泛.

另外,为了方便方案设计与分析,本文引入以下几点定义.

定义1 (网络连通性$P(G)$) 本文利用网络连通性$P(G)$作为脆弱性度量依据,用来衡量对脆弱元素进行破坏后网络中总连通对的变化情况. $P(G)$指的是网络中的连通对总数,即

$$P(G)=\frac{\sum\limits_{i,j\in V,i\neq j}u_{ij}}{2}. \tag{1}$$

$P(G)$可以度量脆弱元素对网络通信或传输能力的破坏情况,其中u_{ij}代表节点i与节点j之间的连通关系,可以表示为

$$u_{ij}=\begin{cases}1,\ \text{节点}i\text{与节点}j\text{之间有路径;}\\ 0,\ \text{节点}i\text{与节点}j\text{之间没有路径.}\end{cases} \tag{2}$$

定义2 (破坏程度$\alpha, 0\leqslant\alpha\leqslant 1$) 为了更加直观地展示分析结果对于网络整体的重要性,利用变量α表示当分析得到的脆弱元素遭到攻击破坏后网络连通性的降级程度. 具体表现在: 当图G为强连通图时,其连通性$P(G)=\begin{pmatrix}n\\2\end{pmatrix}$,若脆弱元素集合为$S$,则去除$S$中元素后剩余残缺图的连通性如下所示:

$$P(G\backslash S)=\frac{\sum\limits_{i,j\in G\backslash S,i\neq j}u_{ij}}{2}=(1-\alpha)\begin{pmatrix}n\\2\end{pmatrix}. \tag{3}$$

其中: $G\backslash S$为对S中脆弱元素进行破坏后剩余的残缺网络图,此时残缺图的连通性为原始网络图的$1-\alpha$倍,即变量α反映了分析得到的脆弱元素对网络整体连通性可达到的破坏程度或等级.

定义3 (破坏代价$c(\cdot)$) 为了站在攻击者的角度分析网络脆弱性,本文引入破坏代价问题,即破坏网络中节点或链路需要付出的代价$c(\cdot)$,具体表现为攻击所用时间、精力、费用或攻击成功的概率的倒数等. 攻击者发动攻击时,无疑试图选择最容易攻击的、开销最小或耗时最短的元素,这就涉及到攻击的最小代价问题,也就是本文方案分析的核心问题. 对于分析得到的脆弱元素集合S,其集合元素总破坏代价如下:

$$C(S)=\sum_{i\in S_V}c(i)+\sum_{(i,j)\in S_E}c(i,j). \tag{4}$$

其中: $c(i)$为节点i的破坏代价,$c(i,j)$为链路(i,j)的破坏代价,S_v为S中的节点集合,S_E为S中的链路集合.

1.2 脆弱性分析方案设计

1.2.1 关键网络元素评估模型

1) 利用度中心性确定关键节点集.

节点的度中心性是指与该节点有直接联系的

节点个数. 一个节点的度数越高说明该节点与其他节点的联系越广泛. 本文分析无向网络,在无向网络图中,节点度数等于与它相连的所有节点的个数总和. 按照度值的大小将对应节点进行排序,一定程度上可以显示出节点在网络中的重要性. 本文方案关键节点集确定过程如下.

step 1: 求出网络模型G中所有节点的度数值;

step 2: 根据值由高到低对节点进行排序,得到一个节点;

step 3: 在集合中确定节点个数为x的高度数节点,组成关键节点集合,这x个节点的度数和约占所有节点度数总和的一半.

2) 利用介数中心性确定关键链路集.

介数值用于量化一个节点或链路经过最短路径桥接其他两个节点的次数,作为衡量网络元素在网络中重要性和中心性的一个关键指标,可以衡量出网络在通信过程中起传输“桥梁”作用的元素. 本文方案关键链路集确定过程如下.

step 1: 求出网络模型G中所有链路的介数值;

step 2: 根据介数值由高到低对链路进行排序,得到一个链路排序集合;

step 3: 在集合中确定链路个数为y的高介数链路组成关键链路集合,这y个链路的介数和约占所有链路介数总和的一半.

3) 确定关键元素集.

网络的关键元素集是关键节点集和关键链路集的合集,关键元素集的确定为进一步针对网络连通性的脆弱性分析提供基础.

1.2.2 破坏代价量化模型

一般情况下,在对网络进行基础防护时会根据网络元素在网络中的直观重要程度对其进行相应的保护. 因此本文认为,网络元素的破坏代价与其在网络中的直观重要性成正比. 本文方案设计中采用度中心性与介数中心性量化网络元素的破坏代价,针对节点i和链路(i,j)的量化分别如下所示:

$$c(i) = aD_G(i) + bB_G(i), \tag{5}$$

$$c(i,j) = B_G(i,j). \tag{6}$$

其中: $D_G(i)$为节点i的度中心性,以识别出网络中最具影响力的节点; $B_G(i)$和$B_G(i,j)$分别为节点i和链路(i,j)的介数中心性,以衡量出最具桥梁作用的节点和链路. $D_G(i)$和$B_G(i)$都是评估节点重要性的重要指标,因此,本文利用这两个指标共同量化节点i的重要程度,即破坏代价,并设置$a = b = 0.5$;一般情况下,链路无度中心性指标,故链路(i,j)采用介数中心性$B_G(i,j)$进行破坏代价量化.

1.2.3 算法思想与步骤

本文方案目标为站在攻击者的角度分析网络中最可能被攻击利用的脆弱元素,方案的算法整体思想分为以下4点:

1) 网络整体连通性作为脆弱性度量依据;

2) 对网络中度中心性或介数中心性值高的关键元素集S_{key}进行分析;

3) 分析结果S_{vul}是关键元素集S_{key}中破坏代价最小的一组元素集合;

4) 对S_{vul}中元素进行破坏可以使网络整体连通性降低α倍.

方案整体的算法步骤如下所示:

step 1: 输入网络图G、连通性破坏程度α;

step 2: 在G中确定由x个关键节点和y个关键链路组成的关键元素集S_{key};

step 3: 量化G中所有元素的破坏代价,构造破坏代价函数$C(S_{\text{vul}})$和连通性函数$P(G\backslash S_{\text{vul}})$;

step 4: 识别关键元素集合S_{key}中达到破坏程度α且破坏代价最小的一组集合,若破坏代价相同则选择破坏程度更大的一组元素集合;

step 5: 得到脆弱元素集合S_{vul}并输出结果.

step 2中的变量x和变量y的值的确定如第1.2.1节中介绍所示.

2 仿真结果与性能分析

接下来对本文方案进行有效性验证,并与传统脆弱性分析方法进行性能对比. 选定的对比方案有两个,分别为基于度中心性的脆弱性分析方法(ND)和基于介数中心性的脆弱性分析方法(NB)[5-6]. 本文对比分析的目标是在对网络连通性(计算方法如式(1)所示)一定的破坏程度下,验证与对比方案相比,本文NLC-C方案分析结果是否更加贴近攻击者的攻击目标,也即是否为网络中极具脆弱性的、急需保护的网络元素.

2.1 理论分析

首先,对比方案是面向节点的脆弱性分析方法,忽略了关键链路的作用和脆弱性. 而本文NLC-C方案面向联合攻击场景,是对网络所有元素的脆弱性分析,使得分析更加全面.

其次,对比方案将脆弱元素单一定义为网络关键元素,并未在网络整体连通角度下进行脆弱性分析,这样的手段不能为提高网络鲁棒性的防护措施提供可靠参考. 本文方案识别关键元素中可破坏网络连通性且破坏代价最小的一组集合,这样的方案设计不

仅可识别出极易成为攻击者目标的元素,而且能够评估出极具损害性的破坏场景. 因此,本文方案对脆弱元素的定位更加准确.

最后,为了进一步验证方案有效性,本文采取一系列实验分析,在不同的网络拓扑下进行仿真,并利用仿真数据对方案性能进行验证.

2.2 仿真数据分析

本文选用真实网络和随机网络模型两种网络结构对本文NLC-C方案与对比方案进行仿真,通过仿真结果验证方案的有效性.

在真实网络中验证的指标有:1) 分析随着对网络连通性破坏程度α的增加,总破坏代价的对比;2) 分析随着对网络连通性破坏程度α的增加,脆弱元素个数的对比. 此外,为进一步验证本文方案在不同网络规模下的有效性,在随机网络模型中验证的指标有:1) 随着网络规模的增大,在对网络连通性一定的破坏程度下,总破坏代价的对比;2) 随着网络规模的增大,在对网络连通性一定破坏程度下,方案结果脆弱元素个数的对比.

以上对比指标可验证NLC-C方案分析结果是否更加贴近攻击者的目标,因为攻击者在发动攻击时,无疑会选择总破坏代价小或总元素个数少的网络元素集合进行攻击. 因此,这些对比指标可以衡量出所提出方案对网络元素进行脆弱性分析的准确程度.

2.2.1 真实网络脆弱性分析

Terrorist网络:包含62个节点和153条链路,可真实反映出参与2001年911事件的恐怖分子之间的关系[14]. 网络拓扑简化图如图1所示.

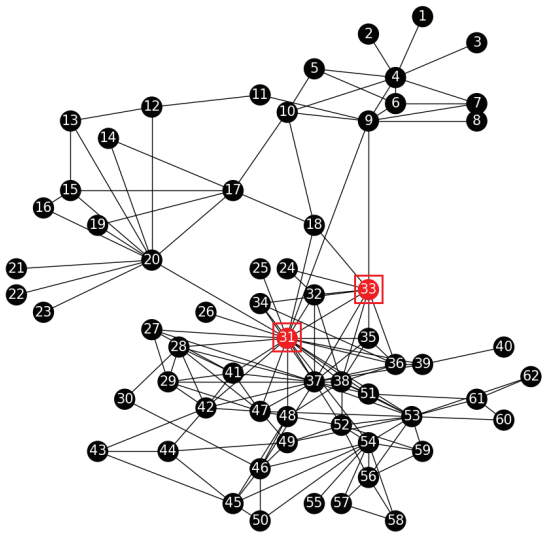

图1 Terrorist网络拓扑结构下NLC-C分析结果分布

图1中圈出的网络元素为当设定破坏程度$\alpha = 50\%$时本文方案分析得到的脆弱元素,对节点31和节点33进行攻击破坏后,网络整体变为两个不可互相通信的子网,而对比方案在破坏程度$\alpha = 50\%$下的分析结果如表1所示.

表1 $\alpha = 50\%$时对比方案分析结果

ND	[31, 37, 53, 20, 54, 4, 33]
NB	[31, 20, 9, 54, 53, 4, 37, 42, 33]

由图1和表1可以看出,与本文方案相比,对比方案需破坏更多的元素才能达到同样的破坏程度.

图2为在Terrorist网络中随着破坏程度α的增加,本文NLC-C方案与对比方案分析结果的脆弱元素个数对比图. 破坏程度α代表分析所得元素对网络整体连通性的破坏程度,由式(3)计算衡量. 此外,本文假设一个理性的网络攻击者在对网络发动攻击时,会选定对网络连通性破坏程度为50%及以上的行为进行攻击破坏,以达到摧毁网络正常通信的目的.

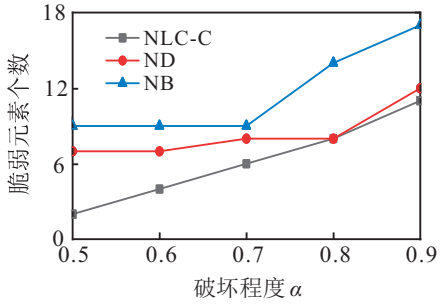

图2 Terrorist网络3种方案分析结果脆弱元素个数对比

由图2可以看出,NLC-C方案在对网络可达到的任何破坏程度下得到的脆弱元素个数都是最少的. 尤其当破坏程度$\alpha = 50\%$时,NLC-C方案分析得到的脆弱元素个数是对比方案的1/3~1/4倍左右. 这种需要破坏更少的元素便可达到同样破坏程度的攻击行为,显然更贴近攻击者的目标,因此NLC-C分析结果更具脆弱性. 此外,攻击者在发动攻击时会考虑需要付出的代价,因此分析脆弱元素的破坏代价可以衡量出更加符合攻击者目标的元素.

图3为在Terrorist网络中随着破坏程度α的增加,本文NLC-C方案与对比方案分析结果的破坏代价对比.

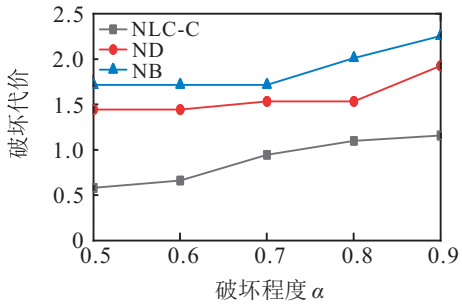

图3 Terrorist网络下3种方案分析结果破坏代价对比

由图2和图3可以看出,随着对网络连通性破坏程度的增加,NLC-C方案和两个对比方案分析得到的脆弱元素的总破坏代价或脆弱元素个数不断增加,这是因为破坏代价或脆弱元素个数与相应的网络破坏程度呈正相关.

另外,由图3可以发现,本文NLC-C方案在对网络可达到的任何破坏程度下得到的脆弱元素的破坏代价都是最小的. 尤其当破坏程度$\alpha = 50\%$时,NLC-C方案结果的破坏代价是对比方案的1/3倍左右,且$\alpha = 50\%$时得到的脆弱元素可以被看作网络中最容易遭受攻击的部分. 在攻击者发动攻击时,会同时考虑对网络破坏程度和相应的需要付出的代价,然后在其二者之间取一个折中,选定破坏程度为50%不仅可以破坏网络中大约一半的网络连接,而且不必付出较大的破坏代价.

综上分析可以得出,与对比方案相比,本文方案结果更加接近攻击者的攻击意愿,即更加脆弱.

2.2.2　NW小世界网络脆弱性分析

研究者们发现,实际网络有一定的小世界网络特性,常常是鲁棒且脆弱的[15]. 实际的社会、生态等网络都是小世界网络,所以对NW小世界网络模型生成的网络进行脆弱性分析,具有极高的理论价值和研究意义.

为了进一步验证本文方案在不同网络规模下的有效性,本文在具有一定实际规律的网络模型下对方案进行仿真验证,由第2.2.1节分析可以得出破坏程度$\alpha = 50\%$是攻击者最可能发动的一种攻击,因此,本节在验证不同网络规模对方案分析结果的影响程度时,设定连通性破坏程度为$\alpha = 50\%$,并通过多次实验仿真取平均得到对比图所示数据.

图4为在NW小世界网络中当连通性破坏程度$\alpha = 50\%$时,随着网络规模的增大,本文方案与对比方案分析结果的脆弱元素个数对比图.

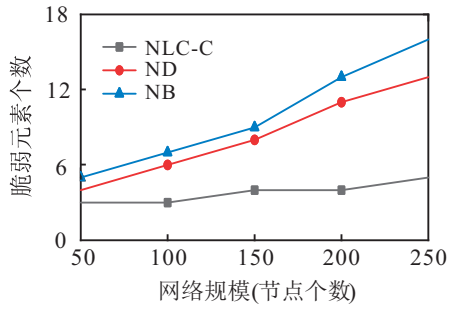

图4　NW小世界网络下3种方案结果脆弱元素个数对比

由图4可以看出,当对网络破坏程度为$\alpha = 50\%$时,本文NLC-C方案在任何网络规模下得到脆弱元素个数都是最少的,且网络规模越大,本文方案的优势越明显. 此外,本文方案分析结果受网络规模影响较小,在节点个数为250的网络规模下,本文方案在连通性破坏程度为$\alpha = 50\%$时分析得到的元素个数为5,是对比方案的1/3～1/4,更加说明本文方案分析结果是网络中极具脆弱的元素.

图5为在NW小世界网络中当连通性破坏程度$\alpha = 50\%$时,随着网络规模的增大,本文方案与对比方案分析结果总破坏代价的对比图.

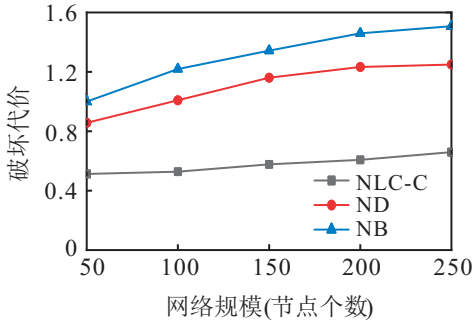

图5　NW小世界网络下3种方案结果破坏代价对比

由图5可看出,当对网络破坏程度为$\alpha = 50\%$时,本文NLC-C方案在任何网络规模下得到脆弱元素的总破坏代价都是最小的. 当在节点总数为50的网络规模下,NLC-C方案分析结果的破坏代价是对比方案的1/2～1/3,且网络规模越大,本文方案的优势越明显. 因此,NLC-C方案分析结果更具脆弱性.

综上分析可以得出,与对比方案相比,本文NLC-C方案分析结果的脆弱元素个数更少、元素破坏代价更小,且这些元素遭受破坏时对网络的损害程度更大,因此极易成为攻击者的目标,对其进行加强保护具有极为重要的现实意义.

2.3　方案复杂度分析

本文通过算法分析时间来有效反映方案复杂度,同样在Terrorist网络和NW小世界网络中进行仿真验证. 图6为在Terrorist网络中随着破坏程度$\alpha = 50\%$的增加,本文NLC-C方案与对比方案算法分析时间对比图. 图7为在NW小世界网络中当连通性破坏程度随着网络规模增大时,本文方案与对比方案算法分析时间对比图.

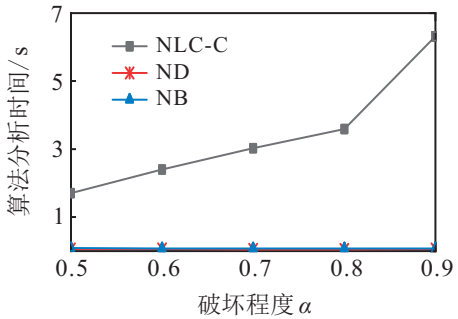

图6　Terrorist网络下3种方案算法分析时间对比

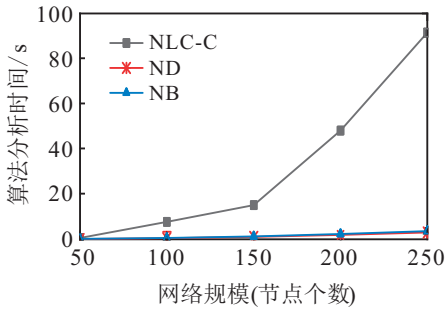

图 7 NW小世界网络下3种方案算法分析时间对比

由图6和图7可以看出,本文NLC-C方案分析时间高于对比分析方案,引发这种结果的因素之一是对比方案ND和NB只是针对网络节点进行脆弱性分析,而NLC-C方案是针对节点和链路联合攻击场景并面向网络中所有元素进行的设计与分析.该方案能够保证分析的全面性,但与此同时,分析元素数量的增多导致算法分析复杂度和分析时间都有所增加.

3 结 论

本文针对现有脆弱性分析中面向节点和链路联合攻击场景的研究较少且脆弱元素定位依据单一的研究现状,提出联合攻击下一种面向网络连通性的关键网络元素脆弱性分析方法,使其更加适用于当今复杂且多元化的网络分析.

本文所提出NLC-C方案重点实现脆弱元素的多重定位,将脆弱元素定义为既是网络中的关键元素,又是可导致网络整体连通性特定降级的元素,更是一定破坏程度下关键元素集合中破坏代价最小一组元素,这样的网络元素既重要又脆弱,极易成为攻击者的目标,若遭受破坏将会造成巨大的损失,对其进行分析识别,从而制定相应的保护措施尤为重要.仿真结果表明,本文方案较为准确地识别出网络中极易被攻击者攻击利用的脆弱元素,可为相应保护措施的制定提供良好的参考.

值得注意的是,本文方案在保证分析更加全面、分析结果更贴近攻击者目标的基础上增大了算法复杂度,增加了方案分析时间,尤其对于大规模网络分析.针对这一问题,引出本文的下步研究计划,即在保证分析全面的基础上降低算法复杂度.

参考文献(References)

[1] 于宝, 冯春, 朱倩, 等. 中国高速铁路网络脆弱性分析[J]. 中国安全科学学报, 2017, 27(9): 110-115.
(Yu B, Feng C, Zhu Q, et al. Vulnerability analysis of China's high speed railway network[J]. China Safety Science Journal, 2017, 27(9): 110-115.)

[2] Yu Y, Guo L, Huang J, et al. A cross-layer security monitoring selection algorithm based on traffic prediction[J]. IEEE Access, 2018, 6: 35382-35391.

[3] Yu Y, Guo L, Liu Y, et al. An efficient SDN-based DDoS attack detection and rapid response platform in vehicular networks[J]. IEEE Access, 2011, 6: 44570-44579.

[4] Yu Y, Ning Z, Guo L. A secure routing scheme based on social network analysis in wireless mesh networks[J]. Science China Information Sciences, 2016, 59(12): 143-154.

[5] Borgatti S P, Everett M G. A graph-theoretic perspective on centrality[J]. Social Networks, 2006,28(4): 466-484.

[6] 蒋一森. 基于结构中心性的航路网络关键节点识别[J]. 计算机与现代化, 2018(7): 108-113.
(Jiang Y S. Key node identification of navigation network based on structural centrality[J]. Computer and Modernization, 2018(7): 108-113.)

[7] Yu Y, Peng Y, Yu Y, et al. A new dynamic hierarchical reputation evaluation scheme for hybrid wireless mesh networks[J]. Computers & Electrical Engineering, 2014, 40(2): 663-672.

[8] Reggiani A, Nijkamp P, Lanzi D. Transport resilience and vulnerability: The role of connectivity[J]. Transportation Research Part A, 2015, 81: 4-15.

[9] Dinh T N, Xuan Y, Thai M T, et al. On new approaches of assessing network vulnerability: Hardness and approximation[J]. IEEE/ACM Transactions on Networking, 2012, 20(2): 609-619.

[10] Shen Y, Nguyen N P, Xuan Y, et al. On the discovery of critical links and nodes for assessing network vulnerability[J]. IEEE/ACM Transactions on Networking, 2013, 21(3): 963-973.

[11] Shen Y, Dinh T N, Thai M T. Adaptive algorithms for detecting critical links and nodes in dynamic networks[C]. MILCOM. Orlando: IEEE, 2012: 1-6.

[12] Bell M G H, Kurauchi F, Perera S, et al. Investigating transport network vulnerability by capacity weighted spectral analysis[J]. Transportation Research Part B Methodological, 2017, 99: 251-266.

[13] Dinh T N, Thai M T. Network under joint node and link attacks: Vulnerability assessment methods and analysis[J]. IEEE/ACM Transactions on Networking, 2015, 23(3): 1001-1011.

[14] Krebs V. Uncloaking terrorist networks[J]. First Monday, 2002, 7(4): 1-4.

[15] Doyle J C, Alderson D L, Li L, et al. The "robust yet fragile" nature of the internet[J]. Proceedings of the National Academy of Sciences of the United States of America, 2005, 102(41): 14497-14502.

作者简介

刘树美(1992–), 女, 博士生, 从事网络脆弱性分析的研究, E-mail: liusmneu@163.com;

于尧(1982–), 女, 副教授, 博士, 从事网络安全等研究, E-mail: yuyao@mail.neu.edu.cn;

郭磊(1980–), 男, 教授, 博士生导师, 从事网络安全、网络优化等研究, E-mail: haveball@gmail.com.

(责任编辑: 孙艺红)