网络安全事件危害度的量化评估

何 慧，张宏莉，王 星，曲晶莹

（哈尔滨工业大学 计算机科学与技术学院，150001 哈尔滨）

摘 要：为评价安全事件造成的危害程度，从网络系统可用性的角度出发提出基于性能指标的网络安全事件危害度量化评估方法.选取路由器节点与链路等网络底层关键组成部分的性能评价指标，利用网络熵值量化描述网络底层性能属性，用网络熵值在安全事件攻击前后的变化来度量攻击对网络可用性的影响程度.搭建了大规模网络蠕虫攻击事件模拟试验平台，采用省级节点的实际网络环境进行验证.实验结果表明，在攻击发生时，选取的底层性能指标能有效反映网络的危害程度，省级节点实验更一步验证该方法能有效地应用于大规模网络可用性量化评估中.

关键词：网络安全；网络可用性；信息熵；量化评估；性能指标

中图分类号：TP393.4；TP309.5 **文献标志码**：A **文章编号**：0367－6234(2012)05－0066－05

Detriment quantitative assessment of the network security incidents

HE Hui, ZHANG Hong-li, WANG Xing, QU Jing-ying

(School of Computer Science and Technology, Harbin Institute of Technology, 150001 Harbin, China)

Abstract: From the point of view on the network system availability, to evaluate the harm caused by security incidents, a performance－based quantification assessment method of network security is proposed. The method references the concept of entropy in information theory to quantify the performance indexes by choosing router nodes, and compares these index changes in the entropy before and after the security incident to measure the impact on the network. Worm simulation and actual provincial nodes experiment show that the proposed approach can be effectively applied to the quantification assessment of large-scale network availability.

Key words: network security; network availability; entropy in information theory; quantification assessment; performance index

随着近年来攻击行为及网络入侵的复杂化、分布化、大规模化、趋利化和严密化[1]，互联网络在全球范围内遭受着愈加频繁的攻击，经常导致网络大面积瘫痪，重要的信息系统安全受到严重威胁，造成巨大经济损失和不良社会影响，甚至危及到国家的安全和社会的稳定.因此，对网络攻击后的整体危害度的评价已经成为网络安全领域重要的研究课题之一[2]. 目前，安全性量化评估方法主要集中于主机系统与网络系统的脆弱性等风险评估上[3]. 而大规模网络攻击通常选择性能（如带宽和延迟）较好的链路传播. 例如：Slammer蠕虫以带宽优先的原则来选路传播，而其他一些蠕虫（如红色代码）是延迟趋向传播[4]. 因此，分析网络攻击传播时考虑链路及节点性能因素，对于其传播路径的选择、传播速度的了解以及攻击损害程度的评价等方面都具有重要价值.

本文提出面向网络可用性的大规模网络安全事件危害度量化评估方法. 用网络熵值描述安全性能，用熵的差值来度量性能变化. 本文考虑底层基础网络构成，分析受影响的节点、链路以及事件情况，根据网络攻击发生后对节点和链路性能指标的影响，综合节点和链路的危害度及重要程度等参数，得出整个网络的疫情危害程度评估模型.

收稿日期：2011－06－30.

基金项目：国家重点基础研究发展规划资助项目(2011CB302605)；国家高技术研究发展计划资助项目(2010AA012504, 2011AA010705)；国家自然科学基金资助项目(60903166, 61173145).

作者简介：何 慧(1974—)，女，博士，副教授；
张宏莉(1973—)，女，教授，博士生导师.

通信作者：何 慧，hehui@hit.edu.cn.

将采用模拟和真实两种实验环境,验证不同网络规模环境下评估结果的有效性.

1　安全事件危害程度评估框架

目前,互联网上爆发的比较典型的网络安全事件有僵尸网络、拒绝服务攻击、蠕虫等[5]. 本文主要针对大规模网络、破坏性强以及易于传播的网络安全事件进行危害程度的评价. 此类网络安全事件往往具有动态发展的性质,依赖于网络底层的连接状况及特点,比如路由器与链路的分布情况. 主要影响网络安全属性[6]中的可用性.

本文考虑底层基础网络的构成情况,分析受影响的节点、链路和事件情况,根据节点所充当的角色类型,即主机节点、服务器节点及负责网络数据转发的路由器节点(此处选择路由节点),根据网络事件发生后对链路带宽以及吞吐量等性能指标的影响,综合节点和链路的危害度及重要程度等参数,得出整个网络的疫情危害程度评估框架. 如图 1 所示,采用细粒度的层次化的评估方法,分成 4 个层面,从底层指标向上逐层计算危害度的指数,最终计算出整个网络的危害度值.

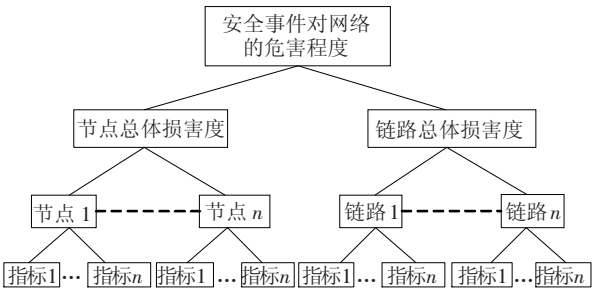


图 1　危害程度评估框架图

2　网络攻击危害程度评价指标计算

2.1　评价指标选择

2.1.1　节点指标选择

针对路由器节点的性能,选择指标包括:丢包率、延迟以及节点吞吐量,这几个参数将直接反映路由节点在遭受攻击情况下的性能状况.

由于此类网络攻击会引起网络拥塞,拥塞到一定程度,即攻击程度达到一定规模,就会造成数据包的丢失,而且随着攻击强度的增强,丢包率亦会增高[7]. 进行路由节点丢包率的计算,其定义为单位时间内,流经节点被丢掉数据包数与所发送过来数据包总数之比:

$$V_{\text{droprate}}(x) = \sum_{i=1}^{n} V_{\text{OutDiscards}} / \sum_{i=1}^{n} V_{\text{OutPkts}}.$$

其中:$V_{\text{droprate}}(x)$ 指 x 路由器的丢包率;n 表示此路由器同 n 个接口相连接;$\sum_{i=1}^{n} V_{\text{OutDiscards}}$ 指路由器接口单位时间内所丢弃的数据包数;$\sum_{i=1}^{n} V_{\text{OutPkts}}$ 指本连接的接口单位时间内传送过来数据包总数.

同样,此类网络攻击亦会影响到路由器节点的吞吐量参数,当攻击大规模爆发时会使得节点的吞吐能力降低[8]. 所以,此处选取路由节点吞吐量为危害度的度量参数之一,定义为路由器各端口上在单位时间内传输正常数据包的总量. 计算公式如下所示:

$$V_{\text{throughput}}(x) = \sum_{j=1}^{n} (\Delta V_{\text{InOctets}} + \Delta V_{\text{OutOctets}}) / \Delta t.$$

式中,$V_{\text{throughput}}(x)$ 指第 x 路由器节点吞吐量,$\Delta V_{\text{InOctets}}$ 指 Δt 时间段内流入 j 端口字节数,$\Delta V_{\text{OutOctets}}$ 指流出 j 端口字节数,Δt 指对应某时间区域,n 表示此路由器同 n 个接口相连接.

另外,此类网络攻击发生时,最明显的变化就是用户在传送数据时的等待时间长,即延迟. 当攻击爆发时,会明显感觉到网络报文传递的时间变长,即延迟参数值增大. 节点延迟是由传输延迟、排队延迟、处理延迟和传播延迟构成. 本文采用经典的计算方法[9],即表示为数据包流入前后相邻路由器间的 RTT 差值.

2.1.2　链路指标选择

在此类网络攻击发生时,链路必然亦会受到影响,表现为链路的吞吐量降低,甚至到阻塞的程度. 选取链路的吞吐量为度量参数之一,链路是全双工的,是双向传送数据,因此,链路上吞吐量定义为单位时间内双向传输的正常报文量总数,计算公式如下:

$$V_{\text{throuthput}}(x) = (V_{\text{InOctets}} + V_{\text{OutOctets}}) / \Delta t.$$

式中,$V_{\text{throuthput}}(x)$ 指第 x 条链路的吞吐量,V_{InOctets} 指 Δt 时间段内流入字节数,$V_{\text{OutOctets}}$ 指 Δt 时间段内流出字节数,Δt 指对应的某时间段.

当攻击爆发时,反映链路性能明显变化的另一参数是链路的可用带宽. 随着攻击发生强度的增大,会导致入侵流量占用的可用带宽增加,使正常的网络带宽下降,甚至无法进行正常的网络访问,网络濒临瘫痪. 选取链路带宽占用率为评价参数之一,定义为某链路在单位时间内可使用的网络容量与链路固有带宽的比值:

$$V_{\text{used}}(x,k) = [V_{\text{B}}(x,k) / T_k] / V_{\text{B}}.$$

式中,$V_{\text{used}}(x,k)$ 指第 x 链路在第 k 采样时间间隔内的带宽占用率,$V_{\text{B}}(x,k)$ 指第 x 链路在第 k 采样时间间隔内传输的数据总量,T_k 指第 k 采样时间

间隔的长度，V_B 指第 x 链路的链路固有容量 —— 带宽.

2.2 攻击损害程度量化

根据指标的正负向属性[10]，对其进行无量纲化处理. 即吞吐量属于正向性的指标，值越大越好，而丢包率、带宽占用率以及延迟等属于负向性的指标. 由此可得网络系统的各性能指标的量化值，并把攻击事件发生前后指标的对比差值作为安全事件损害状况的测度.

2.2.1 节点危害度计算

根据选取的节点性能指标参数进一步定义单节点危害度计算方法，单节点危害度为此节点每个单项性能指标的危害度加权平均：

$$V_{\text{damageN}}(n_i) = \sum_{j=1}^{m} V_{\text{D}_j} * V_{w_j} / \sum_{j=1}^{m} V_{w_j}. \quad (1)$$

式中，$V_{\text{damageN}}(n_i)$ 指第 i 路由器节点 n_i 的危害度，V_{D_j} 指节点 n_i 第 j 个指标的危害度，V_{w_j} 指节点 n_i 第 j 个指标权重，m 指节点 n_i 指标总数.

基于以上单节点的计算方法，推出整体网络的危害度计算公式. 网络中节点整体危害度定义为此网络所有节点危害度加权平均：

$$V_{\text{damageA}}(N) = \sum_{k=1}^{m} V_{\text{damageN}}(n_k) * V_{w_k} / \sum_{k=1}^{m} V_{w_k}.$$

其中，$V_{\text{damageA}}(N)$ 指网络节点整体危害度，$V_{\text{damageN}}(n_k)$ 指第 k 路由器节点 n_k 的危害度，V_{w_k} 指第 k 路由器节点 n_k 的权重，m 指节点总数.

2.2.2 链路危害度计算

单链路危害度定义为与此链路相关各单项指标危害度加权平均.

$$V_{\text{damageE}}(e_i) = \sum_{j=1}^{m} V_{\text{D}_j} * V_{w_j} / \sum_{j=1}^{m} V_{w_j}. \quad (2)$$

其中，$V_{\text{damageE}}(e_i)$ 指第 i 条链路 e_i 危害度，V_{D_j} 指链路 e_i 第 j 指标的危害度，V_{w_j} 指链路 e_i 第 j 指标权重，m 指链路 e_i 指标总数.

基于以上单链路危害度的计算方法，推出整体网络的链路危害度计算公式. 网络中链路整体危害度定义为网络中所有链路的危害度加权平均：

$$V_{\text{damageA}}(E) = \sum_{k=1}^{m} V_{\text{damageE}}(e_k) * V_{w_k} / \sum_{k=1}^{m} V_{w_k}.$$

其中，$V_{\text{damageA}}(E)$ 指整体网络的链路危害度，$V_{\text{damageE}}(e_k)$ 指第 k 链路 e_k 的危害度，V_{w_k} 指第 k 链路 e_k 的权重，m 指链路总数.

2.3 危害程度度量

对已确定的评价指标，做无量纲化和指标归一化处理，并根据作用程度确定每个指标权重，然后计算其网络熵值，从而进一步得到主要链路和路由器的危害度，再根据节点和链路的作用级别赋予对应权重，最后计算出整体网络链路和路由器的危害度.

设定 ΔH 是链路和路由节点的攻击发生前后相关指标熵值差. 差值的大小，直接反映出网络攻击的效果如何，比值越大，说明性能受到的影响越大，遭到的攻击损害越严重. 本文用 ΔH 值来定量评价网络攻击的危害程度，并对网络危害程度进行分级描述（共分六个等级）[11]. 本文进行归一化处理后得到分级见表 1.

表 1 网络危害程度分级描述

危害度	性能指标下降/%	描述
低于 0.01	5	几乎没有
0.01 ~ <0.04	<20	轻微
0.04 ~ <0.16	<50	中等
0.16 ~ <0.27	<70	较严重
0.27 ~ <0.52	<90	严重
0.52 ~ <1.00	≥90	网络几乎瘫痪

3 模拟实验与结果分析

3.1 模拟实验环境设置

3.1.1 路由拓扑模拟

利用 GTNetS 模拟器[12]生成了层次化的实验拓扑，如图 2 所示为自治域之间和路由器节点之间的连接关系图[13]，由 5 个 AS 自治域构成，路由器节点达 1 百多个，网络端节点为 1 万个.

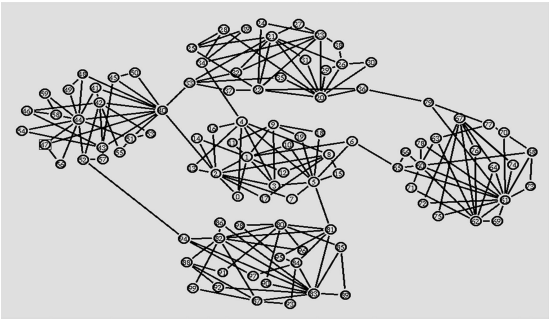


图 2 GTNetS 生成的路由器节点拓扑图

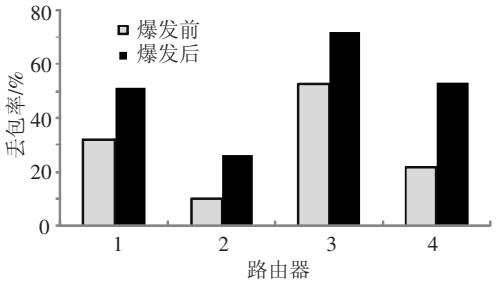
3.1.2 背景流量模拟

流量试验平台采用文献[14]中的自相似流量生成方法，网络背景流量满足伪 Pareto 分布，基于 ON/OFF 的源叠加方式，生成 TCP 流量和 UDP 流量. 实验中采用大小相同的 TCP、UDP 数据包作为发送端，包大小为 550 Byte，其反馈流量的数据包为 64 Byte. 每个 ON/OFF 发送源均满足同一重尾分布特性，分布参数为 $\alpha_{\text{ON}} = 1.5$ 和 $\alpha_{\text{OFF}} = 1.1$. 构造出传输层的基于 ON/OFF 源的发生器以及流量接收端.

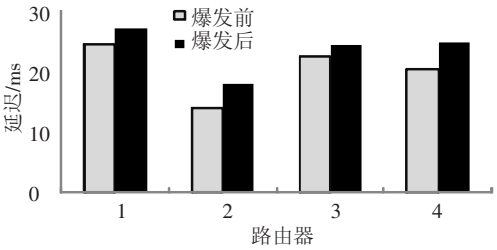
3.2　爆发攻击前后对比实验

实验中模拟 UDP 蠕虫攻击流量,采用 SI 经典传播模型. 被感染主机初始时刻的数量为 1,随机扫描方式,数据包为固定大小(460 Byte),扫描包速率为 10/s. 蠕虫攻击发生时,网络流量由正常流量与蠕虫攻击流量构成. 实验中通过计算路由器节点的延迟和丢包率来度量网络节点的性能情况. 而对于网络链路则通过带宽占用率和链路吞吐量两个指标来衡量.

计算路由器节点性能:分别计算出蠕虫攻击前后路由器节点的丢包率和延迟指标值的变化,图 3 为模拟试验中的 4 个路由器的性能指标比对结果,可见,攻击前后的性能指标结果显著反映出攻击的影响.



(a)丢包率



(b)延迟

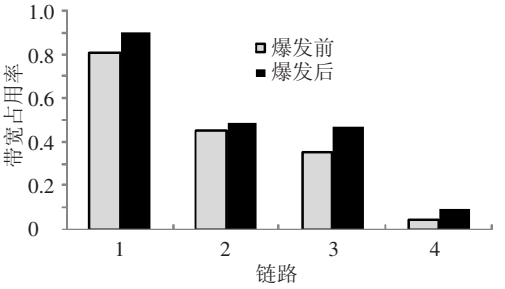
图 3　蠕虫攻击前后路由器性能对比

计算链路性能:分别计算出蠕虫攻击前后链路带宽占用与平均吞吐量性能指标变化. 图 4 为模拟试验中的路由器链路间的性能比对结果. 链路带宽占用和平均吞吐率都会受到一定的影响.

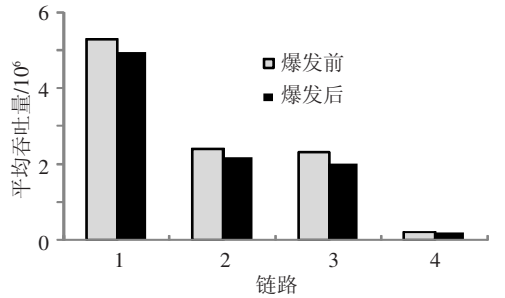
3.3　计算网络危害度

采用本文方法分别计算模拟网络实验中的路由器节点和链路的危害度. 首先,计算路由器节点的危害度,根据各路由器在每个性能指标上的危害度值和指标所占权重来统一计算单一节点的危害度. 表 2 为实验中主要路由器各项指标上的危害度值.

试验中假定指标相互独立,由此暂设定指标权重相同为 1. 根据式(1),先计算单一路由节点的危害度,然后,根据节点不同的权重,计算网络整体节点危害度. 计算得到整体实验网络的路由器危害度值是 0. 2. 对照危害程度分级,此次蠕虫攻击对整体路由器危害程度是较严重的. 同时,亦可定位出攻击后受影响最大的路由器节点.



(a) 带宽



(b) 吞吐率

图 4　蠕虫攻击前后链路性能对比

表 2　路由器节点各指标危害度

路由节点	延迟	丢包率	权值
R94	0. 022	0. 187	0. 139 9
R82	0. 169	0. 093	0. 123 2
R67	0. 228	0. 109	0. 027 4
R52	0. 044	0. 174	0. 143 4
R40	0. 152	0. 031	0. 394 6
R23	0. 229	0. 284	0. 025 0
R12	0. 029	0. 059	0. 025 0
R0	0. 127	0. 063	0. 033 6

试验中,根据式(2),根据各链路在每个性能指标上的危害度值和指标所占权重来统一计算单一链路的危害度. 表 3 所示为实验中主要链路在各指标上的危害度值及其权重.

表 3　链路危害程度

链路	带宽占用率	平均吞吐量	链路权重
R2 < - > R16	0. 023	0. 158	0. 019 0
R21 < - > R20	0. 157	0. 131	0. 109 4
R20 < - > R29	0. 135	0. 025	0. 054 2
R21 < - > R33	0. 423	0. 168	0. 250 2
R40 < - > R45	0. 027	0. 118	0. 052 5
R42 < - > R52	0. 119	0. 093	0. 121 0
R36 < - > R79	0. 018	0. 146	0. 239 4
R82 < - > R81	0. 100	0. 159	0. 154 3

假定指标权重相同,值取 1,根据式(2),在计算单链路危害度之后,根据链路的不同权重,计算

整体网络链路的危害度. 计算得到实验网络整体链路危害度值为0.023. 对照危害程度分级,此次蠕虫攻击对整体链路危害程度是轻微的. 同时,亦可定位出攻击后受影响的最大链路,以便有针对的加以控制.

在校网络中心出入口入侵监测报警库中随机抽取某天的异常事件,同时根据主要楼宇路由器及楼层交换机拓扑连接链路,对相关数据进行采集,用本文方法计算出相应时段网络安全危害度量值,并且平滑其结果,得到其24 h的可用性危害趋势如图5.

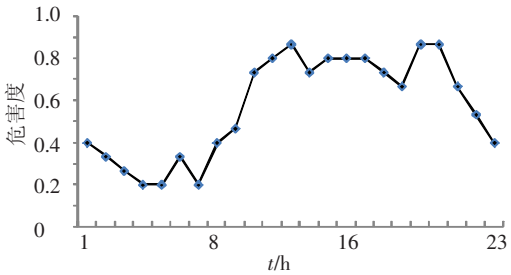


图5 某天网络可用性危害示意图

从图5可发现校园网可用性危害状态,10~22点,网络整体危害指数明显高于其他时段,而10~12点、19~22点两时段为全天最高峰,网络管理员应该高度重视此时段,实验结果与网络日志以及网络当时的实际的安全状况相符. 区别于定性和局部的分析,本文更能够给出方法可靠的量化依据,从而可从网络通讯的底层综合要素来综合发现问题,防止大规模攻击在网络中的泛滥,并可有效定位到具体的链接和传播节点,对进一步的控制提供更有利的依据.

4 结 论

1)本文提出了面向网络可用性的大规模安全事件危害程度量化评估方法. 用网络熵值描述安全性能,用熵的差值来度量性能变化.

2)考虑底层基础网络的构成情况,分析受影响的节点、链路以及事件情况,根据网络事件发生后对节点和链路性能指标的影响,综合节点和链路的危害度及重要程度等参数,得出整个网络的疫情危害程度评估模型. 采用层次化的评估框架,从底层微观细粒度指标逐层向上计算危害度值,最终计算出宏观的整体网络危害度的值.

3)从模拟和真实两种环境下进行了实验. 通过搭建的大规模网络安全事件模拟平台验证了较大网络下的评估方法的有效性. 在中小型的校园网络的实际环境下,通过网管获取的真实数据,进一步证明了量化结果的正确性.

参考文献:

[1] 冯登国, 张阳, 张玉清. 信息安全风险评估综述[J]. 通信学报, 2004, 25(7):10-18.

[2] RITCHEY R, AMMANN P. Using model checking to analyze network vulnerabilities[C]//Proceedings of the IEEE Symp on Security and Privacy. Berkeley: IEEE Computer Society Press, 2000:156-165.

[3] 邢栩嘉, 林闯, 蒋屹新. 计算机系统脆弱性评估研究[J]. 计算机学报, 2004, 1(1): 1-10.

[4] ZOU C C, TOWSLEY D, GONG Weibo. Modeling and simulation study of the propagation and defense of internet E-mail worms[J]. IEEE Transactions on dependable and Secure Computing, 2007, 4(2):115-120.

[5] CLARK K, TYREE S, DAWKINS J, *et al*. Qualitative and quantitative analytical techniques for network security assessment[C]//Proceedings of the 2004 IEEE Workshop on Information Assurance and Security. NY: IEEE Computer Society Aress, 2004:10-11.

[6] 马洪梅. 基于流量特征的网络可用性量化评估与控制[D]. 哈尔滨:哈尔滨工业大学, 2010: 23-27.

[7] CARDOSO R C, FREIRE M M. Intelligent assessment of distributed security in TCP/IP networks[C]//Proceedings of 7th IEEE International Conference on High Speed Networks and Multimedia Communications. LNCS, Toulouse: Spinger-verlay, 2004:1092-1099.

[8] LAKHINA A, CROVELLA M, DIOT C. Mining anomalies using traffic feature distributions[C]//Proceedings of the ACM SIGCOMM. NY: ACM Press, 2005:225-231.

[9] JAJODIA S, NOEL S, O'BERRY B. Managing Cyber Threats: Approaches and Challenges[M]. NY: Springer-Verlag, 2005:247-266.

[10] 曲晶莹. 基于模拟的网络安全事件危害程度评估研究[D]. 哈尔滨: 哈尔滨工业大学硕士论文, 2008: 12-19.

[11] 张义荣,鲜明,王国玉. 一种基于网络熵的计算机网络攻击效果定量评估方法[J]. 通信学报, 2004,25(11):158-165.

[12] RILEY G F. The Georgia Tech Network Simulator[C]//Proceedings of the ACM SIGCOMM Workshop on Models, Methods and Tools for Reproducible Network Research. [S.l.]: ACM Press, 2003: 5-12.

[13] HUANG Lin. Survey on Generators for Internet Topologies at the AS Level[D]. Karlsruhe: University Karlsruhe, 2007:7-9.

[14] KRAMER G, MUKHERJEE B, PESAVENTO G. IPACT: A dynamic protocol for an ethernet PON (EPON)[J]. IEEE Communications Magazine, 2002, 40(2): 190-192.

(**编辑** 杨 波)