软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2015,26(7):1742−1756 [doi: 10.13328/j.cnki.jos.004673]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

一种基于多属性决策的 DDoS 防护措施遴选方法*

黄 亮[1], 冯登国[1], 连一峰[1], 陈 恺[2], 张颖君[1], 刘玉岭[1]

[1](中国科学院 软件研究所 可信计算与信息保障实验室,北京 100190)

[2](中国科学院 信息工程研究所,北京 100195)

通讯作者: 黄亮, E-mail: lancerhuang@tca.iscas.ac.cn

摘 要: DDoS攻击是网络中最大的威胁之一,选取合适的防护措施,能够更加有效地保护目标网络和目标系统.现有的评价方法对于防护措施选择的指导性不足.针对该问题,首先构建了面向 DDoS 攻击的防护措施遴选模型(DCSM).在此基础之上,提出基于多属性决策的 DDoS 防护措施遴选算法.以多属性决策方法综合考虑各方面评估指标;从攻防两方面,以基于历史攻击偏好的方法和熵权法计算重要性权重,消除了传统评价方法中人为指定权重带来的主观性影响.提出的方法为防护措施的选择提供了参考,并通过模拟实验验证了方法的适用性和有效性.

关键词: 多属性决策;DDoS;安全防护;措施遴选;安全评估

中图法分类号: TP393

中文引用格式: 黄亮,冯登国,连一峰,陈恺,张颖君,刘玉岭.一种基于多属性决策的 DDoS 攻击防护措施遴选方法.软件学报, 2015,26(7):1742−1756. http://www.jos.org.cn/1000-9825/4673.htm

英文引用格式: Huang L, Feng DG, Lian YF, Chen K, Zhang YJ, Liu YL. Method of DDoS countermeasure selection based on multi-attribute decision making. Ruan Jian Xue Bao/Journal of Software, 2015,26(7):1742−1756 (in Chinese). http://www.jos.org.cn/1000-9825/4673.htm

Method of DDoS Countermeasure Selection Based on Multi-Attribute Decision Making

HUANG Liang[1], FENG Deng-Guo[1], LIAN Yi-Feng[1], CHEN Kai[2], ZHANG Ying-Jun[1], LIU Yu-Ling[1]

[1](Trusted Computing and Information Assurance Laboratory, Institute of Software, The Chinese Academy of Sciences, Beijing 100190, China)

[2](Institute of Information Engineering, The Chinese Academy of Sciences, Beijing 100195, China)

Abstract: DDoS is one of the biggest threat in the network. Using the proper countermeasure will notably improve the security level of the target network and/or target system. Existing security evaluation methods don't provide sufficient support for countermeasure selection. To solve the problem, this paper builds a DDoS countermeasure selection model (DCSM), and then proposes the DDoS countermeasure selection method. The method not only takes advantage of multi-attribute decision making theory to evaluate multi-dimension metrics, but also uses historical attack preference based method and entropy method to calculate the weight from both attack and defense perspectives, thus reducing the subjective factors in conventional methods. The correctness and the applicability of the method are validated by the experiments.

Key words: multi-attribute decision making; DDoS; security countermeasure; countermeasure selection; security evaluation

自诞生之日起,计算机网络一直在不断地发展,其规模在不断扩大,应用也愈加广泛.在给人们带来便利的同时,计算机网络也存在着众多的安全威胁,分布式拒绝服务攻击(distributed denial of service,简称 DDoS)是其中一种主要的、影响范围广、危害性大的恶意行为.2012 年 4 月 10 日,韩国中央选举管理委员会网站受到 DDoS

* 基金项目: 国家高技术研究发展计划(863)(SQ2013GX02D01211); 国家自然科学基金(61100226, 61303248); 北京市自然科学基金(4122085, 4144089); "十二五"国家科技支撑计划(2012BAK26B01)

收稿时间: 2013-10-23; 定稿时间: 2014-05-05

攻击.2012 年下半年,美国数家银行遭受 DDoS 攻击,使得网上银行及网站间歇性失去响应.2013 年 3 月 28 日,欧洲反垃圾邮件组织 Spamhaus 遭到 DDoS 攻击,随后,为其提供安全服务的 CloudFlare 也遭受到攻击,攻击流量从 10Gbps 增大到 300Gbps,对整个欧洲的网络造成了严重影响.众多网站、运营商因为 DDoS 攻击遭受严重的经济损失,而普通用户也因为 DDoS 攻击造成的网络瘫痪而受到影响.

研究人员针对 DDoS 攻击做了大量研究工作,从不同角度对不同种类的 DDoS 攻击提出了多种防护措施.不同的防护措施适用于不同的攻击方式和保护对象,在实际的网络应用环境中,需要综合考虑保护对象的特性和当前可能面临的攻击行为,选择最为适合的防护措施.针对这一问题,本文研究针对 DDoS 攻击防护措施的评价方法以指导防护措施的遴选,有效提升目标网络和目标系统的安全性.

本文针对 DDoS 攻击防护措施的选取问题,提出 DDoS 防护措施遴选模型(DDoS countermeasure selection model,简称 DCSM).该模型使用多种指标从多角度对防护措施进行评价,并引入多属性决策理论,将防护措施的遴选转化为多属性决策问题加以解决.多属性决策方法(如 TOPSIS 方法[1])的结果受评估属性的重要性权重的影响很大,而现有的重要性权重多依赖专家的主观赋值.本文结合 DDoS 攻防实际提出客观的权重赋值方法,通过分析目标系统在攻防场景下的指标,最终得到评估属性的重要性权重,避免了人为赋值带来的主观影响.具体评估方法从攻击和防护的角度分为基于历史攻击偏好的方法和熵权法两种.最后,本文对提出的方法进行了实验,验证了 DCSM 模型在选择 DDoS 防护措施时的有效性.

本文第 1 节介绍相关研究工作.第 2 节对构建的 DCSM 模型进行阐述.第 3 节描述基于多属性决策方法的 DDoS 防护措施遴选方法,详细描述重要性权重的计算方法.第 4 节通过模拟攻击场景对提出的方法进行验证.最后是全文的总结.

1 相关工作

研究人员对 DDoS 攻击和防护方法进行了大量研究.Peng 等人[2]对 DoS 和 DDoS 的防护手段进行了具体的研究,并分析了每种防护措施针对 DoS 和 DDoS 攻击的防护效果.Mirkovic 等人[3]和 Specht 等人[4]对 DDoS 的攻击措施和防护措施分别进行了分类,Mölsä[5]进一步对泛洪 DoS 攻击的防护措施效果评估指标进行了分类.

在对 DDoS 攻击防护措施进行充分研究的基础上,研究人员开始评估防护措施的效果.Butler[6]提出的 SAEM(security attribute evaluation method)评估方法首先评估每一种安全措施对所有威胁产生的总体减弱效果,然后评估每种安全措施所能应对的威胁种类,最后评估每种安全措施的实施成本.防护措施的最终选取将综合考虑这 3 方面因素.Bellaiche 等人[7]提出应从性能、部署成本、对被保护系统性能的影响和自身健壮性这 4 个方面来评估和比较防护措施.Schwab 等人[8]将 DDoS 评估指标分为 3 类:网络流量指标、攻击效果指标和防护有效性指标,认为攻击效果可以通过评估上述指标在受到攻击时的变化程度得到;防护绩效可以通过评估指定防护措施启用后增加的防护效果得到,但文献[8]并未给出具体评估方法.Meadows[9]定义了防护成本集 C 和攻击能力集 G,并在此基础上定义了容忍关系集 $C\times G$,用以分析协议能否抵御 DoS 攻击.该方法从攻防策略入手,考虑得较为全面,但是不易对结果进行量化计算,在实际应用中操作性不强.Mirkovic 等人在文献[10]中为 DDoS 的评估方法提出了一套评测标准,认为 DDoS 防护措施的核心要素在于是否能够保证合法用户仍旧享受可接受的服务.在文献[11,12]中,Mirkovic 等人进一步在 3GPP(3rd Generation Partnership Project)发布的服务质量(QoS)指标基础上提出了基于阈值的 DDoS 攻击效果评估方法.如果指标不在所属网络应用(如 Web 浏览、FTP 传输等)正常的 QoS 阈值范围内,则认为当前应用是失败的.他们以各类网络应用中失败所占的比例(percentage of failed transactions,简称 PFT)作为 DDoS 攻击效果的评估指标,以流量中各种应用的 PFT 值的加权平均结果反映 DDoS 攻击的整体效果.Li[13]等人提出了一种基于数据包计算的 DDoS 防护效果评估方法.该方法通过计算合法数据包通过率与攻击数据包通过率的比值(LAR)来评价防护系统的强弱.LAR 越高,则防护效果越好.

多属性决策的概念最早在 1944 年由 von Neumann 和 Morgenstern 以对策论的角度提出[14].截至目前,多属性决策问题已广泛存在于社会、经济等领域.在信息安全领域,多属性决策也被应用于多个方面.2001 年,Butler 在文献[1]中指出:在使用专家知识时,引入多属性决策方法可以更好地进行安全措施选择.张义荣在文献[15]中

使用层次分析法(analytic hierarchy process,简称 AHP)来确定提出的攻击效果评估方法中的指标的权重值.Zhao 在文献[16]中提出一种正规化的网络安全评估框架,使用多属性决策方法解决评估指标多、评估过程复杂等问题.Dewri 等人在文献[17]中将“在一定成本下达到最好的防护效果”转化为“最小化残留伤害和最小化安全控制成本”的多属性决策问题,并使用 NSGA-II 遗传算法加以解决.多属性决策的重要性权重将对多属性决策的结果产生很大影响,研究人员对如何更客观、有效地进行权重的赋值提出了 AHP 方法、主成分分析法、离差最大化法、均方差法等方法.本文从 DDoS 攻防实际出发,以防护措施在攻防场景中的指标作为参考,使用历史攻击偏好以及熵权法进行权重计算.

本文将多属性决策方法引入 DDoS 防护措施遴选模型,综合考虑各角度评价指标进行防护措施的最优选择.基于攻防指标进行基于重要性权重的计算,从方法上避免了多属性决策过程中由于人为指定重要性权重而引入的主观因素影响,最终提出了用于 DDoS 防护措施遴选的方法.

2 DDoS 防护措施遴选模型(DCSM)

决策问题可分为单属性决策问题和多属性决策问题.多属性决策具有两大要素:决策方案集、评估属性.决策方案集是候选决策方案的集合,评估属性是指决策过程中需要考虑的各项指标.从多个评估属性对候选决策方案进行评价,并进一步对评价结果进行综合评估,最终确定决策方案的排序.多属性决策问题广泛存在于社会、经济等领域,对它的研究已取得相应成果,并有较为成熟的解决方法.单属性决策问题只需考虑单一属性的排序,而多属性决策问题由于属性数量的增加,不同属性之间存在不可公度性及矛盾性.属性间的不可公度性是指属性间没有统一的度量标准,难以进行比较.属性间的矛盾性是指为了提升某一属性而选取某种方案,可能会使得另外一个或多个属性值不如当前方案.由于多属性决策问题需要解决不可公度性和矛盾性,使得多属性决策问题比单属性决策问题更为复杂,也使得多属性决策问题通常只能得到非劣解,而无法如单属性决策问题般得到最优解.所谓非劣解是指由于多属性决策问题中矛盾性的存在,当一个解是非劣解时,若要选择某一属性更优的解,则该解至少存在一个属性劣于原非劣解.也就是说,如果某一个解是非劣解,则不存在一个解在所有属性上都优于该非劣解.

对于 DDoS 防护措施,可以从诸如响应时间、误报率、漏报率、购买成本、维护成本等多个角度进行评价.本文将对防护措施多种角度的评价对应到多属性决策中的评估属性,将防护措施集对应到多属性决策的决策方案集,从而将 DDoS 防护措施遴选问题转化为多属性决策问题.

下面先给出相关定义,接着我们将构建 DCSM 模型.

定义 1(合法用户平均等待时间 T_{res}). 这是指在实验观测时间内,合法用户向服务器发出请求的时刻 t 和合法用户完全接收到该次请求应答数据的时刻 t'之间的时间间隔 $t'-t$ 关于合法用户的成功请求次数 n 的平均值.本文假设合法用户向服务器请求相同的文件,计算公式如下:

$$T_{res}=\frac{1}{n}\sum_{i=1}^{n}(t_i'-t_i).$$

定义 2(合法用户请求应答率 P_{res}). 这是指在实验观测时间内,合法用户成功接收到服务器响应的请求次数 $C_{Req\_Success}$ 占合法用户发出的总请求次数 C_{Req_Total} 的比值.计算公式如下:

$$P_{res}=\frac{C_{Req\_Success}}{C_{Req\_Total}}\times 100\%.$$

防护措施的目的在于削弱攻击效果,因此,用于评估攻击效果的指标亦可用于评估防护措施.DDoS 攻击对攻击目标一定范围内的主机、网络均会产生影响,受影响的指标众多,从攻击目标角度寻找指标较为繁琐.从 DDoS 攻击定义可知:无论攻击影响的范围多么广,攻击效果都会体现在用户感受中.攻击猛烈时,用户感受到请求等待的时间延长、请求得到响应的概率降低;反之,用户感受到请求等待的时间缩短、请求得到响应的概率提高.本文从用户感受角度进行指标选择,使用合法用户平均等待时间 T_{res} 和合法用户请求应答率 P_{res} 作为指标[18].

定义 3(防护措施的属性). 将使用某一防护措施进行 DDoS 攻防实验收集到的评估属性在该攻防场景中的取值称为该防护措施的属性.防护措施的属性表示多个评估属性对该防护措施多角度的评价.使用向量形式表示的防护措施的属性称为防护措施的属性向量.

防护方案是具体的防护措施,所有待选防护措施的属性构成决策矩阵.一个决策矩阵表示一个 DDoS 防护措施遴选问题.现有 n 个防护方案,则 $Defence=\{d_i|i\in[1,n]\}$ 是防护方案集合.现有评估属性集合 $Attr=\{attr_1, attr_2,\ldots,attr_m\}$,对于任意防护方案 $d_i\in Defence$,有从不同角度得到的 m 个评价结果,即 d_i 的属性为 $\{attr_{1\_i}, attr_{2\_i},\ldots,attr_{m\_i}\}$,则向量$(attr_{i1},attr_{i2},\ldots,attr_{im})$称为防护方案 d_i 的属性向量.那么根据评估属性集合 $Attr$ 收集防护方案集合 $Defence$ 中各个防护措施的属性,可以形成如下决策矩阵:

$$\begin{pmatrix} attr_{11} & attr_{12} & \cdots & attr_{1m} \\ attr_{21} & attr_{22} & \cdots & attr_{2m} \\ \vdots & \vdots & \cdots & \vdots \\ attr_{n1} & attr_{n2} & \cdots & attr_{nm} \end{pmatrix}.$$

本文中使用合法用户平均等待时间和合法用户请求应答率作为评估属性,因此,本文中的决策矩阵形如公式(1):

$$\boldsymbol{M}=\begin{pmatrix} P_1 & T_1 \\ P_2 & T_2 \\ \vdots & \vdots \\ P_n & T_n \end{pmatrix} \tag{1}$$

其中,矩阵 $\boldsymbol{M}$ 的第 i 行是防护方案 d_i 的属性向量,即(P_i,T_i).P_i,T_i 分别是防护方案 d_i 实施后的合法用户请求应答率和合法用户平均等待时间,$i\in\{1,2,3,\ldots,n\}$.

基于上述定义,本文提出一种基于多属性决策的 DDoS 防护措施遴选模型,表示如下:

$$\{Attr,Defence,\gamma,M,\omega,\rho,\boldsymbol{w},H,\varphi,Rank\},$$

其中,

1) $Attr$ 是评估属性集合.$Attr=\{attr_1,attr_2,\ldots,attr_m\}$,其中,$attr_i,i\in\{1,2,\ldots,m\}$是具体的评估属性.本文中:
$$Attr=\{\text{合法用户平均等待时间}(T_{res}),\text{合法用户请求应答率}(P_{res})\},$$
即,本文将使用合法用户平均等待时间(T_{res})和合法用户请求应答率(P_{res})对候选防护措施进行评价;
2) $Defence$ 是防护方案集合.$Defence=\{d_1,d_2,\ldots,d_n\}$,其中,$d_j,j\in\{1,2,\ldots,n\}$是具体的防护方案;
3) γ是映射关系γ:$d_j\rightarrow AVec_j$,其中,$d_j\in Defence$ 是具体的防护方案,$AVec_j$ 是 d_j 的属性向量.映射关系γ表示对根据评估属性集合 $Attr$ 产生的防护方案 d_j 进行多角度的评价,即,通过实验收集防护方案 d_j 的属性向量;
4) $\boldsymbol{M}$ 是决策矩阵. $\boldsymbol{M}=\begin{pmatrix} m_{11} & \cdots & m_{1m} \\ \vdots & \ddots & \vdots \\ m_{n1} & \cdots & m_{nm} \end{pmatrix}$,$m_{ij}$ 表示第 i 个防护方案的第 j 个评估属性的属性值.$i\in\{1,2,\ldots,n\}$,$j\in\{1,2,\ldots,m\}$.$\boldsymbol{M}$ 中第 i 行是防护方案 d_i 的属性向量,也即 $\gamma\begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_n \end{pmatrix}=\boldsymbol{M}$;
5) ω是映射关系,ω:$Attr\rightarrow\boldsymbol{w}$,表示利用熵权法,通过评估属性值计算权重向量 $\boldsymbol{w}$;
6) ρ是映射关系,ρ:$H\rightarrow\boldsymbol{w}$,表示利用历史数据,使用基于历史攻击偏好的方法计算向量 $\boldsymbol{w}$;
7) $\boldsymbol{w}$ 是重要性权重向量,表示评估属性间的重要性,与决策矩阵一起参与多属性决策过程;
8) φ是映射关系φ:$\boldsymbol{w}\times M\rightarrow Rank$,表示决策过程,即根据重要性权重向量 $\boldsymbol{w}$ 及决策矩阵 M 进行防护措施遴选,最终得到防护方案集合 $Defence$ 中防护方案的排序结果;

9) H 是历史数据,用于生成重要性权重;

10) $Rank$ 是防护方案的排序结果.$Rank=\{rank_1,rank_2,\ldots,rank_l\}$,其中,$rank_k=\{d_k,rankNo_k\}$,$k\in\{1,2,\ldots,l\}$,$d_k$ 是防护方案,$rankNo_k$ 是该防护方案经过排序之后的序号.

DCSM 模型中各个元素的关系如图 1 所示.

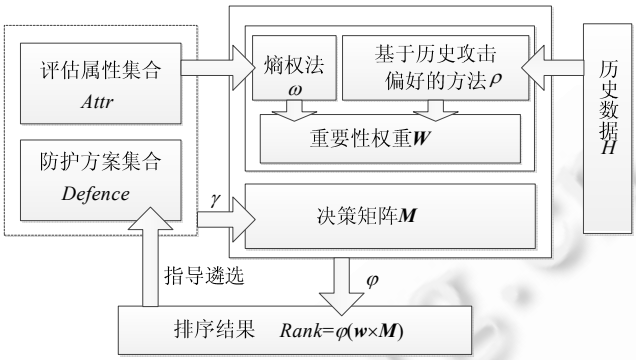

Fig.1 Relation diagram of elements in DCSM

图 1 DCSM 模型元素关系图

3 基于多属性决策的防护措施遴选算法

本节介绍 DCSM 模型框架下的基于多属性决策的 DDoS 防护措施遴选算法,首先介绍评估属性重要性权重的计算方法.评估属性的重要性权重反映了决策过程对不同属性的偏重程度,通常情况下由专家或决策者指定评估属性的重要性权值.虽然专家或决策者相对普通人更有经验,对于各评估属性具有更深的了解,但是人工赋值不可避免地会带有个人偏好,使得评估结果会受到主观影响.本文分别从攻击和防护的角度提出基于历史攻击偏好的方法和熵权法,通过分析攻防指标数据,对评估属性的重要性权重进行计算赋值.然后介绍多属性决策过程,并在最后给出基于多属性决策的防护措施遴选的算法.

3.1 基于历史攻击偏好的重要性权重计算方法

在实际场景中,由于攻击者的偏好,攻击者会倾向于使用特定的 DDoS 攻击方式.不同类型的 DDoS 攻击对各项指标的影响存在差异,因此,不同攻击者的 DDoS 攻击对目标系统的指标的影响程度各有不同.通过对历史数据的分析,发现攻击偏好,确定受影响更大的指标,从候选方案中选择能够更好地抑制该指标变化的防护措施,从而更加有针对性地对抗 DDoS 攻击,提高目标系统的安全性.

历史数据可以通过目标系统的日志获取.然而由于本文使用的是基于用户感受角度的指标,目标系统的日志中并不会对此进行记录,因此我们抽取日志可以记录的瓶颈链路带宽 BW_{thres}、请求频率 R_{att}、半开队列长度 Q_{limit} 等指标,利用神经网络的预测能力得到合法用户请求应答率 P_{res} 和合法用户平均等待时间 T_{res}.

人工神经网络是对人脑神经网络进行抽象的计算模型,具有良好的分类、识别和非线性映射等能力.神经网络包括感知器神经网络、自组织竞争神经网络、径向基函数神经网络、支持向量机等种类.在众多的神经网络中,后向传播神经网络(BP 网络)是应用最为广泛的一种.同时,理论上已经证明,具有 3 层结构的 BP 网络可以实现任意非线性映射.为了实现指标输入到攻击效果输出的映射,本文选择具有 3 层结构的 BP 神经网络对攻击效果进行预测计算.若无特殊说明,下文中提到的神经网络均指 BP 网络.

使用神经网络预测需要进行训练.本文使用网络模拟器 SSFNet[19]模拟多种网络参数和攻击参数下的 DDoS 攻击,并记录每组参数(瓶颈链路带宽 BW_{thres}、请求频率 R_{att}、半开队列长度 Q_{limit})对应的合法用户平均等待时间 T_{res} 和合法用户请求应答率 P_{res}.本文将记录的网络参数和攻击参数以及合法用户平均等待时间和合法用户请求应答率作为训练数据集,以$\langle BW_{thres},R_{att},Q_{limit}\rangle$作为输入向量、以$\langle P_{res},T_{res}\rangle$作为目标向量,将数据向量

和目标向量进行归一化处理之后,使用训练迅速的 LM(Levenburg-Marquardt)算法对神经网络进行训练.整个训练过程将不断重复,直到神经网络的预测准确性满足要求为止.本文中要求均方误差小于等于 10^{-6},或者训练循环次数达到 600 次.设定循环训练次数的限制是为了避免神经网络被过度训练,反而影响预测效果.连接权重值和阈值的初值选取对训练时间至关重要,对训练结果没有影响[20].本文对初值进行随机赋值.

设通过神经网络映射得到受到攻击时的合法用户请求应答率和合法用户平均等待时间为 $P_{Predict}$ 和 $T_{Predict}$,没有受到攻击时的合法用户请求应答率和合法用户平均等待时间为 P_0 和 T_0.由于 DDoS 攻击会影响可用性,因此存在以下不等式:

$$\begin{cases} P_0 \geqslant P_{Predict} \\ T_0 \leqslant T_{Predict} \end{cases} \tag{2}$$

那么,在受到 DDoS 攻击后,合法用户请求应答率和合法用户平均等待时间的相对改变量为

$$\begin{cases} \Delta P_r = \dfrac{P_0 - P_{Predict}}{P_0} \\ \Delta T_r = \dfrac{T_{Predict} - T_0}{T_{Predict}} \end{cases} \tag{3}$$

因此,根据历史数据求得的合法用户请求应答率和合法用户平均等待时间的重要性权重为

$$\begin{cases} \omega_{P\_Hisroty} = \dfrac{\Delta P_r}{\Delta P_r + \Delta T_r} \\ \omega_{T\_History} = \dfrac{\Delta T_r}{\Delta P_r + \Delta T_r} \end{cases} \tag{4}$$

历史数据中可能记录了 m 次 DDoS 攻击,设分别求得的合法用户请求应答率和合法用户平均等待时间的重要性权重为 $\omega_{P_i}, \omega_{T_i}$, $i \in \{1,2,3,\ldots,m\}$,则将 m 个重要性权重进行平均作为综合权重,计算公式为

$$\begin{cases} \omega_P = \dfrac{\sum_{i=1}^{m} \omega_{P_i}}{m} \\ \omega_T = \dfrac{\sum_{i=1}^{m} \omega_{T_i}}{m} \end{cases} \tag{5}$$

3.2 基于熵权法的重要性权重计算方法

基于历史攻击偏好的方法从攻击的角度,根据历史攻击数据,计算得到评估属性的重要性权重.本节将从防护措施的角度出发,利用部署了防护措施后在攻防场景中收集的指标数据,使用熵权法计算评估属性的重要性权重.

熵是热力学中的概念,最初由香农引入信息论,作为系统无序程度的度量,也用于表示数据所包含有效信息量的多少.熵值越高,则评价对象在某项指标上的差异度越小,其包含的有效信息越少,权重越低;反之则越高.特别地,当各评价对象在某项指标的值完全相同时,熵值达到最大,此时,该评价指标对于选择评价对象的决策活动无法提供有用信息,可以考虑从评价指标中剔除,也即其重要性权重为 0.当某一评估属性的区分度越大,也即确定性越大时,其提供的信息量越多,其所需的额外的信息量也就越少.为了充分利用现有信息,减少由于信息获取而增加的成本,该区分度越大的评估属性,其权重越大.

利用熵权法计算第 j 个评估属性的重要性权重的方法如下:

- 首先,计算第 j 个评估属性的熵值:

$$E_j = -\frac{1}{\ln n} \sum_{i=1}^{n} p_{ij} \ln p_{ij} \tag{6}$$

其中, $p_{ij}=\frac{z_{ij}}{\sum_{i=1}^{n}z_{ij}}$ 表示第 i 个方案中的第 j 个评估属性与所有方案的第 j 个评估属性之和的比值,n 是决策方案的数目.

- 然后,计算差异度 G_j.差异度 G_j 表示方案集中第 j 个指标的差异程度.指标差异越大,E_j 越小,G_j 越大;反之,E_j 越大,G_j 越小.计算公式如下:

$$G_j=1-E_j.$$

- 最后,对差异度进行标准化,得到第 j 个指标的权重:

$$w_j=\frac{G_j}{\sum_{j=1}^{m}G_j}.$$

综上,第 j 个评估属性的熵权计算公式为

$$w_j=\frac{(1-E_j)}{m-\sum_{j=1}^{m}E_j} \tag{7}$$

其中,m 是评估属性的个数.本文中,评估属性为合法用户平均等待时间 T_{res} 及合法用户请求应答率 P_{res},即 m=2.

根据公式(7)得到根据熵权法求得的评估属性的重要性权重.

综上,本文分别从攻击和防护的角度提出了基于历史攻击偏好和基于熵权法的评估属性重要性权重计算方法,接下来将介绍如何使用重要性权重进行防护措施的遴选.

3.3 基于多属性决策的防护措施遴选

本文提出的基于多属性决策的 DDoS 防护措施遴选方法参考了 TOPSIS 方法.TOPSIS 方法是常见的多目标决策方法之一,它对原始数据进行同趋势和归一化的处理后,消除了不同指标量纲的影响;利用原始数据的信息,充分反映各方案之间的差距,客观真实地反映实际情况;对样本资料无特殊要求,具有普遍适用性.TOPSIS 方法在企业经济效益分析、顾客满意程度调查、软件项目风险评价等方面都得到了广泛应用.TOPSIS 方法的基本思路是定义决策问题的正理想解和负理想解,通过寻找距离正理想解最近又距离负理想解最远的解来确定最佳方案.正理想解是假定的最好的方案,负理想解是假定的最差的方案,这两者往往是不可行的.在寻找最佳方案时,通常距离正理想解最近的方案未必是距离负理想解最远的方案,因此,实际中使用相对接近度对待选方案进行排序.

本文提出的基于多属性决策的 DDoS 防护措施遴选算法步骤如下.

为了体现攻击和防护对合法用户请求应答率 P_{res} 和合法用户平均等待时间 T_{res} 的改变程度,首先对公式(1)中决策矩阵 $\boldsymbol{M}$ 中的元素使用公式(8)进行变换:

$$\begin{cases}P_{i\_t}=\dfrac{P_i-P_w}{P_0-P_w}\\ T_{i\_t}=\dfrac{T_i-T_0}{T_w-T_0}\end{cases} \tag{8}$$

其中,P_0 和 T_0 分别是目标系统在没有攻击且没有防护时收集的合法用户请求应答率和合法用户平均等待时间,P_w 和 T_w 分别是目标系统在没有防护且受到攻击时收集的合法用户请求应答率和合法用户平均等待时间.

此时,决策矩阵 $\boldsymbol{M}$ 变为 $\boldsymbol{M}_t$.

$$\boldsymbol{M}_t=\begin{pmatrix}P'_{1\_t} & T'_{1\_t}\\ P'_{2\_t} & T'_{2\_t}\\ P'_{3\_t} & T'_{3\_t}\\ \vdots & \vdots\\ P'_{n\_t} & T'_{n\_t}\end{pmatrix} \tag{9}$$

然后,对公式(9)中决策矩阵 $\boldsymbol{M}_t$ 中的元素使用公式(10)进行正规化处理.

$$m'_{ij}=\frac{m_{ij}}{\sqrt{\sum_{i=1}^{n}m_{ij}^2}} \tag{10}$$

其中, m'_{ij} 是正规化之后的第 i 个方案的第 j 个评估属性,m_{ij} 是矩阵 $\boldsymbol{M}_t$ 中第 i 个方案的第 j 个评估属性.

由 m'_{ij} 构成了正规化决策矩阵 $\boldsymbol{M}'$.

$$\boldsymbol{M}'=\begin{pmatrix}P'_1 & T'_1\\ P'_2 & T'_2\\ P'_3 & T'_3\\ \vdots & \vdots\\ P'_n & T'_n\end{pmatrix}.$$

然后,将 $\boldsymbol{M}'$右乘权重向量 $\boldsymbol{w}$,得到加权正规化决策矩阵 $\boldsymbol{Z}$.

$$\boldsymbol{Z}=\boldsymbol{w}\boldsymbol{M}'=\begin{pmatrix}w_p\\ w_t\end{pmatrix}\begin{pmatrix}P'_1 & T'_1\\ P'_2 & T'_2\\ P'_3 & T'_3\\ \vdots & \vdots\\ P'_n & T'_n\end{pmatrix}.$$

在传统 TOPSIS 方法中,$\boldsymbol{w}$ 由专家或者决策者给出,用于反映各个评估属性的重要性.本文为了减少主观因素的影响,分别从攻防两方面以基于历史攻击偏好的方法和熵权法计算 $\boldsymbol{w}$.

然后,选取加权正规化决策矩阵 $\boldsymbol{Z}$ 中各列最好的属性作为正理想解.

$$\boldsymbol{Z}^*=\{\max_i z_{ij}\mid i=1,2,3,...,n\}=\{z_P^*,z_T^*\}.$$

选取加权正规化决策矩阵 $\boldsymbol{Z}$ 中各列最差的属性作为负理想解.

$$\boldsymbol{Z}^-=\{\min_i z_{ij}\mid i=1,2,3,...,n\}=\{z_P^-,z_T^-\}.$$

求解各方案到正理想解和负理想解的距离.对于方案 i,与正理想解的距离为

$$S_i^*=\sqrt{\sum_{j=1}^{2}(z_{ij}-z_j^*)^2},i=1,2,3,...,n;$$

与负理想解的距离为

$$S_i^-=\sqrt{\sum_{j=1}^{2}(z_{ij}-z_j^-)^2},i=1,2,3,...,n.$$

根据到正、负理想解的距离计算方案 i 的相对接近度.

$$C_i^*=\frac{S_i^-}{S_i^*+S_i^-},$$

其中, C_i^* 的值域是(0,1).越接近理想解, C_i^* 的取值就越接近于 1.可以根据各个方案的 C_i^* 的取值对防护方案集 *Defence* 中所有的防护方案进行排序,进而从中选择最优的方法.上述整个过程即为 DCSM 模型中的映射关系 φ.

在此基础上得到 DDoS 防护措施遴选算法,如算法 1 所示.

算法 1. DDoS Defense Countermeasure Selection.

输入: Set of countermeasures with value of evaluation attributes, Historical attack data (if available);

输出: Rank of each countermeasure.

BEGIN

1. Let $\boldsymbol{M}$ represents the decision matrix, each row of which consists of attributes' value of every countermeasure;

2. $\boldsymbol{M\_t}$=*transform*($\boldsymbol{M}$)
3. $\boldsymbol{M\_n}$=*Normolize*($\boldsymbol{M\_t}$);
4. IF based on history attack data *HData* (from attack perspective),
5. $\boldsymbol{w}$=*HistoryBasedMethod*(*HData*);
6. ELSE (from defense perspective)
7. $\boldsymbol{w}$=*EntropyMethod*($\boldsymbol{M\_n}$);
8. $\boldsymbol{Z}=\boldsymbol{w}\times\boldsymbol{M\_n}$;
9. $\boldsymbol{Z}^*$=*FindPositiveIdealSolution*($\boldsymbol{Z}$);
10. $\boldsymbol{Z}^-$=*FindNegativeIdealSolution*($\boldsymbol{Z}$);
11. $S_i^* = \sqrt{\sum_{j=1}^{2}(z_{ij}-z_j^*)^2}, z_{ij}\in\boldsymbol{Z}, z_j^*\in\boldsymbol{Z}^*$;
12. $S_i^- = \sqrt{\sum_{j=1}^{2}(z_{ij}-z_j^-)^2}, z_{ij}\in\boldsymbol{Z}, z_j^-\in\boldsymbol{Z}^-$;
13. $C_i^* = \dfrac{S_i^-}{S_i^*+S_i^-}$;
14. Rank countermeasures accroding to the value of C_i^*;

END

该算法首先记录各个防护措施在受到攻击时每项评估属性的属性值,构建决策矩阵 $\boldsymbol{M}$.将决策矩阵 $\boldsymbol{M}$ 中的元素使用公式(8)进行变换得到矩阵 $\boldsymbol{M}_t$,接着使用公式(10)正规化之后得到正规化决策矩阵 $\boldsymbol{M}'$.如果从攻击的角度计算重要性权重,则使用公式(5)计算权重向量 $\boldsymbol{w}$;否则,使用公式(7).然后,将权重向量 $\boldsymbol{w}$ 左乘正规化决策矩阵 $\boldsymbol{M}'$,得到加权正规化决策矩阵 $\boldsymbol{Z}$.然后,利用 $\boldsymbol{Z}$ 构造正理想解 $\boldsymbol{Z}^*$和负理想解 $\boldsymbol{Z}^-$,并分别计算出每个防护措施与正、负理想解的距离 S^*与 S^-,最终计算出每个防护措施与正理想解的相对接近度 C^*,将防护措施按照 C^*从大到小排序,得到防护措施的排序结果.

4 模拟实验

4.1 实验方案

本文使用网络仿真软件 SSFNet[19]进行模拟实验.为不失一般性,在保证连通性的前提下,实验采取随机生成拓扑的方法对真实网络进行模拟.本文使用 100 台路由器进行随机拓扑的生成,攻击者、受害主机和合法用户均连接在路由器上.攻击者和合法用户向受害主机发送请求,受害主机对合法用户和攻击者的请求做出响应.拓扑示意图如图 2 所示.

实验采用网络中常见的 SYN flood 作为典型的 DDoS 攻击方式.SYN flood 攻击通过与受害主机进行不完全的 TCP 3 次握手,使受害主机长时间维持大量无用的半开连接,无法响应合法用户的正常请求,甚至令受害主机资源耗尽,从而达到拒绝服务的目的.

实验选取地址黑名单和增大半开队列长度两类防护措施作为候选防护措施,从中进行防护措施的遴选.地址黑名单通过识别并阻断攻击源以减少攻击流量,对目标系统进行保护;增大半开队列长度通过增大维持的半开连接的上限,提高目标系统对攻击的抵抗能力.实验分别模拟识别并阻断 10 个、30 个、50 个攻击源以及将半开队列长度从 4 000 分别增大为 5 000 和 6 000 时的情况,即,防护措施集合为

Defence={阻断 10 个攻击源,阻断 30 个攻击源,阻断 50 个攻击源,半开队列长度增大为 5000,
半开队列长度增大为 6000}.

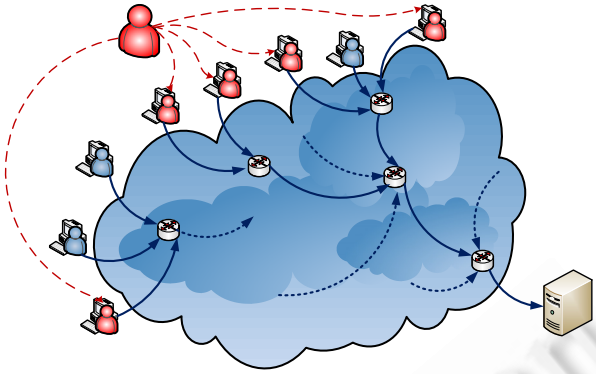

Fig.2 Schematic drawing of the experiment's topology

图 2 实验拓扑示意图

实验分为如下两部分:

- 第 1 部分实验对神经网络进行训练,并通过实验验证预测效果.使用 SSFNet 选取多组 BW_{thres},R_{att},Q_{limit} 进行实验,将实验结果作为训练数据集对神经网络进行训练,并对预测效果进行验证.训练时,BW_{thres},R_{att},Q_{limit} 为输入向量,P_{res} 和 T_{res} 为目标向量;
- 第 2 部分实验利用训练好的神经网络从攻击角度计算重要性权重,同时,使用熵权法从防护角度计算重要性权重,使用这两种权重以基于多属性决策的防护措施遴选方法对候选防护措施进行遴选.最后,对比传统的对重要性权重进行人为赋值的 TOPSIS 方法,分析不同方法对防护措施选择结果的影响.

4.2 实验及结果分析

为了更好地贴近目标系统的实际情况,基于历史攻击偏好的方法使用目标系统受到攻击的历史数据对重要性权重进行计算.由于本文采用的评估指标无法直接通过日志记录,因此我们使用神经网络,以能够记录在日志中的指标作为输入,通过训练,预测出相应的合法用户请求应答率和合法用户平均等待时间.下面将首先对神经网络的预测能力进行验证,通过验证结果说明将神经网络应用在实际计算中的可行性.

使用 SSFNet,在目标系统没有防护的情况下,使用表 1 中的实验参数进行 DDoS 攻击模拟,得到实验数据.其中,僵尸主机数目(S_{zombie})、半开队列长度(Q_{limit})、僵尸主机攻击间隔(I_{att})、瓶颈链路带宽(BW_{thres})、合法用户数目(S_{user})都会影响请求频率(R_{att}).我们将使用这些数据对神经网络进行训练和测试.

Table 1 Experiment parameters to validate the predicting ability of the neural network

表 1 神经网络预测能力验证实验参数

指标	数值
S_{zombie}	70
Q_{limit}	1 000, 3 000, 5 000, 7 000, 9 000, 11 000
I_{att} (s)	2, 3, 4, 5, 6, 7, 8, 9, 10
BW_{thres} (Mbps)	0.5, 1, 3, 5, 7, 9, 11
T' (s)	1 000
S_{user}	20

为了充分证明神经网络的预测能力,实验使用 k 折交叉验证(k-fold cross-validation)方法进行预测效果验证,k=10.具体来说,我们将实验数据随机均等分为 10 份,轮流取出 1 份作为测试集,剩下的 9 份作为训练集,总共进行 10 次训练和预测.通过 10 次的"训练-测试"实验来验证神经网络的预测效果.我们使用预测结果和实际结果的相对误差作为指标.相对误差的计算公式如公式(11)所示.

$$relative\ error=\frac{|predict\ value\text{-}real\ value|}{real\ value} \tag{11}$$

根据公式(11),计算得到的 10 次"训练-测试"实验的相对误差的平均值数据见表 2,可以看到,所有相对误差

均小于 5%,证明了神经网络的预测能力.

接下来将进行模拟攻击实验,并根据实验数据进行防护措施的遴选.

首先使用 SSFNet 对候选防护措施进行模拟,并进行攻击,记录合法用户请求应答率 P_{res} 和合法用户平均等待时间 T_{res},实验数据见表 3.

Table 2 Average of the relative error of the cross validation of the neural network

表 2 神经网络交叉验证相对误差的平均值

指标	相对误差(%)									
P_{res}	1.34	0.54	2.23	0.14	0.90	1.78	0.50	0.44	0.68	0.91
T_{res}	2.07	2.99	2.39	3.75	0.68	1.18	1.10	1.96	1.76	3.60

Table 3 Experiment data under simulated attack

表 3 模拟攻击下的实验数据

防护措施	P_{res}	T_{res}
无防护无攻击	0.998 334	1.985 34
无防护	0.771 101	15.836 6
阻断 10 台僵尸主机	0.775 508	14.101 5
阻断 30 台僵尸主机	0.777 763	13.240 5
阻断 50 台僵尸主机	0.778 585	13.204 9
提升 Q_{limit} 至 5 000	0.969 434	16.769 8
提升 Q_{limit} 至 6 000	0.983 905	16.880 8

然后计算评估属性的重要性权重.下面将分别从攻击和防护角度使用基于历史攻击偏好的方法和熵权法计算评估属性的重要性权重.

当从攻击角度进行评估属性的重要性权重计算时,将使用公式(5)进行计算.其中,没有受到攻击时的合法用户请求应答率和合法用户平均等待时间如表 3 第 1 行所示,受到攻击时的合法用户请求应答率和合法用户平均等待时间使用训练好的神经网络根据收集的模拟攻击指标数据进行预测得到.收集的指标见表 4.

Table 4 Historical attacking data

表 4 历史攻击数据

指标	数值
Q_{limit}	4 000
R_{att}	84.151 0
BW_{thres} (Mbps)	2

将 Q_{limit},R_{att},BW_{thres} 作为神经网络的输入向量,求得 P_{res} 和 T_{res} 分别为 0.771 101,15.836 6.

由于本文模拟实验中只进行了 1 次攻击,因此使用公式(4)计算评估属性的重要性权重.结果为

$$w_{P\_h}=0.206498, w_{T\_h}=0.793502.$$

即,使用基于历史攻击偏好的方法求得的评估属性重要性权重向量为

$$\boldsymbol{w}_h=\begin{pmatrix}0.206498\\0.793502\end{pmatrix} \tag{12}$$

当从防护角度使用熵权法计算重要性权重时,利用公式(6)计算评估属性的熵值:

$$E_P=0.996000, E_T=0.996178,$$

其中,E_P 是指标合法用户请求应答率的熵值,E_T 是指标合法用户平均等待时间的熵值.

之后,利用公式(7)计算重要性权重:

$$w_{P\_e}=0.5108, w_{T\_e}=0.4892.$$

即,使用熵权法求得的评估属性重要性权重向量为

$$\boldsymbol{w}_e=\begin{pmatrix}0.5108\\0.4892\end{pmatrix} \tag{13}$$

接下来将使用算法1对防护措施集合进行遴选,过程如下.

首先,根据表3的数据进行转换和归一化处理,得到矩阵 $\boldsymbol{M}'$:

$$\boldsymbol{M}'=\begin{pmatrix}0.015139 & 0.418094\\ 0.022885 & 0.388383\\ 0.025709 & 0.387155\\ 0.681314 & 0.510169\\ 0.731025 & 0.513999\end{pmatrix}.$$

当从攻击角度进行遴选时,利用 $\boldsymbol{w}_h$ 左乘 $\boldsymbol{M}'$ 计算得到加权正规化决策矩阵 $\boldsymbol{Z}_h$.

$$\boldsymbol{Z}_h=\begin{pmatrix}0.003126 & 0.331758\\ 0.004726 & 0.308183\\ 0.005309 & 0.307208\\ 0.14069 & 0.40482\\ 0.150955 & 0.407859\end{pmatrix}.$$

从加权正规化决策矩阵 $\boldsymbol{Z}_h$ 中选取正理想解 $\boldsymbol{Z}_h^*$ 和负理想解 $\boldsymbol{Z}_h^-$.需要指出的是:合法用户请求应答率是效益型指标,越大越好;合法用户平均等待时间是成本型指标,越小越好.

$$\boldsymbol{Z}_h^*=(0.150955,0.307208),$$

$$\boldsymbol{Z}_h^-=(0.003126,0.407859).$$

分别计算5种防护措施到正、负理想解的距离,求解各个防护措施的相对距离 C_h^*,并进行排序,结果见表5.在5种防护措施中,将优先选择将半开队列长度增大到6 000的防护措施.

Table 5 Relative distance from each countermeasure to the ideal solution evaluated form the attacking aspect and the rank

表5 从攻击角度评估防护措施与正理想解的相对距离及排名

	阻断10台僵尸主机	阻断30台僵尸主机	阻断50台僵尸主机	提升 Q_{limit} 至5 000	提升 Q_{limit} 至6 000
C_h^*	0.336 798	0.405 37	0.408 714	0.583 664	0.594 932 2
排名	5	4	3	2	1

当从防护角度进行遴选时,利用 $\boldsymbol{w}_e$ 左乘 $\boldsymbol{M}'$ 计算得到加权正规化决策矩阵 $\boldsymbol{Z}_e$.

$$\boldsymbol{Z}_e=\begin{pmatrix}0.007733 & 0.204531\\ 0.01169 & 0.189997\\ 0.013132 & 0.189396\\ 0.348015 & 0.249575\\ 0.373408 & 0.251448\end{pmatrix}.$$

从加权正规化决策矩阵 $\boldsymbol{Z}_e$ 中选取正理想解 $\boldsymbol{Z}_e^*$ 和负理想解 $\boldsymbol{Z}_e^-$.需要指出的是:合法用户请求应答率是效益型指标,越大越好;合法用户平均等待时间是成本型指标,越小越好.

$$\boldsymbol{Z}_e^*=(0.373408,0.189396),$$

$$\boldsymbol{Z}_e^-=(0.007733,0.251448).$$

分别计算5种防护措施到正、负理想解的距离,求解各个防护措施的相对距离 C_e^*,并进行排序,结果见表6.在5种防护措施中,将优先选择将半开队列长度增大到6 000的防护措施.

下面使用传统的TOPSIS方法进行实验,与本文方法的实验结果进行对比.假设传统的TOPSIS方法对权重向量赋值为

$$\boldsymbol{w}_t=\begin{pmatrix}0.3\\ 0.7\end{pmatrix}.$$

此时,正规化正交决策矩阵为

$$\boldsymbol{Z}_t=\begin{pmatrix}0.004542 & 0.292666\\ 0.006866 & 0.271868\\ 0.007713 & 0.271008\\ 0.204394 & 0.357118\\ 0.219307 & 0.369799\end{pmatrix}.$$

Table 6 Relative distance from each countermeasure to the ideal solution evaluated form the defending aspect and the rank

表 6 从防护角度评估防护措施与正理想解的相对距离及排名

	阻断 10 台僵尸主机	阻断 30 台僵尸主机	阻断 50 台僵尸主机	提升 Q_{limit} 至 5 000	提升 Q_{limit} 至 6 000
C_e^*	0.113 627	0.145 474	0.147 403	0.838 965	0.854 925
排名	5	4	3	2	1

根据算法 1 最终得到各个防护措施的相对距离 C_t^* 及排序结果,结果见表 7.在 5 种防护措施中,将优先选择将半开队列长度增大到 6 000 的防护措施.

Table 7 Relative distance from each countermeasure to the ideal solution evaluated by traditional TOPSIS and the rank (with the weight of (0.3,0.7))

表 7 传统 TOPSIS 方法计算的防护措施与正理想解的相对距离及排名(权重向量为(0.3,0.7))

	阻断 10 台僵尸主机	阻断 30 台僵尸主机	阻断 50 台僵尸主机	提升 Q_{limit} 至 5 000	提升 Q_{limit} 至 6 000
C_t^*	0.237 232	0.292 811	0.295 723	0.695 777	0.707 497
排名	5	4	3	2	1

通过表 3 可以看出:在地址黑名单的防护措施中,阻断 50 个攻击源的防护措施效果最好;在增大半开队列长度的防护措施中,将半开队列长度增大到 6 000 的防护措施效果最好.这在表 5~表 7 的排名中均有体现.但是阻断 50 个攻击源的防护措施和将半开队列长度增大到 6 000 的防护措施二者各有优劣:前者的合法用户平均等待时间更短,后者的合法用户请求应答率更高.因此,这两个防护措施是所有 5 个防护措施中的非劣解.所谓非劣解是指不存在一个解使得该解的所有属性均优于非劣解.这是由于多属性决策中的矛盾性所导致的.

如上所述,本文提出的基于多属性决策的防护措施遴选方法分别从攻击和防护的角度选择了增大半开队列长度至 6 000 的防护措施,同时,传统的 TOPSIS 方法在重要性权重为(0.3,0.7)的情况下也选择了增大半开队列长度至 6 000 的防护措施.这 3 种方法选择的都是非劣解集中的防护措施,且是同一个防护措施,因此,这 3 种方法的选择都是正确的.

虽然本文提出的方法和传统的 TOPSIS 方法都选择了非劣解集中的防护措施,但是传统的 TOPSIS 方法的权重向量由人为指定,存在主观性,会造成选择结果的不确定.如果实验中传统的 TOPSIS 方法指定的重要性权重为(0.15,0.85),此时通过计算得到的各个防护措施与理想解的相对距离见表 8.此时应选择阻断 50 个攻击源的防护措施,而不是重要性权重为(0.3,0.7)时选择的增大半开队列长度至 6 000 的防护措施.这种赋值的主观性在实际应用中会导致由于是不同的使用者而使得人为赋值的重要性权重有所不同,因此最终选择的防护措施不一致的情况出现.而本文提出的方法只要指标数据确定,无论从攻击角度还是防护角度计算得到的重要性权重都不会改变,即使使用者不同,也不会造成结果的差异,因此减少了传统 TOPSIS 方法的主观性和不确定性.综上,本文提出的措施遴选方法可以选择出非劣解集中的防护措施,减少了由于人为赋值引入的主观性因素.

本文提出的基于多属性决策的防护措施遴选方法分别使用基于历史攻击偏好的方法和熵权法计算重要性权重,其结果都成功选择了非劣解集中的防护措施.但是这两种计算方法还存在不同:前者因为考虑了历史攻击的偏好状况,所以使用该方法计算得到的权重对于实际攻击防护而言更具有针对性,但该方法需要使用历史数据对神经网络进行训练,应用条件较为复杂;后者基于熵权法的计算方法,其最大的优势在于不需要事先获取历史数据,使用范围更广,但是也因此存在选择结果针对性不强的情况.因此,当存在系统日志可以提取历史数据

时,可使用基于历史攻击偏好的方法计算重要性权重,以便结果更有针对性;当无法获取历史数据时,则使用熵权法计算重要性权重更加合适.

Table 8 Relative distance from each countermeasure to the ideal solution evaluated by traditional TOPSIS and the rank (with the weight of (0.15,0.85))

表 8 传统 TOPSIS 方法计算的防护措施与正理想解的相对距离及排名(权重向量为(0.15,0.85))

	阻断 10 台僵尸主机	阻断 30 台僵尸主机	阻断 50 台僵尸主机	提升 Q_{limit} 至 5 000	提升 Q_{limit} 至 6 000
C_{t2}^{*}	0.424 414	0.501 301	0.504 757	0.488 163	0.498 989
排名	5	2	1	4	3

5 总 结

针对现有评价方法对防护措施选择指导性不强的问题,本文首先构建了 DDoS 防护措施遴选模型(DCSM).在此基础上,本文提出基于多属性决策的 DDoS 防护措施遴选方法.该方法利用多角度的评估指标,基于 DDoS 攻防实际,分别从攻击和防护的角度以基于历史攻击偏好的方法和熵权法计算评估属性的重要性权重并进行防护措施的排序,最后,根据计算结果对 DDoS 防护措施的遴选进行指导.在实验部分,使用 SSFNet 模拟常见的 SYN flood 攻击对地址黑名单和增大半开队列长度两类防护措施进行评估,验证了本文提出的防护措施遴选方法的正确性.通过对比传统 TOPSIS 方法,验证了本文方法对于减少主观因素影响的效果.

后续研究工作包括增加对防护措施成本的考虑,更加全面地对防护措施进行考量;引入模糊数学以应对无法获取准确指标值的场景;结合攻防两个角度,提出综合的措施遴选方法等.

References:

[1] Butler SA. Improving security technology selections with decision theory. In: Proc. of the 3rd Workshop on Economics-Driven Software Engineering Research. 2001. 1−4. http://www.cs.cmu.edu/afs/cs/project/vit/ftp/pdf/improv.butler.pdf

[2] Peng T, Leckie C, Ramamohanarao K. Survey of network-based defense mechanisms countering the DoS and DDoS problems. ACM Computing Surveys, 2007,39(1):3. [doi: 10.1145/1216370.1216373]

[3] Mirkovic J, Reiher P. A taxonomy of DDoS attack and DDoS defense mechanisms. SIGCOMM Computer Communication Review, 2004,34(2):39−53. [doi: 10.1145/997150.997156]

[4] Specht SM, Lee RB. Distributed denial of service: Taxonomies of attacks, tools, and countermeasures. In: Proc. of the ISCA PDCS. 2004. 543−550. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.133.4566

[5] Mölsä JVE. A taxonomy of criteria for evaluating defence mechanisms against flooding DoS attacks. In: Proc. of the 1st European Conf. on Computer Network Defence. London: Springer-Verlag, 2006. 13−22. [doi: 10.1007/1-84628-352-3_2]

[6] Butler SA. Security attribute evaluation method: A cost-benefit approach. In: Proc. of the 24th Int'l Conf. on Software Engineering. Orlando: ACM Press, 2002. 232−240. [doi: 10.1145/581339.581370]

[7] Bellaiche M, Gregoire J. Measuring defence systems against flooding attacks. In: Proc. of the Wireless Communications and Mobile Computing Conf. 2008. 600−605. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4600003&tag=1

[8] Schwab S, Wilson B, Thomas R. Methodologies and metrics for the testing and analysis of distributed denial of service attacks and defenses. In: Proc. of the Military Communications Conf. 2005. 2686−2692. [doi: 10.1109/MILCOM.2005.1606072]

[9] Meadows C. A formal framework and evaluation method for network denial of service. In: Proc. of the 1999 IEEE Computer Security Foundations Workshop. 1999. 4−13. [doi: 10.1109/CSFW.1999.779758]

[10] Mirkovic J, Arikan E, Wei SJ, Thomas R, Fahmy S, Reiher P. Benchmarks for DDoS defense evaluation. In: Proc. of the Military Communications Conf. 2006 (MILCOM 2006). 2006. 1−10. [doi: 10.1109/MILCOM.2006.302006]

[11] Mirkovic J, Reiher P, Fahmy S, Reiher P, Thomas R. Measuring denial of service. In: Proc. of the Conf. on Computer and Communications Security. Alexandria, 2006. 53−58. http://dl.acm.org/citation.cfm?id=1179506

[12] Mirkovic J, Hussain A, Wilson B, Fahmy S, Reiher P, Thomas R, Yao WM, Schwab S. Towards user-centric metrics for denial-of-service measurement. In: Proc. of the Workshop on Experimental Computer Science. San Diego, 2007. [doi: 10.1145/1281700.1281708]

[13] Li ZW, Xiang Y, He DS. Simulation and analysis of DDoS in active defense environment. In: Proc. of the Computational Intelligence and Security. Guangzhou, 2006. 878−886. [doi: 10.1007/978-3-540-74377-4_92]

[14] Zuo J. Multi Criteria Decision Making. Hangzhou: Zhejiang University Press, 1991 (in Chinese).

[15] Zhang YR, Xian M, Wang GY. A quantitative evaluation technique of attack effect of computer network based on network entropy. Chinese Journal on Communications, 2004,25(11):158−165 (in Chinese with English abstract).

[16] Zhao JJ, Wen Y, Wang DX. A network security evaluation method framework based on multiple criteria decision making theory. In: Proc. of the 2011 5th Int'l Conf. on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS). 2011. 371−375. [doi: 10.1109/IMIS.2011.38]

[17] Dewri R, Poolsappasit N, Ray I, Whitley D. Optimal security hardening using multi-objective optimization on attack tree models of networks. In: Proc. of the 14th ACM Conf. on Computer and Communications Security. New York: ACM Press, 2007. 204−213. [doi: 10.1145/1315245.1315272]

[18] Huang L, Feng DG, Lian YF, Chen K. Artificial neural network based DDoS defense effectiveness evaluation. Chinese Journal of Computer Research and Development, 2013,50(10):2100−2108 (in Chinese with English abstract).

[19] SSF Research Network. Scalable simulation framework network models. 2013. http://www.ssfnet.org/homePage.html

[20] Han LQ. The Tutorial of Artificial Neural Network. Beijing: Beijing University of Posts and Telecommunications Press, 2006 (in Chinese).

附中文参考文献:

[14] 左军.多目标决策分析.杭州:浙江大学出版社,1991.

[15] 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.通信学报,2004,25(11):158−165.

[18] 黄亮,冯登国,连一峰,陈恺.基于神经网络的 DDoS 防护绩效评估.计算机研究与发展,2013,50(10):2100−2108.

[20] 韩力群.人工神经网络教程.北京:北京邮电大学出版社,2006.

黄亮(1984－),男,陕西西安人,博士,助理研究员,主要研究领域为网络安全,绩效评估.

陈恺(1982－),男,博士,主要研究领域为信息安全,软件漏洞分析与检测,恶意代码分析与防范.

冯登国(1965－),男,博士,研究员,博士生导师,CCF 高级会员,主要研究领域为网络与系统安全.

张颖君(1982－),女,博士,主要研究领域为系统安全.

连一峰(1974－),男,博士,副研究员,主要研究领域为网络安全,绩效评估.

刘玉岭(1982－),男,博士,主要研究领域为网络安全,绩效评估.