doi:10.3969/j.issn.1000-436x.2013.11.008

在线监测的路由器安全威胁态势量化评估方法

杨君刚[1]，梁礼[2]，刘故箐[1]，张倩[1]，张长青[2]
（1. 西安通信学院 信息传输系，陕西 西安 710106；2. 西安通信学院 研究生管理大队，陕西 西安 7101061）

摘 要：在对路由器安全问题本质分析基础上提出路由器安全效能的概念并对路由器攻击进行分类，提出一种在线监测的路由器安全威胁态势量化评估的计算方法。该方法在对路由器攻击分类的基础上，以路由器带宽占用率和 CPU 平均使用率计算服务下降型威胁安全风险因子，以威胁发生可能性和威胁严重程度计算权限提升型安全风险因子，结合路由器本身的重要性计算其安全风险，进而分析路由器的安全威胁态势。实验表明：所提方法能够很好地反映路由器的安全风险，为网络管理员提供直观的安全威胁态势，以便调整路由器安全策略，更好地提高其安全性能。

关键词：路由器安全；威胁态势；在线监测；风险评估
中图分类号：TP393 **文献标识码**：A **文章编号**：1000-436X(2013)11-0059-12

Method for router online security risk assessment quantification

YANG Jun-gang[1], LIANG Li[2], LIU Gu-jing[1], ZHANG Qian[1], ZHANG Chang-qing[2]
(1. Department of Information Transmission, Xi'an Communications Institute, Xi'an 710106, China;
2. Administration Office for Graduate Students, Xi'an Communications Institute, Xi'an 710106, China)

Abstract: The concept of router safety performance was proposed based on the nature of router security issues and router attacks were classified. Then a method for router online security risk assessment quantification was also presented. The security risk factor of service decline was calculated by router bandwidth consumption and average CPU usage and the security risk factor of privilege escalation was calculated by the possibility of threat occurrence and severity based on the router attack classification. The router security threat status was evaluated combining weighting the importance of router and the security risk factor. The experiment results show the method is effective in calculating the quantitive risk of the router and helpful for administrators to assess security risks.

Key words: router security; threat situation; online monitoring; risk assessment

1 引言

随着internet技术的日益成熟和接入互联网主机成几何级倍数增加，网络规模在日益扩大，而作为网络正常运行的有效监控手段，贯穿于信息系统整个生命周期的安全风险评估已受到了越来越多国内外专家和学者高度重视。现有信息网络安全风险评估多以计算机网络中的主机和服务为对象，在评估模型[1~3]、评估方法[4~7]、评估工具[8]和计算机弱点数据库[9,10]等方面取得了很多研究成果并得到了广泛应用。然而目前对路由器安全的研究大部分集中于对其安全性的实施上，而对路由器安全风险评估方面的研究相对较少，并且缺乏系统性和明确性[11~17]。2012 年 9 月 6 日美国互联网流量监测机构Telegeography给出了 2008 年中期至 2012 年中期的互联网流量增长情况，统计数字如图 1 所示，2008 年中期至 2009 年中期互联网流量增长了 74%，而 2011 年中期至 2012 年中期全球网络流量增长了 35%，增速在逐渐放缓，但网络流量依然在稳定增长。思科首席技术官Padmasree Warrior预测到 2013

收稿日期：2013-01-06；**修回日期**：2013-04-23
基金项目：国家自然科学基金资助项目(61072125)；陕西省自然科学基金资助项目(2011JM8033)
Foundation Items: The National Natural Science Foundation of China(61072125); The Natural Science Foundation of Shaanxi Province(2011JM8033)

年全球互联网流量将达到 56 EB，是 2007 年的 11 倍。网络规模进一步扩大，路由器作为IP网络中的核心设备，担负着数据分组转发、网络内部连接和网络间互联的功能，随着黑客攻击手段丰富化和病毒种类多样化发展，路由器受到了黑客越来越多的攻击，成为攻陷整个网络的主要跳板之一，从而对整个网络系统产生巨大危害性和破坏性，甚至可能产生毁灭性影响。只有对路由器进行安全风险评估，才能为网络安全管理员提供直观安全威胁态势，以便调整系统的安全策略，更好地提高整个系统的可靠性和稳定性，因此，对路由器进行安全风险评估就显得至关重要。

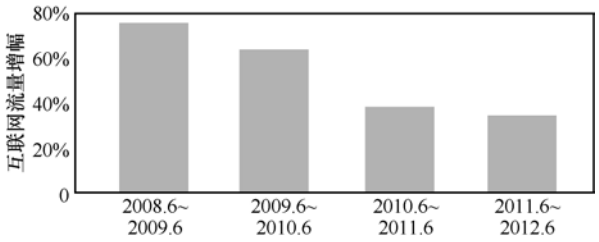


图 1 Telegeography 公布的互联网流量增幅

本文首先对路由器安全问题的本质进行分析，提出路由器安全效能的概念。以路由器安全效能定义为牵引，对构成路由器的安全风险进行分类研究，将错综复杂的路由器安全威胁方式总体分为服务下降型威胁和权限提升型威胁两大类，极大地降低了分析的复杂性。在此基础上，以风险分析中涉及的资产(威胁对象价值)、脆弱性、威胁三要素为出发点，以威胁对象价值、威胁严重程度和威胁发生可能性作为核心变量提出一种基于实时监控信息的路由器安全风险定量评估方法。该方法将威胁对象的价值定义为安全风险影响因子，综合考虑路由器在网络中的地位以及流经路由器端口的数据分组加权转发量，建立相应的判断原则和赋值表，使衡量威胁对象价值的标准统一、规范性强，结合威胁严重程度和威胁发生可能性定义安全风险因子的概念，针对威胁攻击种类的不同确定各自参数：根据服务下降型威胁的原理，提出以路由器带宽占用率和 CPU 使用率计算服务下降型威胁的安全风险因子；以威胁发生可能性和威胁严重程度作为计算权限提升型威胁安全风险因子的指标参数；最后给出了路由器安全风险的定量计算。本文以 Snort 入侵检测设备和简单网络管理协议的软件 SolarWinds 实时告警信息为基础数据，对论文提出的新方法进行分析，最后以实验室网络环境和校园网为基础，对该方法进行实验分析，验证了该方法的准确性和有效性。

2 路由器安全风险评估方法

2.1 安全风险因子

路由器主要担负着网络互联、提供数据分组过滤、转发、路由配置、流量控制等诸多功能，目前，大多数学者从体系结构特点和业务方面将路由器的攻击分为数据平面攻击、控制平面攻击和管理平面攻击 3 大类[18]，该分类方法虽然符合AT&T安全专家Amoroso提出的分类标准，但只是孤立地分析每种攻击的攻击原理、步骤、危害等，不能为评估其风险提供理论支撑。为此，本文从攻击发生后造成安全风险影响结果的角度出发，把路由器安全风险分为两类，一类是造成路由器数据处理能力下降的安全风险，如系统资源耗尽攻击对路由器CPU进行消耗，使其无法满足数据分组正常转发的需求，在本文中将这类安全风险称为服务下降型威胁；另一类是造成路由器保护处理的数据分组安全属性能力下降的安全风险，体现为路由器服务权被非法用户使用，例如基于Cisco IOS认证漏洞的HTTP攻击，攻击者在HTTP服务器启用并使用本地用户认证的前提下，可以绕过认证并以最高特权执行所有命令，达到对路由完全控制并改变路由表配置的目的，在本文中将这类安全风险称为权限提升型威胁，如表 1 所示。

在对构成路由器的安全风险进行分类研究的基础上，认为路由器安全性主要包括 2 个方面：一方面是路由器保证其在硬件（快速路径）或软件（慢速路径）正常处理（转发或丢弃）数据分组的能力，如选择性数据分组丢弃（SPD），SPD 可以确保某些传输数据分组使用较高的优先级，同时在 IOS 处理水平的高通信情形中丢弃较不重要的数据分组，再如保证数据分组高速转发；另一方面是路由器保护其上处理的某些类型数据分组（过境、接收和非 IP 分组，异常分组被丢弃）安全属性的能力，主要包括路由器对处理数据分组保密性、完整性和可用性的保护能力，如路由器在接收的数据分组上执行完整性检查（IP 健康检查），包括 IP 校验和 IP 头格式的验证。因此，给出路由器安全效能定义如下。

定义 1 路由器安全效能指路由器在可接受的性能界限内和适当的成本结构下通过自身的体系

表 1　　**路由器攻击分类**

服务下降型		权限提升型					
大流量攻击	路由欺骗	信息窃取					
带宽耗尽型攻击	OSPF 拒绝服务攻击	IP 地址欺骗					
系统资源耗尽型攻击	BGP 拒绝服务攻击	路由欺骗					
	ICMP 拒绝服务攻击	RIP 欺骗	OSPF 欺骗	IS-IS 欺骗	BGP 欺骗	IP 源路由欺骗	ICMP 重定向攻击
Telnet 攻击		Telnet 攻击、HTTP 攻击、SNMP 攻击、TFTP 攻击、SSH 攻击					
HTTP 攻击							
SNMP 攻击							
TFTP 攻击							
SSH 攻击							

结构对完成数据分组（过境分组、接收分组、非 IP 分组和异常分组）处理的保障能力和某些类型数据分组（过境分组、接收分组和非 IP 分组异常分组被丢弃）的保护能力的综合能力。

通过前面的分析可以看出，路由器安全风险实际上就是引发路由器安全效能下降的各种因素的集合，因此，对路由器安全风险的评估实际上就是量化评估路由器安全风险对其安全效能的影响程度。以风险分析中涉及的资产（威胁对象）、脆弱性、威胁三要素为出发点，以威胁对象价值、威胁严重程度和威胁发生可能性作为核心变量结合路由器自身功能特点对其进行安全风险评估。下面首先介绍安全风险因子的概念。

定义 2　安全风险因子。一个攻击威胁发生可能性和威胁严重程度的乘积被称为安全风险因子。按照安全风险因子的定义，其主要包括攻击威胁发生的可能性 P 和威胁影响严重程度 D 2 个变量。

本文以路由器安全效能定义为指导，以服务下降型威胁和权限提升型威胁作为划分路由器安全风险因子参数的依据，定义路由器安全风险因子为

$$G = G_{\text{decline}}(t) + G_{\text{escalate}}(G_{\text{escalate1}}(t), \cdots, G_{\text{escalaten}}(t)) \quad (1)$$

其中，

1) G_{decline}、G_{escalate} 分别为路由器攻击中服务下降型威胁安全风险因子和权限提升型威胁安全风险因子。

2) 基于攻击次数的威胁分析，难以客观反映服务下降型攻击发生时的状态。本文结合常见DoS攻击的原理：通过消耗路由器带宽或CPU导致拒绝服务[14]，提出使用CPU平均使用率和路由器带宽占用率，确定一次服务下降型威胁发生时的安全风险因子，即

$$G_{\text{decline}}(t) = 1\ \{0B(t-\Delta t,t) \cup C(t-\Delta t,t)] \quad (2)$$

(a) $B(t-\Delta t,t)$ 为 Δt 时间内路由器带宽占用率，$C(t-\Delta t,t)$ 为 Δt 时间内 CPU 平均使用率，Δt 为时间分析窗口。当服务下降型攻击发生时，路由器吞吐量、时延和路由计算能力等功能指标恶化，从路由器性能的角度看，他们都取决于 CPU 的性能，而最能体现 CPU 性能的参数为 CPU 平均使用率，与此同时路由器带宽占用率也在缓慢线性增长，当本次攻击完成后路由器带宽占用率 B 未达到该路由器带宽占用率阈值 B_t，表明本次攻击主要对 CPU 性能造成影响，以 $C(t-\Delta t,t)$ 作为衡量路由器服务下降型威胁安全风险因子的指标参数，此种 DDoS 攻击称为系统资源耗尽型攻击；当在 Δt 时间内路由器带宽占用率 B 已达到路由器带宽占用率阈值 B_t 而本次攻击尚未结束时，CPU 使用率增长迅速减缓，以 $B(t-\Delta t,t)$ 作为衡量本次攻击对路由器服务下降型威胁安全风险因子的指标参数，此种攻击称为带宽耗尽型攻击。这里需要特别指出的是不同厂商不同型号的路由器带宽占用率阈值可能不同，需要按具体情况确定。

(b) $B(t-\Delta t,t) \cup C(t-\Delta t,t)$ 为 t 时刻路由器服务下降型安全风险因子，为了提高评估的合理度，本文对大量的 DDoS 入侵事件的等效性进行调查，大多数安全专家普遍认同：$B(t-\Delta t,t) \cup C(t-\Delta t,t)$ 不能很好地描述出 DDoS 攻击对路由器造成的毁灭性打击，因此，本文把 $B(t-\Delta t,t) \cup C(t-\Delta t,t)$ 修正为 $10\left[B(t,t-\Delta t) \cup C(t-\Delta t,t)\right]$，相比于权限提升类攻击，以突出 DDoS 攻击对整个设备的瘫痪或崩溃造成的影响。

(c) 路由器带宽占用率

本文结合常见带宽耗尽型攻击的原理：攻击者通过放大等技巧消耗掉目标网络的所有可用带宽，造成路由器带宽大部分用来处理攻击报文，而没有多余带宽分配给正常的网络流量，使对正常业务产生DoS[19]，提出使用路由器带宽占用率度量带宽耗尽型攻击发生时的威胁值。路由器带宽占用率定义为

$$B(t-\Delta t,t)=\begin{cases}\dfrac{RB^{'}}{RB_{\max}}\times 100\%, \dfrac{RB^{'}}{RB_{\max}}\geqslant B_t\\ 0, \dfrac{RB^{'}}{RB_{\max}}<B_t\end{cases} \tag{3}$$

其中，$RB^{'}$、$RB_{\max}$ 分别为 Δt 时间内路由器占用带宽和最大可用带宽，B_t 为路由器带宽占用率阈值，即路由器性能急剧下降前的最大路由器带宽占用率，需根据路由器具体型号和实验统计分析确定。

(d) CPU 平均使用率

路由器在转发数据分组时并不会去检测其是否为DDoS攻击的报文（目的IP为路由器除外），在转发过程中路由器会消耗CPU资源以及内存资源，如果转发的数据报文形成了数据流，则此时还会在路由器中形成cache表项，从而消耗一定的内存资源。cache表所消耗的内存资源较小，通常情况下，内存不会对数据分组的转发造成影响[20]，因此为了降低评估复杂度，认为CPU消耗情况可以正确反映系统耗尽型攻击的威胁指数。通过大量实验发现DDoS攻击发生时CPU使用率能够保持在60%以下，说明其能满足提供正常服务的需求；低于70%，则说明CPU资源被过度占用，可以提供服务但效率明显降低[21]，提出使用CPU平均使用率指标度量攻击发生时的威胁。在分析时间窗口 Δt 时间内，以 $C\geqslant 60\%$ 作为前提条件，CPU平均使用率越大，由DDoS引起的路由器安全风险值越高，制定如表 2 所示的CPU平均使用率赋值。

表 2　　CPU 平均使用率赋值

平均使用率	C
60%~61%	0.5
62%~63%	0.6
64%~65%	0.7
66%~67%	0.8
68%~∞	0.9

(e) 通过在客户端部署简单网络管理协议的软件 SolarWinds，同时指定客户端允许连接上的路由器，并在相应的路由器上配 SNMP 及密钥，使客户端与路由器的密钥匹配，从而达到实时监控路由器运行状态的目的。SolarWinds 作为在线监测的数据源，为系统管理员提供路由器带宽占用率、CPU 使用率以及告警接口 down 和 up 状态等相关信息。

(f) 路由器服务下降型威胁安全风险因子算法（算法 1）流程如图 2 所示。

算法1 路由器服务下降型威胁安全风险因子算法
输入：路由器带宽占用率，CPU使用率
输出：路由器服务下降型威胁安全风险因子值
BEGIN
1) Initialization://初始化变量;
2) For each router R_0,R_1,…,R_w;
3) Let SW represent SolarWinds, Eve represent the security events
4) *Eve*=audit(*SW*);//简单网络管理协议的软件获取安全事件;
5) Let *B* represent bandwidth occupancy, *C* represent CPU useage, B_t represent router occupancy threshold;
6) If *B* below B_t (Eve is exhaustion of resources);
7) {$G_{decline}$=*match*(*C*)
}//匹配CPU使用率得到服务下降型安全风险因子;
8) else suppose *B* is more than the threshold (*Eve* is bandwidth depletion mode);
9) {$G_{decline}$=*match*(*B*)
}//匹配路由器带宽占用率得到服务下降型安全风险因子;
10) return 0
END

图 2　路由器服务下降型威胁安全风险因子算法

在算法 1 中，首先对简单网络管理协议的软件 SolarWinds 收集安全事件信息；然后利用路由器带宽占用率阈值 B_t 判断攻击为系统资源耗尽型或者带宽耗尽型；最后利用 C 或 B 计算服务下降型威胁安全风险因子。

3) 权限提升型威胁安全风险因子由攻击所有种类权限提升型安全风险因子求和获得，他们与该权限提升类攻击威胁发生的可能性和威胁严重程度相关，可表示为

$$G_{\text{escalate}}=\sum_{i=1}^{n}G_{\text{escalatei}}(t)=\sum_{i=1}^{n}P_{\text{escalatei}}(t)\times D_{\text{escalatei}}(t) \tag{4}$$

$P_{\text{escalatei}}$ 为一次攻击中第 i 种权限提升型威胁发生的可能性。本文采用流程图的方式对路由器权限提升型威胁发生可能性进行描述，如图 3 所示。威胁发生可能性与路由器的协议开启与否、操作系统、端口开放程度等特征有关，也与威胁利用难易程度有关，其具体判断过程包括以下几个步骤。

(a) 权限提升类攻击发生。

(b) 此权限提升类攻击与网络中目标路由器种

类不一致（对象不一致），威胁发生可能性为E_0，例如某权限提升类攻击针对Cisco宽带路由器，而网络中目标路由器为无线路由器，则威胁发生可能性为E_0。如果此权限提升类攻击与网络中目标路由器种类一致（对象一致），则检验目标路由器是否开启了此次攻击针对的协议。

(c) 如果目标路由器未开启攻击所针对的协议，威胁发生可能性为E_1，如大量发送ICMP请求和ICMP应答，试图对目标路由器CPU造成影响，而目标路由器ICMP协议未开启，故对CPU影响较小，威胁发生可能性为E_1，否则检验目标路由器的操作系统是否一致。

(d) 若目标路由器的操作系统与攻击所针对的路由器操作系统不一致，则威胁发生可能性为E_2，例如，目标路由器操作系统为Cisco IOS操作系统，开启BGP，而某次权限提升类攻击针对的是JUNOS操作系统，远程攻击者利用其对BGP实现上存在漏洞，向JUNOS发送畸形的BGP，UPDATE消息，可能导致BGP会话出现振荡(flap)，也就是当一条路由在被收回后，又被广播出来，故威胁发生可能性为E_2。若目标路由器的操作系统与攻击所针对的路由器操作系统一致，需检验目标路由器操作系统版本号与已发生攻击所针对的操作系统版本号是否一致。

(e) 判断目标路由器操作系统版本号、对应端口与已发生攻击所针对的操作系统版本号、对应端口是否一致的过程同前几步，这里不再赘述。

(f) 在目标路由器与已发生权限提升类攻击所针对的对象、协议开启与否、操作系统、版本号、对应端口与漏洞等特征一致的前提下，结合Snort用户手册中攻击特征规则库把威胁利用难易度（简单、容易、中等和困难）划分的 4 级判断权限提升型威胁发生可能性分别为E_9、E_8、E_7、E_6。

流程图充分体现了路由器特征与权限提升型威胁发生可能性逐项匹配的原则，避免了二义性，具有互斥性，使威胁发生可能性的计算更加完整。最后一项威胁利用难易程度是以Snort用户手册中攻击特征规则库为基础，Snort用户手册把威胁利用难易程度划分为 4 级[22]，表 3 第一行是从用户手册中摘录的威胁利用难易程度划分级别。在图 3 中，发生可能性 $E_0 \sim E_9$ 可以根据实际情况，在 0~1 之间选择，表 4 给出了一种确定方式。

表 3　攻击难易度

Ease of Attack	对应流程图中等级
easy	简单
simple	容易
moderate	中等
difficult	困难

表 4　威胁发生可能性赋值

E_0	E_1	E_2	E_3	E_4	E_5	E_6	E_7	E_8	E_9
0.0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9

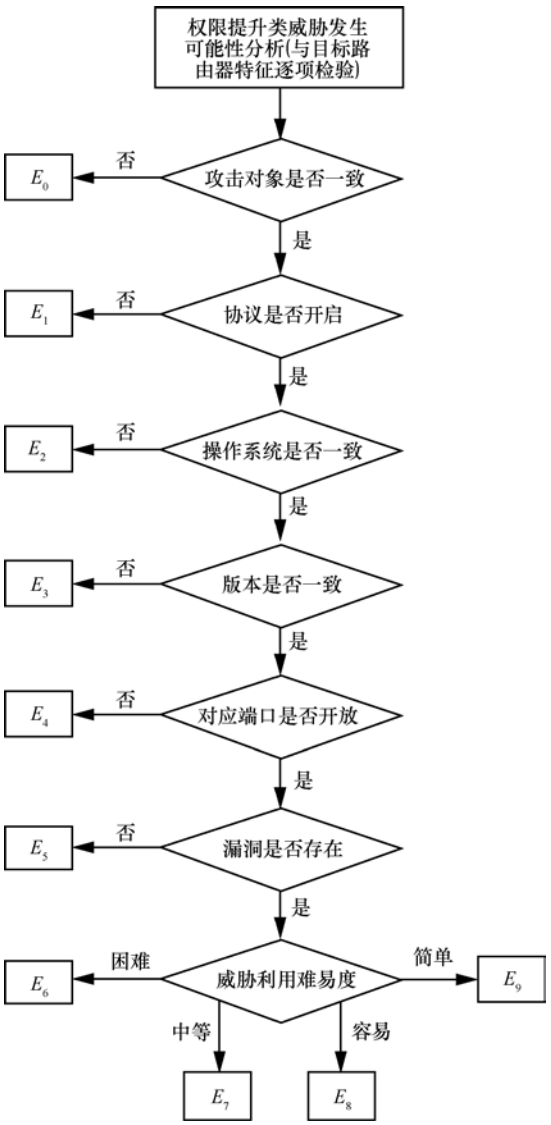


图 3　路由器权限提升型威胁发生可能性流程

$D_{\text{escalatei}}$ 为一次攻击中第 i 种权限提升型威胁发生的严重程度。权限提升型威胁严重程度既与攻击可能带来的后果有关，也与攻击的有效性相关。本文以 Snort 用户手册对攻击优先级（Sig_priority）

的划分为基础并经过归一化处理来度量威胁发生的严重程度。由于一个高优先级的告警所对应的攻击往往比一个低优先级告警所对应攻击的危害程度要大得多，故采用威胁指数方式对威胁严重程度赋值，即 $D_{\text{escalatei}}^{'}(t)=10^{SP}\ (SP=1,2,3,4)$，对此进行归一化处理，得到 $D_{\text{escalatei}}(t)$ 的值，即

$$D_{\text{escalatei}}(t)=\frac{D^{'}(t)}{\sum_{SP=1}^{4}10^{SP}} \tag{5}$$

Snort 手册中对攻击优先级的划分见表 5 第一列，攻击优先级值越低，表示威胁严重程度越高。

表 5　　攻击优先级赋值

Sig _ priority	D_{escalate}
1	0.9
2	0.09
3	0.009
4	0.000 9

(g) 路由器权限提升型威胁安全风险因子算法（算法 2）流程如图 4 所示。

图 4　路由器权限提升型威胁安全风险因子算法

在算法 2 中，首先利用 Snort 得到安全事件信息，然后根据路由器权限提升型威胁发生可能性流程图匹配 Snort 用户手册攻击优先级得到第 i 种威胁发生可能性 $P_{\text{escalatei}}$，结合 *Sig _ priority* 得到此种威胁严重程度，最后根据式(4)得到一次攻击中权限提升型威胁安全风险因子。

2.2　安全风险影响因子

定义 3　路由器安全风险影响因子。在充分考虑被攻击方的重要性对风险值影响基础上，把被攻击对象的权重称为安全风险影响因子。路由器重要性权重反映的是该路由器在网络中的重要程度，在本文中认为一个网络中路由器的重要程度主要和路由器在网络中的地位、流经路由器端口数据分组的加权转发量 2 个因素相关。

一个路由器单位时间内转发的数据字节数越多，表示路由器转发数据能力越强，其重要程度越高。这里，为了降低赋值过程的复杂度，假设数据分组的源主机及其上各项服务重要程度相同，即穿过路由器端口的单位长度报文重要性相同，制定表 6 所示的路由器端口流量重要性判断原则，其中交换容量越大，流量重要性越高。

表 6　　路由器流量重要性判断原则

序号	交换容量	流量重要程度	转发流量重要性赋值
1	[0,10 Mbit/s)	最低	2
2	[10 Mbit/s,100 Mbit/s)	非常低	3
3	[100 Mbit/s,1 Gbit/s)	低	4
4	[1 Gbit/s,10 Gbit/s)	中	5
5	[10 Gbit/s,40 Gbit/s)	高	6
6	[40 Gbit/s,100 Gbit/s)	非常高	7
7	[100 Gbit/s, ∞)	最高	8

路由器在网络中的地位也会对路由器安全风险系数产生重要影响，路由器地位越重要，路由器重要性权重越高，其在网络中地位具体赋值如表 7 所示。

表 7　　路由器在网络中地位赋值

路由器位置	重要程度	赋值
核心路由器，重要部位	非常高	9
核心路由器，非重要部位	高	7
边缘路由器，重要部位	较高	5
边缘路由器，非重要部位	中	3
其他	低	1

注：可以按照具体情况再增加，赋值在 1~10。

定义子网中路由器安全风险影响因子为

$$W = k_R \overline{v}_R + I_R \overline{v}_B \quad (k_R + I_R = 1) \tag{6}$$

其中，

1) $\overline{v}_R$、$\overline{v}_B$ 分别为路由器在网络中地位赋值和数据加权转发量重要性赋值，其中，$\overline{v}_R = \dfrac{v_R}{v_R + v_B}$，$\overline{v}_B = \dfrac{v_B}{v_R + v_B}$；

2) k_R、I_R 分别为路由器在网络中地位影响系数和路由器上数据加权转发量重要性影响系数赋值，基于网络安全管理人员的专家经验和对大量入侵事件的统计分析发现，路由器在网络中地位影响系数对路由器权重的影响较小。需要指出的是对于影响系数并没有固定的赋值，也没有统一的标准，网络安全管理人员的专家经验和具体的实验环境起着主要作用。

2.3　安全风险计算

根据GB/T20984-2007 对安全风险计算原理的阐述[23]，范式形式化为

$$value = R(A,T,V) = R(L(T,V),F(Ia,Va)) \tag{7}$$

其中，R 表示安全风险计算函数；A 表示资产；T 表示威胁；V 表示脆弱性；Ia 表示安全事件所作用的资产价值；Va 表示脆弱性严重程度；L 表示威胁利用资产的脆弱性导致安全事件的可能性；F 表示安全事件发生后造成的损失。结合国标安全风险计算的范式形式和 Snort 告警信息的相关特征，结合式(1)和式(6)，本文定义路由器安全风险计算表达为

$$R = WG \tag{8}$$

其中，W 为路由器安全风险影响因子；G 为路由器安全风险因子。整个量化算法流程如图 5 所示。

算法3 路由器安全威胁态势量化评估算法
输入：服务下降型威胁安全风险因子，权限提升型威胁安全风险因子，安全风险影响因子
输出：路由器安全态势值
BEGIN
1) For each router $R_1, R_2, \cdots, R_n$;
2) *Eve* =*audit*(*SolarWinds*, *Snort*); //简单网络管理协议的软件与IDS在线监测获取安全事件;
3) There is $G_{decline}$ from Algorithm 1;
There is $G_{escalate}$ from Algorithm 2;
$G = G_{escalate} + G_{decline}$ //路由器安全风险因子值;
4) Let W represent the security risk affecting factor which contain the weight of router($\overline{v}_R$) and the importance of traffic forwarded($\overline{v}_B$)
5) $W = k_R \overline{v}_R + I_R \overline{v}_B$ //计算路由器安全风险影响因子;
6) Let R represent the value of router security risk;
7) $R = G \times W$;//计算路由器安全态势值;
8) return 0
END

图 5　路由器安全威胁态势量化评估算法

算法 3 首先通过简单网络管理协议的软件和 IDS 在线监测得到安全事件信息；然后利用算法 1 和算法 2 得到路由器安全风险因子 G，再结合数据加权转发量和其在网络中地位得到安全风险影响因子 W；最后根据式(8)得到路由器安全风险值 R。

3　实验分析

下面详细介绍利用实验室环境和校园网数据进行的实验，以验证在线监测的路由器安全威胁态势量化评估方法的系统性和有效性。

3.1　实验 1

采用网络分析仪作为攻击端，模拟攻击和正常应用融合测试，对真实路由器进行实时攻击，同时部署 Snort 作为 NIDS 对整个网络系统进行实时入侵检测，并结合简单网络管理协议的软件 SolarWinds 获取路由器带宽占用率和 CPU 使用率等安全事件信息，以测试该评估方法的有效性和准确性，简化的网络拓扑如图 6 所示，目标路由器 Router 2 配置如下：操作系统为 Cisco IOS；版本号为 12.3；端口转发率为 100 Mbit/s，路由器带宽占用率阈值为 75%，即最大可用带宽为 153.6 kbit/s $\left(\dfrac{153.6 \times 1\,000 \times 512}{1\,024 \times 1\,024} = 75 \text{ Mbit/s}\right)$，已开启的服务进程为路由守护进程，RIPv1、RIPv2、BGP、HTTP、SNMP。目标路由器 Router 2 位于被攻击子网 LAN2 中，处于边缘路由器的非重要部位，Snort 作为 NIDS 产生的告警信息以及 SolarWinds 获得的安全事件信息作为路由器安全威胁评估的数据源存入数据中心，Router 2 上存在漏洞及相关信息如表 8 所示。为了提高不同攻击的对比性，假设路由器在遭受攻击前 1 min 内的流经路由器各端口数据加权流量相同，重要性为 2。

表 8　　目标路由器漏洞及相关信息

时间	CVE	运行服务	攻击数	平均 CPU 使用率	带宽占用率
8:00	CVE-1999-0111	{RIPv1}	10 000	63.1%	57 Mbit/s
10:00	CVE-1999-0111	{RIPv1}	100	35%	9.2 Mbit/s
12:00	CVE-2005-0068	{ICMP}	10 000	24.4%	6 Mbit/s
14:00	CVE-2002-1350	{BGP}	10 000	69.6%	78.9 Mbit/s
16:00	CVE-1999-0111	{RIPv1}	10 000	63.1%	57 Mbit/s
	CVE-2005-0290	{HTTP}	1		
18:00	CVE-2004-0714	{SNMP}	10 000	61%	56.2 Mbit/s

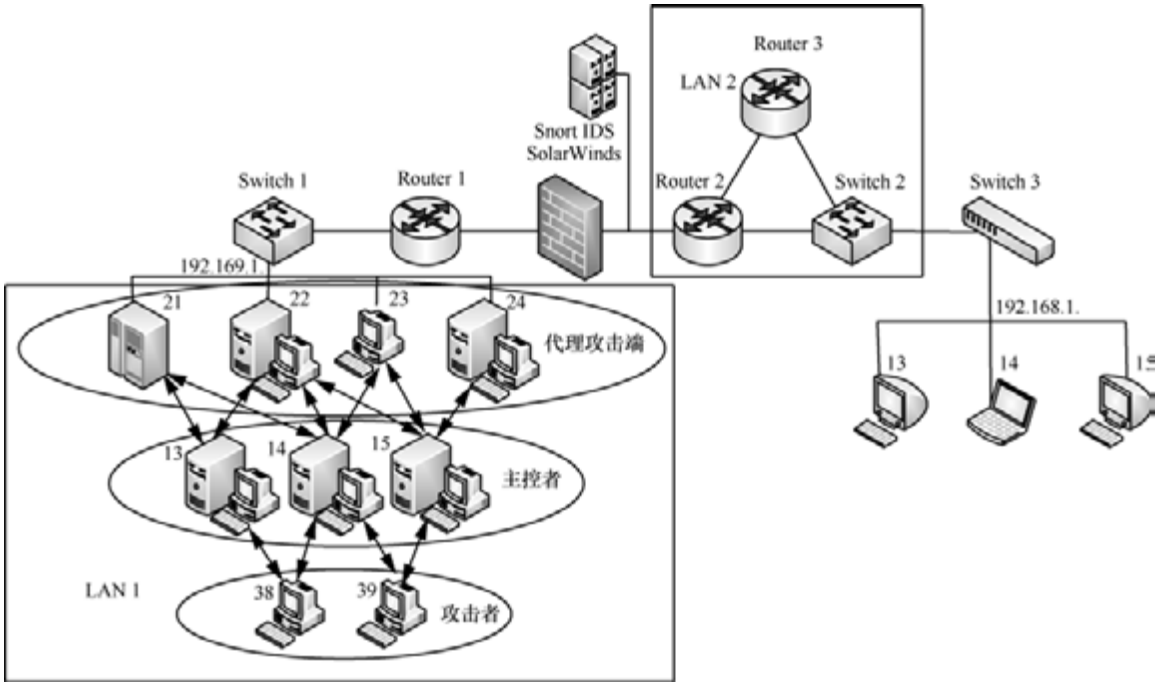


图 6　实验网络环境

利用第 2 节介绍的路由器安全风险评估计算方法，基于 Snort 和 SolarWinds 提供的相关入侵信息，分析图 6 所示的测试拓扑，得到如下实验结果。

1) 目标路由器(Router 2)安全威胁态势

图 7 直观地给出 Router 2 的安全威胁态势，结合入侵检测系统为系统管理员提供以下信息：（a）在 6:00~12:00 时间段内，路由器分别在 8:00、10:00 和 12:00 受到服务下降型攻击，8:00 和 10:00 为同一种攻击(CVE-1999-0111)，但由于攻击次数的原因造成 8:00 路由器风险值很大而 10:00 CPU 未达到临界条件仍正常工作，风险值为 0。12:00 由于 DDoS 攻击是针对 ICMP 服务进程，而目标路由器尚未开启此进程服务，故风险值为 0，提示系统管理员应当对 CVE-1999-0111 严加防范，调整安全策略;（b）14:00 路由器受到了攻击(CVE-2002-1350)，引起路由器带宽占用率急剧增加超过了 75%的阈值，应以路由器带宽占用率指标度量此攻击发生时的威胁;（c）16:00 在同 8:00 攻击相同的基础上增加了 1 次权限提升类攻击(CVE-2005-0290)，远程攻击者可使用 Hex 编码的 URL，如 HEX 编码的文件扩展名以绕过过滤检测，使此时风险值略高于 8:00;（d）8:00、12:00、14:00 和 18:00 遭受了相同次数的 DDoS 攻击，但风险值不同，说明拒绝服务攻击对路由器影响各不相同，其中 CVE-2002-1350 对目标路由器安全威胁最大，系统管理员应该及时判断，调整安全策略，以提高路由器的稳定性。

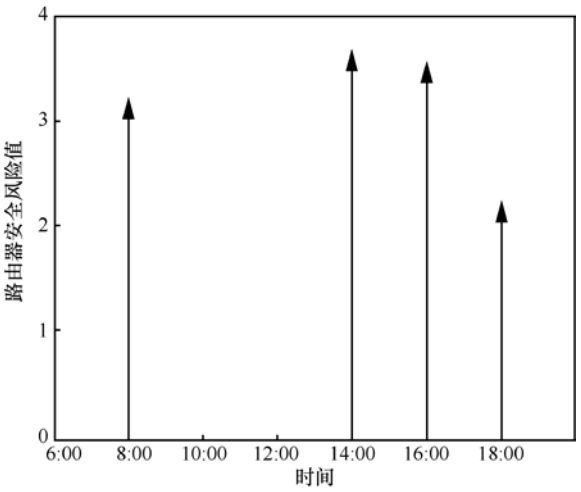


图 7　目标路由器安全威胁态势

2) 目标路由器(Router 2)CPU 威胁严重程度

图 8 给出了目标路由器从 6:00~18:00CPU 的使用率曲线，提供了以下信息：在 8:00, 14:00，16:00，18:00（路由器受到服务下降型攻击时刻）CPU 使用率陡然增长，超过了 60%的稳定性临界条件，其性能会急剧下降，应引起管理员高度重视，尽快分析系统日志，查找遭受攻击的相关信息。

3) 目标路由器(Router 2)带宽占用率

实验过程中，路由器带宽占用率的演化如图 9

所示。在 8:00、10:00、12:00、14:00、16:00、18:00 发起的 DDoS 攻击引起路由器带宽占用率增加，尤其是 14:00 发起的攻击(CVE-2002-1350)使路由器带宽占用率超过了阈值，这时路由器的带宽都用来处理攻击报文，而没有多余的带宽分配给正常的网络流量，使对正常业务产生了拒绝服务，这种攻击为带宽耗尽型攻击，致使 14:00 路由器安全风险最大，如图 7 所示。

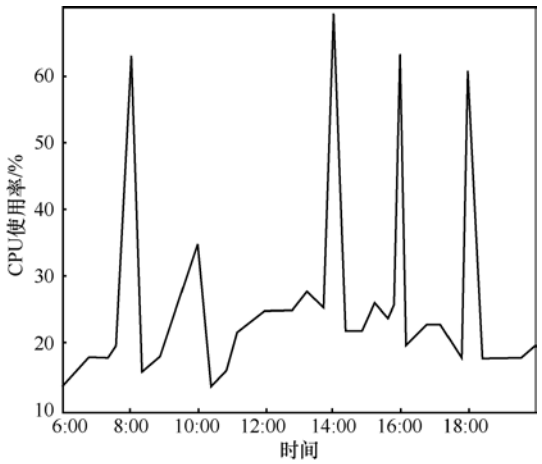


图 8　路由器的 CPU 使用率

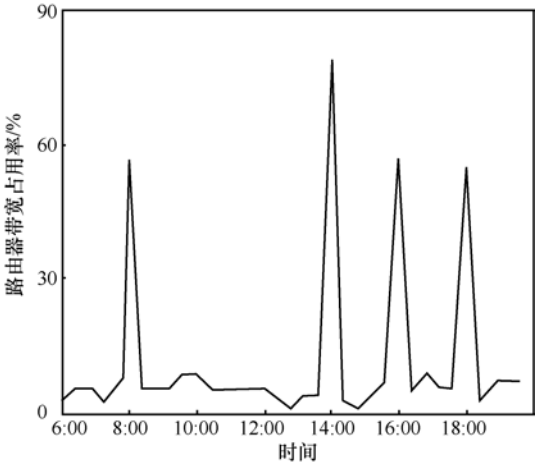


图 9　路由器带宽占用率

3.2　实验 2

以某学院校园网 2012 年 12 月份（1 日-23 日）数据为例进行安全威胁态势评估，分析这 23 天内目标路由器的安全威胁状态演化情况，该数据集包含扫描、针对路由协议的攻击和针对 ICMP 的安全漏洞的攻击等。该学院网络管理中心为本文提供了部分校园网的简化网络拓扑如图 10 所示。在 Router 1、Router 2 和 Router 3 分别布置 Snort 2.0.2, XJTU-Sensor 和

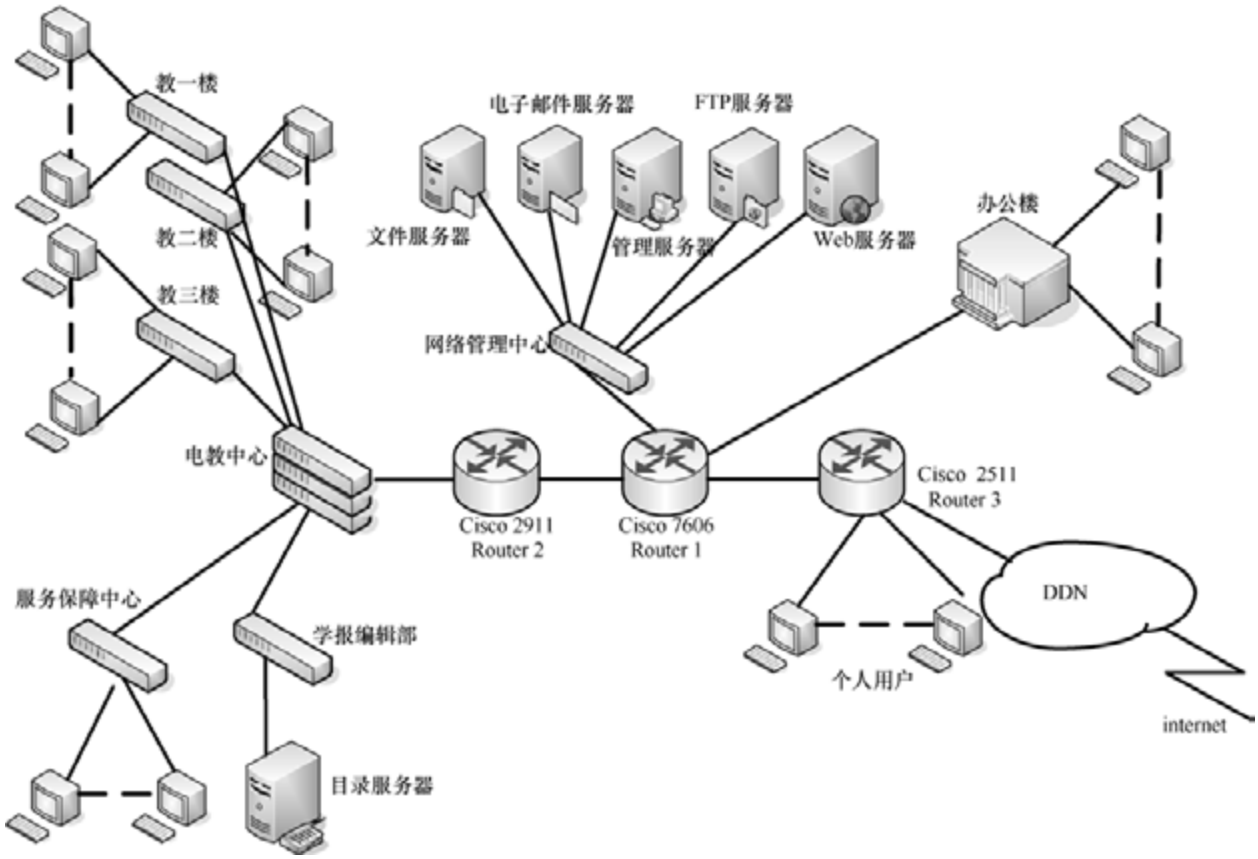


图 10　部分校园网络拓扑

Snort 2.6.0 并同时部署简单网络管理协议的软件 SolarWinds，每个 NIDS 和 SolarWinds 产生的入侵事件存入数据中心，作为在线监测的安全威胁态势评估数据源。3 个路由器的配置信息以及根据表 6、表 7 结合端口数据分组平均正常转发量的大小确定的各个路由器的重要性权重如表 9 所示。为了便于实时监测与统计分析，将 1 天分为上午（6:00~12:00）、下午(12:00~18:00)、晚上(18:00~24:00)和凌晨(0:00~6:00)4 个时段。

表 9　路由器配置信息及重要性权重

Router	路由器类型	软件版本信息	路由器重要性权重
Router 1 (core router)	Cisco 7606	Cisco IOS 12.1(10)E	0.78
Router 2 (edge router)	Cisco 2911	Cisco IOS 15.0(1)M	0.59
Router 3 (edge router)	Cisco 2511	Cisco IOS 12.0(2)T	0.21

实验时间长达 23 天，通过分析 NIDS 报警日志以及路由器资源的使用，利用第 2 节介绍的在线监测的路由器安全威胁态势量化评估计算方法，进一步获取各个时期路由器的安全威胁状况。分析结果如下。

1) 校园网部分拓扑中路由器的安全威胁态势(以路由器 Router 1、Router 2、Router 3 为例)图 11 给出图 10 该学院部分校园网中路由器 2012 年 12 月 1 日至 23 日的威胁态势，可以看出：（a）相比较于星期一至星期五，在周末（2 日、9 日、16 日和 23 日为星期日）前后各路由器（Router 1、Router 2 和 Router 3）均易受到攻击，提示系统管理员在周末前后对路由器的安全应该加倍重视。通过部署在各路由器上的 NIDS 和 SolarWinds 可以实时发现路由器正在遭受黑客攻击的种类并迅速采取相应的规避策略。由于路由器遭受的攻击种类繁多，本文仅举例进行说明。12 月 23 日 Router 1 风险值最大，通过 Snort 2.0.2 发现黑客利用 Router 1 上的 ICMP 安全漏洞使其耗用太多的资源相应 ICMP 不可达信息，造成路由器的 CPU 资源过载，管理员应当在接口上使用 no ip unreachables 命令解决这个问题，此外还可以使用 CAR(control access rate)限制 ICMP 数据分组流量速率。12 月 16 日上午通过监测发现黑客在利用 Cisco 路由器口令没有计数器功能的弱点，一次次的尝试登录口令，在口令字典等工具的帮助下试图破解登录口令，系统管理员可以通过用户模式密码、特权模式密码、会话超时等控制 console 口的安全还可以用访问列表限制远程登陆的用户;(b)相比于 Router 2(边缘路由器)和 Router 3(边缘路由器)，Router 1(核心路由器) 是连接网管中心与各教学楼、保障中心、编辑部、办公楼和个人用户的桥梁，其风险值较高，是黑客攻击的主要对象，管理员应当对 Router 1 提高警惕，实时监控其安全威胁状况。

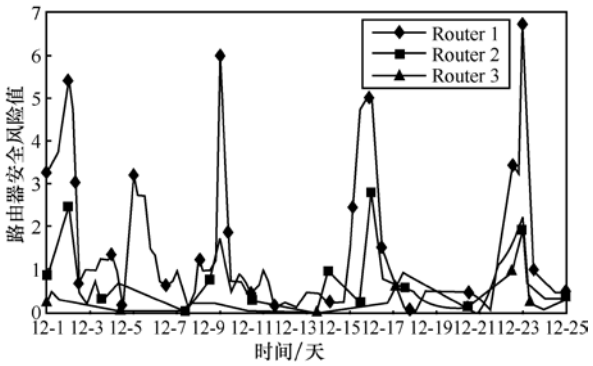


图 11　Router 1、Router 2、Router 3 的安全威胁态势

2) 目标路由器(Router 1、Router 2、Router 3) CPU 威胁严重程度

图 12 给出部分校园网 3 个路由器 CPU 使用率的演化情况：1) Router 3 在 12 月 1 日至 23 日期间，CPU 的使用率未超过 10%，通过 Snort 2.6.0 的实时监测发现其未受到过服务下降型攻击，Router 3 的 CPU 使用率曲线未出现短时间内陡升的情况，符合在线监测的结果，参考 2.1 节提到的 CPU 正常工作使用率(低于 60%), Router 3 的 CPU 转发性能良好；2) 相比于 Router 3，在 1 日至 23 日期间 Router 2 的 CPU 使用率最低值超过了 42%，参考 2.1 节提到的 CPU 正常工作使用率(低于 60%)，流经教学楼、电教中心、服务保障中心的数据量较大，Router 2 的 CPU 大部分时间处于正常工作状态但转发性能一般；3) 通过 Router 1 上部署的 Snort 2.0.2 和 SolarWinds 在线监测收集的数据发现其在 2 日、9 日、13 日、16 日和 23 日前后受到不同种类的 DDoS 攻击，结合 Router 1 的 CPU 使用率曲线可以看出，在 DDoS 攻击前后 CPU 使用率陡增，但很快恢复稳定，特别是 2 日、9 日、16 日和 23 日使用率超过了 60%，CPU 对数据分组的处理能力变慢。

3) 目标路由器(Router 1、Router 2、Router 3)的带宽占用率

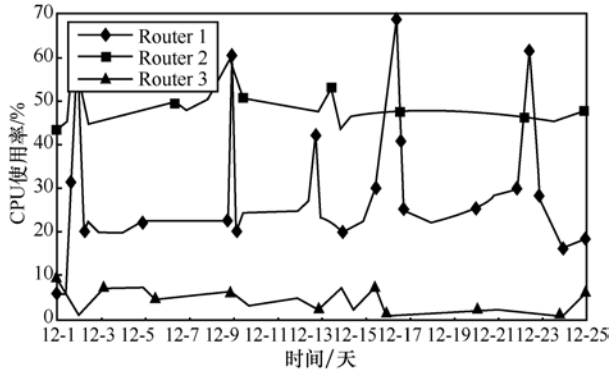


图 12　Router 1、Router 2、Router 3 的 CPU 使用率

12 月 1 日至 23 日在线监测过程中，各路由器带宽占用率的演化情况如图 13 所示。12 月 17 日前后 Router 1 带宽占用率迅速增加，超过了阈值，结合在线监测的数据发现导致带宽增加的 DDoS 攻击为带宽耗尽型攻击。

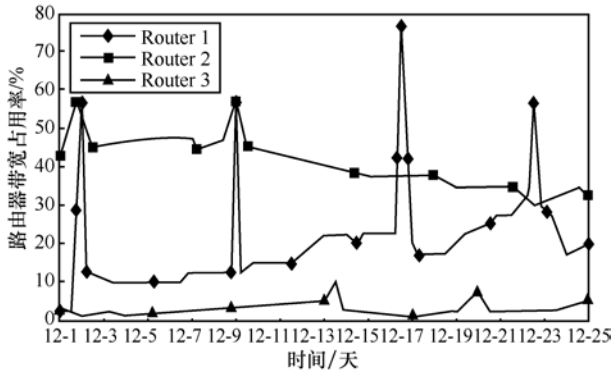


图 13　Router 1、Router 2、Router 3 的带宽占用率

4　结束语

以上实验表明：1) 提出的在线监测的路由器安全威胁态势评估方法具有合理性和准确性，权限提升类威胁的风险值与所受攻击的严重程度、发生可能性和路由器的重要性紧密相关；2) 结合路由器 CPU 使用率和路由器带宽占用率 2 个指标评估服务下降型威胁，使评估结果更加合理。本文仅对路由器安全风险评估进行了理论探讨和实验验证，下一步将扩大评估对象范围，引入交换机等其他网络设备，根据各自的特点进行安全威胁态势评估方法的研究。

参考文献：

[1] 龙门，夏靖波，张子阳等. 节点相关的隐马尔可夫模型的网络安全评估[J]. 北京邮电大学学报，2010, 33(6):121-124.
LONG M, XIA J B, ZHANG Z Y, *et al*. Network security assessment based on node correlated HMM[J]. Journal of Beijing University of Posts and Telecommunications, 2010, 33(6):121-124.

[2] 张保稳，罗铮，薛质等. 基于全局权限图的网络风险评估模型[J]. 上海交通大学学报，2010, 44(9):1197-1200.
ZHANG B W, LUO Z, XUE Z, *et al*. A network risk assessment model based on network global priviliege graph[J]. Journal of Shanghai Jiaotong University, 2010, 44(9):1197-1200.

[3] STIJN V C. Threat Modeling for Web Application Using the STRIDE Model[D]. London: Royal Holloway University of London, 2004.

[4] 付钰，吴晓平，叶清. 基于改进 FAHP-BN 的信息系统安全态势评估方法[J]. 通信学报, 2009, 30(9):135-140.
FU Y, WU X P, YE Q. Approach for information systems security situation evaluation using improved FAHP and Bayesian network[J]. Journal on Communications, 2009, 30(9):135-140.

[5] NGUYEN H V, CHOI Y. Proactive detection of DdoS attacks utilizing *k*-NN classifier in an anti-DDos framework[J]. International Journal of Electrical, 2010, 4(4):247-252.

[6] 谢柏林，余顺争. 基于应用层协议分析的应用层实时主动防御系统[J]. 计算机学报, 2011, 34(3): 452-463.
XIE B L, YU S Z. Application layer real-time proactive defense system based on application layer protocol analysis[J]. Chinese Journal of Computers, 2011, 34(3): 452-463.

[7] LI Z F. Using support vector machines to enhance the performance of Bayesian face recognition[J]. IEEE Transactions on Information Forensics and Security, 2007, 2(2):174-180.

[8] MCNAB C. Network Security Assessment[M]. New York: O'Reilley Media, Inc, 2007.

[9] 张永铮，方滨兴，迟悦. 计算机弱点数据库综述与评价[J]. 计算机科学, 2006, 33(8): 19-21.
ZHANG Y Z, FANG B X, CHI Y. Survey and evaluation on computer vulnerability database[J]. Computer Science, 2006, 33(8):19-21.

[10] 周亮，李俊娥，陆天波等. 信息系统漏洞风险定量评估模型研究[J]. 通信学报, 2009, 30(2): 71-76.
ZHOU L, LI J E, LU T B, *et al*. Research on quantitative assessment model on vulnerability risk for information system[J]. Journal on Communications, 2009, 30(2):71-76.

[11] KAMMERER R, FROMEL B, WASICEK A. Enhancing security in CAN systems using a star coupling router[A]. Proceedings of the 7th IEEE International Symposium on Industrial Embedded Systems[C]. Karlsruhe, Germany, 2012. 237-246.

[12] AL-IBRAHIM M, SAVSAR M, ADI W. A security analysis for label switching routers[A]. ACS/IEEE International Conference on Computer Systems and Applications[C]. Beirut, Lebanon, 2001. 525-529.

[13] WANG Z Q, ZHANG Y Q, LIU Q X. A research on vulnerability discovering for router protocols based on fuzzing[A]. 2012 7th International ICST Conference on Communications and Networking[C].

Kunming, China, 2012. 245-250.

[14] WU Y H, WU J P, XU K, *et al*. The design and implementation of router security subsystem based on IPSec[A]. 2002 IEEE Region 10 Conference on Compute4rs, Communications, Control and Power Engineering[C]. Beijing, China, 2002. 160-165.

[15] VARET A, LARRIEU N. Design and development of an embedded aeronautical router with security capabilities[A]. 2012 Integrated Communications Navigation and Surveillance[C]. Washington, USA, 2012. 1-14.

[16] ROCA A, FLICH J, SILLA F, *et al*. A latency-efficient router architecture for CMP systems[A]. 13th Euromicro Conference on Digital System Design Architectures, Methods and Tools[C]. Lille, France, 2010. 165-172.

[17] 桂宾. 路由器安全风险分析及规避策略[J]. 计算机安全, 2002, 6:16-18.
GUI B. Research on router security risk analysis[J]. Computer Security, 2002, 6:16-18.

[18] SCHUDEL G, SMITH D J. Router Security Strategies: Security IP Network Traffic Planes[M]. Cisco Press, 2008.

[19] QU G Z, PAKASH J, KISHORE R, *et al*. A framework for network vulnerability analysis[EB/OL]. http://www.ece.arizona.edu/~hpdc/projects/nvat/NV-framework.pdf, 2003.

[20] NTULI N, SUNYOUNG H. Detecting router cache snooping in named data networking[A]. 2012 International Conference on ICT Convergence[C]. Jeju Island, Korea, 2012. 714-718.

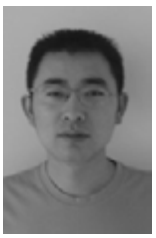
[21] HU N N, LI L, MAO Z M, *et al*. A measurement study of Internet bottlenecks[A]. INFOCOM 2005 24th Annual Joint Conference of the IEEE Computer and Communications Societies[C]. Miami, USA, 2005. 1689-1700.

[22] ROESCH M, GREEN C. Snort uses manual, snort release 2.0.0. 2003[EB/OL]. http://www.snort.org/docs/SnortUsersManual.pdf.

[23] GB/T 20984-2007. 信息安全技术信息安全风险评估规范[S]. 北京: 中国标准出版社, 2007.
GB/T 20984-2007. Information Technology Security Evaluation Criteria[S]. Beijing: China Zhijian Publishing House, 2007.

作者简介：

杨君刚（1973-），男，陕西宝鸡人，博士，西安通信学院副教授、硕士生导师，主要研究方向为网络与系统安全。



梁礼（1983-），男，河北保定人，西安通信学院硕士生，主要研究方向为计算机网络安全检测与评估。

刘故箐（1974-），女，重庆人，西安通信学院讲师，主要研究方向为计算机网络安全漏洞评估。

张倩（1976-），女，陕西西安人，西安通信学院讲师，主要研究方向为系统优化与调度。

张长青（1986-），男，陕西眉县人，西安通信学院硕士生，主要研究方向为人工智能和网络安全。