软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2011,22(4):761−772 [doi: 10.3724/SP.J.1001.2011.03818]

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

IMS 网络中的 SIP 洪泛攻击检测*

王尚广+, 孙其博, 杨放春

(北京邮电大学 网络与交换技术国家重点实验室,北京 100876)

Detecting SIP Flooding Attacks Against IMS Network

WANG Shang-Guang+, SUN Qi-Bo, YANG Fang-Chun

(State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China)

+ Corresponding author: E-mail: sguang.wang@gmail.com, http://www.bupt.edu.cn

Wang SG, Sun QB, Yang FC. Detecting SIP flooding attacks against IMS network. *Journal of Software*, 2011,22(4):761−772. http://www.jos.org.cn/1000-9825/3818.htm

Abstract: To detect the SIP (session initiation protocol) flooding attack against the IP Multimedia Subsystem of 3G core network, this study proposes a double sampling and a variable sampling interval detection approach. Based on the Counting Bloom Filter for the statistical detection of characteristic information, this approach divides the detection space into five areas, namely, the normal range, interesting range, detection range, precise detection range, and attack range, and detects the statistic data falling in each of the different ranges. Simulation experimental results show that this approach has a good detection performance.

Key words: IP multimedia subsystem; session initiation protocol; counting Bloom filter; double sampling and variable sampling interval

摘 要: 为了检测针对 3G 核心网中 IP 多媒体子系统的 SIP(session initiation protocol)洪泛攻击,提出了一种双抽样多点检测方法.该方法在使用计数式布鲁姆过滤器统计检测特征信息的基础上,将检测空间划分为 5 个范围,即正常范围、关注范围、检测范围、精检测范围和攻击范围,然后对落在不同范围内的统计信息给予相应的检测.仿真实验结果表明,该方法具有较好的检测性能.

关键词: IP 多媒体子系统;会话初始协议;计数式布鲁姆过滤器;双抽样与变抽样间隔

中图法分类号: TP393 **文献标识码**: A

IMS(IP multimedia subsystem)是第三代移动通信伙伴组织(3rd Generation Partnership Project,简称 3GPP)在 Release5 版本标准中提出来的支持 IP 多媒体业务的子系统,位于 3G 核心网中,利用全 IP 网络负责 3G 系统中的多媒体通信.它通过由会话发起协议(session initiation protocol,简称 SIP)提供的会话发起能力,建立起端到端的会话,使用 SIP 呼叫控制机制来创建、管理和终结各种类型的多媒体业务,并获得所需要的服务质量.IMS 实

* 基金项目: 国家自然科学基金(60672121); 国家自然科学基金创新研究群体科学基金(60821001); 国家重点基础研究发展计划(973)(2009CB320406); 国家高技术研究发展计划(863)(2006AA01Z448); 国家教育部科学技术研究重点项目(108013); 国家 242 信息安全计划项目(2007A14)

收稿时间: 2009-05-05; 定稿时间: 2010-01-05

现了控制功能和承载能力的分离、呼叫和会话的分离,其终端可以通过不同的接入方式,接入到分组域核心网(WCDMA,CDMA2000,TD-SCDMA 和固定网络等),由 PS(packet switched)提供 SIP 信令和媒体数据的承载,IMS 的核心部分提供会话和业务的控制.IMS 为未来的多媒体数据业务提供了一个通用平台,它是传统电信网与 Internet 业务融合的重要一步,顺应了网络融合发展的趋势.

SIP 协议被用来描述生成、修改和终结一个或多个参与者之间的会话[1],是由 IETF 于 1999 年提出来的一个基于 IP 网络中实现实时通信应用的一种控制协议.它打破了传统电信业务的传输模式,采用基于 Internet 的准则,将蜂窝系统与 Internet 应用融合在一起提供基于 IP 的多媒体业务,3GPP 已将 SIP 作为第三代移动通信系统(3G)多媒体域的信令协议[2].SIP 具有开放性、可扩展性、安全性的特点,然而,SIP 协议也面临着各种各样的安全威胁[3−5].虽然 3GPP,ITU-T 等标准化组织为基于 SIP 协议的 IMS 网络制定了多种安全技术和保护机制,但却没有提出针对 IMS 网络 SIP 洪泛攻击的任何安全机制.

SIP 洪泛攻击是攻击者通过 SIP 终端(计算机、手机等)向 IMS 网络中的 P-CSCF(proxy-session control function)服务器发送大量无用的 SIP(信令)消息,导致服务器辖属用户都无法建立任何呼叫,造成拒绝服务攻击.由于 3G 支持多种接入机制,攻击者可以通过具有移动性的非法 SIP 终端发起攻击,使攻击具有移动性、跨区域性、跨网络性,导致检测和防御更加困难.可以预见,随着 IMS 被全球电信运营商逐渐部署到实际网络中,SIP 洪泛攻击将成为管理者和电信运营商面临的严重安全威胁.

但是,对于 IMS 网络中的 SIP 安全性问题,目前尚未有令人满意的研究成果.文献[6]为了检测 IMS 网络中两种最主要的 SIP 洪泛攻击:INVITE 消息洪泛攻击和 REGISTER 消息洪泛攻击,以检测 INVITE 消息洪泛攻击为例,首先求出某个抽样间隔内所有 INVITE 的消息数量与该抽样间隔以前的所有 INVITE 消息的平均数量的比值,然后减去一个设定的阈值,最后使用 Cumulative Sums(CUSUM)算法进行累积.但该方法存在缺点,由于仅仅根据 INVITE 数量的多少来确定是否发生攻击,而没有考虑网络中正常的呼叫激增,将无法区分正常流量和攻击流量,从而导致误报较高.文献[7]将 IMS 网络中会话功能实体 CPU 的利用率作为检测特征,如果利用率超过设定的阈值,表明遭到 SIP 洪泛攻击.该方法虽然简单,但存在以下两个缺点:其一,攻击者可以通过手工构造攻击数据包,在保持 CPU 利用率低于设定阈值的情况下发动攻击,因此,上述检测方法将失效;其二,该方法无法区分瞬间拥塞与洪泛攻击,导致误报.文献[8]提出了一种基于人工免疫系统算法的检测框架,用于检测 IMS 网络中的 SIP 洪泛攻击,并将其检测性能与基于特征的检测算法进行了比较.该方法的缺点是不能在攻击的早期阶段检测到攻击,导致检测时间过长.文献[9]将 Internet 中洪泛攻击检测常用的 3 种算法,即门限值算法、CUSUM 算法和 Hellinger 距离算法用于 IMS 网络中 SIP 洪泛攻击的检测,并对 3 种算法的性能进行比较.文献[10]针对 IMS 网络中的移动多媒体通信面临的与 SIP,RTP,IP 有关的 DoS 攻击进行了分析,并在 IMS 已有的标准安全机制的基础上提出一种安全体系架构机制,用来为客户和服务提供商提供和保护可靠的通信环境.文献[11]通过建立 SIP 有限状态机来检测 DoS 攻击,该方法对 SIP 事务处理机制原有的 RFC 3261 有限状态机 FSM(finite state machine)进行修改,使其能够检测异常消息.其原理是对进入系统中的所有 SIP 消息的会话 ID(session ID)进行检测,对于新的 ID,如果是请求消息,则记录为正常消息,否则,记录为错误消息;对于已有的 ID,如果能够更新系统中存储的状态表(state table),则记录为正常消息,否则,记录为错误消息.然后统计所有错误消息的数量,如果大于设定的阈值,表明系统遭到攻击.该方法的缺点是不能对伪造的 SIP 消息给予有效的识别和检测,导致检测率较低.文献[12]提出一个在线统计检测系统 vFDS,通过 Hellinger 距离计算正常流量和洪泛攻击流量下的 SIP 协议的概率测度以判断是否为洪泛攻击行为.该方法的缺点是对低密度攻击的检测效果较差.另外,如果采集到的训练数据集中包含洪泛攻击数据包,则该方法会出现大量的漏报.与文献[11]相似,文献[13]使用一个 SIP 有限状态机模型来检测那些偏离正常操作的洪泛攻击行为,并通过与防火墙的通信来阻止 SIP 洪泛流量,使服务器在受到攻击的情况下仍能正常提供服务.文献[14]分析了 IMS 网络所面临的潜在攻击,指出 IMS 网络安全的核心是防止 P-CSCF 服务器遭受 DoS 攻击.基于此,文献[14]提出一个基于 *K*-Nearest Neighbor(KNN)分类算法的入侵检测系统.其缺点是,当检测的样本不平衡时,导致误报率增加.另外,由于需要计算到全体已知样本的距离,计算机资源消耗较大.

针对上述分析,为了高效、准确地检测出 IMS 网络中面临的最严重威胁:SIP 洪泛攻击[7],我们提出一种新的 SIP 洪泛攻击的检测方法.本文以 SIP 洪泛攻击中的 REGSITER 消息洪泛攻击为例,对 REGSITER 消息流进行分析,将抽样间隔内进入 IMS 网络中所有初始 REGISTER 请求消息的数量与正常(信令)消息流数量的差作为检测特征,使用 Counting Bloom Filter(CBF)统计上述差值,然后使用本文提出的双抽样多点检测(double sampling and multi-point detection,简称 DSMD)算法进行检测.DSMD 算法借鉴双抽样与变抽样间隔(double sampling and variable sampling interval,简称 DSVSI)控制图将检测空间划分为 5 个范围,即正常范围、关注范围、检测范围、精检测范围和攻击范围,其中,检测范围和精检测范围内包含浅度检测和深度检测,然后对落在不同范围内的数据给予相应的检测.

为了验证本文提出的方法,我们搭建了仿真实验环境,包括 IMS 网络、攻击工具以及 IMS 客户端,并在 IMS 网络上运行 201 拨号业务.另外,将本文提出的检测方法开发出原型检测系统并将其部署到实验环境中.通过源端和受害端的检测结果表明,该方法具有较好的检测性能.

本文第 1 节介绍 SIP 洪泛攻击.第 2 节阐述 SIP 洪泛攻击的检测方法.第 3 节对检测方法进行仿真实验.第 4 节给出全文总结.

1 SIP 洪泛攻击

从文献[15]可以看出,3GPP 为基于 SIP 协议的 IMS 网络制定了多种安全技术和保护机制,比如加密、认证和安全传输等,使其抵御注册劫持(registration hijacking)、中间人(man-in-the-middle)、密码猜测攻击(password guessing attack)和窃听(eavesdropping)等攻击[7].但由于 IP 网络的先天脆弱性,在现有 IMS 安全架构体系下,互联网上常见的洪泛攻击将会进入 IMS 网络,使 IMS 网络面临潜在的攻击.但是,3GPP 并没有提出针对 IMS 网络洪泛攻击的任何安全机制,导致洪泛攻击成为 IMS 网络面临的最严重威胁.

IMS 网路面临的洪泛攻击主要分为 3 类;TCP/SYN 洪泛攻击、Smurf 攻击和 SIP 洪泛攻击,其中,SIP 洪泛攻击是 IMS 网络所面临的最严重的潜在攻击[7].因此,本文重点研究 IMS 网络中 SIP 洪泛攻击的检测方法.SIP 洪泛攻击主要分为 INVITE 消息洪泛攻击和 REGISTER 消息洪泛攻击[6,7].由于 INVITE 消息洪泛攻击与 REGISTER 消息洪泛攻击相似,因此,本文以 REGISTER 消息洪泛攻击为例来研究 SIP 洪泛攻击的检测方法.

1.1 REGSITER消息洪泛攻击

在正常情况下,IMS 网络中 REGISTER 消息流如图 1 所示,终端在发现 IMS 网络中的 P-CSCF 地址后,构造初始 REGISTER 请求消息向其发送,IMS 网络经过处理后,通过 P-CSCF 发送该 401 Unauthorized 响应到终端,终端根据响应消息 nonce 头中的值和自己的密钥计算一个响应值 response,通过新的 REGISTER 请求发送给 IMS 网络中的 P-CSCF,IMS 网络通过认证向量值比较,如果匹配,则通过该用户认证并返回一个 200 OK 响应.在此后的过程中,终端在 expire 值规定的时间即将到期时,将再次发送重注册 REGISTER 消息进行重注册,并将 expire 头设为 0.IMS 在收到该 REGISTER 消息后,向终端发出 200(OK)响应.

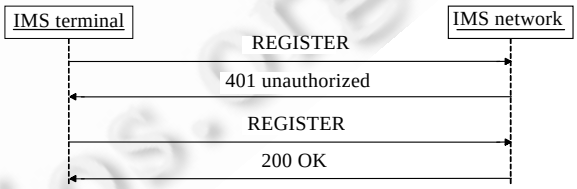


Fig.1 Normal REGISTER message flow

图 1 REGISTER 正常消息流

在攻击情况下,攻击者向攻击 IMS 网络发送大量的 REGISTER 消息,如图 2 所示.该消息可能是伪造消息,其中某个攻击消息流如图 3(a)所示;可能是 IMS 网络无法识别用户,其中某个攻击消息流如图 3(b)所示;或者包含大量被盗用户 URL,其中某个攻击消息流如图 3(c)所示.将导致被攻击服务器忙于处理,耗尽网络或信令资源而无法为合法的正常用户提供服务.

SIP REGISTER 洪泛攻击看似简单,但防御起来相当困难:一方面,这种攻击使用的数据包都是正常数据包,正常网络服务都不会禁止该类型数据包;另一方面,攻击者使用伪造或欺骗的源地址(比如 SIP URL)而使攻击主机无从追查,这使得对它的检测和阻断都变得十分困难,如图 3(a)所示.另外,由于攻击具有移动性、跨网络性,

这是传统的互联网洪泛攻击所不具有的,从而导致对它的检测和防御更加困难.

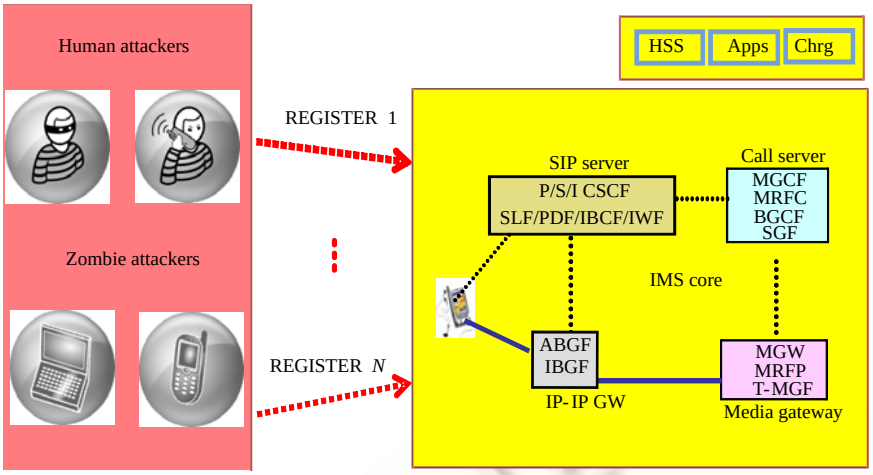


Fig.2 REGISTER message flooding attack

图 2 REGISTER 消息洪泛攻击

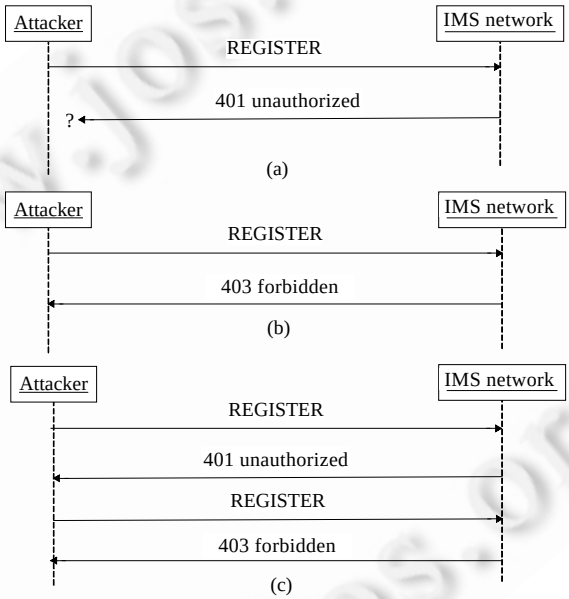


Fig.3 Message flow of the REGISTER attack

图 3 REGISTER 攻击消息流

1.2 检测特征

比较图 1 和图 3 中的 REGISTER 消息流可以发现,在正常情况下,终端和 IMS 网络将形成一个(REGESTER, 200 OK)消息流,其中,REGISTER 是初始注册消息,并且,消息流中所有消息都有相同的 Call-ID,From tag 和 To tag.基于此,为便于提取 SIP 洪泛攻击的检测特征,给出正常消息流定义:

定义 1. 在 SIP 事务处理时间内,REGISTER 的正常消息流是一个二元组(X,Y),它满足:

- X:={401 *Unauthorized*}是 IMS 中 401 Unauthorized 响应消息的集合;

- *Y*:={200 *OK*}是 IMS 注册成功响应消息的集合;
- s.t.*X.attribute*=*Y.attribute*,*attribute*:={*Call-ID*,*From tag*,*To tag*}.

如果在同一个会话中检测出符合定义 1 的消息流,可以判定该会话正常建立,属于正常消息.当然,也可能存在个别正常用户在注册时,由于误操作(比如,用户名或密码输入错误)导致(REGESTER,403 Forbidden)或(REGESTER,401 Unauthorized,REGESTER,403 Forbidden)消息流,会被认为是攻击消息流,对消息流的判断产生干扰.但由于其数量较低,与网络中的正常消息流的数量相比,基本可以忽略不计,本文将其当作背景噪声.

令 $T_{register}(n)$代表第 $n(n=1,2,\ldots)$个抽样间隔在 IMS 网络中监测到的所有 401 Unauthorized 响应消息的总数,即集合 *X*:={401 *Unauthorized*}的总数;$S_{register}(n)$代表该时间段内监测到的满足定义 1 的正常消息流的总数.设 X_n 为第 *n* 个抽样间隔内在 IMS 网络中监测到的 $T_{register}(n)$与 $S_{register}(n)$的数量差,即

$$X_n=T_{register}(n)-S_{register}(n),\ n=1,2,\ldots \tag{1}$$

在 IMS 网络正常运行时,IMS 网络中所有的 401 Unauthorized 响应消息都包含在正常消息流中,所以,其数量是基本相等的,即 X_n 的值将趋近于 0.而在 REGESTER 消息洪泛攻击下,网络中大量的 401 Unauthorized 响应消息由于不满足定义 1 而不包含在正常消息流中,所以 $T_{register}(n)$与 $S_{register}(n)$的数量明显偏离正常情况下的对应关系,$T_{register}(n)$与 $S_{register}(n)$的差值迅速增大,$X_n>>0$,将发生突变.本文所提洪泛攻击检测机制的主要思想是,通过监控 X_n 作为洪泛攻击的检测特征来判断该网络是否正在接收异常的 REGISTER 消息.

1.3 数据处理

Bloom Filter[16]是用于判断一个元素是否在集合里的一种数据结构,早期用在磁盘访问控制上,后来被广泛用于拼写检查和数据库系统中.近年来,Bloom Filter 被广泛应用在 DDoS 检测上[17−20].

最基本的 Bloom Filter 是由一个具有 *m* 位的向量 *V* 组成,每一位的初始值设为 0.为了表达 $S=\{x_1,x_2,\ldots,x_n\}$集合中的 *n* 个元素,Bloom Filter 使用 *k* 个相互独立的 Hash 函数 $h_1,h_2,\ldots,h_k$,它们分别将集合中的每个元素映射到{0,…,*m*−1}的向量 *V* 中.对任意一个元素 $x\in S$,第 *i* 个 Hash 函数映射的位置 $h_i(x)$就会被置为 1($1\leqslant i\leqslant k$),如图 4 所示.在判断 *y* 是否属于 *S* 时,对 *y* 使用 *k* 次 Hash 函数,如果所有 $h_i(y)$的位置都是 1($1\leqslant i\leqslant k$),则说明 $y\in S$,否则说明 $y\notin S$.如图 5 所示,当 *k*=3 时,y_1 不是该集合中的元素,y_2 属于该集合.

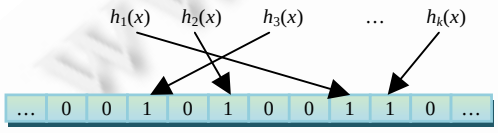


Fig.4 Bloom Filter mapping

图 4 Bloom Filter 的映射

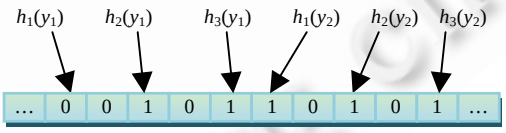


Fig.5 Bloom Filter' element query

图 5 Bloom Filter 中的元素查询

可以看出,Bloom Filter 的实质是将集合中的元素通过 *k* 个哈希函数映射到 *m* 位向量 *V* 中,对于集合中每一个元素只需保存几个比特位[21].Bloom Filters 是一种支持集合查询的高效、简洁的数据结构,Hash 碰撞带来的误报率通过合适参数的选取基本可以忽略,因此,它在增加或查找集合元素时所用的时间几乎完全恒定.但是,Bloom Filter 只支持插入和查找两种操作.为了解决 Bloom Filter 不支持删除操作的问题,Counting Bloom Filter[22]被设计出来.它将 Bloom Filter 位数组的每一位扩展为一个小的计数器(counter),在插入元素时给对应的 *k* 个(*k* 为 Hash 函数个数)Counter 的值分别加 1,删除元素时给对应的 *k* 个 Counter 的值分别减 1,如图 6 所示.

根据第 1.2 节分析的 REGISTER 消息流中 $T_{register}(n)$与 $S_{register}(n)$的对应关系,正常情况下,$T_{register}(n)$与 $S_{register}(n)$的数值基本一致.与文献[20]相似,本文使用 Counting Bloom Filter 来处理上述对应关系.当在第 *n* 个抽样间隔内监测到 401 Unauthorized 响应消息时,$T_{register}(n)$的数量有所增加,同时提取其消息头域值 *attribute*:={*Call-ID*,*From tag*,*To tag*},并将其插入 Counting Bloom Filter 中.当监测到 200 OK 消息时,也提取其头域值,并查询 Counting Bloom Filter,如果查询成功,则 $S_{register}(n)$的数量有所增加,并将其从 Counting Bloom Filter 删除;如果查询失败,则 $S_{register}(n)$数量保持不变.当达到时间,最终在每个抽样间隔内准确地统计出 X_n 的值.

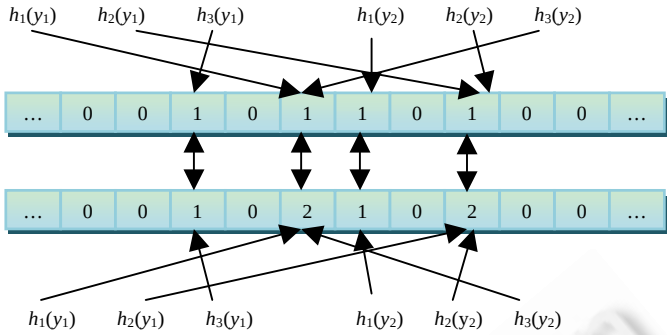


Fig.6 Counting Bloom Filter' counting

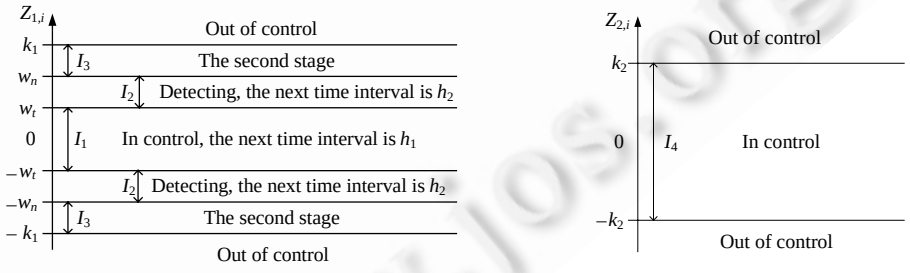
图 6 Counting Bloom Filter 中的计数

2 SIP 洪泛攻击

2.1 DSVSI控制图

控制图主要用于监测生产过程是否处于控制状态,它是统计质量管理的一种重要手段和工具,以保证生产过程中产品质量的稳定性.Carot[23]提出双抽样与变抽样间隔(double sampling and variable sampling interval,简称 DSVSI)控制图,结合了 DS 控制图[24]与 VSI 控制图[25]的优点,提高了对微小偏移变动的监测能力以及减少抽样的样本数,并且控制图的设置、计算与修哈特控制图一样简单、容易.DSVSI 算法有(n_1,n_2),(h_1,h_2),(w_n,w_t),(k_1,k_2)共 8 个参数.n_1,n_2 分别代表第 1 阶段和第 2 阶段抽样的样本数;h_1,h_2 分别代表松、紧抽样间隔;w_n,w_t 分别为进行第 2 次抽样样本数和抽样间隔的控制线;k_1,k_2 分别代表第 1 阶段和第 2 阶段的控制线.

DSVSI 的检测原理如图 7 所示.先抽取 n_1 个样本,并计算出平均数 $\bar{X}_{1,i}$,再将平均数作标准化得到 $Z_{1,i}=\sqrt{n_1}(\bar{X}_{1,i}-\mu_0)/\sigma$;如果 $Z_{1,i}$ 落在区域 $I_1=[-w_t,w_t]$内,则判定为生产过程是可控的且下次抽样间隔时间仍是 h_1;如果 $Z_{1,i}$ 落在区域 $I_1=[-w_t,w_t]$外和区域 $I_2=[-w_n,w_n]$之内,判定为生产过程是在检测之内且下次抽样间隔时间变更为 h_2;如果 $Z_{1,i}>k_1$ 或者 $Z_{1,i}<-k_1$,则表明失控,如果 $Z_{1,i}$ 落在区域 $I_3=[-k_1,-w_n]\cup(w_n,k_1)$之内,则需进行第 2 阶段的抽样;在第 2 次抽样时增加 n_2 个样本,计算出 n_1,n_2 两次抽样的总平均数 $\bar{Y}_i=(n_1\bar{X}_{1,i}+n_2\bar{X}_{2,i})/(n_1+n_2)$,再将其标准化得到 $Z_{2,i}=\sqrt{n_1+n_2}(\bar{Y}_i-\mu_0)/\sigma$, 如果 $Z_{2,i}$ 落在区域 $I_4=[-k_2,k_2]$,则判定生产过程为可控,否则,判定为失控.



(a) Control chart of the first stage

(a) 第 1 阶段控制图

(b) Control chart of the second stage

(b) 第 2 阶段控制图

Fig.7 DSVSI control chart

图 7 DSVSI 控制图

2.2 DSMD算法

从 DSVSI 控制图的原理可以看出,DSVSI 控制图用于工业生产过程中的质量监控.这与网络流量中的特定

流量监控具有相似之处,即对于监控目标的偏移都具有敏感性,因此可以将其借鉴到对 IMS 流量中 SIP 洪泛攻击流量的检测.基于此,本文在 DSVSI 算法的基础上结合洪泛攻击检测的需要,提出双抽样多点检测算法(DSMD).首先,DSMD 考虑到网络流量监测主要检测正向的突变,所以丢弃 DSVSI 中对负值偏移的监测,即仅仅考虑 8 个参数中的 4 个正值参数;其次,与 DSVSI 不同,DSMD 将检测范围细分为正常范围、关注范围、检测范围、精检测范围和攻击范围;最后,对落在检测范围和精检测范围内的 $X_{counter}(n)$进行细粒度检测,即浅度检测和深度检测,如图 8 所示.

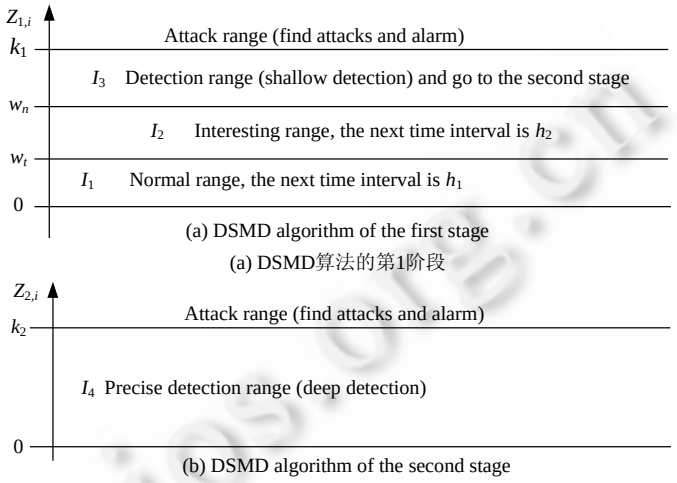


Fig.8 DSMD algorithm

图 8 DSMD 算法

在检测洪泛攻击时,通过 CBF 得到 IMS 网络中第 n 个抽样间隔的 $X_{counter}(n)$.在理想情况下,由于 $T_{register}(n)$与 $S_{register}(n)$所存在的对应关系,CBF 中 counter 保持不变,$X_{counter}(n)$为 0,并且每隔一个抽样时间,counter 进行重置.而在实际网络中,网络上偶尔的拥塞、数据包出现丢失或者其他错误,使得抽样时间内 counter 非 0,假设 $X_{counter}(n)$服从正态分布 $N(u_0,\sigma^2)$.在正常情况下,$X_{counter}(n)$的均值为 u_0;发生洪泛攻击时,$X_{counter}(n)$的均值发生偏移,偏移量 $\delta=\dfrac{u_1-u_0}{\sigma}(\delta>0)$,偏移值 $u_1=u_0+\delta\sigma$.对于 u_1,本文将通过 DSMD 给予检测.

DSMD 在初始条件下,算法运行在第 1 阶段,选取初始序列为 0 的$\{Y_j,j=1,2,\ldots,n\}$作为报警序列,如果检测到攻击,则$\{Y_j,j=1,2,\ldots,n\}=1$,否则,$\{Y_j,j=1,2,\ldots,n\}=0$.首先选取 h_1 作为 DSMD 的抽样间隔,以 CBF 处理过的 $X_{counter}(n)$值作为抽样间隔 h_1 内的检测样本,然后连续选择 n_1 个检测样本 $X_{1,i}$,其中,$X_{1,i}=\{X_{counter}(n)\}(i=1,2,\ldots,n_1)$.计算出 n_1 个样本的均值 $\bar{X}_{1,i}$,再将其作标准化,得到 $Z_{1,i}=\sqrt{n_1}(\bar{X}_{1,i}-\mu_0)/\sigma$. 如果 $Z_{1,i}\leqslant w_t$,则判定为网络在正常范围内(normal range)运行,且下一次抽样间隔仍是 h_1;如果 $w_t<Z_{1,i}\leqslant w_n$,则判定网络是在关注范围内(interesting range)运行,下一次抽样间隔变为 h_2;如果 $Z_{1,i}>k_1$,则判定遭到攻击(attack range),令$\{Y_j,j=j+\inf\{i,Z_{1,i}>k_1\}\}=1$;如果 $w_n<Z_{1,i}\leqslant k_1$,则该网络是在检测范围内(detection range)运行,进行浅度检测(shallow detection);如果 $X_{1,i}>(\alpha+1)\mu_0$,并且 $\sum_{i=1}^{n_1}1\{X_{1,i}>(\alpha+1)\mu_0\}\geqslant K$,则检测到攻击,令$\{Y_j,j=j+\sup\{i,X_{1,i}>(\alpha+1)\mu_0\}\}=1$,其中,$\alpha$表示攻击过程中均值增长的一个阶跃,$K(K>1)$表示在检测时间间隔内可能存在攻击的数量,否则进入第 2 阶段.

在第 2 阶段,抽样间隔变为 h_2,同时增加 n_2 个样本 $X_{2,i}$,其中,$X_{2,i}=\{X_{counter}(n)\}(i=1,2,\ldots,n_2)$,并计算出两次抽样的总平均数 $\bar{Y}_i=(n_1\bar{X}_{1,i}+n_2\bar{X}_{2,i})/(n_1+n_2)$,再将两次抽样的总平均数作标准化,得到 $Z_{2,i}=\sqrt{n_1+n_2}(\bar{Y}_i-\mu_0)/\sigma$. 如果 $Z_{2,i}>k_2$,则判定遭到攻击,否则,判定网络在精检测范围内(precise detection range)运行,进行深度检测.在深度检

测(deep detection)过程中,如果 $X_{2,i}>(\alpha+1)\mu_0$,并且 $\sum_{i=1}^{n_2}1\{X_{2,i}>(\alpha+1)\mu_0\}\geqslant K$,则判定遭到攻击,令$\{Y_j,j=j+b\times\sup\{i, X_{2,i}>(\alpha+1)\mu_0\}\}=1$,否则,返回到第 1 阶段继续运行.

3 仿真实验

我们在仿真实验中,以攻击运行 201 拨号业务的 IMS 网络来对本文方法进行验证.由于没有公用的 SIP 流量数据,与文献[9,14]类似,我们也通过搭建实验平台运行模拟业务来产生 SIP 流量.首先搭建 IMS 网络:使用 OpenIMSCore(subversion-1.6.0.tar.gz)仿真 IMS 网络,OpenIMSCore 是一个 IMS 测试平台,是 IMS 核心网元的实现,包括 P-CSCF,S-CSCF,I-CSCF 和 HSS,可以通过普通 SIP 终端接入 IMS 网络[26].OpenIMSCore 部署在 4 台计算机上(操作系统为 Ubuntu 8.04,内存为 521MB,CPU 为奔腾 3.0GHz,其他计算机配置均与此相同),如图 9 所示;其次,开发出一个简化的 IMS 网络 SIP 洪泛攻击检测系统(SIP-DS):使用 Snort(snort-2.8.3.2.tar.gz),Libosip (libosip2-2.0.6)SIP 协议栈和 BCF 获得检测数据,然后通过 DSMD 算法检测 SIP 洪泛攻击.SIP-DS 系统的结构由采集层、数据层、检测层和响应层这 4 层架构的相关功能模块组成,如图 10 所示.其中:采集层负责完成采集网络中的 SIP 数据包的功能,设有通过使用 Libosip 协议栈抓取实验网络中的 SIP 数据包并进行解析和关联的采集模块;数据层负责对来自采集层的 SIP 数据包进行预处理,并对得到的 REGSITER 消息流进行 CBF 处理,设有对 SIP 数据包中的 REGISTER 消息流进行 Hash 运算的 CBF 模块;检测层负责调用数据层中的数据信息,并采用 DSMD 算法进行检测,得到检测结果,设有对 REGISTER 消息流检测的 DSMD 模块;响应层负责当检测结果数据达到响应层设定的阈值时,发出告警信号,表示遭到 SIP 洪泛攻击,否则表示网络运行正常,未发生 SIP 洪泛攻击,设有接收检测层输出的检测结果数据进行告警的报警模块.该系统安装在如图 9 所示的与交换机 Switch1 (实际网路中应该是路由器)相连的计算机上(与上述 4 台计算机配置相同),通过镜像端口检测所有进入 IMS 网络的 SIP 流量;然后,构建 201 拨号服务器 AS:我们使用 SIP 压力测试工具 SIPp(sipp.3.1.src.tar.gz)和编写 201 拨号场景文件(scenarios file)来构建 AS,AS 部署到 IMS 网络中的 1 台计算机上(与 S-CSCF 配置相同);最后,选取攻击工具和 IMS 终端(供主叫和被叫使用):我们使用 SIP 压力测试工具 SIPp 作为攻击工具,使用 OpenIC_Lite(v1.0 for Windows)和 SIPp 作为 IMS 终端.安装在与交换机 Switch2 相连的计算机上,如图 9 所示,其中,SIPp 安装在操作系统为 Ubuntu 8.04、内存为 521 MB、CPU 为奔腾 3.0GHz 的计算机上.OpenIC_Lite 安装在操作系统为 Windows XP sp2、内存为 521 MB、CPU 为奔腾 3.0GHz 的计算机上.

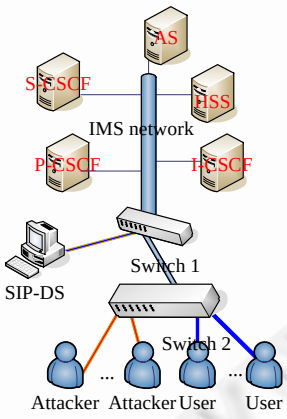


Fig.9 Deployment of SIP-DS

图 9 SIP-DS 部署

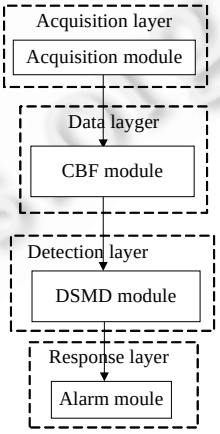


Fig.10 Structure diagram of SIP-DS

图 10 SIP-DS 的结构示意图

平台搭建完成后运行 201 拨号业务,其业务流程描述如下:主叫和被叫用户必须首先完成向 IMS 网络注册的流程,即完成用户代理向 IMS 网络、IMS 网络向用户代理的双向认证和鉴权,使主叫和被叫具备访问和使用

IMS 网络的能力.在成功完成注册流程后,主叫发起呼叫,呼叫号码为一个 21 位号码,其结构为:服务标识码(3位)+卡号(10 位)+被叫号码(8 位).当该呼叫请求传送到在 IMS 网络中的 S-CSCF 时进行初始过滤规则(IFC)的匹配,若服务标识码与设置的初始过滤规则匹配,则 S-CSCF 负责把该请求转向对应的应用服务器 AS,应用服务器从 21 位的呼叫号码中提取 10 位卡号,根据卡号查询该卡上的余额,以判断是否有足够余额来建立这次呼叫.当余额充足时,应用服务器提取 8 位被叫号码,发起一次呼叫,经过 IMS 网络信令转发该呼叫请求给被叫用户,开始建立正常的会话连接流程;当余额不足时,应用服务器向主叫发送 402 用户欠费信息,本次业务结束.

洪泛攻击检测按照部署地点分为源端检测、中间网络检测和受害端检测,本文提出的方法对上述 3 种部署地点均适用.仿真实验中主要用于源端和受害端检测,尤其是源端检测,它具有以下优点:1) 能够在攻击数据流进入 IMS 网络并在瓶颈处造成拥塞之前将其终止;2) 与受害端检测相比,更容易追溯到攻击源;3) 源端出口节点比 IMS 核心网络能够提供更多用于检测的资源.对于源端检测,由于背景流量和攻击流量均较低,所以本文通过对 IMS 网络发送较低的背景流量和攻击流量,在受害端来模拟来自源端网络的攻击.

3.1 正常流量监测

实验中,参数设置如下,T 为 1s,对于 CBF,选取 4 个独立的 Hash 函数;对于 DSMD,当部署在源端检测时,μ_0=2.4, σ=1.7.第 1 阶段抽样的样本数 n_1=1,抽样间隔 h_1=2T,控制线 k_1=7.5,警告线 w_n=5.8,正常线 w_t=4.1;第 2 次抽样的样本数 n_2=2,抽样间隔 h_2=T,控制线 k_2=6.7,K=2,α=0.5.当部署在受害端检测时,历史数据μ_0=10.3,标准偏差 S=3.3,第 1 阶段抽样的样本数 n_1=1,抽样间隔 h_1=2T,控制线 k_1=20.2,警告线 w_n=16.9,正常线 w_t=13.6;第 2 次抽样的样本数 n_2=2,抽样间隔 h_2=T,控制线 k_2=18.6,K=2,α=0.5.以上参数均可根据实际情况进行调整.

对于正常流量下的仿真实验,IMS 网络中的流量均为正常流量,包括 User 注册流量、201 业务流量.在仿真实验中,User 使用 OpenIC_Lite 和 SIPp 及其正常注册场景文件向 IMS 网络进行注册及拨号随机产生多种 IMS 正常流量,图 11 给出其中 3 种 REGSITER 注册请求流量.使用 SIP-DS 对多种正常流量进行检测,均未检测到攻击,表明该方法对正常流量的检测是准确的.

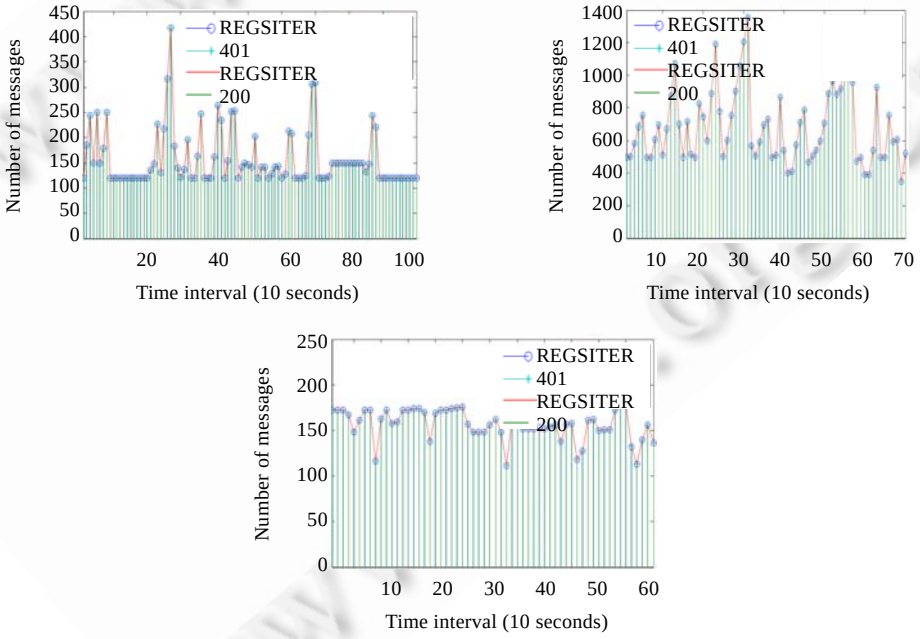


Fig.11 Normal network traffics

图 11 正常网络流量

3.2 洪泛流量监测

本文对洪泛攻击流量的仿真实验主要针对的是两类攻击流量,分别是源端的攻击流量和受害端的攻击流量,实验参数设置与第 3.2 节相同.在源端进行检测,由于源端网络中攻击流量分散且较小,造成一般的检测方法检测率较低.因此,对于源端的有效检测将能对整个 IMS 网络安全产生积极的影响.在受害端进行检测,是 IMS 网络安全关注的重中之重,及早地检测到攻击、及时地采取相应的防范措施,能够大幅度减少攻击带来的影响和损害.如何缩短检测时间,一直是国内外研究者关注的重点.

在洪泛攻击流量检测中,使用第 3.2 节正常流量的的方法随机生成背景流量.对于源端检测,攻击流量通过 Attacker 使用 SIPp 和攻击场景文件向运行 201 业务的 IMS 网络发起洪泛攻击,攻击流量约为实际流量的 50%,可以通过调整 Attacker 的数量和 SIPp 的发包速率控制攻击流量.表 1 为在源端对不同攻击流量进行多次实验的检测结果,从表中我们可以看到,该检测方法具有很好的检测性能,对高于 17REGISTERs/秒的攻击具有 100%的检测率,几乎为 0 的误报,平均检测时间为 2.6s(3 个样本).说明该算法能够有效地检测出在源端的攻击,有利于在较短的时间内准确地发现攻击源并采取相应的防范措施,减轻低流量攻击对 RNC(radio network controller)和 BS (base station)的过度负载、手机电池消耗和信令拥塞造成的影响[27],这将在提高检测能力的同时也大幅度提高对洪泛攻击的防御能力.另外,由于该方法需要的样本数较少,将有利于减小对计算机资源的消耗.

对于受害端的检测,通过多个 Attacker 使用 SIPp 和攻击注册场景文件随机产生攻击流量向 IMS 网络发起洪泛攻击,攻击流量大于实际流量的 200%.由于受害端的攻击流量较大,检测相对容易,对大于 400REGISTERs/秒的攻击流量的检测率达到 100%,检测时间平均约为 2s(2 个样本),误报率几乎为 0.

Table 1 Detection performance of the source-attacks

表 1 攻击源端检测结果

Attack traffic (REGISTERs/s)	Alarm ratio (%)	Alarm time (s)	False alarm ratio (%)
17	100	4.4	0
20	100	2.3	0
40	100	3.1	0
60	100	2.0	0
80	100	2.1	0
100	100	2.3	0
120	100	2.0	0

3.3 讨 论

本文提出的检测方法能够有效地检测出针对 IMS 网络的 SIP 洪泛攻击,它具有以下特点:

(1) 由于源端的攻击流量与正常流量的偏移量较弱,已有的检测方法不能检测出低于 30REGISTERs/s 的攻击流量,而本文的方法用平均不到 3 个样本的时间内 100%地检测出大于 17REGISTERs/s 的攻击流量;

(2) 对于受害端检测,检测时间平均大于 2 个样本,从而有利于保护网络及早采取相应的防御措施,减小攻击带来的损失;

(3) 更低的时间复杂度和可变的抽样间隔,降低了对计算机资源的消耗;

(4) 误报率几乎为 0,不像已有的检测方法产生许多误报.当然,这是在仿真实验中.尽管本文选取的测试例及制定的交互流程经过了二次设计(场景设计符合 3GPP 标准且接近实际应用),但毕竟与真实应用具有一定差距.本文今后将在实际 IMS 网络环境中对该方法作进一步的验证;

(5) 该方法具有一定的可扩展性,不但能够用于 SIP 洪泛攻击的检测,也可用于针对 3G 网络中的呈现服务器(presence servicer)攻击的检测,这将在我们后续的相关工作成果中给予介绍.

当然,本文提出的检测方法也存在不足,由于该算法中的参数设置过多,检测性能受参数设置影响较大,不能对网络流量的变化做出自适应调整.我们将在未来的研究工作中通过引入模糊逻辑(根据双抽样与变抽样间隔控制图在质量管理方面已有研究成果,推理参数之间的内在联系,从而减少参数设置数量,进而在实际应用中起到减少参数数量的作用)及制定相应的模糊规则(根据流量变化影响参数设置)来增加该方法的自适应性.

4 结束语

针对 IMS 网络中存在的 SIP 洪泛攻击,本文提出了一种新的检测方法.该方法通过分析 IMS 网络中的 REGSITER 注册请求消息流并提取检测特征,使用 CBF 对满足检测特征的抽样数据进行处理,然后使用本文提出的 DSMD 算法进行检测.仿真实验结果表明,该方法具有较好的检测性能.

未来的研究工作主要包括:(1) 在 DSMD 算法中,由于参数过多,导致其自适应较差.未来,我们将通过减少参数数量及根据 IMS 网络具体情况自适应地调整参数设置,进而增加算法的自适应性,从而更好地服务于 SIP 洪泛攻击的检测;(2) 研究 DSMD 算法中样本数的选择对检测时间的影响.

References:

[1] Rosenberg J, Schulzrinne H, Camanilo G. SIP: Session initiation protocol. Internet RFC 3261, 2002.

[2] Si DF, Han XH, Long Q, Pan AM. A survey on the core technique and research development in SIP standard. Journal of Software, 2005,16(2):239−250 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/16/239.htm

[3] Gupta P, Shmatikov V. Security analysis of voice-over-IP protocols. In: Proc. of the IEEE Computer Security Foundations Symp. Venice: Institute of Electrical and Electronics Engineers Computer Society, 2007. 49−63. http://www.dsi.unive.it/CSF20/ [doi: 10.1109/CSF.2007.31]

[4] Geneiatakis D, Kambourakis G, Lambrinoudakis C, Dagiuklas T, Gritzalis S. A framework for protecting a SIP-based infrastructure against malformed message attacks. Computer Networks, 2007,51(10):2580−2593. [doi: 10.1016/j.comnet.2006.11.014]

[5] Wu YS, Bagchi S, Garg S, Singh N, Tsai T. SCIDIVE: A stateful and cross protocol intrusion detection architecture for voice-over-IP environments. In: Proc. of the Int'l Conf. on Dependable Systems and Networks. Florence: Institute of Electrical and Electronics Engineers Computer Society, 2004. 433−442. http://2004.dsn.org/ [doi: 10.1109/DSN.2004.1311913]

[6] Rebahi Y, Sher M, Magedanz T. Detecting flooding attacks against IP multimedia subsystem (IMS) networks. In: Proc. of the 6th IEEE/ACS Int'l Conf. on Computer Systems and Applications (AICCSA 2008). Doha: Institute of Electrical and Electronics Engineers Computer Society, 2008. 848−851. http://www3.cs.queensu.ca/trl/aiccsa08/ [doi: 10.1109/AICCSA.2008.4493627]

[7] Sher M. Secure service provisioning (SSP) framework for IP multimedia subsystem (IMS) [Ph.D. Thesis]. Berlin: Technical University Berlin, 2007.

[8] Awais A, Farooq M, Javed MY. Attack analysis bio-inspired security framework for IP multimedia subsystem. In: Proc. of the 10th Annual Conf. on Genetic and Evolutionary Computation 2008 (GECCO 2008). Atlanta: Association for Computing Machinery, 2008. 161−162. http://www.sigevo.org/gecco-2008/papers.html [doi: 10.1145/1389095.1389119]

[9] Akbar MA, Tariq Z, Farooq M. A comparative study of anomaly detection algorithms for detection of sip flooding in IMS. In: Proc. of the 2nd Int'l Conf. on Internet Multimedia Services Architecture and Application (IMSAA 2008). Bangalore: Institute of Electrical and Electronics Engineers Computer Society, 2008. http://www.imsaa.org/imsaa2008/ [doi: 10.1109/IMSAA.2008.4753934]

[10] Sher M, Magedanz T. Mobile multimedia broadcasting vulnerability threats, attacks and security solutions. In: Proc. of the 9th Int'l Conf. on Mobile and Wireless Communications Networks (MWCN 2007). Cork: Institute of Electrical and Electronics Engineers Computer Society, 2007. 56−60. http://www.aws.cit.ie/mwcn2007/papers.html

[11] Chen EY. Detecting DoS attacks on SIP systems. In: Proc. of the 1st IEEE Workshop on VoIP Management and Security (VoIP MaSe 2006). Vancouver: Institute of Electrical and Electronics Engineers Computer Society, 2006. 51−56. http://voipsa.org/pipermail/voipsec_voipsa.org/2005-December/001054.html [doi: 10.1109/VOIPMS.2006.1638123]

[12] Sengar H, Wang H, Wijesekera D, Jajodia S. Fast detection of denial-of-service attacks on IP telephony. In: Proc. of the IEEE Int'l Workshop on Quality of Service (IWQoS). New Haven: Institute of Electrical and Electronics Engineers Inc., 2006. 199−208. http://www.ietf.org/mail-archive/web/nsis/current/msg05899.html [doi: 10.1109/IWQOS.2006.250469]

[13] Ehlert S, Wang C, Magedanz T, Sisalem D. Specification-Based denial-of-service detection for SIP voice-over-IP networks. In: Proc. of the 3rd Int'l Conf. on Internet Monitoring and Protection (ICIMP 2008). Bucharest: Institute of Electrical and Electronics Engineers Computer Society, 2008. 59−66. http://www.iaria.org/conferences2008/ICIMP08.html [doi: 10.1109/ICIMP.2008.14]

[14] Farooqi AH, Munir A. Intrusion detection system for IP multimedia subsystem using *K*-nearest neighbor classifier. In: Proc. of the 12th IEEE Int'l Multitopic Conf. (INMIC 2008). Karachi: Institute of Electrical and Electronics Engineers Computer Society, 2008. 423−428. http://www.conferencealerts.com/seeconf.mv?q=ca1x3ms6 [doi: 10.1109/INMIC.2008.4777775]

[15] Wang ZB, Lucent A. IMS security framework. 3GPP2 S.S0086-B, 2008.

[16] Bloom BH. Space/Time trade-offs in hash coding with allowable errors. Communications of the ACM, 1970,13(7):422−426. [doi: 10.1145/362686.362692]

[17] Kim Y, Lau WC, Chuah MC, Chao HJ. PacketScore: Statistics-Based overload control against distributed denial-of-service attacks. In: Proc. of the IEEE INFOCOM. Hongkong: Institute of Electrical and Electronics Engineers Inc., 2004. 2594−2604. http://www.ieee-infocom.org/2004/ [doi: 10.1109/INFCOM.2004.1354679]

[18] Abdelsayed S, Glimsholt D, Leckie C, Ryan S, Shami S. An efficient filter for denial-of-service bandwidth attacks. In: Proc. of the IEEE Global Telecommunications Conf. (GLOBECOM). San Francisco: Institute of Electrical and Electronics Engineers Inc., 2003. 1353−1357. http://www.globecom2003.com/ [doi: 10.1109/GLOCOM.2003.1258459]

[19] Snoeren AC. Hash-Based IP traceback. In: Proc. of the Computer Communication Review. San Diego: Association for Computing Machinery, 2001. 3−14. http://conferences.sigcomm.org/sigcomm/2001/

[20] Sun C, Hu C, Zhou Y, Xiao X, Liu B. A more accurate scheme to detect SYN flood attacks. In: Proc. of the IEEE INFOCOM. Rio de Janeiro: Institute of Electrical and Electronics Engineers Inc., 2009. http://www.ieee-infocom.org/2009/ [doi: 10.1109/INFCOMW.2009.5072099]

[21] Xie K, Wen JG, Zhang DF, Xie GG. Bloom filter query algorithm. Journal of Software, 2009,20(1):96−108 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3458.htm [doi: 10.3724/SP.J.1001.2009.00096]

[22] Fan L, Cao P, Almeida J, Broder AZ. Summary cache: A scalable wide-area Web cache sharing protocol. IEEE/ACM Trans. on Networking, 2000,8(3):281−293. [doi: 10.1109/90.851975]

[23] Carot V, Jabaloyes JM, Carot T. Combined double sampling and variable sampling interval *X* chart. Int'l Journal of Production Research, 2002,40(9):2175−2186. [doi: 10.1080/00207540210128260]

[24] Torng CC, Lee PH, Liao NY. An economic-statistical design of double sampling *over*(*X*,−) control chart. Int'l Journal of Production Economics, 2009,120(2):495−500. [doi: 10.1016/j.ijpe.2009.03.013]

[25] Lin HH, Chou CY, Lai WT. Economic design of variable sampling intervals *over*(*X*) charts with AL switching rule using genetic algorithms. Expert Systems with Applications, 2009,36(2 PART 2):3048−3055. [doi: 10.1016/j.eswa.2007.10.005]

[26] Vignesh KM, Prateek S. Building an IMS client test bed with open source tools. In: Proc. of the 1st Int'l Conf. on IP Multimedia Subsystems Architecture and Applications (IMSAA 2007). Bangalore: Institute of Electrical and Electronics Engineers Computer Society, 2007. http://www.imsaa.org/imsaa2007/ [doi: 10.1109/IMSAA.2007.4559105]

[27] Lee PPC, Bu T, Woo T. On the detection of signaling DoS attacks on 3G wireless networks. In: Proc. of the IEEE INFOCOM. Anchorage: Institute of Electrical and Electronics Engineers Inc., 2007. 1289−1297. http://www.ieee-infocom.org/2007/ [doi: 10.1109/INFCOM.2007.153]

附中文参考文献:

[2] 司端锋,韩心慧,龙勤,潘爱民.SIP 标准中的核心技术与研究进展.软件学报,2005,16(2):239−250. http://www.jos.org.cn/1000-9825/16/239.htm

[21] 谢鲲,文吉刚,张大方,谢高岗.布鲁姆过滤器查询算法.软件学报,2009,20(1):96−108. http://www.jos.org.cn/1000-9825/3458.htm [doi: 10.3724/SP.J.1001.2009.00096]

王尚广(1982−),男,河南周口人,博士生,主要研究领域为下一代网络安全,服务计算.

孙其博(1975−),男,博士,副教授,主要研究领域为下一代网络安全,网络智能化.

杨放春(1957−),男,博士,教授,博士生导师,CCF 高级会员,主要研究领域为通信软件,网络安全,网络智能化.