基于相对熵的 SIP DoS 洪泛攻击检测算法和仿真①

张晓月, 胡访宇

(中国科学技术大学 信息科学技术学院, 合肥 230022)

摘 要: 随着 SIP 协议的广泛应用, SIP 网络的安全机制也逐渐成为研究热点. 针对 SIP DoS 洪泛攻击, 本文将相对熵引入 SIP 网络, 提出了一种基于相对熵的检测算法, 并与传统的信息熵检测算法进行比较. 实验结果表明: 正常网络流量下信息熵值和相对熵值都基本稳定, 在发生 DoS 攻击时相对熵值波动明显, 比信息熵检测算法检测率更高, 检测结果更准确.

关键词: SIP; DoS 洪泛攻击; 信息熵; 相对熵

Algorithm and Simulation of SIP DoS Flooding Attack Detection Based on Relative Entropy

ZHANG Xiao-Yue, HU Fang-Yu

(Department of Information Science and Technology, University of Science and Technology of China, Hefei 230022, China)

Abstract: With the extensive application of SIP protocol, the security mechanisms of SIP network have gradually become a hot topic. This article introduces relative entropy into SIP network, and proposes a detection algorithm based on it to against SIP DoS flooding attacks. We also compare this algorithm with the traditional entropy detection algorithm. The experimental results showed that: the entropy and relative entropy are both stable under normal network traffic. But relative entropy fluctuated significantly when attack occurred and our algorithm have a higher detection rate and more accurate results than entropy detection algorithm.

Key words: SIP; DoS flooding attack; entropy; relative entropy

1 引言

会话初始化协议 SIP (Session Initiation Protocol)是在 1999 年由互联网工程工作组(IETF)提出的一个信令控制协议, 是类似于超文本传送协议(HTTP)的基于文本的信令协议, 采用客户端/ 服务器的控制方式进行信息交换, 并采用会话描述协议(SDP , Session Description Protocol)进行媒体及会话能力的描述[1].

SIP 在设计之初, 侧重考虑协议的易用性和灵活性, 但没有重点考虑安全性. 在复杂的网络环境中 SIP 应用面临着众多的安全威胁: (1)因 SIP 继承了传统互联网机制, 现有互联网常见安全威胁对于 SIP 都难以避免, 如: 重放攻击、网络篡改、DoS/DDoS 等. (2)由于 SIP 网络自身特点及 SIP 协议脆弱性等因素, SIP 面临其自身特有安全威胁, 如: 注册劫持、服务器伪装等.

目前 SIP 安全机制大都借鉴了现有比较成熟的安全方案, 包括认证和加密. 认证主要是验证 SIP 网络结点的合法性和有效性, 常用的是 HTTP 摘要认证; 加密主要是为了保证 SIP 消息能安全的在网络上传输, 常见加密方式有网络层 IPSec 加密、传输层 TLS 加密和应用层 S/MIME 加密等[2]. 但是认证和加密只能较好的防御网络篡改、注册劫持、服务器伪装等安全问题, 而对于 DoS 攻击则无能为力, 因此, 继续深入研究 SIP 安全机制尤其是 DoS 攻击检测十分有必要. 本文重点研究了 SIP DoS 洪泛攻击的检测算法.

因为 DoS 攻击是人为有意制造的, 所以它一定会影响正常情况下的网络行为的随机性和规则性. 通过分析流量中 IP、端口、消息数目等变量在分布规律上的变化可以有效的发现异常.

① 收稿时间:2014-04-22;收到修改稿时间:2014-05-22

2　SIP DoS攻击检测算法

2.1 传统的信息熵检测算法

信息熵是系统有序化程度的一个度量，能检测出 DoS 攻击对于正常网络流量随机性所产生的影响. 信息熵的定义如下:

$$H = -\sum_{i=1}^{N} p_i \log_2 p_i \tag{1}$$

其中, P 为某一测度当前时段的分布序列.

在正常情况下, 每个时段的信息熵是在一定范围内波动的, 不会出现明显的偏差. 但是当出现 DoS 攻击时, 由于网络行为的随机性和规则性遭到了破坏, 会出现信息熵的显著变化, 从而检测出异常.

但是网络流量是一个动态变迁的过程, 只取其中的一点而不去分析其与相邻时间序列之间的关系, 对于未能引起流量分布显著变化的 DoS 攻击也很难检测出来[3,4]. 因此, 我们提出一种基于相对熵的 SIP DoS 攻击检测算法. 将信息论中的另一重要理论——相对熵引入 SIP 网络中.

2.2 基于相对熵的检测算法

相对熵是指两个随机序列之间距离的度量, 从统计学角度它是指两个随机序列之间的相似程度[6,7]. 相对熵可定义为:

$$D(P \| Q) = \sum_{i=1}^{n} p_i \ln \frac{p_i}{q_i} \tag{2}$$

式中, $P = \{p_1, p_2, ..., p_n\}$, $Q = \{q_1, q_2, ..., q_n\}$. P 为当前时段某一测度的分布序列, Q 为上一时段该测度的分布序列.

在正常情况下, 相对熵也是在一定范围内波动的, 不会出现明显的偏差. 但是当出现 DoS 攻击时, 该时段与上一时段该测度的流量分布会出现显著变化, 因而相对熵值也会出现显著变化, 可以更加有效的检测出异常行为.

具体算法流程如图 1 所示.

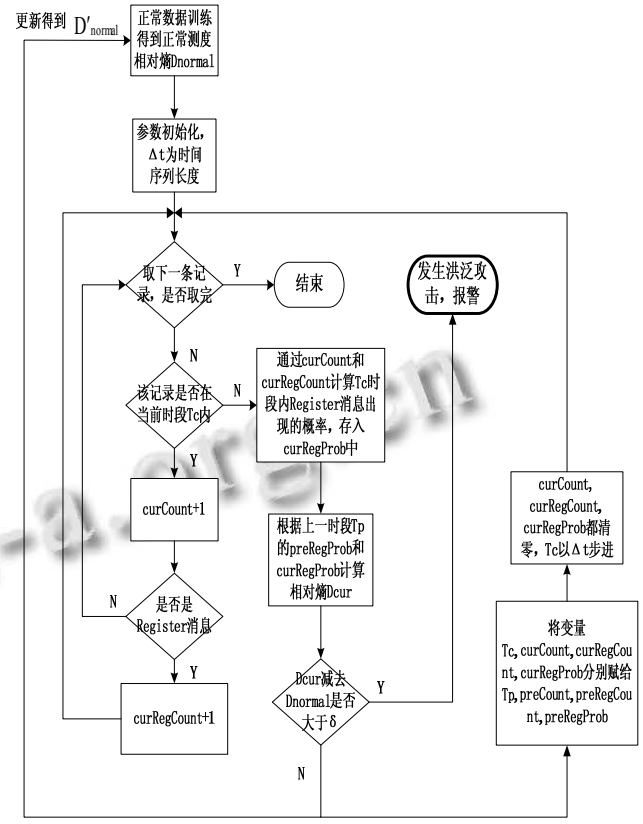

图 1　基于相对熵的检测算法流程图

3　实验与讨论

针对 SIP 的洪泛攻击主要是通过向服务器发送大量的 INVITE/REGISTER 消息而不响应来实现, 故选取 INVITE/ACK 的比率为一个流量测度. 还有一种攻击是向服务器发送大量的 INVITE 或者 REGISTER 消息, 使 SIP 服务器的等待时间过长, 故选取 INVITE 或者 REGISTER 消息数为另一个流量测度. 本文仿真以 REGISTER 消息数为例.

3.1 非攻击时段训练数据处理和统计

数据来源: 安徽教育招生考试综合管理系统项目中的监控平台支持 SIP 协议, 在该平台下通过抓包软件捕获了 20min 内的正常状态下的 SIP 网络流量, 并将流量按需求进行预处理.

3.2 用 SIP Inspector 模拟洪泛攻击并插入正常数据

SIP Inspector 是一个用来模拟不同的 SIP 消息和通讯情景的工具, 可用来创建 SIP 信令、定制 SIP 消息以及兼容输入和输出的消息包, 该工具还可以直接从 pcap 文件中播放 RTP 流. 通过修改其 scenario 文件, 可以模拟用户想要的 SIP 流程.

通过 SIP Inspector 模拟 flood 攻击, 并分别替换正常数据的第 10 个 10s, 第 20 个 10s, 第 30 个 10s....的数据, 作为检测算法的输入.

3.3 基于传统信息熵的 SIP DoS 洪泛攻击检测算法仿真

先用正常数据中的每 10s 的数据作为一个分布序列 P, 算出其中每个 IP 地址的消息数出现的概率 p, 根据上述公式计算正常数据信息熵, 并求出其均值, 根据正常信息熵的波动情况确定一个合理的阈值范围,

如图 2 上下两条蓝线之间. 再将插入 flood 攻击的数据用该算法进行检测, 得出仿真图 3.

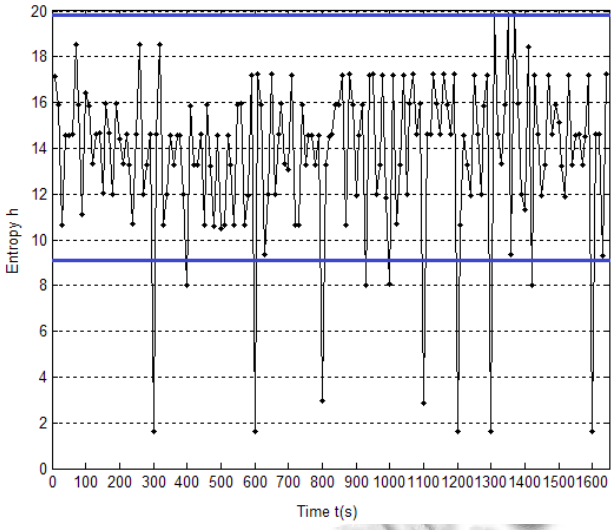

图 2 正常数据信息熵仿真结果

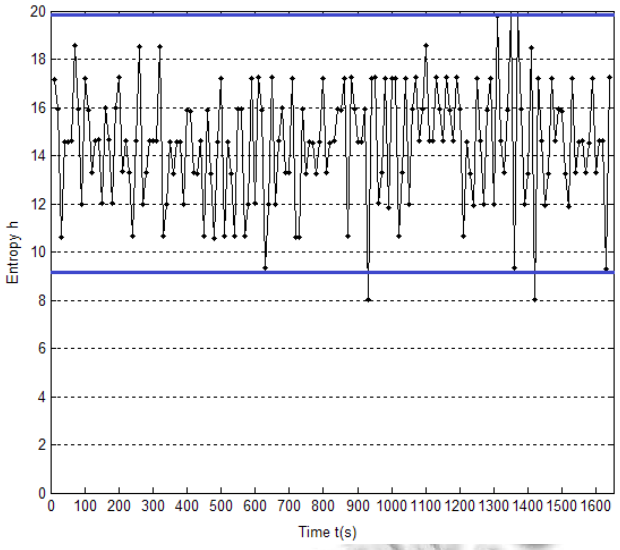

图 3 flood 信息熵仿真结果

由图 3 可以看出, 在 300s, 400s, 600s, 800s, 1000s 等处, 信息熵的值显著减小, 远远小于设定的阈值, 说明正常的流量特征遭到了破坏, 可以判定发生了 DoS 攻击. 但是 100s, 200s, 500s 等也发生了攻击的时段, 信息熵却在阈值以内, 即没有检测出来.

3.4 基于相对熵的 SIP DoS 洪泛攻击检测算法仿真

当前时段的分布序列作为 P, 上一个时段的分布序列作为 Q, 通过计算上个时段和当前时段数据之间的相对熵用于 DoS 的攻击检测.

但是将两个时段的数据进行合并时会出现两种特殊情况:

(1) 对于在当前时段出现而上一时段没有出现的元素及其对应的 $p_i \neq 0$, $q_i = 0$, 此时定义 $p_i \ln \frac{p_i}{q_i} = p_i$, 对于随着时间的推移而消失的元素, 通过下降的幅度来影响相对熵值;

(2)对于在上一时段出现而当前时段没有出现的元素定义其对应的 $p_j = 0$, $q_j \neq 0$, 此时定义 $p_i \ln \frac{p_i}{q_i} = p_i e$, 对于本时段突然出现的元素赋予较高的权值, 通过出现的频率与权值的乘积来影响相对熵值[3].

仿真结果如图 4、图 5 所示:

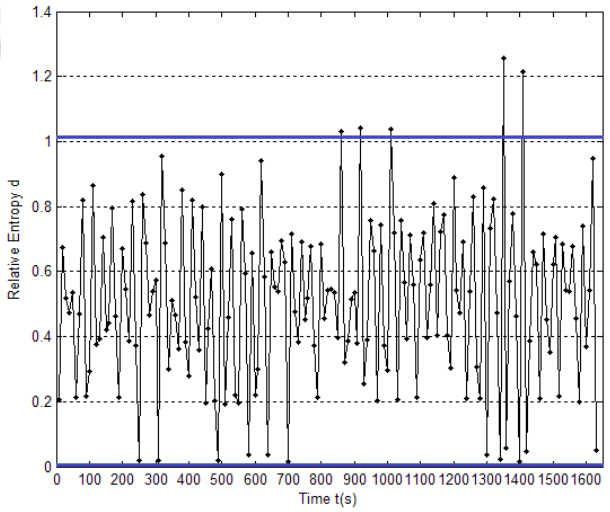

图 4 正常数据相对熵仿真结果

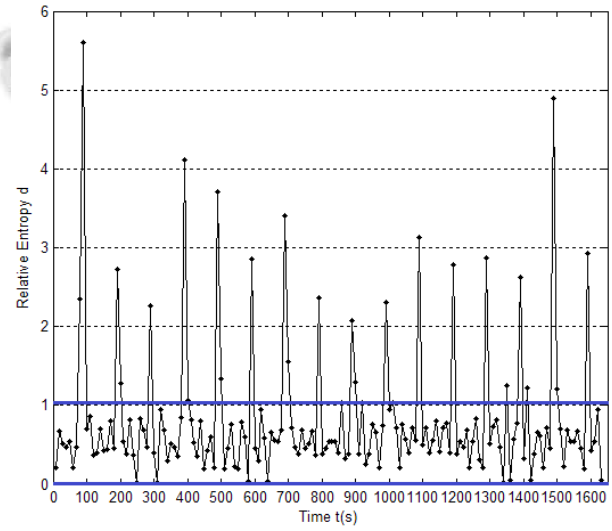

图 5 flood 相对熵仿真结果

由图 5 可以看出, 每次攻击发生时, 相对熵值都

有一个非常大的增加, 大大超过了正常情况下的阈值范围, 这是因为与上一时段相比, 当前时段的消息数明显增多, 两个序列的分布偏差增大, 故而相对熵会呈现明显的增大, 因此可以判断为发生 DoS 攻击.

用两种方法对更多的模拟攻击进行检测, 检测结果如表 1 所示:

表 1 两种方法多次实验结果对比

算法类型	异常次数	正常检测次数	检测率
信息熵	80	51	63.75%
相对熵	80	77	96.25%

3.5 实验结果分析

对上述 3.3 和 3.4 的仿真结果和原始数据进行对比后发现:

(1)当洪泛攻击同时来自多个IP时, 传统的信息熵检测算法可以较好的检测出, 但是当少数 IP 甚至 1、2 个 IP 发生攻击时, 信息熵算法往往检测不出.

(2)而基于相对熵的 SIP DoS 洪泛攻击检测算法对这两种情况都能较好的检测出来. 相对熵反应的网络流量在相邻时间序列的动态变迁过程, 任何一个 IP 的流量变化都会引起整个流量分布的显著变化.

(3)结论: 相对于传统的信息熵检测算法, 引入相对熵后的检测算法对于视频监控系统中的 SIP DoS 攻击有更高的检测率.

4 结语

本文针对 SIP 攻击中的 DoS 洪泛攻击, 提出了一种基于相对熵的检测算法. 该算法将传统的信息熵检测算法的信息熵替换为相对熵, 以反映网络流量中的动态变迁过程. 实验结果表明, 在检测率方面, 基于相对熵的 SIP DoS 洪泛攻击检测算法比之传统的信息熵检测算法有较大幅度的提高.

参考文献

1 Rosenberg J, Schulzrinne H, Camanilog. SIP: Session Initiation Protocol. Internet RFC3261, 2002.
2 李鸿彬.SIP 网络中入侵检测与防御系统关键技术的研究[学位论文].沈阳:中国科学院研究生院沈阳计算技术研究所,2012.
3 夏秦,王志文,卢柯.入侵检测系统利用信息熵检测网络攻击的方法.西安交通大学学报,2013,47(2):14–19.
4 付枫.基于网络流量熵特性的 DoS 攻击检测研究[学位论文].长春:吉林大学,2012.
5 李涵秋,马艳,雷磊.基于相对熵理论的网络 DoS 攻击检测算法.电讯技术,2011,51(3):89–92.
6 Asgharian Z, Asgharian H, Akbari A, et al. A framework for SIP intrusion detection and response systems. 2011 International Symposium on Computer Networks and Distributed Systems (CNDS). IEEE. 2011. 100–105.
7 Chen EY. Detecting DoS attacks on SIP systems. 2006. 1st IEEE Workshop on VoIP Management and Security. IEEE, 2006. 53–58.