采用数据挖掘的拒绝服务攻击防御模型

童 彬，秦志光，贾伟峰，宋健伟

(电子科技大学计算机科学与工程学院 成都 610054)

【摘要】针对拒绝服务攻击的特点，提出了一种采用数据挖掘技术的防御模型。该模型以实时抽样流量作为数据来源，采用关联分析法提取可信IP列表用于数据包的过滤，并利用贝叶斯分类算法对数据包的危险等级进行评估。该模型弥补了传统的基于可信IP列表过滤的不足，并在防御攻击时能有效区分正常流量与异常流量。实验证明该模型能够对拒绝服务攻击进行有效、实时的防御。

关 键 词 关联分析； 贝叶斯分类； 数据挖掘； 拒绝服务

中图分类号 TP393 **文献标识码** A

A DoS Attack Defense Model Adopting Data Mining

TONG Bin, QIN Zhi-guang, JIA Wei-feng, and SONG Jian-wei

(School of Computer Science and Engineering, University of Electronic Science and Technology of China Chengdu 610054)

Abstract According to the characteristics of DoS/DDoS attack, a defense model adopting data-mining technology is proposed. Based on real-time sample traffic, this model extracts trusted IP list by association analysis to filter, and evaluates packets' danger degree by adopting bayes algorithm. This model makes up disadvantages of traditional filtering based on trusted source IP, and effectively differentiates normal traffic and abnormal traffic. Experimental datum proves this model can launch real-time and effective defense against DoS/DDoS attack.

Key words association analysis; Bayes classification; data-mining; denial of service

拒绝服务攻击(DoS)和分布式拒绝服务攻击(DDoS)是目前常见的、难以防御的网络攻击方式[1]。特别是DDoS攻击，由于受控主机自身具有分布性，且攻击数据包采用伪随机IP，使得攻击者具有更强的隐蔽性，DDoS攻击更加难以防御。因此，研究一种能够有效抵御DDoS攻击的防御模型和机制具有很迫切的现实需要。

数据挖掘技术在检测和防御分布式拒绝服务攻击领域有一定的应用[2-5]，但主要应用在攻击检测。针对DDoS进行防御有多种机制和方法[6]，如基于源可信IP过滤、拥塞控制等方案。然而，基于拥塞控制的防御机制无法正确区分恶意攻击流量和合法流量[6]；根据历史流量提取可信源IP防御方法也存在一定程度的失效问题[7]。

本文提出了一种基于数据挖掘技术的DoS/DDoS防御机制模型。该防御模型具有以下特点：(1) 弥补了传统的基于可信IP过滤的缺点，使得基于可信IP的过滤机制更健壮；(2) 能够有效区分正常流量和异常流量；(3) 提取、传输可信IP列表具有高效性，使防御模型可进行实时防御。

1 采用数据挖掘的防御模型

1.1 防御模型

防御模型架构如图1所示。

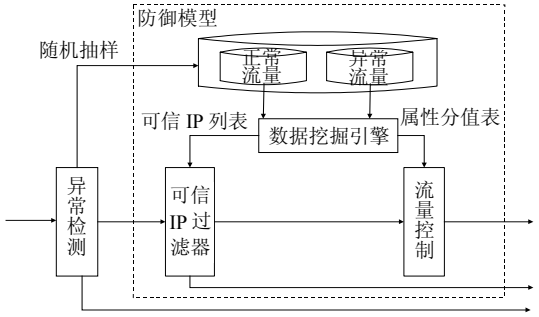

图1 防御模型架构图

该防御模型建立在对DoS/DDoS攻击的异常检测的基础上。异常检测采用协方差的分析方法[8]对DDOS攻击进行有效、实时的检测，并根据随机抽样理论[9]和系统异常状态标志将网络流量随机分别抽样至数据库服务器的正常流量库和异常流量库，

收稿日期：2007－09－20；修回日期：2008－03－08
基金项目：电子信息产业发展基金(信部运[2005]555)
作者简介：童 彬(1982－)，男，博士生，主要从事机器学习和网络安全方面的研究.

从而为防御模型提供了可靠、实时的数据来源。

防御模型主要由数据挖掘引擎、可信IP过滤器、流量控制3大组件构成。其中数据挖掘引擎采用关联分析方法和贝叶斯分类算法，将提取的可信源IP列表与数据包属性分值表分别传送给可信IP过滤器与流量控制组件。当异常检测模块检测当前流量发生异常时，网络数据包会首先经过可信IP过滤器，若数据包中的源IP地址与可信IP过滤器中存储的可信IP列表匹配，认为该数据包为合法数据包，放行该数据包；否则数据包将流入流量控制模块。流量控制模块利用数据包属性分值表对数据包进行危险度评估，若数据包的危险等级越高，则被丢弃的概率就越大；反之，被丢弃的概率就越小。

可信IP列表组件与流量控制组件相互配合。可信度较高的可信IP列表使可信流量尽快通过防御模型，也为流量控制组件分担一部分压力。流量控制组件对可信IP列表组件不能处理的数据包按照危险度等级的不同以不同概率丢包，这样有选择概率的丢包，使正常流量极大限度地通过防御模型，从而保障了网络的服务质量。

1.2　防御模型实现

异常检测和防御模型中的可信源IP、流量控制组件部署在被保护网络边界的网络处理器；防御模型的数据挖掘引擎部署在旁接于网络处理器的数据库服务器中，部署结构如图2所示。

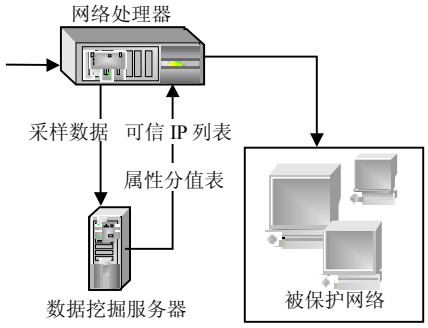

图2　防御模型部署图

1.2.1　可信IP列表

在传统的可信IP列表过滤方案中，经验丰富的DoS/DDoS攻击者可以在不被检测机制检测出异常的情况下，通过发送小流量攻击数据包取得防御系统的信任，使攻击数据包的源IP加入到可信IP列表中，从而使得防御方法失效[7]。本文提出的模型结合访问密度、频繁项集两种频度指标，在正常流量库中提取可信IP列表。同时，在该列表中去掉基于异常流量库用频繁项集方法提取的可疑源IP，有效地解决了失效问题。提取的可信IP列表在内存以哈希链表的形式维护管理，并对可信IP过滤器中的IP列表进行周期增量更新，避免了可信IP的重复传输，保证了防御的实时性。

可信IP列表的生成过程如下：

(1) 在正常访问情况下，同一个源IP地址会较为频繁地访问被保护网络，所以在网络流量正常时，可以将具有一定访问频度的源IP地址近似地认作为被保护网络的可信IP地址。在该防御模型中维护一个按照访问密度降序排序的IP地址列表 $S_1=\{p_i \mid i=1,2,\cdots,N\}$，其中 p_i 为IP地址，N为IP地址个数。

(2) 以随机抽样的正常流量库作为数据源，基于IP数据包的TTL和数据包长度两个属性生成频繁项集 F_1，取出 F_1 对应的源IP，按照访问密度进行降序排序，得到一个IP地址列表 $S_2=\{l_i \mid i=1,2,\cdots,K\}$，其中 l_i 为IP地址，K为 F_1 的大小。

(3) 以随机抽样的异常流量库作为数据源，基于IP数据包的TTL和数据包长度两个属性生成频繁项集 F_2，取出 F_2 中的源IP，得到一个IP地址列表 $S_3=\{m_i \mid i=1,2,\cdots,M\}$，其中 m_i 为IP地址，M为 F_2 的大小。

取 $A_1 \subset S_1$，$A_2 \subset S_2$，且 $\forall p_i \in A_1, \forall l_i \in A_2$，$p_i$、$l_i$ 的访问次数大于1，则可信IP列表 $T=A_1 \cap A_2 - S_3$，其中 $A_1 \cap A_2$ 表示结合访问密度和频繁项集两种频度指标获取的更为可信的IP列表。为了避免攻击源IP出现在可信IP列表中，在取交集后IP列表中去掉 S_3，使得 T 能够更有效地基于源IP过滤进行防御。

1.2.2　属性分值表

数据挖掘引擎还将为流量控制组件提供数据包的属性分值表。属性分值表的生成基于以下事实：当网络流量正常时，数据包的一些属性值的统计特性维持在一个比较稳定的状态，当 DDoS 攻击发生时，这些属性值的统计特性较正常情况下会发生剧烈的变化。相关属性值不对称的、剧烈的变化将作为区分正常流量和 DDoS 攻击流量的有利证据。生成属性分值表以后，流量控制组件将根据属性分值表对数据包进行评分，达到度量数据包危险度的目的。危险度为流量控制模块丢包提供了有利判据，避免了流量控制模块丢包的盲目性。

生成属性分值表的方法参考了文献[10]的基本思想，并进行了修改和扩充。首先，对正常流量库和异常流量库IP数据包的属性值进行频率统计，再根据贝叶斯定理计算IP数据包属性值在特定值情况下数据包为正常包的概率(为了降低计算复杂度，假

设IP数据包各属性是独立同分布的，引入lg算子将乘除运算改进为加减运算，加快了运算速度)。计算公式如下：

$$\lg[\mathrm{CLP}(P)]=\begin{Bmatrix}[\lg(P_n(A=a_p))-\lg(P_m(A=a_p))]+\\ [\lg(P_n(B=b_p))-\lg(P_m(B=b_p))]+\\ [\lg(P_n(C=c_p))-\lg(P_m(C=c_p))]+\cdots\end{Bmatrix}$$

式中 $P_n(A=a_p)$ 表示在正常流量库中，属性 A 值等于 a_p 的概率；$P_m(A=a_p)$ 表示在异常流量库中，属性 A 值等于 a_p 的概率，以此类推；$\mathrm{CLP}(p)$ 表示数据包 p 属性 $A,B,C,\cdots$ 值等于 $a_p,b_p,c_p\cdots$ 情况下为正常数据包的概率。一个数据包 p 的分数由各个属性的分数值相加得到。对于属性 A 的分数值表示为 $\lg(P_n(A=a_p))-\lg(P_m(A=a_p))$，以此类推。一般来说，选取源IP前缀(16 bis)和TTL属性值具有较好的效果。在防御模型中将源IP前缀(16 bis)和TTL属性值等宽离散化，既减少了计算量，又可减少属性分值表的大小，使提取、传输属性分值表的效率提高，但需要选取合适的等宽距。

根据数据库服务器的正常和异常流量库得到属性分值表后，对正常和异常流量库中的数据进行评分，分别计算正常和异常流量分值的标准差(∂_n,∂_m)和平均值(u_n,u_m)。值得注意的是，若 $u_n<u_m$ 则表明提取属性分值表失败，进入下一次的提取过程。若提取成功，在网络处理器中定时更新 ∂_n、∂_m、u_n、u_m 与属性分值表。

当有数据包经过流量控制组件时，对数据包进行评分，再将分数根据 ∂_n、∂_m、u_n、u_m 这 4 个参数映射到 0～9 的危险等级，其中 9 表示的危险等级最高。在流量控制组件规定：数据包的危险等级越高，则以更高的概率丢包。

为了减少贝叶斯分类误差率对映射关系的影响，分数映射为危险等级的方法如下：

(1) 计算稠密系数 $p=\partial_n/\partial_m$；

(2) 计算相对分数刻度 $r_i=i^p$，其中 $i=0,1,\cdots,10$；

(3) 计算绝对分数刻度 $s_i=(u_n-u_m)\dfrac{r_i-r_0}{r_{10}-r_0}+u_m$，其中 $i=0,1,2,\cdots,10$；

(4) 对每一个数据包，根据属性分值表计算其分值 v，则其危险等级 $d=\begin{cases}0 & v>u_n\\ 9-i & s_i\leqslant v<s_{i+1}\\ 9 & v<u_m\end{cases}$，其中 $i=0,1,2,\cdots,9$。

根据危险等级设计丢包率的方法如下：设定危险等级为0时丢包率为0%，危险等级为9时丢包率为100%，其他危险等级可以按照线性或指数函数关系来设定丢包率。

2 实验分析

为了验证防御模型中数据挖掘引擎产生可信IP列表和危险等级的有效性，本节选取了MIT 林肯实验室的2000年分布式拒绝服务攻击数据集LLDOS1.0和正常网络数据集作为数据来源，对防御模型进行实验数据分析。

2.1 可信IP列表实验分析

在网络流量正常的情况下，具有一定访问频度的源IP地址可作为可信IP地址的原始参考。通过实验，把根据数据包TTL值、数据包长度两属性生成频繁项集对应的可信源IP列表与根据源IP访问密度生成的可信IP列表做对比分析，验证频繁项集方法提取可信源IP列表的有效性。在实验中，取支持度为 0.1，首先对TTL值和IP数据包长度进行等宽划分(分类数分别为255和655)，然后生成频繁项集。为了说明生成的频繁项集的有效性，本文取集合 $A_1'\subset S_1$ 和 $A_2'\subset S_2$，并令集合元素个数 $|A_1'|=|A_2'|=L$，令重复度 $\alpha=\dfrac{|A_1'\bigcap A_2'|}{|A_1'|}$。一般地，$\alpha$ 越大，A_1' 与 A_2' 的重复度越大，则表明频繁项集中所包含的IP地址越有效。重复度效果如图3所示。

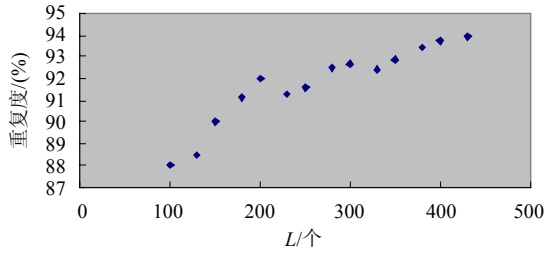

图3 A_1'与A_2' 的IP地址重复度效果图

实验采用的正常训练数据集大约具有800左右的源IP。实验结果表明，使用关联分析法产生的可信源IP地址与基于访问密度提取的源IP地址具有很大的重复度，则表明关联分析方法提取可信IP地址是可行的。

DoS/DDoS攻击发生时，若大规模异常流量的攻击数据包的源IP地址存在于可信IP列表中，在设定合适支持度的情况下，则基于异常流量库生成的频繁项集 S_3 中会包含攻击数据包的源IP；而正常流量源IP的频繁度由于大规模异常流量的影响则降低，当低于一定支持度时，其源IP不会出现在 S_3 中，那

么 $A_1 \cap A_2$ 与异常流量库提取的源IP列表 S_3 做差集运算既使可信源IP不被差集运算所排除，又可提高可信IP列表的可信度。

2.2 危险等级有效性实验分析

流量控制组件根据数据包的危险等级进行不同概率的丢包，危险等级的划分又是根据属性分值表得出的。所以，属性分值表、危险度映射关系对流量控制的效果有重要的影响。本文对属性分值表及危险度映射关系的有效性进行分析，证明它们对正常流量和异常流量的区分度。一般来说，∂_n、∂_m 越小，$|u_n - u_m|$ 越大，属性分值表对数据包的危险度等级划分效果越好。

在实验中，将LLDOS1.0和正常训练数据集分别导入至异常流量库和正常流量库。首先，对TTL值进行等宽划分，当分类数为100、150、200、255时，利用属性分值表对正常/异常流量数据库中的流量进行记分。实验数据表明，当TTL等距分类数为150时，$|u_n - u_m|$ 最大，∂_n 最小。

为了验证危险等级映射关系的有效性，在 TTL 分类数为 150、源 IP 前缀(16 bis)分类数为 655 情况下提取属性分值表后，利用危险度映射关系将正常/异常流量库中的数据包分值映射成 0～9 的危险等级，其百分比效果如图 4 所示。

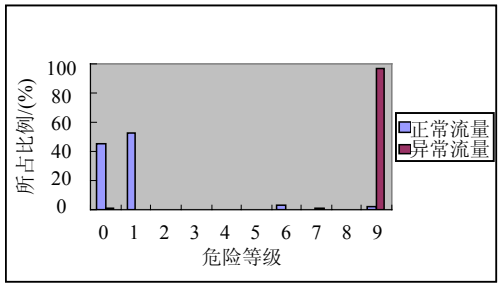

图4　正常/异常流量危险等级的百分比

可以看出，对于正常流量而言，危险等级集中在 0 或 1。而对异常流量而言，危险等级集中在 9。所以属性分值表和危险等级映射方法具有明显效果，从而为流量控制组件丢包提供了有利依据。

3 结 论

本文提出的一种采用数据挖掘的DoS/DDoS防御模型，使提取的源IP列表可靠性更高，并能有效区分正常流量和异常流量。该模型在具有千兆处理能力的双核处理器Octeon3120上实现，实验数据证明了该模型采用方法的有效性，能够对DoS/DDoS攻击进行有效、实时的防御。

参 考 文 献

[1] MIRKOVIC J, REIHER P. A taxonomy of DDoS attack and DDoS defense mechanisms[J]. ACM SIGCOMM Computer Communications Review, 2004, 34(2): 39-54.

[2] MOHIUDDIN S, RSHKOP S, HAN R, et al. Defending against a large scale denial of service attack[C]//In: Proceedings of the 3rd Annual IEEE Information Assurance Workshop. New York: United States Military Academy West Point, 2002.

[3] CHU N C N, WILLIAMS A, ALHAJJ R, et al. Data stream mining architecture for network intrusion detection[C]//In: Proceedings of the 2004 IEEE International Conference on Information Reuse and Integration. Las Vegas, USA: IRI, 2004: 363-368.

[4] ERTOZ L , EILERT S E, LAZAREVIC A, et al. Detection and summarization of novel network attacks using data mining. Technical Report[R]. University of Minnesota, 2003.

[5] 高　能, 冯登国, 向　继. 一种基于数据挖掘的拒绝服务攻击检测技术[J]. 计算机学报, 2006, 29(6): 944-951.
GAO Neng, FENG Deng-guo, XIANG Ji. A data-mining based Dos detection technique[J]. Chinese Journal of Computers, 2006, 29(6): 944-951.

[6] TARIQ U, HONG M, LHEE K S. A comprehensive categorization of DDoS attack and DDoS defense techniques[J]. LNCS, 2006, 4093: 1025 -1036.

[7] TAO P, LECKIE C, RAMAMOHANARAO K. Prevention from distributed denial of service attacks using history-based IP filtering[C]//In: Proceeding of ICC 2003. Anchorage, Alaska, USA: IRI, 2003: 482- 486.

[8] JIN S Y, YEUNG D S. A covariance analysis model for DDoS attack detection[J]. IEEE Communications Society, 2004, 4(6): 1882-1886.

[9] 程　光, 龚　俭, 丁　伟. 基于统计分析的高速网络分布式抽样测量模型[J]. 计算机学报, 2003, 26(10): 1266-1273.
CHENG Guang, GONG Jian, DING Wei. Distributed sampling measurement model in a high speed network based on statistical analysis[J]. Chinese Journal of Computers, 2003, 26(10): 1266-1273.

[10] KIM Y, LAU W C, CHAO M C, et al. Packetscore: statistics-based overload control against distributed denial-of-service attacks[J]. IEEE INFOCOM, 2004, 4: 2594-2604.

编　辑　熊思亮