深度检测 DDoS 攻击*)

徐 图 何大可
(西南交通大学信息科学与技术学院 成都 610031)

摘 要 为了有效地防御 DDoS 攻击,需要在检测环节尽可能多地获取攻击信息,而现有的方法大多仅注重检测攻击的存在,很难同时给出攻击协议、攻击强度和攻击方式等信息。提出使用多分类的方式,将攻击分为 24 个不同的种类,并用快速分类器 HSMC-SVM 作为分类工具,来完成 DDoS 攻击的多种信息的获取。实验表明,这种方法可以快速完成训练和测试工作,并以较高的识别率识别出不同种类的攻击,为防御环节提供攻击协议、攻击强度和攻击方式等信息。在实际网络中,能满足准确性和实时性的要求,有较强的可行性。

关键词 分布式拒绝服务攻击,单边连接密度,相对值特征(RVF)向量,超球体多类支持向量机(HSMC-SVM)

Detecting DDoS Attacks with a Deep Mode

XU Tu HE Da-ke
(School of Information Science and Technology, Southwest Jiaotong University, Chengdu 610031, China)

Abstract For defending DDoS attacks effectively, the more information about the attacks is required. However, the present methods only stress the existence of attacks, so they are hard to indicate the attack protocols, attack density and attack patterns at one time. Advised to solve the problem with multi-class way. All attacks were classified into 24 classes according to attack protocols, attack density, attack patterns and HSMC-SVM, which is rapid and direct multi-class classifier, is employed to classify them. Shown as the experiments, the measure can implement training and testing processes rapidly and distinguish the attacks with a high true positive rate. The attack information about attack protocols, attack density, and attack patterns was provided by this way. At real network, the measure is feasible for its veracity and real time attribute.

Keywords Distributed denial of service attack, One-way connection density, Relative volume feature vector, Hyper sphere multi-class svm

1 引言

分布式拒绝服务(Distributed Denial of Service, DDoS)攻击仍是互联网的主要威胁。由于 DDoS 攻击本身的欺骗性、多样性和复杂性,使得对 DDoS 攻击进行有效检测和防御仍是一个开放性的课题。

有效遏制 DDoS 攻击检测的前提是能准确地识别 DDoS 攻击流。要识别 DDoS 攻击,就必须对 DDoS 攻击本身具有充分的认识。Christos Douligeris 将 DDoS 攻击进行了分类[1]。按照攻击效果,可分为资源损耗型和带宽损耗型,SYN Flood 属于资源损耗型,UDP Flood 和 ICMP Flood 则属于后者;按照攻击方式,可分为直接型攻击和反射型攻击(DR-DoS)。而不同的攻击,使用的攻击工具和 zombie 的数量不尽相同,因此还有一个攻击强度的概念[2]。对于不同类型的攻击,其防御措施可能不同,比如对直接型攻击和反射型攻击的反应措施就完全不同,这是由于前者使用虚假 IP 地址,而后者看上去都是真实 IP 地址。因此,这就要求检测算法能够尽可能多地提供攻击信息,例如能够同时提供攻击协议、攻击方式、攻击强度等。而基于单一特征检测 DDoS 的方法[3-5],很难做到这一点。文献[6,7]将支持向量机(SVM)运用 DDoS 攻击的识别,但他们仅将用 2 类和 4 类 SVM 进行识别,显然是不够的。

为了使用多类 SVM 对 DDoS 进行识别,并同时提供上述 3 种信息,可以将 DDoS 攻击按攻击方式、攻击协议和攻击强度进行分类。攻击方式分为直接型和反射型;攻击协议分为 SYN Flood, UDP Flood, ICMP Flood 和 MIX Flood,其中 MIX Flood 是指 SYN 包、UDP 包和 ICMP 包轮流发送的 Flood 攻击,而且这 4 种方式均可发起直接型和反射型攻击;攻击强度分为轻度、中度、重度。这样,可将 DDoS 攻击总共分为 24 类,其类别说明见表 1 所示。例如,第 6 类是指直接型重度 UDP Flood 攻击,余类推。

表 1 对 DDoS 攻击进行分类

Attack Type	Attack Density	SYN Flood	UDP Flood	ICMP Flood	MIX Flood
Direct	Light	1	4	7	10
	Medium	2		8	11
	Heavy	3	56	9	12
Reflected	Light	13	16	19	22
	Medium	14	17	20	23
	Heavy	15	18	21	24

这里需要指出对攻击强度的区分依据。文献[2]提出了一种度量 DDoS 攻击强度的单边连接密度(OWCD)的概念,

*)基金项目:四川省青年科技基金(基金号:07JQ0060)。徐 图 博士生,从事机器学习与智能网络安全的研究;何大可 教授,博士生导师,从事密码学、信息安全、并行计算的研究。

可以通过 OWCD 来指示攻击强度。当 OWCD<45 时，属于无攻击；当 45≤OWCD<70，属于轻度攻击；当 70≤OWCD<90，属于中度攻击；若 OWCD≥90，则属于重度攻击。

若将正常数据标记为第 0 类，就获得了一个 25 类的多分类问题。由于分类的类别较多，若用基于 SVM 的 1-v-r 和 1-v-1 多分类器，将分别要训练 25 个和 300 个 SVM，其中 1-v-r 还要求全部样本都参与每个 SVM 的训练。这种分类器均是将多类问题转化为一系列的 2 分类问题，因此其训练效率较低。本文使用 Zhu[8] 和 Xu[9] 提出的称为超球体多类支持向量机(Hyper Sphere Multi-Class SVM，HSMC-SVM)的直接型分类器进行 DDoS 攻击识别。

2 超球体多类支持向量机(HSMC-SVM)

不同于 1-v-r 和 1-v-1 这类间接多分类器，HSMC-SVM 是一种直接型多类分类器，每类样本只参加一个超球体的训练。将所有的训练样本点映射到高维特征空间后，为每类训练样本寻找一个超球，使得这个超球在半径尽可能小的情况下包含该类样本数尽可能多。n 类样本形成 n 个超球，于是在空间中形成像肥皂泡一样的分类结构，如图 1 所示。

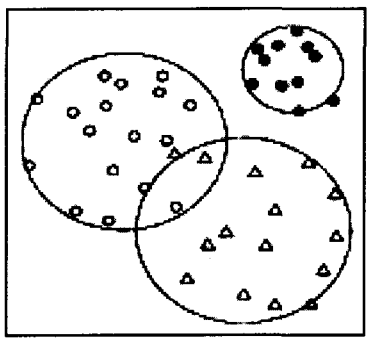

图 1 HSMC-SVM 的分类结构

某个超球体的目标函数可表示为

$$\min R^2+C\sum_i \xi_i$$

$$s.t. \quad ||\Phi(x_i)-a||^2 \leqslant R^2+\xi_i$$

$$\xi_i \geqslant 0 \qquad (1)$$

其中，R 表示超球体半径，a 为球心，x_i 为第 i 个训练样本，$\Phi(x_i)$ 为非线性映射，ξ_i 为松弛变量，C 为正则化参数，C 控制对错分样本的惩罚程度。

式(1)的对偶问题为

$$W(\alpha)=\min\sum_i\sum_j \alpha_i\alpha_j K(x_i,x_j)-\sum_i \alpha_i K(x_i,x_i) \qquad (2)$$

此处 $K(x,y)$ 是满足 Mercer 条件的核函数，$K(x,y)=\langle\Phi(x),\Phi(y)\rangle$，其中 $\langle\Phi(x),\Phi(y)\rangle$ 表示 $\Phi(x)$ 与 $\Phi(y)$ 的内积。

式(2)为二次规划(QP)问题。求解这个 QP 问题，就可获得一个超球体。对于 n 类分类问题，使用基于二次逼近工作集选择法的 SMO 训练算法[10]，分别求解 n 个超球体，就完成了 HSMC-SVM 的训练工作。

在测试阶段，对于某个待测样本 x，计算它到哪个超球面的距离最近，则它就属于哪个类。

对于 n 类分类问题，仅需训练 n 个超球，且每个超球的训练仅需本类的训练样本而不是全部样本，因此 HSMC-SVM 的训练速度远快于 1-v-r 和 1-v-1 多分类器[9]。

3 选择特征向量

为了使用 HSMC-SVM 识别 DDoS 攻击，需要确定一组能够区分上述 24 种攻击的特征向量。由于在 Internet 中，不同结点处，其流量是不同的，为了能适应这种情况，在选择特征时，尽可能选择与绝对流量无关的相对值。此处，首先介绍这组相对值特征(Relative Volume Features，RVF)向量的核心概念——单边连接密度(One-Way Connection Density，OWCD)的概念。

单边连接密度(OWCD)的概念是在文献[2]中提出的，描述如下：在 IP 流中，某个 IP 包发送后，若能收到目标端的回复包，称这两个包构成一个双边连接(Two-Way Connection，TWC)。反之，若某个 IP 包没有收到目标端的回复包，那这个包构成一个单边连接(One-Way Connection，OWC)。在采样间隔 T 中，属于 OWC 的包占总包数的比例，就称为采用间隔 T 下的单边连接密度(OWCD)：

$$OWCD=\frac{\sum OWC\ Packtes}{\sum IP\ Packtes}\times 100\%$$

实验表明，在 DDoS 攻击中，如果使用虚假的源 IP 地址，会使 OWCD 显著增加。正常流中，OWCD 的取值一般在 40 以下；而 DDoS 攻击中，OWCD 会趋于 100。

于是，可以确定一个包含 9 个特征的相对值(Relative Values，RV)特征向量，由于均采用相对值，因此以下各值均为在采样间隔 T 内所采集的总包数中所占的百分比。

(1)tcp_owcd：关于 TCP 协议的 OWCD 值，可用于指示 TCP Flood；

(2)udp_owcd：关于 UDP 协议的 OWCD 值，可用于指示 UDP Flood；

(3)icmp_owcd：关于 ICMP 协议的 OWCD 值，可用于指示 ICMP Flood；

(4)rsyn：携带 SYN 标志的 TCP 包所占的比例，可用于指示 SYN Flood；

(5)rrst：携带 RST 标志的 TCP 包所占的比例，可用于指示反射型 SYN Flood；

(6)rack：携带 ACK 标志的 TCP 包所占的比例，可用于指示 SYN Flood；

(7)rrequest：携带 request 标志的 ICMP 包所占的比例，可用于指示直接型 ICMP Flood；

(8)rreply：携带 reply 标志的 ICMP 包所占的比例，可用于指示反射型 ICMP Flood；

(9)runport：携带“端口不可达”标志的 ICMP 包所占的比例，可用于指示反射型 UDP Flood；

由于在计算 OWCD 时，仅考虑 TCP，UDP，ICMP 协议，因此 OWCD 是 tcp_owcd，udp_owcd，imcp_owcd 之和。

在数据采集时，对每个采样间隔 T 采到的包分别计算上述 9 个值，就获得一个 9 维样本。

4 数值实验

由于 DDoS 攻击原理很简单，我们开发了 DDoS 攻击工具 Attacker，用于发起 24 种不同类型的攻击。实验是在西南交通大学校园网上进行的，实验所使用的网络结构示意图由图 2 所示。在边缘路由器处有约 200k 的正常流量作为检测主机的背景流量。

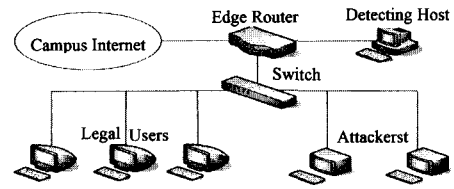

图 2 攻击实验网络结构

4.1 HSMC-SVM 的训练

由 Attacker 分别发起 24 种攻击，使用 1～3 台攻击机分别产生轻度、中度和重度攻击，每台攻击机上的 Attacker 均使用 20 线程进行攻击。使用 WinPcap 抓包，WinPcap 运行于检测主机上，采样间隔取 0.1s，每类攻击采样 120s，获得 1200 个训练数据，包括正常数据在内的 25 类样本，共得 30000 个训练样本。

使用 HSMC-SVM 训练这些样本，取参数 $C=0.8$，训练精度 $e=0.01$，核函数选用 RBF 核，核参数 $\sigma=8$。用于训练的电脑配置为 Pentium IV 2.6G，512M RAM，编译环境为C++ Builder 6.0，训练时间为 151.656s。

4.2 攻击数据的测试

为了验证使用 HSMC-SVM 识别 DDoS 攻击的有效性，这里进行了 2 组测试实验。第 1 组测试数据仍采自 Attacker 发起的攻击；第 2 组测试数据则来自真实的强力攻击工具 TFN2K 和傀儡僵尸 DDoS 攻击集合(以下简称傀儡僵尸)。

第 1 组测试数据的采集方法与训练数据的采集方法相同，仍由 Attacker 发起攻击，采样间隔 0.1s，每类攻击采样 100s，获得 1000 个测试样本，25 类共得测试样本 25000 个，而且每个样本都提前可以给出类标。因此，将这些样本送到训练后的 HSMC-SVM 中进行检测，可以给出每类的检测率。检测结果由表 2 给出。

表 2 第 1 组数据的检测结果

Class	True Positive Rate (%)	Class	True Positive Rate (%)	Class	True Positive Rate (%)	Class	True Positive Rate (%)	Class	True Positive Rate (%)
0	100	1	89.2	2	89.8	3	99.1	4	96.1
5	96.2.	6	100	7	95.6	8	99.2	9	99.9
10	98.1	11	99.4	12	99.3	13	99.2	14	98.2
15	99.9	16	89.9	17	76.35	18	99.9	19	87.6
20	97.4	21	99.3	22	92.48	23	87.78	24	99.59

设总检测率为被正确分类样本数占总样本数的百分比，则总检测率为 95.58%，测试时间为 96.578s，测试一个样本平均耗时 3.86ms。

表 2 的结果表明，HSMC-SVM 完全能将 25 类测试样本分开，并获得较高的检测率。

第 2 组测试数据来自真实的 DDoS 工具，采样间隔 0.1s，每次采样 60s，得 600 个测试样本。由于这些样本的类标需要检测后才能获得，无法提前给出，因此用图表的方法将检验结果显示出来。为了节约篇幅，每张图上将画出多次攻击的检测结果，但并非说明这些攻击是同时发生的。由于 TFN2K 的发包率很快，在一台攻击机上运行 TFN2K，分别发起直接型 SYN Flood，UDP Flood，ICMP Flood 和 MIX Flood 攻击，采样后送到训练好的 HSMC-SVM 进行检测，其结果由图 3 所示，其中横坐标是时间，纵坐标为攻击类型。

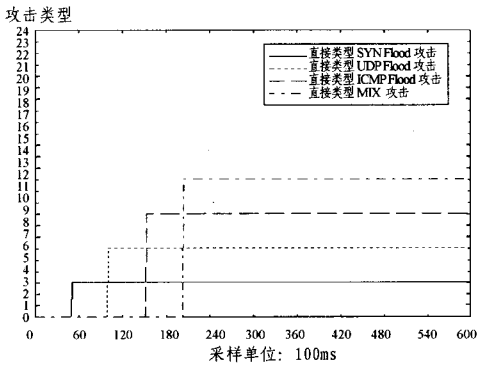

图 3 TFN2K 发起的直接型攻击的检测结果

从图 3 中可以看出，每次攻击发起前，均为正常数据流，不同的攻击给出了正确的类标，而且基本都被识别为重度攻击。从图中还可以看出，一旦攻击发生，立即就进入重度攻击状态，根本没有中间的过渡过程。

图 4 和图 5 分别示出了由傀儡僵尸发起的直接型和反射型攻击，都是在攻击发起以后才开始采集数据。图 4 可以看出傀儡僵尸发起的直接型 TCP SYN Flood 和直接型 UDP Flood 攻击均被识别为重度攻击，而 ICMP Flood 却被识别为中度攻击。可是，从采集样本的 OWCD 值看，应属于重度。分析后发现，由于傀儡僵尸发出的 ICMP 包中的类型标志位被错误地设置成了 69，这是一种非法的 ICMP 类型，从而使得特征中的 rrequest 变得异常，稍稍影响了分类结果。

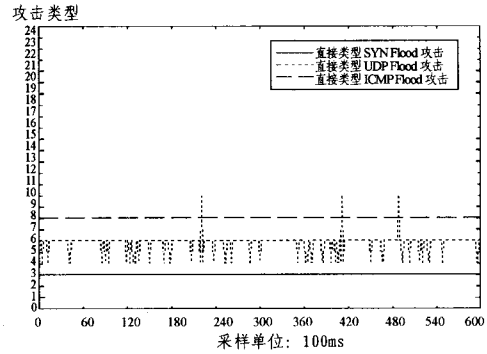

图 4 傀儡僵尸发起的直接型攻击检测结果

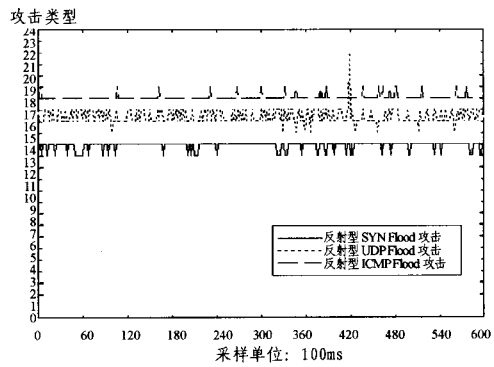

图 5 傀儡僵尸发起的反射型攻击检测结果

图 5 为傀儡僵尸发起的反射型攻击的检测结果，对反射型 SYN Flood 和反射型 UDP Flood 都被识别为重度攻击。由于傀儡僵尸不能发送合法的 ICMP 包，因此无法进行反射型攻击。此处的反射型攻击由 Smurf V12 攻击工具发起，识别结果为轻度攻击，这是由于其发包率较低。

图 3－图 5 的结果表明，识别出攻击的类标后，就可以获

得攻击协议、攻击方式和攻击强度等信息。

5 与相关工作比较

为了分析使用 HSMC-SVM 识别 DDoS 攻击的性能，此处将此算法与已有的工作进行比较，比较的项目为能否识别不同协议发起的攻击，能否指示攻击强度，能否指示攻击协议，能否指示攻击方式 4 个方面。

2003 年，Cheng Jin 提出基于网络包的 TTL 值的检测算法[11]；2004 年出现了基于网络相似度[12]、基于网络的自相似性[13]、基于网络包的 VDR 值[14]的检测算法；2005 年，出现了基于流连接密度（FCD）[6]、基于神经网络[15]、基于多个 SVM[7]以及基于 SYN 包流量分布[16]的检测算法；2007 则出现了以 OWCD 来检测 DDoS 的算法[2]。比较的结果显示在表 3 中，"√"表示具有该功能，反之为"×"。

表 3 的结果显示，目前许多检测算法均将注意力集中到如何检测到攻击，而忽略了提供更多攻击信息的工作，因此显得检测工作并不全面。相比之下，使用 HSMC-SVM 的方法能更深入地检测 DDoS 攻击。

不过，用 HSMC-SVM 检测 DDoS 攻击，也有其不足之处。当出现不同的攻击行为，这种方法将失效。例如，我们曾将 MIX Flood 攻击中三种协议的比例改变后，再送入 HSMC-SVM 检测，则完全不能获得正确的检测结果，这是因为训练样本中的 MIX Flood 攻击的三种协议比例仅为 1∶1∶1。因此，如何提高 HSMC-SVM 检测方法的灵活性，仍是一个待研究的课题。

表 3 与相关工作的比较结果

Algorithm	Distinguish DDoS	Indicate Density	Indicate Protocol	Indicate Pattern
FCD[6]	√	×	×	×
TRA[7]	√	×	×	×
ANN[15]	only UDP Flood	×	×	×
SYN Packets[16]	only SYN Flood	√	×	×
Likeness[12]	√	√	×	×
TTL[11]	√	√	×	×
Self-Similarity[13]	√	√	×	×
OWCD[2]	√	√	×	×
VDR[14]	√	√	√	×
HSMC-SVM	√	√	√	√

结束语 要在低虚警率和低误警率的条件下，有效防御 DDoS 攻击，需要检测环节能提供更多的攻击信息，而目前大多的检测算法仅将注意力集中到如何检测到攻击，很难同时识别攻击强度、攻击协议和攻击方式等信息。本文通过多分类的方式，将攻击分为 24 种不同的类型，并利用快速训练算法 HSMC-SVM，实现了这一目标。实验表明，这种方法通过提供识别的类标，同时提供攻击强度、攻击协议和攻击方式等较全面的攻击信息，为 DDoS 的防御环节针对不同类型的攻击进行有效防御提供了保障。

参 考 文 献

[1] Douligeris C, Mitrokotsa A. DDoS Attacks and Defense Mechanisms: A Classification // Proceedings of the 3rd IEEE International Symposium on Signal Processing and Information Technology. 2003: 190-193

[2] Xu Tu, He Da-ke, Zheng Yu. Detecting DDoS Attack Based on One-way Connection Density // Proceedings of Tenth IEEE International Conference on Communication Systems. 2006

[3] Cheng C-M, Kung H, Tan K S. Use of spectral analysis in defense against Dos attack // Proceedings of IEEE GLOBECOM. Division of Engineering and Applied Science Harvard University

[4] Feinstein L, Schnachenberg D, Balupari R, et al. Statistical Approaches to DDoS Attack Detection and Response // Proceedings of the DARPA Information Survivablility Conference and Exposition. 2003

[5] Jin Shuyuan, Yeung D S. A Covariance Analysis Model for DDoS Attack Detection. IEEE Communications Society, 2004: 1882-1886

[6] 孙钦东，张德运，高鹏. 基于时间序列分析的分布式拒绝服务攻击检测[J]. 计算机学报，2005，28(5)：767-773

[7] Seo J, Lee C, Shon T. A New DDoS Detection Model Using Multiple SVM and TRA // EUC Workshops 2005. LNCS 3832. 2005: 976-985

[8] 朱美琳，刘向东，陈世福. 用球结构解决多分类问题[J]. 南京大学学报：自然科学版，2003，39(2)：153-158

[9] Xu Tu, He Dake, Luo Yu. A New Orientation for Multi-Class SVM // Proceedings of the SNPD. 2007: 899-904

[10] 徐图，罗瑜，何大可. HSMC-SVM 的二次逼近快速训练算法. 电子与信息学报(已录用)

[11] Jin Cheng, Wang Haining, Shin K G. Hop-count Filtering: An Effective Defense Against Spoofed DDoS Traffic // Proceedings of the 10th ACM Conference on Computer and Communications Security. 2003

[12] 何慧，张宏莉，张伟哲，等. 一种基于相似度的 DDoS 攻击检测方法[J]. 通信学报，2004，25(7)：176-184

[13] Xiang Y, Lin Y, Lei W L, et al. Detecting DDoS Attack Based on Network Self-Similarity // IEE Proc. Commun. 2004, 151(3): 292-295

[14] Limwiwatkul L, Rungsawang A. Distributed Denial of Service Detection Using TCP/IP Header and Traffic Measurement Analysis // Proceedings of International Symposium on Communications and Information Technologies. 2004: 605-610

[15] Siaterlis C. Detecting incoming and outgoing DDoS attack at the edge using a single set of network characteristics // Proceedings of the 10th IEEE Symposium on Computers and Communication. 2005

[16] Ohsita Y C, Ata YuiChi, Murata M. Detecting Distributed Denial-of-Service Attacks by Analyzing TCP SYN Packets Statistically // Global Telecommunications Conference. 2004: 2043-2049

（上接第 72 页）

[3] Falk A, Katabi D, Pryadkin Y. Specification for the Explicit Control Protocol (XCP). draft-falk-xcp-02. txt (work in progress), November 2006

[4] Chiu D, Jain R. Analysis of the Increase and Decrease Algorithms for Congestion Avoidance in Computer Networks. Journal of Computer Networks and ISDN, 1989, 17(1): 1-14

[5] Low S, Andrew L, Wydrowski B. Understanding XCP: Equilibrium and fairness // Proc. IEEE INFOCOM. Miami, FL, USA, 2005

[6] Wang P, Mills D L. Simple analysis of XCP equilibrium performance // Proc. CISS 2006. Princeton, NJ, USA, 2006

[7] Xia Y, Subramanian L, et al. One more bit is enough. ACM SIGCOMM Computer Communication Review, 2005, 35(4): 37-48

[8] Wydrowski B P, Zukerman M. MaxNet: A congestion control architecture for max-min fairness. IEEE Commun. Lett., 2003, 6(11): 588-599

[9] Welzl M. Network Congestion Control. John Wiley & Sons Ltd, 2005

[10] The network simulator ns-2. 30. http://www.isi.edu/nsnam/ns