基于 ASPQ 的 LDoS 攻击检测方法

张静[1]，胡华平[1,2]，刘波[1]，肖枫涛[1]
(1. 国防科技大学 计算机学院，湖南 长沙 410073；2. 61070 部队，福建 福州 350003)

摘 要：分析了 LDoS 攻击对缓冲区队列平均报文长度(ASPQ)的影响，通过实验获得队列报文平均长度在遭受攻击情况下的改变。在此基础上提出了基于 ASPQ 的 LDoS 攻击检测方法，并应用在目前典型的队列管理算法(Droptail 和 RED)中。最后，通过实验证明该方法可以有效检测 LDoS 攻击。

关键词：低速率拒绝服务；队列平均报文长度；检测
中图分类号：TP301 **文献标识码**：A **文章编号**：1000-436X(2012)05-0079-06

Detecting LDoS attack based on ASPQ

ZHANG Jing[1], HU Hua-ping[1,2], LIU Bo[1], XIAO Feng-tao[1]
(1. School of Computer, National University of Defense and Technology, Changsha 410073, China;
2. The Army of 61070, Fuzhou 350003, China)

Abstract: Based on the analysis of the effects on average size of packet in the queue which LDoS attack makes, the change of this value was got by simulation on NS2. So detection algorithm was proposed, and was applied on Drop-tail and RED, which were typical queue management algorithm. The result of simulation shows that the algorithm can effectively detect the LDoS attack.

Key words: low-rate denial-of-service; average size of packet in the queue; detection

1 引言

目前，社会对 Internet 的依赖性日益增强，例如电子商务、电子政务、网上银行等技术的应用。但由于网络本身存在一定的不足之处，因此面临很多威胁，拒绝服务攻击便是其中之一。拒绝服务攻击通过大量的垃圾数据来阻塞网络，使正常的数据传输不能得到有效服务。

2003 年，Kuzmanovic 在 SIGCOMM 会议上提出的低速率拒绝服务（LDoS, low-rate denial-of-service）攻击是一种新型的拒绝服务攻击[1]，周期性的发送高强度的短脉冲，即大量短小数据分组，使得攻击流可以周期性地占用路由器的资源，导致报文丢弃，造成所有受其影响的合法 TCP 流进入超时重传状态，最终使得受害者的吞吐量大幅度降低，从而达到攻击目的。随后出现 RoQ 攻击[2,3]和 Pulsing Attacks[4]亦是利用此原理。与传统的拒绝服务攻击相比，LDoS 攻击是一个小流量汇聚的攻击，使得攻击流量更加隐蔽，在网络上更加难以被现有的拒绝服务攻击检测方法发现。

2 相关性研究

由于 LDoS 攻击的原理是利用 TCP/IP 协议中超时重传存在的一致性，因此 Kuzmanovic 在 2003 年提出 Shrew 攻击的同时，就提出了随机化端系统的最小超时等待时间的取值来破坏超时重传的一致

收稿日期：2010-12-28；**修回日期**：2011-04-07
基金项目：国家高技术研究发展计划（“863”计划）基金资助项目（2008AA01Z414）；国家自然科学基金资助项目(61003303)
Foundation Items: The National High Technology Research and Development Program of China (863 Program) (2008AA01Z414); The National Natural Science Foundation of China (61003303)

性[1]，以达到降低 LDoS 攻击效果的目的。但是该方法在网络上的部署需要对现有的协议进行修改，实现非常困难。

LDoS 攻击数据流体现出的行为特征成为 LDoS 攻击检测考虑的出发点。根据攻击数据流在短时间内依然有较高的流量或到达的数据分组个数突然大幅度增加，Kuzmanovic 提出利用路由器队列管理算法对高速数据流的报文进行丢弃来降低攻击效果[2]；文献[5]通过分析路由器队列缓冲区的大小对攻击效果的影响提出相应的对抗措施；HAWK 算法[6]根据 LDoS 攻击数据流的强度、攻击周期内的持续时间和攻击周期，对现有的队列管理算法进行改进，实现对周期性的短时间内高速率数据流进行过滤，与此算法相似的还有 Zhang 提出的 RRED 算法[7]。

Sun H 等则根据攻击对吞吐量的影响，提出一种分布式的检测算法[8]，此外 Chen Yu 在文献[9]中通过对正常和攻击 2 种情况下流量的能量谱密度进行对比，找出攻击数据流的特征，然后通过路由器间广播检测信息来实现对此攻击的协同对抗。

从上面的介绍可以看出，目前针对 LDoS 攻击的对抗主要从是对攻击数据流的时频特征进行分析或破坏攻击存在的条件角度出发，但对 LDoS 攻击对路由器缓冲区的队列平均报文长度有何影响缺乏相应的分析。因此本文分析了 LDoS 攻击对缓冲区队列平均报文长度(ASPQ)的影响，并提出相应的检测方法。

定义 1 队列平均报文长度（ASPQ, average size of packet in queue）。队列平均报文长度是指在时刻 t，队列中所有报文的平均长度即瞬时队列平均报文长度。

3 基于 ASPQ 的 LDoS 攻击检测方法

3.1 检测依据

LDoS 攻击通过周期性地发送高强度的短脉冲，使得攻击流可以周期性地占用路由器的资源，导致报文丢弃，造成受其影响的合法 TCP 流进入超时重传状态，最终使得受害主机的服务能力大幅度降低，从而达到攻击目的。目前对 LDoS 攻击对抗方法的研究有很多，得出了很多有用的结论。本文提出检测方法的主要依据有 2 个，分别是攻击报文在队列的占有比率[10]和攻击报文的大小与攻击效果之间的关系[11]。

依据 1 根据文献[10]中的仿真实验可知，在遭受攻击时，攻击数据流在路由器缓冲区的队列中会占有一定的比例，攻击效果越好，比例越大。在文献[10]的攻击环境下，比例达到 90%以上。由此可知，在攻击时刻，路由器缓冲区队列中的报文中有一部分是攻击报文。

依据 2 在攻击源速率恒定的情况下，若攻击源数目为 N，汇聚后的攻击速率为 C，一个攻击周期的攻击持续时间为 L，攻击报文的大小为 $Size$，则一个攻击周期内攻击流发送的数据分组个数为

$$N\lceil (CL)/(8N\cdot Size)\rceil \tag{1}$$

由式(1)可知，在 C 不变的情况下，攻击报文的长度越大，攻击源发送的数据分组个数就越少。在同样的攻击环境下，不同大小的攻击数据分组带来的攻击性能如图 1 所示[11]。从图中可知，攻击报文的长度越大，对正常数据流的影响越小，从而导致攻击性能的降低。因此，在攻击速率一定的情况下，攻击者必须使用短小数据分组才能达到较好的攻击效果。

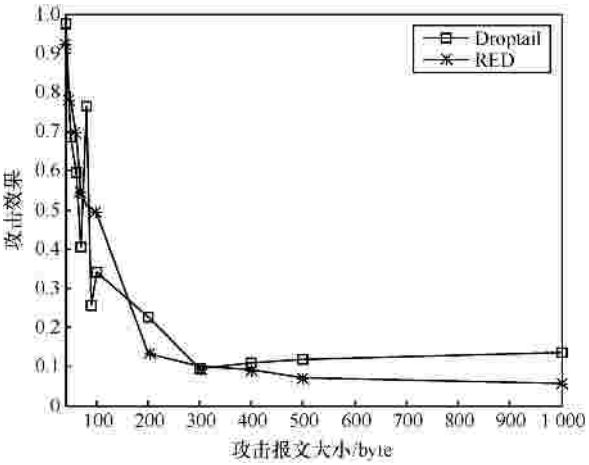

图 1 攻击报文大小对攻击效果的影响

设在时刻 t，攻击报文在队列中所占的比例为 P_{Attack}，正常报文所占比例为 P_{Normal}，正常情况下队列平均报文大小的数学期望值为 $\overline{Size}$，则该时刻队列平均报文长度为

$$L_{\text{Avg}}=P_{\text{Attack}}Size+P_{\text{Normal}}\overline{Size} \tag{2}$$

由式(2)可知，在未遭受攻击的情况下，队列平均报文长度为 $\overline{Size}$；在遭受攻击的情况下，由于 P_{Attack} 占据一定的比例，而且攻击报文的长度和 $\overline{Size}$ 存在一定的差距，因此队列平均报文长度即 ASPQ

的值会有一定的变化。结合前面的 2 个依据可知：在攻击和未攻击 2 种情况下，ASPQ 的值会呈现下降趋势。在此基础上，本文提出基于 ASPQ 的 LDoS 攻击检测方法。

3.2　序列模型的建立

若队列中的瞬时报文数目为 N_t，每个报文的长度为 $L_i, i \in [1, N_t]$，则 ASPQ 值的计算公式为

$$V_{\mathrm{ASPQ}} = \sum_{i=1}^{N_t} L_i / N_t \tag{3}$$

定义 2　采样时间 t。采样时间指计算队列平均报文长度的时刻。队列处理每一个报文的时刻就是队列的采样时刻，计算此时刻的 ASPQ 值。本文中的采样时间 t 与其他文献中的采样时间不同，采样时间间隔不是一个定值，而是一个变化的量，因此它不是一个有规律的值，而是一个变量，取值范围为 $[0, +\infty)$。

根据上面的定义对队列进行数据处理，可以得到在时间长度为 T、采样次数为 N 的情况下，得到 ASPQ 序列，记为 $L_{\mathrm{Avg}}(1), L_{\mathrm{Avg}}(2), \mathrm{L}, L_{\mathrm{Avg}}(N)$，其中，$L_{\mathrm{Avg}}(n) =< t, V_{\mathrm{ASPQ}}(n) >$。通过本节的定义和对数据的处理，得到 ASPQ 序列。

3.3　基于 ASPQ 的 LDoS 攻击检测方法

经过前面的分析可知，在遭受 LDoS 攻击的情况下，队列平均报文长度会发生变化。本文在得到 ASPQ 序列的基础上，采用变化点检测算法对 LDoS 进行检测。

定义 3　队列平均报文变化程度（CDASPQ, change degree of average size of packet in queue）。队列平均报文变化程度指采样时刻 CDASPQ 值的差异与正常情况下的比值。

CDASPQ 的计算方法为

$$V_{\mathrm{CDASPQ}} = (\overline{Size} - L_{\mathrm{Avg}}(n) : V_{\mathrm{ASPQ}}(n)) / \overline{Size} \tag{4}$$

CDASPQ 值的计算公式可做进一步推导，如式(5)所示。

$$\begin{aligned} &(\overline{Size} - L_{\mathrm{Avg}}(n) : V_{\mathrm{ASPQ}}(n)) / \overline{Size} \\ &= 1 - (P_{\mathrm{Attack}} Size + P_{\mathrm{Normal}} \overline{Size}) / \overline{Size} \\ &= 1 - (P_{\mathrm{Attack}} Size / \overline{Size} + P_{\mathrm{Normal}}) \\ &= P_{\mathrm{Attack}} (1 - Size / \overline{Size}) \end{aligned} \tag{5}$$

因此，用式(4)对 ASPQ 序列做进一步的处理，得到 CDASPQ 序列 $D_1, D_2, \mathrm{L}, D_N$，其中，$D_n =< L_{\mathrm{Avg}}(n) : t, V_{\mathrm{CDASPQ}}(n) >, n \in [1, N]$。

通过前面得到的攻击报文大小与攻击性能的关系可知，攻击效果越好，CDASPQ 的值将会越大。由于攻击要持续一段时间，因此 CDASPQ 的值会有一段时间保持在较高的位置。如何消除此种情况，需要对 CDASPQ 序列做进一步的处理。

$$\begin{aligned} &D'_n =< D_n : t_n, V'_{\mathrm{CDASPQ}}(n) \\ &= f(D_n : V_{\mathrm{CDASPQ}}(n) - D_{n-1} : V_{\mathrm{CDASPQ}}(n-1)) D_n : V_{\mathrm{CDASPQ}}(n) >, \\ &n \in [2, N], D'_1 =< t_1, 0 > \\ &f(D_n : V_{\mathrm{CDASPQ}}(n) - D_{n-1} : V_{\mathrm{CDASPQ}}(n-1)) \\ &= \begin{cases} 1\, D_n : V_{\mathrm{CDASPQ}}(n) - D_{n-1} : V_{\mathrm{CDASPQ}}(n-1) \neq 0 \\ 0\, D_n : V_{\mathrm{CDASPQ}}(n) - D_{n-1} : V_{\mathrm{CDASPQ}}(n-1) = 0 \end{cases} \end{aligned} \tag{6}$$

本文采用式(6)的方式对 CDASPQ 序列做进一步的处理得到 CP 序列 $D'_1, D'_2, \mathrm{L}, D'_N$，而且该序列有以下性质：

$$\max\{D'_n : V'_{\mathrm{CDASPQ}}(n)\} \leq P_{\mathrm{Attack}} \tag{7}$$

如何判断是否发生攻击，设检测阈值为 h，根据下式判断是否发生 LDoS 攻击：

$$\begin{cases} D'_n : V'_{\mathrm{CDASPQ}}(n) \geq h, \text{攻击发生} \\ D'_n : V'_{\mathrm{CDASPQ}}(n) < h, \text{攻击未发生} \end{cases} \tag{8}$$

3.4　阈值的设定

检测阈值 h 可根据式(5)推导出如下的关系式：

$$\begin{cases} P_{\mathrm{Attack}}(1 - Size / \overline{Size}) \geq h \Rightarrow Size < (P_{\mathrm{Attack}} - h)\overline{Size} / P_{\mathrm{Attack}} \\ Size > 0 \end{cases} \tag{9}$$

根据 $Size > 0$，可知 h 的设置应满足 $h < P_{\mathrm{Attack}}$，并且对于 h 的每个值，其所能检测的攻击是有一定范围的。阈值的设置有 2 个原则：

1) 尽可能检测出不同报文大小的攻击；

2) 必须检测出攻击效果较好的 LDoS 攻击。

因此面对不同报文大小的 LDoS 攻击，如何设置检测阈值以期达到较好的检测效果，需要根据在不同报文大小的攻击下 CDASPQ 值的变化情况对阈值进行设置。

4　实验结果及分析

4.1　仿真环境

采用文献[11]中的实验环境，攻击数据流如图 2 所示，进行 10 次攻击，每次攻击持续时间为 200ms，

为了获得更好的针对 Droptail 的攻击效果，攻击方式采取多源单点攻击。

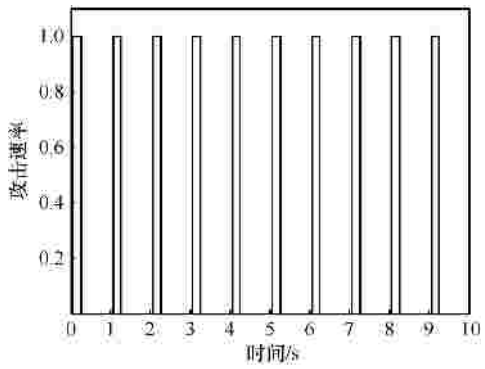

图 2 攻击数据流

4.2 队列平均报文长度

本文通过仿真网络，在 Droptail 和 RED 2 种典型的队列管理算法基础上比较队列平均报文长度在正常和遭受攻击 2 种情况下的变化。

通过仿真实验，获得队列平均报文长度变化在正常情况下和 LDoS 攻击情况下两者的比较，比较结果如图 3 所示。由图 3 可知，在遭受攻击的情况下，此时队列中攻击报文会占据绝大部分，通过队列平均长度的计算公式可知，攻击将导致队列平均报文长度发生急剧的变化。图 3(b)同时还验证了 TCP 协议的超时重传机制中对重传时间的指数增长计算方式。

4.3 检测结果及分析

根据文献[10]得出的攻击流所占的比例，结合式(7)，根据图 3(a)、图 3(c)得到的数据，该实验中 $\overline{Size}$ 值设为 1040byte。在攻击报文大小为 40byte 情况下，得到的 CDASPQ 数据如图 4 所示，CDASPQ 值在攻击情况下的变化与前面分析相吻合。

由图 4 可知，在遭受到攻击的情况下，CDASPQ 的值会快速增加至接近 1 的位置。从实验数据中来看，提出的算法在检测针对 Droptail 的 LDoS 攻击时，仅在 4 次攻击持续时间内检测到攻击的发生。从图 1 可知，此时攻击的效果非常好，结合图 3(b)的数据说明攻击使得 TCP 数据流同步进入超时重传阶段。根据超时重传机制可知其他的 6 次攻击持续时间对 TCP 数据流的影响非常小，因此 ASPQ 值的变化非常小，以致算法无法检测攻击的发生。因

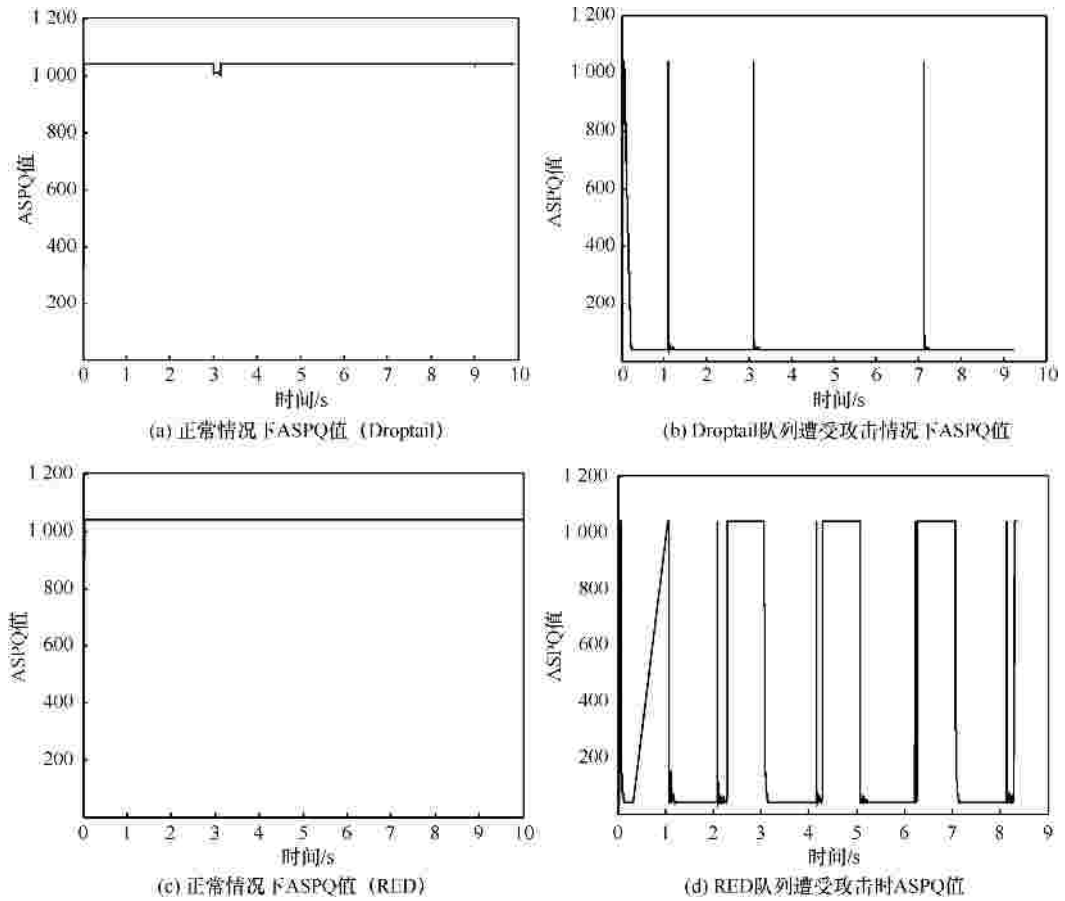

图 3 队列平均报文长度对比

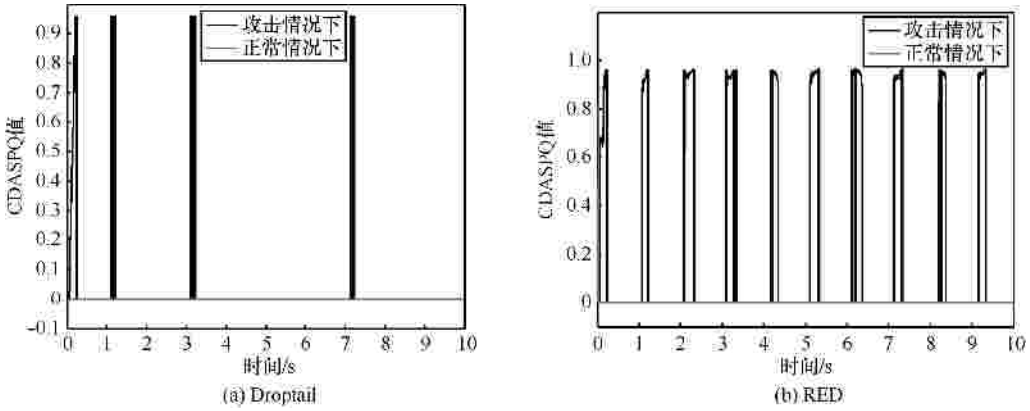

图 4　CDASPQ 值在 LDoS 攻击情况下的变化

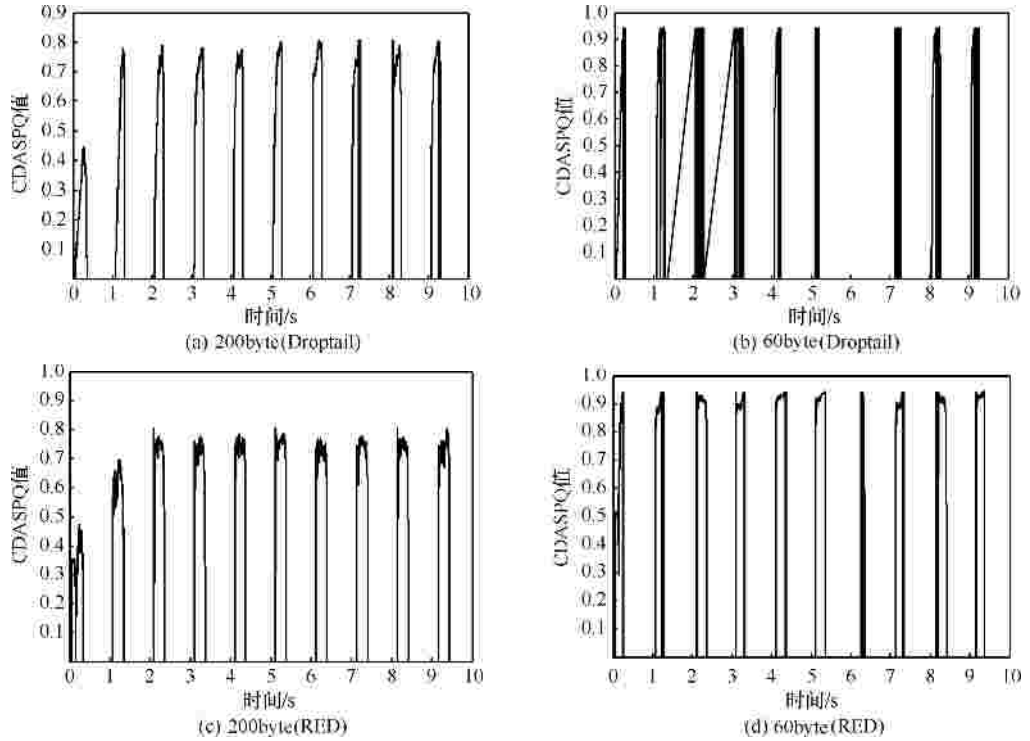

图 5　攻击报文大小改变时 CDASPQ 值的变化

此本文提出的算法仅可以检测出对 TCP 数据流有一定影响的攻击。正如图 4(b)所示，LDoS 对 RED 的攻击效果虽然没有攻击 Droptail 的效果好，但每次攻击均对 TCP 数据流均有一定的影响，因此可以检测出 LDoS 的 10 次攻击。

如果攻击者改变攻击报文的大小，该算法是否依然有效，在本节中以 200byte 和 60byte 为例对算法进行分析。从图 5 可知，攻击报文的大小虽然改变，但攻击时间内依然会引起 CDASPQ 值的增加，算法依然有效，但是随着攻击报文的增大，检测阈值需要相应的降低以提高算法的检测率。从图 1 可知，在 60byte 和 200byte 2 种大小的攻击报文情况下，攻击效果会大幅降低，尤其是 200byte 的情况，攻击效果仅有 0.23。

如何设置阈值，由上面的数据可知，在攻击报文大小为 200byte、攻击效果仅有 0.23(Droptail)、0.14(RED)的情况下，CDASPQ 的值最小变化幅度均超过 0.4。因此，在实验中，算法的检测阈值设为 0.4，可以检测攻击报文大小在 200byte 以内的 LDoS 攻击。攻击者为了逃避该算法可能会增大攻击报文、提高攻击速率，这样就使得主动队列管理算法本身具有对抗 LDoS 攻击的能力。

4.4　与其他方法的对比

文献[5]通过增大缓冲区的大小，迫使攻击者加大攻击速率以达到较好的攻击效果，从而可以使得主动队列管理算法丢弃高速的攻击数据流以达到对抗

LDoS 攻击的目的，而本文提出的方法则可以检测一般的 LDoS 攻击，更加具有普适性。文献[10]通过提取攻击数据流在路由器缓冲区的队列中所占的比例，发现在遭受攻击的情况下，攻击数据比例达到 90%以上，但是随着攻击数据分组的增大，攻击效果的降低，攻击数据所占的比例会大幅下降，此时，文献中提到的方法将会产生一定的漏报，本文提出的方法可以很好地解决这一问题。而 2010 年提出的 RRED 算法如果面对通过分布式实施的 LDoS 攻击，算法的依据将会失去意义，导致对抗效果的降低，基于 ASPQ 的 LDoS 攻击检测方法将报文不能伪造的特性之一——报文长度作为检测的依据，可见算法具有较好的顽健性。

LDoS 攻击可以有多种实现方式，例如变周期、变速率等，本文提出的算法对其他方式实现的 LDoS 攻击依然会有一定的效果。从前面对算法的分析可知，算法进行的实时数据采样，与 LDoS 攻击周期无关，而且变速率是为了更快地达到较好的攻击效果，依然会对 TCP 数据流有一定的影响，结合图 1 和图 5 的数据可知，只要此类攻击有一定的攻击效果，本文提出的算法就可以检测出此类攻击的发生。

5 结束语

本文提出了基于 ASPQ 方法的 LDoS 攻击检测方法，从报文平均大小变化的角度来看 LDoS 攻击对其的影响。通过在 40byte、60byte 和 200byte 3 种情况下获得的 CDASPQ 的值的变化，综合考虑，设定检测阈值。从实验结果来看，该算法简单有效，与其他方法对比，检测准确率较高，有一定的普适性。但是算法还存在一些值得改进之处，例如，没有与相应的对抗措施结合；阈值能否根据具体情况进行实时变化，用以较早地检测出攻击的存在，从而可以较早采取对抗措施，降低攻击效果，这些将是下一步的研究重点。

参考文献：

[1] KUZMANOVIC A, KNIGHTLY E W. Low-rate TCP-targeted denial-of-service attacks[A]. Proceedings of ACM SIGCOMM 2003[C]. Karlsruhe, Germany,2003.

[2] GUIRGUIS M, BESTAVROS A, MATTA L. Exploiting the transients of adaptation for RoQ attacks on Internet resources[A]. Proc IEEE International Conference on Network Protocols (ICNP)[C]. Berlin, Germany, 2004.

[3] GUIRGUIS M. Reduction of quality (RoQ) attacks on Internet end-systems[A]. Proceedings of the 24th IEEE INFOCOM[C]. Miami, Florida, 2005.

[4] LUO X，CHANG R．On a new class of pulsing denial-of-service attacks and the defense[A]. Proceedings of Network and Distributed System Security Symposium (NDSS'05)[C]. San Diego, CA, 2005.

[5] SARAT S, TERZIS A. On the effect of router buffer sizes on low-rate denial of service attacks[A]. Proceedings of the 14th International Conference on Computer Communications and Networks[C]. San Diego, CA, United States, 2005.

[6] KWOK Y K. HAWK: halting anomalies with weighted choking to rescue well-behaved TCP sessions from shrew DDoS attacks[A]. ICCNMC 2005[C]. Zhangjiajie, China, 2005.

[7] ZHANG C W, YIN J P, CAI Z P, *et al*. RRED: Robust RED algorithm to counter low-rate denial-of-service attacks[J]. IEEE Communication Letter,2010,14(5):489-491.

[8] SUN H B, LUI J C S, YAU D K Y. Defending against low-rate TCP attacks: dynamic detection and protection[A]. Proceedings of IEEE International Conference on Network Protocols[C]. Berlin, Germany, 2004.

[9] CHEN Y, HWANG K. Collaborative detection and filtering of shrew DDoS attacks using spectral analysis[J]. Journal of Parallel and Distributed Computing, 2006, 66(9):1137-1151.

[10] 吴志军，张东. 低速率DDoS攻击的仿真和特征提取[J]. 通信学报, 2008, 29(1):71-76.
WU Z J, ZHANG D. Attack simulation and signature extraction of low-rate DDoS[J]. Journal on Communications, 2008, 29(1):71-76

[11] HU H P, ZHANG J, LIU B, *et al*. Simulation and analysis of distributed denial-of-service attacks[A]. 2010 International Conference on Computer Sciences and Convergence Information Technology[C]. Seoul, Korea, 2010.

作者简介：

张静（1984-），女，河北柏乡人，国防科技大学博士生，主要研究方向为网络与信息安全。

胡华平（1967-），男，福建邵武人，国防科技大学博士后、教授、博士生导师，主要研究方向为网络与信息安全、密码学。

刘波（1973-），男，江西九江人，国防科技大学博士生、副研究员、硕士生导师，主要研究方向为网络与信息安全。

肖枫涛（1981-），男，河南沁阳人，博士，国防科技大学讲师，主要研究方向为网络安全。