基于 Snort 的动态自适应多媒体数据处理方法①

赵 旭

(西安工程大学 计算机科学学院，西安 710048)

摘 要：针对 Snort 网络入侵检测系统在大网络流量下出现丢包率高的问题，通过对多媒体数据特征进行分析，设计了对网络流量中多媒体数据包的识别方法和两种处理方法，并提出动态自适应多媒体数据处理方法，该方法可以根据网络流量变化和系统处理能力变化自动调整对多媒体数据的处理方式，从而有效降低丢包率。

关键词：NIDS；多媒体；动态自适应多媒体数据处理方法

Dynamic Self-Adapting Multimedia Data Processing Method Based on Snort

ZHAO Xu

(Department of Computer Science, Xi'an Polytechnic University, Xi'an 710048, China)

Abstract: To address the problem of high rate of dropping packets in high network flow of Snort network intrusion detection system, a way of multimedia data identification in network flow and two approaches to processing multimedia data has been designed by analyzing the characteristic of multimedia data in this article. The method of Dynamic Self-Adapting Multimedia Data Processing is also introduced. According to the changes of network flow and the capability of Snort disposal, this method could automatically adjust the way of detecting multimedia data. This method could effectively reduce packet loss ratio of Snort.

Keywords: NIDS; multimedia; dynamic self-adapting multimedia data processing method

1 引言

Snort 是一款著名的开源网络入侵检测系统，它可以对网络中捕获的每个数据包都与存储在规则库中的 3 千多条规则进行模式匹配，从中发现可能存在的攻击。当网络流量较大时，Snort 常常会因复杂的模式匹配过程出现丢包（漏检），从而使部分带有攻击性的数据包流入网络，对网络安全构成威胁。为了减少 Snort 的丢包率，必须减少 Snort 对每个数据包的处理时间。目前国内对这方面的研究主要集中在改进或提出新的模式匹配算法[1,2]和优化规则链表[3,4]。文献[1]提出一种基于BM思想的多模式匹配算法—SSPBM算法来提高匹配速度。文献[3]提出在保持 Snort 原有规则匹配方法的基础上，增加宽度优先搜索算法，从而减少规则匹配所需时间。这些研究主要针对提高 Snort 检测引擎的效率。但是从网络流量的文件类型方面入手的研究还基本没有。

本文曾对某校园网的网络流量做过多次测试，测试结果显示：网络中的多媒体数据占到网络总数据量的 70%以上。如果能够在 Snort 中将这些多媒体数据识别，并进行针对性的检测和筛选，将大大提高 Snort 的检测效率。

基于此，曾设计在 Snort 中对网络流量中多媒体数据的识别、处理方法，本文将在此基础上提出动态自适应多媒体数据处理方法，该方法使 Snort 能够根据网络流量和系统剩余处理能力的变化，自动调整对多媒体数据的处理方式，从而有效降低丢包率。

① 基金项目:陕西省教育厅专项科学研究项目(2010JK568);西安工程大学基础研究基金(XGJ08006).
收稿时间:2010-08-06;收到修改稿时间:2010-09-15

2　HTTP协议下多媒体数据识别方法的设计

对于服务器端发出的多媒体数据，识别方法较为简单，即对一个会话中第一个带有负载的数据包进行检查，如果发现其负载前部固定位置出现具体的媒体类型信息，就可以确定这个数据包带有多媒体数据，并且可以确定在同一会话中与之顺序号相连并带有负载的其它数据包也都带有多媒体数据。对客户端发出的多媒体数据的识别方法与之类似，只是需要通过模式匹配方法对一个会话中所有带负载的数据包搜索媒体类型信息。

3　对多媒体数据包处理方法的设计

本文对多媒体数据包的处理设计了两种方法：放行和相应媒体类型检测。放行方法的设计比较简单，当发现某数据包带有多媒体数据后就对该数据包做标记，当搜索引擎看到这个标记时就可对其越过常规的规则匹配过程。使用放行方法可使系统整体检测效率大大提高，但是因为个别多媒体信息也可能携带危险信息（例如黑客在图片中加入木马），所以只能在安全性要求不高的环境下使用。而相应媒体类型检测处理方法可以弥补这个缺点。

3.1 相应媒体类型检测方法的设计

Snort 的常规检测过程是将捕获的数据包与规则库中相应规则头下数千条规则进行模式匹配，这个过程耗费时间很长，所以往往是 Snort 产生丢包率的瓶颈，而在 Snort 的规则库中有些规则是针对具体的媒体类型而制定的。根据这一特点，本文在所有与多媒体数据相关的规则中，从匹配项 content 和 pcre 中抽取特征字符串，存放在专门的多媒体数据规则库中。当判定某数据包携带有多媒体数据时，就可以使用模式匹配算法在数据包负载中搜索相应媒体类型的特征字符串，如果没有发生匹配，证明其较安全，就可对其放行，如果有匹配，则意味着这个数据包中可能含有危险信息，就将其按照普通数据包对待，进行常规检查。

相应媒体类型检测方法的优点是：对占网络流量比例很大的多媒体数据包，只进行针对性的检测，从而大幅度减少了模式匹配的处理时间，有效提高 Snort 的丢包阈值。

4　动态自适应多媒体数据处理方法的设计

“Snort 的常规检测方法（即对所有数据包全部检测）”和本文设计的对多媒体数据“放行”和“相应媒体类型检测”这三种处理方法的应用环境不同。常规检测方法检测详细，耗费时间长，可用于流量较低没有丢包的情况下；放行和相应媒体类型检测方法检测时间短，可用于流量较高且丢包率也随之较高的情况下。因为通常服务器端数据相对可信，所以本文中相应媒体类型检测和放行两种方法主要针对服务器端多媒体数据。

经过多次实验测试发现，以上三种处理方法的丢包阈值都不相同，而且随着网络运行状况的不同随时产生变化，但是都满足这种情况，即 Snort 常规检测方法丢包阈值(W1)<相应媒体类型检测方法丢包阈值(W2)<放行方法丢包阈值(W3)，如图 1 所示。

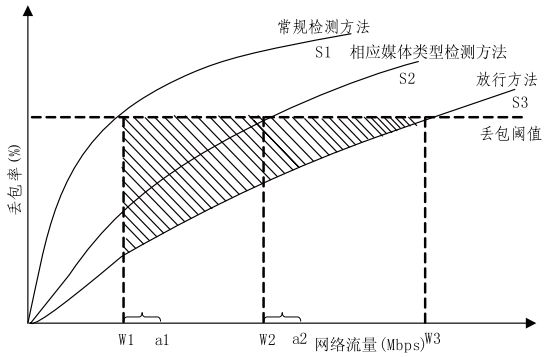

图 1　三种不同处理方法的丢包阈值

从图 1 可以看出，为了对尽可能多的数据包作详细检测，在基本不丢包的前提下，只要网络流量持续稳定在 W1 以下，就可以使用常规检测方法；如果网络流量在 W1~W2 之间，就可以采用相应媒体类型检测方法；如果网络流量超过 W2，就可以采用放行方法。

另外，当网络流量在 W1~W2 之间且靠近 W1 时，例如保持在 W1 至 a1 范围内，那么此时系统处理能力可能还留有一定的余地，如图 1 中 S1 与 S2 之间的阴影部分，这时可以在不丢包的前提下对一部分多媒体数据进行常规检测方法，将漏检率降到最低。

同样，当网络流量在 W2~W3 之间且靠近 W2 时，例如保持在 W2 至 a2 范围内，也可以在不丢包的前提下对一部分多媒体数据按照相应媒体类型检测，进一步利用其处理能力。

这一部分多媒体数据的数量是多少？因为在系统不同的运行状态下结果都不同，所以本文采用试探的

办法，在小范围内逐步增加处理多媒体数据包的数量，直到出现丢包为止。

综合以上描述，本文提出动态自适应多媒体数据处理方法，其基本思想如下：

(1) Snort 启动后先按照常规检测方法工作，同时统计一段时间内稳定的网络流量，根据网络流量大小的所处区间，在常规检测方法、相应媒体类型检测、放行三种方法中选择适当的方法处理。如果网络流量数值从一个区间跨越到另一个区间，应重新选择处理方法；

(2) 如果当前处理方法为相应媒体类型检测，网络流量长时间趋向 W1，则应在不出现丢包的前提下，用递增方法使用常规检测方法处理更多的多媒体数据包，如果发生丢包，立即用递减方法减少处理多媒体数据包；

(3) 如果当前处理方法为放行，网络流量长时间趋向 W2，则应在不出现丢包的前提下，用递增方法使用相应媒体类型检测方法处理更多的多媒体数据包，如果发生丢包，立即用递减方法减少处理多媒体数据包。

递增方法由使用二分法[5]的 f1(x)函数完成。f1(x)是多处理的多媒体数据包个数 x 与系统剩余处理能力 y 在[W1,W2]区间的单调递减函数，当 x 增大到一定程度，y 的值为 0，即到达丢包阈值。令 a=W1，b=W2，首先 x0 取区间中点 $\frac{1}{2}(a+b)$，则 y0= $f(\frac{(a+b)}{2})$，根据 y 的值，分两种情况[5]：

(1) 如果 y0>0，表示还没有到丢包阈值，取 a1= $\frac{(a+b)}{2}$，b1=b；

(2) 如果 y0<0，表示已经超过到丢包阈值，出现丢包，取 a1=a，b1= $\frac{(a+b)}{2}$，[a,b] ⊂ [a1，b1]，且 b1－a1= $\frac{(b-a)}{2}$；

那么 x1 即 $\frac{(a_1+b_1)}{2}$，y1= $f(\frac{(a_1+b_1)}{2})$，对于后续的 xi 和 yi 分别按照上述方法求得。

当满足以下两种情况时，计算停止：

(1) 当 yi<0，丢包个数<η（η 预先设定，例如 10 个）；

(2) y1=0 或满足上述条件。

递减方法是：如果 yi>0，丢包个数>η，则 xi 回退到 xi-1,xi-2,…,x0，直到丢包个数<η 为止。

5 实验结果

实验环境由 15 台计算机（操作系统：WIN XP、CPU：2.6GHz、内存：2GB）构成，通过 13 台计算机发送由之前捕获的网络真实流量而产生的背景流，2 台计算机向安装 Snort 的测试机发送使用 DARPA 1999 IDS 测试数据集而产生的攻击数据流，通过两种混合流量分别测试使用 Snort 常规检测方法、放行方法、相应媒体类型检测方法和动态自适应多媒体数据处理方法后的 Snort 丢包率情况，测试结果如图 2 所示。

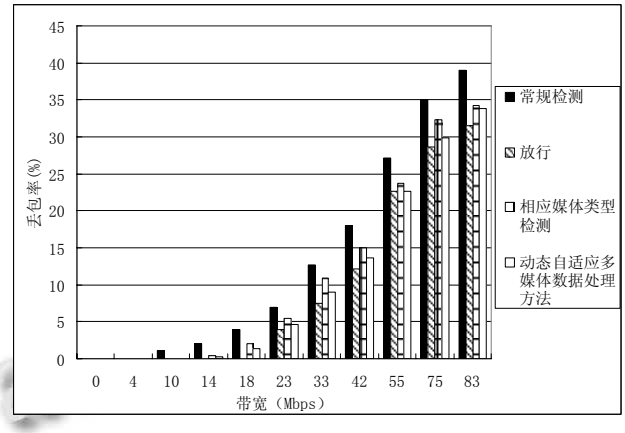

图 2 使用不同处理方法对 Snort 丢包率影响

测试结果显示，在相同带宽条件下，使用放行方法后丢包率降低 15.7~28.3%，使用相应媒体类型检测方法后丢包率降低 11.9~22.5%，使用动态自适应多媒体数据处理方法后丢包率降低 13.3~25.1。虽然使用放行方法测得的丢包率最低,但是最终报警数却分别高于后两种方法 5.1%和 4.7%。通过以上数据可以看出,使用本文设计的以上三种方法后，Snort 的丢包率得到显著降低。虽然从丢包率降低幅度上看,动态自适应多媒体数据处理方法要次于放行方法，但是完备性却是最好。

（下转第 181 页）

人在复杂环境下因躲避某一障碍物的同时又遇到另一障碍物，致使机器人越走越远，最后掉队的现象，致使跟踪失败。

4 结论

本文针对机器人在未知复杂环境下队形控制的适应性进行研究，文中结合了 leader-follower 法和基于行为法。重点讨论了机器人在复杂环境下的避障行为，提出了采用跟踪链的策略穿越障碍，并融合了 leader 和 follower 处理事件的独立性和协调性，较好的避免了在队形控制中机器人走失或组队失败的现象，使机器人在复杂环境下的灵活处理能力增强，并在机器人避障活动障碍时采用了有预见的避开运动物体的思维方式。仿真结果表明了该方法的有效性。

参考文献

1 张磊,秦元庆,孙德宝.基于行为的多机器人任意队形的控制.控制工程,2005,3:174–176.
2 李波,王祥凤.基于动态 Leader 多机器人队形控制.长春工业大学学报,2009,4:210–214.
3 苏治宝,陆际联.多移动机器人队形控制的研究方法.机器人,2003,1:88–90.
4 Cheng L, Wang YJ. Communication-based multiple mobile robots rigid formation control. International Conference on Control, Automation, Robotics and Vision. Kunming, China, 2004,12:729–734.
5 谭民,王硕,曹志强.多机器人系统.北京:清华大学出版社,2005.114–116.
6 任德华,卢桂章.对队形控制的思考.控制与决策,2005,6:601–606.
7 王月海,洪炳熔.基于行为的机器人部队队形控制方案.机器人技术与应用,2001,4:28–32.
8 韩逢庆,李红梅,李刚.一种改进的多机器人任意队形控制算法.机器人,2003,11:521–525.
9 Huang TY, Chen XB. A geometric method of swarm robot formation controls. Proc. of the 7th Word Congress on Intelligent Control and Automation. Chongqing, china, 2008. 3202–3206.

（上接第 213 页）

6 结束语

针对 Snort 在高网络流量下丢包率高的问题进行分析，从占网络流量比重较大的多媒体数据入手研究，设计了对多媒体数据的识别方法和两种单独处理方法，并提出动态自适应多媒体数据处理方法，该方法能够根据网络流量和 Snort 处理能力的动态变化，对多媒体数据选择最佳的处理方法。实验证明，使用该方法可有效降低 Snort 丢包率。

参考文献

1 曾慧惠,袁世忠,胡鹏.入侵检测系统中高效模式匹配算法的研究.计算机应用与软件,2008,5(4):256–257.
2 高朝勤,陈元琰,黎芸.入侵检测中一种节约内存的多模式匹配算法.计算机工程与应用,2009,45(11):107–110.
3 严书亭.Snort 规则链表结构的分析与改进.燕山大学学报,2006,30(3):272–275.
4 胡大辉,刘乃琦.高效的 Snort 规则匹配机制.微计算机信息,2006,(6):10–12.
5 袁慰平,等.计算方法与实习.上海:东南大学出版社,1991.