

文章编号:1001-9081(2006)10-2341-03

## 一种基于 FPGA 的 IPv6 网络入侵检测系统

王艳秋<sup>1</sup>, 兰巨龙<sup>1</sup>, 何 斌<sup>2</sup>

(1. 信息工程大学 信息技术研究所, 河南 郑州 450002;

2. 信息工程大学 理学院, 河南 郑州 450001)

(brekeley@126.com)

**摘 要:** IPv6 技术将是下一代互联网的核心技术, 对 IPv6 网络入侵检测系统的研究与下一代网络的安全问题息息相关。在分析了现有网络安全系统的基本原理和 IPv6 网络主要特点之后, 提出了一种 IPv6 网络入侵检测系统的框架, 并着重分析了采用现场可编程门阵列 (FPGA) 来实现模式匹配的方法。

**关键词:** IPv6; 现场可编程门阵列; 入侵检测; 模式匹配

**中图分类号:** TP393.08 **文献标识码:** A

## FPGA-based intrusion detection system in IPv6

WANG Yan-qiu<sup>1</sup>, LAN Ju-long<sup>1</sup>, HE Bin<sup>2</sup>

(1. Institute of Information Technology, University of Information Engineering,  
Zhengzhou Henan 450002, China;

2. College of Science, University of Information Engineering, Zhengzhou Henan 450001, China)

**Abstract:** IPv6 will be the core technology in the next generation Internet. Therefore, the study on intrusion detection system in IPv6 is closely linked with the security of the next generation Internet. After analyzing the fundamentals of network security system today and the primary characteristics of IPv6, a framework of intrusion detection system in IPv6 was put forward. And then, pattern matching by using Field Programmable Gate Array (FPGA) was focused in the study analysis.

**Key words:** IPv6; Field Programmable Gate Array (FPGA); intrusion detection; pattern match

随着 Internet 的蓬勃发展, 各种入侵事件与入侵手法层出不穷, 引发了一系列安全问题。目前防范网络入侵最常用的方法是防火墙, 但由于传统防火墙暴露出来的不足和弱点, 引发了人们对入侵检测系统的研究和开发。入侵检测系统 (Intrusion Detection System, IDS) 可以弥补防火墙的不足, 为网络安全提供实时的入侵检测并采取相应的防护手段。随着下一代网络中 IPv6 安全机制的引进, 网络层的安全性得到增强, 同时, IPv6 安全机制的应用对现有的网络安全体系也提出了新的要求和挑战。

### 1 入侵检测系统概述

入侵检测系统通过收集和分析计算机网络或计算机系统中若干关键点的信息, 检查网络或系统中是否存在违反安全策略的行为和被入侵的迹象。根据不同的分类标准, 入侵检测系统可以分为不同的种类。

按照检测数据的来源, 入侵检测系统分为基于主机的入侵检测系统 (Host-Based Intrusion Detection System) 和基于网络的入侵检测系统 (Network-Based Intrusion Detection System)。按照所采用的检测机制, 入侵检测系统可分为基于异常的入侵检测系统 (Anomaly-based Intrusion Detection System) 和基于误用的入侵检测系统 (Misuse-based Intrusion Detection System)。

目前的入侵检测系统大都是独立研究与开发的, 不同系

统之间缺乏互操作性和互用性。通用入侵检测框架 (Common Intrusion Detection Framework, CIDF) 是由 Teresa Lunt 发起的, 专门针对入侵检测进行标准化的组织, 开发一些协议和应用程序接口, 以便入侵检测研究项目能够共享信息和资源, 同样入侵检测系统组件也可以被其他系统应用。

CIDF 将 IDS 系统的构成划分为 5 类构件: 事件构件、分析构件、数据库构件、响应构件和目录服务构件, 如图 1 所示。这里是功能划分, 而不是模块划分, 在实际实现中事件构件可以是多个构件, 而分析构件可能包括事件分析构件和指令分析构件。从图中可看出, 各构件之间采用松散的耦合方式, 实现 IDS 功能的 4 个构件通过目录服务构件进行定位、认证、通信和调用。

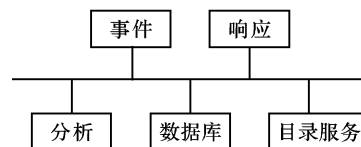


图 1 公共入侵检测框架 CIDF

#### 1.1 IPv6 网络的安全性问题

作为 IPv6 的一个组成部分, IPsec 协议定义了认证报头 (Authentication Header, AH) 和封装安全载荷报头 (Encapsulating Security Payload, ESP), 实现了基于网络层的身份认证, 确保了数据包的完整性和机密性, 在一定程度上实现了网络层安全。

收稿日期: 2006-04-27; 修订日期: 2006-06-20 基金项目: 国家信息技术领域重大专项项目 (2005AA121210)

作者简介: 王艳秋 (1982-), 女, 河南泌阳人, 硕士研究生, 主要研究方向: 网络信息安全; 兰巨龙 (1962-), 男, 河北张家口人, 教授, 博士生导师, 主要研究方向: 高速宽带信息网络技术; 何斌 (1978-), 男, 甘肃张掖人, 硕士研究生, 主要研究方向: 无线网络安全理论与技术研究。

由于 IPsec 是网络层协议,它只负责其下层的网络安全,因此在 IP 层以上以及网络应用软件中存在的漏洞和缺陷仍然存在。IPv6 只是在 IP 层对原有的网络协议进行了改造和扩展,而没有对其他协议层进行构造。在 IPv6 实现商业化普及之后,其他协议层存在的攻击行为很容易移植到 IPv6 上来。例如,在 TCP 层的 Xmas、Synflood 等攻击行为,还有 HTTP 服务器存在的漏洞等,这些在 IP 层是很难得到安全保护的。所以需要基于 IPv6 网络的入侵监测系统协助实现网络安全。

而 IPv6 的安全机制也对现有的网络安全体系提出了新的要求和挑战,具体说明如下:

1) IPsec 协议提供了加密和认证两种安全机制。加密是通过将数据进行编码来保证数据的机密性,以防数据在传输过程中被他人截获而失密;认证使得 IP 通信的数据接收方能够确认数据发送方的真实身份以及数据在传输过程中是否遭到改动。由于 IPsec 的加密功能提供的是端到端的保护,并且可以任选加密算法,密钥是不公开的,所以入侵检测系统根本就不能解密,更无从知道 TCP/UDP 端口号。这样的话,入侵检测系统对被加密的 IPv6 数据就无从下手。

2) 在 IPv4 中,IP 报头和 TCP/UDP 报头是紧接在一起的,而且其长度基本是固定的,所以入侵检测系统都很容易找到报头,并使用相应的规则进行过滤。然而在 IPv6 中 TCP/UDP 报头的位置有了变化,IP 报头与 TCP/UDP 报头之间常常还存在其他的扩展报头,如路由选项报头、AH/ESP 报头等。要对数据包进行过滤就必须逐个找到下一个报头,直到 TCP/UDP 报头为止,这对入侵检测系统的处理能力和处理速度会有很大的影响。

根据以上讨论,目前 IPv4 环境下的入侵监测系统不能有效地检测 IPv6 数据包,这就需要提出一种高效的基于 IPv6 网络的入侵检测系统模型,本文采用 FPGA (Field Programmable Gate Array) 来实现。

## 2 IPv6 网络入侵检测系统结构

尽管目前入侵检测系统广泛采用的都是技术已相当成熟的模式匹配技术,但是针对 IPv6 的特点,本节将提出一种将协议分析技术与模式匹配技术进行融合的 IPv6 网络入侵检测系统框架。

由于协议分析技术是把数据包视为具有严格定义格式的数据流,可以根据各层网络协议的定义,对各层协议的解析结果进行逐层分析。与传统的模式匹配技术相比,在准确性和整体性等方面都有一定优势。所以在处理 IPv6 报头时采用协议分析技术,在处理数据部分时采用成熟的模式匹配技术,能够充分发挥二者的优点,提高检测效率。

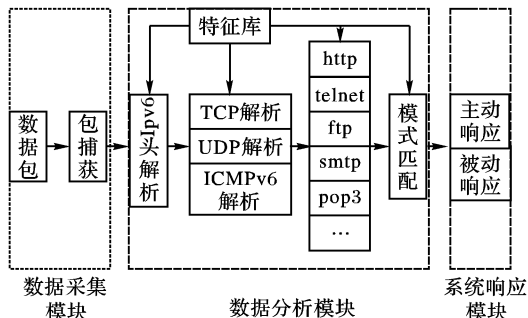


图2 IPv6 网络入侵检测系统结构

IPv6 网络入侵检测系统的基本思想是:捕获目标地址属于受保护网络的数据包,送往协议分析模块,通过具体协议字

段判断各层协议,送往相应协议解析器,解析数据包的数据部分,再根据特征库中的模式进行模式匹配,判断该数据包是否有人入侵企图,最后由响应模块对该数据包做出相应的响应。IPv6 网络入侵检测系统的结构如图 2 所示。

### 2.1 数据采集模块

数据采集模块属于底层处理,把地址属于受保护网络的数据包提取出来,送往协议分析模块解析处理,为整个系统提供数据来源。该模块是网络入侵检测系统的基本组成部分,是实现整个入侵检测系统的基础。随着网络的规模越来越大,流入网络的数据包流量也越来越大,必须保证该模块工作高效、稳定、可靠。

基于 IPv6 的网络入侵检测系统可采用专门为数据监听应用程序设计的库文件 WinPcap (windows packet capture) 来实现数据包的捕获。WinPcap 是 Windows 平台下一个免费、公共的网络访问系统,它的主要功能在于独立于主机协议(如 TCP/IP)而发送和接收原始数据报。也就是说,WinPcap 不能阻塞、过滤或控制其他应用程序数据报的收发,它只是监听共享网络上传送的数据报。

### 2.2 数据分析模块

数据分析模块是 IPv6 入侵检测系统的主要部分,包括协议分析部分和模式匹配部分。协议分析部分对数据包进行逐层剥离,分析各个协议的包头和一部分数据;模式匹配部分对协议分析部分获得的数据进行分析,与特征库中预先定义的模式进行比较,来判断该数据包是否有人入侵企图。

协议分析将输入数据包视为具有严格定义格式的数据流,并将输入数据包按照各层协议报文封装的反向顺序,层层解析出来。然后,再根据各层网络协议的定义,对各层协议的解析结果进行逐层分析。

协议解码带来了效率上的提高,因为系统在每一层上都沿着协议栈向上解析,故可以使用所有当前已知的协议信息,来排除所有不属于这一个协议结构的入侵。例如,传输层上的协议是 TCP,就没必要再检测传输层上如 UDP 等其他协议的入侵了。

以处理 TCP 的 HTTP 报文为例,协议分析模块的处理流程图如图 3 所示。

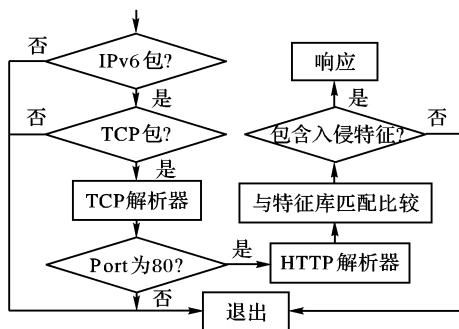


图3 协议分析模块流程

模式匹配就是将收集到的信息与已知的网络入侵和系统已有模式数据库进行比较,从而发现违背安全策略的行为。该过程可以通过字符串匹配寻找一个简单的条目或指令,也可以利用正规的数学表达式来表示安全状态的变化。

该方法只需收集相关的数据集合,显著减少系统负担,且技术已相当成熟。根据具体特征库进行判断,无需学习过程,当发现新的攻击手段后,IDS 只要在特征库中添加新的规则即可。但是,该方法需要不断的升级以对付不断出现的入侵

手法,不能检测到从未出现过的入侵手段。

### 2.3 系统响应模块

当入侵检测系统发现系统有入侵事件发生时,就要让系统管理员等相关安全人员了解已经有安全问题发生,并需要采取相应的响应措施。系统响应模块对经过检测的数据包执行具体的响应,是一个入侵检测系统必不可少的部分。从响应的方式上分,入侵检测系统的响应可以分为主动响应和被动响应。

在主动响应中,系统自动地或以用户设置的方式阻断入侵过程或以其他方式影响入侵过程,主要有断开 TCP 连接和发送 ICMP 报文。被动响应是指为用户提供信息,由用户决定接下来应该采取什么措施。包括:Alert,使用选定的报警方式生成警报信号,然后记录该数据包;Log,记录该数据包;Pass,丢弃该数据包。在这里,可以采用主动响应和被动响应相结合的方式对入侵行为做出响应。

## 3 基于 FPGA 实现的数据分析模块

### 3.1 使用 FPGA 实现本系统的原因

网络入侵监测系统的规则既指向包头也指向包负载,包头的检查采用协议分析的思想就比较简单,可是当规则库中的模式很多时,包负载的检查要在线速完成,进行模式匹配的计算量就很大。

FPGA 适合完成在线速下的文本匹配,并且基于 FPGA 的可重配置硬件具有开发成本低、设计周期短、编程灵活、易于调整,能够根据需要重新配置硬件功能等特点。而且 FPGA 具有比软件技术更快的处理速度和比硬件技术 ASIC (Application Specific Integrated Circuit) 的成本更低,能够使 IDS 在数据处理能力与网络接口速度保持一致的同时,迅速适应网络攻击手段和模式不断发展变化的需要。

所以本文采用了 FPGA 可编程器件来实现,并用扩展的高增益的流水线结构处理输出、匹配和编码的瓶颈。为了增加系统的吞吐量,这里使用了多重比较器,并允许多重搜索模式的并行匹配。

### 3.2 基于 FPGA 的数据分析模块的结构

图 4 即为基于 FPGA 的数据分析模块的结构。报头与数据部分的处理串行,报头的比较根据协议分析的思想进行,协议位是固定的,实现相对比较简单;数据部分的比较采用模式匹配技术,用 FPGA 实现,相对复杂,下面主要描述这一部分。

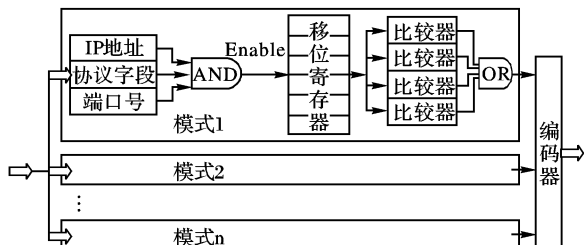


图 4 基于 FPGA 的数据分析模块结构

如果模式匹配时每个周期只能处理一个输入,那么系统的总吞吐量就被工作频率所限制。为了减少这一瓶颈,我们使用数据包并行技术,但有一点,它并不能提供稳定的处理带宽。我们使用独立的比较器来实现类似 CAM 的功能,就能在较宽的数据通道上使用多重的比较来搜索匹配的模式。

在每个子模块都使用了高增益的流水线:包数据输出到比较器,比较器本身,还有匹配规则的编码。为达到较高的处

理吞吐量,每搜索一个规则使用  $N$  个并行的比较器,这样可以同时处理  $N$  个包字节。

### 3.3 基于 FPGA 的模式匹配模块的实现

比较器是流水线结构的,而且每一个流水线级的最小逻辑数适合一个 4 输入的查找表 (Look Up Table, LUT) 和与之对应的寄存器,用于组合逻辑的每个逻辑单元也包括一个触发器。这种深度流水线的唯一缺点就是在时钟周期里输出的总延迟相对较长,但这对我们的系统体系结构而言不是关键的限制。

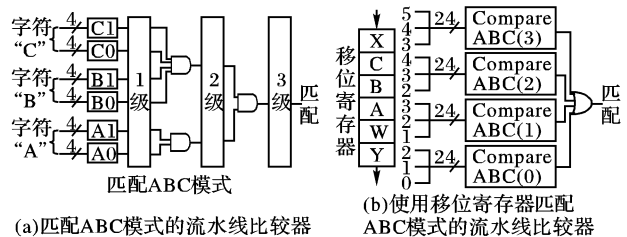


图 5 匹配“ABC”模式的流水线

图 5(a) 是一个匹配“ABC”模式的流水线比较器。在每一级中,比较器匹配输入数据包的 6 个 4 比特,用 6 个 4 输入的查找表来实现。后面的两级中,部分匹配的结果进行与操作产生最后的匹配信号。在每一级,组合逻辑由最多 4 输入 1 输出的逻辑功能描述。

图 5(b) 是 4 个比较器相连匹配同样的模式,分别移位 0, 1, 2, 3 个字符 (由比较器标志位的数字后缀显示)。比较器 compare\_ABC(0) 检查 0 到 2 字节,compare\_ABC(1) 检查 1 到 3 字节,以此类推。这里选择 4 个比较器仅仅是个例子,一般可以使用  $N$  个比较器,每个周期允许处理  $N$  个字节。单个匹配完成后,被匹配的规则要被编码然后报告给系统的其他部分。

这里的编码器不是一个优先级编码器,即假设最多只有一个匹配发生。虽然在一个周期中多重匹配能够发生,但实际上可以通过检查模式字符串来确定这种情况是否会发生。如果所有的模式有不同的后缀,那么在一个周期中就不会有多重匹配。然而,这样的保证变得越来越困难,因为我们增加了并发比较器的数量,也就是增加了并行匹配的模式数量。

输出延迟是必须要考虑的主要变慢因素。它虽然不包含逻辑,但信号必须经过很长的距离,这样就会有显著的延迟。为减小这种瓶颈我们用寄存器树让输入数据流入比较器。树的叶子是移位寄存器,数据由此流入比较器,中间节点同时作为缓存和流水线寄存器。

### 3.4 基于 FPGA 的网络入侵检测系统的应用

随着当前网络带宽的逐步提高,各种待分析网络数据的产生速度已经远远超过入侵检测软件的处理能力,丢包现象时有发生,使基于软件的网络入侵检测系统无法正常检测入侵行为。我们将产生系统处理速度瓶颈的网络数据包模式匹配部分用 FPGA 加以实现,使网络数据包的处理并行化,加快了数据包的处理速度,提高了整个系统的吞吐量。同时,对于入侵者行为和模式的频繁更新和改变,FPGA 允许我们对检测算法和模式匹配的具体应用做出相应的调整,甚至将一些高层协议栈用可重配置硬件加以实现,进一步提高网络入侵检测系统的处理速度和精度。

## 4 结语

虽然 IPv6 提供了较好的安全体系结构,但这些只是在 IP (下转第 2346 页)

表1 攻击实验结果

| 内存系统    | 攻击次数   | 成功次数   |
|---------|--------|--------|
| C 运行时间库 | 10 000 | 10 000 |
| 地址混淆    | 10 000 | 7 150  |
| 随机匹配    | 10 000 | 25     |

### 3.2 实验结果分析

AO 算法在分配长度为 28 字节的内存块时,理论上随机增加的长度值在 0~6 之间分布。当该值为 0~4 时,相当于没有随机化,其概率:

$$P_{theory} = 5/7 = 71.43\%$$

实际概率:

$$P_{practise} = 7150/10000 = 71.50\%$$

理论值与实际值很吻合。

对随机匹配算法,由于随机化时没有 1/4 内存块大小的限制,且两个块之间的距离由两次生成的随机数决定,理论上可以取到整个 chunk 中任意两个大小满足要求且没有重叠的块。从长度为  $N$  字节的内存区间中取两个长度为  $L$  字节的内存块,设两个内存块所有可能的位置组合数目为  $D$ ,相对距离有  $R$  种可能。当  $N > 3L$  时有:

可能的位置组合数目:

$$D = \sum_{0 \leq i \leq L-1} (N-i-2L+1) + \sum_{L \leq i \leq N-2L} ((i-L+1) + (N-i-2L+1)) + \sum_{N-2L+1 \leq i \leq N-L} (i-L+1) \\ = (N-2L+2)(N-2L+1)$$

相对距离数:

$$R = 2(N-2L+1)$$

攻击者猜中两块相对距离则攻击成功。一次攻击猜中相对距离的平均概率:

$$P_{(avg)} = 1/R = 1/((N-2L+1) \times 2)$$

最大概率(两块紧邻):

$$P_{max} = (N-2L+1)/D = 1/(N-2L+2)$$

最小概率(两块分别在 chunk 首尾):

$$P_{min} = 1/D = 1/((N-2L+1)(N-2L+2))$$

考虑到内存分配的边界对齐因素,设分配的内存块按  $A$  字节对齐,以上公式中的  $N, L$  分别应该用  $N/A, L/A$  替换。

在测试用例中  $N = 2512, L = 16, A = 8$ , 解得  $P_{avg} = 0.16\%, P_{max} = 0.31\%$ , 与实际数据 0.25% 较吻合。

由以上分析和测试结果可见随机匹配算法可以有效防范

堆溢出攻击。

## 4 结语

本文提出的随机匹配算法在分配小内存块时不会退化为确定性算法,分配大内存块时也没有太多额外的空间开销,并且随机化非常彻底,能有效降低堆溢出攻击成功概率。

由于攻击手段的多样性,只依赖单一的防范措施是远远不够的,必须综合应用多种防范手段,才能达到更好的安全性。就内存块随机化来讲,目前只实现了堆上数据的随机化,将来的工作中还包括针对栈、静态数据和动态链接库地址的随机化进行研究。

### 参考文献:

- [1] SALKEVER A. The Ever-Growing Virus Crisis [J/OL]. [http://yahoo.businessweek.com/technology/content/aug2003/tc20030826\\_4386\\_tc047.htm](http://yahoo.businessweek.com/technology/content/aug2003/tc20030826_4386_tc047.htm), 2003.
- [2] GCC documents. Specifying How Stack Checking is Done [CP/OL]. <http://gcc.gnu.org/onlinedocs/gccint/Stack-Checking.html>, 2005.
- [3] MSDN. Visual C++ Compiler Options [CP/OL]. <http://msdn2.microsoft.com/en-us/library/9598wk25.aspx>, 2005.
- [4] CONOVER M. w00w00 on Heap Overflows [R/OL]. <http://www.w00w00.org/files/articles/heaptut.txt>, 1999.
- [5] CONOVER M, HOROVITZ O. Reliable Windows Heap Exploits [R/OL]. <http://www.cybertech.net/~sh0ksh0k/heap/CSW04%20-%20Reliable%20Windows%20Heap%20Exploits.ppt>, 2005.
- [6] HOARE T. 21 世纪的智能编译器 [R/OL]. [http://research.microsoft.com/asia/dload\\_files/21century/3\\_tony\\_hoare\\_E.pdf](http://research.microsoft.com/asia/dload_files/21century/3_tony_hoare_E.pdf), 2001.
- [7] Pax Documentation [CP/OL]. <http://pax.grsecurity.net/docs/pax.txt>, 2003.
- [8] DESIGNER S. Non-executable user stack [R/OL]. <http://www.openwall.com/>, 2000.
- [9] WOJTCZUK R. Defeating Solar Designer's Non-executable Stack Patch [R/OL]. [http://www.insecure.org/spl0its/non-executable\\_stack.problems.html](http://www.insecure.org/spl0its/non-executable_stack.problems.html), 1998.
- [10] BHATKAR S, DUARNEY D, SEKAR R. Address obfuscation: An efficient approach to combat a broad range of memory error exploits [A]. In Proceedings of the 12th USENIX Security Symposium [C]. 2003. 105-120.

(上接第 2343 页)

层实现的,而对于 IP 层以上的一些缺陷和应用程序的漏洞在 IPv6 中还不能提供全面的保护。通过分析 IPv6 协议的特点及其安全性能,设计了一种协议分析技术与模式匹配技术相结合的 IPv6 网络入侵检测系统,提出了一个基于可重配置硬件的网络入侵检测系统体系结构,将其中网络数据包的特征匹配用 FPGA 加以实现,使网络数据包的处理并行化。

由本文的分析可以看出, FPGA 等可重配置硬件将成为未来高速网络入侵检测系统以及网络安全系统开发和运行的理想硬件平台,值得我们在相关领域进行更深入的研究和探索。

### 参考文献:

- [1] LEE W. A Data Mining Framework for Building Intrusion Detection Model [J]. In IEEE Symposium on Security and Privacy, 1999, 7: 120-132.

- [2] SOURDIS I, PNEVMATIKATOS D. Fast, Large-Scale String Match for a 10Gbps FPGA-based Network Intrusion Detection System [A]. In 13th Conference on Field Programmable Logic and Applications [C]. Lisbon, Portugal, September Springer-Verlag, 2003.
- [3] 刘航, 戴冠中, 李晖晖, 等. 基于 FPGA 的高速网络入侵监测系统 [J]. 计算机应用, 2004, 24(5): 33-35.
- [4] 李建武. 基于 IPv6 的网络入侵检测系统研究和设计 [D]. 西安: 西北工业大学, 2005.
- [5] 王玲, 钱华林. IPv6 的安全机制及其对现有网络安全体系的影响 [DB/OL]. <http://www.77125.com/download/2003/11/27/160306.pdf>, 2003-11/2005-10.
- [6] ROESCH M. Snort: The open source network intrusion detection system [EB/OL]. <http://www.snort.org>, 2003-10.