第35卷 第14期 计 算 机 工 程 2009年7月
Vol.35 No.14 Computer Engineering July 2009
·安全技术· 文章编号：1000—3428(2009)14—0160—03 文献标识码：A 中图分类号：TP393.03

基于 IPv6 报头的隐蔽通道分析与防范

郭浩然[1]，王振兴[1]，余 冲[1]，王 倩[2]
(1. 国家数字交换系统工程技术研究中心，郑州 450002；2. 解放军信息工程大学测绘学院，郑州 450052)

摘 要：研究 IPv6 基本报头，从网络安全的角度出发，对其中可被用于隐蔽通道载体的字段及其隐蔽通道构建方法进行分析和探讨，在此基础上提出 2 类构建方法。探讨基于 Hop-Limit 字段的比特变换隐蔽通道构建方法，分别给出每种方法的通信容量等关键性能指标。对基于 IPv6 报头的隐蔽通道的防范措施进行讨论。

关键词：网络安全；隐蔽通道；IPv6 协议；报头

Analysis and Preservation of Covert Channel Based on IPv6 Header

GUO Hao-ran[1], WANG Zhen-xing[1], YU Chong[1], WANG Qian[2]
1. National Digital Switching System Engineering & Technological R&D Center, Zhengzhou 450002;
2. Institute of Surveying and Mapping, PLA Information Engineering University, Zhengzhou 450052)

【Abstract】 This paper researches IPv6 basic header, and from the angle of network security, analyzes and discusses the fields which can be used to explore covert channel, presents two kinds covert channel creating methods. It focuses on the Bit-Convert methods based on Hop-Limit and separately gives out the key performance indictors such as communication capacity to each method. The preserving measures of covert channel based on IPv6 header are discussed.

【Key words】 network security; covert channel; IPv6; header

1 概述

隐蔽通道(covert channel)又称隐蔽信道[1]，它能使通信双方绕过系统安全访问机制的检查，并以违反系统安全策略的方式传递秘密信息。它通常指系统的一个用户以违反系统安全策略的方式传送信息给另外一个用户的机制。在一个系统中，给定一个非自主安全策略模型 M 及其解释 $I(M)$，在 $I(M)$ 中的任何 2 个主体 $I(S_h)$ 和 $I(S_i)$ 之间的潜在通信是隐蔽的，当且仅当 M 的相应主体 S_h 和 S_i 之间的通信在 M 中是非法的[2]。在传统的隐蔽通道的定义中，都把隐蔽通道定义在操作系统的内部，即 2 个实体之间必须有共享资源，隐蔽通道才能够建立。隐蔽通道的概念已经扩展到计算机网络中，把整个计算机网络看作一个巨大的计算机系统，网络中的各种软硬件设备和信息实体都是该计算机系统的一部分资源，任何利用非正常的手段、以违反系统安全策略的方式在网络中传递信息的通道都可以称作网络隐蔽通道。

参照对隐蔽通道的划分，把网络隐蔽通道分为存储型隐蔽通道和时间型隐蔽通道。存储型隐蔽通道是指一个潜在的隐蔽通信发送端直接或间接地修改了资源属性，接收端可以直接或间接地读取到这个属性的变化。时间型隐蔽通信是指通过调整系统资源(如 CPU)的使用时间影响了发送端的实际响应时间，从而发送信息给接收端。本文只讨论存储型隐蔽通道。在传统的基于 IPv4 协议的网络环境中，文献[3]提出基于数据包操作和数据包排序的经典隐蔽通信方法，文献[4]提出利用 TCP 序列号和确认号字段以及 IP 标识字段进行隐蔽通信的策略，文献[5]提出利用 IP 报头保留字段和未使用字段进行数据隐藏的隐蔽通信策略。

IPv6 在安全性方面优于 IPv4，但其设计仍然有不严密的地方，例如协议存在保留字段、定义不完整的字段，以及节点处理和转发数据包时易被忽略的字段等，这些为网络隐蔽通道的构建创造了条件。

本文以 IPv6 基本报头为切入点，从网络攻击的角度出发，探讨 IPv6 协议作为隐蔽通道载体的可能性及相应方法。基于对 IPv6 基本报头的分析和研究，选出其中可用作隐蔽通道载体的字段。根据实施方法的不同，本文将隐蔽通道的构建方法归纳为基于数据包操作和比特变换 2 类，以 Hop-Limit 字段为例重点讨论了基于比特变换的隐蔽通道方法。

2 IPv6 报头字段分析

IPv6 报头结构如图 1 所示。

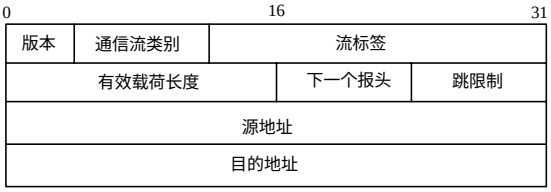

图 1 IPv6 报头结构

版本(Version)：该字段长度为 4 bit，字段值为 6。用于指明 IP 协议的版本号。版本字段的意义在 IPv4 和 IPv6 中的定义是相同的。

通信流类别(Traffic Class)：该字段长度为 8 bit，代替了 IPv4 中的服务类型(Type of Service)字段，它有助于处理实时数据以及任何需要特别处理的数据。发送节点和路由器可以使用该字段来识别和分辨 IPv6 数据报的类别和优先级。

作者简介：郭浩然(1987－)，男，硕士研究生，主研方向：网络与信息安全，IPv6 与下一代互联网；王振兴，教授、博士、博士生导师；余 冲，硕士研究生；王 倩，博士研究生

收稿日期：2008-12-15 **E-mail：**haoran006@yahoo.com.cn

RFC2460 未定义该字段的值，RFC2474 以区分服务字段的形式，为该字段提供一个可替换的定义。

流标签(Flow Label)：该字段区分需要相同处理的数据包，以此来促进实时性流量的处理。长度为 20 bit，其适用的详细细节还没有定义。

有效载荷长度字段(Payload Length)：该字段表示 IPv6 有效载荷长度。有效载荷的长度包括扩展报头和上层 PDU。16 bit 长度的该字段可表示最大长度为 65 535 Byte 的有效载荷。如果有效载荷长度超过 65 535 Byte，则会将该字段的值置 0，而有效载荷的长度用逐跳选项扩展报头中的超大有效载荷选项表示。本文只限于讨论 IPv6 基本报头，扩展报头不在本文讨论范围内。相关说明详见文献[6]。

下一个报头(Next Header)：在 IPv4 中，该字段为协议类型(Protocol Type)字段。IPv6 则被重新命名以反映出重新组织的 IP 数据包，该字段长度为 8 bit，表示第 1 个扩展报头(如果存在)和上层 PDU 中的协议。

跳限制(Hop-Limit)：该字段长度为 8 bit，源主机在生成 IPv6 数据包时，把该字段值设定为一个大于零的初始值，表示该数据包在被丢弃前可以通过的最大链路数。

源地址(Source Address)和目标地址(Destination Address)：分别用于指明源主机和目标节点的 IPv6 地址，长度为 128 bit。

3 基于 IPv6 报头的隐蔽通道

IPv6 报头字段定义各不相同，功能相互独立。本文以字段的详细定义和功能特性为研究基础，分析节点对各字段的处理过程以及字段值在传输过程中的变化特点，归纳出 2 类实施隐蔽通信的方法。

3.1 基于数据包操作的隐蔽通道

基于数据包操作(packet manipulation)的隐蔽通道通常利用协议的保留字段和未完全定义字段存在的可利用空间，对其中特定的比特位进行映射操作使其代表特定的含义，从而通过通信双方的共享密钥或事先约定的解码规则进行隐蔽通信。

由于协议的设计者对 IPv6 中的某些应用的具体标准尚未达成一致，应用程序在节点中对这些未明确定义的字段采用相对简单的默认处理，这就为基于此类字段的隐蔽通道实施提供了良好的条件。

IPv6 报头中的通信流类别字段用以表示数据包的类和优先级，该字段的值在 RFC2460 中没有定义，但它在 IPv6 中是需要实现的。支持部分或全部通信流类别数据位的某一特定用法的节点可以根据其用法修改它们所生成(接收、转发)的数据包中的这些比特的值。如果节点不支持这一用法，应忽略这些位，并保持其值不变。同时，通信流类别字段中还存在 2 bit 的保留位。

流标签字段也面临类似的问题，RFC2460 对流标签字段使用的详细细节也没有定义，对于不支持流标签字段功能的 IPv6 节点，应在初始化数据包的时候将此字段设为 0，传输包时保持不变，接收包时忽略。

对通信流类别和流标签字段通过数据包操作的方法，采取合适的隐写编码方式，使尽可能少的比特位隐藏尽可能多的信息，同时通信双方共享隐写信息的编解码规则，就可以实施隐蔽通道。

IPv6 报头中的下一个报头字段的值表示了其基本报头之后第一个扩展报头(如果存在有扩展报头)的类型或者上层 PDU(协议数据单元)中的协议，参考 http://www.iana.org/assignments/protocol-numbers 所列出的 IPv6 协议的下一个报头字段的保留值的最新列表(2008-05-01)，138~252 未被分配，255 用于保留，共计 116 个无用值，同时对照 ASCII 码表示的 95 个可显示字符，采取合适的隐写算法来映射这 95 个字符，即可构建隐蔽通道进而实施隐蔽通信。

综上，IPv6 报头中有可能通过数据包操作的方法被用作隐蔽通道载体的字段有通信流类别字段、流标签字段和下一个报头字段。针对这些字段的基于数据包操作的隐蔽通道，方法较为简单成熟，本文不再赘述。

3.2 基于比特变换的隐蔽通道

基于比特变换的隐蔽通道是利用协议中存在的值在传输过程中可改变的字段，根据其字段值变化特点，采取特定的隐写方法对其字段中的某些比特位进行变换，使之代表通信双方约定的语义来进行隐蔽通信。

本文以 Hop-Limit 字段作为基于比特变换的隐蔽通道载体，因为 Hop-Limit 字段的值的改变被安全策略视为是正常状态。8 bit 的 Hop-Limit 字段表示数据包可穿越最多 255 个中间节点，由于网络状况和路由信息的改变是高概率事件，该字段的值的改变不会被视为异常。而且对该字段的值的操作是允许的、合法的，发送节点可自行设定或改变 Hop-Limit 字段的值。

3.2.1 基于 Hop-Limit 字段的比特变换隐蔽通道

约定隐蔽通信的发送方为 Alice，接收方为 Bob，Warden 代表网络安全策略。Alice 和 Bob 事先知道比特变换的规则，也就是隐蔽信息的编解码约定。在隐蔽通信开始的时刻，Alice 将 Hop-Limit 字段的最低比特位设为 1 发送给 Bob，1 代表一种信息；Alice 将最低比特位设为 0 发送给 Bob，0 代表另外一种信息。基于 Hop-Limit 比特位变换的编码方法如表 1 所示。

表 1 基于 Hop-Limit 比特位变换的编码方法

数据报序号	Hop-Limit 字段	传送的隐蔽信息
1	XXXXXXX1	隐蔽传送“1”
2	XXXXXXX0	隐蔽传送“0”

该方法的优点是 Hop-Limit 字段的值的轻微变化对于 Warden 来说显得非常自然，Alice 和 Bob 的隐蔽通信行为和内容难以被检测出。在不考虑网络阻塞和误码率的理想情况下，这种隐蔽通信方法的容量是 1 bit/packet，假设在一个数据包速率为 100 packet/s 的网络环境中，单通信流的带宽即可达到 100 bit/s。在实际通信中可以通过多通信流并行发送的方法来提高通信容量。

3.2.2 针对可靠性改进的 Hop-Limit 比特变换隐蔽通道

上节所提出的方法的优点是隐蔽通信难以被检测，但除非 Alice 和 Bob 明确知道双方通信链路中的路由器的跳数，否则该通信行为要限定在同一个本地链路内，只在静态路由情况下可用。因为 Hop-Limit 字段值在经过若干个路由器之后其变化会严重干扰其中隐藏的信息，使 Bob 接收到的信息无法使用约定的规则解码。

针对该问题，提出改进的比特变换隐蔽通信方法，其过程描述如下：

(1)Alice 设定 Hop-Limit 初始值 h，“$0<h<255$”，发送给 Bob，约定作为隐蔽通信开始的标志；

(2)Alice 取一个整数 δ，设定 Hop-Limit 的值为 $h+\delta$，$0<\delta<255-h$，代表“1”，发送给 Bob；

(3)Alice 设定 Hop-Limit 的值为 $h-\delta$，代表“0”，发送给 Bob；

(4)Alice 设定 Hop-Limit 的值为 $h+1$，发送给 Bob，约定作为隐蔽通信结束的标志。基于 Hop-Limit 字段值改变的编码方法如表 2 所示。

表 2　基于 Hop-Limit 字段值改变的编码方法

数据报序号	Hop-Limit 字段	传送的隐蔽信息
1	XXXXXXXX	隐蔽传送“开始”
2	YYYYYYYY	隐蔽传送“1”
3	ZZZZZZZZ	隐蔽传送“0”
4	UUUUUUUU	隐蔽传送“结束”

采用这种改进的方法，在不考虑时延的情况下，当 Alice 发送 n 个数据包，该隐蔽通信的通信容量是 $(n-2)/n$ bit/packet, $n>4$。在理想情况下，h 应该选取一个较大的整数，δ 取 Alice 和 Bob 之间的跳数；同时出于隐蔽性的考虑，$h\pm\delta$ 对 Hop-Limit 的值不能造成剧烈的改变。上述过程使得隐蔽通信容量有所下降，但是提高了隐蔽通信的鲁棒性。

3.2.3　针对通信容量改进的 Hop-Limit 比特变换隐蔽通道

针对上一节的通信方法存在的带宽低的问题，提出另外一种改进的隐蔽通信方法，仍然是基于 Hop-Limit 字段的比特变换方法。

通过上面的分析，Alice 如何选取合适的 δ，是影响隐蔽通信的性能指标(可靠性、通信容量)的关键。在理想情况下，δ 取通信双方之间的路由器跳数。但是在一般情况下，通信双方并不知道精确的跳数，就要在可容忍的误差范围内，取适当的置信水平，应用概率统计的方法，对跳数进行估算。

在 Alice 和 Bob 之间，统计出这些到达的数据包的 Hop-Limit 值，并计算其与初始值的差别的分布(方差分布)，然后选取合适的置信水平，对跳数进行区间估计。

设 I 是 Alice 设定的 Hop-limit 的初始值，Alice 发送 n 个数据包给 Bob。随机变量 $X_1, X_2, \cdots, X_n$ 是 Bob 收到的数据包中的 Hop-Limit 值，x 是 X_n 的所有可能取值。μ 是 $I-x$ 的数学期望，即跳数的均值，$0<\mu<255$，δ^2 是 x 的方差。则对于任意的正数 ε，根据切比雪夫(Chebyshev)不等式，有：

$$P\{|(I-x)-\mu|<\varepsilon\}\geq 1-\frac{\delta^2}{\varepsilon^2} \tag{1}$$

式(1)给出了 Alice 到 Bob 之间在跳数的分布未知的情况下，实际跳数与平均跳数之间的差别的概率上限。可以近似地把这个概率值作为隐蔽通信的误码率，μ 作为 Alice 到 Bob 之间的平均跳数。

统计 Bob 收到的 n 个数据包中 Hop-Limit 的值看作 1 次样本容量为 n 的抽样。设随机变量 $X_1, X_2, \cdots, X_n$ 是总体 X 的样本，近似服从正态分布，即 $X\sim N(\mu,\sigma^2)$。$\bar{X}$，S^2 分别是样本均值和样本方差，则有：

$$\bar{X}\sim N(\mu,\sigma^2/n) \tag{2}$$

$$\frac{\bar{X}-\mu}{S/\sqrt{n}}\sim t(n-1) \tag{3}$$

根据正态总体均值与方差的区间估计计算公式，在 σ^2 未知的情况下，μ 的一个置信水平为 $1-\alpha$ 的置信区间为

$$\left(\bar{X}\pm\frac{S}{\sqrt{n}}t_{\alpha/2}(n-1)\right) \tag{4}$$

因此，在 3.2.2 节提到的方法中选取的 δ 应分布在式(4)的区间内。

重设式(1)中的参数 μ，指定 μ 为变量 x 的数学期望，$0<\mu<255$。r 为 Alice 到 Bob 的数据包发送速率。在式(1)的保证下，由式(3)和式(4)计算得该隐蔽通信的带宽为

$$r\times\lg n\times\frac{\delta^2}{\varepsilon^2}$$

误码率为

$$1-\frac{\delta^2}{\varepsilon^2}$$

隐蔽通信的通信容量为($\lg n$) bit/packet，n 的区间为 $(\mu,\frac{I-\mu}{\varepsilon})$。由 n 的取值范围可知，该隐蔽通信的通信容量与通信双方之间的平均跳数近似于反比例关系。

4　基于 IPv6 报头隐蔽通道的防范措施

网络隐蔽通道并非主动进行攻击的程序或通信行为，在对其技术特点未知的情况下，常规的安全措施诸如杀毒软件、防火墙等很难对其进行防范。针对本文提出的 2 类隐蔽通道，以下方法可视为对其的有效防范措施：

(1)强制 IPv6 报头字段遵守设计规范。这是消除网络隐蔽通道的基本措施。每一个报头字段的值都能够严格按照协议设计规范去实现，在通信过程中就可以大大减少产生基于字段值变化的隐蔽通道的几率。

(2)重置报头字段值。节点在转发或接收时强制重置未完整定义字段和保留字段的设定值，可破坏基于此类字段的隐蔽通道通信双方共享秘密信息的语义或完整性。基于 Hop-Limit 字段的隐蔽通道也并非无法检测和防范，只是难度相对较大，节点或网络安全设备将某个通信流的所有数据包的 Hop-Limit 字段的值强制重置为该通信流的最小 Hop-Limit 值，虽然不能保证完全消除该类型隐蔽通道，但是重置 Hop-Limit 字段值所带来的噪声大大降低了其通信容量。

(3)使用通信代理。通信代理会通过映射或转换等方法对 IP 协议带来一定的变化，这些变化又影响到 IPv6 报头字段值的改变，会对隐蔽通道造成强烈的干扰和破坏。

防范隐蔽通道会给网络性能带来一定的影响，而且防范方法很大程度上依赖于对隐蔽通道构建方法的了解。随着网络安全理论的进步和技术的发展，针对网络隐蔽通道的检测和防范必将会出现新的方法和策略。

5　结束语

由于网络协议的多样性，因此存在多种基于网络协议的隐蔽通道的构建方法。IPv6 在设计中存在未完全定义字段和保留字段等问题，为提高性能，限制了中间节点对 IPv6 数据包的处理，并要求路由器对数据包做尽量少的改动。这些因素为在 IPv6 报头中隐藏秘密信息提供了条件。本文通过分析和研究指出 IPv6 报头中潜在的隐蔽通道构建方法，并提出相应的防范措施。

隐蔽通道在网络安全领域有特殊的作用。如何绕过网络安全机制，建立稳定的秘密通信信道，是网络隐蔽通道的任务之一。网络隐蔽通道也可看作是网络附加带宽，如何充分利用这些附加带宽资源进行网络管理和安全防护是一个值得研究的方向。因此，从网络攻击和防御 2 个方面对网络隐蔽通道进行研究是一种有益探索。

(下转第 165 页)