基于扩展首部 hop-by-hop 的 IPv6 包标记算法研究*

李明珍, 蒋 华, 王 鑫
(桂林电子科技大学 计算机科学与工程学院, 广西 桂林 541004)

摘 要: 针对如何将 IPv4 环境下的包标记技术应用于 IPv6 的问题,结合已有的算法思想提出一种改进的算法,该算法采取固定概率将路由信息标记到扩展首部 hop-by-hop,隧道模式下节点标记数据包时增加一个复制操作,扩大标记算法的适用范围;利用 ESP 的加密算法有选择地对标记消息进行加密。实验结果表明,新方案的兼容性和安全性得到了极大的提高。

关键词: IPv6; 分布式拒绝服务; IP 追踪; 包标记; 扩展首部; hop-by-hop; 加密
中图分类号: TP393 **文献标志码**: A **文章编号**: 1001-3695(2012)06-2313-04
doi:10.3969/j.issn.1001-3695.2012.06.083

IPv6 packet marking algorithm research based on extension header hop-by-hop

LI Ming-zhen, JIANG Hua, WANG Xin
(*School of Computer Science & Engineering*, *Guilin University of Electronic Technology*, *Guilin Guangxi* 541004, *China*)

Abstract: Aiming at how to solve the problem of IPv4 packet marking applying to IPv6 packet marking, this paper proposed an improved algorithm. The improved algorithm used deterministic probability to mark route information into extension header hop-by-hop. In tunnel mode, the improved algorithm added a copy operation to expand the scope of application of the algorithm. It used the encryption algorithm of ESP electively to encrypt marking information. Experiment shows that the compatibility and security of the new scheme is greatly improved.

Key words: IPv6; DDoS; IP traceback; packet marking; extension header; hop-by-hop; encryption

0 引言

随着网络技术和 Internet 的迅猛发展,基于 IP 的设备大规模使用,给人们生活带来便利的同时也导致了 IP 地址过快消耗且即将耗尽的问题。为解决这一问题,IPv6 应运而生。

IPv6 解决了地址空间的不足,适应日益复杂的编址需求,提供了一定的安全机制,但其通信机制并没有发生实质的改变,IPv4 下的网络威胁 DDoS 攻击仍然存在。

包标记技术作为一种有效防御 DDoS 攻击的 IP 追踪技术,近几年来成为网络安全领域研究的一个重点。IPv4 下,从包标记技术(PPM)的提出[1],到高级标记和高级认证包标记[2]、动态自适应概率包标记(ADPPM)[3],其研究取得了很大的进展。尽管 IPv4 下的包标记技术已经很成熟,但 IPv6 自身的特点[4,5]使得以往的包标记算法不能直接应用于 IPv6。近几年来,有不少学者对 IPv6 下的追踪技术进行研究,文献[6,7]提出一种对单个数据包追踪的 SPIE(源路径隔离引擎)改进方案,该方案过多占用 CPU 和内存资源,存在较大的局限性;文献[8]对各种追踪技术进行了综述,流标签的定义日益明确且长度有限,故提出利用扩展首部的 hop-by-hop 选项作为标记区域的标记算法,离攻击者最近的边界路由器标记所有经过该路由器的数据包,标记信息为该边界路由器接口的 IP 地址,不足的是边界路由器要对所有数据包进行标记,处理负担过重,若边界路由器不可信则该算法完全失效;文献[9]中选用 hop-by-hop 作为标记区域,采用动态概率,将相邻两个路由器的 IP 地址标记到该区域,利用 PMTU 协议对 MTU 进行修改,避免过多分片,但该算法没有考虑到 IPv6 的隧道模式,以及 IPv6 现有的安全机制不能防止攻击者对扩展首部中的内容进行窜改。

本文从 IPv6 协议出发,研究适用于该环境下的标记方案,在文献[9,10]算法的基础上,提出 IPv6 传输模式和隧道模式下标记功能兼容的算法改进方案,并提出对标记信息进行加密,增加对标记信息的安全保证,对 IPv6 安全机制进行补充。

1 IPv6

1.1 IPv6 报头格式[4]

IPv6 报头由首部和扩展首部两部分组成,前者是报头的不变部分,后者由若干个功能不同的扩展首部组成。首部格式如图 1 所示。

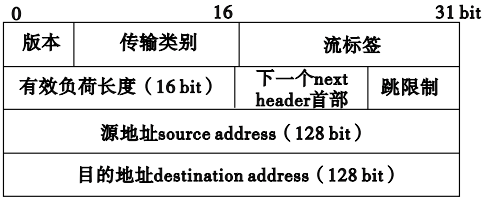


图1 IPv6报头首部格式

图 1 中,next header 标志下一个尾随首部的扩展首部,source address 和 destination address 分别标志数据包的源地址和目的地址。

收稿日期: 2011-10-15; **修回日期**: 2011-11-27 **基金项目**: 广西壮族自治区自然科学基金资助项目(0991071)

作者简介:李明珍(1986-),女,河南新乡人,硕士研究生,主要研究方向为网络技术与网络信息安全(583185636@qq.com);蒋华(1963-),男,河南信阳人,教授,博士,主要研究方向为数据库系统与信息安全;王鑫(1976-),男,陕西蓝田人,副教授,硕士,主要研究方向为网络与信息安全.

扩展首部位于 IPv6 首部和上层协议首部之间,IPv6 定义了 hop-by-hop options 等若干个扩展首部,可以提供对多种应用的支持,每一个首部由“next header”标志,多于一个扩展首部时,hop-by-hop 选项必须紧跟 IPv6 首部,其他的扩展首部排列顺序不作要求,其格式如图 2 所示。除目的节点外,不允许任何中间节点检测和处理 hop-by-hop 之外的其他扩展首部,但传输路径上每个中间节点必须检测和处理 hop-by-hop 选项。路由器处理扩展首部的顺序严格按其排列的顺序进行,不能针对某一首部进行查找、检测操作。

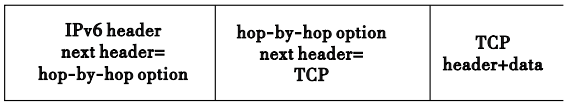
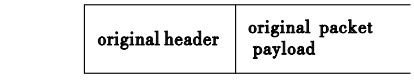


图2 扩展首部格式

1.2 隧道技术[5]

IPv6 隧道技术旨在解决使用不同网络协议的网间互通信问题和数据包的传输安全。该技术将一个数据包作为 IPv6 数据包的有效载荷进行封装,在隧道中转发,到达目的节点时解封装。进行封装操作的节点称为入口节点,解封装的节点称为出口节点,封装好的包称为隧道包,隧道包在源节点和目的节点之间传输的路径称为隧道。一种典型的 IPv6 隧道方案是,中间节点通过为封装包指定特定的转发路径,来施以显式路由控制。这种路由控制是通过为已选择的包添加封装首部来实现的。本文以点对点单向单层封装隧道为例,封装格式如图 3 所示,隧道通信如图 4 所示。在入口节点 *B* 进行封装,封装好的隧道包在 *B*→*C* 隧道中传输时,每个中间节点按照 IPv6 协议规则处理隧道包,在出口节点处解封装,得到源数据包,并转发给 *D*。



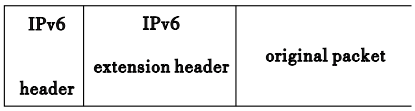


图3 数据包封装格式

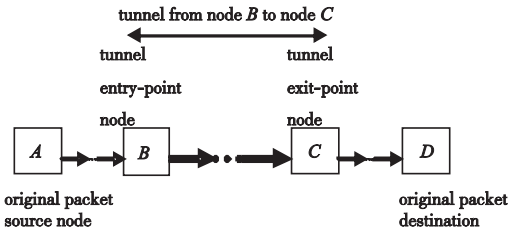


图4 隧道

1.3 安全架构[11]

IPSec(Internet protocol security)是一种开放标准的框架结构,在网络层提供安全服务,旨在保证网络层和上层协议的安全。该框架提供的安全服务集包括访问控制、无连接传输模式的完整性、数据源认证、防重放攻击(局部完整性)、加密和通信数据流保密性。

SA(security association)提供安全服务的单向连接。IKE(Internet key exchange)用来管理密钥的交换和管理。SA 是 IPSec 的基础,AH 和 ESP 都是利用 SAs 和 IKE 的一个维持安全关联的主要功能。

通过使用 AH(authentication header)和 ESP(encapsulating security payload)、密钥管理规章和协议,实现 IPSec 提供的安全服务。

1.3.1 AH[12]

AH 提供无连接完整性、IP 数据包数据源身份认证和抗重放攻击,但不提供数据包的保密服务。在传输过程中,IP 报头中有发生变化的字段,AH 不能提供对这些字段的认证。传输模式和隧道模式下 AH 的位置和认证范围如图 5 所示。

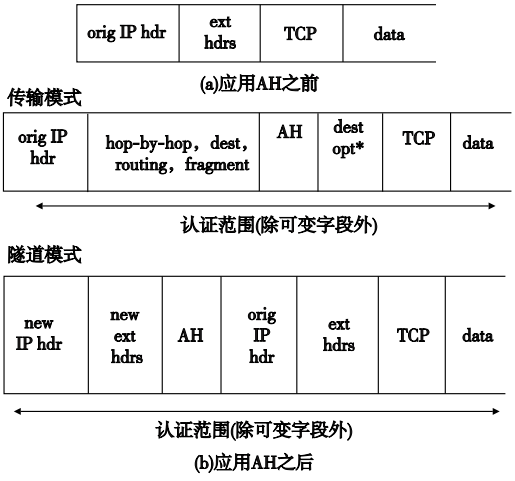


图5 AH

1.3.2 ESP[13,14]

ESP 提供加密、数据源认证、无连接完整性、抗重放攻击和有限数据流保密。往往 ESP 和 AH 联合使用才能防御多种攻击提供更高级的安全保证。ESP 的位置和认证加密范围如图 6 所示。

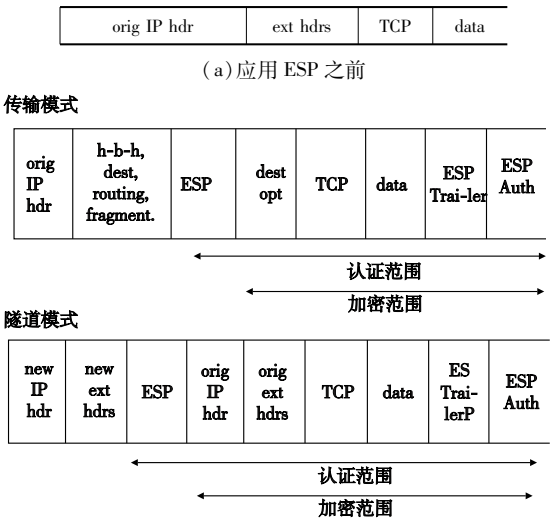


图6 ESP

ESP 所使用的加密算法由 SA 指定,一般使用对称式加密算法 DES-CBC,它采用一个 56 bit 的密钥以及附加的 8 bit 奇偶校验位,产生最大 64 bit 的分组大小。目前,常采用 DES 的变体 DES3,它使用 168 bit 的密钥对数据进行三次加密,可以提供极强的安全性。

2 基于扩展首部 hop-by-hop 的 IPv6 包标记算法

2.1 V6PPM 算法描述[9,10]

选择 IPv6 报头的扩展首部 hop-by-hop 作为标记区域,满

足类型—长度—值(TLV)的编码格式,便于相关节点对其进行处理。标记格式如图 7 所示。

next header	exten header length	pad N option	opt data length=0	opt type=X	opt data length=34	sttl	distance
ESAddr(128 bit)							
EEAddr(128 bit)							

图7　标记格式

用三元组〈distance, ESAddr, EEAddr〉表示一条边,其中,distance 表示该边的起点距离受害者的跳数,ESAddr 和 EEAddr 分别表示该边的头尾节点的 IPv6 地址。这里对 IPv6 地址不作任何处理而直接作为标记信息,可降低路径重构时的算法复杂度。Distance 表示数据包离开攻击者的跳数;sttl 表示数据包第一次被标记过后离受害者的跳数,路径重构时用于对标记包的分类[9]。若一个节点决定以概率 $p=0.04$(文献[1]中验证该概率为最优概率)标记数据包,IP 地址标记到 ESAddr 字段,则该节点的下一个节点必须标记该数据包,将其 IP 地址标记到 EEAddr 字段[10]。

2.2　算法改进

2.2.1　隧道模式下标记算法的改进

IPv6 封装由 IPv6 首部和若干个扩展首部组成。对 IPv4 数据包、IPv6 数据包和上层协议数据包进行封装(此处,以 IPv6 数据包为例),发生在隧道的入口节点,封装过的数据包在隧道内传输,在隧道的出口节点处解封装。

路由信息的标记可以发生在任何一个节点,包括隧道内的任一节点。若数据包传输过程中无隧道,路由信息标记和路径重构过程与 IPv4 环境下的类似。若传输过程中有隧道,隧道中节点标记的路由信息在封装的 IPv6 扩展首部 hop-by-hop 中,而不是在源数据包的扩展首部中,因此,在隧道的出口节点处解除封装时,增加一个步骤,检查扩展首部中的 hop-by-hop 是否有标记信息。有的话进行一个复制操作,将标记信息复制到源数据包的扩展首部 hop-by-hop 的相应标记字段里;无标记信息的话,不作任何操作。算法描述如下:

```
for each tunnel packet p1 that its source packet is packet p
  if(p1.ESAddr! =NULL)
    p.sstl = p1.sstl +1;
    p.distance = p1.distance +1;
    p.ESAddr = p1.ESAddr;
    p.EEAddr = p1.EEAddr;
  else
return;
```

2.2.2　标记信息的加密

IPv6 协议的 AH 和 ESP 具有的认证功能,只能对数据源身份进行认证,不能保证标记信息的安全,而 ESP 中的加密算法具有信息保密功能,但 ESP 加密的字段如图 6 所示,不包括封装的新的扩展首部。因此,综合考虑算法复杂度和其他各种因素,本文选取沿用 ESP 的加密算法 DES3(与 ESP 的加密算法保持一致),对标记信息进行加密,完善 IPv6 的安全机制。

DES 为分组密码算法,分组长度为 64 bit,有效密钥长度为 56 bit,明文和密文长度均为 64 bit。DES 使用 56 bit 密钥对 64 bit 的一个明文分组,经过 16 轮迭代,完成加密过程。具体过程如图 8 所示。IP 表示初始置换,L_i 和 R_i 为明文经过初始置换后分成的两个分组。F 为轮函数,DES 的核心,由扩展置换(E 盒)、非线性代换(S 盒)和线性置换(P 盒)三部分组成,处理过程如图 9 所示。DES 的加密过程描述为

$$L_0R_0 \leftarrow \mathrm{IP}(\langle 64\ \text{bit 明文}\rangle)$$
$$L_i \leftarrow R_{i-1} \qquad i=1,2,\cdots,16$$
$$R_i \leftarrow L_{i-1} \oplus F(R_{i-1},K_i) \qquad i=1,2,\cdots,16$$
$$\langle 64\ \text{bit 密文}\rangle \leftarrow \mathrm{IP}^{-1}(R_{16}L_{16})$$

DES 的解密过程描述为

$$R_{16}L_{16} \leftarrow \mathrm{IP}(\langle 64\ \text{bit 密文}\rangle)$$
$$R_{i-1} \leftarrow L_i \qquad i=16,15,\cdots,1$$
$$L_{i-1} \leftarrow R_i \oplus F(L_i,K_i) \qquad i=16,15,\cdots,1$$
$$\langle 64\ \text{bit 明文}\rangle \leftarrow \mathrm{IP}^{-1}(R_0L_0)$$

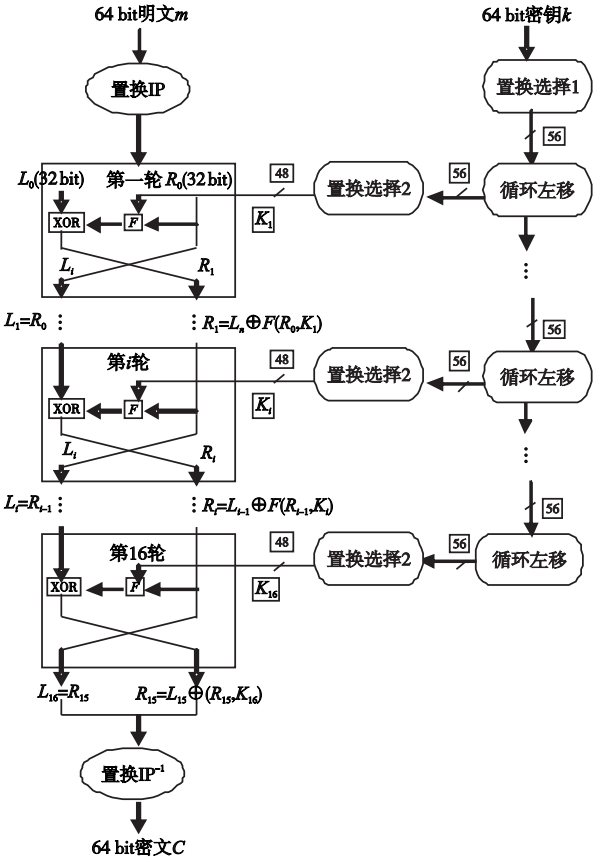


图8　DES基本结构

多重 DES 使用多个不同的 DES 密钥,利用 DES 加密算法对明文进行多次加密。三重 DES 的密钥长度≥112 bit,抗穷举攻击和抗中途相遇攻击,算法性能很好,尽管有诸如加密时处理速度较慢等不足,但在众多的加密算法中还是很有优势的。

本文可以将 128 bit 的 IPv6 分为两个 64 bit 明文分组进行加密,每个分组获取 128 bit 或 168 bit 的密钥,通过安全信道将密钥传送给接收方,接收方根据密文和密钥进行解密,恢复明文。

DES3 使用不同的密钥对明文进行三次加密,每次加密进行 16 轮的迭代,算法复杂度大大提高,因此,对标记信息的加密一般运用在安全系数要求极高的环境下。

3　性能分析

包标记方案性能的好坏主要体现在标记算法的复杂度和路径重构时所需的标记包的数量。

3.1　性能开销分析

3.1.1　算法复杂度

文献[9]中的 V6PPM 算法的复杂度为 $O(1)$。如果不选

择对标记信息加密,与 V6PPM 算法相比,包标记算法多一个将封装包中的标记信息复制到源数据包的操作,该操作的时间复杂度仍为 $O(1)$,对标记算法本身几乎没影响,但该算法却能在 IPv6 环境下的传输模式和隧道模式下正常运行,扩大了包标记算法的使用范围。

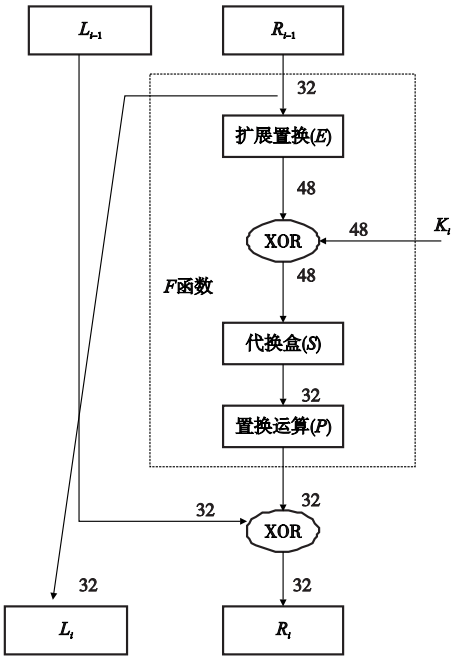


图9 轮函数F的处理过程

如果选择 DES3 对标记信息加密,则标记算法的复杂度将大大增加。DES3 算法的核心是矩阵的置换和变换,其时间复杂度为 $O(n^2)$,与 $O(1)$相比,复杂度大大增加。

3.1.2 重构路径时所需标记包的数量

路由器以概率 p 标记数据包,该节点与其下跳节点视为一个逻辑节点,标记概率仍为 p,与其他节点标记数据包的概率相同且相互独立。受害者收到一个标记包的概率为 $dp(1-p)^{d-2}$,一个标记包可以得到一个边,改进的标记算法路径重构时所需的标记包的期望值为

$$E(X) < \frac{\ln(d)}{p(1-p)^{d-2}}$$

与文献[10]中的算法相比,

$$\frac{\ln d}{p(1-p)^{d-2}} \Big/ \frac{\ln d}{p(1-p)^{d-3}} = \frac{1}{1-p} = 1.04$$

改进的算法重构路径时所需的标记包几乎相同,而本文的算法使用范围大,且可以有选择性地进行加密。

3.2 实验结果

本文实验环境 Linux + NS2,使用 Tcl 和 C ++ 语言实现。文献[15]中指出,一个数据包在网络中经过的跳数不超过 30,故实验设置 $p = 0.04$,攻击路径 d 从 1 取到 30,做 3 000 次实验,得出的标记包数量取平均值,实验结果如图 10 所示。

从图 10 中 ADPPM、文献[9](标记概率 $r = 0.04$)、文献[10](标记概率 $p = 0.04$)和本文改进的算法(标记概率 $p = 0.04$)性能比较可以看出,后三者的性能比较接近,但本文算法的优势在于,吸取了文献[10]中算法的优点,标记算法简单,标记概率不用计算而由节点事先设定好,普遍适用于 IPv6 网络环境,在保证重构效率的前提下,提高了算法的兼容性和灵活性,可以有选择性地进行加密。

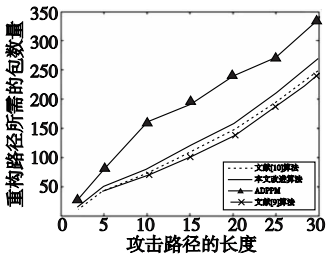


图10 各种包标记算法重构所需的标记包

4 结束语

实验结果表明,本文的标记算法适用于 IPv6,并且具有较好的算法性能,标记算法兼容性和标记信息安全性有了很大提高。不足的是,重构路径时所需的数据包和准确度大致相同,没有改进;增加的兼容性算法和加密算法增加了算法复杂度,给路由器造成较大的处理负担。今后的研究重点是如何减少重构路径时所需的标记包和降低算法的复杂度。

参考文献:

[1] SAVAGE S, WETHERALL D, KARLIN A, *et al*. Practical network support for IP traceback [C]//Proc of ACM SIGCOMM Conference. New York: ACM Press, 2000: 295-306.

[2] SONG D, PERRIG A. Advanced and authenticated marking schemes for IP traceback [C]//Proc of IEEE INFOCOM. [S. l.]: IEEE Press, 2001: 878-886.

[3] PENG Tao, LECKI C, RAMAMOHANROA K. Adjusted probabilistic packet marking for IP traceback [C]//Proc of NETWORKING. London: Springer-Verlag, 2002: 697-708.

[4] DEERING S, HINDEN R. RFC 2460, Internet protocol, version 6 (IPv6) specification[S]. [S. l.]: IETF, 1998.

[5] CONTA A, DEERING S. RFC 2473, Generic packet tunneling in IPv6 specification[S]. [S. l.]: IETF, 1998.

[6] STRAYER W T, JONES C E, TCHAKOUNTIO F, *et al*. SPIE-IPv6: single IPv6 packet traceback, local computer networks[C]//Proc of the 29th Annual IEEE International Conference on Local Computer Networks. Washington DC: IEEE Computer Society, 2004.

[7] 占勇军,谢冬青,周再红,等. IPv6 下基于改进的 SPIE 源追踪方案[J]. 计算机工程与科学,2007,29(4):11-13.

[8] OBAID C S, SEON H C. On IPv6 traceback[C]//Proc of ICACT. 2006: 2139-2143.

[9] 杨俊,王振兴,郭浩然. 基于扩展头随机标记的 IPv6 攻击源追踪方案[J]. 计算机应用研究,2010,27(6):2335-2337,2340.

[10] 蒋华,李明珍,王鑫. 一种基于概率包标记 PPM 的算法改进方案[J]. 山东大学学报:理学版, 2011,46(9):85-88.

[11] KENT S, ATKINSON R. RFC 2401, Security architecture for the Internet protocol[S]. [S. l.]: IETF, 1998.

[12] KENT S, ATKINSON R. RFC 2402, IP authentication header[S]. [S. l.]: IETF, 1998.

[13] KENT S, ATKINSON R. RFC 2406, IP encapsulating security payload (ESP)[S]. [S. l.]: IETF, 1998.

[14] PEREIRA R, ADAMS R. RFC 2451, ESP CBC-Mode cipher algorithms[S]. [S. l.]: IETF, 1998.

[15] THEIMANN W, ROTHERMEL K. Dynamic distance maps of the Internet[C]//Proc of IEEE INFOCOM. 2000: 275-284.