

基于 MPLS 的电子商务匿名技术模型研究与实践

解争龙¹, 吴振强², 弋改珍¹, 王 芳¹

(1 咸阳师范学院 信息工程学院, 陕西 咸阳 712000; 2 陕西师范大学 计算机学院, 陕西 西安 710062)

摘 要: 电子商务作为贸易手段已经进入人们的日常生活, 如何保护商业机密、个人隐私是电子商务贸易中急需解决的问题. 根据 MPLS 工作原理, 在 Onion 匿名技术的基础上, 建立基于 MPLS 的电子商务匿名模型, 使用 Nettrace 对纯 Onion 匿名模型与基于 MPLS 匿名模型从安全和效率进行了比较. 结果表明, 基于 MPLS 匿名技术在保护用户隐私的同时, 提高 Onion 匿名模型的通信效率.

关键词: MPLS; 匿名技术; 电子商务; Onion

中图分类号: TP391

文献标识码: A

文章编号: 1000-7180(2012)02-0176-04

Study and Practice of the Anonymity Technology Model for Electronic Commerce Based on MPLS

XIE Zheng-long¹, WU Zhen-qiang², YI Gai-zhen¹, WANG Fang¹

(1 School of Information & Engineering, Xianyang Normal University, Xianyang 712000, China;

2 School of Computer Science, Shaanxi Normal University, Xi'an 710062, China)

Abstract: Electronic Commerce has stepped into the daily life of people. But how to protect the business confidentiality and personal privacy is one of the problems resolved quickly. According to the operating principle of MPLS, on the anonymity technology of Onion, their security and efficiency has been compared for the anonymity models of the pure Onion and the MPLS. The results show that the anonymity technology of MPLS-based protected the user's privacy, while developed the efficiency of the model of Onion.

Key words: MPLS; anonymity technology; electronic commerce; onion

1 引言

随着互联网技术的快速发展, 基于互联网技术的电子商务应运而生, 并以它的便捷、低成本等优势极大地刺激了消费者购买积极性, 使其发展迅速, 而且电子商务正在以一种现代商务模式逐步取代传统的商业运营模式. 而在消费者消费的过程中个人信息安全就成了主要问题, 他不希望别人知道自己的消费情况, 例如他买了什么, 买了多少, 消费了多少等等, 所以电子商务在整个运营过程中消费者个人信息安全也就成为电子商务发展的核心和关键问题, 它包括个人购买信息的网上传送、电子支付、物

流和电子商务销售商以营销为目的对消费者数据的挖掘和发布等环节, 每一个环节都可能造成消费者隐私信息的泄密. 本文主要研究保证消费者的个人隐私信息在购买信息传送过程中的不泄漏.

近年来, 研究的热点是通过匿名技术实现信息和个人身份的保密, 而洋葱路由是主要的匿名通信实现技术之一, 洋葱路技术以代理机制为基础, 不需要对互联网的应用层做任何修改就能实现洋葱路由技术, 洋葱路由的通信原理如图 1 所示, 由代理路由器对 IP 包所经过的路由节点进行层层加密并加一个明文头封装形成洋葱包, 中间的各级洋葱路由器对所收到的洋葱包进行解密运算剥去洋葱包的最外

收稿日期: 2011-05-13; **修回日期:** 2011-07-25

基金项目: 陕西省科技厅计划项目(SJ08ZT14-8); 陕西省教育厅基金项目(08JK481)

层,并由明文头部得到下一跳的路由器地址,在包尾填充任意字符,使得包的大小不变,并把新的洋葱包明文头所指示的地址传递给下一个洋葱路由器,这样即使攻击者获得了洋葱包,他也只知道前一跳和后一跳地址,再无法向前和向后追踪地址,也就无法获知信息包的发送者或接收者,更无法知道包的内容,这样它不但实现了路径匿名,而且实现了发送者

和接收者匿名。在后来的研究中,对洋葱路由技术进行了多种改进,其中文献[1]应用群签名认证技术进行了改进,弥补了洋葱路由安全可靠性的不足,解决了扰乱性攻击问题。但在各种改进方案中缺乏考虑其实现的效率问题,它以系统带宽为代价换得匿名性;使用公钥算法耗费 CPU 资源,当网络流量比较大时,洋葱路由就成为了网络通信的瓶颈。

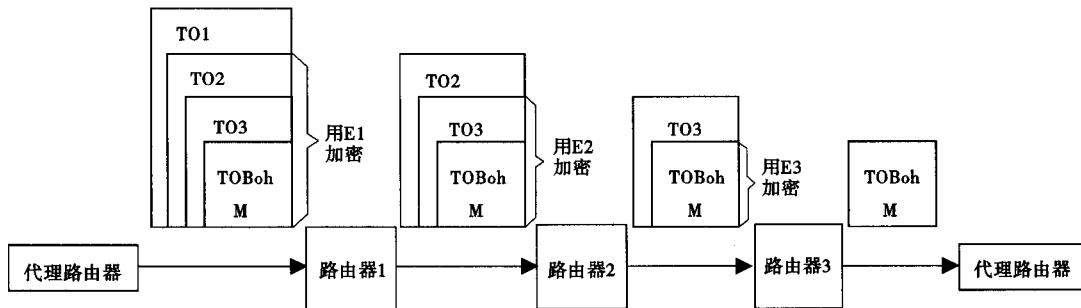


图1 洋葱路由通信模型

目前,在 Internet 主干网中的通信方案结合了路由和交换技术,出现了 G 位线速的路由交换机,洋葱路由器已经不能适应主干网络环境。因此,在大规模网络中实现匿名,必须提出新的匿名技术或对现有匿名技术进行改进。本文基于多协议标记交换技术(MPLS)的工作原理,利用 MPLS 实现匿名的技术优势,给出结合洋葱路由和 MPLS 技术的匿名通信模型,并分析了该模型的安全性和效率。

2 多协议标记交换(MPLS)的工作原理

多协议标记交换(MPLS)协议最初是为了提高转发速度而提出的,是一种用于快速数据包交换和路由的体系。MPLS 独立于二层和三层协议,使用定长标记作为分组在 MPLS 网络中传输时的唯一标志。在通信网络中,将 IP 地址映射为简单的具有固定长度的标记进行数据的交换与传输。MPLS 技术具有灵活性、可扩展性与高性能的特征,是 Internet 网络中一种理想的骨干组网技术^[2-4]之一。MPLS 的以下特征非常适合匿名通信:

(1) MPLS 是一种隧道技术。MPLS 将 IP 分组封装在 MPLS 帧中,帧中标记被当作内部表中的一个索引,以确定该使用哪一条输出线路,同时也确定该为它使用哪一个新的标记。数据的交换与转发通过识别标记实现,无法获得网络地址和信息内容。因此,MPLS 在能够保证数据传输的安全性和匿名性。

(2) MPLS 具有标签共享功能。将多个目标端

相同的流组合起来,并为这些流使用同一个标记,这些被组合起来共享一个标记的分组交换流属于同一个转发等价类,该类不但规定了这些分组的去向,而且也隐含了它们的服务类别。这一功能能够实现 Chaum 所定义的混淆(Mixes)功能。

(3) MPLS 的定长标签机制。在网络中转发分组时,MPLS 使用定长标签,使得分组转发简化、快捷。可以有效支持路由器的容量扩展功能。

(4) MPLS 中的路由。MPLS 的功能实现介于网络层与数据链路层之间,相当于 2.5 层。使用显式实现路由,与链路层无关,支持 X.25、帧中继等多种网络类型。

3 基于 MPLS 的匿名通信模型

基于 MPLS 的匿名通信模型分为两部分:主机代理模型和带标记交换模型。

主机代理模型由应用程序层、应用代理系统、网络层、MPLS 标记封装层构成。其中应用代理系统又由应用过滤层、特定转换层和 Onion 管理层组成,如图 2 所示。在网络通信的过程中,应用进程发出服务请求;应用过滤层对输入/输出信息进行验证,限制一些非法访问;特定转换层的主要任务是将应用进程协议数据单元分割为固定长度的信元(cell),信元长度因网络而不同,在第二代洋葱路由技术模型^[5]中,信元大小由原来的 42 byte 扩大到 128 byte;Onion 管理层是洋葱路由技术的核心层,通过该层建立传输层的匿名连接。因此在 Onion 管理层

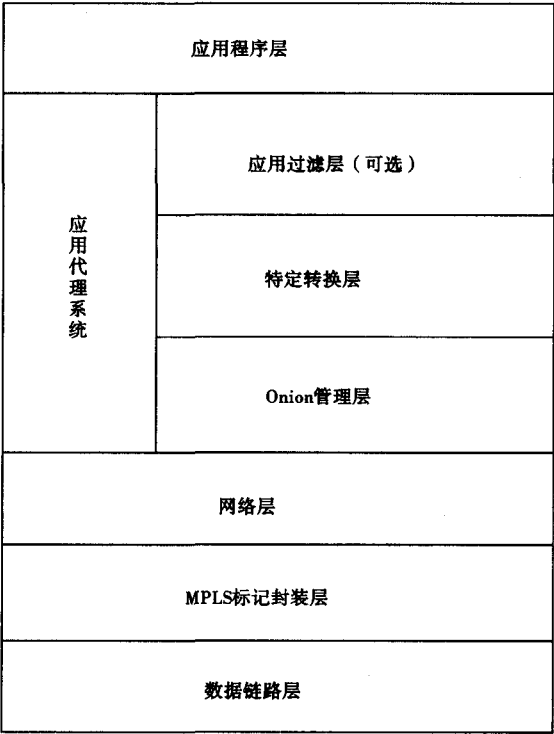


图 2 主机代理模型

能够获取连接的目的地址,以及该包到达目的节点所经历的路由信息、传输的公钥认证、节点的加入与退出策略。本模型中使用应用代理系统,在网络层加入洋葱路由策略,实现显式路由,容易与现有的 Internet 实现集成。MPLS 标记封装层对网络层的数据进行封装,采用标记路由,可直接连接到标签交换路由器(Label Switching Router, LSR),便于实现带标记洋葱路由交换,以提高效率。

带标记交换模型(图 3)应用于数据传输,由标记路由和 Onion 路由、MPLS 标记和物理层组成。物理层实现数据、控制等信息位的编码、同步传送;MPLS 标记实现与主机代理模型中同等层的协议,实现被封装包的交换,以提高效率;标记路由与 Onion 路由将 MPLS 标记封装数据包上传到该层进行路由,由软件完成,每台交换路由器只需识别 IP 地址,即可决定采用何种策略进行路由转发。该模型使用 MPLS 标记提供了路由交换的高效性,同时也达到了与目前路由器兼容的目的。

4 模型性能分析

4.1 安全性分析

该模型将电子商务通信网分为主机、网络、服务器三段。在主机-网络接口,由洋葱路由策略提供其安全性;在 MPLS 内部,由 IPSEC 确保 MPLS 安全

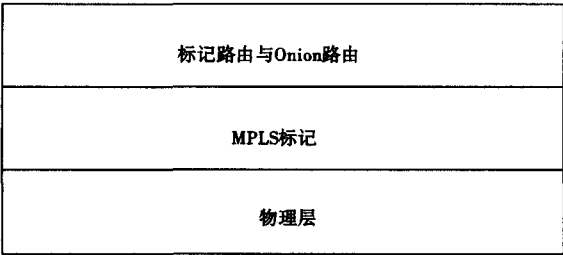


图 3 带标记交换

性。该模型利用 MPLS 隧道特性,封装加密的洋葱路由分组。这样,攻击者只可获得包的目的 LER,无法得知发送者与接收者的地址信息。因此,该模型的安全性不低于纯 Onion 网络的安全性。如果需要考虑 LER 之间的路由器 IP 地址的隐藏,那么在相邻 LER 再进行端到端的加密。此时该模型的匿名性更强。

4.2 模型效率

从协议和传输两个方面进行分析。假设传输信元头有 8 byte,信元为 128 byte,Onion 层的包头是 12 byte,密钥和证书等信息长度为 16 byte,中间路由器数目为 5 至 11。经过该模型,传送的有效数据包信息长度为 128+8=136 B,利用效率公式:

$$p = (128 + 8) / (128 + 8 + 12x + 16x),$$

式中, x 为路由器的数目,计算协议效率近似为 49.3%~30.6%。然而,在大多是网络环境下,路由器数都大于 11;通过 nettrace 软件测得发往 Microsoft 公司的路由器数为 17,如图 4 所示,如果采用纯 Onion 技术,协议效率仅为 22.2%。由此路由协议的效率随着路由器数的不同而发生变化。根据串 Onion 设计原理,利用填充技术是的洋葱路由包长度相等,加大攻击者分析难度,达到了混淆的效果。因此,纯 Onion 网络一般按照最大可能的路由器数进行实现,最大数不超过 32^[6]。如果最大路由器数为 32,在 Internet 上采用纯 Onion 路由实现匿名技术,协议效率只有 13.2%;如果采用基于 MPLS 匿名模型,由图 4 可知,如果收发双方的本地网路由器按 2 级计算,中间路由使用 MPLS 路由进行交换,则本文建议的模型协议效率为 54.8%,效率高于纯 Onion 路由。

根据传输效率公式:

$$P = \frac{\text{包的长度 } L(\text{bit})}{\text{延迟时间 } T(\text{s})},$$

传输效率 P 取决于延迟时间 T ,延迟时间 T 由包在路由器中的排队等待时间和洋葱变换时间两部分构成。假设收发双方的本地网络的 2 级路由由方案相同。如果主干路由采用纯 Onion 路由,包在经过每个路

由器是需要进行排队,并利用 P-K 公式^[7]: $D_{SK}(E_{PK}(X))=X$ 进行解密交换,纯 Onion 包的延迟时间取决于平均包到达率、包的平均发送时间和方差值,当网络流量超过 80% 时,延迟时间将逐渐趋于无穷大;对于相同的网络配置,如果采用基于 MPLS 匿名模型,当包到达 MPLS 交换机时,只根据包携带

的标签搜索标记库 LIB,进而建立输入与输出的连接,将包直接交换至下一个节点.因而,包在 MPLS 交换机中无需进行存储,也不需要加解密,与纯 Onion 相比,交换时间可以忽略.因此,本文建议的匿名模型在传输效率上优于纯 Onion 技术.

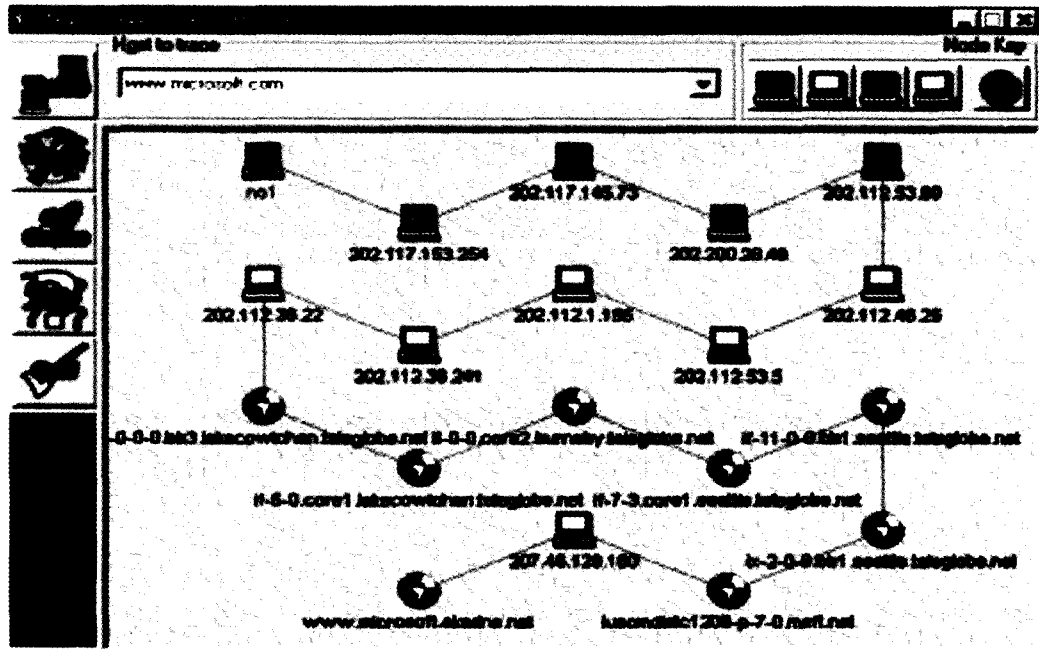


图4 发往 Microsoft 公司的数据包跳数

5 结束语

本文在洋葱路由匿名通信模型的基础上,提出适合电子商务的基于 MPLS 的匿名通信模型.在网络中,该模型的实现分为两个阶段:收发双方本地网络内部匿名和主干网络匿名通信.基于 MPLS 匿名模型主要在主干网中实现高效通信和匿名.与纯 Onion 方案相比,在安全性方面,本文建议的模型具有更高的安全性;在传输效率方面也优于前者.利用 MPLS 与 Onion 技术的结合,在电子商务中不但实现了匿名通信,保护了消费者隐私,而且提高了传输效率.

参考文献:

- [1] 赵福祥,王育民,王常杰.可靠洋葱路由方案的设计与实现[J].计算机学报,2001,24(5),463-467.
- [2] 吴江,赵慧玲.下一代的 IP 骨干网络技术——多协议标记交换[M].北京:人民邮电出版社,2001.

- [3] IETF MPLS 工作组草案. draft-ietf-mpls-lsr-mib-08.txt [S]. 2002-01.
- [4] IETF MPLS 标记栈编码. draft-ietf-mpls-label-encaps-04.txt [S]. 1994-03.
- [5] Paul F Syverson, Gene Tsudik, Michael G. Reed, et al. Towards an analysis of Onion routing security [J]. Workshop on Design Issues in Anonymity and Unobservability Berkeley, CA, 2000.
- [6] Robert Carter, Mark Crovella. Dynamic server selection using dynamic path characterization in wide-area networks [C]// Proceedings of the 1997 IEEE INFOCOM Conference, Kobe Japan; IEEE, 1997.
- [7] 谢希仁. 计算机网络[M]. 2 版. 北京:电子工业出版社,1999.

作者简介:

解争龙 男,(1961—),硕士,教授.研究方向为计算机网络与信息安全.