移动IP中通信匿名技术的设计与实现

Design and Implement of the Anonymous Communications in the Mobile IP Networks

康 凯 郭 伟 吴诗其

(电子科技大学通信抗干扰国防重点实验室 成都610054)

Abstract One of the key problems in the mobile communication is the anonymous communication. The mobile user wants to hide his real identifying information to the visiting domain and the public network which he does not trust, and prevent from being tracked and located. In this paper, we have discoursed the anonymous communications in the mobile IP, and presented a novel strategy of the dynamic address allocation and the routing with anonymity. The suggested method enables any identifying information can be carried over the anonymous and secure connections, and provide end-to-end security. The implements of the mobile host and the mobile subnet are also presented.

Keywords Anonymous communications, Security, Mobile IP, Routing

一、引言

移动IP[1~2]是一个在互联网上支持移动性功能的网络层解决方案,可以使移动节点以一个永久IP地址接入到任何网络上,并实现将IP包路由到位置不断改变的移动节点上。IP本身没有任何安全特性,容易造成对网络中通信的攻击。IP Sec体系结构为此定义了一个网络层的系统解决方案[3]。

移动通信中的一个重要的安全问题是身份匿名。对于在外地链路的移动用户,基于安全性原因,希望对不可信任的访问域和公用网隐藏其真实身份和防止对其位置移动性进行跟踪。匿名性是移动通信协议设计中的一个重要问题,在匿名交易、虚拟专网、军用通信保密中都有广泛的应用[2~6]。本文中我们主要讨论移动IP环境下的身份匿名和相应的路由问题,限定在由移动性引入的安全问题和IP层的安全处理。

二、移动IP中的通信匿名策略

本文所提出的通信匿名策略的基本思想是,为在外地链路的移动节点动态分配一个临时IP地址,并利用移动节点和家乡代理之间的共享密钥加密后传给移动节点。移动节点在外地链路采用临时IP地址申请入网,通过匿名和安全的连接传送报文,实现了移动节点与家乡代理之间端到端的保密性,使第三方无法从通信连接中获得移动用户的真实身份信息。新的通信匿名策略可以定义为注册、临时地址更新和数据包路由三个系统进程。以下我们进一步分别说明这三个系统进程的实现。

1 注册

移动节点(MN)离开家乡子网时,由家乡代理向DHCP服务器代理申请获得一个临时IP地址,前缀为家乡代理的某个端口的前缀。家乡代理中建立绑定表项[MN,MN1],并对临时地址MN1执行代理ARP。移动节点使用临时地址在外地链路时标志其身份。

1)移动节点在外地链路上使用外地代理转交地址(FCOA)的注册:

移动节点使用临时地址向外地代理提交注册请求消息。

IP[MN1,HA]| UDP| Reg Req[D=0,MN1,HA,FCOA]

外地代理需要记录下源数据链路层地址,源IP地址,源UDP端口号,家乡代理地址,标识域和请求的生存时间,外地代理将注册请求消息中继到移动节点的家乡代理:

IP[FA,HA]| UDP| Reg Req[D=0, MN1, HA, FCOA]

家乡代理中建立对移动节点的绑定[MN1,FCOA],返回注册应答。

IP[HA,FCOA]| UDP| Reg Resp[lifetime,MN1,HA]

如果注册应答消息是有效的,外地代理将注册应答消息中继给移动节点。

IP[FA,MN1]| UDP| Reg Resp[lifetime, MN1, HA]

在这里虽然外地代理对移动节点的注册消息进行了应用层中继,但是外地代理所记录的只是移动节点的临时地址。由于临时地址是动态分配和更新的,并不能够根据临时地址进一步得到移动节点的身份信息。

2)移动节点在外地链路上使用配置转交地址(CCOA)的注册:

移动节点使用临时地址向访问域的DHCP服务器申请获得配置转交地址。移动节点使用与家乡代理的共享密钥,以AH-ESP传送模式向家乡代理发送注册请求消息。

IP[CCOA, HA]| AH| ESP| UDP| Reg Req[D=1, MN, HA, CCOA]

家乡代理建立对移动节点的绑定表项[MN, CCOA],同样使用AH-ESP传送模式返回注册应答消息。

IP[HA, CCOA]| AH| ESP| UDP| Reg Resp[lifetime, MN, HA]

移动节点返回家乡子网时,要向家乡代理同时注销临时IP地址和转交地址的绑定。

2 临时地址的动态更新

当使用临时地址完成一次通信或者安全关联(SA)预约的生存期将耗尽时,移动节点要和家乡代理之间协商新的临时地址。保持对临时IP地址的动态更新,可以有效地防止对移动用户位置移动性进行跟踪。移动节点向家乡代理发绑定警告(Binding Warn)消息,请求更新临时IP地址。

康 凯 博士生.郭 伟 教授.吴诗其 教授.

IP[MN1,HA]| AH| ESP| UDP| Binding Warn[MN, MN1]

家乡代理会发现绑定警告消息中的目标节点(Target Node Address)地址为MN1,表明是从移动节点发来的更新临时地址的请求,就会代理移动节点申请获取一个新的临时IP地址MN2。家乡代理向移动节点返回绑定更新消息,并置A比特为1,要求移动节点返回绑定应答。

移动节点使用新的临时地址MN2作为身份标识,并返回绑定应答消息。家乡代理收到绑定应答后,建立[MN, MN2]绑定表项,注销[MN, MN1]表项,通知DHCP服务器回收临时地址MN1,以重新分配。

3 通信匿名中的数据包选路

对端节点发往移动节点的数据包首先路由到移动节点的家乡子网,并被家乡代理截获。移动节点以外地代理转交地址注册时,家乡代理首先使用AH-ESP通道模式对原始IP包进行封装,通道出口地址为MN1。

IP[HA, MN1]| AH| ESP| IP[CN, MN]| Payload

该数据包与家乡代理中的绑定表项[MN1,FCOA]匹配,再进行第二次封装,隧道出口地址为移动节点的外地代理转交地址。完成第二次封装后,将IP包经输出端口发送。

IP[HA, FCOA]| IP[HA, MN1]| AH| ESP| IP[CN, MN]| Payload

外地代理将接收到的IP包剥去最外层的IP报头后,转交给移动节点:

IP[HA, MN1]| AH| ESP| IP[CN, MN]| Payload

移动节点调用IP Sec核心,进行相关的安全处理,剥去外层IP报头、AH头、ESP头,得到原始的IP包,重新交与网络层,按照普通的IP协议进行处理。

移动节点在外地链路上以配置转交地址注册时,家乡代理对原始IP包使用AH-ESP通道模式进行封装后发送,通道出口地址为移动节点的配置转交地址。

IP[HA, CCOA]| AH| ESP| IP[CN, MN]| Payload

数据包直接路由到移动节点,由移动节点完成相应的拆封操作和安全处理。可以看到,移动节点使用外地代理转交地址时,家乡代理需要进行一次AH-ESP通道模式的安全封装,通道出口地址为MN1;以及一次路由封装,隧道出口地址为外地代理转交地址。移动节点使用配置转交地址时,家乡代理只需要进行一次AH-ESP通道模式的安全封装,通道出口地址为CCOA。

4 移动网络中通信匿名的实现

移动网络[2]是指主机和路由器之间的相对位置是固定的,但是作为一个整体相对于网络的固定部分来说是移动的。移动路由器作为移动网络的缺省网关,负责维护路由表和执行隧道功能,对子网内主机屏蔽移动性。以下讨论移动网络的通信匿名问题,分别以MH和MR表示移动主机和移动路由器。

与移动主机相同,在外地链路的移动路由器向其家乡代理注册了一个临时地址MR1,和一个配置转交地址MR-COA。发往移动网络中主机的数据包被移动网络的家乡代理截获后,首先完成通道模式的AH-ESP安全封装,隧道出口地址为移动路由器的临时地址MR1。封装后的IP包会再次封装到一个目的地址为移动路由器的转交地址的IP包中发送。

IP[HA, MRCOA]| AH| ESP| IP[CN, MH]| Payload

经过封装的数据包路由到达移动路由器,在这里被拆除外层的IP报头后,完成相关的认证和解密操作,即得到原始的IP包,交与移动主机。

在相反的方向上,移动网络中所产生的数据包,如果目的地址不在移动网络上,移动路由器将原始数据包进行AH-ESP通道模式的封装,通道的出口地址为其家乡代理地址。

IP[MRCOA, HA]| AH| ESP| IP[MH, CN]| Payload

如果移动路由器与家乡代理间要求通过一条双向隧道交换路由更新信息[2],移动路由器对于自己产生的路由更新消息分组也要进行安全封装。

以下考虑了一个更为复杂的情况,一个外地匿名主机MH连接到一个移动网络上,而该移动网络连接在外地链路上,并且同样要求匿名通信。移动路由器为连接在移动网络上的移动主机提供外地代理功能。与文[2]同样地假设移动路由器向家乡代理MRHA注册了一个配置转交地址MRCOA;移动主机以移动路由器的家乡地址向家乡代理MHHA注册。另外,移动主机和移动路由器向各自的家乡代理分别注册了一个临时地址MH1和MR1。

对于发往匿名移动主机MH的数据包,按照常规路由协议[2],移动主机和移动路由器的家乡代理都要分别进行封装操作,最终将会得到一个经过两次安全封装复杂的报文格式:

IP[MRHA, MRCOA]| AH| ESP| IP[MHHA, MR]| IP[MHHA, MH1]| AH| ESP| IP[CN, MH]| Payload

应当注意到,在上面的报文中,由移动路由器的家乡代理所执行的安全封装对于发往移动主机的IP包是不必要的,因此应当对路由算法进行改进,来避免这一无谓的安全处理和封装开销。移动路由器在代理广播消息后附加一个RS扩展选项[7],通告其转交地址。外地移动主机从中获得移动路由器的配置转交地址,向家乡代理注册。家乡代理中建立绑定表项[MH1,MRCOA]。这样发往移动主机的数据包被家乡代理截获后,直接封装转发到移动路由器的转交地址。

IP[MHHA, MRCOA]| IP[MHHA, MH1]| AH| ESP| IP[CN, MH]| Payload

下图分别表示了两种情况下数据包的选路情况,图中以虚线表示无线链路,以黑体表示数据包路由过程中的隧道。

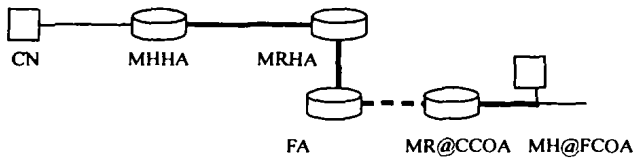

图1 移动网络中移动主机的数据包选路

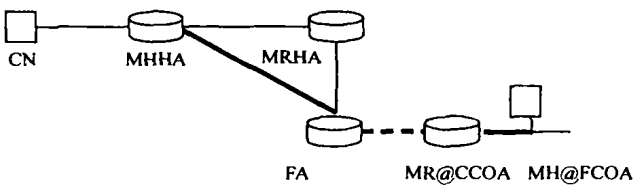

图2 移动网络中移动主机的数据包选路优化

在相反的方向上,为了避免造成重复的安全封装,移动路由器在转发数据包时要注意,对于由移动网络中的外地主机所产生的数据包,不必进行安全封装,而是直接传送。

(下转第108页)

的要求。

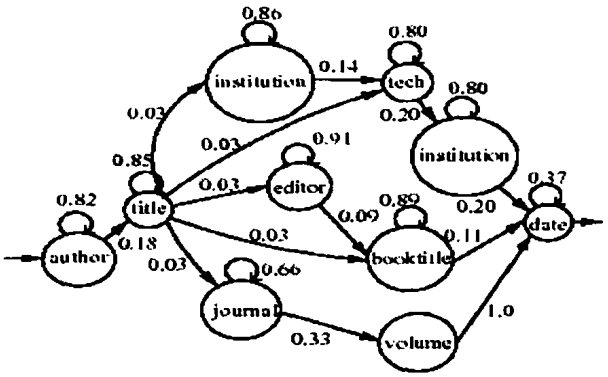

图6 基于 HMM 的信息抽取实例

总结与展望 在走出了网络经济的低谷之后，B2C 电子商务即将进入一个快速发展的时期，而信息抽取技术很有希望成为推动 B2C 电子商务发展的主要力量之一。在目前存在的信息抽取技术中，利用网站查询表格的信息抽取技术的信息查全率低；基于归纳学习的信息抽取技术和基于自定义查询语言的信息抽取技术的信息查全率与查准率较高，但是用户负担重；基于网页结构分析的信息抽取技术不需要用户参与，但是难以扩充；基于模式匹配的信息抽取技术和基于隐式马尔科夫模型的信息抽取技术则增加了用户负担。由此可见，目前存在的信息抽取技术均难以满足 B2C 电子商务的特殊要求。因此，研制一种对个人能力要求低、用户负担轻、信息查全率与查准率高、抽取速度快并且容易扩充的信息抽取技术不仅可以帮助 B2C 电子商务企业在网络经济市场中取得竞争优势，还可以吸引更多的消费者参与 B2C 电子商务，从而促进 B2C 电子商务的发展。

参 考 文 献

1 楼德宏. 国际互联网和企业电子商务. 轴承，2001(5)：33～37
2 http://www. the-dma. org/library/whitepapers/eCommerce_b2c_Exec_Summ_SS. pdf
3 http://www. linan. net/dzsw/b2c. htm
4 Doorenbos R, Etzioni O, Weld D. A Scalable Comparison-Shopping Agent for the World-Wide Web. In: Proc. First International Conference Autonomous Agents, Marina del Rey, CA, 1997. 39～48
5 Kushmerick N, Weld D, Doorenbos R. Wrapper induction for information extraction. In: Proc. IJCAI-97, Nagoya, Japan, 1997
6 Hgu C, Dung M. Generating finite-state transducers for semi-structured data extraction from the Web. J. Information Systems, 1998, 23(8)
7 Freitag D, Kushmerick N. Boosted wrapper induction. In: Proc. of the Seventeenth National Conference on Artificial Intelligence (AAAI2000), 2000. 577～583
8 Muslea I, Minton S, Knoblock C. A hierarchical approach to Wrapper induction. In: Proc. 3rd International Conference Autonomous Agents, 1999
9 Kushmerick N. Wrapper induction: Efficiency and expressiveness. Artificial Intelligence, 2000 (118): 15～68 (this issue)
10 Embley D W, Jiang Y, Ng Y K. Record-boundary discovery in web-documents. In: Proc. of the 1999 ACM SIGMOD, Philadelphia, Pennsylvania, USA, 1999
11 Chang C H, Hsu C N. Automatic extraction of information blocks using PAT trees. In: Proc. of the National Computer Symposium, Taipei, Taiwan, 1999
12 Buttler D, Liu L, Pu C. A Fully Automated Object Extraction System for the World Wide Web. Intel. Conf. on Distributed Computing Systems, 2001
13 Sahuguet A, Azavant F. W4F: a WysiWyg web wrapper factory. Technical report, 1998
14 Bauer M, Dengler D, Paul G. Instructible information agents for Web mining. In: Proc. 2000 Conference on Intelligent User Interfaces, 2000
15 Califf M, Mooney R. Relational learning of pattern-match rules for information extraction. In: Workshop in Natural Language Learning, Conference Assoc. Computational Linguistics, 1997
16 Soderland S. Learning to extract text-based information from the World Wide Web. In: Proc. 3rd Intl. Conf. Knowledge Discovery and Data Mining, 1997
17 黄豫清，戚广志，张福炎. 从 WEB 文档中构造半结构化信息的抽取器. 软件学报，2000，11(1)：73～78
18 Soderland S. Learning information extraction rules for semi-structured and free text. Machine Learning, 1999, 34(1-3): 233～272
19 McCallum A, et al. A machine learning approach to building domain-specific search engines. In: Proc. IJCAI-99, Stockholm, Sweden, Morgan Kaufmann, San Francisco, CA, 1999. 662～667
20 Freitag D, McCallum A. Information extraction with HMM structures learned by stochastic optimization. In: Proc. of the Seventeenth National Conference on Artificial Intelligence (AAAI-2000), 2000

(上接第88页)

结束语 本文对移动 IP 环境下的通信匿名和路由问题作了探讨，提出了一种具有匿名特性的动态地址分配和路由策略。新的通信匿名策略具有以下特点：

1)移动节点在外地链路使用临时 IP 地址标志其身份，数据报文通过匿名和安全的连接传送，实现了通信匿名。

2)临时 IP 地址利用移动用户和家乡代理的共享密钥加密后传给移动用户，保证了移动用户身份信息的端到端保密性。

3)临时 IP 地址动态分配和更新，防止了对移动用户位置移动性进行跟踪。

4)能够有效地支持移动 IP 下的虚拟私用网。

同时我们对移动主机和移动网络的实现情况分别进行论述。新的通信匿名策略不需要对原有的认证与加密算法、密钥分配协议和路由协议进行修改，在实际应用中易于实现。

参 考 文 献

1 Perkins. Mobile IP. IEEE communication magazine, May, 1997. 84～99
2 Solomon. 移动 IP. 机械工业出版社，2000. 1
3 Doraswamy. IP Sec: the new security standard for the Internet, intranet, and virtual private networks. 机械工业出版社, 2000
4 Murhammer. 虚拟私用网络技术. 清华大学出版社，2000
5 Fasbender. Variable and Scalable Security: Protection of Location Information in Mobile IP. IEEE VTC, 1996
6 Reed. Anonymous Connections and Onion Routing. IEEE JSAC, 1998, 10(4)
7 Distributed Registration to Mobile IP. draft-chuahli-mobileip-dremip-00. txt