第 34 卷 第 7 期 计 算 机 工 程 2008 年 4 月
Vol.34 No.7 Computer Engineering April 2008
·网络与通信· 文章编号：1000—3428(2008)07—0087—02 文献标识码：A 中图分类号：TP393

主机身份标识协议在异质无线网络中的应用

王全礼，傅 彦
(电子科技大学计算机科学与工程学院，成都 610054)

摘 要：未来的无线通信网络是一种不同无线技术和网络体系相结合的异质网络环境，同质无线网络的技术已不适合异质网络的发展。该文论述异质网络的移动管理和通信安全，利用主机身份标识协议(HIP)与上层协议的结合来实现技术要求，提出用 HIP-SIP 模型进行移动管理，在 TCP-HIP 模型上利用 IPsec 机制来保障通信安全。

关键词：主机身份标识协议；移动管理；会话发起协议；移动 IP；IPsec 协议

Application of Host Identity Protocol in Heterogeneous Wireless Network

WANG Quan-li, FU Yan
(Computer Science and Engineering College, University of Electronic Science and Techonology of China, Chengdu 610054)

【Abstract】 Since homogeneous wireless network technology is no longer suitable for the development of heterogeneous networks, the future wireless communication network is going to be a heterogeneous network environment which combines different wireless technology and network architectures. This paper proposes a new mobility management scheme based on Host Identity Protocol (HIP) and Session Initiation Protocol (SIP). The hybrid model HIP-SIP scheme is for all services, and the IPsec scheme in the model TCP-HIP is used to ensure communication in security.

【Key words】 Host Identity Protocol(HIP); mobile management; Session Initiation Protocol(SIP); mobile IP; IPsec

随着各种无线技术的快速发展，以前单一标准的无线网络的技术已经不适用于异质无线网络。主机身份标识协议(Host Identity Protocol, HIP)的出现在网络层次引起了较大的改变，它增加了网络安全性、可移动性，解决了 IP 地址在网络中由于多种协议需要其标识身份而带来的困难。本文重点讨论 HIP 在异质无线网络中的应用。

1 背景介绍

在对无线网络研究的过程中，涌现出了大量的相关技术。在同质无线网络中，移动管理能在数据链路层或者物理层进行处理；而在异质网络中，引入了不同的无线网络技术，上层(如网络层到应用层)是移动管理比较合适的选择，目前热门的有会话发起协议(Session Initiation Protocol, SIP)与移动 IP 相结合的模型，文献[1]对此机制作了详细的阐述和研究。

通信安全是无线网络的一项关键技术。文献[2]阐述了通过解决 IPsec 和 TCP PEP 之间矛盾的方式来解决安全通信问题，提出了相关的 4 个解决方案，总结出一个将 IP 数据报分解为几个部分，各个段分别有相应的保护机制，本文在引入 HIP 的情况下，将 IPsec 引入 HIP-TCP 模型来实现无线网络的安全通信。

1.1 会话发起协议

目前 SIP 被用来基于 IP 地址的无线网络的移动管理。但是其对移动性的支持有很大的局限性，本文通过将其和 HIP 结合起来实现对应用层各种应用移动性的全面支持。

1.2 主机身份标识协议

HIP 定义了一个新的名字空间主机身份。主机身份有 2 种表示方法：full Host Identity(HI)和 Host Identity Tag(HIT)。HI 是一个非对称密钥对中的公钥，主机本身持有此密钥对中的私钥，不同的公钥算法所产生的 HI 的长度并不固定。因此，用 HI 来作为报文的标示理论上可行，但不方便，而 HIT 是定长的，常使用 HIT 来标示主机身份。HIT 由 HI 通过哈希计算获得，由哈希的性质可知 HIT 表示主机身份是安全的。

2 HIP-SIP 模型

2.1 RVS 机制

HIP 是通过 RVS 机制来实现移动性的。RVS 类似移动 IP 中家乡代理的服务器。移动终端在 DNS 系统中登记自己的 RVS 服务器，一旦一个移动终端需要和另一个移动终端通信时，就发送一个 DNS 请求，获得对端的主机标识以及它的 RVS 服务器地址。然后，主机就可以使用对端的 HIT 作为目的 HIT，而把 RVS 服务器的地址作为目的地址发送 I1 报文，RVS 服务器会把报文中继到真正的目的主机。目的主机在收到 RVS 转发的 I1 后，马上发送地址更新信息到对端进行地址更新，也可以根据 RVS 服务器提供的服务类型，继续由服务器进行其他基本报文的转发。直到建立 HA 后，才发送包含 REA 参数的报文，通知对端自己的真实地址。

移动中的双跳和在 4 次交换的过程中 IP 地址改变的问题，在使用 HIP 协议 RVS 服务器的移动网络中，由于移动节点可以在更新自己优先地址的过渡期内使用原来的优先地址，直到新的优先地址有数据收到才真正切换到新的优先地

基金项目：国家自然科学基金资助项目(10476006)；国家“863”计划基金资助项目(2006AA10184143)；四川省应用基础研究基金资助项目(05JY029-067-2)

作者简介：王全礼(1983－)，男，硕士，主研方向：网络技术，数据挖掘；傅 彦，教授、博士

收稿日期：2007-04-29 **E-mail：**quanli83@yahoo.com.cn

址，这种网络在网络层解决了双跳问题。但在这种情况下，只有链路层同时拥有和网络中漫游前后的 2 个接入点在过渡期内同时具有通信链路，才能保证通信不中断。为避免移动主机的通信中断，也可以用 RVS 服务器。RVS 服务器转发包含 REA 参数报文(即更新报文 UPDATE(REA, SEQ))。在通信双方都是移动主机时，当移动主机的地址发生变化时，除了发送 REA 参数到对端主机外，还要发送 REA 参数给对方，即使双方都不能直接得到对方地址更新的通告，也必然会得到由自己 RVS 服务器转发的 REA 参数，从而能够继续发送数据到对端的当前位置，保证了通信的连续性。

2.2 HIP-SIP 模型

为了解决对移动性的全面支持，本文提出了一个 HIP-SIP 模型。该模型类似于 HIP-移动 IP 模型，只是移动 IP 在安全上存在问题，而 HIP 在这方面做得很好，另外在转发信号的时延方面相临层之间要比跨层之间要小得多。图 1 显示了 HIP-SIP 模型对移动管理的处理过程。该模型能处理所有应用层上的移动管理问题。要使 SIP 扩展能支持 HIP 协议，将 SIP 头部和 SDP 数据包上的 IP 地址用 HIT 来取代。

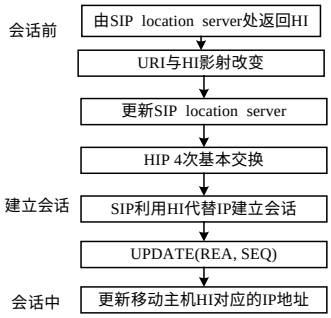

图 1 HIP-SIP 处理过程

在建立会话前，从本地 SIP 服务器(相当于移动 IP 中的家乡代理和 HIP 中的 RVS 服务器)处返回移动主机的 HIT，如果 URI 与 HIT 之间的影射改变的话就要更新 SIP 本地服务器，然后建立 HIP 连接的 4 次基本交换。通过 SIP 建立会话，此时 UDP 头部的 IP 地址被 HI 取代，下面的 IP 地址的改动对上层具有透明性。建立会话以后，SIP 就无须再向对端发送 INVITE 报文。更新动作由 HIP 来完成，移动管理由 RVS 机制来解决。

3 HIP-TCP 模型

TCP协议被应用到所有基于IP地址的无线网络中，包括3G/4G中的卫星网络和无线PAN，以及移动Ad hoc网络中。但是，文献[3-7]所描述的无线网络并不适合使用标准TCP协议，这是由于上述网络的某些特征对TCP协议来说是不合适的，比如无拥塞丢失[3]、长延迟[4]、不同的带宽[5]和动态改变拓扑结构等问题，为解决这些问题，文献[6]提出了TCP协议的增强机制TCP PEP。IPsec是无线网络中必需的安全机制，而IPsec与TCP PEP是冲突的[2]，文献[2]提出使用多层的IPsec机制来解决冲突问题。本文提出使用TCP-HIP机制来实现TCP PEP，在不改动TCP PEP机制的情况下，使用下层HIP协议来保证安全性，既简单又能解决IP地址的负担问题。

IPsec协议是由IETF设计通过认证头(AH)和封装安全载荷(ESP)来实现数据报的安全通信。由于HIP是端到端协议，而IPsec是保证端到端安全的协议，因此两者能结合。HIP本身已实现了认证，这里主要考虑的是与ESP的结合问题[9]。

为了能在 TCP 协议下使用 HIP 协议，本文使用一种在 HIP 4 次基本交换上的 TCP 连接。此模型要增加一个 TCP 选择项。这只是一个测试性的选项，也就是将 HIT 作为一个 TCP 选项放入建立 TCP 连接所要发出的 SYN 报文中。此模型解决了在 TCP 协议下使用 HIP 协议的问题。首先，发起者发出带有 HIT 的 SYN 报文。如果响应者支持 HIP 协议的话就会返回 R1 而忽略 SYN 报文。后面就是剩余的 3 次 HIP 报文交换。然后由发起者发出普通的 SYN(不含 HIT)报文以建立 TCP 连接。因此，在 HIP 层使用 IPsec 并与 TCP 共同实现 TCP PEP 机制是一个很有效的方法。

4 实验及结论

这里只对移动性进行实验，HIP-TCP 模型还只是一个构想，这部分实验可以作为未来工作的参考。

无线网络中的一个关键因素是信号的传递，它会直接影响到信息转发的时间延迟。图 2 显示了信号传递的基本过程，可以得出时间延迟公式如下：

$$D_{\text{handoff}} = D_{\text{dhcp}} + D_{\text{更新}} \quad (1)$$

由于SIP和HIP工作在不同的层次上，因此传递消息时的头部是不相同的，本文对信号传递的分析只是对更新信息本身内容而不包括头部的分析。在式(1)中，$D_{\text{更新}}$的大小取决于移动节点和通信节点之间的距离，也就是跳数(hop)。则 式(1)可写为

$$D_{\text{handoff}} = D_{\text{dhcp}} + (L \times (H-1)/BW_{\text{wired}} + L/BW_{\text{wireless}} + L_{\text{wired}} + L_{\text{wireless}}) \quad (2)$$

其中，D_{dhcp}表示通过DHCP分配地址时的延迟，典型值为 1 s；$D_{\text{更新}}$表示移动节点向所要通信的节点发出更新通知的时延；BW_{wired}与BW_{wireless}分别表示有线和无线链接的带宽，通常为 100 Mb/s和 11 Mb/s; L_{wired}和L_{wireless}分别表示有线和无线链接的时延，通常为 0.5 ms和 2 ms；H表示移动节点与通信节点之间的跳数；L表示报文的长度。

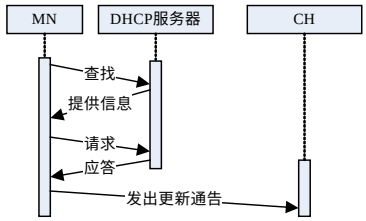

图 2 信号传递流程

图 3 为在不同策略下的信号传递时间延迟，如果以 ms 为单位很难显示出 3 种策略之间的差距，这里将时延都减去 1 s 后将再将尾数以 ms 为单位显示。可以看出 SIP 策略是最差的，而移动 IP/SIP 是最好的，HIP-SIP 次之。

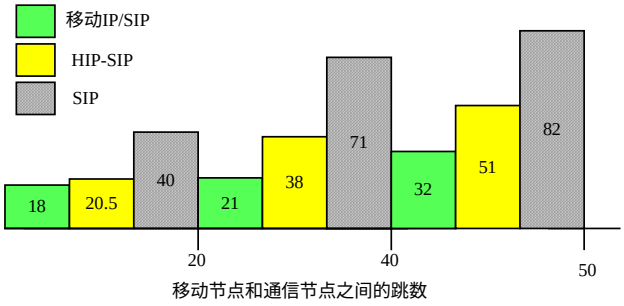

图 3 信号传递延迟

但是移动 IP/HIP 需要使用家乡代理，因此一次完整的信号发送需要 2 次图 2 的信号传递过程。而 HIP-SIP 模型只需 1 次信号传递过程。因此，一般来说 HIP-SIP 模型信号传递时延比较小。 （下转第 91 页）