移动 IPv6 通信对端绑定更新安全研究

吴开贵　谢　琪　朱郑州　王　洁　廖振岚
（重庆大学计算机学院　重庆 400044）

摘　要　本文基于新的 WTLS 证书和 ECC 加密算法，使用 WAP 中的 WTLS 协议来提供 MN 和 CN 之间通信的保密性、数据整合以及鉴权，保证了 MN 和 CN 之间绑定更新的安全，从而较好地解决了移动 IPv6 环境下的安全绑定更新问题。论文最后在 OMNET++平台上对该方法进行仿真实验，结果表明该方法在时间性能上具有一定的优势。

关键词　移动 IPv6，绑定更新，WTLS，OMNeT++仿真平台，ECC

Research on Security of Binding Update to Correspond Nodes in Mobile IPv6

WU Kai-Gui　XIE Qi　ZHU Zheng-Zhou　WANG Jie　LIAO Zhen-Lan
(College of Computer Science and Engineering, Chongqing University, Chongqing 400044)

Abstract　Based on the new WTLS certificates, ECC and the WTLS protocol in WAP, a new method is designed to provide privacy, data integrity, and authentication between MN and CN, and it provides the security of Binding Update between MN and CN, and it solves the problem of security binding update in mobile IPv6. This method is simulated on the OMNET++, and its performance is excellent.

Keywords　Mobile IPv6, Binding updates, WTLS, Simulation platform, ECC

在移动 IPv6(Mobile IPv6，MIPv6)中，移动节点(Mobile Node，MN)的位置不固定，为了保证 MN 在移动通信中的正常进行，就要求 MN 不断向家乡代理(Home Agent，HA)和通信对端(Correspondent Node，CN)分别发送绑定更新，以告知自己当前所处的位置，这就产生了很多安全问题。

本文分析移动 IPv6 中的 MN 身份认证过程存在的问题，提出了通过使用无线应用协议(Wireless Application Protocol，WAP)中的 WTLS 协议，结合无线传输层安全(Wireless Transport Layer Security，WTLS)证书和椭圆曲线加密算法(Elliptic Curve Cryptography，ECC)，来保护 MN 的绑定过程的新方法。

1　移动 IPv6MN 身份认证过程存在的问题

移动 IPv6 中有三个重要的实体：(1)MN：指移动 IPv6 中能够从一个链路的连接点移动到另一个连接点，同时仍能通过其家乡地址访问的节点。(2)CN：指所有与 MN 通信的节点，它可以是静止或移动的。(3)HA：指 MN 家乡链路上的一个路由器，允许 MN 向其注册当前的转交地址，并且当 MN 离开家乡时，截取其家乡链路上目的地址是 MN 家乡地址的分组，通过隧道转发到 MN 注册的转交地址[1]。

移动 IPv6 在提供移动性支持的同时，也面临更多的安全问题，主要来自绑定的管理机制与移动 IPv6 的路由优化机制。绑定更新相关的安全威胁主要有：(1)攻击者伪造绑定更新中的转交地址；(2)恶意 MN 伪造绑定更新，声称自己拥有受害者家乡地址；(3)攻击者把重定向的分组转发到 MN，扮演 MN 和 CN 之间的中间人，从而窃听 MN 和 CN 的通信；(4)攻击者重放 MN 曾经发送过的绑定更新，也可能破坏 MN 当前的通信。移动 IPv6 中采用返回路径可达过程(Return Routability Procedure，RRP)来加强 CNBU 的保护，但仍存在许多问题。

2　返回路径可达过程的优点与不足

返回路径可达过程由 HoTI 和 HoT 消息对、CoTI 和 CoT 消息对等 4 条消息组成。RRP 的主要优势是限制了潜在攻击者对 Internet 上特定路径的接入，并拒绝了从 Internet 上任何其他位置所发送的伪造的绑定更新，但这种方案存在中间人攻击的威胁。MN 发送的 BU，无论是给 HA 还是给 CN，如果不采取一定的安全措施，就会带来安全问题。如果恶意节点截获 MN 发送过来的 CoTI 消息，用虚假的转交地址伪造新的 CoTI 消息发送给 CN 进行绑定更新，而 CN 没有相应的认证机制，恶意节点可以得到基于虚假转交地址的应答和相应的转交密钥生成令牌。同时，由于在 HA 和 CN 之间没有相应的加密措施，恶意节点可以监听这两点之间的通信，从而得到家乡密钥生成令牌，并用这两个令牌生成绑定所需的密钥发送给黑客主机。拥有虚假地址的黑客主机利用这个密钥来发送假的绑定更新，从而使本应发送到 MN 的数据包发送给黑客主机。所以有必要对 RRP 进行改进，本文引入 WTLS 来保证信息传输的安全。

3　使用 WAP 中的 WTLS 来提供 MN 和 CN 之间通信的保密性、数据整合以及鉴权

3.1　WAP 中的 WTLS 简介

WAP 是一个使用无线设备来为无线用户提供信息的访问和交互理念的全球开放规范[2]。与通常的 PC 相比，无线终端用户设备的 CPU 功能弱，存储容量少，显示窗口小，功耗受限制并且输入设备多样化；无线网络具有窄带宽、多延时、

吴开贵　副教授，硕士生导师，主要研究方向：网络信息安全，神经网络；谢　琪　硕士研究生，研究方向：网络安全，移动 IP；朱郑州　讲师，博士生，主要研究方向：现代远程教育，网格计算；王　洁　硕士研究生，研究方向：网络安全；廖振岚　硕士研究生，研究方向：网络安全。

差连接稳定性、少可扩展的可用性等缺点[3]，要求 WAP 设备和软件必须高效，因此 WAP 协议与基于 Web 的协议相比效率要求更高。简单地说，WAP 提供了一种更快、更安全、更有效的无线网络通信方法。

WAP 安全结构由 WTLS、无线识别模块(WAPIdentity-Module，WIM)、无线公开密钥体系(Wireless Public Key Infrastructure，WPKI)和 WMLScript 四部分组成，每个部分在实现无线网络应用的安全中起着不同的作用。其中 WTLS 协议以及有线环境下处于传输层上的安全协议 TLS，SSL，TCP/IP 组成了安全协议平台。WTLS 保证移动终端和 WAP 网关之间的无线安全传输，SSL/TLS 保证 WAP 网关和网络服务器之间的有线安全传输。

WTLS 主要目的是在两个进行通信的应用间提供保密性、数据整合以及鉴权。WTLS 对窄带的、有相对较长反应时间的承载网络是最优的，它支持三种类别的安全服务[4]。

Class 1：使用交换的公共密钥建立安全传输，使用对称加密算法加密、解密数据、检查数据完整性，建立安全通信的通道，为无线用户和 WAP 网关之间提供可靠、完整的数据交换。

Class 2：除完成 Class 1 的功能外还可以交换服务器证书，完成对服务器的鉴别。

Class 3：除完成 Class 2 的功能外还可以交换客户证书，在服务器鉴别的基础上，增加了无线用户的识别。

从 Class 1 到 Class 3 安全级别逐级升高，可根据实际应用在握手协商的过程中由客户端与服务器端共同协商，选定一个相应安全服务类别。

3.2 WTLS 证书及 ECC 算法简介

WTLS 证书是标准 PKI 证书的子集，它可与标准 PKI 交互，但实现代码简洁紧凑，易于 WAP 客户进行初始化。由于使用 ECC 算法，与采用 RSA 算法的证书相比，所需存储空间可减少 100 字节左右[5]。

无论是运算速度，还是资源的占用，传统的签名摘要算法在无线环境中是不可行的。ECC 是目前认为最有效的算法，最适合无线应用环境[6]。与其它签名方案相比，ECC 的密钥具有安全性能更高、计算量小、处理速度快、存储空间占用小和带宽要求低的特点，更适合于无线环境中的安全。

3.3 WTLS 在 MN 和 CN 之间身份认证的具体应用

移动 IPv6 中 CN 的绑定更新所面临的威胁，实质是 MN 和 CN 不能进行身份的相互鉴别，而在 WTLS 中能够提供端到端通信的保密性、数据整合以及鉴权。本文对 WTLS 协议做一定修改，使得在移动 IPv6 中能解决对 CN 的绑定过程中所遇到的安全问题。

假定 MN 和 CN 都从认证中心 CA(CA 可由家乡代理或其他固定的节点担当)获得 WTLS 证书，当 MN 移动时，它同时往 HA 和 CN 发送绑定更新，往 HA 发送绑定更新的方式与 RRP 过程相同，往 CN 发送绑定更新的过程采用 WTLS 协议认证方式来进行。

如图 1 所示，把 WTLS 中的 Client 作为 MN，把 Server 作为 CN。(1) 如果 CN 是固定的，由于 CN 是拥有较高计算性能的固定机器，并且连接在有线网络上，因此有作为 Server 的能力。(2)如果 CN 是移动的，则把 CN 的家乡代理作为 Server。

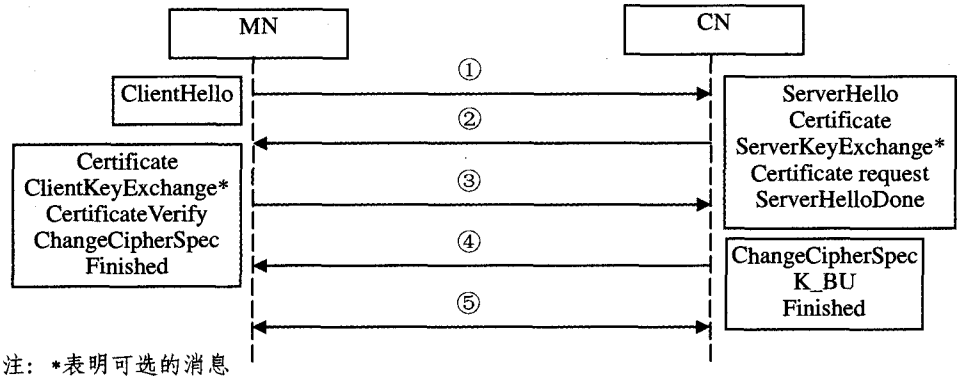

图 1 修改后 WTLS 完整的握手协议

修改后 WTLS 完整的握手协议流程如下所示：

①由 MN 发送 Client Hello 消息开始握手协议。

②CN 应答，发送 CN 自己的公钥证书和其他会话参数。例如，加密套和为这一特殊会话形成主密钥的预备密钥。在 WTLS class 3 的情况或者端到端协议版本下，CN 要求 MN 的证书来认证 MN。在这个具体应用中公钥证书采用 WTLS 证书格式，实体身份认证和密钥交换则采用 ECC。使用 WTLS class 3 安全服务类别方案，网关和服务器合并在一起作为 CN。

③MN 验证 CN 的证书并且回送 MN 自己的证书和其余的会话参数。

④CN 验证 MN 证书并发送应答消息给 MN。

⑤MN 和 CN 双方都被认证，计算会话主密钥和定义所使用的加密套。

基于 WTLS 握手协议，为防止 BU 受到反射攻击，在第④步 CN 发送给 MN 的应答消息中增加一个密钥 K_BU。

K_BU=PRF(master secret，N1)

其中 master secret 是会话主密钥，N1 是由 CN 产生的 nonce 值。密钥 K_BU 在 MN 和 CN 完成绑定过程后，撤消其有效性。

首先使用加密套和计算出的会话主密钥对 BU 报文进行 MAC 和加密，然后把加密后的 BU 报文由 MN 发往 CN。BU 报文格式如下：

BU={Src=CoA，Des=CN，HoA，Seq#，LT_BU，MAC_BU}

其中 MAC_BU=K_BU(care-of address | correspondent node address | BU)

MAC_BU 认证 BU 报文，Seq# 是检验重放攻击的序列号，而 LT_BU 是绑定的寿命。这样 MN 和 CN 完成了相互之间的身份认证，在重用会话中，WTLS 握手协议产生的主

密钥可以生成新的 K_BU 来保护 MN 对新转交地址进行绑定更新。

与 RRP 相比，在本方案中 MN 和 CN 直接通信，没有经过 HA，这是由于利用证书和私钥已经可以确定节点身份信息，不需再对节点进行家乡地址认证。

在 WTLS 中使用 ECC 验证实体身份和交换密钥，比 RSA 更能节省时间开销和减少一定字节数的传输。

MN 和 CN 是用 WTLS 协议来进行身份认证，对 WTLS 一个完整的握手协议来说，一旦会话在早期建立，当双方同意时可重用多次。在重用会话中，通信双方存储先前的会话参数，可立即使用会话 ID 和共享密钥，不需再发送证书和预备密钥，从而简化了 MN 和 CN 之间身份认证过程，节省认证时间。

4 分析和比较

在无线通信环境中，通信的安全性和性能是重点考虑的两个要素。下面分别从这两个角度具体分析本方案的特点。

4.1 安全性分析

WTLS 有两个重要的协议，握手协议和记录协议。握手协议可以提供连接的安全性：身份鉴别(本文采用双向鉴别)；协商得到的共享密钥是安全的，中间人不能够知道；协商的过程是可靠的。记录协议提供连接的安全性表现在保密性和完整性。

(1)防止中间人攻击，如果有恶意节点想冒充 MN 向 CN 发送绑定更新，就必须需要有 MN 的私钥和证书，而恶意节点不能得到 MN 的私钥，CN 对 MN 的认证就不能通过。请求被拒绝。如果有恶意节点想冒充 CN 来接受 MN 的绑定更新，同样，在 WTLS 握手协议中，恶意节点没有 CN 的私钥，MN 对 CN 的认证就不能通过，绑定失效。

(2)对绑定信息不能进行监听和篡改，WTLS 的记录协议保证了 BU 消息的保密性和完整性。

(3)防止重放攻击。在 WTLS 握手协议中的时间戳，可以降低重放带来的威胁。

(4)MN 和 CN 发送的每个数据包都是在接受对方应答后才能产生相应的回复，从而保证绑定过程的安全有序。

(5)如果恶意节点想重放以前的一个绑定请求，由于在 BU 报文中加入了 Seq＃字段，这是专门用来检测重放攻击的序列号，并且 K_BU 是随机产生的，在一次绑定更新完成后该密钥被撤消，故防止了该类攻击。

(6)防止反射攻击，如果一个合法的 MN 向 CN 提供一个虚假的转交地址来试图进行绑定，而使得 CN 往虚假地址发送大量的数据包。对位于虚假地址的数据包主机有很大的威胁。由于 CN 会往 MN 所声称的转交地址发送绑定密钥，也就是 CN 会把绑定密钥发送给虚假的转交地址，因此 MN 就不能得到绑定密钥，从而也就不能进行虚假地址的绑定。

从以上分析可以看出，该方案的身份认证方式是可靠的。

4.2 性能分析

移动 IPv6 在性能方面主要考虑的是通信所带来的时间开销。本方案分析的对象是从 MN 发送 ClientHello 开始身份认证到 CN 接受绑定更新所花的时间。

在 RRP 中，尽管 HoTI 和 CoTI 同时发出，但它们却是经过 HA 转发的，增加了时间开销。本文使用适合无线环境下通信的更小、更简化的 WTLS 证书，并使用 ECC 算法，与采用 RSA 算法的证书相比，所需存储空间可进一步减少 100 字节左右。此外 MN 和 CN 之间直接进行通信，没有经过 HA，节省了时间开销。

作者在 OMNET＋＋(对象导向式模块化离散式建模仿真器)平台上，对该方法进行了仿真实验，OMNET＋＋是一个开放资源仿真包，最初用于通信网络及分布式系统的仿真，可运行在 Unix 和 Windows 环境下。实验结果表明该方法在时间性能上具有一定的优势。

在仿真过程中，设置网络延时为 0.03s，数据包传输时间由每次发送数据包的大小来决定，数据包在 MN 和 CN 两个端点的处理时间，由它们所处理的数据和各自处理速率共同决定(这里把 MN 的处理速率设置为 1MBps，CN 处理速率设为 30KBps)。在本仿真环境中，数据包在协议上层或下层传递的延迟用一个统一分配的随机产生器产生(uniform(0.05，0.1))。使用完整的 WTLS 握手协议来实现 MN 和 CN 的绑定更新，其运行结果如图 2 所示。

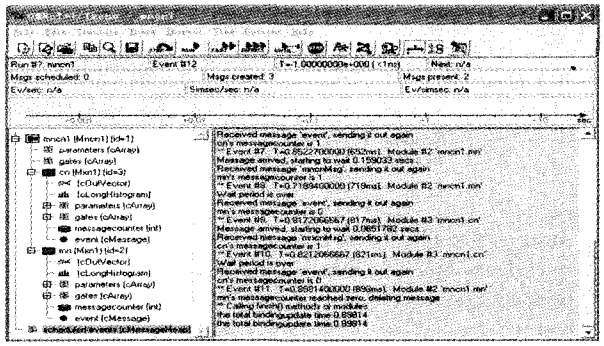

图 2 运行结果图

从图 2 中可看出一个完整绑定更新过程所花的模拟时间为 0.89814s。在此基础上重用已有的会话，实现绑定更新，可得到如表 1 所示的一系列数据。

表 1 每次绑定更新时间的平均值

重用会话的次数	绑定更新的平均值
1	0.826205s
2	0.802227s
9	0.768657s
19	0.761463s

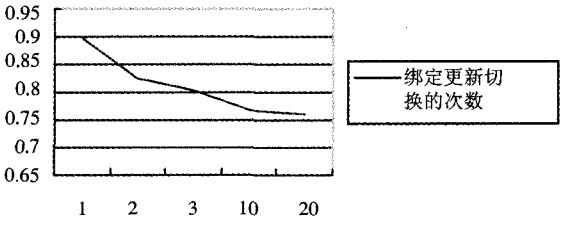

图 3 数据分析图

从图 3 中可看出：切换次数越多，每次绑定更新平均所花的时间呈现出一个递减趋势。由此可看出在本方案中对 BU 切换频率高的用户来说具有很好的时间效率。

结论与展望 本文使用基于新的 WTLS 证书和 ECC 算法，通过使用 WAP 中的 WTLS 协议来提供 MN 和 CN 之间通信的保密性、数据整合以及鉴权，改进了 MN 和 CN 之间的认证机制。该解决方案保证了 MN 和 CN 之间的安全，较好地解决了移动 IPv6 环境下的安全绑定更新问题。同时也具有较好的时间性能，从而能有效地保证通信的安全性和服务质量。

(下转第 50 页)

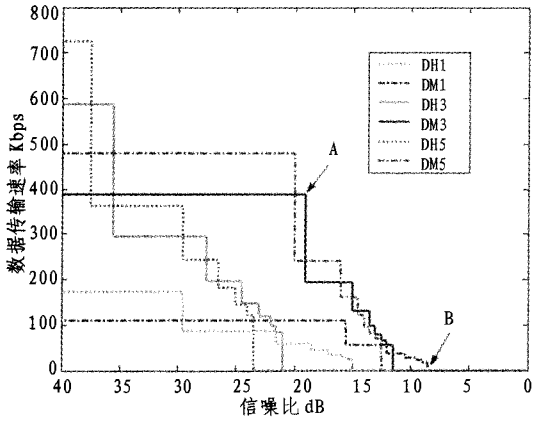

图 2　达到 99%的广播成功率，蓝牙各个数据分组的最大传输吞吐量

表 2　各种信噪比下，达到 99%的广播成功率并且要实现最大传输吞吐量应选用的数据分组形式和重传次数

信噪比(dB)	分组类型	重传次数	传输速率(Kbps)
37.5<SNR	DH5	1	723.2
[35.5,37.5]	DH3	1	585.6
[20,35.5]	DM5	1	477.8
[19,20]	DM3	1	387.2
[16,19]	DM5	2	238.9
[15,16]	DM3	2	193.6
[14.5,15]	DM5	3	159.3
[13.5,14.5]	DM3	3	129.1
[13,13.5]	DM3	4	96.8
[12.5,13]	DM3	5	77.4
[12,12.5]	DM3	6	64.5
[11.5,12]	DM3	7	55.3
[10.5,11.5]	DM1	3	36.2
[9.5,10.5]	DM1	4	27.2
[9,9.5]	DM1	5	21.8
[8.5,9]	DM1	6	18.1

表 2 表示在不同的信噪比下，要达到 99%的广播成功率，蓝牙数据分组选择策略，给出了分组类型切换的信噪比门限值，并且给出了要达到最佳性能的分组重传次数和最大吞吐量。

图 3 显示了要达到 99%的广播成功率，采用自适应分组选择策略时，蓝牙最好的广播性能。可见，在不同的信噪比条件下，选择合适的数据分组格式，能够取得一个最好的广播性能。

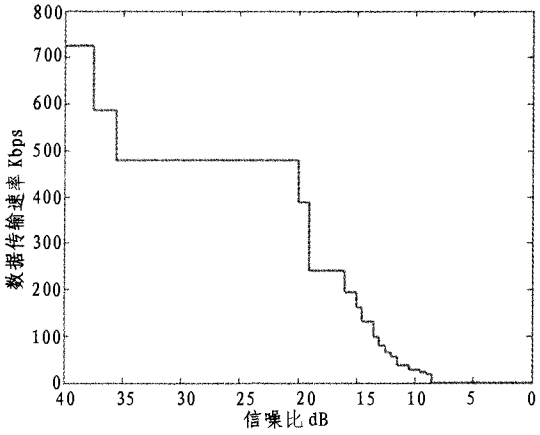

图 3　采用自适应分组选择策略的广播数据传输性能

结论　本文对蓝牙规范的 ACL 数据分组特性及其抗干扰方式进行了研究，以加性高斯白噪声信道(AWGN)为信道模型，分析了蓝牙数据分组重传概率与位错误率的关系，推导出了各个数据分组类型在不同的信噪比下要达到最好的广播性能需要的重传次数，并且给出了实现最大的传输吞吐量的分组选择策略。利用这种自适应分组选择策略能够明显改善不同信噪比信道下的蓝牙广播数据传输性能。

参 考 文 献

1　SIG. Specification of the Bluetooth System. Core, Version 1.2. http://www.bluetooth.com, 2004

2　Stranne A, Edfors O, Molin B A. Thoughout Dependence on Packet Length in Bluetooth Network. RVK 05, Linkoping, Sweden, June 2005

3　Matthew C. Valenti Lane dept. of Comp. Sci. & Elect. Eng. West Virginia University Morgantown. On the throughput of Bluetooth data transmissions. In: IEEE Wireless Communications and Networking Conference [C], 2002. 119～123

4　Golmie N, Van Dyck R E, Soltanian A. Interference of Bluetooth and IEEE 802.11: Simulation Modeling and Performance Evaluation. In: Proceedings of the Fourth ACM International Workshop on Modeling, Analysis, and Simulation of Wireless and Mobile Systems, MSWIM'01, Rome, Italy, July 2001

5　Pasolini G, Verdone R. Analytical Evaluation of Throughput for a Bluetooth Piconet with MAC Level Link Adaptation. Special Issue on WLAN Optimization at the MAC and Network Levels. Journal On Special Topics In Mobile Networking And Applications (KLUWER)

6　Kleinschmidt J H, Pellenz M E, Jamhour E. Bluetooth network performance in Nakagami-m fading channels. In: IFIP TC6 International Conference on Mobile and Wireless Communications Networks, Singapore, October 2003

7　Proakis J. Digital Communications. New York, NY: McGraw Hill, Inc., fourth ed, 2001

(上接第 47 页)

下一步研究方向：(1)WTLS 证书的具体实现(如密钥的产生，证书签发，密钥使用，证书撤消链表的管理等等)还需要进一步完善。(2)用程序来实现认证的一部分功能。(3)在 WTLS 握手协议第四条消息中，新增的一个 K_BU 绑定密钥可使用组合密钥来产生，通信双方都拥有一个密钥池，传送密钥时只需发送索引不用再发送密钥，从而又可以减少 MN 和 CN 之间数据的传输。

参 考 文 献

1　孙利民，阚志刚，郑健平，等. 移动 IP 技术[M]. 北京：电子工业出版社，2003

2　Andersson M, Bergström K. WAP – a study of the concept for mobile service provisioning

3　Wireless Application Protocol Architecture Specification. http://www.wapforum.org

4　何世华，杨磊，秦永华. 对 WAP 中端到端技术的安全研究. 九江学院学报，2005，1：11～14

5　Härnetvaara V. Certificate Management in Mobile Devices: [M. Sc. Thesis]. Tampere University of Department of Computer and Information Sciences, 2002

6　王治国，肖德贵. 基于无线 PKI 的微型证书的分析与实现. 科学技术与工程，2006，6(3)：278～282