计算机科学1999Vol. 26№. 9

无线接入宽带网中的安全通信

Secure Communications in the Wireless Access Broadband Networks

刘晓宇　陈明奇　吴伟陵
（北京邮电大学信息工程系　北京 100876）

Abstract　Based on the architecture of the wireless access broadband network we proposed, this paper studies the secure communications in the wireless link and proposes a new secure ATM architecture.

Keywords　Wireless access broadband network, ATM network, Secure communication

1　引言

移动通信在过去二十年中获得了飞速发展，已成为现代通信中一个极为重要的领域。国际互连网的发展以及随之而来的网络信息时代要求移动通信系统能够提供多媒体业务，因此，从九十年代中期开始，人们致力于第三代移动通信系统的开发和研究，以提供移动多媒体通信能力并获得与固定通信网相当的业务质量。

与此同时，ATM 技术作为传递多媒体业务的解决方案在主干网中已经得到采用，如何将 ATM 扩展到移动通信网，实现基于 QoS 的多媒体网络应用在 ATM 主干网和移动用户终端之间的无缝连接，已经逐渐成为人们的研究课题。与传统的无线接入网络结构不同，多媒体业务的传输特性对无线接入宽带网络体系结构提出了许多新的要求。

无线接入宽带网为用户提供了方便，高效的多媒体服务，吸引了用户将许多重要的信息放在宽带移动通信网上传输，因此，如何保护这些通信内容的安全，已引起了人们的高度重视。本文主要讨论在我们所提出的无线接入宽带网的体系结构中建立安全机制，将安全服务集成在该网络体系中以保证多媒体业务的通信安全。

2　宽带移动接入的网络结构

本节中我们提供一种空中接口采用 CDMA 方式的无线接入宽带网结构，以适应多媒体业务的要求。

第一代、第二代移动通信系统以提供话音业务为主，基站通过移动交换中心连接到公用电话交换网，控制、数据库和管理功能分布在基站和移动交换中心。这种网络结构以电路交换为基础，明显不能适应第三代移动通信的要求。ATM 技术使多媒体业务在同一个宽带网络中传输成为可能，因此，九十年代中期以来，人们提出了多种宽带移动接入方案[1~4]，力求实现移动通信网和 ATM 主干网的有效结合。

考虑无线接入宽带网时，通常有两种方式可供选择：

第一种方式是移动通信网与 ATM 主干网相互独立，它们之间通过一个网关（IWU）相互连接，在互连组网单元中对两个网络的业务和协议进行处理和转换。文[1]、[3]提出的宽带无线接入网结构就属于这种方式。这种相对独立的网络结构的优点是系统设计具有高度的灵活性。空中接口的设计可以不考虑固定宽带网对它的约束，例如可以使用更低速率的声码器提高无线频谱的利用率，保证每个用户的业务质量。同时，这种宽带接入方式对 ATM 主干网的影响也较小，无需修改 NNI 接口协议来支持无线通信中的移动业务管理。其缺点是网络的重复建设不够经济，另外由一个接口处理的控制复杂度大为增加。

第二种方式是两个网络实现部分资源共享，这是一种更为经济的方式。文[2]、[4]提出的网络结构属于这种方式，这种宽带接入结构对业务和协议的共享可以视为 ATM 主干网的移动扩展，但是，这样一个集成网络必须同时满足固定用户和移动用户的要求，对两个网络的设计均产生一定的影响，提出了

新的要求。

总之，在无线接入宽带网中，传统的基站收发信机，基站控制器，和移动交换中心各自作为独立实体的概念被重新加以考虑，功能分配趋向于引入智能网的概念，控制与交换相分离，以便于系统实现。我们的原则是采用第三代移动通信的空中接口标准，通过 ATM 网络接口单元进行信息处理，对 ATM 主干网的业务结点加以改造以支持移动性管理。下面就图1所示的无线接入宽带网的各个功能实体作进一步的说明。

2.1 空中接口

第三代移动通信系统的空中接口物理层采用 CDMA 还是 TDMA 方式，其各自的优缺点已经有大量的论文进行了讨论并且进行了实验系统的开发。尽管从性能角度出发，两者没有根本差别，但从多媒体混合业务的传输角度看，CDMA 具有更大的灵活性。此外，在多速率混合业务的情况下，CDMA 能够获得比 TDMA 更高的频谱利用效率，因此，CDMA 在第三代移动通信系统中得到采用。

文[2]、[4]提出的宽带无线接入方案中，空中接口第二层采用 ATM 信元传输。ATM 技术的设计背景之一是高信息率(Gbps)和低误码率(信元损失率 10^{-9})。与此相反，无线链路传输速率相对较低(2Mbps)并且误码率相对较高(典型误码率 10^{-3})。除此之外，多径效应、阴影效应以及终端的移动性导致无线链路严重地衰落。无线链路的这种特性对固定宽带通信网所定义的业务的分组损失率、延时和抖动特性有直接的影响。为此，无线链路需要有更复杂的差错控制，这会带来额外的开销，降低传输效率，其结果与 ATM 的初衷发生了冲突。因此，图1中的宽带移动接入方案直接采用第三代移动通信基于 CDMA 的空中接口，这是一种经济而现实的方式。

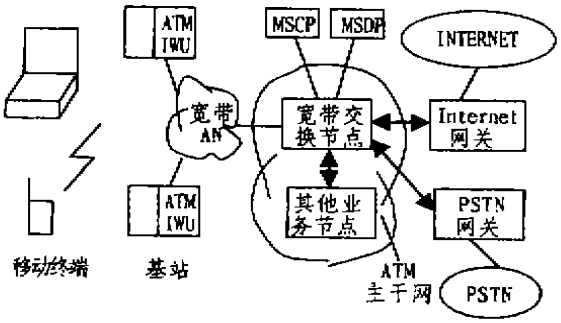

图1 无线接入宽带网的体系结构

2.2 ATM 网络接口单元(IWU)

ATM 网络接口单元是移动通信网与 ATM 主干网的接口，移动通信网的集成对 ATM 的协议产生许多影响，本文仅就两个重要问题加以讨论。

ATM 网络接口单元在空中接口的信道与 ATM 网络传输中的虚电路之间作出映射，ATM 适配层将提供 CDMA 的帧与 ATM 信元之间的转换，并适当分配信头标识符(VCI 和 VPI)。现有的 AAL 协议在支持 CDMA 空中接口的高效率、低时延、可变速率的低比特话音业务流方面有很大缺陷。为满足对时延敏感，可变长度的短分组的需要，ITU-T 提出了 AAL2协议。有关 AAL2的 SSCS 部分，还有待进一步研究。

另外一个重要问题是呼叫接入控制和资源分配问题。在无线接入宽带网中的 QoS 控制必须同时考虑有线资源和无线资源，无线接入宽带网还必须将无线链路的传输特性和移动特性考虑进去，因为一个移动终端在呼叫建立时提供的连接并没有考虑切换后一个新的连接在有线网中是否拥有足够的资源分配。因此，在 ATM 网络接口单元中，我们需要提供新的呼叫接入控制算法。

2.3 宽带接入网(AN)

宽带接入网的目的是将用户网络接口(UNI)的信令和数据流以最有效的方式复用，连接到宽带业务节点上。宽带接入网的主要功能是集中，对信令作尽可能透明的传输，而将移动管理的功能放在宽带业务节点上处理。宽带接入网通过 V_B 接口与宽带业务节点相连接。

2.4 宽带业务节点

宽带业务节点由宽带交换节点、移动业务控制点(MSCP)和移动业务数据点(MSDP)组成。移动业务控制点和移动业务数据点分别完成智能网的功能实体 SCP 和 SDP 的功能。采用智能网的概念将宽带业务节点的交换和控制功能相分离的目的是可以将业务节点对移动性功能的支持以模块化的方式实现，从而减小对原有的 ATM 主干网体系结构的影响。移动管理功能如位置更新和切换功能可以作为新业务加载，与修改信令协议相比实现方式更加简单。

上文讨论的新的网络体系结构将第三代移动通信系统与基于 ATM 的 B-ISDN 相结合，力图实现多媒体业务在宽带信息网中的无缝接入。

3 无线接入宽带网络的安全结构

无线接入宽带网络中一个合理的安全体系结构

应满足两个基本要求：

·提供一个集成的，可配置的安全功能服务和机制以灵活适应不同类型的业务要求。

·安全服务及功能应对用户和应用程序提供一个透明的安全应用接口。

3.1 无线链路中的安全服务

尽管与模拟通信系统相比，CDMA 调制方式使码片更难被截获和破译，但从系统安全看，这是远远不够的。移动通信系统的安全服务应满足如下要求[5]：

(1)通信保密。需要保护的信息包括：呼叫建立信息；用户的话音和数据；用户的位置信息。在漫游时防止入侵者伪装成合法用户进行欺骗；用户的身份标识，防止对用户的呼叫模式和流量参数进行分析。

(2)防止盗用。安全机制应防止个人终端被复制(cloning)。

(3)满足移动性的要求。安全系统在漫游时，用户的安全信息在不同的业务提供者之间要求能够实时切换；认证过程的实时性也必须得到满足，对切换过程的影响要尽可能小。此外，无线链路的衰落效应和噪声干扰不能影响安全系统的可靠性。

无线系统中的安全问题要通过设备供应商对系统的改进，政府部门加强监管力度以及提高用户和运营商的安全意识等等综合措施，以提高系统的安全性。我们仅从系统设计角度看，通常有三种方式实现无线系统中的安全服务：密钥系统、认证系统、多层加密。

当前移动通信系统实用的安全服务通过一个认证和密钥分配协议(AKA)来实现。主要有两大类：基于 GSM 的 AKA 和基于 IS-41的 AKA。它们的实现方式非常相似，可用一个通用的接入控制模型来描述[6]，下面就以此模型分三个部分对两种 AKA 作简要说明：

(1)为用户分配证书并在网络中注册。GSM 型安全系统给用户一个 SIM 卡，内含128位的唯一的一个号码，称为"Ki"，IS-41型系统首先给用户一个64位的安全号码，称为"A-Key"。然后由本地业务提供者利用"A-Key"和特定的安全协议生成一个共享安全数据(SSD)。这两类系统的共同特点是无论"Ki"还是"A-Key"都只能存储在本地网络(Home Network)中。

(2)接入控制。由于终端的移动性，向其提供服务的可能不是本地网络，而是另外的业务提供者(Visited Network)。GSM 系统中，归属局(HLR)向拜访局(VLR)以"三元组"的形式提供三个安全参数(RAND、SRES、Kc)，IS-41系统由 HLR 向 VLR 提供 SSD，用于进行认证。

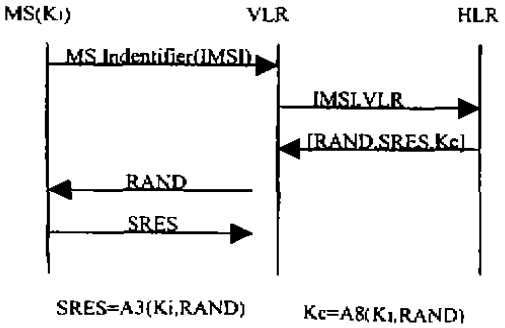

图2 GSM 型安全系统的 AKA

(3)认证和私钥分配。通过 AKA 协议，系统保证用户获得安全服务。这两类安全系统都利用"Challege/Response"协议进行认证和生成密钥。

上述过程在图2中作了说明。由于篇幅有限，仅以 GSM 为例，IS-41安全系统与此类似。这两类系统同属私钥安全系统，由于用户的移动性，系统需要通过网络传送用户的安全信息，而且信息传送以明文形式进行，因此，它们都容易遭到来自固定网络中的攻击。

为了克服这个缺陷，人们引入了公钥加密的概念，提出"公钥/私钥"混合加密系统，其具体过程可见文[6]。在认证过程中它可以直接在移动终端注册时完成认证过程，避免安全信息在网络中的传输。但目前实用的系统尚未采用这种方式，例如 PCS-1900 采用 GSM 型安全系统，而 WCDMA 空中接口采用 IS-41型安全系统。

如上文所述，目前无线链路中的安全服务是建立在固定网的安全性的基础上。因此，考虑图1中的无线接入宽带网的安全问题必须保证 ATM 网络的安全性。下面我们将就这一问题作详细讨论。

3.2 ATM 网络中的安全服务

在下面的讨论中，我们假定无线接入宽带网络(图1)中的空中接口是安全的，而在 ATM 网络内部则存在可能的入侵者试图进行主动或被动的攻击。ATM 网络所面临的安全风险包括：信息泄漏；信息在传输过程中被进行了非法操作；假冒合法的网络实体；拒绝使用资源等等。我们所讨论的无线接入宽带网中 ATM 网部分应提供下列安全服务[7,8]：

1)实体认证：建立一个连接的双方的相互认证，

防止假冒攻击。

2)连接的可靠性:保护一次连接中的所有用户数据,防止由窃听和网络的寻径错误而导致的信息泄漏。

3)连接的完整性:监测对用户数据的非法改动,防止对用户数据的修改,插入、删除和重传等主动攻击。

4)不可否认:是用户无法否认自己在网络上所作的一切,通过对 hash 函数产生的信息摘要而实现。

5)存取控制:控制不同用户及应用程序对资源对象的存取及操作,防止用户超越自己的存取权限,进行不应该有的访问和操作。

6)安全审计:在安全日志中记录所有与系统安全相关事件,这对安全系统的维护,及发现入侵者都很有帮助。

在 ATM 网络中安全服务的实现必须考虑到下面要求:安全服务必须是面向连接的;安全服务应与现有的 ATM 网络结构实现无缝连接;安全服务必须保证 ATM 网络服务的 QoS,这要求所采用的密码技术和安全协议必须尽可能简单而有效。

在 ATM 网络协议参考模型中的物理层、AAL 层或者更高层上实现安全服务均是可行的,下面就对在不同层次上的实现进行讨论[7,8]。

1. 在物理层提供数据加密

在物理层上的加密可保护所有在物理链路上传输的数据,其优点是:对上层协议透明,也就不依赖于任何特定的网络结构;可有效地防止入侵者进行业务流量分析,还可抵御某些类型的拒绝服务;如果加密是在每条链路上独立进行,并且不同的链路采用不同的加密密钥,那么一条链路上的失误不影响其他链路上的信息安全;不影响网络数据传输的有效频宽,但技术上要求有连续的密钥流。其主要缺点在于:数据在网络链路上是加密的,在接入交换节点之前必须解密数据,以提取出信元中的 VPI、VCI 来,所以,必须要求中间交换节点内部是安全的;为了维护中间节点的安全性,除了一次性的加密硬件和安全物理环境开销外,还有许多运行过程中的维护费用,这些费用大大增加了成本。

2. 在 ATM 层提供信元加密

在 ATM 层提供信元加密,加密时仅加密用户数据,即信元净荷部分,信头仍以明文形式出现,接入中间交换节点时无需进行解密。ATM 层的信元可以避免由于信元在交换节点内部以明文形式出现而带来的安全隐患。这种加密最简单的实现形式是对所有的信息流都采用同一密钥,缺点是缺乏灵活性及存在着潜在的安全性问题。改进的方法是对每一虚通道(VC)使用唯一的密钥,但是由于穿过 LAN/WAN 边界的信元地址信息是不可预测的,因此,密钥的捷变能力是必须的,ATM 层上的信元加密算法对实时性要求很高。

3 在 AAL 层及其上层提供安全服务

在 AAL 层或在其上层提供安全服务可为复用同一个 VC 的不同连接提供相应的 QoS 保护,但实现代价一般要比在底层实现要多出许多。通常,在一个典型的企业网络内并存着不同的传输协议或 IP 协议,因此,保护在 ATM 网络上的所有信息意味着所提供的安全性必须能在所有的传输协议或 IP 协议上实现。

3.3 ATM 网的安全协议结构

目前,针对 ATM 网络的安全协议结构,文[7,8]中已作了初步探讨。本文针对图1中的 ATM 网提出的安全协议结构如图3所示。我们把 AAL 层中有关实现信令和数据安全的子层称为数据流安全层(DSSL—Data Stream Security Layer)。

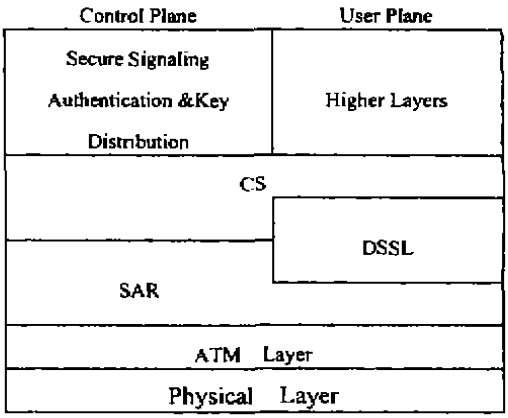

图3 ATM 的安全协议结构

我们所提出的安全协议结构中把 DSSL 放在 AAL 层中的 CS 和 SAR 中间,其优点是:

·DSSL 的存在和操作对其上层和下层都是透明的,它作为 CS 和 SAR 的补充功能,提供对数据的保护。

·SAR 可接受可变长度服务数据单元(SDUs),DSSL 数据单元中由 DSSL 导致的数据扩张可直接交给 SAR 去处理。

文[7]中的 ATM 安全协议结构中完成类似功

能的安全子层 Data Protect Layer(DPL)是放在 CS 下面的 SAR 中，文[8]中的 ATM 安全协议结构中的安全子层 Security Layers 是放在 SAR 子层和 ATM 层之间。本文的 DSSL 与 DPL 相比，DSSL 在 CS 和 SAR 之间，CS 对来自高层的不同业务接入点的业务进行处理，其具体功能与用户业务类型相关。因此，DSSL 比 DPL 提供更加灵活的多媒体业务的安全服务。DSSL 与 SL 相比，SL 在 ATM 层中实现 ATM 信头加密，会导致类似物理层加密带来的缺陷。而 DSSL 仅修改 AAL 层协议，减少了对现有 ATM 协议的修改，简化了安全结构的实现。此外，SL 层在固定大小的 SAR-PDU 上进行加密，必须采用无数据扩张的加密算法，而 DSSL 则无此限制，可根据不同业务的特点和不同用户的要求任意选用不同的加密算法。

另外，DPL 和 SL 仅考虑了终端系统与 ATM 交换节点通过 UNI 节点的相互认证，并没有考虑 ATM 网络中交换节点通过 NNI 进行相互认证的情况，这是其结构中的安全隐患。本文中的安全结构对此作了全面考虑，

连接的可靠性，连接的完整性，存取控制和安全审计等具体安全服务功能的实现在本文中限于篇幅就不再一一详细讨论。由于认证和密钥交换是安全服务的基础，两者是紧密联系的，具体通信内容的会话密钥的交换往往是认证过程的一部分。因此，下一节中我们将详细讨论我们提出的 ATM 安全协议中的认证及密钥交换问题。

4 ATM 网络中的认证和密钥交换

ATM 网络中认证的目的在于防止假冒攻击，确信对方是要与之建立连接或交换信息的对象。密码学中有许多认证协议，如基于 DES 的 Kerberos 系统是与安全认证服务器紧密相连的认证软件，是远程认证的事实上的标准；基于公钥加密系统的 X.509认证标准则是 ITU 的建议标准，此外，还有一些基于 Diffie-Hellman 协议的认证标准。

在 ATM 网络中交换密钥，特别是对安全性要求很高的环境中，安全系统并不信任终端或其他网络元素，这意味着建立连接时在呼叫连接和连接确认之间必须建立密钥交换机制，而且此过程应是透明的。

建立对呼叫透明的安全密钥分配协议方案和建立点到点连接的双方的相互认证分别见文[7]和[9]，我们着重讨论建立中间交换节点之间的安全密钥分配和相互认证。

ATM 中间节点的相互认证可基于 ATM 局间信令功能来完成。ITU-T 的 Q.2764介绍了建立和终止网络连接的基本信令处理，这适用于各种类型的交换。我们所讨论的基于 X.509协议的 ATM 网络的中间交换机 A，B 之间的相互认证及密钥交换是通过交换下列两个信息而完成的：

$A \rightarrow B$: Cert－A，$S_A\{T_A, B, E_B\{K_A\}, SQoS_A\}$

$B \rightarrow A$: Cert－B，$S_B\{T_B, A, E_A\{K_B\}, SQoS_B\}$

其中：$E_X\{D\}$：采用中间交换机 X 的公钥加密的数据流 D。Cert－A：中间交换机 X 的证书。$S_X\{D\}$：中间交换机 X 的私钥加密的数据流 D，T_X：中间交换机 X 产生的时戳，以帮助其他中间节点，检测出重传的信息。K_X：中间节点 X 产生的会话密钥，保护与 X 通信的其他中间节点之间的通信信息。$SQoS_X$：中间交换机 X 所要求或能提供的安全服务的 QoS 保护，

认证及密钥交换过程如下：

1. 主叫节点发出请求建立业务消息，除有标准的 NNI 信令参数外，还包含主叫方的安全服务参数，如：主叫方的安全识别符等。

2. 被叫中间节点如果无法满足主叫方所需的 QoS 保护或主叫方未通过认证，发回 IAR 消息，并终止接续。

3. 主叫方通过被叫中间节点的认证，而且被叫方可提供所要求的 QoS 保护，被叫方发回 IRA 消息，除有标准的 NNI 信令参数外，还包含被叫方的安全服务参数，如：被叫方的安全识别符等。

4. 如果被叫中间节点未通过主叫方节点认证或无法接受被叫方选择的 QoS 保护，则终止接续。

5. 被叫方节点通过认证且 QoS 保护协商的结果可接受，则成功地建立接续，完成中间交换节点双方的认证及密钥交换。

结论 我们提出 ATM 安全结构不仅解决了终端系统的相互认证和用户数据的安全，实现了与现行 ATM 网络的无缝连接，而且解决了 ATM 网络中间节点，相互认证及会话密钥的交换，消除了 ATM 网络中的一大安全隐患。

关于无线宽带接入网，人们正在致力于研究新的 AAL 层协议，并针对 ATM 对信道的统计复用特点研究新的切换算法。另外，有关 ATM 网络安全服务的标准化，尤其是与控制面和管理面相关的安全服务问题仍需要大量的工作来加以解决。

（参考文献共9篇，略）