第33卷 第23期 计 算 机 工 程 2007年12月
Vol.33 No.23 Computer Engineering December 2007
·开发研究与设计技术· 文章编号：1000—3428(2007)23—0270—03 文献标识码：A 中图分类号：N945.12

一种嵌入式WLAN安全系统的设计与实现

芦 伟，曾文华
（厦门大学软件学院智能信息技术福建省重点实验室，厦门 361005）

摘 要：介绍无线局域网的概念。在分析无线局域网的安全机制原理的基础上，提出无线局域网存在的安全问题，给出一种嵌入式安全系统的设计方案，该方案采用安全性更高的加密算法以及更完善的数据校验机制，对解决无线局域网中的安全问题具有一定的实用价值。
关键词：无线局域网；802.11；嵌入式

Design and Implementation of Embedded WLAN Security System

LU Wei, ZENG Wen-hua
(Intelligent Information Technology Laboratory, Software School, Xiamen University, Xiamen 361005)

【Abstract】 The paper introduces the basic concept of WLAN, and on the base of analyzing the theory of security policy, discusses the security problem of WLAN. A design of security system that is based on embedded flat is proposed, which combines encryption algorithm with higher security and advance verification policy. It is of some value in solving the security problem in WLAN.
【Key words】 wireless local area network(WLAN); 802.11; embedded

无线局域网(wireless local area network, WLAN)是利用无线技术实现快速接入以太网的技术。随着移动通信终端的处理能力不断增强，WLAN由于具有接入灵活、组网方便、能够提供较高质量的服务——通信速率能达到11Mb/s等特点，在近几年迅速普及，而WLAN的安全问题也日益引起重视。

1 WLAN的安全问题

IEEE802.11标准中定义了2种安全机制来实现WLAN中的访问控制和保密[1]。

(1)SSID(service set identifier)。是WLAN中用于客户端(client)与AP(access point)之间通信的可设置的标识。client只有拥有正确的SSID时才能与特定的AP通信。SSID在WLAN中实际起到了client与AP之间的共享密钥的作用。在WLAN中，基于SSID的身份认证是单向的，即只有AP对client进行身份鉴别，client并不能识别假冒的AP。

(2)WEP(wired equaption private)。采用对称加密方案，可配置3种模式：没有加密，40位密钥加密，128位加密。

802.11的安全问题主要表现在以下几个方面。

1.1 密钥的发布问题

802.11本身并未规定密钥如何分发，它缺少一种有效的密钥管理和分发机制。一般情况下，WEP密钥被静态地分配给客户机，密钥存储在客户机的磁盘存储器中或者存储在客户机的无线适配器的内存中。在实际应用中，密钥一般都是手工设置，并长期固定使用4个可选密钥之一。一旦客户机密钥丢失后，非正常用户就具有了访问网络的权限，这种情况下管理员并不能检测到有可能对网络安全的破坏，WLAN将无安全性可言。当管理员接到机主的报告后，必须对与丢失客户机密钥相同的其他客户机的静态密钥重新编码。

1.2 WEP的弱点

WEP对MAC层的数据加密过程很简单，WEP利用了RC4加密算法，首先将共享密钥和一个24位初始向量***IV***作为伪随机产生器(PRNG)的种子，产生一个与明文及校验和*ICV*(在WEP算法中，采用了CRC-32计算校验和)等长度的密钥序列*K*；然后密钥序列*K*与明文及其校验和进行异或运算产生密文；最后将密文连同初始向量***IV***发送给接收方。接收方接收到消息后，利用共享密钥的一份本地拷贝和接收到的***IV***产生一个与*K*完全相同的密钥序列，将其与密文异或恢复出明文；同时计算明文校验和*ICV'*，比较*ICV*和*ICV'*，以判定接收到的消息是否合法。

这种数据加密方式存在的问题是：RC4加密算法的缺陷(由于密钥是静态不变的，密钥序列的改变就由***IV***来决定)；***IV***随机产生且与加密数据一起传送，***IV***本身并未加密；密钥序列重复使用；CRC-32带来的问题等。

1.3 用户身份认证方法的缺陷

802.11标准规定了2种认证方式：开放系统认证和共享密钥认证。前者是默认的认证方法，任何移动站点都可以加入基本服务集(basic service set, BSS)，并可以与AP通信，能监听到所有未加密的数据，这种方法根本没有提供认证，无安全性可言[2]。

共享密钥认证是一种请求响应认证机制，它相对于开放系统认证方式有较高的安全系数，采用此种认证方式的STA(Station)必须实施WEP加密算法，认证过程为：AP在收到STA的请求接入信息后，发送询问信息，STA对询问信息使用共享密钥进行加密并回送给AP，AP解密并校验信息的完整性，若成功，则允许STA接入WLAN。攻击者只需截获加密前后的询问信息，将二者进行异或运算就可以得到密钥序列，然后攻击者则可以向AP发送认证请求信息，并用得

作者简介：芦 伟(1983－)，男，硕士研究生，主研方向：嵌入式系统；曾文华，教授、博士生导师
收稿日期：2007-01-31 **E-mail：**ymym_1983@hotmail.com

到的密钥序列加密询问信息，从而可以成功地通过 AP 认证，冒充合法身份接入 WLAN。

另外 802.11 缺少一种双向认证机制，AP 可以验证客户机的身份，而客户机不能验证 AP 的身份。如果一个假的 AP 被放置在无线局域网中，它可以通过“劫持”合法客户机成为拒绝访问的平台。

1.4 服务集标识符 SSID 和 MAC 地址过滤

服务集标识符 SSID 用以对网络进行访问控制，与 AP 有相同的 SSID 的客户机才允许访问 WLAN。AP 存有合法客户机的 MAC 地址列表并且拒绝 MAC 地址不在列表中的客户机接入被保护的网络。由于 SSID 和 MAC 地址很容易被窃取，因此安全性较低。

2 基于嵌入式平台的 WLAN 安全解决方案

802.11 仅仅规定了 WLAN 在 MAC 层的安全措施，由于 MAC 层不会对数据包进行分析，因此会产生很大的安全问题。解决 WLAN 的安全问题不仅要通过加强 MAC 层的安全算法以及安全协议来解决，另外还要借助于高层，完成密钥的动态分配，访问控制以及实施其他的安全策略，从而全面地保障 WLAN 安全。

2.1 WLAN 的安全方案

WLAN 安全方案是以 MAC 层安全策略，802.1x 认证和密钥分配实现的。

(1)采用安全性更高的加密算法

如前所述，WEP 采用流密码加密，但是却不能保证密钥不相关，因此不能够保证数据的机密性，这是其存在着严重的安全漏洞的主要原因。另外，明文与生成的具有一定相关性的密钥流进行简单的异或运算，不能抵御已知明文攻击。可以考虑使用 3DES(data encryption standard), IDEA (international data encryption algorithm)或者 AES(advance encryption standard)等分组加密算法[3]。如 802.11i 使用 AES＋OCB 算法来对数据进行加密。

(2)数据鉴别

WEP 中的 CRC-32 只能用于检测数据传输中由于线路问题产生的偶然差错，不能够检测出对传输数据人为的恶意窜改。对数据的完整性保护应当采用消息鉴别码，也就是带密钥的单向散列函数。可以采用 MD5 以及 SHA-1 对数据进行完整性校验[4]。

(3)认证与密钥分配

802.11 的认证是基于共享密钥的。认证的过程采用的是挑战-应答方式。这种认证方法的实施过程中存在以下问题：密钥是静态的，也就是在相当长的时间内该密钥不变(802.11b 并没有规定密钥的更新和分配方案)；认证是对设备并没有对设备的人进行认证；只有 AP 对基站而没有基站对 AP 的认证。这些原因都导致了认证的安全漏洞[5]。

文章采用的解决方法为上层采用 IEEE 802.1x 进行认证，并且在认证过程中完成密钥的更新和分配。

下面介绍 802.1x 协议。802.1x 是 IEEE 为解决基于端口的接入控制(port-based access control）而定义的一个标准[6]。

(1)802.1X 首先是一个认证协议，是一种对用户进行认证的方法和策略。

(2)802.1X 是基于端口的认证策略(这里的端口可以是一个实实在在的物理端口也可以是一个像 VLAN 一样的逻辑端口，对于无线局域网来说，一个“端口”就是一条信道)。

(3)802.1X 的认证的最终目的就是确定一个端口是否可用。对于一个端口，如果认证成功，那么就“打开”这个端口，允许所有的报文通过；如果认证不成功，就使这个端口保持“关闭”，此时只允许 802.1X 的认证报文 EAPOL(extensible authentication protocol over LAN)通过。

802.1X 的认证体系分为 3 部分：客户端(supplicant system)，认证系统(authenticator system)，认证服务器(authentication server system)。

802.1x 的认证过程如下：

(1)认证通过前，通道的状态为 unauthorized，此时只能通过 EAPOL 的 802.1X 认证报文；

(2)认证通过时，通道的状态切换为 authorized，此时从远端认证服务器可以传递来用户的信息，比如 VLAN、CAR 参数、优先级、用户的访问控制列表等；

(3)认证通过后，用户的流量接受上述参数的监管，此时该通道可以通过任何报文，注意只有认证通过后才有 DHCP 等过程；

(4)客户端(supplicant system-client)是 1 种需要接入 LAN，及享受 switch 提供服务的设备(如 PC 机)。客户端需要支持 EAPOL 协议，且端必须运行 802.1X 客户端软件，如：802.1X-complain, Windows XP 等。

2.2 系统的设计

WLAN 安全嵌入式系统是在实现 WLAN 通信的基础上增加了安全处理模块和多认务管理功能。目的是使设备能够提供安全可靠地 WLAN 通信功能，同时减轻主机的负担，并且为用户采用不同的安全机制和安全策略提供足够的空间和能力。WLAN 安全嵌入式系统的硬件结构如图 1 所示。

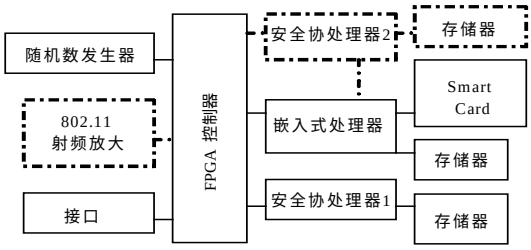

图 1 系统结构

(1)802.11 信号处理部分主要负责 802.11 信号的接收、放大、混频、基带处理以及无线 MAC 相关协议的实现。主要的器件构成如下：

1)射频放大器选用 LSL3984；

2)射频/中频转换器、混频器选用 ISL3685；

3)I/Q 调制解调混频器选用 HFA3783；

4)ISL3783B 是集成有基带信号处理器和 MAC、PCMCIA 及 USB 的芯片，可大大减小电路板的体积并减轻设计负担。

(2)嵌入式微处理器负责整个平台的任务调度、资源管理与分配。选用具有强大网络功能的 ARM920T 作为处理器。

(3)安全协议处理器负责所有与密码有关的运算和一些与密码密切相关的安全协议的实现，是运算量最大的部件。DSP 结构和指令是专门为信号处理而设计和开发的，具有很高的编译效率和执行速度。在这里，采用具有强大的计算功能和丰富的外围接口的 TITMS320C6202 作为安全协议处理器，负责所有的密码运算。

(4)对各个芯片的控制通过 FPGA(field programmable gate array)来实现。

(5)安全处理器的存储器采用 256KB*8 Flash 和 512KB*8 DDR SDRAM，用来存储应用程序和中间数据；主处理器的存储采用 512KB*8 Flash 和 16MB*64 SDRAM，用来存放嵌入式操作系统，并提供相应的可调用的地址空间。

(6)接口采用 PCMCIA, USB，满足高速数据传送的需要。

2.3 WLAN 安全嵌入式系统

该系统所能实现的安全功能如下：

(1)在安全协处理器上实现多种密码算法，包括用于数据加密的多种分组密码算法，如 DES, 3DES, IDEA 以及 AES 等；用于数字签名以及分配密钥的公开密钥算法 RSA 以及 Deffi-Hellman 算法；用于数据鉴别的 HMAC, MD5 以及 SHA 算法。

(2)在安全协处理器上实现 IKE(Internet key exchange)协议。

(3)在嵌入式操作系统中实现 VPN(virtual private network)的管理与配置。

(4)应用 SmartCard 卡完成对用户身份的鉴别。

(5)平台应用于 AP 时，利用 ARM920T 上的以太网接口与有线网络互联。AP 与有线网的网关或服务器也通过 VPN 相连接。

(6)这个平台应用于 STA 时，将 STA 配置成 VPN 的客户端，以便 STA 与 AP 之间建立有效的 VPN 连接，如图 2 所示。

(7)能够实施 802.11i 规定的 RSN(robus security Network)安全机制：

1)除了已经存在的 AES 算法之外，还可以实现 AES-OCB 算法；

2)可以加载 802.11i 规定的 MIC 算法；

3)支持密钥导出的分级结构；

4)能够加载 EAP-TLS 协议。

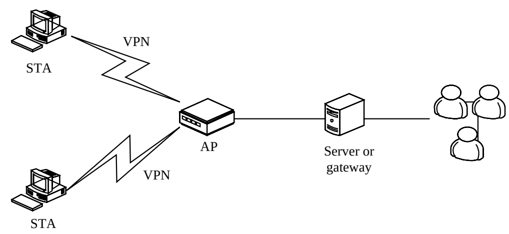

图 2 VPN 实现

3 结束语

本文分析了基于 802.11 的 WLAN 安全问题，其安全问题表现在认证、密钥管理以及数据完整性校验上。针对这些问题，根据现有的安全算法以及安全协议，提出了基于嵌入式平台的 WLAN 安全解决方案。该方案对于解决无线局域网中的安全问题具有较好的参考价值。

参考文献

1 王曼珠, 何文才, 杨亚涛. 无线局域网 IEEE802.11 的安全缺陷分析[J]. 微电子学与计算机, 2005, 22(7): 189-192.

2 魏志宏. 无线局域网安全性分析[J]. 计算机应用, 2004, 24(5): 40-43.

3 苏 鹏, 胡志远, 塔维娜, 等. 802.11WLAN 的安全缺陷及其对策[J]. 计算机工程, 2004, 30(5): 133-136.

4 King J S. An IEEE 802.11 Wirless LAN Security White Paper[EB/OL]. (2001-10-22.) http://www.techonline.com/community/tech _topic/internet/tech_paper/20667.

5 Potter B. Wireless Security's Future[M]. [S. l.]: IEEE Security and Privacy, 2003.

6 Mishra A, Arbaugh W A. An Initial Security Analysis of the IEEE 802.1x Standard[EB/OL]. (2002-02-06.) http://www.cs.umd.edu/～waa/1x.pdf.

（上接第 263 页）

参考文献

1 程少华, 吴 华. 两相邻 3 次 B 样条曲面 G^1 连续充分条件[J]. 河南师范大学学报(自然科学版), 2006, 34(3): 48-50.

2 程少华. 两邻接二次 B 样条曲面 G^1 光滑拼接的充分条件[J]. 郑州大学学报(理学版), 2006, 38(1): 33-36.

3 施锡泉, 赵 岩. 双三次 B 样条曲面的 G1 连续条件[J]. 计算机辅助设计与图形学学报, 2002, 14(7): 676-682.

4 赵庶丰. NURBS 曲面 G^1/G^2 光滑拼接方法[J]. 工程图学学报, 2003, 24(2): 105-115.

5 车翔玖, 梁学章. 两邻接NURBS曲面间的 G^2 连续条件[J]. 吉林大学学报(理学版), 2002, 40(1): 19-23.

6 袁友伟, 鄢腊梅, 郭庆平. 点云数据重构三维网格形状的新算法[J]. 计算机工程, 2005, 31(23): 4-10.

7 施法中. 计算机辅助几何设计与非均匀有理 B 样条[M]. 北京: 高等教育出版社, 2001.

（上接第 269 页）

参考文献

1 蒋东兴, 史宗恺, 陈怀楚. 大学资源计划的方案研究[J]. 清华大学学报(自然科学版), 2004, 44(4).

2 李培峰, 朱巧明. 基于 Web 服务的校园信息化平台的设计和实现[J]. 计算机工程与设计, 2006, 27(19).

3 王 威, 蒋东兴, 刘启新. 支持信息集成的校园信息门户的研究与设计[J]. 计算机工程与设计, 2006, 27(20).

4 冯登国. 计算机通信网络安全[M]. 北京: 清华大学出版社, 2001.

5 吴 敏, 刘晓强, 陈家训. 基于 Web services 的安全服务框架及其在数字化校园中的应用研究[J]. 东华大学学报(自然科学版), 2006, 32(6).

6 李培峰, 朱巧明, 钱培德. 基于组件的异构数据集成平台的设计与研究[J]. 计算机应用与软件, 2005, 22(9).