无线局域网络安全性的研究*)

熊 江[1] 顾君忠[2]

(重庆三峡学院计算机科学系 重庆万州 404000)[1] (华东师范大学多媒体技术研究室 上海 200062)[2]

Study on Wireless Local-Area Network Security

XIONG Jiang[1] GU Jun-Zhong[2]

(Department of Computer Science, Chongqing Three Gorges College, Wanzhou 404000 ,China)[1]

(Lab. of MMIT, East China Normal University, Shanghai 200062)[2]

Abstract Wireless Network rapid development and use present more high security request for constantly extensive network system. By analyzing existing wireless LAN safety measure at this paper proposes and realizes overall information safe protection solution,strengthens the security of the communication data in the wireless LAN greatly.

Keywords Wireless local-area network, Access point, Media access control, Wired equivalent privacy, Remote authentication dial-in user service

1. 无线局域网简介

无线局域网(Wireless local-area network,WLAN)是计算机网络与无线通信技术相结合的产物。WLAN 利用了无线多址信道的一种有效方法来支持计算机之间的通信,并为通信的移动化、个性化和多媒体应用提供支持,使用无线电或红外线信号来处理数据传输,以替代传统线缆的同时,提供以太网或者令牌网络的功能。

1.1 无线局域网的优点

无线网络越来越受欢迎,是因为用户可以在无线局域网覆盖的范围内自由移动而不必受线路的影响。它不但可以使用户在办公楼里很方便地接入网络,而且在办公楼外也同样适用。因此具有有线网络不可取代的优势,早已经成为潜力巨大的市场。1997 年 6 月,第一个无线局域网标准 IEEE 802.11 正式颁布实施,为无线局域网的物理层和 MAC 层提供了统一的标准,有力推动了该市场的快速发展。

无线局域网具有的优势是:一是可移动性,它提供了不受线缆限制的应用,用户可以随时上网;二是容易安装、无须布线,大大节约了建网时间;三是组网灵活,即插即用,网络管理人员可以迅速将其加入到现有网络中,并在某种环境下运行;四是成本低,特别适合于变化频繁的工作场合。

1.2 无线局域网的应用

无线局域网不仅可以实现许多新的应用,还可以克服线缆限制引起的不便性,解决某些特殊区域无法布线的问题。目前,无线局域网已经在教育、金融、健康、旅馆以及零售业、制造业等各方面有了广泛的应用,比如:(1)接入网络信息系统:电子邮件、文件传输和终端仿真。(2)难以布线的环境:老建筑、布线困难或昂贵的露天区域、城市建筑群、校园和工厂。(3)频繁变化的环境:频繁更换工作地点和改变位置的零售商、生产商,以及野外勘测、试验、军事、公安和银行等。(4)使用便携式计算机等可移动设备进行快速网络连接。(5)用于远距离信息的传输:如在林区进行火灾、病虫害等信息的传输;公安交通管理部门进行交通管理等。(6)专门工程或高峰时间所需的暂时局域网:学校、商业展览、建设地点等人员流动较强的地方利用无线局域网进行信息的交流;零售商、空运和航运公司高峰时间所需的额外工作站等。(7)流动工作者可得到信息的区域:需要在医院、零售商店或办公室区域流动时得到信息的医生、护士、零售商、白领工作者。(8)办公室和家庭办公室用户,以及需要方便快捷地安装小型网络的用户。

当然,作为一个新产品,与有线网络相比,无线局域网也有很多不足。目前无线局域网还不能完全脱离有线网络,它只是有线网络的补充,而不是替换。

2. 无线局域网的不足

无线局域网的有效数据传输受周围电磁环境的影响。如果电磁波很高,效率就会降低,甚至导致整个通信的中断。由于无线 LAN 产品和微波炉都使用 2.4GHz 的频带,所以最有可能干扰无线 LAN 传输的就是微波炉,不过,一般只要距离微波炉 3m 以外就没有什么问题了。

无线局域网依靠无线电波的传播。这些电波是从无线网络全向发射装置发射的,墙壁、大型用具和其他障碍物都可阻碍它们,使得网络的性能降低。

无线局域网络与有线网络相比较的话,无线网络安全性的问题的确引人重视,因为无线网络是利用空间当作数据传输的媒介,所以比较容易收到攻击。在无线网络的安全防护上,最大的问题出在无线波传播的范围是如此之大。攻击者要进入无线网络,可以不必动用任何物理连接线,如果使用接收天线放大器,在无线电波广播范围内的任何人,都可以监听网络的通信,他甚至不必靠近攻击的目标。攻击者可以在你完全不知道的情况下,花很长的时间来破解你的密码,而后进入网络窃取你的资料。与普通互联网上的情况不同,没有什么防火墙可以用来保护无线网络上的电脑。例如,在停车场附近的人可以很容易地破坏办公室的无线网络,利用访问代码和适当的设备截取敏感数据。

*)国家高技术研究发展计划(863 计划)经费资助(项目名称:无线局域网信息安全保护与漫游;项目编号:2001AA143060)。熊 江 讲师,主要研究方向是无线网络。顾君忠 教授,博士生导师。

无线局域网络的速率比有线局域网络要慢得多，数据访问速率的范围是1Mbps～11Mbps。无线网络的速度较慢，在具体应用中，效果会很不同。例如，希望通过无线网络传递效果好的视频流数据是不太可能的。音频数据的传递上会好些，但也不是很令人满意。

但随着时间的发展，无线网络正暴露出越来越多的安全问题。据美国Gartner发表的有关企业WLAN导入的安全方面的调查报告表明，因企业在采取无线LAN系统时都未采取适当的安全对策，到2002年底，30%的企业将为数据泄漏等严重安全问题所困扰。据介绍，现在有50%以上的企业已采用或正计划采用无线LAN。但据推测至少少于20%的企业内部网络的无线LAN“存在问题”。RSA Security在英国伦敦进行的一项调查也表明，67%的WLAN毫无安全可言。

3. 现有无线局域网安全措施、不足及其改进思路

一般网络的安全性可以从三个要素分析：访问控制、身份验证、数据保密性。如果这三个要素都没有问题了，就不仅能保护传输中的信息免受危害，还能保护网络和移动设备免受危害。分析表明IEEE 802.11标准中没有关于身份认证的机制，而现存的访问控制机制和数据保密机制都存在严重的漏洞。

3.1 ESSID(Extended Service Set Identifier)

在通讯前所有的移动节点必须和无线接入点(Access Point，AP)建立连接，多数情况下这要求移动台和AP配置为具有相同的网络扩展服务集标识符(ESSID)，每个AP具有一个唯一的网络ESSID，这使得一组设置为具有相同ESSID的用户可以使用此AP，也就是说，若移动用户想连接某一AP，则必须知道此AP的ESSID，若AP的ESSID设置和用户的ESSID设置不一致，则用户无法访问AP。这种方式提供了无线网络最基本的安全措施。

3.1.1 WLAN ESSID的不足　然而这种安全措施是十分有限的，只是一个简单的口令，只能提供一定的安全；而且如果配置AP向外广播其ESSID，那么安全程度还将下降。一般情况下，由于是用户自己配置客户端系统，所以很多人都知道该ESSID，很容易共享给非法用户。目前有的厂家支持“任何”ESSID方式，只要无线工作站在任何AP范围内，客户端都会自动连接到AP，这将跳过ESSID安全功能，现在许多无线网卡产品能自动搜索周围环境中的AP和AP的ESSID参数，并允许用户进行自由选择连接的AP，这是因为AP会定期广播自己的ESSID。一般地说，ESSID是最大长度为32位的字符串，并对大小写字母是区分的。

3.1.2 WALN ESSID的改进思路　为了提供给移动用户最大限度地方便使用周围地无线AP，很多无线网卡和AP都提供了ANY这个保留关键字来使得网卡能够连接最可用的附近的AP，但方便性带来了安全的隐患，如果需要增强ESSID上的安全，就需要关闭这个ANY关键字、不配置AP向外广播其ESSID和不让用户自己配置客户端系统，由系统管理员配置客户端系统，不让用户知道该ESSID，但这会加大系统管理员的工作量。

3.2 MAC(Media Access Control)地址过滤

每个无线工作站网卡都由惟一的物理地址标示，因此可以在AP中手工维护一组允许访问的MAC地址列表，实现物理地址过滤。这需要在AP设备的永久性存储器中存放一组用户的MAC地址列表，只有列表中的用户可以访问对应的AP，其它用户是被拒绝使用此AP的。在移动用户向网络发出联网请求后，AP首先检查自己的MAC地址列表，以判断此用户是否允许访问网络。当然，管理员可以很方便地对AP中存储的用户MAC地址列表进行添加、删除等修改，以控制可以访问AP的用户数量。物理地址过滤属于硬件认证，而不是用户认证，是目前在无线局域网中最简单、最基本的安全防范手段。特别是对于AP数量不太多的无线局域网系统是比较适合的。

3.2.1 MAC地址过滤的不足　其一是目前这种方式要求AP中的MAC地址列表必须随时更新，都是手工操作，如果用户增加，则工作量很大。并且其扩展能力很差，因此只适合于小型网络规模。AP设备所支持的无线用户的数量是有限的，若在一个无线环境中，有上千个AP都采用手工方式配置用户MAC地址列表，这将是十分麻烦的。如果允许一个用户在整个无线网络中漫游，则需要在每个AP的用户MAC地址列表中加入该用户的MAC地址。所以MAC地址列表过滤法的使用在实际中受到了一定程度的限制。

其二是使用MAC地址列表也是一种比较脆弱、麻烦的安全手段，因为许多无线网卡支持通过重新配置的方法来改变网卡的MAC地址，另一方面，很多生产厂商为方便用户会把网卡的MAC地址印刷在无线网卡背面的标签上。非法入侵者可以从无线电波中截获数据帧从而分析出合法用户的MAC地址，进而修改自己的MAC地址，伪装成合法地址以访问网络，这就使得网络的安全遭到破坏。

其三是基于设备MAC地址的认证策略会因为设备的丢失或失窃而失效，而且每当类似事件发生时，都需要对保存在每一台网络接入点设备内的MAC地址数据库进行变更。

3.3 WEP技术(Wired Equivalent Privacy)

有线等效保密(WEP)技术是所有经过Wi-Fi认证的无线局域网所支持的一项标准功能，是对无线网卡到接入点间的数据进行加密的。由电子与电气工程师协会(IEEE)制定的WEP是用来：(1)提供基本的安全性保证；(2)防止有意的窃听；(3)利用一套基于40位共享加密密钥的RC4加密算法对网络中所有通过无线传送的数据进行加密，从而有效地保护网络。静态WEP是一种可选的、基于RC-4的40位或128位加密算法。40位WEP加密因其附加了24位的表明局域网设备特性的初始字符串，有时也称为64位WEP。静态WEP密钥配置在AP设备端，形式上为10位或26位的十六进制数。

移动用户和AP可以配置4组WEP密钥，加密传输数据时可以轮流使用，这允许加密密钥动态改变，但密钥只能是4组中的一个，其实质上还是静态WEP加密。同时，AP和它所联系的所有移动用户都使用相同的加密密钥，使用同一AP的用户也使用相同的加密密钥。

3.3.1 WEP的不足　其一是若其中一个用户的密钥泄漏，其他用户的密钥也无法保密了。造成WEP密钥无法被广泛使用的另一个问题是WEP密钥必须是手工操作，对于一个网络管理员来说，配置几百个AP或客户端网卡的密钥是一件很头疼的事情。

其二是2000年10月，WEP被发现存在安全漏洞，已经证明现有的静态WEP加密技术通过“截获数据报”后进行分析，高速的计算设备只需几秒钟即可计算出40位WEP密钥，这是利用了RC4初始向量的错误使用，40位的钥匙在今天很容易被破解，钥匙是静态的，并且要手工维护，扩展能力差。

3.3.2 WEP的改进思路 思路一是IEEE最近定义了一种称为TKIP(Temporal Key Integrity Protocol)的加密技术,这种技术又被称为WEP2,WEP2采用128位加密钥匙,从而提供更高的安全。但是WEP2目前不保证互操作性,理论上,解密128位WEP密钥需要的时间是40位的指数倍数,然而实际中,在个人计算机上解密128位WEP密钥只需二分多钟。入侵者可以把自己的数据通过非法截获的WEP密钥加密以伪装成合法的数据,或者通过获取的WEP密钥解密在空中传输的加密信息。

思路二是最理想的方式是WEP的密钥能够在用户登录后进行动态改变,这样,黑客想要获得无线网络的数据就需要不断跟踪这种变化。基于会话和用户的WEP密钥管理技术能够实现最优保护,为网络增加另外一层防范。这就是动态WEP的方法。

3.4 虚拟专用网络(VPN)

虚拟专用网是指在一个公共IP网络平台上通过隧道以及加密技术保证专用数据的网络安全性,是端对端数据加密,目前许多企业以及运营商已经采用VPN技术。只要具有IP的连通性,就可以建立VPN。VPN技术不属于802.11标准定义,因此它是一种增强性网络解决方案。严格来讲,VPN可以替代连线对等保密解决方案以及物理地址过滤解决方案,也可以与WEP协议互补使用。采用VPN技术的另外一个好处是可以提供基于Radius的用户认证以及计费。虚拟网(VPN)则是保护网络后门安全的关键,VPN具有比WEP协议更高层的网络安全性(第三层),能够支持用户和网络间端到端的安全隧道连接。VPN协议包括第二层PPTP/L2TP协议以及第三层的IPsec协议。VPN可以提供目前最高级别的168位3DES加密算法,其安全程度明显好于WEP协议。

3.4.1 VPN的不足 VPN不仅成本高,难以扩展,而且限制了IT部门对通过网络传输的数据的控制。

3.5 端口访问控制技术(802.1x)

该技术也是用于无线局域网的一种增强性网络安全解决方案。当无线工作站STA与无线访问点AP关联后,是否可以使用AP的服务要取决于802.1x的认证结果。如果认证通过,则AP为STA打开这个逻辑端口,否则不允许用户上网。802.1x要求无线工作站安装802.1x客户端软件,无线访问点要内嵌802.1x认证代理,同时它还作为Radius客户端,将用户的认证信息转发给Radius服务器。802.1x除提供端口访问控制能力之外,还提供基于用户的认证系统及计费。IEEE 802.1x是运行在无线网设备关联之后,其认证层次包括两方面:客户端到802.1x认证端,认证端到认证服务器。802.1x定义客户端到认证端采用EAP over LAN协议,认证端到认证服务器采用EAP over Radius协议。

3.6 提高已有的RADIUS服务

大公司的远程用户常常通过RADIUS(远程用户拨号认证服务)实现网络认证登录。企业的IT网络管理员能够将无线局域网集成到已经存在的RADIUS架构内来简化对用户的管理。这样不仅能实现无线网络的认证,而且还能保证无线用户与远程用户使用同样的认证方法和帐号。

3.7 集成无线和有线网络安全策略

无线网络安全不是单独的网络架构,它需要各种不同的程序和协议。制定结合有线和无线网络安全的策略能够提高管理水平,降低管理成本。例如,不论用户是通过有线还是无线方式进入网络时,都采用集成化的单一用户ID和密码。

通过上面分析了第一代无线网络的安全机制,表明其已经不能给现在的企业或组织提供足够的安全性能。由于第一代无线局域网的种种安全漏洞,无线网络的安全问题已经引起了国外不少公司或组织的重视。本课题主要针对802.11b无线以太网技术提出"全面信息安全保护"解决方案。

4. "全面信息安全保护"解决方案

我们针对802.11b无线以太网技术提出"全面信息安全保护"解决方案,在实现中采用RADIUS认证机制对无线以太网用户进行认证、采用ESSID认证机制和MAC地址访问限制列表对访问者进行过滤、采用WEP会话安全密钥对传送的数据进行保护,以此来充分保护用户数据的私密性。

整个解决方案从层次上可以通过核心功能的视图分成三个层面(图1),它们分别是:

(1)无线设备层:这个层面是核心功能层所管理的设备,在此层中,主要包含系统操作的对象,其直接对象是AP设备,间接对象是由AP进行连接并通过AP设备进行网络访问的无线从业人员,可以说,系统之所以存在,就是为了使此层中的用户能够安全方便地使用AP设备。

这个层面对外提供两个操作访问界面,分别是AP设备访问层和Radius数据库访问层,所有外界借对此层的操作必须通过这两个访问模块来进行,这两个访问模块属于系统实现部分。

(2)无线安全及漫游管理层:无线安全及漫游管理层的主要功能就是对系统无线环境进行管理,加强其安全性,方便地实现用户、设备、安全一体化管理,为了实现其目的,在此层中包含了多个模块和模块引擎,包括安全策略分析引擎、用户漫游管理引擎、用户管理模块、无线设备安全策略引擎、预警模块、日志管理引擎、无线设备发现引擎、无线设备组群管理引擎、无线设备维护模块。正是由于这些模块的存在及其相互作用,系统得以实现安全地管理无线环境和用户漫游。

(3)数据库访问层:为了很好地实现无线安全和漫游管理,系统必须能够对各类数据进行统一有效地处理,这些数据应该有一个可管理的中心来存放,这也就是数据库访问层存在的原因,由于其在系统中的特殊地位(上层无线安全及漫游管理层的基石),所以单独把数据库访问作为一个单独的层次划分出来。

本解决方案的设计思路:

(1)交互认证:原来的IEEE 802.11无线局域网技术提供了两种认证方式:开放系统认证和共享密钥认证。顾名思义,开放系统认证即是不进行任何认证。通过窃听大量交互认证帧的被动攻击方法,当前的共享密钥认证协议就可以很容易地被攻破。而且,共享密钥认证只是AP对用户的认证,即单向认证。这些都成为导致无线局域网不安全的隐患,容易使无线局域网受到字典攻击、MIM攻击和会话攻击等一系列的攻击。而新系统利用IEEE 802.1X框架中的EAP认证,实现交互认证,为无线LAN实体提供强大的清晰的交互认证及会话密钥协商。即不仅是服务器端对客户端进行认证,无线客户端也可以对服务器端进行认证,从而有效地避免了字典攻击、MIM攻击和会话攻击等。

(2)基于的用户认证:IEEE 802.11认证是基于设备的,设备的使用者对认证者来说是透明的,所以未授权的用户可以通过简单地获取授权设备的使用权而获得网络的访问权。使用IEEE 802.11无线网卡的笔记本电脑,如果只是使用静

态 WEP 进行 IEEE 802.11 认证，当其被窃后，就可能会给网络造成严重危害。这种事情要求管理者迅速地更改无线网络和所有用户的 WEP 密钥。这种情况是经常发生的而且成为无线网络应用的主要负担。而基于用户的认证就可以很好地解决这一问题。

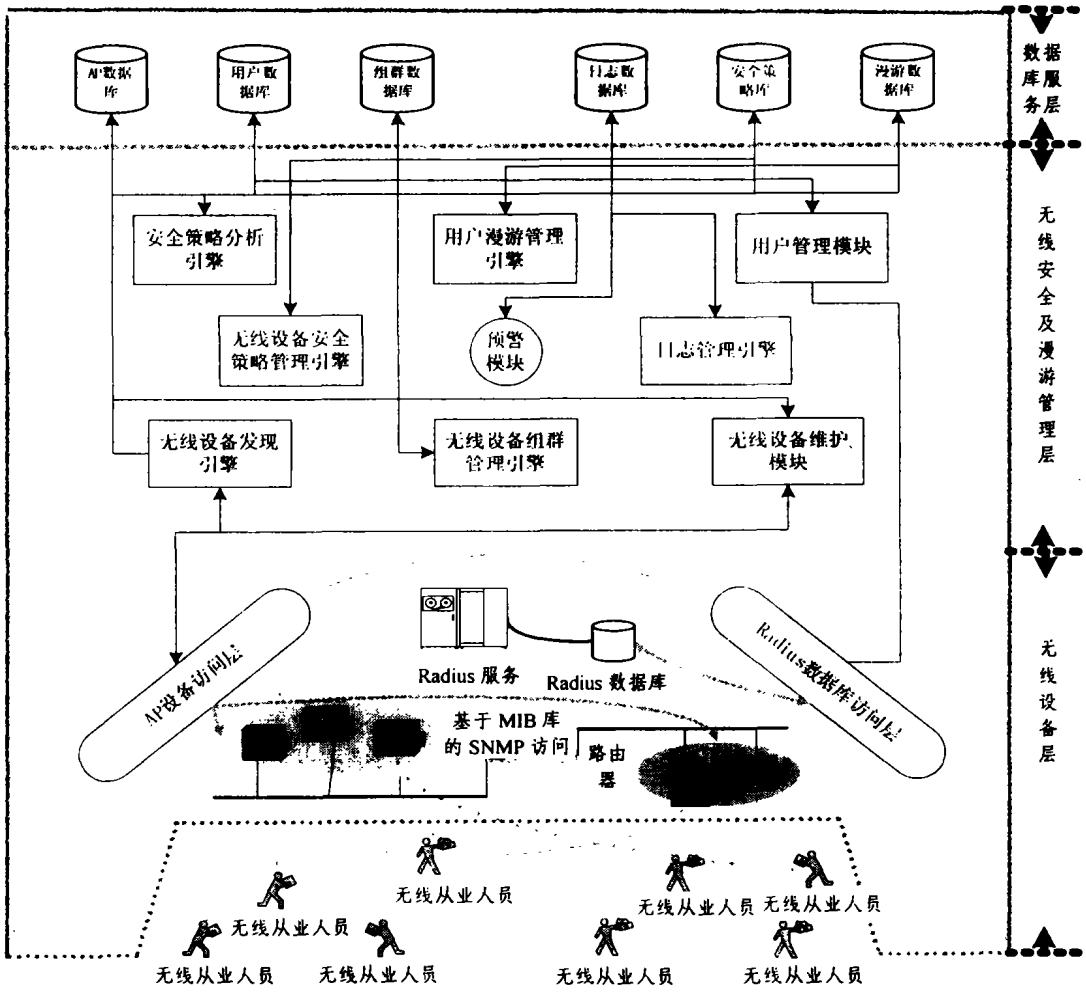

图 1

(3)使用 TKIP 的数据保密：TKIP 是 IEEE 工作组 TGi 制定的一个草稿。TKIP 主要对 WEP 进行了两方面的加强：它将加密密钥提高到 128 位，从而减小了无线局域网的易受攻击的可能性。对所有 WEP 加密的数据帧进行信息完整性(MIC)校验；所有 WEP 加密的数据帧有唯一的密钥。

(4)信息完整性校验：信息完整性检验是对 IEEE 802.11 标准中的完整性校验函数(ICV)的改进。

总结 在无线局域网络市场迅猛发展的今天，用户迫切要求为无线局域网络的使用提供全面的网络安全保证，本解决方案经过实践证明能极大地增强无线局域网内通信数据安全，并且本解决方案管理方便，控制容易，扩展性好，维护方便，填补了国家在无线局域网信息安全领域的空白。

参 考 文 献

1 (美)Wheat J. 无线网络设计. 北京：机械工业出版社，2002
2 (美)Geier J. 无线局域网. 北京：人民邮电出版社，2001
3 Monly M，Pautet M-B. The GSM system for mobile communications. ISBN7-5053-3634-7/TP. 1499. 电子工业出版社，1996. 259～271
4 Macaulay T. Hardening IEEE 802.11 wireless networks. 2002
5 http：// www. chinawlan. net/articleDetail. asp? CatID = 12&NewsID=5513. 无线局域网安全挑战自由. 2002
6 Macaulay T. Hardening IEEE 802.11 wireless networks. http：// www. ewa-canada. com . 2002
7 Fluhrer S，Mantin I，Shamir A. Weaknesses in the Key Scheduling Algorithm of RC4. http：// www. drizzle. com/～ aboba/IEEE/rc4_ksaproc. pdf. 2001，07