基于 WEP 协议的无线局域网安全性的改进思路*)

熊 江
(重庆三峡学院计算机科学系 万州 404000)

摘 要 无线网络系统的迅速发展和广泛应用令市场对其安全要求不断提高,本文通过分析 WEP 协议的安全性能,在 WEP 协议的基础上,针对其安全漏洞,提出了 EWEP 协议,彻底消除了已知攻击的危害并且实现了抵御这类攻击的最佳效果,保证了数据在无线局域网中的安全性。

关键词 无线局域网络,安全,WEP,802.1X,EAP

WEP Protocol-based Wireless LAN Secure Improvement Mentality

XIONG Jiang
(Department of Computer Science, Chongqing Three Gorges College, Wanzhou 404000)

Abstract Wireless Network is rapid developed and useed, and make market improve to security request of system, Through analyzing existent WEP protocol safety measure, this paper discovers the flaws in WEP, and improves it, presents the new protocol — EWEP(Enhancement Wired Equivalent Privacy)on the base of WEP. It will nullify known attacks to WEP ,Guarantee the security of data in the wireless local area network.

Keywords Wireless local area networks, Security, Wired equivalent privacy, Port based network access control protocol, Extensible authentication protocol

1 无线局域网络技术

无线局域网络(Wireless Local Area Networks;WLAN)是利用射频(Radio Frequency;RF)的技术,取代旧式有线双绞铜线所构成的局域网络,WLAN 利用电磁波在空气中发送和接受数据,而无需线缆介质。WLAN 的数据传输速率现在已经能够达到 11Mbps(802.11b),最高速率可达 54Mbps(802.11a),传输距离可远至 20km 以上。它是对有线连网方式的一种补充和扩展,使网上的计算机具有可移动性,能快速方便地解决使用有线方式不易实现的网络连通问题。

1.1 无线局域网络的优点

①安装便捷。在网络建设中,施工周期最长、对周边环境影响最大的是网络布线施工工程。在施工过程中,往往需要破墙掘地、穿线架管。而 WLAN 最大的优势就是免去或减少了网络布线的工作量,一般只要安装一个或多个接入点 AP(Access Point)设备,就可建立覆盖整个建筑或地区的局域网络。

②使用灵活。在有线网络中,网络设备的安放位置受网络信息点位置的限制。而一旦 WLAN 建成后,在无线网的信号覆盖区域内任何一个位置都可以接入网络。

③经济节约。由于有线网络缺少灵活性,这就要求网络规划者尽可能地考虑未来发展的需要,这就往往导致预设大量利用率较低的信息点。而一旦网络的发展超出了设计规划,又要花费较多费用进行网络改造,而 WLAN 可以避免或减少以上情况的发生。

④易于扩展。WLAN 有多种配置方式,能够根据需要灵活选择,并且能够提供像"漫游(Roaming)"等有线网络无法提供的特性。

1.2 无线局域网所面临的安全问题

①无线电窃听。无线电波可以穿透建筑物等设施,覆盖到外面的停车场甚至几个街区,处于这些位置的人使用无线网卡,就会被动地接受到公司的敏感信息。

②网络访问控制。无线电波传输的范围超出了网络拥有者所在的物理范围,一个站在公司围墙外的攻击者只要知道访问口令,就可以通过接入点侵入到内部的有线网络而不用四处寻找网线插座。

③拒绝服务攻击。无线局域网存在一种比较特殊的拒绝服务攻击,攻击者可以发送与无线局域网相同频率的干扰信号来干扰网络的正常运行,从而导致正常的用户无法使用网络。

由于 WLAN 具有多方面的优点,其发展十分迅速,WLAN 已经在政府、军队、油田、酒店、医院、商场、工厂和学校等不适合网络布线的场合得到了广泛的应用。但随着应用的深入,无线网络也暴露出越来越多的安全问题。

2 WEP 安全协议在保证无线局域网安全性中的重要性

IEEE 802.11 协议内考虑的安全技术主要有 3 种:ESSID、MAC 地址访问控制机制和 WEP 协议。

2.1 ESSID(Extended Service Set Identifier)

在通讯前所有的移动节点必须和无线接入点 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

*)重庆市教委科研项目(编号:KJ061107)和重庆三峡学院校级科研项目(2005-sxxyyb-002)资助。熊 江 副教授,硕士,研究方向为计算机网络及硬件。

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。

2.2 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，只有在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。

2.3 WEP(Wired Equivalent Privacy)技术

WEP 称为“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，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 位共享加密秘钥的 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，依靠共享密钥 K 来实施对链路层数据的保护。

由于网络扩展服务集标识符 ESSID 可通过窃听获得以及 MAC 地址的可被修改性，因此由 ESSID 和 MAC 地址访问控制机制所提供的访问控制策略是很初级和脆弱的。其安全性主要是由 WEP 协议来保障的。WEP 提供的安全保护主要体现在如下 4 个方面：(1)数据的保密性；(2)数据的完整性；(3)用户认证；(4)密钥管理。

由此可见，WEP 对无线局域网的安全有着重要的意义，其安全与否直接决定了无线局域网的安全性。通过改进 WEP 协议的安全性能，也就达到了提高 802.11 无线局域网的安全性的目的。

3 WEP 安全协议在保证无线局域网安全性中的不足

WEP 安全协议的安全漏洞实例一：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 或客户端网卡的的密钥是很头疼的事情。

WEP 安全协议的安全漏洞实例二：2000 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。

以上实例说明了 WEP 协议从数据通信的保密性，数据的完整性，用户认证以及密钥管理四个方面揭示了 WEP 协议都存在安全漏洞。

4 WEP 安全协议在保证无线局域网安全性的改进思路

在对 WEP 协议安全性分析的基础上，针对其安全漏洞，提出了改进方案 EWEP(Enhancement Wired Equivalent Privacy)协议。EWEP 协议成功地解决了数据的保密性、数据的完整性、用户认证和密钥管理四个方面的漏洞，所以能抵御针对 WEP 的各种攻击并且实现了抵御这类攻击的功能，保证了数据在无线环境中的安全性。EWEP 协议并不是一个完全重新设计的协议，它是在 WEP 协议的基础上，针对 WEP 协议的 4 个安全漏洞，通过引入新的安全方法与机制(如 802.1X 协议)改进而来的。

4.1 用户的认证机制的改进

将 IEEE 802.1X 协议(又称为基于端口的访问控制协议；Port based network access control protocol)应用到具体的 802.11 无线局域网中，首先要确定所使用的认证服务。由于远程拨入用户认证服务 RADIUS 支撑灵活的认证机制，具有良好的扩展性等诸多的优点，选择 RADIUS 作为后端认证服务器。此时，802.1X 中的三大组件——请求方、认证方和认证服务器分别对应为移动终端、接入点和 RADIUS 服务器。其中接入点就是接入控制单元。它划分为两个逻辑端口：“受控端口”和“非受控端口”。“非受控端口”用来验证用户，只允许 802.1X 数据流通过；而另外一些类型的网络数据流，如动态主机配置协议(DHCP)、超文本传输协议(HTTP)、文件传输协议(FTP)、简单邮件传输协议(SMTP)和邮局协议(POP3)等，只能在移动终端通过验证后，通过“受控端口”(未通过认证前为非认证状态)进行传输。

在 EWEP 协议中选择 TLS(Transport Level Security)。EAP-TLS(Extensible Authentication Protocol-TLS)不但提供认证，而且同时提供动态会话密钥的分发。所有的无线客户端以及服务器都需要事先申请一个标准的 X.509 证书并安装，在认证的时候客户端和服务器要相互交换证书。在交换证书的同时，客户端和服务器要协商出一个基于会话的密钥，一旦认证通过，服务器将会话密钥传给接入点并通知无线接入点允许该客户端使用网络所提供的服务。该改进方案定义了 802.1X 在 802.11 无线网络中的具体应用方式。

4.2 密钥管理的改进

在认证过程中，客户端和服务器会协商出一个基于会话的密钥，一旦认证通过，服务器将会话密钥传给无线接入点并通知无线接入点允许该客户端使用网络服务，同时 AP 用会话密钥加密广播密钥并将密文发送至移动终端，移动终端用会话密钥解密密文以得到广播密钥。

至此密钥的生成与分发过程结束，AP 的受控端口置为已认证状态，移动终端利用会话密钥与广播密钥与 AP 进行通讯。当初始化向量空间用尽或重新认证计时器超时，将重复上述过程，以获得新的会话密钥。该改进方案提出了密钥的集中管理和动态分发机制，以动态的会话密钥代替了原协议中静态的 WEP 密钥，解决了密钥的管理问题。

4.3 数据通信的保密性的改进

为了有效地防止密钥相关性攻击，在 EWEP 协议中采用了对不同的数据报文采用不同的加密密钥。如图 1 所示，Ⅳ(初始化向量：Initialization Vector)和 WEP 会话密钥利用哈希函数产生一个唯一的每包密钥。由每包密钥和Ⅳ值首尾相连作为 RC4 加密算法的输入，产生一个密钥序列。利用针对每一个数据报文而采用不同的 RC4 密钥序列，极大地增强了数据的安全性。

每次会话开始以后，Ⅳ值从零开始随着每个数据报文递增，当Ⅳ空间耗尽时，将强制结束会话，并重新进行认证以开始一个新的会话，新的会话将采用新的会话密钥。这样就确保了在Ⅳ空间耗尽前密钥得到及时正确的更新，防止了Ⅳ值的冲突。

该改进方案利用每包密钥机制和具有序列功能的初始化向量，弥补了 WEP 协议在数据保密性方面所存在的漏洞。

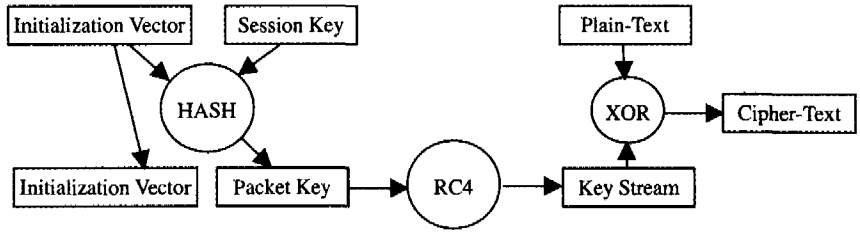

图 1　每包密钥

4.4　数据的完整性的改进

CRC-32 算法一般用于检测随机的错码，但却无法防止人为篡改。在 EWEP 协议中提供了一种更强的机制来保证数据的完整性。

在 EWEP 协议中，分别增加了一个 MIC(Message Integrity Check)字段和 SEQ 字段，如图 2 所示。

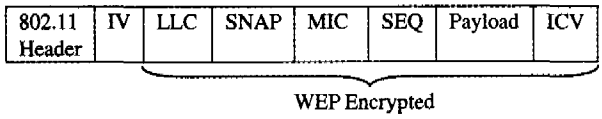

图 2　EWEP 加密后的报文格式

在发送方，对源 MAC 地址、目的 MAC 地址、SEQ 字段和载荷数据利用 MD5 算法计算消息摘要，并将摘要结果置于 MIC 字段。在接收端，用密钥解密密文，然后对源 MAC 地址、目的 MAC 地址、SEQ 字段和载荷数据重新计算消息摘要，并将计算得到的消息摘要与接受到的消息摘要相比较以决定消息是否合法。

SEQ 字段是一个顺序增加的计数器，它将随着报文发送的先后顺序递增，接入点将丢弃那些乱序的报文。数据的完整性是指保证数据不被非法地改动和销毁，EWEP 协议通过消息完整性检查功能保证了通信数据的完整性。

4.5　EWEP 协议的交互工作过程

发送方的操作如下：

(1)利用 802.1X 协议对用户进行认证，认证通过后协商会话密钥，并将会话密钥和广播密钥分发给移动终端和接入点；

(2)对源 MAC 地址、目的 MAC 地址、SEQ 字段和有效载荷首尾相连，计算其消息摘要，并将消息摘要填充至完整性检查字段 MIC；

(3)检查是否已经用尽初始化向量的空间，若已用尽，则结束此次会话。重新认证以开始一个新的会话过程，协商新的会话密钥，否则Ⅳ值加 1，并与会话密钥首尾相连，计算其消息摘要作为 RC4 算法的输入，生成密钥序列，其长度与明文 P 等长度；

(4)通过密钥序列和明文相异或得到密文，发送给接受方。

接受方接受到消息以后，进行加密过程的反过程，其操作如下：

(1)从数据报首部取出初始化向量Ⅳ，并与会话密钥首尾相连，计算其消息摘要，得到每报文加密密钥，以加密密钥作为 RC4 的输入产生密钥序列；

(2)用密钥序列与密文相异或以恢复明文；

(3)计算报文中的源 MAC 地址、目的 MAC 地址、SEQ 字段和有效载荷的消息摘要，其计算结果若与报文中的 MIC 字段相一致，则接受此数据帧，否则丢弃。

结论　WEP 安全协议在保证无线局域网安全性的改进思路方案通过提供一种身份认证机制，使合法用户平滑的进入网络而将非法用户拒之门外和通过加密等手段保证数据在无线环境中的安全性。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。

参 考 文 献

1　Borisov N. Wireless Privacy: Analysis of 802.11 Security. http://www.drizzle.com/~aboba/IEEE/wep-draft.zip. 2005,12

2　Stubblefield A, Ioannidis J, Rubin A D. Using the Fluhrer, Mantin, and Shamir Attack to Break WEP. http://www.cs.rice.edu/~astubble/wep/. 2006,01

3　苏鹏，胡志远，塔维娜，等. 802.11 无线局域网安全现状及其解决方案[J]. 计算机工程，2003(4)

4　吴越，曹秀英，胡爱群，等. 无线局域网安全技术研究[J]. 电信科学，2002(6)

5　左晓东，戴英侠. 无线局域网的安全性分析[J]. 电信科学，2001(7)

6　沈基明，曹秀英. 802.11WLAN 安全漏洞分析和改进方案[J]. 通信技术，2002(7)

7　徐敏，罗汉文. 无线局域网安全问题研究[J]. 通信技术，2002(7)

8　Walker J R. An analysis of the WEP encapsulation. http://www.drizzle.com/~aboba/IEEE/0-362.zip. 2005,11

9　Cam-Winget N, Walker J, Aboba B, et al. Rapid Re-keying WEP a recommended practice to improve WLAN Security. http://www.drizzle.com/~aboba/IEEE/wepimprovF.ppt. 2006,1

10　凌畅宇，刘乃安，王蔚. 应用 802.1X 标准部署安全的无线局域网[J]. 航空计算技术，2002(9)

11　熊江. 无线局域网络安全性的研究[J]. 计算机科学，2003(7)