

电力物联网环境下 WLAN 安全研究

华 晔，张 涛，王玉斐，黄秀丽

（中国电力科学研究院，江苏 南京 211106）

摘 要：随着电网规模的不断扩大以及电力营销市场的迅速发展，大量的电网作业点分散于环境恶劣的野外，对电力系统通信方式提出了新的要求。无线网络以其在网络建设的灵活性、便捷性、扩展性、性能价格比等方面的优势在电力系统中通信中得到了应用和普及。WLAN 是无线网络中的一个重要的组成部分，随着智能电网的全面建设，WLAN 已被应用于电力通信之中，其安全问题也显得至关重要。本文首先介绍了电力通信的背景，接着，对 WLAN 安全机制及其理论研究趋势进行了分析，最后，提出了对电力物联网环境下 WLAN 安全防护的思考。

关键词：电力系统；物联网；智能电网；无线局域网安全

0 引言

电力通信是现代电力系统中的重要组成部分，是构建智能电网的基本要素。电力通信网是电网调度自动化、网络运营市场化和管理现代化的基础，为了确保电网安全、稳定、经济的运行，电力系统必须有一个可靠的通信系统作为支持。

目前，大多数的电力通信网仍主要构建在有线网络之上。传统的有线网络通过传输介质进行通信，受到布线的限制，如设计方式或环境条件的制约等，当涉及到网络移动或重新布局时，其在移动性、扩充性和投资的经济性上都暴露出缺陷和不足^[1]。

随着电网建设规模的不断扩大和电力营销市场的迅速发展，大量的电网作业点分布于环境恶劣的野外，这对电力系统通信方式提出了新的要求：实时准确高效的电力数据传输、高性价比的设备配置、便捷的安装方式等，这些是仅采用有线网络进行通信所不能达到的。

无线通信技术日趋成熟，具有构建灵活、简便、易扩展和性价比较高等优势，能够较好地满足当今电力系统对通信的要求，为电力系统延伸服务、加强服务力度提供了保证。在智能电网构建的总体规划之中，移动办公系统、智能变电站无线巡检系统、电子围栏系统、抗灾指挥系统和应急抢修等诸多业务均需采用无线通信网络来实现^[2]。

无线局域网（WLAN）是无线通信的一个重要组成部分。WLAN 是计算机网络和无线通信技术相结合的产物，它以无线多址信道作为传输介质，利用电磁波完成数据交互，实现传统有线局域网的功能，具有安装方便、移动性好、容易扩展等优点^[3]。

由于无线局域网传输的开放性，其面临着诸多的安全威胁，如：未授权访问、窃听、伪装、篡改信息等，这些安全威胁将给无线局域网带来各种安全风险，用户和网络资源有可能遭受损失。随着无线通信在电力系统中的应用和普及，WLAN 的安全性将成为电力系统无线安全通信中所要研究的一个重要问题。

1 WLAN 安全机制

目前 WLAN 具有多种安全机制，本文将对 WEP、WPA、WPA2 和 WAPI 机制进行介绍。

1.1 WEP

WEP 称为有线等效保密协议（Wired Equivalent Privacy），是 IEEE 802.11b 协议中保障数据传输安全的核心部分，是一种基于链路层的安全协议，其目标是使无线局域网拥有与有线局域网同级别的安全性，保障无线网络中的数据传输的机密性，并对接入无线网络的用户进行身份认证^{[4][5]}。

在认证机制方面，WEP 提供了两种身份认证方式：开放系统认证（OSA）和共享密钥认证（PSK）。开放系统认证不需要任何密钥就可以接入，任何无线终端都可以通过 AP 连接至无线局域网。实际而言

开放系统认证并没有提供有效的认证方式，所有请求认证的 STA 均会通过认证。共享密钥认证要求 STA 和 AP 拥有一个静态的共享密钥。当 STA 向 AP 请求认证时，AP 发送给 STA 一个 Challenge 包，STA 必须使用正确的 WEP 密钥对包中的询问文本进行加密，并将它返回给 AP。如果 AP 能够使用相同的密钥对密文进行解密，恢复出原始的询问文本，则将允许 STA 接入，否则终止与 STA 的通信。共享密钥认证方式为 AP 对 STA 的单向认证。

WEP 采用 RC4 加密算法，使用流密码技术对无线传输的数据进行加密。WEP 使用 24 位的初始向量 (IV) 和 40 位的用户密钥共同构成种子密钥。加密时，将计算出的原始数据包明文数据的 32 位 CRC 冗余校验和 ICV 与明文一起构成传输负载，IV 和用户密钥构成的种子密钥通过流密码算法 RC4 的伪随机数发生器 (PRNG) 生成与传输负载长度一致的随机数，即为加密密钥流，加密密钥流与传输负载按位异或就得到密文。将 IV 和 WEP 密钥指数 KEYID 加在密文前面，形成 WEP 帧。解密的时，从包中提取 IV 和密文，将 IV 和用户密钥一起通过伪随机数发生器得到解密密钥流，解密密钥流和加密密钥流是相同的，将解密密钥流与密文相异或，得到原始明文和它的 CRC 校验和 ICV。将得到的明文采用相同的 CRC 表达式计算校验和 ICV'，并与 ICV 比较，考察数据的完整性，若两者相等，则可认为数据没有被篡改，否则丢弃该数据包。

WEP 采用 CRC-32 循环冗余校验和来保证数据的完整性。发送方在发出数据包前要先计算明文的 CRC-32 校验和 ICV，将其与明文一起加密后发送。接收方在收到 WEP 数据帧后，先对数据进行解密，然后计算出明文的 CRC-32 校验和 ICV'，并将其与 ICV 进行比较，若两者相同则认为数据在传输过程中没有被篡改，接受该数据包，否则丢弃该数据包。

1.2 WPA 与 WPA2

WEP 存在着诸多安全缺陷，为了弥补 WEP 的安全缺陷，Wi-Fi 联盟和 IEEE 于 2002 年 10 月共同发布了 WPA (Wi-Fi Protected Access)，WPA 是向 IEEE 802.11i (WPA2) 的过渡，WPA2 于 2004 年 6 月正式通过 IEEE 的批准。WPA 和 WPA2 从密码强度和用户认证方面着手，强化了无线网络的安全。WPA2 拥有比 WPA 更强的安全性。

WPA 是 IEEE 802.11i 的一个子集，它和 IEEE 802.11i 的正式版 WPA2 采用相同的认证机制和动态密钥管理机制。802.11i 提供了企业版和个人版两种认证方式。企业版是基于 IEEE 802.1x 和 EAP 的认证方式，需要一台具有 802.1x 功能的 RADIUS 服务器；个人版采用预先共享密钥的方式进行验证，用户手工输入密钥，适合家庭和 SOHO 使用^[6]。802.1x 协议称为基于端口的访问控制协议，其体系结构共包含了三个实体：申请者系统（通常为 STA）、认证系统（通常为 AP）和认证服务器系统（AS）。802.1x 本身并不提供实际的认证机制，需要和扩展认证协议 EAP 配合来实现用户的认证和密钥的分配。

802.1x 包含两个端口：非受控端口和受控端口。非受控端口允许认证者和 LAN 上其它计算机之间交换数据，无需考虑计算机的身份验证状态如何，非受控端口始终处于双向连通状态（开放状态），用以传递 EAPOL 协议帧，将 EAP 封装在 LAN 上，可保证客户端始终可以发出或接受认证；受控端口允许通过验证的 LAN 用户和验证者之间交换数据，平时处于关闭状态，只有在客户端通过认证时才打开，用以传递数据和提供服务。认证时，用户通过非受控端口和 AP 进行数据交换，请求者和认证者之间传输 EAPOL 协议帧，认证者和认证服务器同样运行 EAP 协议，认证者将 EAP 协议封装到如 Radius 等高层协议中，以便 EAPOL 协议穿越复杂的网络到达认证服务器。若用户通过认证，AP 就会为用户打开一个受控端口，通过受控端口用户可以传输各种类型的数据帧。EAP 只是一种封装协议，在具体应用中可以选择 EAP-TLS、EAP-MD5、EAP-TTLS、LEAP 等多种具体的认证方法。802.1x 实现的是 STA 和 AS 之间的双向认证。

802.1x 提供了一套密钥生成管理机制，生成动态的、临时的密钥。与 WEP 中预先设置好的密钥不同，802.1x 只在用户通过认证，安全环境建立之后才生成密钥。密钥受到时间的限制，每隔一段时间就会被更新，当安全环境结束之后，临时密钥自动销毁。认证和密钥的交互过程如下：（1）认证者和认证服务器通过互认证创建一个安全通道；（2）申请者和认证服务器通过互认证生成一个主密钥，认证过程

必须在认证者和认证服务器所创建的安全通道上完成；(3) 申请者和认证者分别通过自己的 EAP 主密钥产生 PMK，认证者的主密钥是在认证成功后由认证服务器向其发送的；(4) 申请者和认证者采用四步握手协议确保 PMK 的存在性，由 PMK 生成 PTK，并按照需要加载加密/完整性校验机制；(5) 认证者向申请者发送 GTK，以允许申请者传收广播消息，并能够有选择地向认证者发送单播数据包。其中，四步握手协议是密钥管理系统中最主要的步骤，其目的是确定申请者和认证者拥有相同且最新的 PMK，以保证能够生成最新的 PTK。同时，通过四步握手协议的结果通知申请者是否可以加载加密/完整性校验机制。组密钥更新握手是密钥管理过程中的最后一个阶段，它在上一阶段安全联盟建立的基础上，使用它已派生出的加密密钥和验证密钥来保护本阶段的通信，生成 GTK 用以保护以后组播消息的安全。

在数据加密和完整性校验方面，WPA 使用了临时密钥完整协议 TKIP^[7]。TKIP 仍然采用 RC4 加密算法，但它将密钥长度增加至 128 位，IV 长度增加至 48 位，并且通过两次加密混合函数生成最终的加密密钥流，安全性相对 WEP 而言大大增加^[8]。TKIP 中采用数据完整性编码 MIC 来保证数据的完整性，并在 MIC 校验失败时提供了抵抗措施。WPA2 缺省的加密机制 CCMP 为 128 位的分组加密算法，其使用了 CCM 模式的高级加密算法 AES^{[9][10]}。CCM 模式是指使用 counter 模式来加密，使用成组链块的消息认证码 (CBC-MAC) 来提供数据完整性认证。CCM 算法本身就能够提供有效的数据完整性校验机制，故在 CCMP 中没有额外的完整性保护机制。

1.3 WAPI

无线局域网鉴别与保密基础结构 WAPI (WLAN Authentication and Privacy Infrastructure) 是我国自主研发的无线局域网安全机制。WAPI 包括无线局域网鉴别基础结构 WAI 和无线局域网保密基础结构 WPI 两个重要组成部分，WAI 用于鉴别用户身份，WPI 用于对传输数据进行加密^[11]。

WAI 采用基于椭圆曲线的公钥证书机制，客户端 STA 和接入点 AP 之间通过鉴别服务器 AS 进行双向身份认证。WAI 与 IEEE 802.1x 相类似也有三个实体：鉴别请求实体 ASUE、鉴别器实体 AE 和鉴别服务实体 ASE，同样也采用双端口机制。除了鉴别数据之外，系统中 AP 和 STA 间的网络协议数据交换都是通过一个或多个受控端口来实现的，受控端口的状态由系统鉴别控制参数来确定。当 STA 连接 AP 时，必须进行认证，认证成功则 AP 允许其接入，否则解除其链路验证，整个过程包括证书鉴别、单密钥协商和组密钥通告。

WPI 是一组强度很高的分组加密算法，采用可控的会话协商动态密钥，对数据进行加密，安全系数很高。WPI 采用国家密码管理委员会批准的用于 WLAN 的 SSF43 对称分组加密算法对 MAC 子层的 MSDU 进行加密处理。其共有两种工作模式：OFB 模式和 CBC-MAC 模式，OFB 模式用于数据加密，CBC-MAC 模式用于完整性校验。

2 WLAN 安全机制分析

2.1 WLAN 安全机制差异

WEP 是较早的 WLAN 安全机制，存在着较多的安全缺陷，WPA 针对 WEP 的不足进行了改进，安全性比 WEP 有所提高。两者的差异主要在于：(1) WEP 没有提供有效的认证方式，WPA 使用 802.1x/EAP 来进行用户认证；(2) WEP 中的用户密钥是静态的，预先设置的，而 WPA 提供一套动态密钥管理系统；

(3) WEP 和 WPA 都采用 RC4 加密算法，WEP 的种子密钥由 40 位的用户密钥和 24 位的 IV 构成，而 WPA 的种子密钥由 128 位的密钥和 48 位的 IV 构成，并且要通过两次加密混合函数生成最终的加密密钥流；(4) WEP 采用 CRC-32 来进行数据完整性校验，WPA 中使用的是 MIC 机制。

WPA 是向 IEEE 802.11i (WPA2) 的过渡，两者都采用了基于 802.1x/EAP 的认证和动态密钥管理机制，它们的差异主要在于加密机制：WPA 采用了基于 RC4 加密算法的 TKIP 协议对数据进行加密，而在 WPA2 中 TKIP 是可选的加密机制，其默认的加密机制为基于 CCM 模式的高级加密算法 AES 的 CCMP 协议，并且不需要额外的完整性抵抗措施。WPA2 具有比 WPA 更高的安全性。

IEEE 802.11i 与 WAPI 都是采用基于端口的访问控制方式，它们的主要区别在于：(1) WAPI 实现的是

在STA和AP间的双向认证，802.11i只实现了STA和AS之间的双向认证；（2）WAPI仅使用公约证书作为身份凭证，802.11i通常采用口令或者数字证书等作为身份凭证；（3）WAPI认证与密钥协商部分脱节，缺乏密钥确认的过程，802.11i比较成熟，认证和密钥协商协议没有较大安全问题；（4）WAPI采用国密办规定认证的分组加密算法，802.11i采用 128 位的AES算法；（5）WAPI在STA和AP之间进行密钥协商，802.11i在STA与AS间协商密钥，STA与AP必须依赖与四步握手协议进行密钥确认等工作^[12]。

WEP、IEEE 802.11i、WAPI 三种 WLAN 安全机制的差异比较如表 1 所示。

表 1 三种 WLAN 安全机制差异表

安全机制	WEP	WPA2 (IEEE 802.11i)	WAPI
认证	开放式系统认证或共享密钥认证	基于 IEEE 802.1x/EAP 认证	WAI鉴别，基于椭圆曲线的公钥证书体制
加密	算法：64位的 RC4 密钥：静态	算法：CCMP（128位的 AES 算法），可选 TKIP（RC4算法） 密钥：动态（基于用户、基于认证、通信过程中动态更新）	算法：WPI加密 密钥：动态
完整性	CRC-32	CCM模式自带完整性保护，TKIP中为MIC	MIC

2.2 WLAN 安全机制缺陷

WEP 的安全缺陷主要有以下几个方面：（1）开放系统认证为空认证，允许任何用户接入，而共享密钥认证容易被破解，并且是单向认证，没有提供 STA 对 AP 的认证；（2）加密方式存在缺陷，如密钥流重用、弱密钥、密钥生成过于简单、对密钥的管理存在缺陷等问题；（3）CRC-32 不能提供有效的完整性保护。

IEEE 802.11i 是对 WEP 的改进，包含过渡阶段的 WPA 和成熟阶段的 WPA2，安全性比 WEP 大大增加。但其也存在着一定的安全缺陷，主要有以下几点：（1）802.1x 未能提供 STA 和 AP 之间的双向认证，易受到中间人攻击和会话劫持；（2）TKIP 仍采用较为薄弱的 RC4 加密算法，存在一定的缺陷；（3）TKIP 中的数据完整性保护机制 MIC 存在缺陷，易受到相关消息攻击，且在一定条件下 MIC 密钥可以被破解；（4）802.1x 的缺陷导致系统容易遭受拒绝服务攻击。

我国自主研发的 WAPI 具有较高的安全性，但其也存在以下几点安全缺陷：（1）STA 给 AP 发送数字证书时是以明文的方式发送，容易暴露 STA 的身份信息；（2）AUS 只验证 STA 证书的合法性，而不管证书的持有者是否合法，存在非法 STA 持有合法证书接入的可能性；（3）AP 向 STA 发送鉴别激活分组中没有相应的有效的身份信息，存在伪造 AP 的情况；（4）STA 与 AP 的密钥协商阶段以及密钥协商算法存在安全缺陷；（5）使用系统时间戳来抵抗重放攻击存在安全缺陷。

2.3 WLAN 安全机制理论研究的趋势

WEP 存在着诸多的安全缺陷，目前这种安全机制已经可易被完全破解，使用 WEP 机制实际上是不安全的。802.11i 虽然弥补了 WEP 种存在的安全缺陷，但其自身也并不是完美的。

文献 13 针对 IEEE 802.1x 缺乏请求者和认证系统之间的双向认证的安全缺陷从而可能导致受到中间人攻击和会话劫持而提出了改进方案。提出一种基于 802.1x 协议的改进方案，通过 RADIUS 服务器来实现客户端和 AP 之间的相互认证，有效阻止 EAP 上层协议采用单向认证的中间人攻击，同时在客户端建立 AP 信息表，使客户端有能力判断 EAP-Success 消息的真实性，有效地阻止 EAP 上层协议采用双向认证的中间人攻击即（EAP-Success 攻击），客户端和 AP 之间的相互认证结合客户端建立 AP 信息表能有效阻止会

话截取攻击，从而提高 802.1x 认证机制的安全性^[13]。

文献 14 在对 IEEE 802.1x 认证之后的四步握手协议进行分析的时候发现了其存在 DoS 漏洞，提出了一种可以减弱 DoS 攻击的改进方法，对原协议改动较小，易于实现。改进方法主要是针对消息 M1 没有采取任何保护认证措施，而导致很容易被伪装，从而产生 DoS 攻击提出的：在 M1 上采取保护认证措施，利用在 IEEE 802.1x 认证结束后 STA 和 AP 产生共同的 PMK，结合公钥机制来实现^[14]。

文献 15 回顾与分析了无线局域网的新一代安全标准 IEEE 802.11i 与四次握手协议。结合对实际协议的分析，指出四次握手协议的缺陷及可能带来的攻击，针对 802.11i 建议的方案及其局限性和仍然可能存在的攻击，提出了 STA 上使用 TKIP 随机丢弃队列进行 PTK 管理、对消息 1 进行身份认证两种改进方案，并对改进设计进行了验证与分析^[15]。

而针对目前 WAPI 存在的缺陷，国内的学者也提出了一些改进的方案。

文献 16 中，对 STA 身份认证问题以及密钥协商过程中 STA 和 AP 双方没有对已有的会话密钥进行确认的情况，提出了对 STA 启用数字签名，采用三次握手和 MIC 进行密钥确认来加强认证和密钥协商部分的安全性^[16]。

文献 17 中，对 AP 和 STA 间没有直接的认证机制从而容易造成中间人攻击的情况，提出了一种双策略的认证方式。双策略包括身份策略和签名策略，文章要求 AP 和 STA 在协议交互时，每个实体都要用证书和时间戳作为身份标识，证书表明实体的真实身份，时间戳保证身份数据的变化性；签名保证身份数据不被篡改，具有不可伪造性，签名增加私钥验证环节，具有不可抵赖性。根据双策略，AP 和 STA 交互协议中加入协议发起者的证书、系统时间和签名，从而保证认证接入的安全^[17]。

文献 18 对 WAPI 中的认证密钥交换协议 WAI 进行了安全性分析，指出存在的一些缺陷并作了相应的改进，给出了改进的 WAI 协议在 CK 安全模型下的安全证明。分析结果表明，WAI 具备 CK 安全模型下相应的安全属性，符合 WAPI 标准的要求^[18]。

2.4 WLAN 安全增强建议

除了选用有效的加密协议，并在条件允许的情况下对协议进行改进，我们还能从以下几个方面增强 WLAN 的安全性：（1）及时和定期修改无线接入点和路由器的管理员用户名和口令；（2）修改缺省的 SSID 网络名；（3）启用 MAC 地址过滤；（4）关闭 SSID 网络名广播；（5）关闭终端自动连接到开放 WLAN 的功能；（6）为网络设定静态的 IP 地址；（7）在每个计算机和路由器上启用防护墙；（8）合理选择接入点和路由器的摆放位置；（9）不用网络时，关闭网络。

3 电力物联网下的 WLAN 安全防护

WLAN 以其各种优势，将成为智能电网通信平台的重要组成部分。电力物联网下，WLAN 的应用前景十分广阔，WLAN 的构建可以扩大有线网络的覆盖范围，便于在郊外等不易构建有线网络的地方传输数据，确保安全、快速和可靠地接入企业内部网络，进行各种应用和资源存取。WLAN 能够减少国家电网公司的成本，提高生产效率，为实现“一强三优”现代公司的发展目标提供更为广泛、灵活的通信手段和网络平台。电力物联网下的 WLAN 安全防护问题是我们必须考虑的，可以从以下几点增强电力物联网下 WLAN 的安全性：（1）采用强健有效的 WLAN 安全协议，包括认证、数据加密、完整性保护三方面；（2）在技术条件允许的情况下，针对安全协议的缺陷进行改进；（3）隐藏 SSID，防止不明用户访问 WLAN；（4）物理地址过滤；（5）保护 AP 的射频信号，合理安置 AP 等设备；（6）非法 AP 的检测和定位；（7）无线网络内入侵检测和防护；（8）启用防火墙和防病毒软件；（9）为网络设置静态 IP；（10）经常更改 AP 和路由器的管理员用户名和口令。

4 结束语

随着智能电网的全面建设，WLAN 已被应用于电力通信之中，其安全问题也显得至关重要。为了保证电力物联网下的 WLAN 传输安全，我们必须选择合理的安全协议，并针对协议存在的缺陷进行研究和

改善,同时辅以其他方法全面提高 WLAN 的安全性。

参考文献:

- [1] 包广斌. WLAN安全体系结构研究与设计[D]. 兰州: 兰州理工大学, 2005.
- [2] 尤天晴, 刘洁. 无线局域网技术在智能电网中的应用研究[J]. 吉林电力, 2010,38 (2): 20-23.
- [3] 李静, 魏晓菁, 邹宇. 国家电网公司西单办公大楼无线局域网设计方案[J]. 电力信息化, 2006,4 (6): 54-57.
- [4] W.A.Arbaugh. An inductive chosen plaintext attack against WEP/WEP2[M]. IEEE Document 802.11-01/230, 2001-05.
- [5] Borisov N, Goldddberg I, et al. Security of the WEP Algorithm[D]. University of California at Berkeley, Feb. 2001.
- [6] IEEE Std 802.1x-2004. IEEE Standard for Local and metropolitan area networks-Port-Based Network Access Control[S]. LAN/MAN Standard Committee of the IEEE Computer society, 2004-02.
- [7] J.Walker. 802.11 Security Series-Part II:The Temporal Key Integrity Protocol(TKIP). Intel Corporation, 2002.
- [8] 欧阳亮, 陈春法. WLAN安全规范WPA的研究[J]. 计算机工程与设计, 2005,26 (11): 2986-2988.
- [9] IEEE Std 802.11i. Wireless Medium Access Control(MAC) and Physical Layer(PHY) Specifications[S]. July,2004.
- [10] Housley R, Whiting D and Ferguson N. Counter with CBC-MAC(CCM)[DB/OL]. <http://csrc.nist.gov/encryption/modes/proposedmodes/>, 2002-06-03.
- [11] 历丹, 张永平, 刘莘. 无线局域网中WAPI安全机制分析[J]. 计算机工程与设计, 2006, 27 (13): 2393-2395.
- [12] 张帆, 马建峰. WAPI认证机制的性能和安全性分析[J]. 西安电子科技大学学报(自然科学版), 2005, 32 (2): 210-215.
- [13] 赖胜枢. 无线局域网认证机制的分析与改进[D]. 中山: 中山大学, 2007.
- [14] 周世健. 基于串空间理论的无线网络安全协议分析与设计[D]. 南京: 东南大学, 2008.
- [15] 王小军, 陆建德. 基于802.11i四次握手协议的攻击分析与改进[J]. 计算机工程, 2007, 33 (3): 169-171.
- [16] 秦兴桥, 赵龙. WAPI安全性分析和改进[J]. 光盘技术, 2007 (1): 32-33.
- [17] 罗作民, 秦严等. 基于双策略的WAPI协议改进[J]. 计算机应用, 2009, 29 (2): 347-352.
- [18] 吴柳飞, 张玉清, 王凤娇. 一种新的WAPI认证和密钥交互协议[J]. 计算机工程, 2008, 34 (8),164-169.

作者简介:

华 晔 (1985—), 男, 江苏南京人, 工程师, 研究方向为网络信息安全, E-mail: huaye2@epri.sgcc.com.cn。