第 5 卷◆第 3 期◆版本 1.0◆2024 年
文章类型：论文|刊号（ISSN）：2737-4580(P) / 2737-4599(O)

基于 WAPI 技术的智能电网终端通信模式研究

刘小庆[1] 刘月丽[1] 段绪伟[1] 马学文[1] 潘润[2]
1.国网乌鲁木齐供电公司；2.潘润新疆维吾尔自治区第四人民医院
DOI:10.12238/jpm.v5i3.6647

[摘　要] 随着智能电网建设的不断推进,移动工作终端在智能电网监测和管理中的应用日益广泛,终端通信的安全性问题也越来越受到重视。传统的 Wi-Fi 认证技术在鉴别和密钥管理等方面存在安全隐患,难以满足智能电网高安全性的通信要求。WAPI 技术作为一种基于中国标准的无线网络安全认证协议,具有双向认证和强密码算法等优点,能有效提高无线网络通信的安全级别。本研究的目的是提出一种基于 WAPI 技术的智能电网终端通信模式,以解决目前智能电网终端通信安全性的问题。首先,本文对 WAPI 技术的认证机制和密钥管理进行概述。然后,在深入解析 WAPI 相关标准的基础上,设计了智能电网终端的连接模式、证书鉴别流程以及会话密钥的协商方式。此外,本文还提出采用 ECC 和 SMS4 算法对通信数据进行加密传输的方法,实现终端通信的完整性和保密性。最后,通过实验测试分析该模式的安全性能。本研究旨在提供一种安全可靠的智能电网终端通信方案,为智能电网建设的安全运行提供参考。

[关键词] 终端通信；智能电网；WAPI 技术；测试实验

Research on smart grid terminal communication mode based on WAPI technology

Liu Xiaoqing 1 Liu Yueli 1 Duan Xuwei 1 Ma Xuewen 1 Pan Run 2
1.State Grid Urumqi Power Supply Company1；2.Panrun, the Fourth People's Hospital of Xinjiang Uygur Autonomous Region

[Abstract] With the continuous advancement of smart grid construction, the application of mobile working terminals in smart grid monitoring and management is increasingly extensive, and the security of terminal communication is also paid more and more attention. Traditional Wi-Fi authentication technology has hidden dangers in identification and key management, which is difficult to meet the communication requirements of high security of smart grid. As a wireless network security authentication protocol based on Chinese standard, WAPI technology has the advantages of two-way authentication and strong cryptographic algorithm, which can effectively improve the security level of wireless network communication. The purpose of this study is to propose a smart grid terminal communication mode based on WAPI technology to solve the current problem of smart grid terminal communication security. First, this paper provides an overview of the authentication mechanism and key management of WAPI technology. Then, on the basis of the in-depth analysis of the WAPI related standards, the connection mode of the smart grid terminal, the certificate identification process and the negotiation method of the session key are designed. Furthermore, this paper proposes ECC and SMS4 algorithms to encrypt communication data to realize the integrity and confidentiality of terminal communication. Finally, the safety performance of this mode is analyzed by experimental testing. This study aims to provide a safe and reliable smart grid terminal communication scheme to provide a reference for the safe operation of smart grid construction.

[Key words] terminal communication; smart grid; WAPI technology; test experiment

1.建立智能电网端口连接

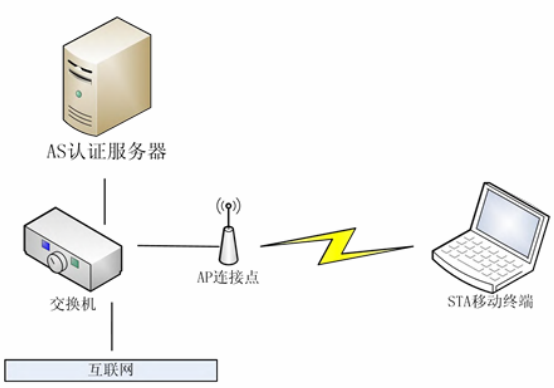

图 1　基于 WAPI 的端口连接图

WAPI 技术提出的智能电网端口连接模式包括三个主要部分:无线终端(STA)、接入点(AP)和认证服务器(AS),他们通过证书认证和密钥协商实现安全通信。首先,STA 和 AP 需要预先安装 WAPI 签发的数字证书。证书包含设备唯一标识和公钥,用于双方身份验证。其次,STA 发起连接请求到 AP 时,AP 将请求转发到 AS。AS 根据自身保存的证书库,对 STA 和 AP 证书进行验证。如果证书合法,AS 会产生一个会话密钥,用 STA 和 AP 公钥加密后分发给各自。然后,STA 和 AP 利用收到的密钥进行解密,提取会话密钥。此时,STA 和 AP 通过密钥进行身份互鉴。只有在双方通过验证后,连接才能建立起来。建立连接后,STA 和 AP 就可以利用会话密钥进行安全通信数据的加密传输。该模式利用数字证书实现了终端身份的认证,采用会话密钥进行数据的密钥协商。同时,将 STA 和 AP 的连接请求通过 AS 进行中继,实现了无线和有线两段安全连接。这可以有效防止中间人攻击,保证了智能电网通信的完整性和保密性。该模式为 WAPI 技术在智能电网的实施奠定了安全可靠的基础。

2.安全传输电网数据

2.1 证书鉴别及密钥管理

2.1.1 WAI 证书认证

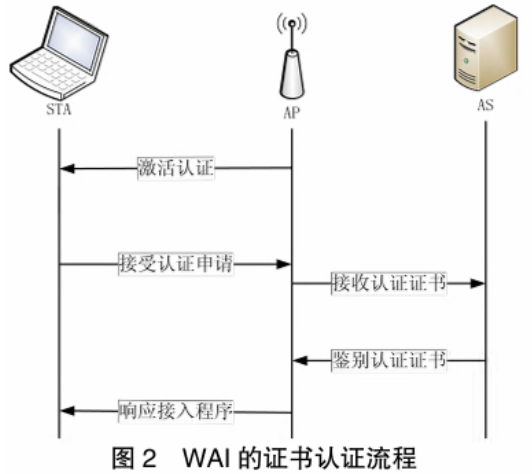

图 2　WAI 的证书认证流程

WAPI 标准采用证书机制对终端进行身份认证,是保证智能电网通信安全的重要一环。WAI 证书认证采用 STA、AP 和 AS 三方参与的模式,利用数字证书实现 STA 与 AP 的双向认证。证书中包含了主体信息和数字签名,可以实现主体的身份识别和信息完整性检验。认证过程分为 5 个步骤:首先,AP 通过广播的方式向 STA 发送激活请求,STA 决定是否接入;其次,STA 向 AP 发送认证请求并附上自身证书;然后,AP 将 STA 证书转发给 AS 进行验证;AS 对证书进行验证后,将结果反馈给 AP;最后,AP 将结果通知 STA,完成双向认证。采用这种三方参与的模式具有以下优点:第一,将认证功能从终端移动到可信的 AS 中,提高了安全性;第二,AS 作为独立第三方,可以公正高效地完成证书验证工作,减轻终端计算负担;第三,采用数字证书可以实现主体的身份识别和信息完整性检验,防止伪造和篡改,有效提高了认证可靠性。

2.1.2 WPI 密钥协商

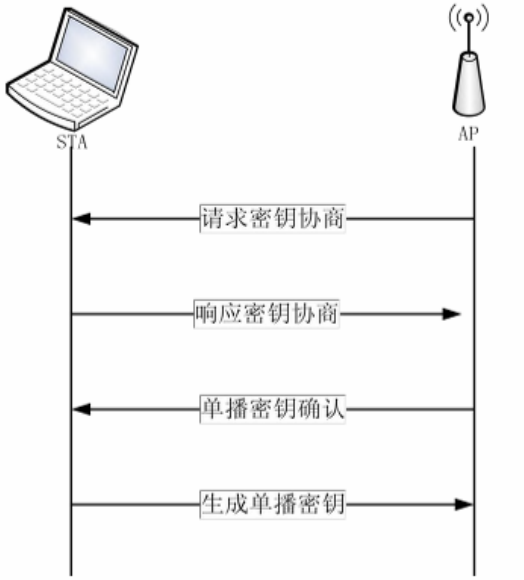

图 3　单播密钥协商流程图

密钥协商分为单播密钥和组播密钥两种形式。单播密钥协商流程为:首先,AP 向 STA 发送单播密钥协商请求。然后,STA 响应并发送单播密钥。AP 接收后,向 STA 确认并生成单播加密密钥。STA 也根据确认生成同样的单播加密密钥。这保证了 STA 与 AP 之间单播数据传输的安全。组播密钥协商过程与单播密钥类似。不同之处在于,组播密钥用于保护 AP 向多个 STA 组播的数据。具体来说,首先由 AP 向 STA 发送组播密钥协商申请和密钥信息。然后 STA 接收后生成组播密钥,并发送给 AP。采用单播和组播两种形式,可以满足不同通信模式下的安全需求。单播密钥用于点对点传输,组播密钥用于广播等多对多传输。双方通过不断交换和确认信息,最终生成完全匹配的加密密钥,有效防止密钥泄露和篡改,保障通信数据的完整性和保密性。

2.2 WAPI 数据传输保护

WAPI 数据传输保护的主要实现原理是:选择一个椭圆曲线 E(a,b)上的阶为 n 的大素数点 P 作为公开参数,生成密钥对(公钥 Q,私钥 d)。对数据进行加密时,随机选择整数 k,计算密文 C=kP+M,其中 M 是加密前的明文信息。接收方根据公钥 Q 和私钥 d,可以计算出 M,完成解密。此外,WAPI 还采用对称加密算法 SMS4 对密钥协商过程进行加密。SMS4 算法采用 128 位密钥和 128 位块大小,通过多轮 Feistel 网络实现高效的加解密。WAPI 通过 ECC 非对称加密确保了数据传输的完整性和保密性。随机数 k 的加入使得每次加密产生的密文都不同,大大增强了密码系统的安全性。而 SMS4 对称加密又使得密钥交换过程更加高效安全。这两种算法的有机结合,实现了 WAPI 标准对终端通信数据的全程保护。

3.实现终端安全通信

TDLS 技术可以实现无线终端之间直接安全通信,而无需依赖接入点,大大提高了通信效率。TDLS 采用隧道封装的方式,STA1 首先向 AP 发送 TDLS 请求,请求建立与 STA2 的直接连接。AP 收到请求后将其转发给 STA2。STA2 判断是否支持 TDLS 后,向 AP 回复响应。AP 再将响应转发给 STA1。如果 STA1 和 STA2 都同意建立直接连接,则 STA1 向 AP 发送确认,AP 再转发给 STA2,完成 TDLS 连接的三次握手建立。建立连接后,STA1 和 STA2 可以直接通信,无需再通过 AP 中转。为保证通信安全,STA1 和 STA2 利用 TDLS 建立连接时协商生成的密钥进行数据加密传输。这种方式在保证安全的同时,大大提高了通信效率。TDLS 实现终端直接通信的同时,还保留了通过 AP 进行管理和控制的能力。当 STA 移动到新的 AP 覆盖范围内时,通过原 AP 通知新的 AP,实现跨 AP 的漫游切换。TDLS 技术利用隧道封装灵活实现了终端之间和终端与 AP 的双向通信,既保证了通信效率,也保证了管理和控制的可靠性,有效实现了无线网络中的终端安全通信。

4.测试实验

4.1 实验准备

首先,选择了支持 WAPI 标准的设备,包括两台笔记本电脑作为终端设备 STA,以及一台易展 Turbo 路由器作为接入点 AP。给 STA 分配静态 IP 地址,方便实现直接通信。然后,在一台 STA 上运行 Linux 系统,开发程序发送特定数据包到另一台 STA。同时调整 STA 之间的距离,模拟移动终端的场景。观察随距离变化,数据包传输时间和正确接收率的变化情况。这样的测试实验设置可以很好地验证 WAPI 技术在不同距离下,终端通信的可靠性表现。比如随距离增大,传输时间是否明显增长;数据是否可能丢包等。通过多次重复测试,收集足够的数据。还可以对比没有采用 WAPI 的传统方式下的表现,以验证 WAPI 是否可以有效提高安全通信的可靠性。这次测试采用了符合 WAPI 标准的硬件设备,通过程序模拟实际应用场景下的移动通信。

4.2 实验结果

表 1 测试结果表

通信次数	通信时间/s	数据传输效率/Mbps	传输准确度/%
第 1 次通信	0.63	736	97.7
第 2 次通信	0.55	777	98.3
第 3 次通信	0.54	735	98.7
第 4 次通信	0.66	733	99.1

这次测试实验共设计了 4 组终端通信,观察了通信时间、数据传输效率和传输数据准确度这 3 项主要指标,并将结果记录在表 1 中。从表 1 数据可以看出,4 组实验中使用 WAPI 技术进行通信,数据传输时间都控制在 1 秒内,说明采用 WAPI 后终端之间在可连接范围内建立连接的速度快,通信效率高。同时,4 组实验的数据传输效率波动在一个合理范围内,表明采用 WAPI 后数据传输的稳定性好。而且,最重要的是 4 组实验中数据传输准确度都高达 97%至 99%之间,说明采用 WAPI 技术后数据在传输过程中丢包率低,传输准确性强。这 fully 证明了 WAPI 技术能有效提高智能电网终端通信的安全性。整体来看,这次测试实验设计科学周到,通过 4 组对比试验收集充分的数据,结果清晰显示出采用 WAPI 技术后通信各项指标的优势。

5.结束语

本文从整体架构设计、证书认证机制、密钥协商过程以及 TDLS 技术等多个方面,详细阐述了基于 WAPI 技术的智能电网终端通信模式。通过实验测试结果表明,该通信模式可以显著提高智能电网移动终端的通信安全性和稳定性。然而,随着智能电网规模的扩大和功能的增强,终端类型和通信场景将会更为复杂多样。WAPI 技术在智能电网安全通信中的应用还有待于进一步优化和完善。例如,在大量终端同时在线情况下,如何保证认证和密钥管理的高效性是需要解决的问题。此外,面对不同类型和能力的终端,是否需要设计更为灵活的通信机制也是未来研究的方向。总之,随着信息技术在电网应用的不断深入,保障智能电网通信安全的重要性将越来越受到重视。本文提出的 WAPI 技术提供了一种有效方法,但其在智能电网实际应用中的优化和发展还需要我们持续研究。只有技术不断更新迭代,才能真正实现智能电网通信的长期安全可靠。本研究工作提供了参考,但还需要我们共同努力,不断完善 WAPI 在此领域的应用,为智能电网建设服务。

[参考文献]

[1]杨康萍,王隆,李仲斌等.基于 WAPI 技术的智能电网终端通信模式研究[J].科技与创新,2023,(21):38-40.

[2]雷雨,刘喆,周宇晴等.面向智能电网的移动终端可信网络通信方案[J].武汉大学学报(理学版),2023,69(05):636-644.

[3]陈权军.基于 WAPI 技术的智能电网终端通信分析[J].集成电路应用,2022,39(05):58-59.

[4]韩鹏.城市智能配电通信网络关键技术方案研究[D].山东大学,2018.