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 S-WAPI 的无线 Mesh 网络认证系统研究

刘月丽[1] 段绪伟[1] 刘小庆[1] 姜威威[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.v5i3.6639

[摘　要] Mesh 网络具有自组织和自管理的特点,但信息在网络中的传输缺乏有效的保密机制,给用户带来隐私安全隐患。WAPI 协议应用在 Mesh 网络中提高了安全性,但集中式认证机制需要进一步优化。本研究针对 Mesh 网络用户隐私安全问题,提出了基于改进的 S-WAPI 协议的无线 Mesh 网络集中式认证测试系统。该系统采用中心认证服务器,对网络中的所有设备进行身份认证管理。认证服务器与网络中的各节点通过安全通道进行通信,并采用对称加密算法对重要信息进行加密传输,有效防止信息泄露。
[关键词] 无线 Mesh 网络；网络安全；S-WAPI 协议

Research on Wireless Mesh Network Certification System Based on S-WAPI

Liu Yueli 1 Duan Xuwei 1 Liu Xiaoqing 1 Jiang Weiwei 1 Pan Run 2
(State Grid Urumqi Power Supply Company) 1
(Panrun, the Fourth People's Hospital of Xinjiang Uygur Autonomous Region) 2

[Abstract] Mesh network has the characteristics of self-organization and self-management, but the transmission of information in the network lacks an effective confidentiality mechanism, which brings hidden privacy and security risks to users. WAPI protocol application improves security in Mesh network, but the centralized authentication mechanism needs to be further optimized. This paper proposes a centralized authentication test system for wireless Mesh network based on the improved S-WAPI protocol to address the privacy security problem of Mesh network users. The system adopts the central authentication server to conduct identity authentication management for all devices in the network. The authentication server communicates with each node in the network through the secure channel, and uses the symmetric encryption algorithm to encrypt and transmit the important information to effectively prevent information leakage.
[Key words] wireless Mesh network; network security; S-WAPI protocol

1.无线 Mesh 网络的概述

无线 Mesh 网络作为一种新型的无线网络架构,具有自组网能力强、覆盖范围广泛、网络健壮性高等优点,这为其在移动互联网应用提供了广阔的发展前景。无线 Mesh 网络采用分布式结构,每个节点都可以作为路由器参与数据转发,使网络覆盖范围不再限于单个接入点。这一特点使其在需要覆盖广大区域的场景下具有明显优势,如城市公共场所、校园等。此外,Mesh 网络采用多跳传输,如果某一节点故障,数据包可以选择其他路径转发,整个网络不会瘫痪,有很强的自我修复能力,网络稳定性较好。但是,Mesh 网络作为一种新兴技术,在实际应用中也面临一定挑战。首先,分布式网络中,节点间通过无线通信传输数据,容易产生空口拥塞,需要设计合理的空口协调机制来优化网络性能。其次,分布式网络中每个节点的独立性较弱,需要对节点进行唯一标识管理。此外,节点间通过无线传输数据存在信息安全隐患,需要采用强密码算法对通信进行加密保护。

除此之外,Mesh 网络的实时性能也需要进一步优化。在不同应用系统资源间需要设计开放性强的统一交互机制,同时需要对网络进行充分容量评估,选择适合特定应用场景的终端设备,以优化传输效率和稳定性。只有充分认识到 Mesh 网络在技术应用上的难点和挑战,采取 targeted 的技术改进,例如对网络拥塞控制、节点管理、信息安全等关键技术进行研究,并

通过实验测试进行验证,Mesh 网络才能在移动互联网领域真正发挥其应用潜力,开拓广阔应用前景。

2.WAPI 的分析和改进

WAPI 全称是 Wireless Authentication and Privacy Infrastructure,它作为无线局域网鉴别和保密基础结构的安全协议标准,同时也是中国无线局域网安全的强制性标准。WAPI 是专门针对原有 WEP 协议在安全方面的缺陷而研发出来的。WAPI 标准通过两个基础结构来实现无线局域网设备的安全认证和数据传输的加密保护。一个是无线局域网鉴别基础结构 WAI,它主要用于实现无线设备的实体认证;另一个是无线局域网保密基础结构 WPI,它负责对无线数据传输进行加密保护。通过 WAI 和 WPI,WAPI 标准得以实现无线局域网的安全认证和数据通信保密功能。但是,尽管 WAPI 标准解决了 WEP 协议的安全问题,但在实际应用和研发过程中,WAPI 自身也暴露出一些固有的安全缺陷。首先,WAPI 采用的是自主研发的加密算法,这与国际标准有差异,不利于与国际标准的兼容。其次,WAPI 标准本身在算法强度和密钥管理等方面存在一定程度的安全隐患,无法完全防范各种攻击。此外,WAPI 标准缺乏完善的安全审计机制,难以及时发现和修补潜在的安全漏洞。最后,WAPI 对不同厂商的无线网卡也不具有很好的兼容性,给用户和设备提供商带来一定不便。为了解决 WAPI 标准自身的这些安全缺陷问题,提出了 S-WAPI 改进方案,旨在在保留 WAPI 基础结构的同时,通过技术改进来增强 WAPI 的整体安全性能。

2.1.证书数据结构方面

在 WAPI 标准的数字证书数据结构设计中,存在一个较大的问题,就是证书中包含大量不定长字段,这对证书的编码和解码工作造成很大影响。具体来说,WAPI 数字证书结构中,字段长度非常长的颁发者名称和持有者名称字段,以及其他一些可变长度字段,分布在证书结构中无规律且顺序混乱。这就给证书的编码和解码带来很大困难。比如在编码时,需要反复计算字段长度以确定下一个字段的偏移位置;解码时也需要逐个读取字段才能分辨出每个字段的内容。这对系统资源的占用率和工作效率都有很大影响。S-WAPI 通过对 WAPI 证书结构进行优化,解决了这个问题。它的主要改进措施如下,S-WAPI 将证书结构中定长字段部分向前移动,放在结构体首部;其次,S-WAPI 精确定义和简化了原 WAPI 中各可变长度字段的含义,减少了重复字段;最后,S-WAPI 增加了总长度字段,用来标识整个证书结构的总字节长度。通过这些改进,S-WAPI 使证书结构更加简洁明了。它规范了字段顺序,并通过总长度字段直接定位各个字段,这大大提高了证书编码和解码的效率。这使得数字证书在 S-WAPI 标准下可以实现更快速高效的处理,从而提升了整体系统性能。

2.2.WAPI 鉴别协议方面

首先,S-WAPI 在各个鉴别阶段都对数字证书和信息进行数字签名,实现真实身份的双向鉴别。而原 WAPI 标准仅发送未签名的证书,难以识别对方身份,存在欺骗风险。其次,S-WAPI 在密钥协商阶段加入了流量控制机制。它可以识别恶意客户发送大量无效请求,限制其请求频率,避免因流量攻击导致网络瘫痪。这样保护了网络资源,提高了系统可靠性。另外,S-WAPI 标准还增加了会话密钥确认过程。即在证书鉴别成功后,协商方会对互相协商生成的会话密钥进行数字签名确认,这可以有效防止中间人攻击。例如防止恶意客户在协商过程中修改会话密钥而导致数据泄露。

2.2.1.各项网络数据创新融合

需要设计出一套统一的网络数据格式标准,这套标准需要兼容不同业务部门采集到的各类终端电力通信数据。它可以为电量、温度、流量等各类原始数据设计标准字段,为位置、时间戳等附加信息设计标准字段,以此来统一不同数据的结构。其次,在系统存储层面实现这套标准的格式转换。对采集到的各项原始数据进行解析提取,按标准的字段填充进行结构化处理,然后存储。同时在本地 IP 地址管理模块中,增加对地址前缀的快速识别和标准格式的转换功能,实现本地和远程网络地址的兼容。最后,在网络层增加对标准数据格式的识别和解析能力。它可以从存储层面提取并解析结构化后的数据,实现主动推送给上层应用或被动响应上层查询,为上下游系统和业务提供统一规范的接口,从而保证不同系统和部门在数据交互过程中的高效协调。通过上述方式,可以在保障各项原始数据特征的同时,实现不同网络数据在结构和格式上的创新融合,有效支撑无线 Mesh 系统网络的多业务协同运维。

2.2.2.系统接入和组网技术的创新融合

在系统接入端口号管理模块中,增加对各类通信协议的动态识别能力。它可以识别数据包中的传输层和应用层协议类型,然后快速匹配到对应的系统接入端口进行进一步处理。在安全认证模块中增加对多种加密算法和用户权限验证方式的支持。它可以根据业务特点和安全级别,动态选择最佳的加密算法进行数据传输,或灵活结合多个权限因素进行多级验证,提高安全性。同时,需要在组网设备中增加对不同网络类型的快速识别能力。它可以识别数据包来源是否为本机 LAN,还是公网 WAN,然后选择内外网地址进行匹配转发。另外,也要增强数据传输控制模块的智能性。它可以根据网络拥塞程度,动态调整数据

发送速率和包大小,保证实时性较高的控制类业务优先传输。

2.2.3.软件信息资源交换机制的融合应用

首先,需要在通信控制层面实现不同级别系统间数据的交叉传输。比如让分布式能源和次级变电站系统的数据,不再仅限于上级能源管理系统传输,同时允许下级电网公司直接访问,简化传输路径。其次,可以在资源共享模块中,增加跨系统资源调用功能。例如给变电站系统提供分布能源运行数据查询接口,给能源公司提供电网负荷数据监测接口,实现资源双向开放共享。此外,还要优化通信传输流程控制。例如采用异步传输机制,允许业务查询直接发送到目的系统,而不必等待上级系统中转,大幅简化流程。同时,还要增强各个系统的自我适应调度能力。让系统能根据当前通信拥塞状况,自动调整查询频率和包传输速率,保证关键业务优先高效传输。

3.无线 Mesh 网络的网络认证系统

在搭建无线 Mesh 网络的过程中,合理设计电力数据资源的采集方式和分布式存储管理形式,是保障电力系统运维管理和通信网络稳定运行的重要一环。首先,在数据采集方面,可以根据不同级别电力设备的功能特点,采用多种方式同时采集。例如对于变电站等重要设备,可以实时采集重要运行参数;对于分布式能源等,则采用间歇采集主要数据。此外,还可以结合物联网技术采集环境和外部条件数据。其次,在数据存储上可以采用分布式和层次式结合的形式。重要实时数据如变电站运行数据在本地进行实时存储,同时同步上传到上级能源管理系统。其他参数数据则采区域分布式存储管理,通过 Mesh 网络相互传输调用。另外,不同级别系统还可以设置私有云区域,实现跨系统资源共享调用。如给变电自动化系统提供能源预测数据服务。最后,需要建立完善的安全管理机制。

3.1.无线 Mesh 网络的应用场景

有可信任第三方参与的 Mesh 网络,适用于长期稳定运行的场景,如智慧城市建设。它采用数字证书验证节点合法性,保证个人信息安全传输。这对需要长期运营的城市信息系统、能源通信等重要基础设施来说是必需的。而没有第三方参与的 Mesh 网络,适用于应急救援等临时性场景。比如发生地震、洪水等自然灾害时,可以快速在受灾区部署这类 Mesh 网络,实现初期通信联系。由于没有中心节点,它具有高度弹性和可扩展性。只需少量设备,就可以在受灾地创建一个临时的无线网络。这为救援工作提供了重要支撑,可以及时传达指令,搜寻生还者等,大大缩短救援时间。总之,两种 Mesh 网络各有优势。需要根据实际应用环境,选择合适的模式。长期基础设施应用需要第三方认证保证安全;而临时应急救援场景,由于时间紧迫,采用无中心化的 Mesh 网络更高效。

3.2.S-WAPI 协议的实施方案

S-WAPI 是我国针对无线局域网安全的一套标准,它在无线 Mesh 网络中的实施方案主要包括以下几个方面:

3.2.1.ASU(Authentication Server Unit)的设计。

ASU 承担数字证书的管理和鉴别工作,它由证书管理模块和鉴别模块组成。证书管理模块负责证书的发行、更新、撤销等管理工作;鉴别模块支持数字证书和预共享密钥两种鉴别模式,对通信中的身份进行验证。

3.2.2.数据存储设计。

根据数据分类,将用户信息、证书信息、密钥对等数据分别存储在不同的数据库中,便于管理。同时设计了分布式存储架构,利用数据中心对各数据库进行集中管理和控制。

3.2.3.鉴别与加解密模块。

鉴别模块支持 WAPI 认证和密钥管理;加解密模块通过对称加密算法对数据进行加密与解密,保护通信安全。

3.2.4.实施工具支持。

利用开源软件如 OpenSSL 提供加解密算法支持;Netfilter 和 Netlink 框架支持数据包的过滤转发;Socket 编程接口支持设备间的通信。

3.2.5.认证测试。

采用集中式认证模式,由 ASU 服务器集中进行节点认证。测试时先搭建了由 5 台服务器组成的 ASU 认证中心。然后在 Mesh 网络节点初始化时,通过 ASU 验证节点合法性,为后续通信奠定基础。

4.结束语

综上所述,S-WAPI 标准为我国无线 Mesh 网络的数据传输提供了安全保障。本文设计实现了基于 S-WAPI 的无线 Mesh 网络集中式认证测试系统。测试结果表明,该系统能够有效地完成节点的身份鉴别与管理任务。但是,随着网络规模的扩大,集中式认证也将面临一定挑战。未来值得我们进一步研究的方向是,设计一套更适应大规模网络的分布式认证架构。

[参考文献]

[1]崔晨,孙严智,田丰等.基于 S-WAPI 的无线 Mesh 网络认证系统研究[J].产业与科技论坛,2023,22(12):37-38.

[2]李计.基于 S-WAPI 的无线 Mesh 网络认证系统研究[D].北京交通大学,2011.

[3]毛风鹏.基于 WAPI 的无线 Mesh 网络认证系统[J].科技信息,2010,(34):637.