

一种基于EPON的配网自动化通信加密方案

文/国网信通产业集团北京智芯微电子科技有限公司 汪波涛

配网通信系统作为配电自动化各类信息传输的载体，支撑配电自动化、电动汽车充换电站、充电桩、配变监测、智能台区、分布式能源接入、微网接入、智能巡检及配电房环境监控等业务。由于与其他技术相比，EPON技术在组网可靠性、带宽可分配、维护成本低、网络可扩展性等方面均有优势，适用于对可靠性有较高要求的配用电接入应用。

基于EPON的配网自动化架构

1. 配网EPON系统架构

基于EPON技术的配电自动化典型应用场景如图1所示，在变电站部署光线路终端OLT，在环网柜、小区配电房、柱上变压器、充电站、分布式能源、营业厅等接入点部署光网络单元ONU，通过以太网口与业务终端连接，可承载配电自动化、用电信息采集、电能质量监测、分布式能源（10 kV）、电动

汽车充换电服务系统、配变监测、微网、配电线路视频监控、智能台区、营业厅等业务，各业务终端可以根据地理位置情况接入一台或多台ONU，经光纤信道和OLT接入骨干数据网。

2. 配网EPON系统存在的问题

随着配网通信系统承载的业务类型越来越多，数据容量越来越大，配电各终端与后台主站信息交互不断增强。当前EPON系统采用

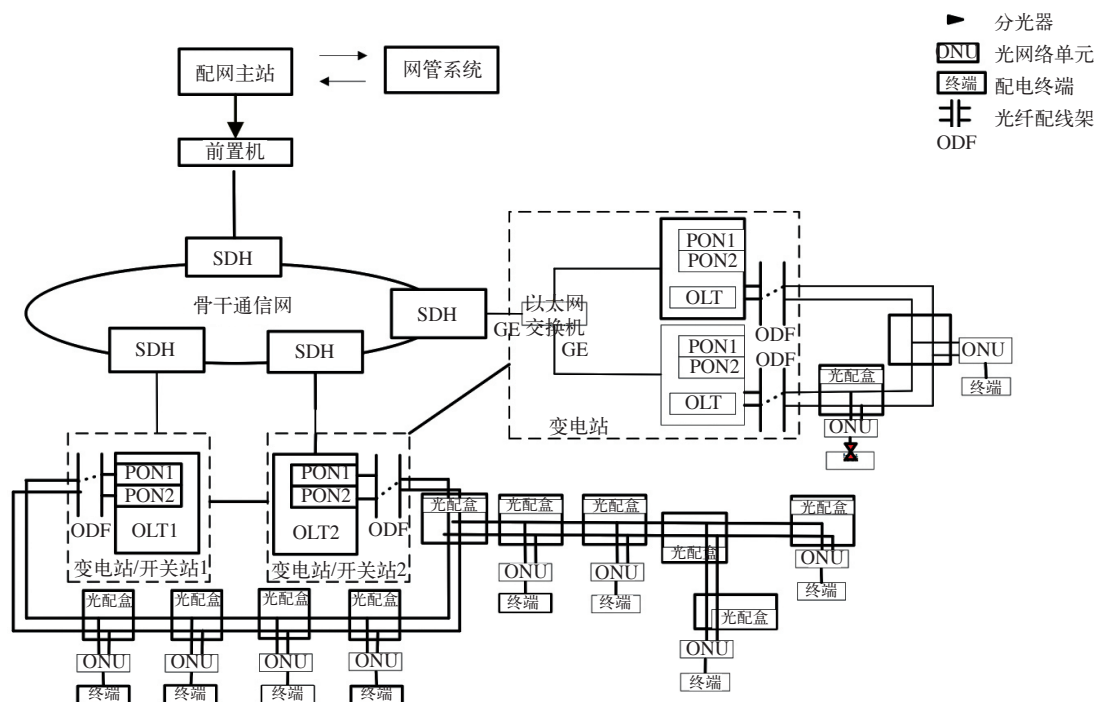


图1 基于EPON的配网自动化架构

自动发现、自动注册机制所带来的安全隐患如图2。保证底层终端接入网络，防止非法访问，保证配网自动化通信系统的信息安全成为必须解决的问题。在EPON系统中，下行数据传输采用广播方式，网络中的每一个ONU都能接收到所有下行数据，存在数据泄露风险。

EPON MPCP具有自动发现、注册功能，对于新加入的ONU，存在非法注册和伪装注册问题。恶意的ONU可以向EPON网络系统发送大量有效或无效的信息，造成网络堵塞。即自动发现和注册过程中非法ONU自动注册到OLT；非法入侵ONU假装合法的ONU发送数据从而威胁正常的EPON系统通信。

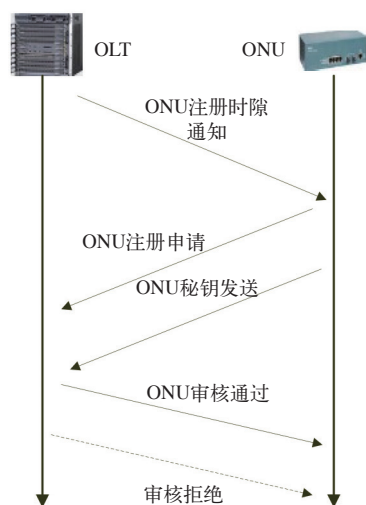


图2 MPCP注册的简单加密认证过程

配网EPON主动加密方案

1. 主动加密方案

802.3ah中规定的三重搅动加密算法。是一种基本的加密方法，无法保证上行方向的数据具有安全性。针对目前配网通信存在的问题，需要可靠的加密手段来保证配网EPON系统的安全性。

本项目提出一种ONU解决方案，通过改进目前EPON系统的发现、注册机制，增加终端认证、用户鉴权、数据加密功能，同时划分VLAN实现信息数据物理隔离。保

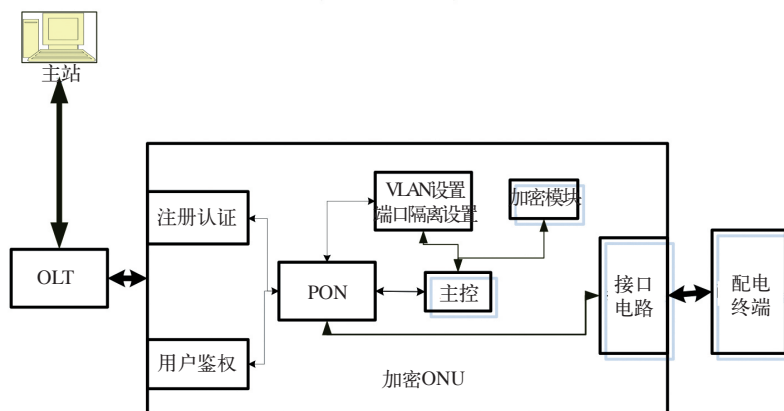


图4 配网EPON主动加密实现原理框图

证非法终端无法接入网络，数据不被篡改。具体是：

(1) 在ONU发现、注册阶段和数据通信时两个阶段均采用鉴权机制。在发现、注册状态，对将要接入的ONU进行鉴权认证，通过认证才允许该ONU注册通过。接下来，在数据通信过程中，对用户进行鉴权，确认通信方是否为合法用户。

(2) 数据通信过程，对合法用户信息进行加密。采用国密SM1算法，兼容现有“三重搅动”等加密算法，保证接入设备间的数据传输安全性。每个LLID（逻辑链路连接标识）具有独立的密钥。

(3) 通过VLAN划分、端口隔离设置，实现ONU报文之间的链路层隔离。如图3所示。

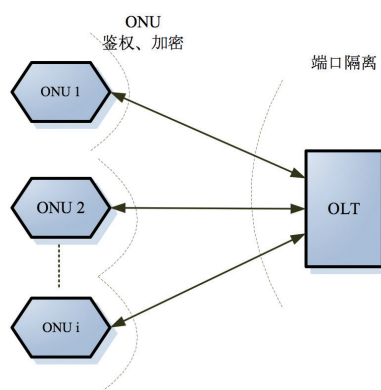


图3 EPON主动加密方案

2. 方案实现

EPON主动加密方案实现原理如图4所示。主站下行和终端上行

数据主控模块。通过主控模块设置数据的加密、VLAN划分、端口配置等。接口电路具有以太网口、URAT口形式，连接配电终端。数据通信加密过程可描述如下：

(1) 主站与终端通信交互数据由主控模块判断是否为加、解密数据；

(2) 加、解密过程处理由主控模块负责与主站交互进行；

(3) 主控模块与配电终端之间只进行应用层透明的数据报文通信；

(4) 主控通过接口与加密模块进行加密算法、密钥的交互。

ONU加密、解密采用TCP端口隔离的方式。主控在内部建立一个CLIENT和SERVER端。主控的CLIENT端与主站（SERVER）进行连接，CPU的SERVER端和终端（CLIENT）进行连接。主控的CLIENT端接收到主站的下行数据，进行解密然后再通过SERVER端发送；主控的SERVER端接收终端发送的上行数据，将信息进行加密再通过其CLIENT端发给主站。

结束语

该方案能有效解决配网EPON系统中数据泄露、篡改以及身份认证问题，对于提高配网通信系统信息安全具有较好的作用，为智能配电系统的建设与发展提供了技术支撑。EA