[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 29/06 (2006.01)
H04Q 11/00 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200610078931.9

[43] 公开日 2007 年 10 月 31 日

[11] 公开号 CN 101064719A

[22] 申请日 2006.4.27
[21] 申请号 200610078931.9
[71] 申请人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为总部办公楼
[72] 发明人 杨 敏 高 海 吴 炜

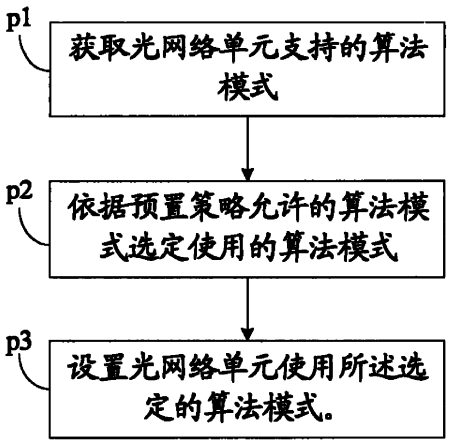
[74] 专利代理机构 北京集佳知识产权代理有限公司
代理人 逯长明
权利要求书 2 页 说明书 11 页 附图 3 页

[54] 发明名称

PON 系统中加密算法协商方法

[57] 摘要

本发明公开了 PON 系统中加密算法协商方法，该方法包括步骤：获取光网络单元支持的算法模式；依据预置策略允许的算法模式选定算法模式；设置光网络单元使用所述选定的算法模式。 本发明可以提供在系统配置过程中多种加密算法模式的算法协商过程方法，通过改进现有协议，实现多种加密算法并存的应用需求，提高产品的兼容性。



1. PON 系统中加密算法协商方法，其特征在于，包括步骤:

1）获取光网络单元支持的算法模式;

2）依据预置策略允许的算法模式选定算法模式;

3）设置光网络单元使用所述选定的算法模式。

2. 根据权利要求 1 所述的方法，其特征在于，所述步骤 1)获取的过程包括:

11）发送获得支持算法模式的命令到光网络单元;

12）光网络单元反馈支持的算法模式。

3. 根据权利要求 1 所述的方法，其特征在于，所述步骤 1）获取的过程包括:

当光网络单元属性值变化的时候，所述光网络单元通过属性值变化 AVC 消息上报支持的算法模式。

4. 根据权利要求 3 所述的方法，其特征在于，所述光网络单元上报支持的算法模式之前，包括:

c1）发送复位命令到光网络单元;

c2）光网络单元响应复位结果。

5. 根据权利要求 1 所述的方法，其特征在于，所述预置的策略包括: 依据不同国家、不同地区或不同网络运营商而采用的不同使用标准。

6. 根据权利要求 1 所述的方法，其特征在于，所述步骤 2）选定的过程包括:

判断所述允许的算法模式和所述光网络单元支持的算法模式是否有相同的算法模式，如果是，从所述相同的算法模式中选定算法模式，否则，作为协商失败处理。

7. 根据权利要求 6 所述的方法，其特征在于，所述协商失败处理过程包括:

从所述允许的算法模式中选定算法模式; 或将不表示任何实际算法的无效算法模式作为选定的算法模式，所述无效算法模式使用特定形式的值表示。

8. 根据权利要求 1 所述的方法，其特征在于，所述步骤 3）设置的过程包括:

31）发送包括所述选定的算法模式的设置命令到光网络单元;

32）光网络单元回应设置结果。

9. 根据权利要求 1～8 其中之一所述的方法，其特征在于，使用连续的取值表

示所述算法模式。

10. 根据权利要求 1～8 其中之一所述的方法，其特征在于，使用比特 bit 表示所述算法模式。

PON 系统中加密算法协商方法

技术领域

本发明涉及光通讯领域无源光网络技术，尤其涉及 PON 系统中多种加密算法协商过程的方法。

背景技术

目前接入网领域在 DSL 充分发展的时候，光接入技术也得到蓬勃的发展，尤其以点到多点传输为特征的光接入技术——PON（Passive Optical Network，无源光网络）再次受到业界的瞩目。与点到点光接入相比，PON 局端用一根光纤，即可分成数十甚至更多路光纤连接用户，大大降低建网成本。

请参考图 1，PON 系统由三个部分组成：OLT（Optical Line Termination，光线路终端）、ODN （Optical Distribution Network，光分布网）和 ONU/ONT（Optical Network Unit，光网络单元/ Optical Network Termination，光网络终端）。

OLT 为 PON 系统提供网络侧接口（SNI），连接一个或多个 ODN。无源分光器件，将 OLT 下行的数据分路传输到各个 ONU，同时将多个 ONU/ONT 的上行数据汇总传输到 OLT。ONU 为 PON 系统提供用户侧接口(UNI)，上行与 ODN 相连，如果 ONU 直接提供用户端口功能，如 PC 上网用的以太网用户端口，则称为 ONT。

无特殊说明，本说明书提到的 ONU 包括 ONU 和 ONT。

在 PON 系统中，从 OLT 到 ONU 称为下行，反之为上行。下行数据方式为 OLT 广播到各 ONU，ONU 的上行数据方式为由 OLT 分配发送区间，数据经时分复用后上传到 OLT。

PON 技术包括 BPON（Broadband Passive Optical Network，宽带无源光网络），GPON （Gigabit Passive Optical Network，Gbit 无源光网络）等，GPON 是在 BPON（Broadband Passive Optical Network，宽带无源光网络）的基础上继承发展的，是当前几种 PON 中技术最全面的、最成熟的技术，具有线路速率高、维护管理完善等优点。BPON 和 GPON 都是由国际电信联盟（ITU-T）制定的。BPON 只支持 ATM 信元的承载，而 GPON 支持承载 ATM 信元，也

支持适应于 IP 数据的 GEM 封装。它们具有相似的管理模式，例如使用同样的 OMCI（ONT management and control interface，ONT 管理控制接口）管理协议和近似的 PLOAM（Physical Layer OAM，物理层 OAM）消息机制。BPON 和 GPON 标准中的 OMCI 分别在 G983.2 和 G.984.4 中定义，其中 G.984.4 是对 G983.2 的继承和补充。

请参考图 2，是 GPON 协议栈模型。GPON 标准协议将物理介质以上分为 GPM 层（G-PON Physical Media Dependent Layer，GPON 物理介质相关层）和 GTC 层（G-PON Transmission Convergence Layer，GPON 传输汇聚层）。GTC 再分为成帧子层（GTC framing sub-layer）和 TC 适配子层（GTC adapter sub-layer）。GTC 层提供两种业务数据的封装方式：ATM 封装方式将业务数据封装在 ATM 信元中传输，信元是长度 53 字节；GEM 封装方式是变长封装的，支持根据业务数据帧的长度改变 GEM 封装帧的长度。

OLT 和 ONU 之间的数据传输基于 T-CONT（Transmission Container，传输容器），T-CONT 的标识是 alloc id。一个 T-CONT 只能是 ATM 或者 GEM 类型的，一个 T-CONT 通道内可以分成由 VPI、VCI 标识的多个 PVC 通道，在 GEM 封装时可分成 PORT id 标识的多个 port 通道。

GPON 的管理维护有 3 种方式。Embedded OAM 方式（Embedded Operations, Administration and Maintenance，嵌入操作、管理和维护），在帧头的个别字段中携带，实时性强，实现如上行带宽授权等功能。PLOAM 方式，提供 13 字节固定格式的消息，需要时在帧头中插入，实现物理线路 OAM 功能。OMCI 方式，有自己的报文格式，承载在指定 VPI、VCI 或 port id 的通道上，适合实时性不强的消息传输，如配置消息。OMCI 是主从式管理协议，OLT 是主设备，ONU 是从设备，OLT 通过 OMCI 通道控制 OLT 下面连接的多个 ONU 设备。

业务数据和管理数据分别作为 ATM client/GEM client 和 OMCI client。GTC 适配子层向上层提供 ATM、GEM 和 OMCI 处理接口，将数据封装成 ATM 信元或 GEM 报文，即指定了 VPI、VCI 或 port id，也就确定了 T-CONT 的 id。GTC 成帧子层生成 GPON 帧头，在帧头中插入 PLOAM 消息，将 ATM 信元和 GEM 报文放入净荷部分，组装成 GPON 帧。最后经 GPM 层传送到光纤上，

在接收端进行逆处理。Embedded OAM 功能直接在成帧子层完成。

由于下行数据是广播的，虽然在 ONU 上会根据配置的 port id 过滤丢掉不属于自己的数据，但是仍面临数据被窃的风险，所以对 GPON 帧的净荷部分需要加密。下行数据的加密是很必要的。目前 GPON 国际标准中只规定了一种加密算法——AES 算法（Advanced Encryption Standard，高级加密标准），所有下行单播数据需要加密时都使用 AES 算法。每个 ONU 使用独立的密钥，并不断更新密钥，保证加密的可靠性。

OMCI 现有机制中和加密有关的定义只有两个属性，位于表示 ONU 设备的全局性信息和能力（如设备版本、是否支持 GEM 和 ATM 等）的 ONT2-G 或 ONU2-G ME 中。为了描述方便，本说明书将 ONT2-G 和 ONU2-G ME 合称为 ONU/T2-G ME。表示同样的信息的还有 ONT-G 或 ONU-G ME，ONT2-G 或 ONU2-G ME 附属于 ONT-G 或 ONU-G ME。安全能力（Security Capability）表示 ONU 能够支持的加密算法模式，安全模式（Security Mode）表示当前 ONU 选用的算法模式。不过因为国际标准中目前只定义了一个加密算法，不需要进行任何选择，所以安全模式属性中定义 ONU 创建 ME 时，该属性直接取值为 1，表示采用 AES 加密算法。这两个参数在 OMCI 配置过程中是用不到的，加密配置完全由 PLOAM 消息实现。以下是现有技术对 Security Capability 和 Security Mode 的定义：

Security Capability: 本属性表示 ONU 能够支持的高级安全模式。编码格式定义如下：

0: 保留为以后使用；

1: 支持对下行净荷的 AES 加密算法；

2..255: 保留为以后使用.

(只读) (强制实现) (长度: 1 byte)

Security Mode: 本属性表示 ONU 实际选用的高级安全模式。注意，不管何时，一个 ONU 上所有加密的 VP/VC 或者 GEM 端口的数据必须使用相同的安全模式。编码格式定义如下：

0: 保留为以后使用；

1: 对单播流量将使用 AES 加密算法；

2..255: 保留为以后使用.

ONU 自动创建该 ME 的实例时，本属性的值取 0x01. (可读，可写) (强制实现) (长度： 1 byte)

BPON 与 GPON 的数据加密机制相似，目前国际标准中对 BPON 只定义了一种高级加密算法。

PON 产品的研发要求能够适应不同国家、不同地区和不同网络运营商的应用需要，不同国家可能使用不同的加密算法，不同网络运营商也可能使用不同的加密算法。

从以上对 PON 国际标准的介绍可以看出，现有技术方案只考虑了一种数据加密算法模式，没有在 ONU 连接到 OLT 的配置阶段提供多算法模式协商过程，缺乏对多种加密算法的兼容处理，不能满足多国家，多地区和多网络运营商对 PON 设备要求支持多种加密算法的需求。

发明内容

本发明要解决的技术问题是提供一种 PON 系统中加密算法协商方法，该协商方法可以实现 PON 设备对多种加密算法的支持。

为解决上述技术问题，本发明是通过以下技术方案实现的:

PON 系统中加密算法协商方法，其特征在于，包括步骤: 1）获取光网络单元支持的算法模式; 2）依据预置策略允许的算法模式选定算法模式; 3）设置光网络单元使用所述选定的算法模式。

优选的，所述步骤 1)获取的过程包括: 11）发送获得支持算法模式的命令到光网络单元; 12）光网络单元反馈支持的算法模式。

优选的，所述步骤 1）获取的过程包括: 当光网络单元属性值变化的时候，所述光网络单元通过属性值变化 AVC 消息上报支持的算法模式。

优选的，所述光网络单元上报支持的算法模式之前，包括: c1）发送复位命令到光网络单元; c2）光网络单元响应复位结果。

优选的，所述预置的策略包括: 依据不同国家、不同地区或不同网络运营商而采用的不同使用标准。

优选的，所述步骤 2）选定的过程包括: 判断所述允许的算法模式和所述光网络单元支持的算法模式是否有相同的算法模式，如果是，从所述相同的算

法模式中选定算法模式，否则，作为协商失败处理。

优选的，所述协商失败处理过程包括：从所述允许的算法模式中选定算法模式；或将不表示任何实际算法的无效算法模式作为选定的算法模式，所述无效算法模式使用特定形式的值表示。

优选的，所述步骤 3）设置的过程包括：31）发送包括所述选定的算法模式的设置命令到光网络单元；32）光网络单元回应设置结果。

优选的，其特征在于，使用连续的取值或比特 bit 表示所述算法模式。

从以上技术方案可以看出，本发明在 ONU 配置阶段，首先获取 ONU 支持的算法模式，然后把依据预置策略选定的算法模式设置到 ONU 上，从而实现支持多种加密算法模式的算法协商过程。本发明通过改进现有协议，实现多种加密算法并存的应用需求，提高产品的兼容性。

进一步，本发明还提供了通过使用连续的取值或使用比特 bit 定义算法模式，扩充了安全能力和安全模式两个参数的表达能力，使得多种加密算法的选用具有灵活性。

附图说明

图 1 为 PON 系统连接图；

图 2 为 GPON 协议栈模型；

图 3 为本发明的加密算法协商方法流程图；

图 4 为本发明的加密算法协商方法实施例一示意图；

图 5 为本发明的加密算法协商方法实施例二示意图。

具体实施方式

本发明提供了 PON 系统中加密算法协商方法，应用于 ONU 连接到 OLT 后的配置阶段。

请参考图 3，是本发明的加密算法协商方法流程图。该方法流程包括以下步骤：

p1）光线路终端获取光网络单元支持的算法模式；

p2）光线路终端依据预置策略允许的算法模式选定使用的算法模式；

p3）光线路终端设置光网络单元使用所述选定的算法模式。

为了便于进一步理解本发明，以下结合具体实施例对本发明进行详细的描

述，以下描述的两个实施例基于 GPON 系统。

在 ONU 连接到 OLT 后，启动过程分成链路层注册阶段和 OMCI 配置阶段两部分。在链路层注册阶段，设备使用 PLOAM 消息完成链路建立，包括配置光路物理层使其正确连通，以及 ONU 向 OLT 的注册过程。注册过程主要环节为 ONU 向 OLT 上报自己的串号（serial number，ONU 设备的全球唯一的编号），OLT 给该 ONU 分配 ONU id，ONU id 在 OLT 一个光接口连接的所有 ONU 中是唯一的。注册建链后，OLT 再用 PLOAM 消息创建 ONU 上的第一个 T-CONT，并在该 T-CONT 内建立 port 或 pvc 通道，用于 OMCI 消息交互，然后进入 OMCI 配置阶段，由 OMCI 通道完成业务通道建立、配置数据下发等后续启动操作。整个启动过程完成后，PLOAM 消息还需要处理 OLT 和 ONU 之间链路的维护，以及处理其它底层相关的信息和命令交互，如链路故障指示的告警传达、通道加密功能启用等。

OMCI 协议将 OLT 管理 ONU 的各种数据抽象成协议独立管理信息库（protocol-independent Management Information Base ，简称 MIB），管理信息库的基本信息单元是管理实体（manage entity 简称 ME）。根据 ONU 的各种类型的配置数据，OMCI 定义了用于 OLT 控制 ONU 的各种 ME，ONU 在 OLT 的控制下实现各种 ME 的配置管理功能。ME 由属性（Attributes）组成，属性可以被 OLT 读写。有的 ME 由 ONU 自动创建，有的 ME 由 OLT 下发命令创建。

本技术方案利用了已有的 ONU/T2-G ME 中的属性定义，本方法在 ONU 连接到 OLT 启动过程的 OMCI 配置阶段中，增加了一个多算法模式协商的过程定义。

在 ONU 的管理实体中，ONU/T-G 是其他所有 ME 的根节点，在表示基本设备信息的 ME 创建后，才能进行具体业务的配置，所以 ONU/T-G 和 ONU/T2-G ME 在 OMCI 配置过程开始前就创建了。现有加密功能的配置过程使用在加密算法已经选定的情况，故本发明新增的协商过程位于原有加密过程之前，这个协商过程属于 OMCI 的具体业务配置阶段。

请参阅图 4，为为本发明的加密算法协商方法实施例一示意图，在本实施例中，OLT 通过使用 Get 命令获取支持的加密算法模式。

本技术方案的加密算法协商过程如下:

A1）OLT 使用 Get 命令,读取 ONU 上 ONU/T2-G ME 中 security capability 属性的值。

A2) ONU 响应 Get 命令，上报自身支持的加密算法模式。

A3) OLT 收到后，根据事先静态或动态配置的策略决定应当使用的算法模式。

具体的，在决定使用算法模式之前，依据不同国家、不同地区或不同网络运营商的使用标准允许不同的算法模式，判断所述允许的算法模式和所述光网络单元支持的算法模式是否有相同的算法模式，如果是，从所述相同的算法模式中选定算法模式，否则，作为协商失败处理。

上述协商失败处理过程可为从允许的算法模式中选定算法模式。

上述协商失败处理过程也可为将不表示任何实际算法的无效算法模式作为选定的算法模式，所述无效算法模式使用特定形式的值表示。

A4) OLT 使用 Set 命令，设置 ONU 上 ONU/T2-G ME 中 Security mode 属性为选定的算法模式取值。

A5) ONU 配置完成后，响应 OLT，表示 Set 操作结果。

A6) 系统启动加密流程。

以下为使用 AES 算法对下行数据加密时的启动过程:

1）用通道加密 PLOAM 消息对有需要的 port 通道下发加密命令，一般用于单播数据的通道都应加密;

2）OLT 向 ONU 请求加密用的密钥;

3）收到请求的 ONU 自主生成一个 AES 算法的密钥，送交 OLT，并在本地保留该密钥，用于解密;

4）OLT 收到密钥后，对相关的 ONU 下发密钥切换命令，在确定的时刻开始使用该密钥。

对于步骤 1)、4)，OLT 命令下发后，需要 ONU 回应确认消息。

与密钥切换相关的步骤 2）到步骤 4)，还用于密钥的新旧替换控制。

为了支持多算法模式，在保持 Security capability 和 Security mode 属性的意义不变的基础上，本发明对这两个参数取值定义进行扩充。

1）security capability 使用连续的取值表示 ONU 能够支持的算法模式，包括同时支持多种算法模式的组合选项，举例如下：

Security Capability: 本属性表示 ONU 能够支持的高级安全模式。编码格式定义如下：

0: 只支持加密算法 A;

1: 只支持加密算法 B;

2: 只支持加密算法 C;

3: 同时支持加密算法 A 和 B;

4: 同时支持加密算法 B 和 C;

5..255: 保留为以后使用.

(只读) (强制实现) (长度: 1 byte)

上述连续的取值可为：包含 0 在内的自然数值或整数。

可以理解的是，以上所举的组合选项例子，不一定遍历算法的所有组合关系。不排除在应用中根据本发明原理衍生出其他组合方法。

2）security mode 的取值定义可以和 security capability 相同，通常只需要表示单个算法模式的值；当协商失败，可以使用特定形式的值表示无效算法，比如：使用 255 表示无效算法。举例如下：

Security Mode: 本属性表示 ONU 实际选用的高级安全模式。注意，不管何时，一个 ONU 上所有加密的 VP/VC 或者 GEM 端口的数据必须使用相同的安全模式。编码格式定义如下：

0: 将使用加密算法 A;

1: 将使用加密算法 B;

2: 将使用加密算法 C;

3..254: 保留为以后使用;

255: 表示无效算法.

(可读, 可写) (强制实现) (长度: 1 byte)

请参阅图 5，为本发明的加密算法协商方法实施例二示意图，在本实施中，ONU 通过 AVC（Attribute Value Change，属性值变化）消息上报支持的加密算法模式。

本实施例从 ONU 连接到 OLT 开始，然后到启动阶段 OMCI 配置过程，在 ONU 上创建 ONU/T2-G ME 后，ONU 使用 AVC 功能上报 security capability 属性的数值，即 ONU 实际支持的能力，本方法使用 ONU 的 AVC 上报替换第一种实施例中的 OLT 的 Get 操作。安全能力属性属于 ONU/T2-G ME，这个 ME 是 OMCI 配置过程的开始时创建的。

B1）ONU 上电启动，ONU 还没有 mib，先创建 ONU/T-G、ONU/T2-G 和 ONT data ME。ONT data ME 保存 mib 同步状态参数，用于检查 ONU 上 mib 和 OLT 上保存的对应 mib 之间的同步状态。mib 同步状态参数是一个序列号，在 ONU mib 发生变化时该值增加。OLT 在本地保留对 ONU mib 的映象，通过核对该值以判断是否需要更新本地 mib。

B2）OLT 下发 ONTData MIBReset cmd 命令，ONU 接受到该命令后清除自身的 mib，使 ONU 上的 mib 只剩下缺省的 ME，缺省 ME 表示设备基本软硬件信息，包括 ONU/T-G、ONU/T2-G、ONT data 和其他必要的 ME。

B3）ONU 回应 ONTData MIBReset rsp，表示 mib 复位成功。

B4）OLT 本地创建对应此 ONU 的 mib，包括 ONU/T-G、ONU/T2-G、ONT data 和其他必要的 ME。

B5）这时，ONU 和 OLT 上创建的 ME 属性都是缺省值，不一定符合 ONU 实际情况，例如 Security Capability 属性的值并没有正确表示 ONU 实际的能力。所以本步骤中，ONU 根据内存中的实际设备信息更新 ONU/T-G、ONU/T2-G ME 的属性值，刷新后的值通过 AVC 消息主动上报给 OLT。

B6）OLT 从收到的 AVC 消息中得到变化后的属性值（包括上报 Security Capability 属性的值），刷新 OLT 上的 mib 映象数据，并根据事先静态或动态配置的策略决定应当使用的算法模式。

具体的，在决定使用算法模式之前，依据不同国家、不同地区或不同网络运营商的使用标准允许不同的算法模式，判断所述允许的算法模式和所述光网络单元支持的算法模式是否有相同的算法模式，如果是，从所述相同的算法模式中选定算法模式，否则，作为协商失败处理。

上述协商失败处理过程可为直接中断加密算法配置过程。

B7）OLT 使用 Set 命令，设置 ONU 上 ONU/T2-G ME 中 Security mode 的

属性为选定的算法模式取值。

B8) ONU 配置完成后，响应 OLT，表示 Set 操作结果。

B9) 系统启动加密过程。

在本实施例中，本发明对 Security capability 和 Security mode 属性的取值使用了另一种方式进行定义。

1）security capability 通过使用字段比特 bit 表示 ONU 支持的一种算法模式，几个 bit 值同时有效表示同时支持几种算法模式。举例如下：

Security Capability: 本属性表示 ONU 能够支持的高级安全模式。编码格式定义如下：

bit0: 为 1 表示支持加密算法 A，为 0 表示不支持;

bit1: 为 1 表示支持加密算法 B，为 0 表示不支持;

bit2: 为 1 表示支持加密算法 C，为 0 表示不支持;

bit3..bit7: 保留为以后使用.

(只读) (强制实现) (长度: 1 byte)

2）security mode 的取值定义同 security capability。在选定了有效算法时，同一时间只有一个算法模式有效，表示选用的算法；当协商失败，可以使用特定形式的值表示无效算法，比如：使用 bit7 或同时使多个算法模式同时有效的形式表示无效算法。举例如下：

Security Mode: 本属性表示 ONU 实际选用的高级安全模式。注意，不管何时，一个 ONU 上所有加密的 VP/VC 或者 GEM 端口的数据必须使用相同的安全模式。编码格式定义如下：

bit0: 为 1 表示将使用加密算法 A，否则为 0;

bit1: 为 1 表示将使用加密算法 B，否则为 0;

bit2: 为 1 表示将使用加密算法 C，否则为 0;

bit3..bit6: 保留为以后使用.

bit7: 为 1 表示无效算法，否则为 0.

(可读，可写) (强制实现) (长度: 1 byte)

上述的比特bit可为：由若干个bit组成的二进制计数值。

可以理解的是，在以上两个实施例中，本发明使用连续的取值或比特bit

定义算法模式和算法模式的组合，扩充了安全能力和安全模式两个参数的表达能力，不排除对安全能力和安全模式属性字段的长度进行扩展的可能，以及扩展长度后改变所属ME的可能。

需要说明的是，因为 BPON 系统使用和 GPON 系统相同的 OMCI 协议，上述两个基于 GPON 系统实施例的多算法协商过程思路同样可以用在 BPON 系统。可以理解的是，不排除其他 PON 技术使用本技术方案原理实现多算法协商。

以上对本发明所提供的一种 PON 系统中加密算法协商方法进行了详细介绍，本文中应用了具体个例对本发明的原理及实施方式进行了阐述，以上实施例的说明只是用于帮助理解本发明的方法及其核心思想；同时，对于本领域的一般技术人员，依据本发明的思想，在具体实施方式及应用范围上均会有改变之处，综上所述，本说明书内容不应理解为对本发明的限制。

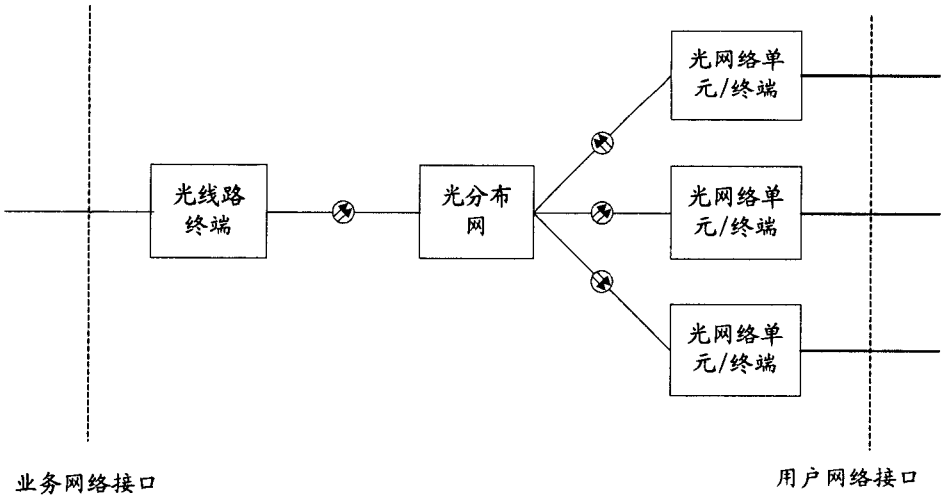

光网络单元/终端
光线路终端
光分布网
光网络单元/终端
光网络单元/终端
业务网络接口
用户网络接口

图 1

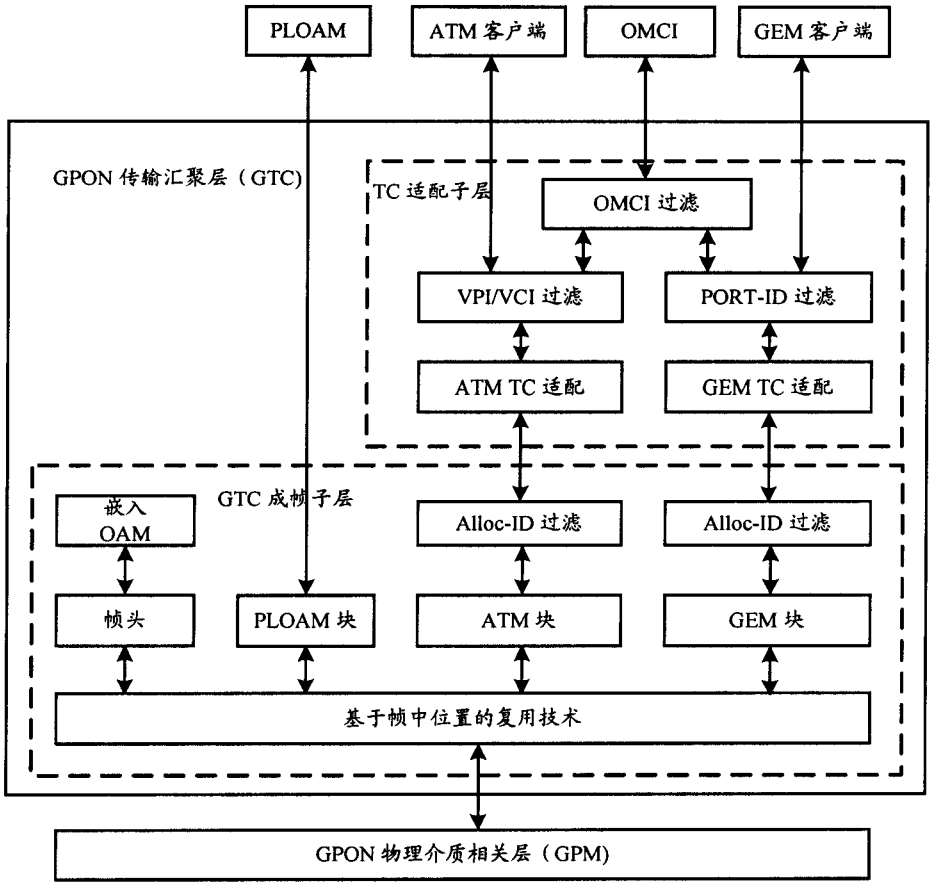

PLOAM
ATM 客户端
OMCI
GEM 客户端
GPON 传输汇聚层（GTC）
TC 适配子层
OMCI 过滤
VPI/VCI 过滤
PORT-ID 过滤
ATM TC 适配
GEM TC 适配
GTC 成帧子层
嵌入 OAM
Alloc-ID 过滤
Alloc-ID 过滤
帧头
PLOAM 块
ATM 块
GEM 块
基于帧中位置的复用技术
GPON 物理介质相关层（GPM）

图 2

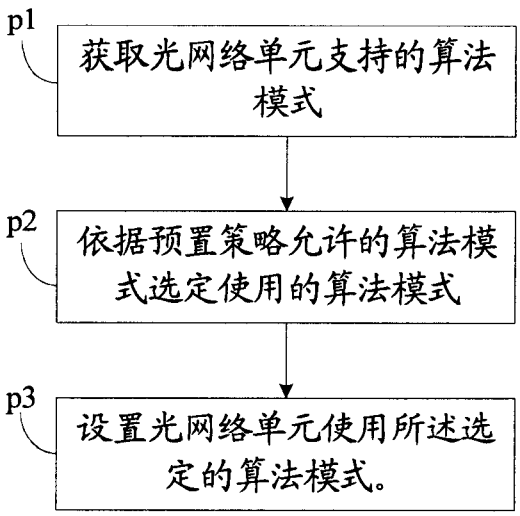

p1
获取光网络单元支持的算法模式
p2
依据预置策略允许的算法模式选定使用的算法模式
p3
设置光网络单元使用所述选定的算法模式。

图 3

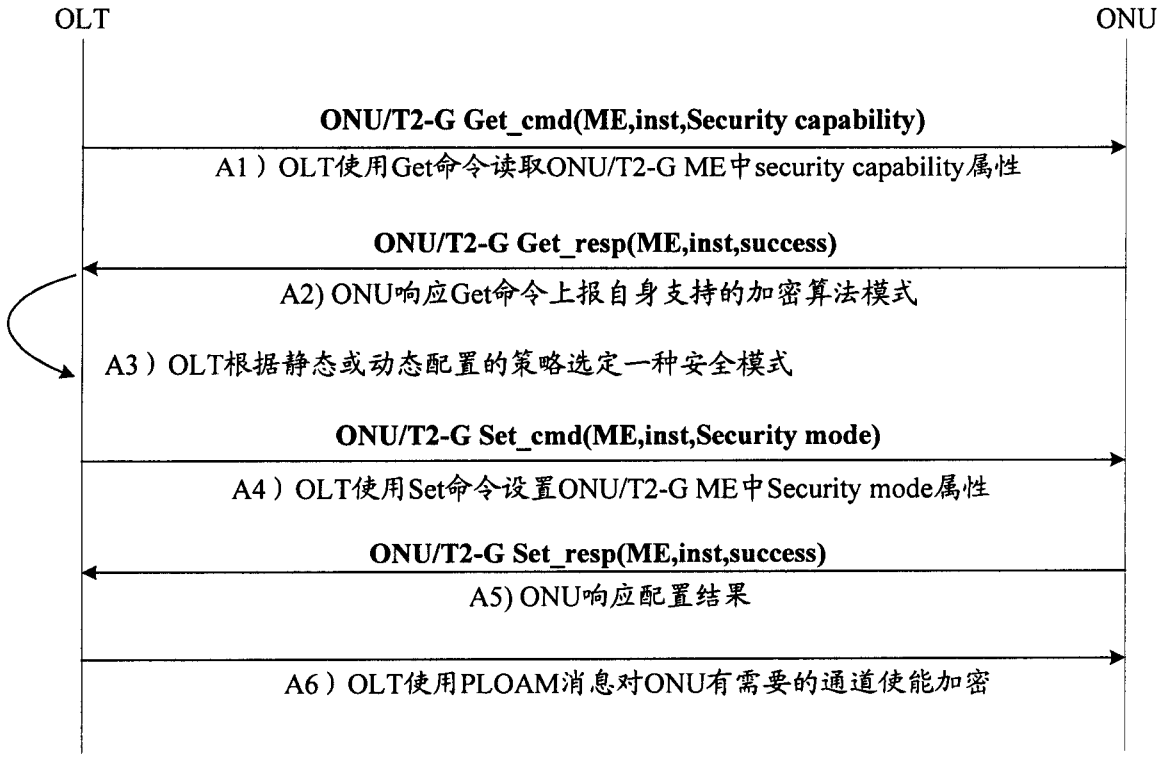

OLT
ONU
ONU/T2-G Get_cmd(ME,inst,Security capability)
A1）OLT使用Get命令读取ONU/T2-G ME中security capability属性
ONU/T2-G Get_resp(ME,inst,success)
A2) ONU响应Get命令上报自身支持的加密算法模式
A3）OLT根据静态或动态配置的策略选定一种安全模式
ONU/T2-G Set_cmd(ME,inst,Security mode)
A4）OLT使用Set命令设置ONU/T2-G ME中Security mode属性
ONU/T2-G Set_resp(ME,inst,success)
A5) ONU响应配置结果
A6）OLT使用PLOAM消息对ONU有需要的通道使能加密

图 4

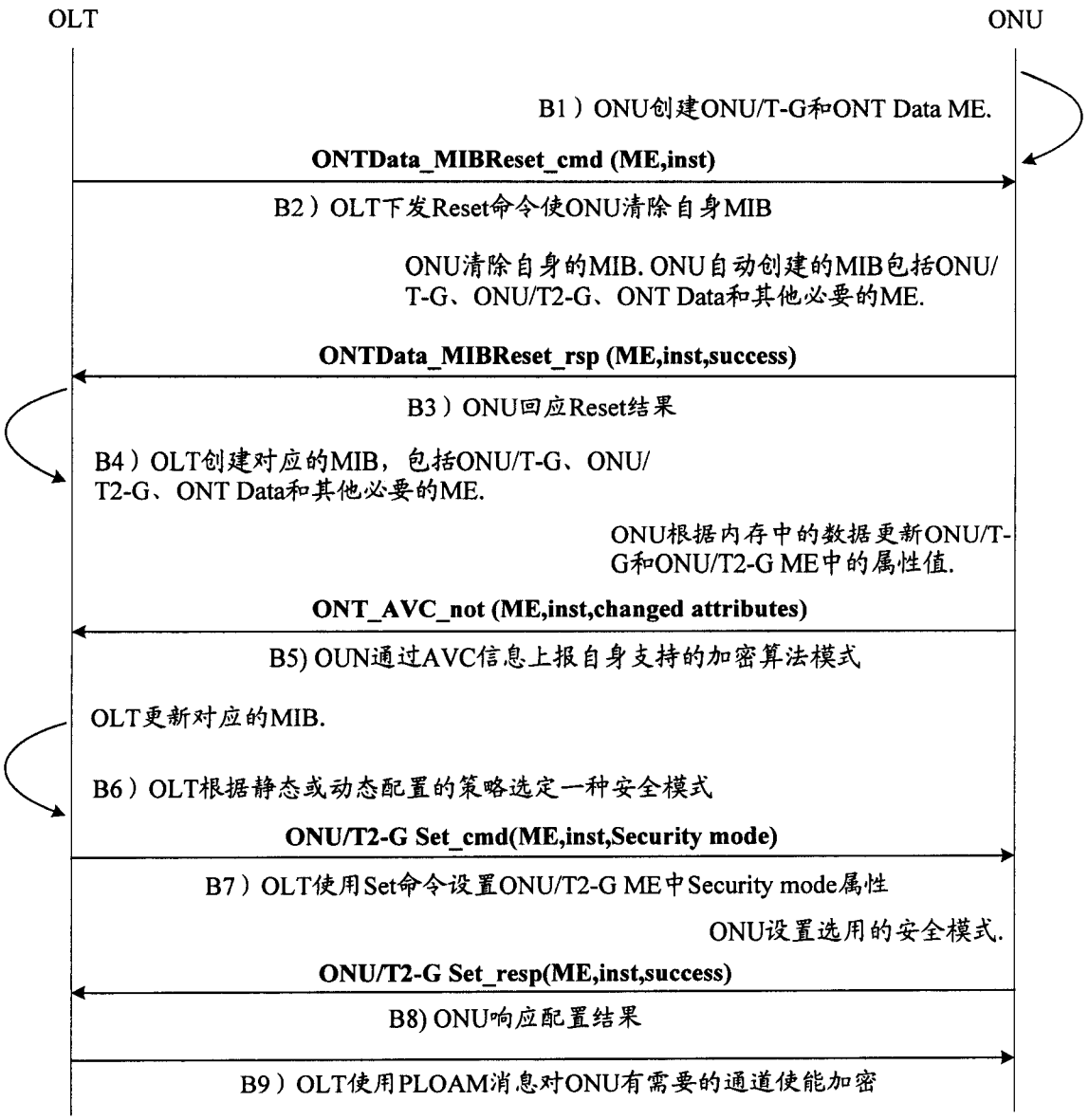

OLT
ONU
B1）ONU创建ONU/T-G和ONT Data ME.
ONTData_MIBReset_cmd (ME,inst)
B2）OLT下发Reset命令使ONU清除自身MIB
ONU清除自身的MIB. ONU自动创建的MIB包括ONU/T-G、ONU/T2-G、ONT Data和其他必要的ME.
ONTData_MIBReset_rsp (ME,inst,success)
B3）ONU回应Reset结果
B4）OLT创建对应的MIB，包括ONU/T-G、ONU/T2-G、ONT Data和其他必要的ME.
ONU根据内存中的数据更新ONU/T-G和ONU/T2-G ME中的属性值.
ONT_AVC_not (ME,inst,changed attributes)
B5) OUN通过AVC信息上报自身支持的加密算法模式
OLT更新对应的MIB.
B6）OLT根据静态或动态配置的策略选定一种安全模式
ONU/T2-G Set_cmd(ME,inst,Security mode)
B7）OLT使用Set命令设置ONU/T2-G ME中Security mode属性
ONU设置选用的安全模式.
ONU/T2-G Set_resp(ME,inst,success)
B8) ONU响应配置结果
B9）OLT使用PLOAM消息对ONU有需要的通道使能加密

图 5