

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.

H04L 12/56 (2006.01)

H04L 29/06 (2006.01)



[12] 发明专利申请公布说明书

[21] 申请号 200910150415.6

[43] 公开日 2009 年 12 月 30 日

[11] 公开号 CN 101616087A

[22] 申请日 2009.6.19

[21] 申请号 200910150415.6

[30] 优先权

[32] 2008.6.24 [33] FR [31] 0854201

[71] 申请人 阿尔卡特朗讯公司

地址 法国巴黎

[72] 发明人 E·瓮弗鲁瓦 E·布鲁 B·马凯

J·阿劳约 A·安西奥

[74] 专利代理机构 北京市中咨律师事务所

代理人 杨晓光 于 静

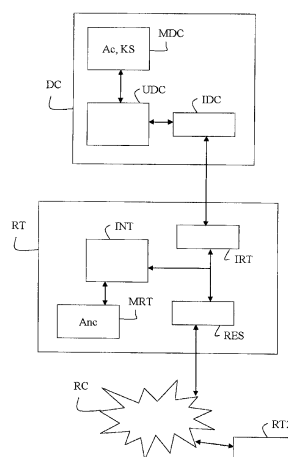
权利要求书 2 页 说明书 9 页 附图 2 页

[54] 发明名称

关联至安全设备的路由器

[57] 摘要

本发明涉及一种关联至安全设备(DC)且包含于通信网络(RC)中的路由器,包括用于在由安全设备认证路由器之后与该安全设备通信的接口(IRT),并且包括用于控制由安全设备对一个或多个路由协议的关键操作的执行的协议解释器(INT)。路由协议的敏感的或关键的部分是以安全可靠的方式在例如芯片卡的安全设备中被执行的。



1. 一种关联至安全设备 (DC) 且包含于通信网络 (RC) 中的路由器, 包括用于在由所述安全设备认证所述路由器之后与该安全设备通信的接口 (IRT), 其特征在于, 包括用于控制由所述安全设备对路由协议的至少一部分的执行的装置 (INT)。

2. 根据权利要求 1 所述的路由器, 包括用于标识待执行的路由协议部分并且确定由所述路由器和所述安全设备之外的哪个单元来执行所标识的路由协议部分的装置 (INT)。

3. 根据权利要求 2 所述的路由器, 包括第一路由协议部分与所述路由器之间的、以及第二路由协议部分与所述安全设备之间的匹配表, 所述第一和第二协议部分是不同的并且完全地定义了所述路由协议。

4. 根据权利要求 1 至 3 之一所述的路由器, 其特征在于, 至少一个路由协议部分是用于创建通过所述路由协议所请求的控制消息的算法。

5. 一种关联至包含于通信网络 (RC) 中的路由器的安全设备, 包括用于在由所述安全设备认证所述路由器之后与该路由器通信的接口 (IDC), 其特征在于, 包括用于通过所述路由器的控制来执行路由协议的至少一部分的装置 (UDC)。

6. 根据权利要求 5 所述的安全设备, 包括用于就所述路由协议的至少一部分的执行而生成消息且签署它、并且将签署的消息发送至所述路由器的装置 (UDC)。

7. 根据权利要求 5 或 6 所述的设备, 其特征在于, 所述安全设备是芯片卡。

8. 一种用于在通信网络 (RC) 内安全执行路由协议的一部分的方法, 其特征在于, 包括在关联至安全设备的路由器 (RT) 中执行下列步骤:

标识 (E1) 待执行的路由协议的一部分,

确定 (E2) 由所述路由器和关联至该路由器的安全设备之外的哪个单元来执行所标识的路由协议部分, 以及

就由所述安全设备对所述路由器的认证而控制 (E4) 由所述安全设备对所述路由协议部分的执行,

其特征还在于, 包括在所述安全设备中通过所述路由器的控制来执行 (E5) 所述路由协议部分。

关联至安全设备的路由器

技术领域

本发明涉及关联至基于分组的通信网络内的安全设备的路由器。

背景技术

路由器是包含于例如基于分组的网络的给定通信网络中的信息技术设备，其功能特别是提供给定网络与至少一个其他网络之间的连接以在给定网络中指引数据分组并且从给定网络向另一网络发送数据分组。

对路由器的攻击会造成路由器功能失常以及各种有害后果，例如网络崩溃、服务中断、网络用户行为中断、以及巨大成本和负面广告。

这种攻击由于路由器是网络中的重要角色而通常针对路由器，并且它们可以是不同类型的，例如针对监控网络内的数据业务的“中间人”攻击、服务拒绝攻击、或颠覆攻击。

在颠覆攻击中，攻击者可以利用当前用户权限或可能地利用管理员权限连接到路由器。这种权限使得攻击者能够修改路由器的配置并且控制路由器中执行的所有过程。

存在各种不同的路由协议，例如用于在网络中指引数据分组的 OSPF（开放最短路径优先）、BGP（边界网关协议）或 RIP（路由信息协议）。在颠覆攻击期间，攻击者可以修改生成路由协议消息的过程以使用假地址并且在不利的路由上指引数据分组。例如，数据分组可以被指引到属于攻击者的设备以便该攻击者可以访问这种数据分组从而潜在地能够修改它们。这种不利的路由信息可以被传播至网络中的所有路由器。

为了确保网络的两个路由器之间的安全数据交换，一些机制认证通过网络所用的路由协议而生成的所有消息。这个认证借助于密钥进行，该密

钥被部署及存储于网络中的所有路由器中并且可以由每个路由器的管理员更改。这种认证机制具有下列缺点：

- 当攻击者拥有路由器管理员权限时，他/她可以修改路由器安全功能所需要的密钥；
- 攻击者可能能够更改路由协议的执行以修改发送的或接收的消息的内容；以及
- 密钥管理非常繁重，因为密钥通常从不更改。

因此，基于分组的网络的运营商有必要防止或限制对网络路由器的攻击，攻击者可以通过攻击将所有或部分数据业务指引至讹用的网络地址。

发明内容

本发明的一个目的是通过改进基于分组的网络中的路由器的安全性来弥补上述缺点。

为达到该目的，本发明提供了一种关联至安全设备且包含于通信网络中的路由器，其包括用于在由所述安全设备认证所述路由器之后与该安全设备通信的接口，其特征在于，包括用于控制由所述安全设备执行路由协议的至少一部分的装置。

有利地，根据本发明的路由器可以执行所述路由协议中被认为是非关键的特定协议部分，并且可以将所述路由协议中被认为是关键的其他协议部分的执行移至所述安全设备。在所述安全设备中执行的协议部分不能被所述路由器本身执行和/或修改，并且被认为是可靠的，这与由所述路由器执行的其他协议部分相反，由于所述路由器可以被潜在攻击者操纵而认为所述其他协议部分是不可靠的。

根据本发明的另一特征，所述路由器可以包括用于标识待执行的路由协议的一部分并且确定由所述路由器和安全设备之外的哪个部件执行所标识的路由协议部分的装置。这个标识可以借助于第一路由协议部分与所述路由器之间的、以及第二路由协议部分与所述安全设备之间的匹配表来执行，所述第一和第二协议部分是不同的并且完全地定义了所述路由协议。

作为例子，所述至少一个路由协议部分可以是一种用于创建所述路由协议所需要的控制消息的算法、或者是一种用于创建或修改存储于所述安全设备中的路由表的算法。

本发明还涉及一种关联至包含于通信网络中的路由器的安全设备，其包括用于在由所述安全设备认证所述路由器之后与该路由器通信的接口，其特征在于，包括用于就所述路由器的控制而执行路由协议的至少一部分的装置。

根据本发明的另一特征，所述安全设备可以包括用于签署就路由协议的所述至少一部分的执行而生成的消息并且将所签署的消息发送至所述路由器的装置。由所述安全设备生成且签署的消息具有可靠且不可修改的内容；由所述路由器对该消息的任何修改都会使得该消息无效，因为修改的消息由于错误签名而不会被其他路由器接受。

例如，所述安全设备可以是芯片卡。有利地，与路由协议有关的数据和算法可以被不可改变地且安全地存储在该芯片卡上。

本发明还涉及一种用于在通信网络内安全地执行路由协议的一部分的方法，其特征在于，包括在关联至安全设备的路由器中执行下列步骤：

标识待执行的路由协议的一部分，

确定由所述路由器和关联至该路由器的安全设备之外的哪个部件来执行所标识的路由协议部分，和

就所述安全设备对所述路由器的认证而控制所述安全设备对所述路由协议部分的执行，

其特征还在于，包括通过所述路由器的控制而在所述安全设备中执行所述路由协议部分。

附图说明

参考附图，通过阅读下面的描述，将更好地理解本发明及其优点，其中：

- 图 1 是关联至可信设备且包含于基于分组的网络中的根据本发明的

路由器的示意性框图；和

- 图 2 是根据本发明的用于在关联至路由器的可信设备内执行路由协议的一部分的方法的算法。

具体实施方式

作为介绍，下面定义有助于理解本发明的几个术语和概念。

路由器是通信网络中的用于路由消息的信息技术设备。具体地，路由器控制消息在网络中的传输并且可以确定数据分组应当被发送至的最近的网络节点以使得所述分组尽可能快地到达网络中的预定目标。为此，路由器在其存储器中具有路由表，所述路由表根据对于与至网络内其他路由器的最短路径相关联的度量而包含所述最短路径。换句话说，路由表是目标网络位置的网络地址与路由器向其发送消息的下一节点之间的匹配表。这个称为“选路”的过程在 OSI（开放系统互连）模型的“网络”层中进行并且通常关联于 IP（互联网协议）协议。

路由器可以是专用于路由功能的计算机，其特别地包括主板、微处理器、操作系统和用于与例如服务器或其它路由器的其他部件通信所必需的网络资源。

路由协议实现了路由器之间的路由信息交换以及对所使用的不同应用之间的交换模式的定义，例如发送消息或对消息接收的确认，具体地是对所交换消息的特征的定义，例如消息交换所涉及的路由器的标识符，其属性和内容，以及期望的消息处理。

路由器具有涉及三个等级的不同功能性：

- 控制级，其基于通过路由器的路由协议所收集的信息来编辑路由表，
- 数据级，其组合重传功能性以将分组路由至期望的目的地，和
- 管理级，其例如从命令线接口或由网络管理员来管理路由器。

本发明借助于关联至路由器的可信设备而将信任级添加至路由器。信任级提供了用于在安全地处理安全数据之后提供可靠信息的功能性。例如，可信设备由网络设备供应商来提供并且由网络运营商或网络管理员来配

置。

下面描述通过网络运营商获得例如芯片卡的可信设备的一个例子。卡制造商提供芯片卡以及初始密钥给网络设备提供商。所述初始密钥使得该提供商能够安装 Java 程序（即载入芯片卡且在芯片卡中执行的程序）、特别涉及关联于该卡的路由器的数据、协议算法以及该卡中的密钥。当完成安装时，根据提供商和网络运营商之间的约定，提供商可以选择移除密钥并且所安装的 Java 程序然后不能再被修改，也可以选择不移除密钥，在不移除密钥的情况下所安装的 Java 程序可以被更新。提供商然后可以销售关联于芯片卡的路由器给网络运营商。当路由器初次被配置和使用时将可信设备关联于路由器。根据运营商的策略，可信设备可以永久地关联于路由器，或者它可以借助于专用设备而被修改和更新。

参考图 1，路由器 RT 包含于通信网络中并且关联至可信设备 DC。路由器 RT 适于与基于分组的网络中的至少另一个路由器 RT2 通信。

通信网络 RC 例如是 IP（互联网协议）型高速网络，例如互联网或内联网，或甚至是指定公司的专用网。

路由器 RT 包括用于与可信设备 DC 通信的访问接口 IRT、用于执行认为是“非关键的”路由协议部分的 INT 协议解释器、其中特别存储有对应于非关键协议部分的预定算法（后文称作非关键算法 Anc）的存储器 MRT、以及用于与通信网络 RC 中的例如另一路由器 RT2 的部件通信的网络接口 RES。

可信设备 DC 包括用于与路由器 RT 通信的访问接口 IDC、用于执行认为是“关键的”路由协议部分的处理单元 UDC、以及其中特别存储有密钥 KS 和对应于路由协议的“关键”部分的预定算法（后文称作关键算法 Ac）的存储器 MDC。

因此，对应于所有路由协议部分的所有算法以共享的方式被存储在路由器和可信设备中，并且路由协议的非关键部分在路由器中执行，而关键部分在可信设备中执行。协议的关键部分因而必须不同于协议的非关键部分并且与之互补，以使得关键的和非关键的部分完整地定义了路由协议。

作为例子，所述关键部分在于一种用于生成特定信息以例如构造或认证消息或者创建或修改数据库或路由表的算法。所述关键部分可能在于一种攻击者可能用来执行颠覆攻击的功能。路由器执行的非关键的协议部分被认为是**不安全且不可靠的**，而关键的协议部分被认为是**安全的且可靠的**。

因此，信任级管理关键协议部分，而控制级管理非关键协议部分。

可信设备 DC 是安全的无法攻破的设备，其实现了过程执行隔离概念。可信设备 DC 例如是可拆卸的接触性或非接触性芯片卡，其也称为微控制器卡或集成电路卡，该卡可以经由用于进行例如射频型通信的装置而从路由器到达。根据另一个例子，可信设备是具有加密功能的硬件安全模块 HSM，并且可以是集成在路由器中的插件电子卡或经由非接触性或接触性连接而连至路由器的移动硬盘。

路由器 RT 和可信设备 DC 经由各自的访问接口 IRT 和 IDC、借助于共享通信密钥而相互通信。例如，路由器 RT 可以在与可信设备 DC 通信之前从该可信设备请求识别码。这些通信密钥防止在另一路由器上执行可信设备。

路由器 RT 和可信设备 DC 是相关联的，即它们可以借助于有线或无线连接而互连。例如，可信设备 DC 可以是非接触性或接触性连接芯片卡，该芯片卡可被引入路由器 RT 的合适的阅读器中。

可选地，路由器 RT 包括用于检测路由器 RT 是否真正关联至可信设备 DC 并且在适当情况下提供功率给该可信设备的现场（presence）控制器。

参考图 2，根据本发明的用于在关联至路由器的可信设备内执行路由协议的一部分的方法包括步骤 E1 至 E7，这些步骤中的一部分在路由器中自动执行而另一部分在根据本发明的可信设备内自动执行。

在步骤 E1 中，根据路由器 RT 所使用的路由协议，事件触发了路由器对一部分协议的执行。这个事件例如可以是路由器经由网络接口 RES 接收到来自通信网络 RC 的另一路由器的请求。协议解释器 INT 标识了待执行的协议部分。

在步骤 E2 中，路由器的协议解释器 INT 确定所标识的协议部分是由路由器执行还是由可信设备执行，即它检验协议部分是关键算法 Ac 还是非关键算法 Anc。为此，协议解释器例如查询匹配表，在该匹配表中每个协议部分关联至路由器或可信设备。

如果这个协议部分是非关键的，则路由器本身在步骤 E3 中执行与这个非关键协议部分对应的 Anc 算法。

如果这个协议部分是关键的和因而在匹配表中关联于可信设备，则协议解释器在步骤 E4 中请求经由 IRT 和 IDC 访问接口来访问可信设备 DC。在利用可信设备认证路由器之后，这两个部件可以相互通信，并且协议解释器例如通过向可信设备特别地发送该协议部分或匹配算法的标识符来控制可信设备执行关键的协议部分。

在步骤 E5 中，可信设备的处理单元 UDC 执行存储于存储器 MDC 中且例如通过接收自关键算法 Ac 的标识符而匹配于关键协议部分的关键算法 Ac。

在可选步骤 E6 中，根据步骤 E5 中执行的关键算法的属性，处理单元 UDC 在协议部分执行结束时生成消息 MES 并且借助于存储在存储器 MDC 中的密钥 KS 来签署所生成的消息。作为例子，如果关键算法对应于通过所用路由协议而请求的控制消息的创建，则执行步骤 E6；以及，如果关键算法对应于对存储在可信设备中的路由表的修改则执行步骤 E6。

在可选步骤 E7 中，处理单元 UDC 发送签署的消息 MES 至协议解释器 INT，该协议解释器然后就仿佛所述消息已由协议解释器生成那样来处理该消息，即例如发送签署的消息至另一路由器。由于消息 MES 被签署，路由器不能再修改该消息的内容。

根据本发明的实施例，可信设备 DC 执行至少一个路由协议的关键部分，例如 OSPF、BGP 或 RIP 协议。根据本发明的特定例子，可信设备 DC 执行 Hello 协议，该协议是使得路由器能够相互检测到从而在它们之间交换路由信息的 OSPF 协议的关键部分。每个路由器定期发送控制消息给相邻的路由器，所述消息包含随时间增长的密码序号。Hello 协议使之能够

建立路由器之间的邻接关系，具体地是按照 OSPF 协议为通信网络内的每个本地网络选出指定路由器 DR 和备用的指定路由器 BAR。

给定路由器发送的控制消息还包含与已知相邻路由器以及在给定路由器与相邻路由器之间的连接的状态有关的信息。

下面描述 Hello 协议在关联至路由器 RT 的可信设备 DC 中的执行的例子。

只要路由器是可操作的，它就定期地经由所有专用接口发送 HELLO 控制消息给路由器的 OSPF 协议。具有接收的 HELLO 消息的路由器发送响应给相邻路由器。为此，解释器 INT 将 HELLO 协议标识为 OSPF 协议的关键协议部分，并且对于可信设备控制 HELLO 消息构造算法的执行。处理单元 UDC 然后构造 HELLO 消息并且在将该消息发送至路由器的协议解释器 INT 之前签署它，该协议解释器又将该消息发送至另一路由器。

由安全设备对 Hello 协议的处理因而确保了 HELLO 消息是可信的并且它源自安全的源。

在对路由器的颠覆攻击中，攻击者可以修改包含于未关联至可信设备的路由器中的操作系统、路由协议和密钥。

根据本发明，受攻击的路由器可以被隔离以阻止攻击向整个网络的传播。实际上，如果未使用可信设备，则路由器被隔离成就好像它不再访问包含于可信设备中且符合请求的路由协议的算法和数据。

例如，对于 OSPF 路由协议而言，受攻击的路由器不再正确地签署和认证 HELLO 消息，并且其他路由器不再识别受攻击的路由器。受攻击的路由器从其他路由器所知道的路由表中消失并且数据业务将不再经过受攻击的路由器。

路由器因而在下列情形中被隔离：

- 当攻击者修改在路由器与可信设备之间共享的通信密钥或将可信设备与路由器断开连接时，路由器生成的消息不会再被签署且被可信设备认证，因此这种消息不能被发送给相邻路由器。

- 当攻击者修改所接收的控制消息的数据时，攻击者不能签署该消息，

并且可信设备由于路由器不能认证该控制消息而无法接受该消息。之后，受攻击的路由器不再从相邻路由器接收到任何信息并且不再应答它们的消息。以及

- 当攻击者修改由可信设备签署且待发送至另一路由器的控制消息的数据时，攻击者无法签署修改的消息，并且这种修改的消息不会被另一路由器接受。

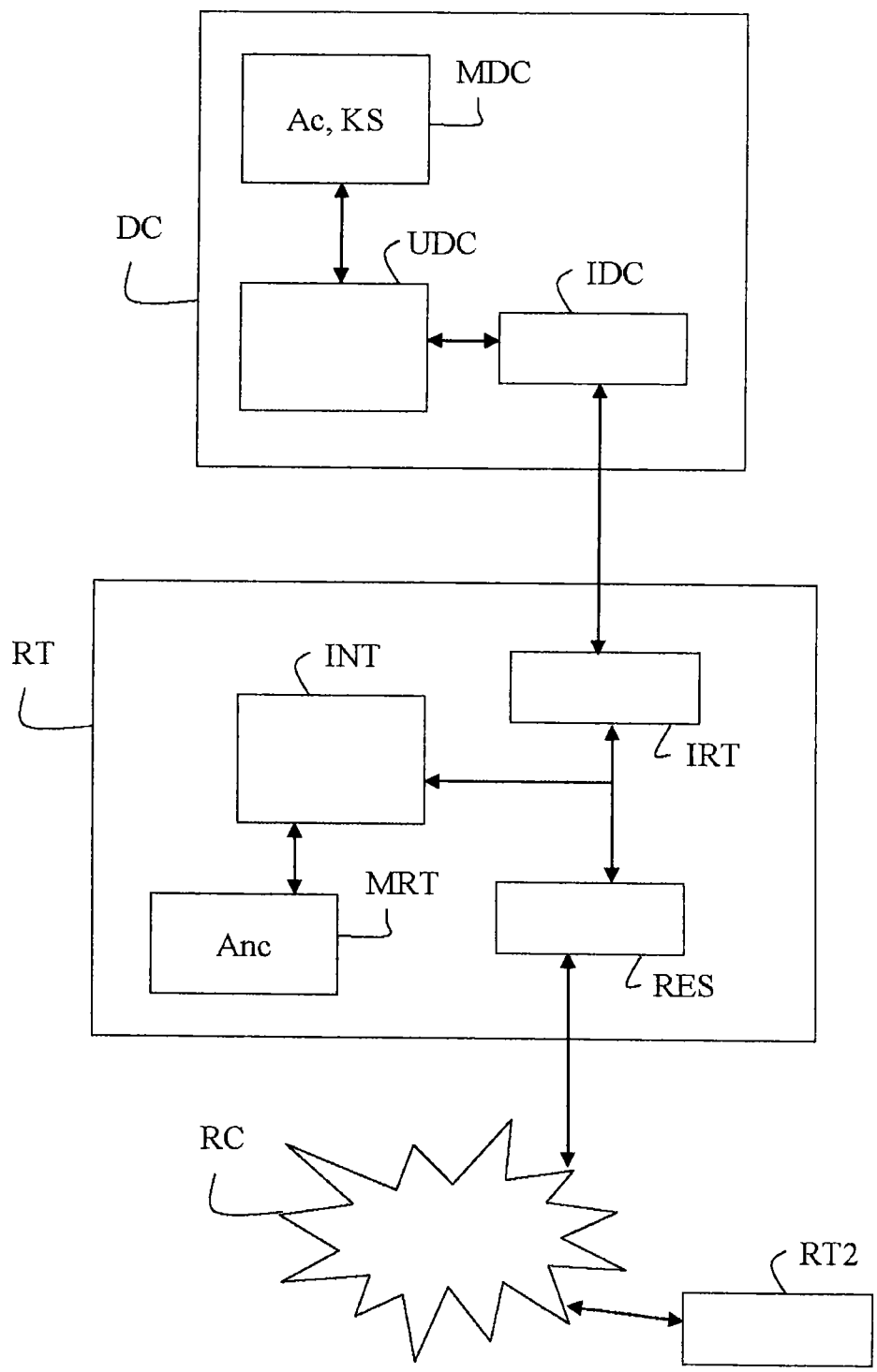


图 1

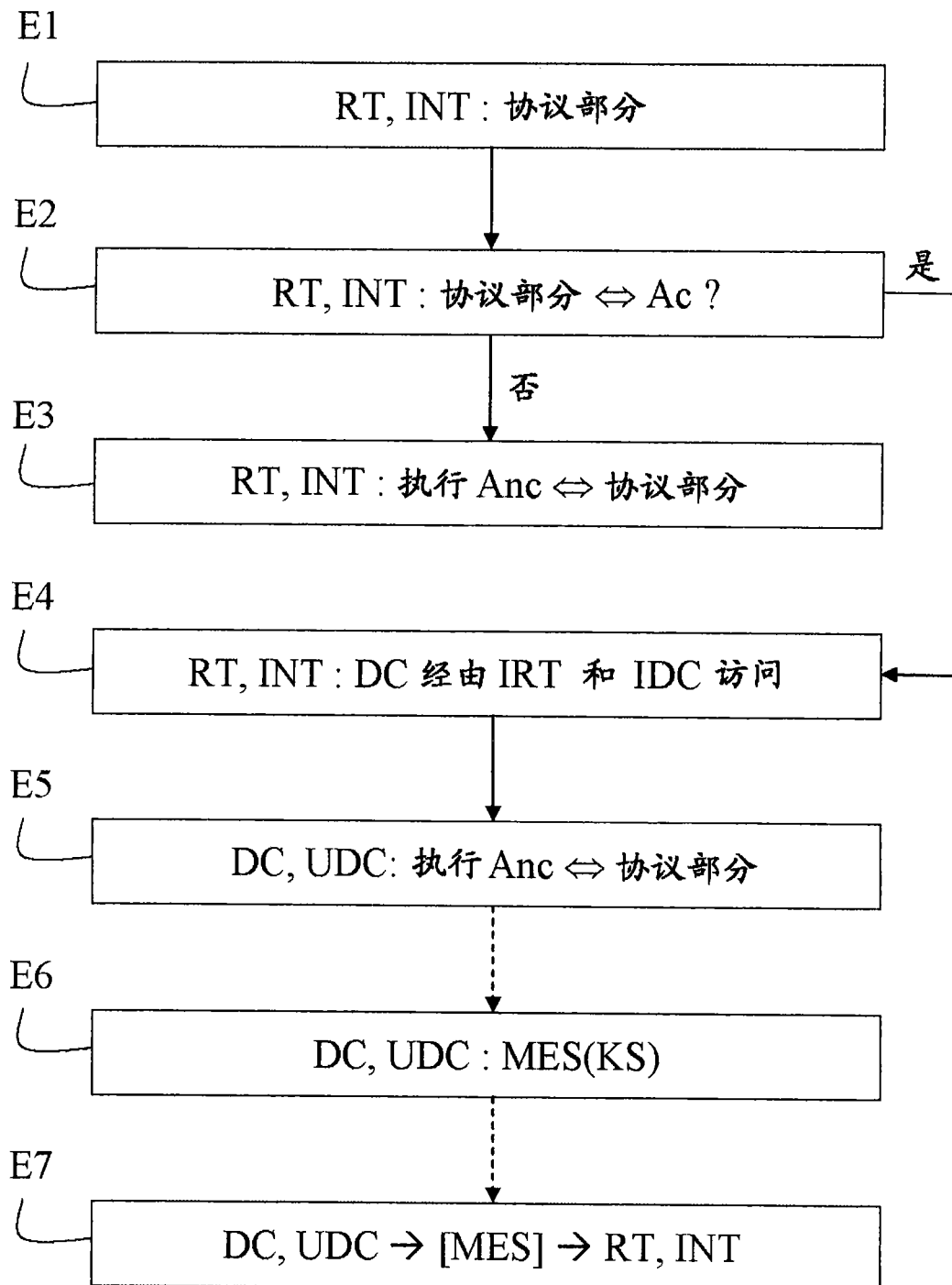


图 2