



(12) 发明专利申请

(10) 申请公布号 CN 103957097 A

(43) 申请公布日 2014. 07. 30

(21) 申请号 201410145386. 5

H04W 40/00(2009. 01)

(22) 申请日 2014. 04. 14

(71) 申请人 河海大学

地址 211100 江苏省南京市江宁开发区佛城
西路 8 号

(72) 发明人 吴学文 孔飞 谭国平 周燕
朱晓凯 曹锋 李鹏 崔楠 江磊
秦操

(74) 专利代理机构 南京经纬专利商标代理有限
公司 32200

代理人 杨楠

(51) Int. Cl.

H04L 9/00(2006. 01)

H04W 12/00(2009. 01)

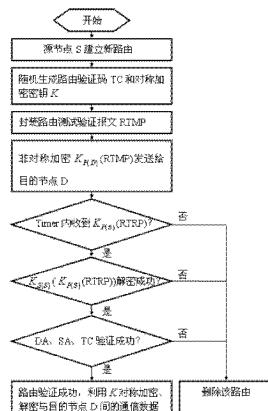
权利要求书1页 说明书4页 附图3页

(54) 发明名称

移动 Ad Hoc 网络路由和数据安全保障方法

(57) 摘要

本发明公开了一种移动 AdHoc 网络路由和数据安全保障方法，属于网络安全技术领域。本发明对建立的路由进行端到端的测试验证，同时为防止恶意节点窃取路由测试验证报文，冒充目的节点伪造测试应答消息欺骗源节点，对路由测试验证报文进行非对称加密，增强安全性。本发明同时对在该路由上的数据通信进行对称加密，为了保护对称加密密钥的安全性，将对称加密密钥封装在路由测试验证报文中，一起进行非对称加密后发送给目的节点，同时完成了路由测试认证和数据对称加密密钥的安全传输，起到同时保护路由与数据安全的效果。本发明方法能够以较小的网络开销同时保护网络中的路由与数据安全，尤其适合于移动 AdHoc 网络，也可用于其它网络。



1. 一种移动 Ad Hoc 网络路由和数据安全保障方法,其特征在于,

在网络初始化阶段,各节点分别生成各自用于非对称加密的公钥和私钥,公钥对其它节点公开,私钥自己保存,各节点中均存储有其它节点的公钥;

当新的路由建立后首先进行以下路由验证:

源节点先为该路由生成路由验证码及对称加密密钥,将两者封装于路由测试验证报文中,再用目的节点的公钥将封装后的路由测试验证报文进行非对称加密之后,发给目的节点,并等待一段预定的时间,如在该段时间内未收到目的节点发送的路由测试应答报文,则路由验证失败,源节点删除该路由记录;

目的节点用自身的私钥对收到的路由测试验证报文进行解密,得到路由验证码与对称加密密钥,然后生成包含该路由验证码的路由测试应答报文并用源节点的公钥对路由测试应答报文进行非对称加密之后,发给源节点;如目的节点用自身的私钥无法对收到的路由测试验证报文进行解密,则路由验证失败,目的节点将路由测试验证报文丢弃,不做其它处理;

源节点用自身的私钥对收到的路由测试应答报文进行解密,并根据路由测试应答报文中的路由验证码与初始生成的路由验证码是否一致,判断路由验证是否成功;如源节点用自身的私钥无法对收到的路由测试应答报文进行解密,或者,路由测试应答报文中的路由验证码与初始生成的路由验证码不一致,则路由验证失败,源节点删除该路由记录;

路由验证成功后,启用该路由并用所述对称加密密钥进行通信数据的加解密。

2. 如权利要求 1 所述移动 Ad Hoc 网络路由和数据安全保障方法,其特征在于,源节点为各路由随机生成路由验证码及对称加密密钥,且不同路由的路由验证码及对称加密密钥也不同。

3. 如权利要求 1 所述移动 Ad Hoc 网络路由和数据安全保障方法,其特征在于,所述路由测试验证报文包括:源节点地址、目的节点地址、报文类型、路由验证码、对称加密密钥。

4. 如权利要求 1 所述移动 Ad Hoc 网络路由和数据安全保障方法,其特征在于,所述路由测试应答报文包括:目的节点地址、源节点地址、报文类型、路由验证码。

移动 Ad Hoc 网络路由和数据安全保障方法

技术领域

[0001] 本发明涉及移动 Ad Hoc 网络, 尤其涉及一种移动 Ad Hoc 网络路由和数据安全保障方法, 属于网络安全技术领域。

背景技术

[0002] 移动 Ad Hoc 网络是一种特殊的无中心、自组织、多跳的无线通信网络。它与传统网络的显著差别有三点: 无固定基础的网络设施(基站、路由器、交换机等)、动态的网络拓扑、资源受限。自由开放的网络环境、脆弱的无线信道使其面临着诸多的安全问题, 尤其体现在路由与数据安全方面。

[0003] 移动 Ad Hoc 网络中不存在路由器等中心基础设施, 网络节点既是主机又是路由器, 相互协作, 共同担任着执行路由协议的任务。因此, 路由的安全依赖于所有节点都能严格按照路由规则去执行路由的建立与维护工作, 这是移动 Ad Hoc 网络路由安全脆弱性的关键所在。恶意节点趁机而入, 采取各种非法手段进行路由攻击。移动 Ad Hoc 网络路由面临的攻击方式多种多样, 典型的有 blackhole 黑洞攻击、虫洞攻击、篡改 RREP 报文信息等。同时, 移动 Ad Hoc 网络数据通信建立在多跳路由上, 源节点发送的数据通过中间节点的依次转发才能达到目的节点。数据的安全依赖于路由的正确性、路由沿途中间节点的诚实性、无线信道的安全性, 这在移动 Ad Hoc 网络中是难以保证的。因此, 移动 Ad Hoc 网络数据极易受到窃取、篡改、重放、泄漏、伪造等各类攻击行为。

[0004] 移动 Ad Hoc 网络面临的路由与数据安全问题通常比较隐蔽且难以防范, 对于路由安全, 往往通过改进路由协议, 增加一系列的安全机制来增强路由安全性, 如身份认证、数字签名技术等。数字签名等技术源于非对称加密技术, 非对称加密需要两个密钥: “公钥”和“私钥”。公钥对外公开, 私钥自己保留, 两者互为一对。如果用公钥加密, 只有对应的私钥才能解密, 反之亦然。非对称加密安全性高, 但复杂度大, 在资源受限的 Ad Hoc 网络并不能频繁使用。此外路由攻击方式多种多样, 往往只是针对其中部分进行相应的防范, 很难以偏概全。对于数据安全, 往往采取数据加密技术来保证数据安全, 由于 Ad Hoc 网络资源受限, 一般采取复杂度小的对称加密技术, 如 DES 加密算法。但对称加密安全性低, 加密解密采用同一个密钥, 需要一条绝对安全的信道将密钥发送给对方, 这在移动 Ad Hoc 网络中是无法保证的。其次, 路由与数据传输, 后者虽然依赖前者, 但两者的网络功能相对独立, 两者面临的安全问题也不相同, 以往的研究, 对路由安全与数据安全问题往往分开考虑, 分别提出相应的解决方案, 缺乏一种统一的方案能够同时有效保护移动 Ad Hoc 网络路由与数据安全。

发明内容

[0005] 本发明所要解决的技术问题在于克服现有技术不足, 提供一种移动 Ad Hoc 网络路由和数据安全保障方法, 能够以较小的网络开销同时保护移动 Ad Hoc 网络的路由与数据安全。

[0006] 本发明具体采用以下技术方案:

一种移动 Ad Hoc 网络路由和数据安全保障方法，

在网络初始化阶段，各节点分别生成各自用于非对称加密的公钥和私钥，公钥对其他节点公开，私钥自己保存，各节点中均存储有其他节点的公钥；

当新的路由建立后首先进行以下路由验证：

源节点先为该路由生成路由验证码及对称加密密钥，将两者封装于路由测试验证报文中，再用目的节点的公钥将封装后的路由测试验证报文进行非对称加密之后，发给目的节点，并等待一段预定的时间，如在该段时间内未收到目的节点发送的路由测试应答报文，则路由验证失败，源节点删除该路由记录；

目的节点用自身的私钥对收到的路由测试验证报文进行解密，得到路由验证码与对称加密密钥，然后生成包含该路由验证码的路由测试应答报文并用源节点的公钥对路由测试应答报文进行非对称加密之后，发给源节点；如目的节点用自身的私钥无法对收到的路由测试验证报文进行解密，则路由验证失败，目的节点将路由测试验证报文丢弃，不做其它处理；

源节点用自身的私钥对收到的路由测试应答报文进行解密，并根据路由测试应答报文中的路由验证码与初始生成的路由验证码是否一致，判断路由验证是否成功；如源节点用自身的私钥无法对收到的路由测试应答报文进行解密，或者，路由测试应答报文中的路由验证码与初始生成的路由验证码不一致，则路由验证失败，源节点删除该路由记录；

路由验证成功后，启用该路由并用所述对称加密密钥进行通信数据的加解密。

[0007] 本发明技术方案能够同时有效保护移动 Ad Hoc 网络路由与数据安全。基于非对称加密的路由测试验证保证了路由的正确性。基于对称加密的数据保护，并将对称加密密钥封装在路由测试验证报文中，一起进行非对称加密后发送给目的节点，既节省了开销又保证了对称加密密钥的安全，同时排除了如果正确的路由中存在恶意节点发起数据窃取、伪造、篡改等攻击的可能性。此外，路由测试验证只需源节点和目的节点之间的一次双向传输，数据量少，而数据通信传输频繁，数据量大，将非对称加密用于路由测试验证，对称加密用于数据保护，对于资源受限的移动 Ad Hoc 网络是比较合适的，减小了网络的开销，可行性高。本发明也可用于对其他网络的路由与数据安全保护。

附图说明

[0008] 图 1 为本发明的路由和数据安全保障方法中源节点端的工作流程图；

图 2 为具体实施方式中使用的一种路由测试验证报文的结构图；

图 3 为本发明的路由和数据安全保障方法中目的节点端的工作流程图；

图 4 为具体实施方式中使用的一种路由测试应答报文的结构图。

具体实施方式

[0009] 多数路由攻击行为采取的方式不同，但都会导致共同的最终结果，即破坏路由的正确性，制造虚假的路由信息。因此，本发明从结果的角度出发，对建立的路由进行端到端的测试验证，同时为防止恶意节点窃取路由测试验证报文，冒充目的节点伪造测试应答消息欺骗源节点，对路由测试验证报文进行非对称加密，增强安全性。本发明同时对在该路面上的数据通信进行对称加密，为了保护对称加密密钥的安全性，将对称加密密钥封装在路

由测试验证报文中,一起进行非对称加密后发送给目的节点,同时完成了路由测试认证和数据对称加密密钥的安全传输,起到同时保护移动 Ad Hoc 网络路由与数据安全的效果。

[0010] 基于以上分析即可得到本发明的移动 Ad Hoc 网络路由和数据安全保障方法,具体如下:

在网络初始化阶段,各节点分别生成各自用于非对称加密的公钥和私钥,公钥对其他节点公开,私钥自己保存,各节点中均存储有其它节点的公钥;

当新的路由建立后首先进行以下路由验证:

源节点先为该路由生成路由验证码及对称加密密钥,将两者封装于路由测试验证报文中,再用目的节点的公钥将封装后的路由测试验证报文进行非对称加密之后,发给目的节点,并等待一段预定的时间,如在该段时间内未收到目的节点发送的路由测试应答报文,则路由验证失败,源节点删除该路由记录;

目的节点用自身的私钥对收到的路由测试验证报文进行解密,得到路由验证码与对称加密密钥,然后生成包含该路由验证码的路由测试应答报文并用源节点的公钥对路由测试应答报文进行非对称加密之后,发给源节点;如目的节点用自身的私钥无法对收到的路由测试验证报文进行解密,则路由验证失败,目的节点将路由测试验证报文丢弃,不做其它处理;

源节点用自身的私钥对收到的路由测试应答报文进行解密,并根据路由测试应答报文中的路由验证码与初始生成的路由验证码是否一致,判断路由验证是否成功;如源节点用自身的私钥无法对收到的路由测试应答报文进行解密,或者,路由测试应答报文中的路由验证码与初始生成的路由验证码不一致,则路由验证失败,源节点删除该路由记录;

路由验证成功后,启用该路由并用所述对称加密密钥进行通信数据的加解密。

[0011] 优选地,源节点为各路由随机生成路由验证码及对称加密密钥,且不同路由的路由验证码及对称加密密钥也不同。

[0012] 为便于公众理解,下面结合附图对本发明的技术方案进行进一步地详细说明:

在网络初始化阶段,各节点 i 产生各自用于非对称加密的公钥 $K_{P(i)}$ 和私钥 $K_{S(i)}$, (其中 $i = 0, \dots, N$, i 为节点 i 的编号, N 为网络节点总数), 公钥 $K_{P(i)}$ 对其他所有节点公开,私钥自己保留,各节点将其它节点的公钥存储在自身的存储器中。

[0013] 图 1 示出了本发明的路由和数据安全保障方法中源节点端的工作流程,如图所示,每当源节点 S ($S \in [0, N]$) 建立到目的节点 D ($D \in [0, N]$) 的新路由时,首先对该路由的正确性进行端到端的测试验证。源节点 S 为该路由随机生成路由验证码 TC(Testing Code) 与数据对称加密密钥 K , 并将 TC 与 K 两项信息添加存储到对应的路由表项中, 不同路由的验证码 TC 与数据对称加密密钥 K 也不同。然后将 K 和 TC 封装在路由测试验证报文 RTMP 中, 图 2 示出了一种封装后的路由测试验证报文结构, 该路由测试验证报文包括源节点地址 SA、目的节点地址 DA、报文类型码 Type、路由验证码 TC、以及数据对称加密密钥 K 五项信息。SA、DA 用于目的节点 D 确认该测试消息的来源和是否发送给自己; Type 用于表明报文类型为路由测试验证报文; TC 用于路由验证, 目的节点 D 只需将 TC 原封不动地回发给源节点, 由源节点验证其前后的一致性以判断路由的正确性; K 用于之后数据通信的对称加解

密。源节点 S 将封装后的路由测试验证报文 $RTMP$ 利用自身存储器中保存的目的节点 D 的公钥 $K_{P(D)}$ 进行非对称加密 $K_{P(D)}(RTMP)$ ，沿待测试的路由发送给目的节点 D ，同时启动定时器 $Timer$ 来等待目的节点 D 的应答。

[0014] 图 3 示出了本发明的路由和数据安全保障方法中目的节点端的工作流程，如图所示，目的节点 D 接受到 $K_{P(D)}(RTMP)$ 后，利用自己的私钥 $K_{S(D)}$ 进行解密 $K_{S(D)}(K_{P(D)}(RTMP))$ 得到路由测试验证报文 $RTMP$ 与对称加密密钥 K 。若解密失败，说明该路由可能存在风险，直接丢弃，不做处理。解密成功后，在对 $RTMP$ 中路由测试验证报文 Type、SA、DA 各项参数验证无误后，目的节点 D 保存本条路由数据通信的对称加密密钥 K ，然后生成路由测试应答报文 $RTRP$ ，图 4 示出了一种路由测试应答报文的结构，该路由测试验证报文包括目的节点地址 DA、源节点地址 SA、报文类型 Type、路由验证码 TC 四项信息。其中 DA、SA 用于源节点 S 确认该测试消息的来源和是否发送给自己；Type 用于表明消息类型为 $RTRP$ ；测试码 TC 用于路由验证，其值应与路由测试验证报文 $RTMP$ 中 TC 值一致。目的节点 D 利用存储器中保存的源节点 S 的公钥 $K_{P(S)}$ 对路由测试应答报文 $RTRP$ 进行非对称加密 $K_{P(S)}(RTRP)$ ，回发给源节点 S 。

[0015] 如图 1 所示，源节点 S 若在定时器 $Timer$ 超时后仍未收到目的节点 D 发送的 $K_{P(S)}(RTRP)$ ，则认为该路由不正确或稳定性不高，删除该路由。若在定时器 $Timer$ 设定时间内接收到 $K_{P(S)}(RTRP)$ ，利用用自己的私钥 $K_{S(S)}$ 进行解密 $K_{S(S)}(K_{P(S)}(RTRP))$ 得到测试应答报文 $RTRP$ 。若解密失败，说明该路由可能存在风险，同样删除该路由。解密成功后，在对测试应答报文 $RTRP$ 中的 Type、DA、SA 各项参数验证无误后，进行 TC 路由验证码前后一致验证，若 $RTRP$ 和 $RTMP$ 中 TC 相同，则路由验证成功，启用该路由；否则，认证失败，删除该路由。由于采用安全性较强的非对称加密，除了目的节点，其他节点无法获取路由测试验证报文 $RTMP$ 里的内容 TC 的值，克服了恶意节点伪造 $RTRP$ 欺骗源节点的弊端，具备较高安全性。

[0016] 路由认证成功后，源节点 S 与目的节点 D 便可利用该路由的数据对称加密密钥 K 进行通信数据的对称加密，实现安全的数据通信。同样，因为密钥 K 封装在路由测试验证报文 $RTMP$ 中并采用非对称加密保护，除了目的节点，其他任何节点都无法获取，克服了对称加密密钥安全性得不到保障的弊端，同时排除了如果正确的路由中存在其他恶意节点发起数据窃取、伪造、篡改等攻击的可能性，具备较高安全性。因此，本发明能同时高效地保护移动 Ad Hoc 网络路由与数据安全。

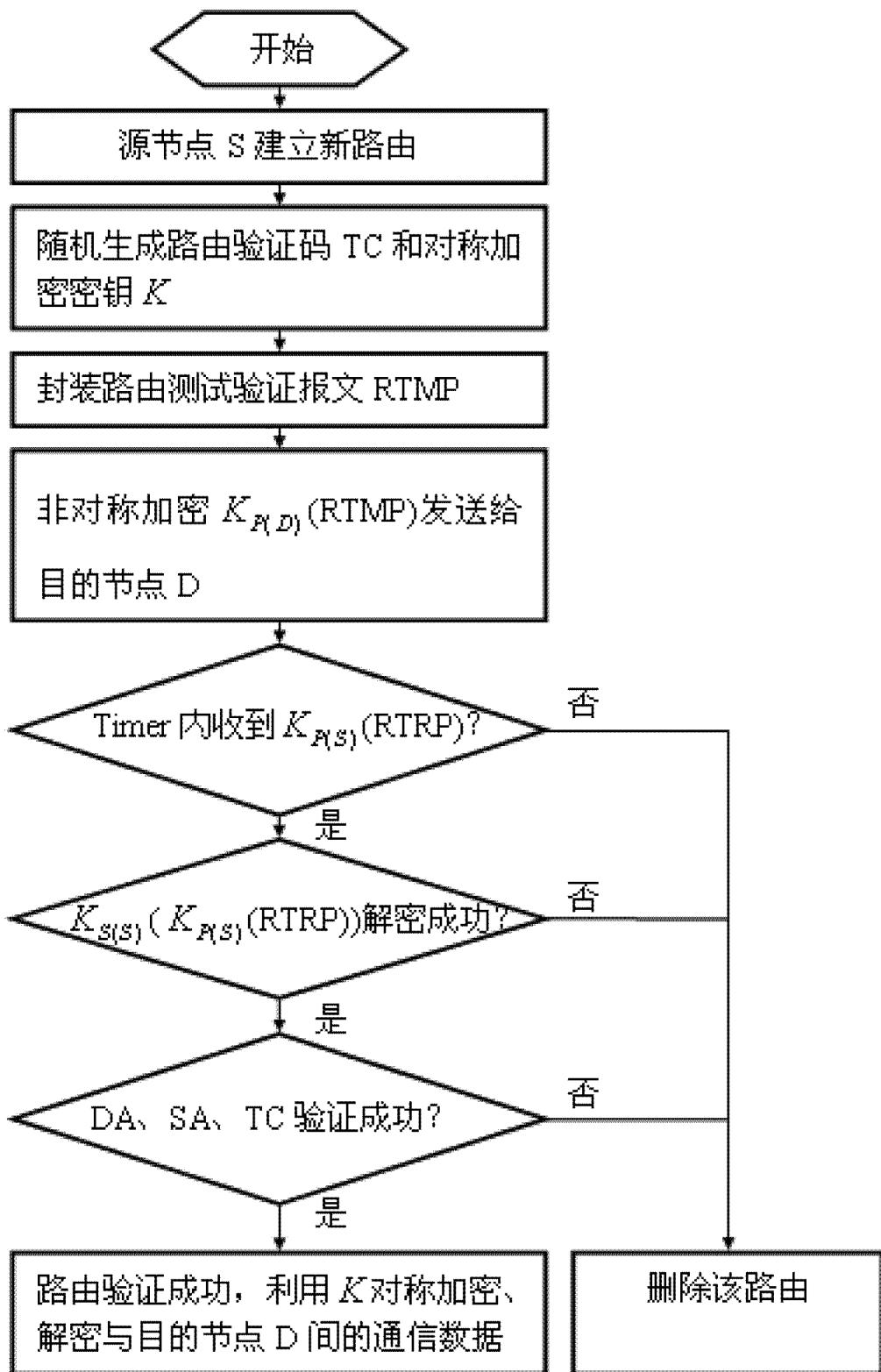


图 1

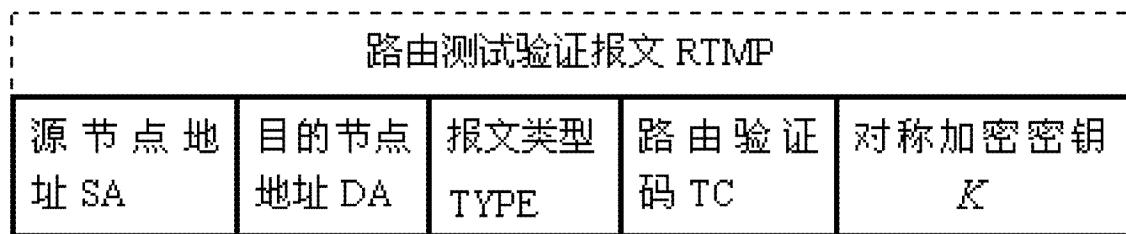


图 2

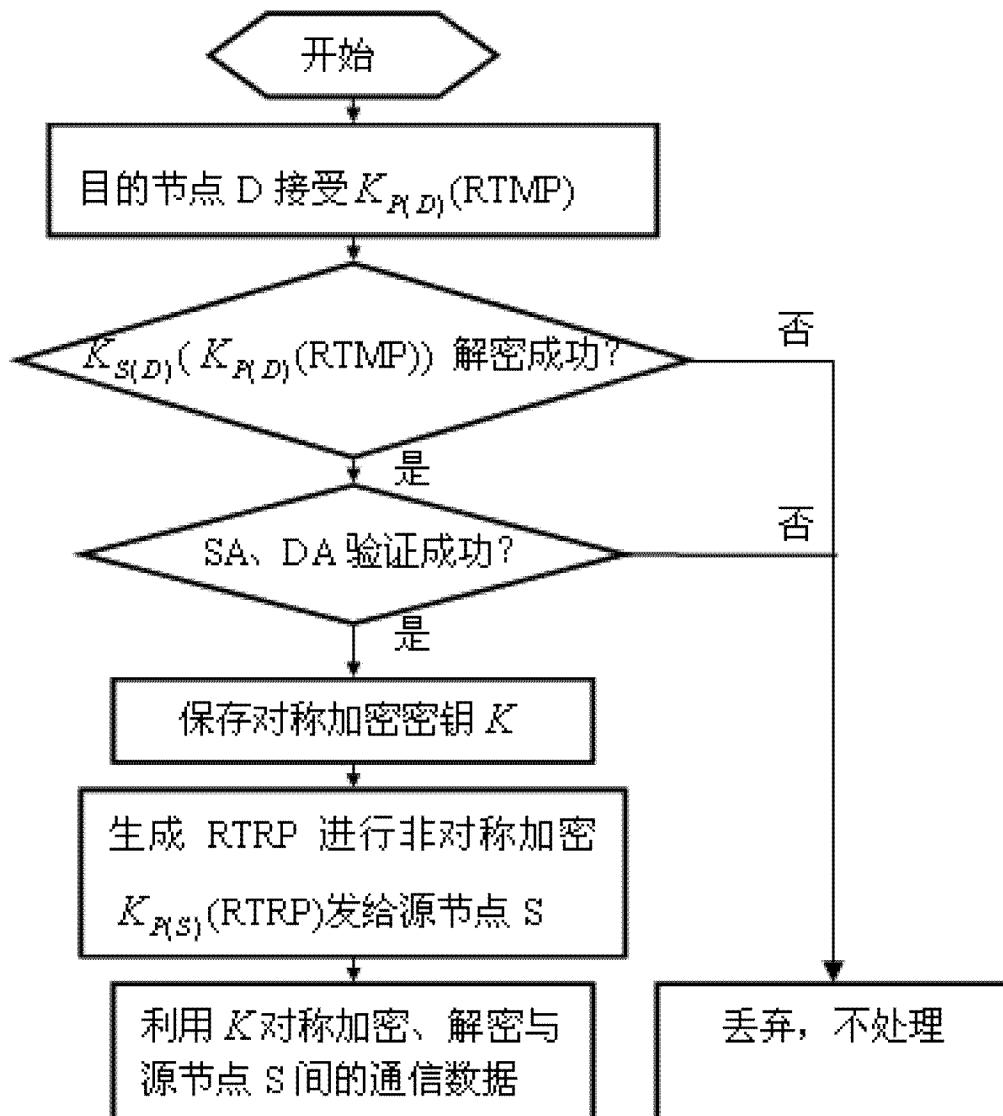


图 3

路由测试应答报文 RTRP			
目的节点地址 DA	源节点地址 SA	报文类型 TYPE	路由验证码 TC

图 4