(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 108737431 B
(45)授权公告日 2020.09.15

(21)申请号 201810524809.2

(22)申请日 2018.05.28

(65)同一申请的已公布的文献号
申请公布号 CN 108737431 A

(43)申请公布日 2018.11.02

(73)专利权人 深圳职业技术学院
地址 518000 广东省深圳市南山区西丽街道西丽湖镇西丽湖畔

(72)发明人 成荣

(74)专利代理机构 深圳市汉唐知识产权代理有限公司 44399
代理人 刘海军

(51)Int.Cl.
H04L 29/06(2006.01)
H04W 12/02(2009.01)
H04W 12/06(2009.01)

(56)对比文件
CN 107317789 A,2017.11.03
US 9197411 B2,2015.11.24
US 7551915 B1,2009.06.23
US 2017272252 A1,2017.09.21

审查员 薛乐梅

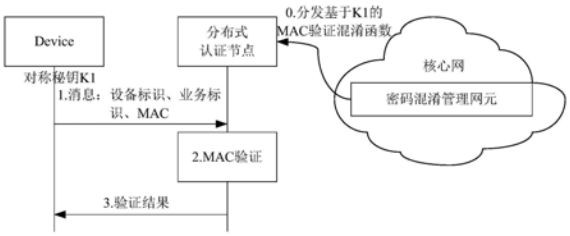
权利要求书2页 说明书8页 附图3页

(54)发明名称

IoT场景下基于混淆的分等级分布式认证方法、装置及系统

(57)摘要

一种IoT场景下基于混淆的分等级分布式认证方法及系统，联网终端设备用于通过网络与分布式认证节点或基站连接，联网终端设备内存储有MAC函数和对称秘钥K1，并可计算MAC，并将用于MAC计算的参数的至少一项发送至分布式认证节点或基站；分布式认证节点或基站用于通过网络接收联网终端设备发送的信息，根据设备标识确定验证混淆函数f1，输入MAC以及计算MAC用到的参数，若函数f1输出1，则代表验证通过；若输出0，则代表验证不通过；密码混淆管理网元根据对称密钥K1，计算基于对称密钥K1的MAC验证混淆函数f1，实现为验证MAC计算是否正确，同时发送设备标识和函数f1至分布式认证节点或基站。



CN 108737431 B

1.一种IoT场景下基于混淆的分等级分布式认证系统,其特征是:所述的认证系统包括终端设备、分布式认证节点或基站以及密码混淆管理网元,

所述的终端设备用于通过网络与所述分布式认证节点或所述基站连接,终端设备内存储有消息验证码函数和对称秘钥K1,并可根据消息验证码函数、所述对称秘钥、终端设备标识、业务标识以及新鲜参数计算消息验证码,并将终端设备标识、业务标识、消息验证码以及用于消息验证码计算的新鲜参数发送至所述分布式认证节点或所述基站;

所述分布式认证节点或基站用于通过网络接收终端设备发送的信息,根据设备标识确定消息验证码验证混淆函数f1,输入消息验证码以及计算消息验证码用到的参数,若消息验证码验证混淆函数f1的输出为1,则代表验证通过;若消息验证码验证混淆函数f1的输出为0,则代表验证不通过;

所述的密码混淆管理网元根据隐藏的秘钥K和设备标识推衍子验证混淆函数f2计算出对称秘钥K1,并根据对称秘钥K1,计算基于对称秘钥K1的消息验证码验证混淆函数f1,实现功能为验证消息验证码计算是否正确,同时发送设备标识和消息验证码验证混淆函数f1至所述分布式认证节点或所述基站。

2.根据权利要求1所述的IoT场景下基于混淆的分等级分布式认证系统,其特征是:所述的新鲜参数为时间值、随机数、序列号和计数值中的至少一项。

3.根据权利要求1所述的IoT场景下基于混淆的分等级分布式认证系统,其特征是:所述的终端设备为IoT设备或UE。

4.一种IoT场景下基于混淆的分等级分布式认证系统中的密码混淆管理网元,其特征是:所述的密码混淆管理网元包括混淆控制单元、混淆存储单元和混淆网络传输单元,混淆存储单元用于存储隐藏秘钥K,并能将隐藏秘钥K传输给混淆控制单元,所述的混淆控制单元用于根据隐藏秘 钥K和设备标识推衍子验证混淆函数f2计算出对称秘钥K1,并根据对称秘钥K1,计算消息验证码验证混淆函数f1,实现功能为验证消息验证码计算是否正确,所述的混淆网络传输单元与混淆控制单元连接,混淆网络传输单元用于将设备标识和消息验证码验证混淆函数f1发送至分布式认证节点或基站。

5.一种与权利要求4所述的密码混淆管理网元配合使用的终端设备,其特征是:所述的终端设备包括终端网络传输单元、终端存储单元和终端控制单元,所述的终端存储单元用于存储消息验证码函数和对称秘钥,终端存储单元与终端控制单元连接,所述的终端控制单元用于根据消息验证码函数、所述对称秘钥、终端设备标识、业务标识、以及新鲜参数计算消息验证码,所述的终端网络传输单元与终端控制单元连接,终端网络传输单元用于将设备标识、业务标识、消息验证码以及用于消息验证码计算的新鲜参数发送至分布式认证节点或所述基站。

6.一种与权利要求4所述的密码混淆管理网元配合使用的分布式认证节点,其特征是:所述的分布式认证节点包括节点网络传输单元和节点混淆验证单元,节点网络传输单元与节点混淆验证单元连接,所述的节点网络传输单元用于接收终端设备发送的信息,所述的节点混淆验证单元用于根据设备标识确定消息验证码验证混淆函数f1,输入消息验证码以及计算消息验证码用到的参数,通过消息验证码验证混淆函数f1对消息验证码进行验证。

7.一种IoT场景下基于混淆的分等级分布式认证装置,其特征是:所述的认证装置包括密码混淆管理网元、终端设备和分布式认证节点或基站,所述的密码混淆管理网元包括混

淆控制单元、混淆存储单元和混淆网络传输单元，混淆存储单元用于存储对称秘钥，并能将对称秘钥传输给混淆控制单元，所述的混淆控制单元用于根据对称秘钥计算消息验证码验证混淆函数f1，实现功能为验证消息验证码计算是否正确，所述的混淆网络传输单元与混淆控制单元连接，混淆网络传输单元用于将设备标识和消息验证码验证混淆函数f1发送至分布式认证节点或基站；所述的终端设备包括终端网络传输单元、终端存储单元和终端控制单元，所述的终端存储单元用于存储消息验证码函数和对称秘钥，终端存储单元与终端控制单元连接，所述的终端控制单元用于根据消息验证码函数、所述对称秘钥、终端设备标识、业务标识、以及新鲜参数计算消息验证码，所述的终端网络传输单元与终端控制单元连接，终端网络传输单元用于将设备标识、业务标识、消息验证码以及用于消息验证码计算的新鲜参数发送至分布式认证节点或所述基站；分布式认证节点或基站包括节点网络传输单元和节点混淆验证单元，节点网络传输单元与节点混淆验证单元连接，所述的节点网络传输单元用于接收终端设备发送的信息，所述的节点混淆验证单元用于根据设备标识确定消息验证码验证混淆函数f1，输入消息验证码以及计算消息验证码用到的参数，通过消息验证码验证混淆函数f1对消息验证码进行验证。

8.一种利用如权利要求1或2或3所述的IoT场景下基于混淆的分等级分布式认证系统的IoT场景下基于混淆的分等级分布式认证方法，其特征是：所述的认证方法包括下述步骤：

步骤1：终端设备根据消息验证码函数、所述对称秘钥、终端设备标识、业务标识以及新鲜参数计算消息验证码，终端设备发送设备标识、消息验证码以及用于消息验证码计算的时间值、随机数、序列号和计数值中的至少一项至分布式认证节点或基站；

步骤2：分布式认证节点或基站基于设备标识确定消息验证码验证混淆函数f1，输入消息验证码以及终端设备标识、业务标识、新鲜参数，若消息验证码验证混淆函数f1的输出为1，则代表验证通过，若消息验证码验证混淆函数f1的输出为0，则代表验证不通过。

9.根据权利要求8所述的IoT场景下基于混淆的分等级分布式认证方法，其特征是：采用基站时，消息验证码验证混淆函数f1输入还包括基站标识，消息验证码验证混淆函数f1输出为0或者1。

10.根据权利要求8所述的IoT场景下基于混淆的分等级分布式认证方法，其特征是：所述的终端设备计算消息验证码需要用到基站标识，所述的终端设备获得基站标识的方式为基站广播自己的标识信息，当终端设备接入基站时获得；或者基站标识预置在终端设备内。

IoT场景下基于混淆的分等级分布式认证方法、装置及系统

技术领域

[0001] 本发明公开一种分等级分布式认证方法，特别是一种IoT场景下基于混淆的分等级分布式认证方法、装置及系统。

背景技术

[0002] 未来是一个物联网(即IoT)的时代，将会有海量的设备部署在现有网络中。另外，物联网也是5G的一个重要场景，因此将会有海量的IoT设备接入5G的网络。物联网支撑的业务包括车联网、传感器网络等业务形式，其最大的特征为，更多低成本设备的部署。从安全的角度考虑，海量设备的接入也会带来更大的安全挑战。

[0003] 传统移动通信(如LTE)，每个智能终端就是一个设备，其内的USIM(Universal Subscriber Identity Module，全球用户身份模块)存储着一个安全密钥K，而核心网的HSS(Home Subscriber Server，归属用户服务器)存储相同的安全密钥K，并且都可以通过UE(User Equipment，用户设备)的标识IMSI(International Mobile Subscriber Identification Number，国际移动用户识别码)进行检索。

[0004] 请参看附图1，图1为LTE网络中UE的认证方式。由图1中可以看到，UE与HSS共享对称密钥K。首先UE发送IMSI至RAN(Radio Access Network，无线接入网络基站)，并由RAN发送IMSI至MME(Mobility Management Entity，，移动管理单元，LTE接入网络的关键控制节点)，之后MME发送认证向量请求至HSS，所述认证向量请求包括IMSI，HSS根据IMSI确定对称密钥K，并计算认证向量，然后发送认证向量至MME，之后MME利用认证向量执行与UE的双向认证，从而验证UE是否合法。可以看出，传统LTE的认证方式要求每次认证都需要HSS的参与，另外，执行认证的主题为核心控制网元MME。

[0005] 请参看附图2，图2为直接采用传统LTE方式的IoT网络认证框架图，从图2中可以看到，若每个IoT device都直接采用移动通信的认证方式，将会对HSS造成海量的信令，以及安全操作的冲击，对运营商核心网造成负担，主要原因为，每次认证都会向HSS发送认证向量请求。

[0006] 常规的基于与LTE方式类似的对称认证技术，虽然对称认证与传统移动通信的安全流程类似，方案也比较简单，但是容易造成核心网的信令风暴。不利于海量IoT网络的部署。

[0007] 现有技术中，还存在有基于证书类似的非对称认证技术，即每个IoT device都分发了公私钥对(PK，SK)，同时被颁发了PK的证书(cert)；此时通过在RAN侧部署验证证书Cert的公钥，即可完成对于IoT设备的验证，基本流程为，IoT device利用SK对消息m计算签名(即Sign)；并发送cert、PK、m和Sign至RAN；RAN首先验证Cert的正确性，若验证Cert通过，则相信PK为所述IoT device的公钥，再使用PK验证Sign，若Sign也验证通过，则相信消息m为合法的IoT device发送。

[0008] 上述基于非对称认证的方式支持分布式的认证方式，即任意分布式的节点(如RAN)通过简单的配置都可以执行对于IoT Device的认证，但是，为了确保PK与IoT device

身份的绑定,需要Cert的参与,此时运营商必须要部署所有PKI基础设备才可,因此,此方式将会提供整体安全管理的复杂度。

发明内容

[0009] 针对上述提到的现有技术中的联网设备部署在现有网络中认证方法复杂度高或核心网通信压力大的缺点,本发明提供一种IoT场景下基于混淆的分等级分布式认证方法及系统,其采用混淆函数进行MAC认证,可实现单向验证的效果,简化认证方法复杂度。

[0010] 本发明解决其技术问题采用的技术方案是:一种IoT场景下基于混淆的分等级分布式认证系统,认证系统包括终端设备、分布式认证节点或基站以及密码混淆管理网元,

[0011] 所述的终端设备用于通过网络与所述分布式认证节点或所述基站连接,终端设备内存储有消息验证码函数和对称秘钥K1,并可根据消息验证码函数、所述对称秘钥、终端设备标识、业务标识以及新鲜参数计算消息验证码,并将终端设备标识、业务标识、消息验证码以及用于消息验证码计算的新鲜参数发送至所述分布式认证节点或所述基站;

[0012] 所述分布式认证节点或基站用于通过网络接收终端设备发送的信息,根据设备标识确定验证混淆函数f1,输入消息验证码以及计算消息验证码用到的参数,若验证混淆函数f1的输出为1,则代表验证通过;若验证混淆函数f1的输出为0,则代表验证不通过;

[0013] 所述的密码混淆管理网元根据隐藏的秘钥K和设备标识推衍子验证混淆函数f2计算出对称秘钥K1,并根据对称密钥K1,计算基于对称密钥K1的消息验证码验证混淆函数f1,实现功能为验证消息验证码计算是否正确,同时发送设备标识和验证混淆函数f1至所述分布式认证节点或所述基站。

[0014] 一种IoT场景下基于混淆的分等级分布式认证系统中的密码混淆管理网元,密码混淆管理网元包括混淆控制单元、混淆存储单元和混淆网络传输单元,混淆存储单元用于存储隐藏秘钥K,并能将隐藏秘钥K传输给混淆控制单元,所述的混淆控制单元用于根据隐藏密钥K和设备标识推衍子验证混淆函数f2计算出对称秘钥K1,并根据对称密钥K1,计算消息验证码验证混淆函数f1,实现功能为验证消息验证码计算是否正确,所述的混淆网络传输单元与混淆控制单元连接,混淆网络传输单元用于将设备标识和验证混淆函数f1发送至分布式认证节点或基站。

[0015] 一种与上述的密码混淆管理网元配合使用的终端设备,终端设备包括终端网络传输单元、终端存储单元和终端控制单元,所述的终端存储单元用于存储消息验证码函数和对称秘钥,终端存储单元与终端控制单元连接,所述的终端控制单元用于根据消息验证码函数、所述对称密钥、终端设备标识、业务标识、以及新鲜参数计算消息验证码,所述的终端网络传输单元与终端控制单元连接,终端网络传输单元用于将设备标识、业务标识、消息验证码以及用于消息验证码计算的新鲜参数发送至分布式认证节点或所述基站。

[0016] 一种与上述的密码混淆管理网元配合使用的分布式认证节点,所述的分布式认证节点包括节点网络传输单元和节点混淆验证单元,节点网络传输单元与节点混淆验证单元连接,所述的节点网络传输单元用于接收终端设备发送的信息,所述的节点混淆验证单元用于根据设备标识确定验证混淆函数f1,输入消息验证码以及计算消息验证码用到的参数,通过验证混淆函数f1对消息验证码进行验证。

[0017] 一种IoT场景下基于混淆的分等级分布式认证装置,认证装置包括密码混淆管理

网元、终端设备和分布式认证节点或基站，所述的密码混淆管理网元包括混淆控制单元、混淆存储单元和混淆网络传输单元，混淆存储单元用于存储对称秘钥，并能将对称秘钥传输给混淆控制单元，所述的混淆控制单元用于根据对称密钥计算消息验证码验证混淆函数f1，实现功能为验证消息验证码计算是否正确，所述的混淆网络传输单元与混淆控制单元连接，混淆网络传输单元用于将设备标识和验证混淆函数f1发送至分布式认证节点或基站；所述的终端设备包括终端网络传输单元、终端存储单元和终端控制单元，所述的终端存储单元用于存储消息验证码函数和对称秘钥，终端存储单元与终端控制单元连接，所述的终端控制单元用于根据消息验证码函数、所述对称密钥、终端设备标识、业务标识、以及新鲜参数计算消息验证码，所述的终端网络传输单元与终端控制单元连接，终端网络传输单元用于将设备标识、业务标识、消息验证码以及用于消息验证码计算的新鲜参数发送至分布式认证节点或所述基站；分布式认证节点或基站包括节点网络传输单元和节点混淆验证单元，节点网络传输单元与节点混淆验证单元连接，所述的节点网络传输单元用于接收终端设备发送的信息，所述的节点混淆验证单元用于根据设备标识确定验证混淆函数f1，输入消息验证码以及计算消息验证码用到的参数，通过验证混淆函数f1对消息验证码进行验证。

[0018] 一种利用如上述的IoT场景下基于混淆的分等级分布式认证系统的IoT场景下基于混淆的分布式认证方法，所述的认证方法包括下述步骤：

[0019] 步骤1：终端设备根据消息验证码函数、所述对称密钥、终端设备标识、业务标识以及新鲜参数计算消息验证码，终端设备发送设备标识、消息验证码以及用于消息验证码计算的time、nonce、SQN和counter的至少一项至分布式认证节点或基站；

[0020] 步骤2：分布式认证节点或基站基于设备标识确定验证混淆函数f1，输入消息验证码以及终端设备标识、业务标识、新鲜参数，若验证混淆函数f1的输出为1，则代表验证通过，若验证混淆函数f1的输出为0，则代表验证不通过。

[0021] 本发明解决其技术问题采用的技术方案进一步还包括：

[0022] 所述的新鲜参数为time、nonce、SQN和counter中的至少一项。

[0023] 所述的终端设备为IoT设备或UE。

[0024] 采用基站时，消息验证码验证混淆函数f1输入还包括基站标识，验证混淆函数f1输出为0或者1。

[0025] 所述的终端设备计算消息验证码需要用到基站标识，所述的终端设备获得基站标识的方式为基站广播自己的标识信息，当终端设备接入基站时获得；或者基站标识预置在终端设备内。

[0026] 本发明的有益效果是：本发明与传统方法不同，基于混淆的分等级分布式对称认证方法，分布式认证节点仅需部署混淆后的MAC验证程序；而设备则跟普通对称密钥机制相同，仅需要存储一个对称密钥即可。方案满足分布式节点在没有对称密钥K的情况下也可以验证设备的接入认证。本发明将通过采用密码混淆技术，在对称密码的基础上设计更高效的分布式分等级认证方案，本发明中的分布式是指，通过安全的配置，可以在任一分布式的节点验证device的消息，不需要调用核心节点，如HSS，从而降低核心处理节点的安全复杂度，提高整网的最优资源部署。另外分等级是分布式认证节点不需要存储单个设备的验证功能，仅存储上层根密钥的验证方式。基于此上层根密钥的验证方式，即可验证所有。

[0027] 下面将结合附图和具体实施方式对本发明做进一步说明。

附图说明

[0028] 图1为现有技术中LTE网络中UE的认证方式示意图。

[0029] 图2为直接采用传统LTE方式的IoT网络认证框架图。

[0030] 图3为本发明实施例一认证方法的基本流程图。

[0031] 图4为本发明实施例二认证方法的基本流程图。

[0032] 图5为本发明实施例三认证方法的基本流程图。

[0033] 图6为本发明实施例四认证方法的基本流程图。

具体实施方式

[0034] 本实施例为本发明优选实施方式,其他凡其原理和基本结构与本实施例相同或近似的,均在本发明保护范围之内。

[0035] 本发明中所涉及到的混淆技术,混淆(Obfuscation)就是将一段可执行程序转换成另一段不可理解的程序的过程,转换过后的程序能保持原程序的功能性,但不泄露其秘密信息。也就是说,混淆之后的程序能被当作一个黑盒使用,不会泄露黑盒中的任何信息。具体的说,即任何能从混淆之后的程序中获得的信息,都可以通过对原程序的预言访问得到,因此混淆程序和一个真正的黑盒不可区分。目前,基于多线性映射以及全同态加密技术,已经实现了对任意多项式规模电路的不可区分混淆(Indistinguishable Obfuscation)。

[0036] 本发明中所采用的消息验证码(即MAC),是一种安全验证机制,基于安全密钥进行计算,例如MAC1＝MAC_K_(m),代表利用密钥K计算消息m的消息验证码MAC1。若需要验证MAC1的正确性,则通过K和m再次进行消息验证码的计算,得到MAC2,若MAC1与MAC2相同,则代表之前的MAC1是正确合法的。

[0037] 本发明为一种IoT场景下基于混淆的分等级分布式认证系统,该认证系统包括联网终端设备、分布式认证节点或基站以及密码混淆管理网元,联网终端设备用于通过网络与分布式认证节点或基站连接,联网终端设备内存储有MAC函数(MAC函数是一个基于设备秘钥K1的消息验证码函数计算,这种MAC函数已有非常多成熟的方案,本发明中选取常用的MAC函数即可)以及设备秘钥K1(本实施例中,设备秘钥K1根据隐藏秘钥K和设备标识采用常规的算法函数推衍得到的,本实施例中,隐藏秘钥K仅存储在密码混淆管理网元中,其他设备仅能获取对称秘钥K1,无法获取隐藏秘钥K),并可根据存储的函数计算MAC＝MAC_K1_(设备标识和(time、nonce、SQN和counter的至少一项)),并将设备标识、业务标识、MAC函数以及用于MAC计算的time、nonce、SQN和counter的至少一项发送至分布式认证节点或基站;分布式认证节点或基站用于通过网络接收联网终端设备发送的信息,分布式认证节点或基站内存储有与MAC函数对应的验证混淆函数f1(本实施例中的验证混淆函数f1的含义是指原本有一个函数f_k1_((MAC,设备标识等计算MAC需要的参数),基站标识),此函数是基于秘钥K1的消息验证码的验证函数,作用是为了验证消息验证码是否正确。现在把这个函数f_k1用混淆技术(常规的混淆技术)处理一下,就是验证混淆函数f1＝IO(f_k1),IO就代表混淆处理的过程,现在也已有成熟的技术来实现混淆处理的过程,本发明中可选用常规的混

淆技术进行处理。混淆处理之后生成的函数f1就称为验证混淆函数，验证混淆函数f1的功能和验证函数f_k1是一模一样的，也就是说验证混淆函数f1也是实现消息验证码的验证功能。但是基于混淆处理的特性，f1将f_k1中的秘密信息，也就是秘钥K隐藏起来了，现在任何一个设备，只要内置了验证混淆函数f1，就可以验证消息验证码，但是无法得知秘钥K)，分布式认证节点或基站根据接收到的设备发来的信息中的设备标识确定相应的验证混淆函数f1，输入MAC以及计算MAC用到的参数，若验证混淆函数f1输出为1，则代表验证通过；若验证混淆函数f1输出为0，则代表验证不通过；密码混淆管理网元根据隐藏的秘钥K和设备标识推衍子验证混淆函数f2计算出设备密钥K1，利用设备密钥K1计算子验证混淆函数f1＝f_K1_(MAC,设备标识等计算MAC需要的参数)，输入MAC和MAC计算所需要的参数，输出为0或者1。若利用设备密钥K1和MAC计算所需要的参数，计算出来的MAC1与验证混淆函数f1输入MAC相同，则验证混淆函数f1输出为1，否则，输出为0代表函数内计算的MAC1与MAC不同。当且仅当生成验证混淆函数f1是用的设备密钥K1，与计算MAC用的密钥相同时，f1才验证通过，并输出1。此处验证混淆函数f1为验证MAC是否正确的黑盒子，而函数中密钥K是隐藏起来的，因此函数可以分布式部署，而分布式节点不能获得密钥K。

[0038] 计算基于K的MAC验证混淆函数f1，实现功能为验证MAC计算是否正确，同时发送设备标识和验证混淆函数f1至分布式认证节点或基站。本实施例中，联网终端设备为IoT设备或UE。

[0039] 上述IoT场景下基于混淆的分等级分布式认证系统中的密码混淆管理网元包括混淆控制单元、混淆存储单元和混淆网络传输单元，混淆存储单元用于存储对称秘钥，并能将对称秘钥传输给混淆控制单元，所述的混淆控制单元用于根据对称密钥计算消息验证码验证混淆函数f1，实现功能为验证消息验证码计算是否正确，所述的混淆网络传输单元与混淆控制单元连接，混淆网络传输单元用于将设备标识和验证混淆函数f1发送至分布式认证节点或基站。

[0040] 上述IoT场景下基于混淆的分等级分布式认证系统中的终端设备包括终端网络传输单元、终端存储单元和终端控制单元，所述的终端存储单元用于存储消息验证码函数和对称秘钥，终端存储单元与终端控制单元连接，所述的终端控制单元用于根据消息验证码函数、所述对称密钥、终端设备标识、业务标识、以及新鲜参数计算消息验证码，所述的终端网络传输单元与终端控制单元连接，终端网络传输单元用于将设备标识、业务标识、消息验证码以及用于消息验证码计算的新鲜参数发送至分布式认证节点或所述基站。

[0041] 上述IoT场景下基于混淆的分等级分布式认证系统中的分布式认证节点包括节点网络传输单元和节点混淆验证单元，节点网络传输单元与节点混淆验证单元连接，所述的节点网络传输单元用于接收终端设备发送的信息，所述的节点混淆验证单元用于根据设备标识确定验证混淆函数f1，输入消息验证码以及计算消息验证码用到的参数，通过验证混淆函数f1对消息验证码进行验证。

[0042] 本发明同时保护一种IoT场景下基于混淆的分等级分布式认证装置，认证装置包括密码混淆管理网元、终端设备和分布式认证节点或基站，所述的密码混淆管理网元包括混淆控制单元、混淆存储单元和混淆网络传输单元，混淆存储单元用于存储对称秘钥，并能将对称秘钥传输给混淆控制单元，所述的混淆控制单元用于根据对称密钥计算消息验证码验证混淆函数f1，实现功能为验证消息验证码计算是否正确，所述的混淆网络传输单元与

混淆控制单元连接，混淆网络传输单元用于将设备标识和验证混淆函数f1发送至分布式认证节点或基站；所述的终端设备包括终端网络传输单元、终端存储单元和终端控制单元，所述的终端存储单元用于存储消息验证码函数和对称秘钥，终端存储单元与终端控制单元连接，所述的终端控制单元用于根据消息验证码函数、所述对称密钥、终端设备标识、业务标识、以及新鲜参数计算消息验证码，所述的终端网络传输单元与终端控制单元连接，终端网络传输单元用于将设备标识、业务标识、消息验证码以及用于消息验证码计算的新鲜参数发送至分布式认证节点或所述基站；分布式认证节点或基站包括节点网络传输单元和节点混淆验证单元，节点网络传输单元与节点混淆验证单元连接，所述的节点网络传输单元用于接收终端设备发送的信息，所述的节点混淆验证单元用于根据设备标识确定验证混淆函数f1，输入消息验证码以及计算消息验证码用到的参数，通过验证混淆函数f1对消息验证码进行验证。

[0043] 本发明为一种IoT场景下基于混淆的分等级分布式认证方法，其包括下述步骤：

[0044] 步骤1：联网终端设备计算MAC＝MAC_K1_(设备标识、业务标识、m和(time、nonce、SQN和counter的至少一项))，本实施例中，业务标识可以选择包含，也可以选择不包含在内。消息m代表联网终端设备希望发送的消息，若仅认证的话，联网终端设备也可以不发消息m。联网终端设备发送设备标识、业务标识、MAC以及用于MAC计算的time(时间值)、nonce(随机数)、SQN(序列号)和counter(计数值)的至少一项至分布式认证节点或基站。若MAC计算未使用业务标识，则设备也可以不发送业务标识。另外，若SQN或counter为设备与分布式节点或基站同时保存的计数器，也可以不发。

[0045] 步骤2：分布式认证节点或基站基于设备标识确定验证混淆函数f1，并在验证混淆函数f1中输入MAC以及计算MAC用到的参数，若验证混淆函数f1的输出为1，则代表验证通过。若验证混淆函数f1的输出为0，则代表验证不通过。本实施例中，若采用基站时，MAC的验证混淆函数f1绑定基站的标识，使得此验证混淆函数仅用于此基站，则f1＝IO(f_k_((MAC，设备标识等计算MAC需要的参数)，基站标识))，本实施例中，IO为Indistinguishable Obfuscation的简称，即不可区分混淆。输入MAC和MAC计算所需要的参数，输出为0或者1。此时联网终端设备计算MAC也需要用到基站标识，联网终端设备获得基站标识的方式可以为基站广播自己的标识信息，当联网终端设备接入基站时获得。也可能预置在联网终端设备内，此时被预置了基站标识的联网终端设备仅适用此基站标识对应的基站覆盖范围内。

[0046] 步骤3：本实施例中，还可包括步骤3，即分布式认证节点发送认证结果至设备。

[0047] 下面将以IoT设备作为联网终端设备为例结合几个具体实例对本发明进行具体说明，具体实施时，该方法也可以用于其他联网设备终端。

[0048] 实施例一：

[0049] 请参看附图3，本实施例的认证方法包括下述步骤：

[0050] 步骤1：IoT设备计算MAC＝MAC_K1_(包括设备标识、业务标识、消息m、(time、nonce、SQN或counter的至少一项))，本实施例中，业务标识为可选项，消息m代表IoT device希望发送的消息，若仅认证的话，IoT device也可以不发消息m。

[0051] 设备发送设备标识、业务标识、MAC以及用于MAC计算的(time、nonce、SQN和counter的至少一项)至分布式认证节点，若MAC计算未使用业务标识，则设备也可以不发送业务标识，另外，若SQN或counter为设备与分布式节点同时保存的计数器，也可以不发。

[0052] 步骤2:分布式认证节点基于设备标识,确定验证混淆函数f1,并输入MAC以及计算MAC用到的参数,若验证混淆函数f1输出为1,则代表验证通过;若验证混淆函数f1输出为0,则代表验证不通过。

[0053] 步骤3:分布式认证节点发送认证结果至设备。

[0054] 本实施例的使用前提是,IoT device内保存设备标识和K,也可能存储有业务标识。

[0055] 步骤0:密码混淆管理网元,根据隐藏的秘钥K和设备标识推衍子验证混淆函数f2计算出设备密钥K1,利用设备密钥K1计算子验证混淆函数f1=f_K1_(MAC,设备标识等计算MAC需要的参数),输入MAC和MAC计算所需要的参数,验证MAC计算是否正确,同时发送设备标识和验证混淆函数f1至分布式认证节点。

[0056] 本实施例中的步骤3为可选步骤。

[0057] 实施例二:

[0058] 请参看附图4,本实施例的基本步骤与实施例一相同,不同之处在于本实施例的认证方法的基站中并没有预置针对K1的验证混淆函数,需通过发送请求至密码混淆管理网元,才可获得相应的验证混淆函数。

[0059] 本实施例的认证方法包括下述步骤:

[0060] 步骤1:IoT设备计算MAC=MAC_K1_(包括设备标识、业务标识、消息m、(time、nonce、SQN或counter的至少一项)),本实施例中,业务标识可选,消息m代表IoT device希望发送的消息,若仅认证的话,IoT device也可以不发消息m。

[0061] 设备发送设备标识、业务标识、MAC以及用于MAC计算的(time、nonce、SQN和counter的至少一项)至分布式认证节点,若MAC计算未使用业务标识,则设备也可以不发送业务标识,另外,若SQN或counter为设备与分布式节点同时保存的计数器,也可以不发。

[0062] 步骤2:分布式认证节点在接收到IoT设备发送的请求后,发送设备标识至密码混淆管理网元。

[0063] 步骤3:密码混淆管理网元首先根据设备标识确定K1,之后基于K1计算MAC验证混淆函数f1,并分发此验证混淆函数f1至分布式认证节点。

[0064] 步骤4:分布式认证节点基于设备标识,确定验证混淆函数f1,并输入MAC以及计算MAC用到的参数,若验证混淆函数f1的输出为1,则代表验证通过;若验证混淆函数f1输出为0,则代表验证不通过。

[0065] 步骤5:分布式认证节点发送认证结果至设备。

[0066] 实施例三:

[0067] 请参看附图5,本实施例为双向认证的模式,本实施例的基本步骤与实施例一相同,不同之处在于本实施例的认证方法密码混淆管理网元在第0步分配了基于对称秘钥K1的MAC计算混淆函数,使得分布式认证节点也具有了MAC计算能力。

[0068] 本实施例的认证方法包括下述步骤:

[0069] 步骤0:计算基于对称秘钥K1的MAC验证混淆函数与实施例一相同,密码混淆管理网元额外计算基于对称秘钥K1的MAC计算混淆函数(该函数也采用常规的计算混淆函数)g=IO(g_K1_(MAC计算所需要的参数))。所述计算混淆函数g的输入为MAC计算所需要的参数,输出为MAC2;

[0070] 步骤1:IoT设备计算MAC＝MAC_K1_(包括设备标识、业务标识、消息m、(time、nonce、SQN或counter的至少一项))，本实施例中，业务标识可选，消息m代表IoT device希望发送的消息，若仅认证的话，IoT device也可以不发消息m。

[0071] 设备发送设备标识、业务标识、MAC以及用于MAC计算的(time、nonce、SQN和counter的至少一项)至分布式认证节点，若MAC计算未使用业务标识，则设备也可以不发送业务标识，另外，若SQN或counter为设备与分布式节点同时保存的计数器，也可以不发。

[0072] 步骤2:分布式认证节点基于设备标识，确定验证混淆函数f1，并输入MAC以及计算MAC用到的参数，若验证混淆函数f1的输出为1，则代表验证通过;若验证混淆函数f1输出为0，则代表验证不通过;基于函数g计算得到MAC2，MAC2计算所用到的参数包括:分布式认证节点标识、设备标识、业务标识以及新鲜参数(如随机选择的随机数，或者nonce，或者SQN)，其中业务标识为可选，分布式认证节点标识为可选。

[0073] 步骤3:分布式认证节点发送MAC2，以及计MAC用到的非共享参数(即分布式认证节点的特有参数，如:新鲜参数)等至IoT device;

[0074] 步骤4:IoT Device基于对称秘钥K1、新鲜参数以及设备标识，还可能包括业务标识或者分布式认证节点标识计算MAC2'，若MAC2'与MAC2相同，则验证分布式认证节点通过。

[0075] 本实施例中，分布式认证节点还可采用如实施例二的方式通过请求获得f1和g。

[0076] 实施例四:

[0077] 请参看附图6，本实施例为基于5G场景的应用模式，分布式认证节点可以5G基站，本实施例的基本步骤与实施例一相同，不同之处在于本实施例的MAC验证混淆函数绑定基站的标识，使得此验证混淆函数f1仅用于此基站，即验证混淆函数f1＝IO(f_k1_((MAC，设备标识等计算MAC需要的参数)和基站标识))。输入MAC和MAC计算所需要的参数，输出为0或者1。

[0078] 此时UE计算MAC也需要用到基站标识。UE获得基站标识的方式可以为基站广播自己的标识信息，当UE接入基站时获得。也可能预置在UE内，此时被预置了基站标识的UE仅适用此基站标识对应的基站覆盖范围内。

[0079] 针对上述所有实施例还可能包括，计算MAC还可以用到网络标识;这里网络标识包括但不限于运营商标识、骨干网网络标识(如电信网络标识)等。例如UE内计算MAC以及验证混淆函数f1和g黑盒子中的计算。

[0080] 本发明与传统方法不同，基于混淆的分布式对称认证方法，分布式认证节点仅需部署混淆后的MAC验证程序;而设备则跟普通机制相同，仅需要存储一个即可。本发明方案满足分布式节点在没有K1的情况下也可以验证设备的接入认证。

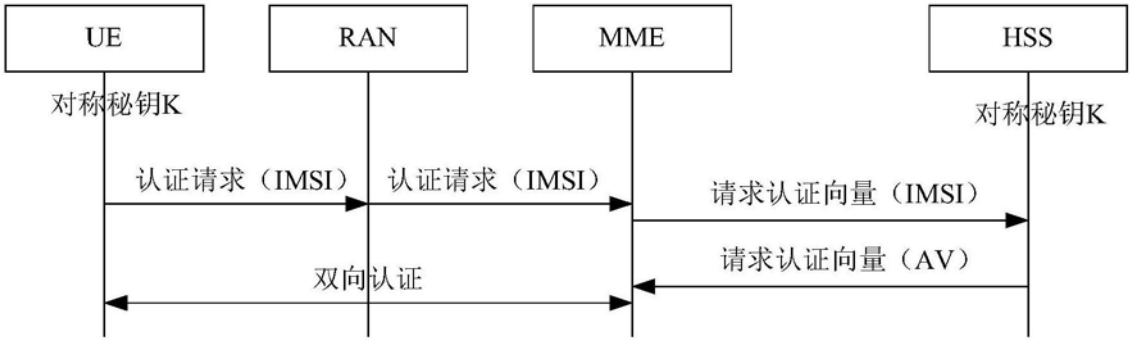

UE
RAN
MME
HSS
对称秘钥K
对称秘钥K
认证请求（IMSI）
认证请求（IMSI）
请求认证向量（IMSI）
请求认证向量（AV）
双向认证

图1

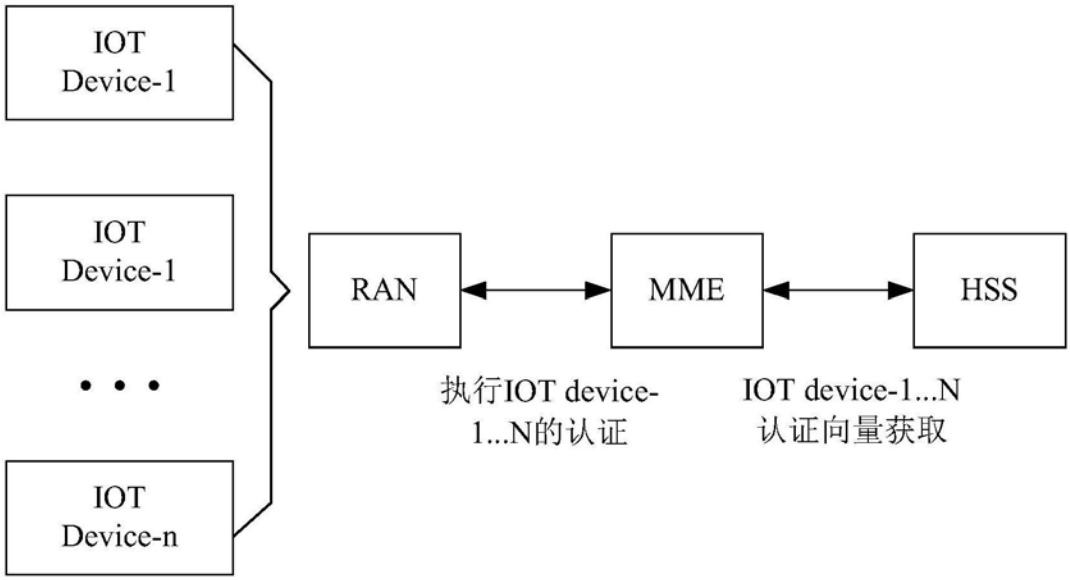

IOT
Device-1
IOT
Device-1
• • •
IOT
Device-n
RAN
MME
HSS
执行IOT device-
1...N的认证
IOT device-1...N
认证向量获取

图2

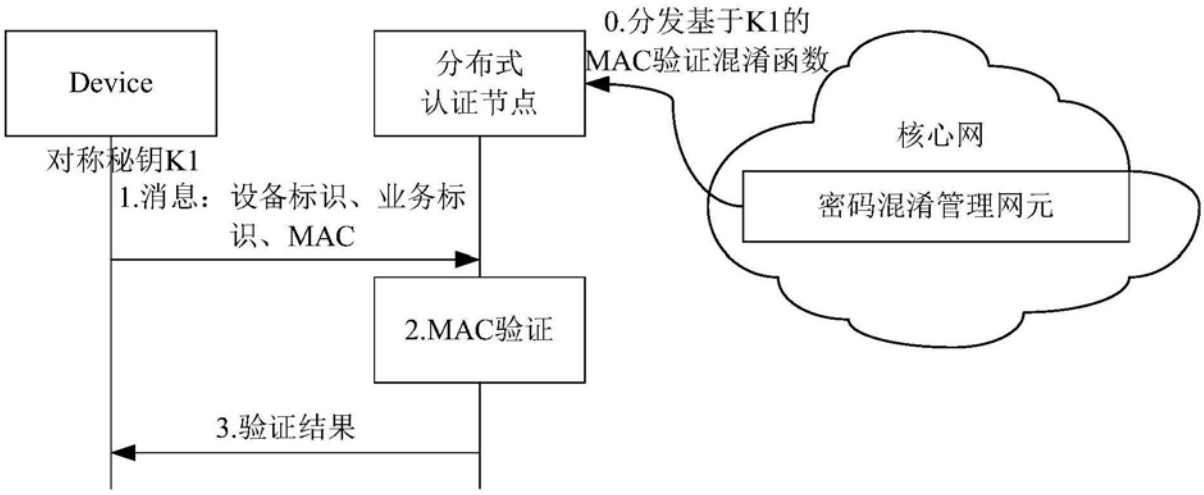

Device
对称秘钥K1
分布式
认证节点
0.分发基于K1的
MAC验证混淆函数
核心网
密码混淆管理网元
1.消息：设备标识、业务标
识、MAC
2.MAC验证
3.验证结果

图3

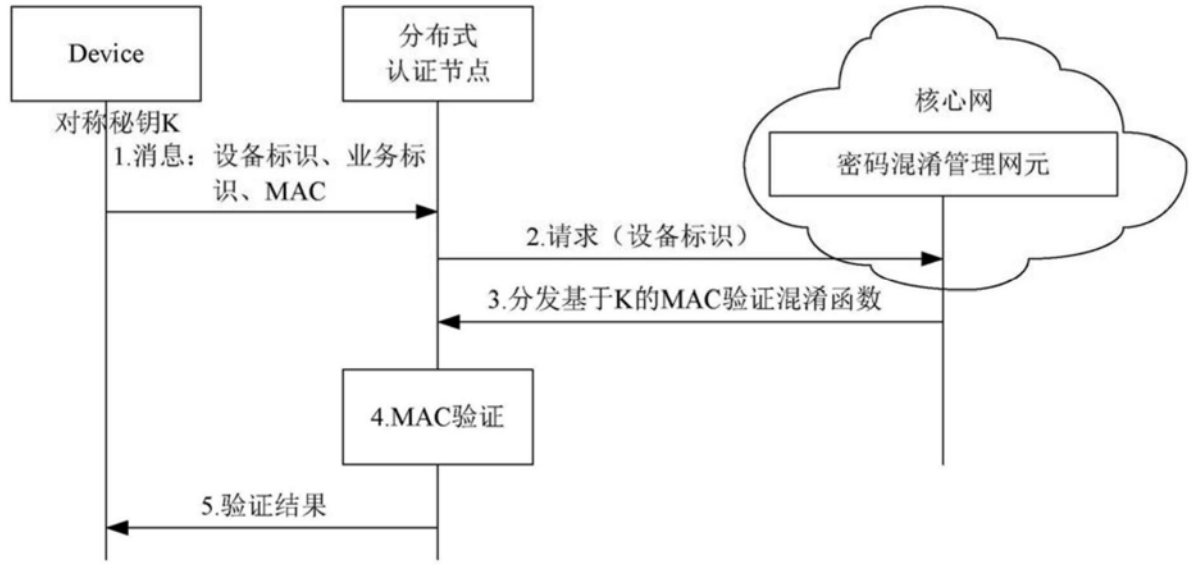

Device
分布式
认证节点
核心网
密码混淆管理网元
对称秘钥K
1.消息：设备标识、业务标识、MAC
2.请求（设备标识）
3.分发基于K的MAC验证混淆函数
4.MAC验证
5.验证结果

图4

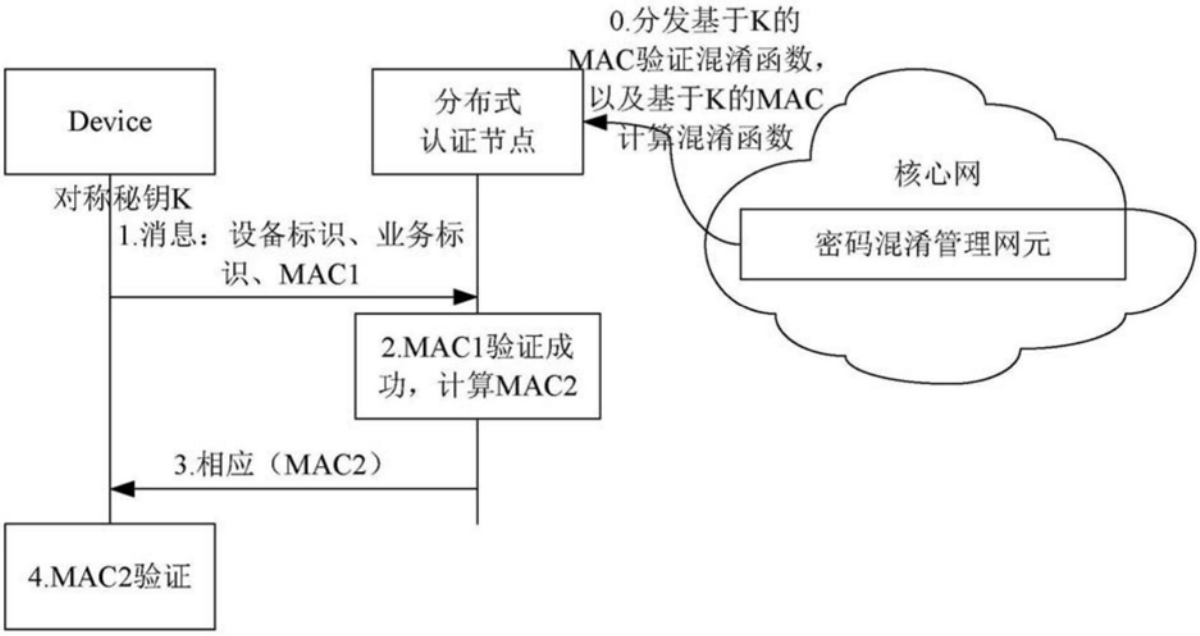

0.分发基于K的MAC验证混淆函数，以及基于K的MAC计算混淆函数
Device
分布式
认证节点
核心网
密码混淆管理网元
对称秘钥K
1.消息：设备标识、业务标识、MAC1
2.MAC1验证成功，计算MAC2
3.相应（MAC2）
4.MAC2验证

图5

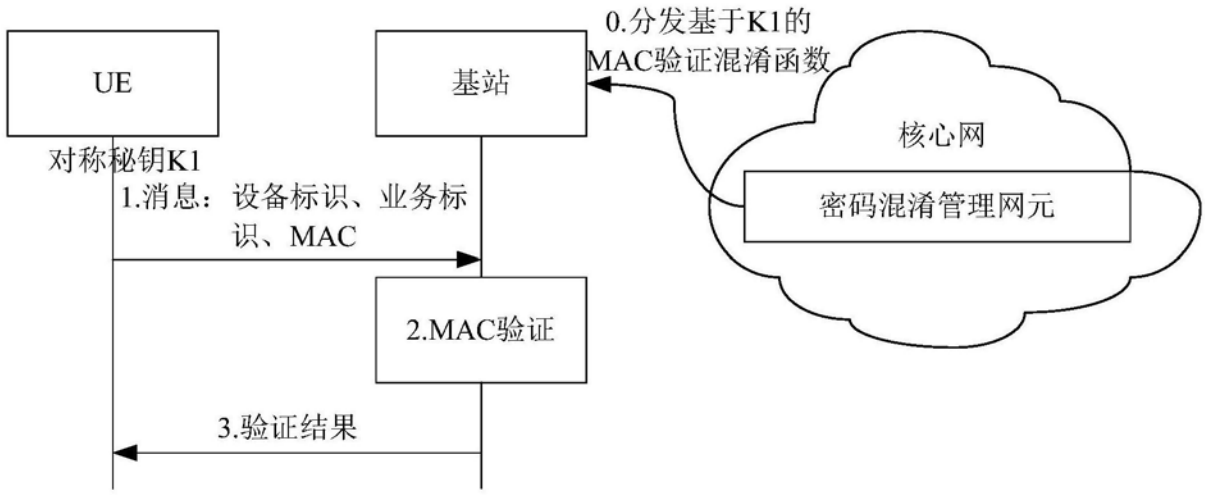

UE
基站
0.分发基于K1的
MAC验证混淆函数
核心网
密码混淆管理网元
对称秘钥K1
1.消息：设备标识、业务标识、MAC
2.MAC验证
3.验证结果

图6