(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 113242548 B
(45)授权公告日 2021.09.17

(21)申请号 202110777176.8
(22)申请日 2021.07.09
(65)同一申请的已公布的文献号
申请公布号 CN 113242548 A
(43)申请公布日 2021.08.10
(73)专利权人 四川大学
地址 610000 四川省成都市一环路南一段24号
(72)发明人 陈文 周兰 康明
(74)专利代理机构 四川省成都市天策商标专利事务所 51213
代理人 张秀敏
(51)Int.Cl.
H04W 12/0431(2021.01)
H04W 12/0471(2021.01)
H04W 12/06(2021.01)
G16Y 30/10(2020.01)
(56)对比文件
CN 112911588 A,2021.06.04
CN 113037467 A,2021.06.25
审查员 张长梅

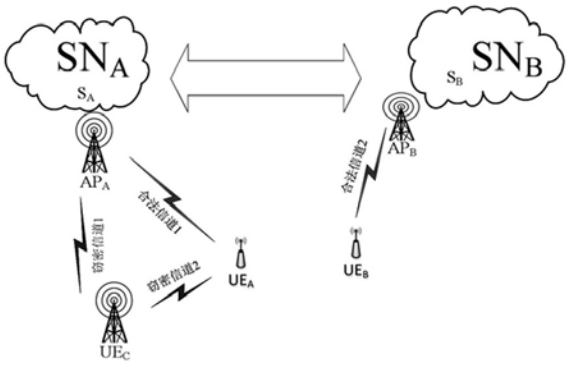
权利要求书2页 说明书5页 附图1页

(54)发明名称

5G网络环境下的无线物联网设备通信密钥交换方法

(57)摘要

本发明公开了一种5G网络环境下的无线物联网设备通信密钥交换方法，包括IoT网络中准备建立保密通信的终端设备UE_A和终端设备UE_B，以及位于5G服务网络中的签名验证模块S_A和签名验证模块S_B，终端设备UE_A和终端设备UE_B分别通过无线接入点AP_A和无线接入点AP_B接入各自对应的服务网络中；通信密钥交换方法包括：终端设备UE_A和终端设备UE_B协商通信密钥；根据终端设备UE_A或UE_B与各自对应的无线接入点AP_A或AP_B之间的无线信道物理特征进行身份签名验证，双方通过各自所属5G服务网络中的签名验证模块S_A和签名验证模块S_B向无线接入点AP_A和无线接入点AP_B验证签名的有效性；本发明实现了对中间人攻击的防御以及避免对第三方CA/PKI的依赖。



CN 113242548 B

1.一种5G网络环境下的无线物联网设备通信密钥交换方法,其特征在于,包括IoT网络中准备建立保密通信的终端设备UE_A和终端设备UE_B,以及位于5G服务网络中的签名验证模块S_A和签名验证模块S_B,所述终端设备UE_A和终端设备UE_B分别通过无线接入点AP_A和无线接入点AP_B接入各自对应的服务网络中;所述的通信密钥交换方法包括以下步骤:

步骤1、终端设备UE_A和终端设备UE_B协商通信密钥;

所述步骤1具体包括以下步骤:

(1)其中一个终端设备选取一个生成元g和一个大素数p,发送(g,p)给另外一个终端设备;

(2)终端设备UE_A和终端设备UE_B分别选取介于2到p-2之间的一个随机数x和y,即$2\leqslant x\leqslant p-2$,$2\leqslant y\leqslant p-2$,计算中间值$X=g^x \bmod p$和$Y=g^y \bmod p$;

(3)终端设备UE_A以过去T秒内采集到的终端设备UE_A与无线接入点AP_A之间的无线信道物理特征V_A作为签名密钥对中间值$X=g^x \bmod p$进行签名,生成终端设备UE_A的身份签名$MAC_X=f(X||V_A)$,终端设备UE_B以过去T秒内采集到的终端设备UE_B与无线接入点AP_B之间的无线信道物理特征V_B作为签名密钥对中间值$Y=g^y \bmod p$进行签名,生成终端设备UE_B的身份签名$MAC_Y=f(Y||V_B)$,其中f()为哈希散列函数,||为连接操作;

(4)终端设备UE_A将协商向量(X,MAC_X,$TMSI_A$,SN_AID)传给终端设备UE_B,终端设备UE_B将协商向量{Y,MAC_Y,$TMSI_B$,SN_BID}传给终端设备UE_A,$TMSI_A$和$TMSI_B$分别为终端设备UE_A和终端设备UE_B在其对应的服务网络SN_A和服务网络SN_B中注册的临时身份标识,SN_AID和SN_BID分别为终端设备UE_A和终端设备UE_B所在的服务网络ID;

步骤2、根据终端设备UE_A或UE_B与各自对应的无线接入点AP_A或AP_B之间的无线信道物理特征进行身份签名验证,双方通过各自所属5G服务网络中的签名验证模块S_A和签名验证模块S_B向无线接入点AP_A和无线接入点AP_B验证签名的有效性;

在步骤2中,终端设备UE_A的身份签名验证具体包括以下步骤:

(a)终端设备UE_A将收到的协商向量{Y,MAC_Y,$TMSI_B$,SN_BID}传给签名验证模块S_A,由签名验证模块S_A根据SN_BID将验证请求{Y,$TMSI_B$,SN_BID}转发给服务网络SN_B的签名验证模块S_B;

(b)签名验证模块S_B检查SN_BID是否是本服务网络的ID,若不是,则设置返回值Res_B='$error_1$',转步骤(e),否则将{Y,$TMSI_B$}转发给无线接入点AP_B,请求计算$TMSI_B$对应终端设备的哈希签名;

(c)无线接入点AP_B接收到{Y,$TMSI_B$}检查$TMSI_B$是否为本接入点注册的本地设备,若不是设置返回值Res_B='$error_2$',转步骤(d);否则以过去T秒内采集到的终端设备UE_B与无线接入点AP_B之间的无线信道物理特征V_B作为签名密钥对Y进行签名,生成终端设备UE_B的身份验证签名$MAC_Y'=f(Y||V_B)$,其中f()为哈希散列函数,||为连接操作,无线接入点AP_B设置返回值为Res_B='MAC_Y'';

(d)无线接入点AP_B将Res_B返回给签名验证模块S_B;

(e)签名验证模块S_B将Res_B转发给签名验证模块S_A;

(f)若Res_B为'$error_1$'或'$error_2$',则签名验证模块S_A直接返回Res_B给终端设备UE_A,否则签名验证模块S_A比较终端设备UE_B的身份签名MAC_Y与Res_B中包含的终端设备UE_B的身份验证签名MAC_Y':若$MAC_Y=MAC_Y'$,设置Res_B='OK',否则设置Res_B='FAILED',随后返回Res_B给终端设备UE_A;

(g)终端设备UE_A检查Res_B的返回结果,若Res_B为'OK',则计算$Y^x \bmod p$,即$(g^y)^x \bmod p$得到会话密钥$K_1=g^{xy} \bmod p$,否则重新发起与终端设备UE_B的密钥协商过程;

终端设备UE_B的身份签名验证具体包括以下步骤:

(A)终端设备UE_B将收到的协商向量{X,MAC_X,$TMSI_A$,SN_AID}传给签名验证模块S_B,由签名验证模块S_B根据SN_AID将验证请求{X,$TMSI_A$,SN_AID}转发给服务网络SN_A的签名验证模块S_A;

(B)签名验证模块S_A检查SN_AID是否是本服务网络的ID,若不是,则设置返回值Res_A='$error_1$',转步骤(E),否则将{X,$TMSI_A$}转发给无线接入点AP_A,请求计算$TMSI_A$对应终端设备的哈希签名;

(C)无线接入点AP_A接收到{X,$TMSI_A$}检查$TMSI_A$是否为本接入点注册的本地设备,若不是设置返回值Res_A='$error_2$',转步骤(D);否则以过去T秒内采集到的终端设备UE_A与无线接入点AP_A之间的无线信道物理特征V_A作为签名密钥对X进行签名,生成终端设备UE_A的身份验证签名MAC_X'=f(X||V_A),其中f()为哈希散列函数,||为连接操作,无线接入点AP_A设置返回值为Res_A='MAC_X'';

(D)无线接入点AP_A将Res_A返回给签名验证模块S_A;

(E)签名验证模块S_A将Res_A转发给签名验证模块S_B;

(F)若Res_A为'$error_1$'或'$error_2$',则签名验证模块S_B直接返回Res_A给终端设备UE_B,否则签名验证模块S_B比较终端设备UE_A的身份签名MAC_X与Res_A中包含的终端设备UE_A的身份验证签名MAC_X':若MAC_X=MAC_X',设置Res_A='OK',否则设置Res_A='FAILED',随后返回Res_A给终端设备UE_B;

(G)终端设备UE_B检查Res_A的返回结果,若Res_A为'OK',则计算$X^y \bmod p$,即$(g^x)^y \bmod p$得到会话密钥$K_2=g^{xy} \bmod p$,否则重新发起与终端设备UE_B的密钥协商过程;

若会话密钥$K_1=K_2=g^{xy} \bmod p$,则终端设备UE_A和终端设备UE_B的完成身份签名验证和密钥协商过程。

5G网络环境下的无线物联网设备通信密钥交换方法

技术领域

[0001] 本发明涉及网络安全技术领域,特别是一种5G网络环境下的无线物联网设备通信密钥交换方法。

背景技术

[0002] 5G的出现为智慧城市、智慧医疗以及智能电网的发展提供了更加完善的解决方案。在5G网络环境下,物联网技术IoT得到了极大的促进,网络实现了人与物之间,以及物与物之间的通信。因此在5G网络内当成千上万的IoT设备无线接入网络进行通信时,为确保通信数据的机密性和完整性,设计高效且安全的无线网络通信密钥交换方法,以支持在任意一对IoT节点之间建立可靠的无线加密传输通道十分重要。

[0003] 传统的密钥交换方法存在以下问题:

[0004] 问题(1):对第三方权威密钥分发系统CA/PKI的依赖:

[0005] 传统的RSA密钥协商算法采用数字信封原理,通信发起方Alice利用接收方Bob的公钥PKBob和RSA算法对通信密钥Key进行加密Enc=RSA(Key, PkBob)并发给Bob,Bob用私钥解开Enc,获取到通信密钥Key。为了避免中间人攻击,上述过程中Alice需要向可信的第三方CA/PKI查询Bob的公钥。然而,在实际应用中,由于物联网设备规模巨大,且设备资源有限,很多入网的IoT设备并没有在CA/PKI中注册公钥,且对CA/PKI的海量公钥查询可能导致网络性能瓶颈。

[0006] 问题(2):不依赖CA/PKI,但易被中间人攻击:

[0007] 另一类广泛使用的密钥交换算法DHKE(Differ-Hellman Key Exchange), 不提供直接的加密或者解密,而是利用"离散对数问题"的复杂性进行密钥的协商。DHKE避免了对CA/PKI的依赖,然而密钥交换协议不验证公钥发送者的身份,无法阻止中间人攻击。为了实现DHKE对中间人攻击的防御,现有改进方法提出利用通信双方的私钥对密钥协商过程进行签名,然而该过程又引入了利用第三方CA/PKI进行可信的公钥分发过程,回到了问题(1),重新依赖于CA/PKI。

发明内容

[0008] 为解决现有技术中存在的问题,本发明针对1)传统的无线物联网节点进行密钥交换易受中间人攻击;2)对抗中间人攻击需要依赖CA/PKI传递私钥;3)大量物联网设备未在CA/PKI注册私钥的问题提供一种5G网络环境下的无线物联网设备通信密钥交换方法,本发明在5G无线物联网环境下进行密钥交换时,基于无线信道的独立性,IoT设备与5G服务网络接入点之间的无线物理信道特征只为IoT终端与接入点所感知这一特点,提出基于IoT设备与接入点之间的物理信道特征对通信双方协商的通信密钥进行签名认证,以实现对中间人攻击的防御,以及避免对第三方CA/PKI的依赖。

[0009] 为实现上述目的,本发明采用的技术方案是:一种5G网络环境下的无线物联网设备通信密钥交换方法,包括IoT网络中准备建立保密通信的终端设备UE_A和终端设备UE_B,以

及位于5G服务网络中的签名验证模块S_A和签名验证模块S_B,所述终端设备UE_A和终端设备UE_B分别通过无线接入点AP_A和无线接入点AP_B接入各自对应的服务网络中;所述的通信密钥交换方法包括以下步骤:

[0010] 步骤1、终端设备UE_A和终端设备UE_B协商通信密钥;

[0011] 步骤2、根据终端设备UE_A或UE_B与各自对应的无线接入点AP_A或AP_B之间的无线信道物理特征进行身份签名验证,双方通过各自所属5G服务网络中的签名验证模块S_A和签名验证模块S_B向无线接入点AP_A和无线接入点AP_B验证签名的有效性。

[0012] 作为本发明的进一步改进,所述步骤1具体包括以下步骤:

[0013] (1)其中一个终端设备选取一个生成元g和一个大素数p,发送(g,p)给另外一个终端设备;

[0014] (2)终端设备UE_A和终端设备UE_B分别选取介于2到p-2之间的一个随机数x和y,即2≤x≤p-2,2≤y≤p-2,计算中间值$X=g^x \bmod p$和$Y=g^y \bmod p$;

[0015] (3)终端设备UE_A以过去T秒内采集到的终端设备UE_A与无线接入点AP_A之间的无线信道物理特征V_A作为签名密钥对中间值$X=g^x \bmod p$进行签名,生成终端设备UE_A的身份签名$MAC_X=f(X||V_A)$,终端设备UE_B以过去T秒内采集到的终端设备UE_B与无线接入点AP_B之间的无线信道物理特征V_B作为签名密钥对中间值$Y=g^y \bmod p$进行签名,生成终端设备UE_B的身份签名$MAC_Y=f(Y||V_B)$,其中f()为哈希散列函数,||为连接操作;

[0016] (4)终端设备UE_A将协商向量$(X,MAC_X,TMSI_A,SN_AID)$传给终端设备UE_B,终端设备UE_B将协商向量$\{Y,MAC_Y,TMSI_B,SN_BID\}$传给终端设备$UE_A$,$TMSI_A$和$TMSI_B$分别为终端设备$UE_A$和终端设备$UE_B$在其对应的服务网络$SN_A$和服务网络$SN_B$中注册的临时身份标识,$SN_AID$和$SN_BID$分别为终端设备$UE_A$和终端设备$UE_B$所在的服务网络ID。

[0017] 作为本发明的进一步改进,在步骤2中,终端设备UE_A的身份签名验证具体包括以下步骤:

[0018] (a)终端设备UE_A将收到的协商向量$\{Y,MAC_Y,TMSI_B,SN_BID\}$传给签名验证模块$S_A$,由签名验证模块$S_A$根据$SN_BID$将验证请求$\{Y,TMSI_B,SN_BID\}$转发给服务网络$SN_B$的签名验证模块$S_B$;

[0019] (b)签名验证模块S_B检查SN_BID是否是本服务网络的ID,若不是,则设置返回值$Res_B=‘error_1’$,转步骤(e),否则将$\{Y,TMSI_B\}$转发给无线接入点AP_B,请求计算$TMSI_B$对应终端设备的哈希签名;

[0020] (c)无线接入点AP_B接收到$\{Y,TMSI_B\}$检查$TMSI_B$是否为本接入点注册的本地设备,若不是设置返回值$Res_B=‘error_2’$,转步骤(d);否则以过去T秒内采集到的终端设备UE_B与无线接入点AP_B之间的无线信道物理特征V_B作为签名密钥对Y进行签名,生成终端设备UE_B的身份验证签名$MAC_Y'=f(Y||V_B)$,其中f()为哈希散列函数,||为连接操作,无线接入点AP_B设置返回值为$Res_B=‘MAC_Y’’$;

[0021] (d)无线接入点AP_B将Res_B返回给签名验证模块S_B。

[0022] (e)签名验证模块S_B将Res_B转发给签名验证模块S_A。

[0023] (f)若Res_B为$‘error_1’$或$‘error_2’$,则签名验证模块S_A直接返回Res_B给终端设备UE_A,否则签名验证模块S_A比较终端设备UE_B的身份签名MAC_Y与Res_B中包含的终端设备UE_B的身验证份签名MAC_Y':若$MAC_Y=MAC_Y'$,设置$Res_B=‘OK’$,否则设置$Res_B=‘FAILED’$,随后返回Res_B

给终端设备UE_A。

[0024] (g)终端设备UE_A检查Res_B的返回结果，若Res_B为‘OK’，则计算$Y^x \bmod p$，即$(g^y)^x \bmod p$得到会话密钥$K_1=g^{xy} \bmod p$，否则重新发起与终端设备UE_B的密钥协商过程；

[0025] 终端设备UE_B的身份签名验证具体包括以下步骤：

[0026] (A)终端设备UE_B将收到的协商向量{X,MAC_X,$TMSI_A$,SN_AID}传给签名验证模块S_B，由签名验证模块S_B根据SN_AID将验证请求{X,$TMSI_A$,SN_AID}转发给服务网络SN_A的签名验证模块S_A；

[0027] (B)签名验证模块S_A检查SN_AID是否是本服务网络的ID，若不是，则设置返回值Res_A=‘$error_1$’，转步骤(E)，否则将{X,$TMSI_A$}转发给无线接入点AP_A，请求计算$TMSI_A$对应终端设备的哈希签名；

[0028] (C)无线接入点AP_A接收到{X,$TMSI_A$}检查$TMSI_A$是否为本接入点注册的本地设备，若不是设置返回值Res_A=‘$error_2$’，转步骤(D)；否则以过去T秒内采集到的终端设备UE_A与无线接入点AP_A之间的无线信道物理特征V_A作为签名密钥对X进行签名，生成终端设备UE_A的身验证份签名MAC_X’=f(X||V_A)，其中f()为哈希散列函数，||为连接操作，无线接入点AP_A设置返回值为Res_A=‘MAC_X’’；

[0029] (D)无线接入点AP_A将Res_A返回给签名验证模块S_A。

[0030] (E)签名验证模块S_A将Res_A转发给签名验证模块S_B。

[0031] (F)若Res_A为‘$error_1$’或‘$error_2$’，则签名验证模块S_B直接返回Res_A给终端设备UE_B，否则签名验证模块S_B比较终端设备UE_A的身份签名MAC_X与Res_A中包含的终端设备UE_A的身份验证签名MAC_X’：若MAC_X=MAC_X’，设置Res_A=‘OK’，否则设置Res_A=‘FAILED’，随后返回Res_A给终端设备UE_B。

[0032] (G)终端设备UE_B检查Res_A的返回结果，若Res_A为‘OK’，则计算$X^y \bmod p$，即$(g^x)^y \bmod p$得到会话密钥$K_2=g^{xy} \bmod p$，否则重新发起与终端设备UE_B的密钥协商过程；

[0033] 若会话密钥$K_1=K_2=g^{xy} \bmod p$，则终端设备UE_A和终端设备UE_B的完成身份签名验证和密钥协商过程。

[0034] 本发明的有益效果是：

[0035] 本发明在密钥交换过程中利用了无线信道的独立性：根据IoT设备与5G无线网络接入点之间的无线物理信道特征只为IoT终端与接入点所感知用这一特点，提出基于IoT设备与服务网络接入点之间的物理信道特征对密钥交换算法DHKE进行签名认证，以实现对中间人攻击的防御以及避免对第三方CA/PKI的依赖。解决了5G网络环境下物联网设备数量众多，且大多没有在CA/PKI中进行密钥注册认证，难以依靠CA/PKI进行安全的密钥分发，而脱离CA/PKI的传统DHKE密钥分发方法又面临中间人攻击的问题。

附图说明

[0036] 图1为本发明实施例中的系统组成结构示意图；

[0037] 图2为本发明实施例中密钥协商与签名认证的流程图。

具体实施方式

[0038] 下面结合附图对本发明的实施例进行详细说明。

实施例

[0039] 如图1所示，一种5G网络环境下的无线物联网设备通信密钥交换方法，包含IoT网络中准备建立保密通信的两个终端设备UE_A和终端设备UE_B，终端设备UE_A和终端设备UE_B所属的服务网络(Serving Network,SN)分别为:SN_A,SN_B，服务网络无线接入点AP_A和无线接入点AP_B，位于5G软件定义网络SDN的签名验证模块S_A,S_B。

[0040] 两个终端设备UE_A和UE_B已经分别根据5G网络身份认证协议EAP-AKA'或5G-AKA进行服务网络入网身份认证，通过无线接入点AP_A和AP_B接入5G网络，并记录下了各自的服务网络ID:SN_AID,SN_BID。

[0041] 1、终端设备UE_A和UE_B正式通信前，首先执行通信密钥协商步骤，协商基本流程如图2所示。

[0042] 1)UE_A选取一个生成元g和一个大素数p，发送(g,p)给UE_B；

[0043] 2)随后UE_A选取介于2到p-2之间的一个随机数x，$2 \leqslant x \leqslant p-2$，计算中间值$X=g^x \bmod p$；

[0044] 3)UE_A以过去T秒内采集到的UE_A与无线接入点AP_A之间的无线信道物理特征V_A作为签名密钥对$X=g^x \bmod p$进行签名，生成$MAC_X=f(X||V_A)$，其中f()为哈希散列函数，||为连接操作；

[0045] 4)UE_A将协商向量(X,MAC_X,$TMSI_A$,SN_AID)传给UE_B，$TMSI_A$为UE_A在服务网络中注册的临时身份标识，SN_AID为UE_A所在的服务网络ID；

[0046] 5)UE_B选取介于2到p-2之间的一个随机数y，$2 \leqslant y \leqslant p-2$，计算中间值$Y=g^y \bmod p$；

[0047] 6)UE_B以过去T秒内采集到的UE_B与无线接入点AP_B之间的无线信道物理特征V_B作为签名密钥对$Y=g^y \bmod p$进行签名，生成$MAC_Y=f(Y||V_B)$，其中f()为哈希散列函数，||为连接操作；

[0048] 7)UE_B将{Y,MAC_Y,$TMSI_B$,SN_BID}传给UE_A，$TMSI_B$为UE_B在服务网络中注册的临时身份标识，SN_BID为UE_B所在的服务网络ID。

[0049] 2、UE_A和UE_B开始身份签名验证，双方通过各自所属5G服务网络中的签名验证模块S_A,S_B向无线接入点AP_A和AP_B验证签名的有效性，签名验证基本流程如图2所示：

[0050] 1)UE_A将收到的{Y,MAC_Y,$TMSI_B$,SN_BID}传给S_A，由S_A根据SN_BID将验证请求{Y,$TMSI_B$,SN_BID}转发给服务网络SN_B的签名验证模块S_B；

[0051] 2)S_B检查SN_BID是否是本服务网络的ID，若不是设置返回值Res_B='$error_1$'，转步骤5)，否则将{Y,$TMSI_B$}转发给无线接入点AP_B，请求计算$TMSI_B$对应终端的哈希签名；

[0052] 3)AP_B接收到{Y,$TMSI_B$}检查$TMSI_B$是否为本接入点注册的本地设备，若不是设置返回值Res_B='$error_2$'，转步骤4)；否则以过去T秒内采集到的UE_B与AP_B之间的无线信道物理特征V_B作为签名密钥对Y进行签名，生成$MAC_Y'=f(Y||V_B)$，其中f()为哈希散列函数，||为连接操作，AP_B设置返回值为Res_B='MAC_Y''；

[0053] 4)AP_B将Res_B返回给S_B；

[0054] 5)S_B将Res_B转发给S_A；

[0055] 6)若Res_B为'$error_1$'或'$error_2$'，则S_A直接返回Res_B给UE_A，否则S_A比较MAC_Y与Res_B中包含的MAC_Y'：若$MAC_Y=MAC_Y'$，设置Res_B='OK'，否则设置Res_B='FAILED'，随后返回Res_B给UE_A；

[0056] 7)UE_A检查Res_B的返回结果，若Res_B为‘OK’，则计算$Y^x \bmod p$得到会话密钥$K_1=g^{xy} \bmod p$，否则重新发起与B的密钥协商过程；

[0057] 8)UE_B的签名检验过程与UE_A一样，若最终S_B返回给UE_B的Res_A为‘OK’，则计算$X^y \bmod p$得到会话密钥$K_2=g^{xy} \bmod p$。

[0058] 从上述密钥协商和签名验证过程可以看出，若UE_A，UE_B均为真实身份，则最终可以生成相同的通信密钥$K_1=K_2=g^{xy} \bmod p$；反之，如图1所示，存在非法用户UE_C意图实施中间人攻击，由于窃密信道与UE_A，UE_B与无线接入点AP_A和AP_B之间的合法信道的物理独立性，UE_C无法获知信道状态特征向量V_A，V_B；而UE_C的窃密信道通信特征V_C与V_A，V_B不同，因此无法利用$f(Y||V_C)$与$f(X||V_C)$冒充UE_A或UE_B通过签名验证。

[0059] 本发明利用了5G网络通信速度快，在一个全双工的通信周期内，IoT终端与接入点之间的无线物理信道特征保持稳定，且信道特征只为终端与接入点所感知的特点进行通信者身份认证。优选的，可选择的与无线物理信道相关的物理信道特征有：信道增益(GAIN)、接收信号强度(RSSI)、信道状态信息(CSI)：幅度、相位、载波频率(FRE)、信道脉冲响应(CIR)、信道频率响应(CFR)、接收信号包络(Env)、误比特率(BER)，均可通过物理层信号分析完成上述信号的收集。在一次具体实施例中，可以根据IoT终端类别、网络环境等选择其中某一项特征或某几项特征的组合。

[0060] 以上所述实施例仅表达了本发明的具体实施方式，其描述较为具体和详细，但并不能因此而理解为对本发明专利范围的限制。应当指出的是，对于本领域的普通技术人员来说，在不脱离本发明构思的前提下，还可以做出若干变形和改进，这些都属于本发明的保护范围。

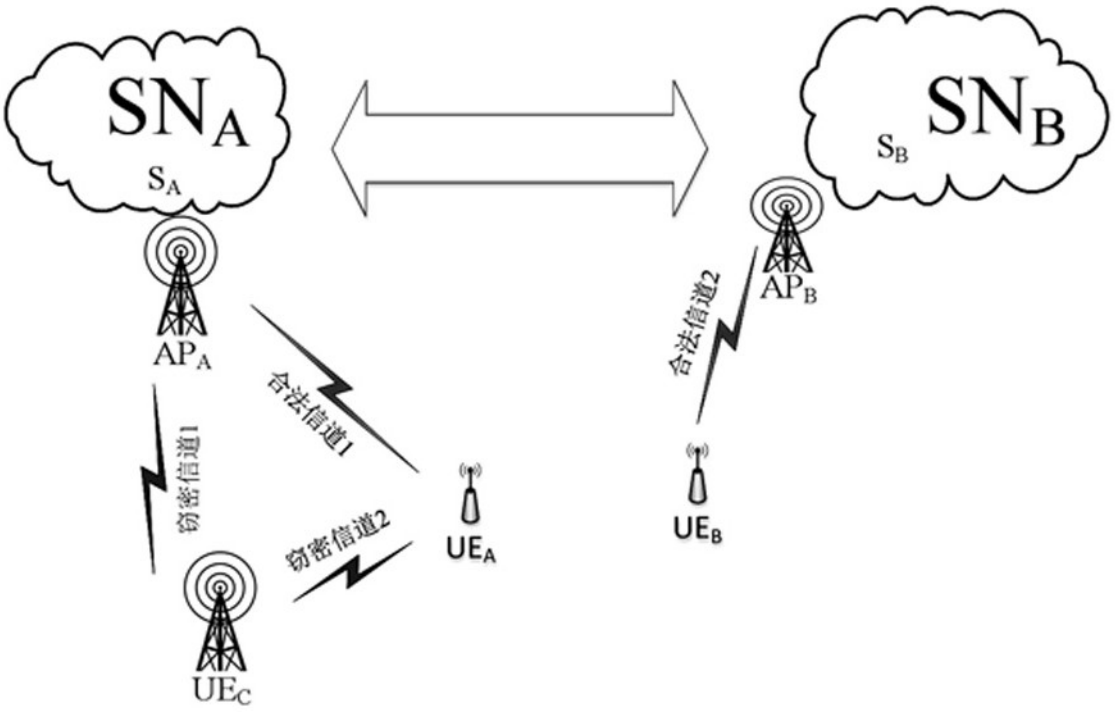

SNA
SA
SNB
SB
APA
APB
合法信道1
合法信道2
窃密信道1
窃密信道2
UEA
UEB
UEC

图1

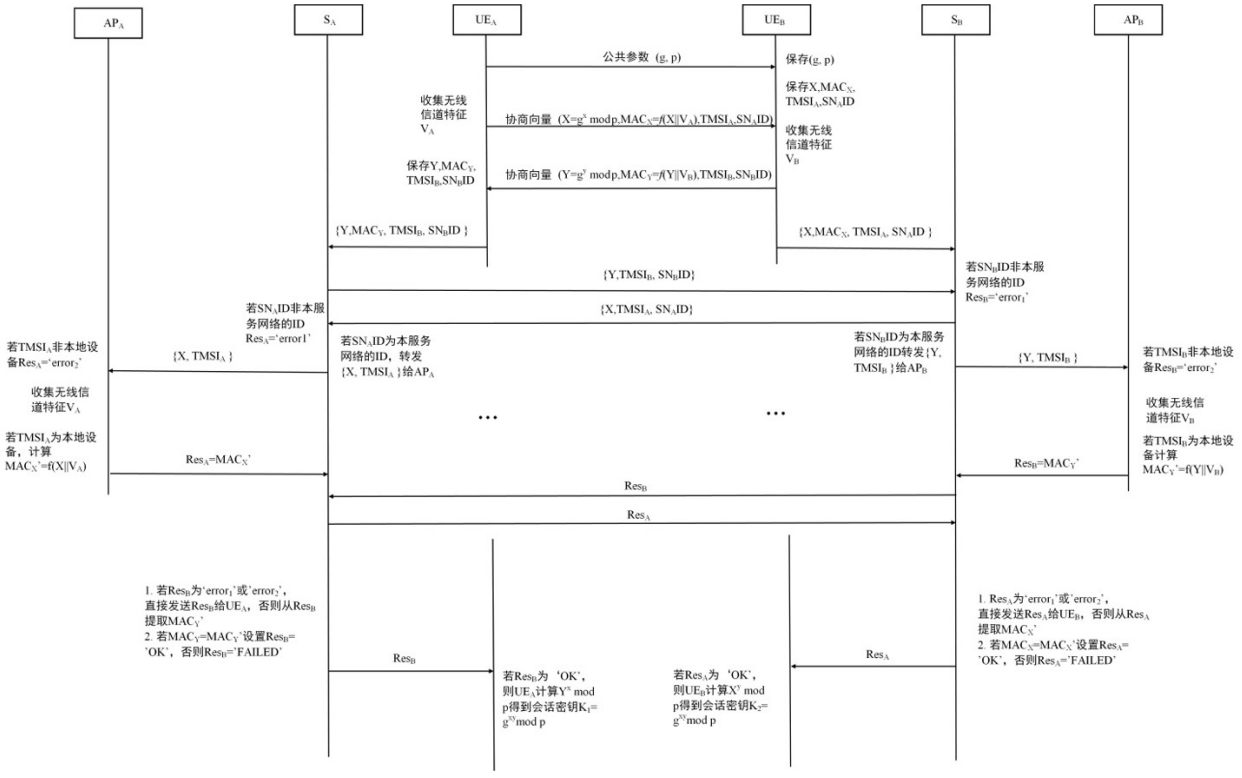

APA
SA
UEA
UEB
SB
APB
公共参数 (g, p)
保存(g, p)
保存X,MACX,
TMSIA,SNAID
收集无线
信道特征
VA
协商向量 (X=g^x mod p,MACX=f(X||VA),TMSIA,SNAID)
收集无线
信道特征
VB
保存Y,MACY,
TMSIB,SNBID
协商向量 (Y=g^y mod p,MACY=f(Y||VB),TMSIB,SNBID)
{Y,MACY, TMSIB, SNBID }
{X,MACX, TMSIA, SNAID }
{Y,TMSIB, SNBID}
若SNBID非本服
务网络的ID
ResB='error1'
若SNAID非本服
务网络的ID
ResA='error1'
{X,TMSIA, SNAID}
若TMSIA非本地设
备ResA='error2'
{X, TMSIA }
若SNAID为本服务
网络的ID，转发
{X, TMSIA }给APA
若SNBID为本服务
网络的ID转发{Y,
TMSIB }给APB
{Y, TMSIB }
若TMSIB非本地设
备ResB='error2'
收集无线信
道特征VA
收集无线信
道特征VB
若TMSIA为本地设
备，计算
MACX'=f(X||VA)
若TMSIB为本地设
备计算
MACY'=f(Y||VB)
ResA=MACX'
ResB=MACY'
ResB
ResA
1. 若ResB为'error1'或'error2'，
直接发送ResB给UEA，否则从ResB
提取MACY'
2. 若MACY=MACY'设置ResB=
'OK'，否则ResB='FAILED'
1. ResA为'error1'或'error2'，
直接发送ResA给UEB，否则从ResA
提取MACX'
2. 若MACX=MACX'设置ResA=
'OK'，否则ResA='FAILED'
ResB
ResA
若ResB为 'OK'，
则UEA计算Y^x mod
p得到会话密钥K1=
g^xy mod p
若ResA为 'OK'，
则UEB计算X' mod
p得到会话密钥K2=
g^xy mod p

图2