



(12)发明专利申请

(10)申请公布号 CN 107105067 A

(43)申请公布日 2017.08.29

(21)申请号 201610878876.5

(22)申请日 2010.08.31

(30)优先权数据

09305807.1 2009.09.02 EP

(62)分案原申请数据

201080048755.9 2010.08.31

(71)申请人 金雅拓股份有限公司

地址 法国默东

(72)发明人 K. 尼施

(74)专利代理机构 北京市柳沈律师事务所

11105

代理人 李芳华

(51)Int.Cl.

H04L 29/12(2006.01)

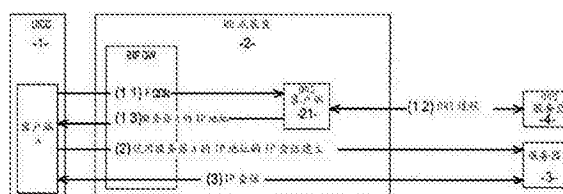
权利要求书1页 说明书4页 附图2页

(54)发明名称

用于操作安全装置的方法、移动设备和安全装置

(57)摘要

本发明涉及用于操作安全装置的方法、移动设备和安全装置。一种用于操作安全装置以在该安全装置和其IP地址被动态分配的目标装置之间建立IP会话的方法,所述安全装置适合于插入在无线装置中,该方法包括:-所述安全装置向所述无线装置上驻留的DNS客户端发送请求以将全称域名FQDN解析为目标服务器的IP地址;-在所述安全装置上从所述无线装置上驻留的DNS客户端接收所述目标服务器的IP地址;和-所述安全装置使用接收的IP地址发起与目标服务器的独立承担协议会话。



1. 一种用于操作安全装置以在该安全装置和其IP地址被动态分配的目标装置之间建立IP会话的方法,所述安全装置适合于插入在无线装置中,该方法包括:

-所述安全装置向所述无线装置上驻留的DNS客户端发送请求以将全称域名FQDN解析为目标服务器的IP地址;

-在所述安全装置上从所述无线装置上驻留的DNS客户端接收所述目标服务器的IP地址;和

-所述安全装置使用接收的IP地址发起与目标服务器的独立承担协议会话。

2. 根据权利要求1的方法,其中所述DNS客户端自己解析IP地址。

3. 根据权利要求1的方法,其中所述DNS客户端连接到用于解析目标服务器的IP地址的DNS服务器,然后该DNS服务器将所解析的IP地址返回到该无线装置上驻留的DNS客户端。

4. 根据权利要求1的方法,其中所述安全装置使用所解析的地址来发起与目标服务器的独立承担协议会话。

5. 根据权利要求2或3的方法,其中所述DNS客户端打开与目标服务器的BIP信道。

6. 根据前述权利要求之一的方法,其中所述方法包括使用智能卡作为安全装置。

7. 一种移动设备,包括安全装置并且在内部具有DNS客户端,所述安全装置通过使用根据前述权利要求之一的方法来解析它想要接入的目标服务器的IP地址。

8. 一种安全装置,被配置为向无线装置上驻留的DNS客户端发送请求以解析目标服务器的IP地址,所述请求包括主动式命令,所述主动式命令具有全称域名FQDN作为它的参数之一。

用于操作安全装置的方法、移动设备和安全装置

[0001] 本专利申请是下列发明专利申请的分案申请：

[0002] 申请号：201080048755.9

[0003] 申请日：2010年8月31日

[0004] 发明名称：安全装置解析目标服务器的因特网协议地址的方法

技术领域

[0005] 本发明涉及无线电信领域。本发明特别涉及一种由安全装置解析安全装置想要接入的目标服务器的IP地址的方法。

背景技术

[0006] 为了由诸如UICC (通用集成电路卡) (还称为智能卡) 的安全装置发起与位于因特网中某处的服务器的IP连接,安全装置首先需要知道目标服务器的IP地址。

[0007] IP地址可以动态地分配并且随时间改变。这样,安全装置需要基于服务器的诸如FQDN (完全合格域名) 的已知信息来解析IP地址。DNS客户端 (如果需要,利用来自DNS服务器的支持) 可解析IP地址。

[0008] 然后,除非安全装置支持内部的DNS客户端,安全装置需要请求诸如移动设备 (ME) 的无线装置上驻留的DNS客户端来解析IP地址。

[0009] 主要的问题在于,DNS解析器驻留在无线装置上,并且不存在用于安全装置请求DNS解析器解析OTA (空中下载) 服务器的IP地址的标准方式。不存在用于安全装置请求在无线装置内部的DNS客户端解析目标服务器的IP地址的标准方式。

[0010] 当前的ETSI或3GPP标准例如没有提供用于由UICC请求移动设备 (ME) 上驻留的DNS客户端解析UICC想要接入的服务器的IP地址的手段。并且,当前的标准假设UICC预先知道所述服务器的IP地址。这防止UICC发起与位于因特网中某处的服务器的IP会话,特别是在服务器的IP地址动态地改变时,因为UICC不能解析目标服务器的IP地址。

[0011] 对于在可以为ME或UICC的装置上要解析的OTA服务器IP地址,一种已知解决方案是将DNS解析器功能放在UICC中。如果UICC需要解析IP地址,则UICC需要与DNS服务器交谈。为此,UICC需要知道ME在网络附接时从网络接收的DNS服务器IP地址。然而,UICC不能得到这个DNS服务器IP地址。

[0012] 然后,一种方法在于取决于装置管理协议。在OMA (开放移动联盟) 装置管理协议中,UICC包括能够诊断ME配置的DM服务器。这允许DM服务器得到在ME中存储的DNS IP地址。通过在UICC内具有DM服务器功能,UICC可以例如使用BIP (独立承担协议 (Bear Independent Protocol)) UICC服务器模式来从ME得到DNS IP地址。一旦获得了DNS IP地址,UICC将在BIP UICC客户端模式中进行其它步骤。BIP UICC服务器模式和客户端模式是公知的。BIP UICC服务器模式对应于智能卡万维网服务器。主要地,在BIP中,存在两种模式,UICC服务器或UICC客户端。这里,由于使用了UICC中的DM服务器,所以它仅仅在这个步骤需要BIP服务器模式。然而,这个方法的一个主要缺点是DM服务器的可用性,其需要BIP

UICC服务器模式,并且从今天起(as of today)没有在中很好部署。

[0013] 然后,仍旧需要提供用于由智能卡解析UICC想要接入的目标服务器的IP地址的方法。

发明内容

[0014] 本发明的目标是提供一种用于由安全装置解析该安全装置想要接入的目标服务器的IP地址的方法,所述安全装置适合于插入在无线装置中,其中所述安全装置向所述无线装置上驻留的DNS客户端发送请求以解析目标服务器的IP地址,所述目标服务器通过其FQDN来标识。

[0015] 根据本发明的另一方面,

[0016] 一所述请求可包括主动式(proactive)命令;

[0017] 一所述DNS客户端可以自己解析IP地址;

[0018] 一所述DNS客户端可连接到用于解析目标服务器的IP地址的DNS服务器以,然后DNS服务器将所解析的IP地址返回到该无线装置上驻留的DNS客户端;

[0019] 一DNS客户端将所解析的目标服务器的IP地址返回到安全装置;

[0020] 一所述安全装置可以使用所解析的地址来发起与目标服务器的独立承担协议会话;

[0021] 一所述DNS客户端可打开与目标服务器的BIP信道;

[0022] 一所述方法可包括使用智能卡作为安全装置。

[0023] 所述安全装置可有利地发起与服务器的IP会话,所述服务器的IP地址被动态地分配、并且可以由无线装置上的DNS客户端(如果需要,利用来自DNS服务器的支持)来解析。

[0024] 利用这个方法,安全装置能够使用在ETSI TS 102 223中定义的独立承担协议来请求与服务器的IP会话。

[0025] 本发明的又一目标是提供包括安全装置并且在内部具有DNS客户端的移动设备,所述安全装置通过使用所述方法来解析它想要接入的目标服务器的IP地址。

[0026] 本发明的又一目标是提供一种用于操作安全装置以在该安全装置和其IP地址被动态分配的目标装置之间建立IP会话的方法,所述安全装置适合于插入在无线装置中,该方法包括:-所述安全装置向所述无线装置上驻留的DNS客户端发送请求以将全称域名FQDN解析为目标服务器的IP地址;-在所述安全装置上从所述无线装置上驻留的DNS客户端接收所述目标服务器的IP地址;和-所述安全装置使用接收的IP地址发起与目标服务器的独立承担协议会话。

[0027] 本发明的又一目标是提供一种安全装置,被配置为向无线装置上驻留的DNS客户端发送请求以解析目标服务器的IP地址,所述请求包括主动式命令,所述主动式命令具有全称域名FQDN作为它的参数之一。

[0028] 现在参考附图来作为示例描述本发明。

[0029] 为了获得上面陈述的方式以及本发明的其它优点和特征,将通过参考来呈现上面简要描述的本发明的更具体描述。

附图说明

[0030] 尽管任何其它形式可落入本发明的范围,但是现在还是仅参考附图作为示例来描述本发明的优选形式,在附图中:

[0031] 图1示意性示出了根据本发明的方法的图,其中所解析的IP地址被返回到安全装置。

[0032] 图2示意性示出了根据另一实施例的方法的图,其中所解析的IP地址没有被返回到安全装置。

具体实施方式

[0033] 根据这里提供的详细描述可以理解本发明。

[0034] 图1中示出了根据本发明实施例的方法。所述方法包括不同步骤,允许诸如UICC 1的安全装置与无线装置(诸如ME 2)上驻留的DNS客户端21对话,以便获得UICC 1想要连接的目标服务器3的已解析IP地址。在接下来的描述中,所述目标服务器3被称为服务器A。

[0035] 为此,UICC请求ME 2上驻留的DNS客户端21解析所述IP地址。所述请求可以为主动式命令的形式,其例如可以为在ETSI TS 102 223中已经定义的现有主动式命令的扩展、或者为新的主动式命令。响应于这个主动式命令,ME中的所述DNS客户端21将返回目标服务器3的已解析IP地址。

[0036] 更精确地,所述方法包括步骤11,其中UICC 1请求ME 2中驻留的DNS客户端21解析通过它的FQDN标识的服务器的IP地址。请求可以是现有的主动式命令,其例如可以是现有的提供本地信息(PROVIDE LOCAL INFORMATION)命令或现有的打开信道(OPEN CHANNEL)命令。在主动式命令中,可能设置一些参数。当前的标准不允许将FQDN设置为所述参数之一。一种扩展允许那些主动式命令具有目标服务器的FQDN作为它的参数之一。

[0037] ME 2上驻留的所述DNS客户端21首先尝试自己解析所述IP地址,即通过搜索例如在高速缓冲存储器中本地存储的它自己的数据库。

[0038] 如果ME 2中的DNS客户端进行管理以在本地发现或解析IP地址,则它不需要连接到已知的DNS服务器4。否则,在另一步骤12中,DNS客户端21连接到DNS服务器4,并且DNS服务器4返回目标服务器3的已解析IP地址。

[0039] 在接下来的步骤13中,ME 2上驻留的DNS客户端21向UICC 1返回服务器A 3的已解析IP地址。通过遵循该过程,UICC 1可以得到目标服务器3的IP地址,并然后在步骤20中使用这个解析的IP地址来发起与目标服务器的例如根据ETSI TS 102 223的独立承担协议会话。在这个步骤20中,主动式命令是打开信道,将服务器A的IP地址设置为这个主动式命令的参数之一。

[0040] 利用这个实施例,然后在首先获得解析的IP地址、并且建立与服务器A的IP会话的两个主要步骤中牵涉UICC。将解析的IP地址返回到UICC 1。

[0041] 特别当期望向UICC 1提供从DNS服务器返回的、并且在这个主动式命令的应答中接收的几个地址中选择IP地址的可能性时,这个选项是有效的。例如,如果DNS服务器向一个IP地址解析请求返回两个IP地址(主地址和从地址),则它可能是这样的情况。如果将两个IP地址返回到UICC 1,则UICC 1在设置连接时可以自由地使用它们之一。如果操作者让UICC 1管理主服务器和从服务器之间的负载平衡,则这可能是有用的。

[0042] 图2中示出了当UICC提供目标服务器的FQDN时的方法的另一实施例。

[0043] 在这个实施例中,所述方法提供用于请求ME 2打开IP会话的方式。当UICC 1为目标服务器提供FQDN时请求ME 2打开IP会话的所述方法可以为现有的打开信道命令的扩展的形式,其正发起独立承担协议。

[0044] 更精确地,所述方法包括步骤110,其中UICC 1请求ME 2中驻留的DNS客户端21解析通过它的FQDN标识的服务器的IP地址。如刚才在上面描述的,现有的主动式命令例如可以是将FQDN设置为主动式命令的参数之一的现有的打开信道命令。现有的打开信道命令有利地允许打开BIP信道并建立IP会话。

[0045] ME 2上驻留的DNS客户端21首先尝试自己解析IP地址,即通过搜索本地存储的它自己的数据库。如果ME 2中的DNS客户端21进行管理以在本地发现或解析IP地址,则它不需要连接到DNS服务器。否则,在另一步骤120中,DNS客户端21连接到已知的DNS服务器4,并且DNS服务器4返回目标服务器3的已解析IP地址。

[0046] 在接下来的步骤130中,ME 2上驻留的DNS客户端21没有向UICC 1返回服务器A3的已解析IP地址。DNS客户端21通过设置解析的IP地址打开与目标服务器的BIP信道。

[0047] 通过提供在打开信道中设置FQDN的可能性,ME 2解析IP地址,并且打开与目标服务器3的IP会话。在这个情况下,一旦建立了这个IP会话,则UICC 1仅仅从ME 2接收通知。

[0048] 在这个实施例中,UICC 1仅提供FQDN,并且仅仅在建立与服务器A 3的IP连接的一个主要步骤中牵涉。从DNS服务器21返回的IP地址没有被返回到UICC 1。

[0049] 图2中所示的实施例有利地提供了用于UICC 1的最简单解决方案,因为UICC 1需要做的唯一事情是提供目标服务器的FQDN。然后,其它步骤由ME 2中的DNS客户端21来处理,并且UICC 2在没有任何进一步动作的情况下得到所建立的到服务器3的连接。

[0050] 这两个实施例二者都取决于ME 2中的DNS客户端21。

[0051] 当操作者希望UICC 1在主IP地址和从IP地址之间进行一些选择或者操纵时,图1中所示的根据该实施例的方法具有优点。

[0052] 当操作者希望具有完全取决于ME 2中的DNS客户端21的最简单解决方案时,图2中所示的根据该实施例的方法具有优点。

[0053] 借助于本发明,UICC 1能够发起与服务器的IP会话,该服务器的IP地址被动态地分配、并且可通过ME 2上驻留的DNS客户端21(如果需要,利用来自DNS服务器的支持)来解析。

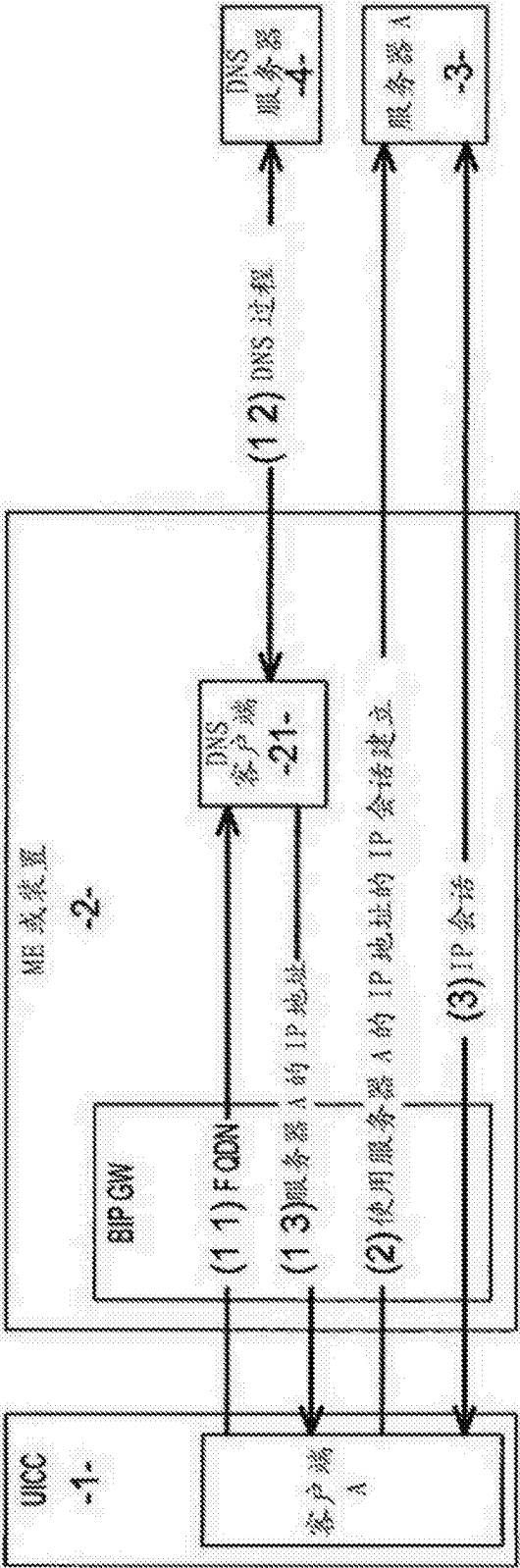


图1

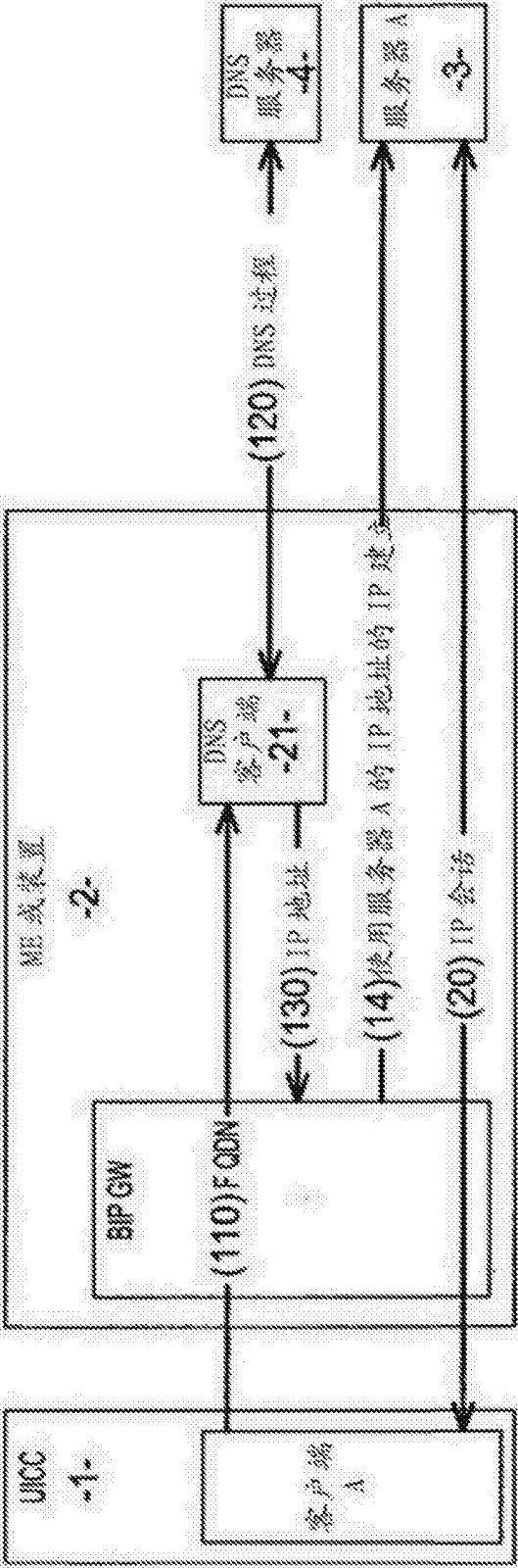


图2