(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2007 年4 月26 日 (26.04.2007)

PCT

(10) 国际公布号
WO 2007/045155 A1

(51) 国际专利分类号:
H04Q 7/32 (2006.01)

(21) 国际申请号: PCT/CN2006/002703

(22) 国际申请日: 2006 年10 月13 日 (13.10.2006)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
200510100415.7
2005 年10 月15 日 (15.10.2005) CN
200610034929.1
2006 年4 月6 日 (06.04.2006) CN
200610034928.7
2006 年4 月6 日 (06.04.2006) CN
200610141483.2
2006 年9 月29 日 (29.09.2006) CN

(71) 申请人 (对除美国外的所有指定国): 华为技术有限公司(HUAWEI TECHNOLOGIES CO., LTD.) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

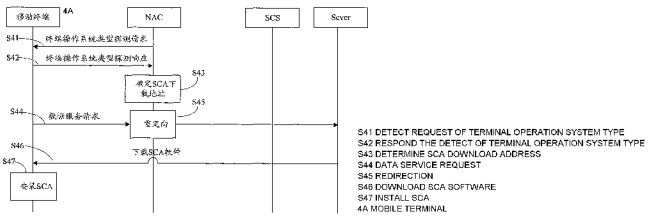
(72) 发明人; 及

(75) 发明人/申请人 (仅对美国): 姬长锋(JI, Changfeng)

[见续页]

(54) Title: A METHOD FOR REALIZING MOBILE STATION SECURE UPDATE AND CORRELATIVE REACTING SYSTEM

(54) 发明名称: 一种实现移动台安全更新的方法及关联响应系统



(57) Abstract: A correlative reacting system(CRS) and method for realizing mobile station secure update is provided in the invention, the CRS includes security correlative agent(SCA) and security correlative server(SCS) which is in the network side and communicates with SCA though air interface. In the invention, the CRS interchanges information with mobile station and control mobile station to update automatically. The automatic secure update includes automatic download install, updating SCA and repairing insecure factor of mobile station automatically and so on. In the invention, mobile station can automatically be controlled to finish automatic secure update without user's participance, thus mobile station's security can be improved and it's burden of security process can be decreased, and service communication quality can be increases, synchronously communication burden of operation manager can be decreased.

(57) 摘要:

本发明公开一种通过关联响应系统及实现移动台安全更新的方法，所述关联响应系统包括位于终端侧的安全关联代理，以及位于网络侧，通过空中接口与安全关联代理通信的安全关联服务器。本发明中，所述关联响应系统与所述移动台进行信息交互，控制移动台进行自动安全更新。所述自动安全更新包括自动下载安装、更新安全关联代理，以及对移动台的不安全因素进行自动修复等等。本发明可以控制移动台完成自动安全更新，而不需要用户的参与，从而增加了移动台的安全性，降低了用户的安全处理负担，提高用户的业务通信质量，同时能够降低运营商的通信负担。

WO 2007/045155 A1

[CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 **位继伟(WEI, Jiwei)** [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 **刘淑玲(LIU, Shuling)** [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 **郑志彬(ZHENG, Zhibin)** [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(74) 代理人：北京集佳知识产权代理有限公司(UNITALEN ATTORNEYS AT LAW); 中国北京市朝阳区建国门外大街22号赛特广场7层, Beijing 100004 (CN)。

(81) 指定国（除另有指明，要求每一种可提供的国家保护）：AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国（除另有指明，要求每一种可提供的地区保护）：ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 欧洲 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)。

本国际公布：

— 包括国际检索报告。

所引用双字母代码及其它缩写符号，请参考刊登在每期PCT公报期刊起始的“代码及缩写符号简要说明”。

一种实现移动台安全更新的方法及关联响应系统

技术领域

本发明涉及移动网络安全技术，尤其涉及一种实现移动台安全更新的方法及关联响应系统。

背景技术

关联响应系统（Correlative Reacting System，CRS）是一种通过控制不安全终端，即不符合移动网络指定的安全策略（例如有安全漏洞或感染病毒）的移动台的接入，避免移动网络遭受不安全终端的安全威胁的系统。CRS 通过移动台和网络侧的安全联动，对移动台的网络接入进行控制，同时对其应用服务的接入进行限制，从而提高移动网络对病毒、蠕虫、网络攻击等的安全免疫力。

图 1 示出关联响应系统的结构。关联响应系统包括移动台（Mobile station，MS）侧的安全关联代理（Security Correlative Agent，SCA）110、安全关联服务器（Security Correlative Server，SCS）120 以及与移动台、SCS 120 连接的网络接入控制器（Network Access Controller，NAC）131 和应用服务控制器（Application Service Controller，ASC）132。在具体实现上，NAC 131 和 ASC 132 可以是两个独立的实体，或者是一个实体中两个独立的功能单元。一个 SCS 120 可以连接多个 NAC 131 和/或 ASC 132，一个 NAC 131 和/或 ASC 132 可以对多个移动台的网络接入和/或应用服务进行控制。

SCA 110 收集移动台的安全相关信息（Security Correlative Information，SCI），并将收集到的安全相关信息上报到 SCS 120。

SCS 120 是 CRS 的控制单元和分析处理单元，负责接收、分析、存储 SCA 110 上报的安全信息，进行关联分析，向 NAC 131、ASC 132 或者 SCA 110 发送 CRS 控制指令；通过与 NAC 131 的联动，实现对用户接入网络的限制，以防止不安全终端对网络资源的不合理占用，阻止恶意病毒在网络中传播；通过与 ASC 132 的联动，限制或禁止用户使用特定应用服务，从而保护移动网络免受不安全服务带来的安全风险。

关联响应系统和方法在具体实现时，移动台需要具备相应的组件，因此，需要提供相应的机制来实现移动台组件的安装。由于安装和配置的过程较为复杂，一般来说应尽量减少用户的参与，以保证安装的效率和准确度。此外，在移动台的状态发生变化时，特别是在终端侧出现安全隐患时，需要对其进行实时更新，尽量降低移动台的不安全状态持续的时间，以避免影响用户的正常使用，避免给网络的安全性能带来不利的影响。此外，在现有技术中，还缺少移动台安全相关信息的收集、整理、上报、分析以及根据安全相关信息对移动台的接入策略进行控制更新的实现方案。

发明内容

本发明提供一种实现移动台安全更新的方法和关联响应系统，可以根据移动台的信息进行移动台的自动安全更新，可以降低出错的几率，提高系统的安全性能。

根据本发明的一个方面，一种实现移动台安全更新的方法，包括:

关联响应系统中的实体与移动台进行信息交互;

当根据所述信息交互确认需要安全更新时，所述关联响应系统的网络侧向移动台下发安全更新控制信息;

根据所述安全更新控制信息完成移动台的自动安全更新。

可选地，所述关联响应系统与移动台进行信息交互为：关联响应系统的网络接入控制器向移动台发送安全关联代理探测请求消息，该消息中携带安全关联代理的初始化配置信息;

所述当根据所述信息交互确认需要安全更新时，所述网络侧向移动台下发安全更新控制信息为：如果移动台未响应所述探测请求消息，则判定移动台需要安装安全关联代理；所述网络接入控制器触发移动台启动安全关联代理的下载安装;

所述完成移动台的自动安全更新为：将安全关联代理下载并安装到移动台。

可选地，所述移动台未响应所述探测请求消息包括：所述网络接入控制器在定时内未收到移动台的探测响应，或者网络接入控制器发送安全关联代理探测请求消息的次数超过设定门限。

可选地，该方法还包括：当移动台安装有安全关联代理且工作正常时，移动台的安全关联代理提取并保存所述安全关联代理探测请求消息中的初始化配置信息，并向网络接入控制器返回安全关联代理探测响应消息。

可选地，所述安全关联代理探测响应消息中包含移动台不需要安装安全关联代理的通知信息、安全关联代理的标识和/或 IP 地址信息。

可选地，所述关联响应系统与移动台进行信息交互为：关联响应系统的安全关联服务器向移动台发送安全关联代理探测请求消息，该消息中携带安全关联代理的初始化配置信息；

所述当根据所述信息交互确认需要安全更新时，所述网络侧向移动台下发安全更新控制信息为：如果移动台未响应所述探测请求消息，则判定移动台需要安装安全关联代理；所述安全关联服务器触发移动台的下载安装操作；

所述完成终端的自动安全更新为：将安全关联代理下载安装到移动台。

可选地，所述移动台未响应所述探测请求消息包括：所述安全关联服务器在定时内未收到移动台的探测响应，和/或安全关联服务器发送安全关联代理探测请求消息的次数超过设定门限。

可选地，所述关联响应系统的安全关联服务器向移动台发送安全关联代理探测请求消息之前，还包括：关联响应系统的网络接入控制器向安全关联服务器发送移动台连接报告。

可选地，在所述判定移动台需要安装安全关联代理时，安全关联服务器发送移动台连接响应 A 类消息给网络接入控制器，通知网络接入器所述移动台需要安装安全关联代理。

可选地，该方法还包括：当移动台安装有安全关联代理且工作正常时，移动台的安全关联代理提取并保存所述安全关联代理探测请求消息中的初始化配置信息，并向安全关联服务器返回安全关联代理探测响应消息。

可选地，所述安全关联代理探测响应消息中包含移动台不需要安装安全关联代理的通知信息、安全关联代理的标识和/或 IP 地址信息。

可选地，所述将安全关联代理下载并安装到移动台，包括：

所述关联响应系统的网络接入控制器接收移动台的数据服务请求，将

所述数据服务请求重定向到安全关联代理的下载地址;

移动台根据所述安全关联代理的下载地址下载安装对应的安全关联代理。

可选地，所述安全关联代理的下载地址是由网络接入控制器确定的，包括:

所述网络接入控制器向移动台发送操作系统类型探测请求消息，请求获取移动台的操作系统/平台类型信息;

所述移动台向网络接入控制器返回操作系统类型探测响应消息，消息携带移动台的操作系统/平台类型信息;

所述网络接入控制器根据移动台的操作系统/平台类型信息确定与所述操作系统/平台类型信息对应的安全关联代理的下载地址。

可选地，所述下载地址对应提供安全关联代理的下载服务器;

所述下载服务器根据与移动台连接过程中传递的参数判断移动台需要下载的安全关联代理。

可选地，所述关联响应系统的网络接入控制器接收移动台的数据服务请求时，如果移动台尚未完成安全关联代理的下载或者网络接入控制器尚未获悉移动台需要安装安全关联代理，则网络接入控制器对移动台的数据服务请求进行安全处理。

可选地，所述安全关联代理探测请求消息的目的地址为移动台的 IP 单播地址或者组播地址；所述初始化配置信息包括安全关联服务器的 IP 地址或服务端口。

可选地，所述关联响应系统与移动台进行信息交互为：网络侧向移动台发送安全关联代理探测请求消息;

所述当根据所述信息交互确认需要安全更新时，所述网络侧向移动台下发安全更新控制信息为：如果移动台未响应所述探测请求消息，则判定移动台需要安装安全关联代理；所述网络侧触发移动台启动安全关联代理的下载安装;

所述完成移动台的自动安全更新为：将安全关联代理下载并安装到移动台。

可选地，所述关联响应系统与移动台进行信息交互为：位于终端侧的关联响应系统的安全关联代理收集移动台的安全相关信息，上报给关联响应系统的安全关联服务器；

所述当根据所述信息交互确认需要安全更新时，所述网络侧向移动台下发安全更新控制信息为：所述安全关联服务器分析安全关联代理上报的安全相关信息，在需要时向安全关联代理返回安全相关信息响应；

所述完成终端的自动安全更新为：所述安全关联代理保存所述安全相关信息响应。

可选地，所述位于终端侧的关联响应系统的安全关联代理收集移动台的安全相关信息，包括：

所述安全关联代理通过移动台的软件接口收集移动台的安全相关信息；

所述安全关联代理整理所述安全相关信息，选择向安全关联服务器上报的信息内容；

所述上报给关联响应系统的安全关联服务器为：所述安全关联代理通过与安全关联服务器之间的安全信息传送通道向安全关联服务器发送安全相关信息报告，携带所述选择后的信息内容。

可选地，所述选择向安全关联服务器上报的信息内容为：安全关联代理选择其收集的移动台的安全相关信息的全部信息或者部分信息。

可选地，所述发送安全相关信息报告的步骤为定期的、或者是由移动台的安全事件触发的，或者由安全关联服务器主动查询触发的。

可选地，所述安全相关信息报告还包含可选的安全相关信息报告消息序列号、安全关联代理标识、安全关联服务器标识。

可选地，所述安全关联服务器分析安全关联代理上报的安全相关信息，在需要时向安全关联代理返回安全相关信息响应为：

所述安全关联服务器对安全关联代理上报的安全相关信息进行有效性检查；对所述安全相关信息进行关联分析；根据所述关联分析的结果更新本地保存的移动台的安全相关信息；

所述安全关联服务器根据所述关联分析的结果通过与安全关联代理之

间的安全信息传送通道向安全关联代理返回安全相关信息响应，携带安全关联服务器向安全关联代理反馈的安全控制信息和移动台安全等级评估结果。

可选地，所述关联分析为单用户信息关联分析和多用户相似信息的关联分析。

可选地，在根据所述关联分析的结果更新本地保存的移动台的安全相关信息之后，还包括：

所述安全关联服务器根据所述关联分析的结果判断是否更新移动台的安全控制策略，是则通过与网络接入控制器或者应用服务控制器之间的安全信息传送通道向网络接入控制器或者应用服务控制器发送安全控制策略更新请求，携带安全关联代理标识、用户标识以及更新后的安全控制策略信息；

所述网络接入控制器或者应用服务控制器通过所述安全信息传送通道向安全关联服务器返回安全控制策略更新响应，通知安全关联服务器移动台的安全控制策略更新结果。

可选地，所述安全关联服务器向安全关联代理反馈的安全控制信息中包含有移动台的安全控制策略更新信息。

可选地，该方法还包括：所述安全关联代理保存移动台最新的安全相关信息、安全相关信息报告内容、安全相关信息报告策略。

可选地，该方法还包括：安全关联代理根据收集的移动台的安全相关信息和安全关联服务器返回的安全相关信息响应生成移动台安全状况评估报告或安全提示信息。

可选地，该方法还包括：所述安全关联代理根据安全关联服务器返回的安全相关信息响应更新移动台的安全应用软件或者给操作系统/平台打补丁。

可选地，所述关联响应系统与移动台进行信息交互为：位于终端侧的关联响应系统的安全关联代理收集移动台的安全相关信息，上报给关联响应系统的安全关联服务器；

所述当根据所述信息交互确认需要安全更新时，所述网络侧向移动台

下发安全更新控制信息为：所述安全关联服务器分析安全关联代理上报的安全相关信息，在所述移动台存在不安全因素时，向安全关联代理返回控制信息；

所述完成终端的自动安全更新包括：所述安全关联代理根据所述控制信息协助移动台修复不安全因素。

可选地，所述完成终端的自动安全更新在网络侧设定的时段进行。

可选地，所述关联响应系统与移动台进行信息交互为：位于终端侧的关联响应系统的安全关联代理收集移动台的安全相关信息，上报给关联响应系统的安全关联服务器；

所述当根据所述信息交互确认需要安全更新时，所述网络侧向移动台下发安全更新控制信息为：所述安全关联服务器分析安全关联代理上报的安全相关信息，在所述移动台的安全关联代理需要更新时，向安全关联代理返回控制信息；

所述完成终端的自动安全更新包括：所述移动台从安全关联服务器下载软件，实现安全关联代理的自动更新。

可选地，该方法还包括：在移动台自动安全更新而造成用户的服务受限时，安全关联代理将服务受限信息通知用户。

可选地，所述关联响应系统与移动台进行信息交互为：当移动台注册到网络后，如果终端侧的安全关联代理已经启动，则所述安全关联代理向安全关联服务器注册；

所述当根据所述信息交互确认需要安全更新时，所述网络侧向移动台下发安全更新控制信息为：如果安全关联代理没有启动或没有安装，则安全关联服务器提供下载安全关联代理所需的信息或发出安全关联代理使能指示；

所述完成终端的自动安全更新包括：将安全关联代理下载安装到移动台。

根据本发明的另一方面，一种关联响应系统，与移动台进行信息交互，包括网络侧的安全关联服务器、与安全关联服务器相连的网络接入控制器和应用服务控制器，所述关联响应系统的安全关联服务器或网络接入控制

器在根据所述信息交互确认需要安全更新时，向移动台下发安全更新控制信息；根据所述安全更新控制信息协助移动台实现自动安全更新。

可选地，所述网络接入控制器用于向移动台发送安全关联代理探测请求消息，该消息中携带安全关联代理的初始化配置信息；如果移动台未响应所述探测请求消息，则判定移动台需要安装安全关联代理；触发移动台启动安全关联代理的下载安装。

可选地，该系统还包括位于移动台侧的安全关联代理，用于提取并保存所述安全关联代理探测请求消息中的初始化配置信息，并向网络接入控制器返回安全关联代理探测响应消息。

可选地，所述安全关联服务器用于向移动台发送安全关联代理探测请求消息，该消息中携带安全关联代理的初始化配置信息；如果移动台未响应所述探测请求消息，则判定移动台需要安装安全关联代理；触发移动台启动安全关联代理的下载安装。

可选地，所述网络接入控制器用于向安全关联服务器发送移动台连接报告。

可选地，该系统还包括：安全关联代理下载服务器，用于在网络接入控制器重定向移动台的数据服务请求后，向移动台提供安全关联代理的下载服务。

可选地，该系统还包括位于移动台侧的安全关联代理，用于提取并保存所述安全关联代理探测请求消息中的初始化配置信息，并向安全关联服务器返回安全关联代理探测响应消息。

可选地，所述网络接入控制器用于接收来自安全关联服务器在判定移动台需要安装安全关联代理时发送的移动台连接响应 A 类消息。

可选地，该系统还包括位于移动台侧的安全关联代理，用于收集移动台的安全相关信息，上报给关联响应系统的安全关联服务器；

所述安全关联服务器用于分析安全关联代理上报的安全相关信息，在需要时向安全关联代理返回安全相关信息响应。

可选地，所述网络接入控制器和应用服务控制器用于接收安全关联服务器在根据分析结果判断需要更新移动台的安全控制策略时下发的安全控

制策略更新请求，向安全关联服务器返回安全控制策略更新响应，通知安全关联服务器移动台的安全控制策略更新结果。

可选地，该系统还包括：安全状态报告或安全提示信息生成单元，用于根据收集的移动台的安全相关信息和安全关联服务器返回的安全相关信息响应生成移动台安全状况评估报告或安全提示信息；所述安全状态报告或安全提示信息生成单元位于安全关联代理内。

可选地，该系统还包括：更新单元，用于根据安全关联服务器返回的安全相关信息响应更新移动台的安全应用软件或者操作系统；所述更新单元位于安全关联代理内。

根据本发明的又一方面，一种关联响应系统，包括网络侧和移动台，所述的网络侧用于与移动台进行信息交互；当根据所述信息交互确认需要安全更新时，向移动台下发安全更新控制信息。

可选地，所述网络侧包括第一消息发送接收模块和判断模块，所述的第一消息发送接收模块用于向所述的移动台发送安全关联代理探测请求消息，并用于接收所述的移动台发送的探测响应消息；所述的判断模块用于根据所述的探测响应消息判断所述的移动台是否应安装安全关联代理；

所述的移动台包括第二消息发送接收模块，用于接收所述的安全关联代理探测请求消息，并向所述的网络侧发送探测响应消息。

可选地，所述的移动台还包括下载安装模块，用于当所述的判断模块判断所述的移动台需要安装安全关联代理时，下载并安装所述的安全关联代理。

本发明通过关联响应系统和终端侧进行信息交互，根据信息交互的结果来控制移动台完成自动安全更新，从而可以移动台状态的变化进行自动处理，从而增加移动台的安全性，进而可以减少网络遭受的不安全终端的威胁。此外，安全更新过程是自动进行的，不需要用户的参与，可以降低用户的安全处理负担，提高用户的业务通信质量，能够降低运营商的通信负担。

本发明的一个可选方案中，可以通过NAC来自动探测移动台是否需要安装SCA，并在移动台需要安装SCA时，触发移动台完成SCA的下载安

装操作，避免用户手工下载安装 SCA，方便用户使用。

本发明的一个可选方案中，可以通过 SCS 来自动探测移动台是否需要安装 SCA，并在移动台需要安装 SCA 时，触发移动台完成 SCA 的下载安装操作， 避免用户手工下载安装 SCA，方便用户使用。

本发明的一个可选方案中，可以实现 SCA 对移动台 SCI 的自动收集、整理、上报，以及 SCS 根据 SCA 上报的 SCI 更新移动台的接入控制和服务控制，从而通过移动台和网络侧进行交互，对移动台的安全状况进行有效的响应，适应移动台的状态变更，更有效地保证网络的安全性能。

此外，终端侧的安全关联代理可以自动向用户提示安全状态，可以根据从终端侧收集到的安全信息和从 SCS 返回的终端安全等级评估结果自动生成终端安全状态报告，供用户主动查询，可以在安全关联服务器的控制下协助移动台修复不安全的因素，提高网络的安全性能。

附图说明

图 1 是现有技术中的关联响应系统的结构示意图；

图 2 是本发明的关联响应系统的实施例的框图；

图 3 是本发明的方法中 NAC 探测移动台是否需要安装 SCA 的实施例的流程图；

图 4 是本发明的方法中移动台安装 SCA 的一个实施例的流程图；

图 5 是本发明的方法中 SCS 探测移动台是否需要安装 SCA 的实施例的流程图；

图 6 是本发明的方法中移动台安装 SCA 的另一个实施例的流程图；

图 7 是本发明的方法中安全相关信息更新的实施例的流程图；

图 8 是本发明的关联响应系统的另一实施例的框图。

具体实施方式

本发明可以基于图 2 所示的关联响应系统实现终端侧的自动安全更新服务。

关联响应系统包括移动台（Mobile station，MS）侧的安全关联代理（Security Correlative Agent，SCA）110、网络侧的安全关联服务器（Security Correlative Server，SCS）120 以及与移动台、SCS 120 连接的网络接入控制

器（Network Access Controller，NAC）131 和应用服务控制器（Application Service Controller，ASC）132。在具体实现上，NAC 131 和 ASC 132 可以是两个独立的实体，或者是一个实体中两个独立的功能单元。一个 SCS 120 可以连接多个 NAC 131 和/或 ASC 132，一个 NAC 131 和/或 ASC 132 可以对多个移动台的网络接入和/或应用服务进行控制。

SCA 110 收集移动台的安全相关信息（Security Correlative Information，SCI），安全相关信息包括应用安全配置信息和安全状况信息，例如感染病毒情况、系统安全配置信息、应用安全配置信息以及漏洞库和病毒库版本情况等，并将收集到的安全相关信息进行初步处理和组织，上报到 SCS 120。

此外，SCA 110 接收 SCS 120 的安全更新命令和指示，一方面向用户报告移动台的安全信息摘要，另一方面为移动台外部组件提供必要的信息和配合，以修复不安全的移动台。

SCS 120 通过空中接口与 SCA 110 通信，是 CRS 的控制单元和分析处理单元，负责接收、分析、存储 SCA 110 上报的安全信息，进行关联分析，根据网络侧设置的安全策略，SCS 120 控制不安全移动台的网络接入能力，并与相关网络设备配合，协助移动台进行安全更新。具体地，可以向 NAC 131、ASC 132 或者 SCA 110 发送 CRS 控制指令，通过与 NAC 131 的联动，实现对用户接入网络的限制，以防止不安全终端对网络资源的不合理占用，阻止恶意病毒在网络中传播；通过与 ASC 132 的联动，限制或禁止用户使用特定应用服务，从而保护移动网络免受不安全服务带来的安全风险；通过向 SCA 110 发送 CRS 控制指令，来协助终端侧完成自动安全更新服务。

在 SCS 120 中设有 SCS 数据库 SDB （图未示），保存用户的安全联动信息以及选择服务描述等，是 CRS 提供安全联动服务所必须固定的用户信息，以及一些动态的用户安全状态、服务情况等信息。

NAC 131 对执行安全策略中的网络接入控制策略，移动台进行基于流量控制等手段的网络接入控制，包括流量的限制、阻断、重定向等。ASC 132 执行安全策略中的服务接入控制策略，移动台进行基于应用层的服务接入控制。为了节约网络资源，在终端侧的 SCA 可以与移动台相互配合，保证

终端用户不能发起已经被禁用的服务。

CRS 通过 CRS 服务接口与外部组件进行通信，CRS 服务接口包括终端侧 SCA 的外部接口和网络侧 SCS 的外部接口。也就是说，SCA 110 和 SCS 120 不仅在 CRS 内部通信，还可以通过各种 CRS 服务接口接收来自外部组件的安全信息，并通过 CRS 联动过程，遵从网络的安全策略，共同实现移动台网络接入控制和服务接入控制等 CRS 功能。

其中，SCA 110 通过终端侧 SCA 的外部接口与终端侧的安全应用软件（Security Application Software，SAS）140、移动台操作系统（Mobile Station Operating System，MSOS）150 之间通过定义的接口进行信息的双向传递。例如，SCA 110 可以利用所述接口收集移动台的安全相关信息（Security Correlative Information，SCI）。

SCS 120 通过网络侧 SCS 的外部接口与 SAS-S（Security Application Software Server，安全应用软件服务器）以及 MSOS-US（Mobile Station Operating System Update Server，移动台操作系统更新服务器）相连。

此外，SCS 120 还与外部网络的 ASP（Application Service Provider，应用服务提供商）160 连接通信。所述 ASP 160 包括 MSOS-US 和 SAS-S 以及其它的服务资源等。

在终端侧，CRS 为用户提供的自动安全更新服务主要包括终端安全状态报告和终端安全环境增强等。

终端安全状态报告是 SCA 根据从终端侧收集到的安全相关信息和从 SCS 返回的终端安全等级评估结果自动生成的，供用户主动查询。

终端安全环境增强是指当 CRS 发现移动台存在不安全因素时，控制移动台自动完成安全更新过程。终端安全环境增强的完成不仅需要 SCA 和 SCS 的共同参与，而且还需要 CRS 与终端侧和网络侧的相关系统一起进行联动。终端安全环境增强可以减少移动台所受的安全威胁，通过保护移动台、限制移动台对网络的访问来保护移动网络免受不安全终端带来的安全威胁，避免移动台无意中被病毒当作实施其他攻击的跳板，同时保证网络能够提供给用户可靠的服务质量，及时停止病毒或误操作带来的非预期消费，保护消费者利益。

SCA 对移动台的安全状态报告和安全环境增强，一般都是当 CRS 发现移动台存在不安全因素时启动的，具体包括:

（1）自动完成移动台 SCA 的发现、安装和升级

在用户完成第一次到网络的注册过程后，如果移动台的SCA已经启动，则 SCA 发起初始化过程，同时完成 SCA 向 SCS 的注册过程；如果终端侧 SCA 没有启动或没有安装，但移动台提供对 CRS 功能的支持，则网络侧通知 SCS，通过 SCS 提供 SCA 下载软件的地址信息或发出 SCA 使能指示，自动完成 SCA 的安装和启动。SCA 的安装，可能需要由运营商网络侧提供下行信道承载，并以适当方式提示安装或启动。

当 SCS 发现 SCA 版本需要更新时，通过告知 SCA 更新的下载资源地址和更新紧急程度的方式进行自动更新。也就是说，当网络侧发现移动台存在安全隐患时，可以控制移动台完成自动安全更新，对安全隐患进行修复。CRS 系统提供自动安全更新功能时，大多数的 CRS 过程是自动进行的，一般不需要终端用户的参与和确认，保证移动台进行自动安全更新。

（2）自动修复不安全移动台

SCA 通过 CRS 服务接口，主动或被动收集移动台的安全环境信息，上报网络侧 SCS。SCS 根据总体安全策略，以及该用户安全服务等级信息和 SDB 中存储的用户的其他安全信息和用户的其他定制服务信息，检查和判断是否有与安全策略不匹配的不安全因素。如果发现移动台存在不安全因素，例如病毒库需要升级，病毒软件版本需要更新等，则通知 SCA。同时，如果有必要，例如必须由防病毒软件开发商的软件服务器发起更新过程时，SCS 自动通知防病毒软件开发商或终端系统开发商服务器，告知相关信息或指令，控制终端 MSOS/SAS-A 与远程安全应用服务器、操作系统服务器进行交互，进行进一步的自动安全更新和修复过程。

SCS 对移动台存在的不安全因素评估后，如果有必要，将根据安全策略与 NAC 和 ASC 联动，对移动台进行网络接入控制和服务控制。

此外，当 CRS 系统不清楚移动台的安全状况或者发生安全事件时，例如移动台可能或者已经感染病毒时，CRS 系统对移动台数据流量进行一定的安全处理，使得网络的安全性通过不影响用户的安全技术手段来实施，

例如通过网络的防病毒网关，将用户数据包中的不安全内容过滤后再转发出去。

对于在上述过程中引起的用户业务受限信息或者不可用信息，CRS 系统要通知用户，必要时提供进一步的引导服务。如果用户主动查询，还需要提供相关安全服务的结果和相关安全信息。用户可以忽略或禁止所有提供给用户的移动台安全状态报告信息，以免打扰用户。

在网络资源有限的情况下，移动台的自动更新可能会受到影响，SCA 或 SCS 会根据用户定购的安全服务等级，逐步完成自动安全升级任务，优先保证高安全服务等级的移动台完成安全更新。

需要说明的是，对于必须进行的用户移动台安全更新过程，例如杀毒软件升级或安装漏洞补丁，通过安全策略设置，可以不依赖网络资源的占用情况，在网络侧设定的时段进行。

需要注意的是，CRS 在终端侧提供的服务，一般必须在 SCA 使能时才有效。

对于终端侧引起的安全更新失败，SCA 会自动保存状态信息，启动异常定时器，通过定时器再次触发安全更新过程；对于网络资源或其他网络问题引起的更新失败，则由 SCS 根据移动台的安全状态，评估后临时调整安全策略并自动实施，以避免更大的安全风险。异常处理都会进行日志保存，通过一个 CRS 管理界面，由管理员进行进一步的检查和处理。

（3）网络侧管理员禁用 CRS 功能

该功能由 CRS 系统提供，在网络侧，管理员可以设定个别移动台不受 CRS 系统的限制，但是不推荐使用这种功能。

在本发明中，可以有多个实施方式来实现自动安全更新，但都以移动台或网络的软件/硬件自动更新为原则，尽可能减少用户在维护网络安全方面的参与。

本发明的一种具体应用是实现 SCA 的自动下载安装，NAC 自动探测移动台上是否安装 SCA，如移动台未安装 SCA，则协助移动台下载安装，并为移动台上的 SCA 提供必要的初始化配置信息。此种情况下，移动台已经通过无线网络的用户验证，并且完成与数据网络的连接过程，在 NAC 和

SCS 之间已经存在安全信息传送通道。

请参阅图 3，本发明的实施例中提供的 NAC 探测移动台是否需要安装 SCA 的流程包括:

步骤 S31，NAC 向移动台发送 SCA 探测请求消息(SCA Probe Request)。

探测请求消息中包括 SCS 的域名、访问点名、IP 地址、服务端口等 SCA 需要的初始化配置信息。探测请求消息的具体内容由 SCS 配置，并通过 SCS 和 NAC 之间的安全通道加密传输，作为控制信息预先下发给 NAC。

探测请求消息的发送策略，例如探测请求消息的发送间隔、发送次数、无反馈的超时定时器时间设置等，也可以由 SCS 预先下发给 NAC。发送策略可以由 NAC 自主决定何时更新（定期更新或者按需要更新）、可以由 SCS 主动更新或者由 NAC 和 SCS 之间协商确认更新方式。

探测请求消息的目的地址，可以是移动台的 IP 单播地址，或者是特定的组播地址（SCA 组）。当 NAC 需要同时向大量的移动台发送相同的探测请求时可以采取组播方式，能够降低 NAC 的负荷和网络的带宽消耗，例如当大量的移动台通过 NAC 同时启动数据网络连接进行数据网络访问时。组播发送的探测请求消息中可以设置需要哪些 SCA 响应，例如需要所有的 SCA 响应或者需要连接到数据网络后从未发送过响应消息的 SCA 响应等。当很少的移动台同时启动数据网络连接，或者某些移动台用户需要区别对待时，NAC 可以采取单播方式发送探测请求消息。

步骤 S32，如果移动台上没有安装 SCA，或者 SCA 因软件损坏等原因而无法正常工作时，移动台将无法对 NAC 的探测请求消息进行应答。则此时需要移动台安装 SCA。

具体地，NAC 侧可以设置超时定时器，如果 NAC 在超时定时器的定时内没有收到移动台返回的应答，则判断移动台需要安装 SCA。

作为本发明的另一个实施例，NAC 侧进一步设置探测请求消息发送门限，如果 NAC 在超时定时器的定时内没有收到移动台返回的应答，NAC 重复向移动台发送探测请求消息，如果 NAC 在超时定时器的定时内没有收到移动台返回的应答，且发送的探测请求消息数目超过探测请求消息发送门限时，判决移动台需要安装 SCA。

步骤 S33，如果 NAC 判决移动台需要安装 SCA，则触发移动台执行 SCA 下载安装流程。

步骤 S34，如果移动台已经安装有 SCA 并能正常工作，则 SCA 提取并保存 NAC 发送的探测请求消息中包含的 SCS 域名、访问点名、 IP 地址、服务端口等初始化配置信息。

步骤 S35，SCA 向 NAC 发送探测响应消息（SCA Probe Response）。

探测响应消息中包含有不需要安装 SCA 的通知信息，还可以包含 SCA ID（标识）、SCA IP 地址等信息，探测响应消息的具体内容可以由 NAC 在探测请求消息中要求，或者由 SCA 根据默认的策略决定。

如步骤 S33 所述，当 NAC 已经检测到移动台需要安装 SCA 时，则触发移动台执行 SCA 自动安装过程。需要说明的是，移动台是否需要安装 SCA 由 NAC 进行探测并决定，但是移动台执行 SCA 自动安装是由移动台向某个 ASP 发送数据服务请求时触发的。

请参阅图 4，本发明提供的一个实施例中移动台安装 SCA 的实现流程包括:

步骤 S41，当 NAC 判决移动台需要安装 SCA 时，向移动台发送移动台操作系统类型探测请求（MSOS Probe Request），探测移动台操作系统/平台的类型。

一般可以在移动台特定的端口上请求特定的信息，通过反馈信息来获知移动台的操作系统/平台的类型、共享资源等信息。NAC 可以同时通过多个端口向移动台发送移动台操作系统类型探测请求，然后侦听相应端口的响应信息。

步骤 S42，移动台向 NAC 返回移动台操作系统类型探测应答（MSOS Probe Response），携带移动台的操作系统类型等信息。

步骤 S43，NAC 根据移动台的操作系统类型等信息，判断移动台需要下载安装的 SCA 的下载地址。

步骤 S44，NAC 收到移动台向 ASP 发起的数据服务请求，当 NAC 收到移动台向 ASP 发起数据服务请求时，数据服务请求需要经过 NAC 转发。

步骤 S45，NAC 将移动台的数据服务请求重定向到 SCA 的下载地址。

步骤 S46，移动台根据 SCA 的下载地址登陆相关服务器，下载与自身操作系统类型对应的 SCA。

步骤 S47，移动台安装 SCA。

作为本发明的一个实施例，在上述过程中，当 SCA 是用跨平台技术开发的终端软件形式时，例如采用 Java 语言开发时，NAC 可以不需要向移动台发送操作系统类型探测请求获取移动台的操作系统类型信息，即上述步骤 S41、S42、S43 可以省略。

在上述过程中，移动台可能在完成 SCA 下载前向 ASP 请求服务，此时数据服务请求经过 NAC 转发。由于 SCA 安装未完成，NAC 无法获取 SCA 上报的移动台的安全相关信息，从而难以确定移动台的安全状态，移动台发出的数据服务请求可能会对网络带来安全威胁。因此，NAC 对移动台的数据服务请求进行相应的安全处理，例如全部丢弃、有选择的放行、重定向到专用安全设备，例如防病毒网关等处理，具体可以由 NAC 配置、也可以由 SCS 配置下发给 NAC 执行，或者由 NAC 和 SCS 之间协商确定等。

作为本发明另外一个实施例，NAC 也可以不对移动台操作系统/平台的类型进行探测，当移动台向 ASP 发起数据服务请求时，NAC 将数据服务请求重定向到 SCA 的下载地址，由移动台用户手工选择下载安装适合移动台操作系统类型的 SCA 或者由 SCA 的安装下载服务器通过移动台的连接信息来判断移动台的操作系统/平台的类型，从而决定移动台需要下载哪个合适的 SCA 软件。

上述的实施例是由 NAC 完成对移动台是否需安装 SCA 的探测。当然也可以由其他的网络侧设备，例如 SCS 完成对移动台的探测。请参阅图 5，本发明的实施例中提供的由 SCS 探测移动台是否需要安装 SCA 的流程包括:

步骤 S51，移动台用户连接到数据网以后，NAC 向 SCS 发送移动台连接报告（MS Connect Report）。

移动台连接报告包含移动台的 IP 地址、User ID 等信息。

此外，NAC 开放移动台到 SCS 的访问权限。

步骤 S52，SCS 向 NAC 确认收到有效的移动台连接报告。

步骤 S53，SCS 向移动台发送 SCA 探测请求消息（SCA Probe Request），要求移动台上的 SCA 向 SCS 汇报移动台的安全状况。

SCA 探测请求消息中可以包含 SCS 的 IP 地址和服务端口，作为 SCA 和 SCS 间通讯的初始化信息。

如果移动台上没有安装 SCA，或者 SCA 因软件损坏等原因而无法正常工作时，移动台将无法对 SCS 的 SCA 探测请求消息进行应答。此时 SCS 确定移动台需要安装 SCA，进入步骤 S54。

具体地，SCS 侧可以设置超时定时器，如果 SCS 在定时器的定时内没有收到移动台的响应，则判断移动台需要安装 SCA。

作为本发明的另一个实施例，SCS 进一步设置 SCA 探测请求消息发送门限，如果 SCS 在超时定时器的定时内没有收到移动台返回的应答，SCS 重复向移动台发送探测请求消息，如果 SCS 在超时定时器的定时内没有收到移动台返回的应答，且发送的 SCA probe request 请求消息数目超过探测请求消息发送门限时，判决移动台需要安装 SCA。

步骤 S54，SCS 通知 NAC 移动台需要安装 SCA，具体可以是发送移动台连接响应 A 类消息（MS Connect Response A）给 NAC。

移动台连接响应 A 类消息可以包含移动台 IP 地址、移动台 User ID 等信息。

步骤 S55，SCA 启动 SCA 的自动安装过程，实现 SCA 的自动安装。

如果移动台上已经安装 SCA 并能正常工作，则进入步骤 S56，SCA 向 SCS 反馈 SCA 探测响应信息。

SCA 探测响应消息包含 SCA ID、User ID、移动台 IP 地址等信息，向 SCS 证明移动台上已经安装 SCA 并能正常工作。

如步骤 S55 所述，SCS 检测到移动台需要安装 SCA 后，通知 NAC，则将会开始 SCA 自动安装过程。移动台是否需要安装 SCA 由 SCS 进行探测并决定，但是 SCA 自动安装过程是通过移动台向某个 ASP 发送服务请求触发的。

请参阅图 6，本发明的一个实施例中移动台的 SCA 自动安装流程包括：

步骤 S61，NAC 收到移动台向 ASP 发起的数据服务请求。

步骤 S62，在 NAC 未收到来自 SCS 的移动台需要安装 SCA 的通知时，对于步骤 S61 收到的数据服务请求，按照默认策略处理。

因为此种情形下，网络侧还不清楚移动台的安全状态，移动台发出的数据报文可能会对网络带来安全威胁。因此，NAC 对这些报文的处理策略可以是全部放行、全部丢弃、按照某些原则有选择的放行、重定向到专用安全设备（如防病毒网关等等）检查处理等等，具体策略由 SCS 制定并下发给 NAC 执行，具体的策略是和用户相关的，每个用户之间可能不同。

步骤 S63，NAC 收到来自 SCS 的移动台需要安装 SCA 的通知，NAC 开始针对移动台执行重定向措施。

步骤 S64，移动台继续向 ASP 发起数据服务请求。

步骤 S65，NAC 将移动台的数据服务请求重定向到 SCA 的下载服务器（Servers）。

步骤 S66，移动台连接到 SCA 的下载服务器。所述连接可以但不限于是 HTTP 类型的。

步骤 S67，下载服务器根据移动台与自己连接过程中传递过来的参数判断移动台需要下载的 SCA。参数可以是操作系统类型等信息。

步骤 S68，移动台下载 SCA。

步骤 S69，移动台安装 SCA。

需要说明的是，步骤 S62 是在 NAC 未收到来自 SCS 的移动台需要安装 SCA 的通知，且无法评估移动台的安全状态时才会进行。

本发明的另一种具体应用是实现安全相关信息 SCI 的更新、安全策略的自动安全更新等。在本发明的实施例中，SCA 根据内置的或 SCS 下发的策略，收集整理移动台的安全相关信息 SCI，并生成安全相关信息报告上报给 SCS。SCS 获取移动台的 SCI 后，可以与移动台用户的接入控制策略、服务控制策略等信息进行关联分析，评估移动台的安全情况，更新移动台的接入控制策略和服务控制策略。并且，SCA 可以根据移动台的 SCI 和 SCS 对 SCI 的关联分析结果，为用户生成终端安全状态报告。

移动台的SCI可以用于SCS确定移动台的安全状况，SCS将移动台的SCI存储在SDB中。移动台的SCI主要包括以下信息:

1、报告序列号

报告序列号是一个渐增的正整数，用于标识移动台的一次数据网络连接会话过程中各个SCI报告的先后顺序。SCS可以利用报告序列号来识别SCI报告是否发生了重传、丢失、乱序，报告序列号为SCI报告中的可选项。

2、SCA ID

SCA ID用来在移动台中唯一标识一个已安装的SCA。SCA ID用来标识SCS服务器的SCI响应消息应该发给哪个SCA，如果SCA从SCS服务器收到了一条消息，但其中的SCA ID和自己的不符，SCA就认为发生了错误，丢弃这个消息并向SCS服务器发送错误通知。

3、移动台ID

移动台ID用来唯一的标识一个移动终端的硬件设备。

4、SCS ID

SCS ID用来唯一的标识一个SCS服务器，如果SCS服务器收到一个SCI报告，其中的SCS ID和自身的不符，则丢弃此报文。

5、移动台的用户身份信息

移动台的用户身份信息用于SCS对移动用户进行区分。

6、报告主体，包含以下内容:

（1）移动台操作系统/平台的类型信息，移动台操作系统的漏洞、补丁信息;

（2）移动台操作系统安全日志、告警信息;

（3）移动台的安全软件安装信息，例如是否安装了反病毒软件或者防火墙软件等;

（4）移动台安全软件的版本、数据库日期、病毒扫描策略、更新病毒库后是否进行过全面扫描以及病毒发现情况等信息;

（6）SCA向SCS上报安全相关信息报告（SCI Report）的策略，例如SCA定期向SCS发送安全相关信息报告、SCS主动查询安全相关信息报告

或者移动台的事件触发上报安全相关信息报告等，例如终端反病毒软件发现病毒、终端防火墙检测到对终端的网络攻击等。

本发明实施例中的 SCI 更新过程发生在安全信息传送通道建立过程之后，SCI 报告、响应信息和安全控制策略更新请求、响应信息在安全的信息传送通道中加密传输，以保证信息的一致性、完整性和不可抵赖性。

图 7 示出了本发明实施例提供的自动更新的实现流程。

步骤 S71、SCA 通过与移动台的 MSOS 以及 SAS 等软件的接口实时收集移动台安全相关信息，例如移动台操作系统的漏洞/补丁信息、移动台操作系统安全日志和告警信息、移动台安全软件的版本和数据库日期、移动台用户身份或者 SCA 向 SCS 发送的 SCI Report 的策略等信息。

步骤 S72、SCA 对收集到的移动台安全相关信息进行初步整理和过滤，并按照 SCS 规定的安全报告策略，选择相应的发送内容和合适的发送时机上报给 SCS。SCA 保存移动台最新的 SCI、最近几次 SCI Report 中发送的信息内容、安全报告策略或者从 SCS 接收到的安全相关信息响应（SCI Response）等信息。

作为本发明的一个实施例，SCA 可以每次将收集到的移动台的全部 SCI 上报给 SCS。

作为本发明的另一个实施例，SCA 不需要每次都把收集到的全部安全相关信息发送给 SCS，而是按照 SCS 制定的安全报告策略进行发送。安全报告策略由 SCS 制定并下发给 SCA，例如 SCA 可以只发送两次 SCI Report 之间的发生变化的信息。作为一个实施例，SCA 在用户通过认证连接到数据网络后，第一次发送的 SCI Report 中需要包含全部的 SCI 信息，以后的 SCI Report 按照安全报告策略只需发送 SCI 的更新信息或者仅发送对上一次 SCS 返回的 SCI Response 的执行结果的反馈信息。

步骤 S73、当到达安全报告策略规定的发送时机时，SCA 选择相应的内容通过安全信息传送通道向 SCS 发送 SCI Report。SCI Report 的内容除了移动台的相关 SCI 外，还可以包含消息序列号、SCA ID 或 SCS ID 等信息。SCA ID、消息序列号和 SCS ID 用于唯一标识一条 SCI Report 消息，

SCS 利用这些信息可以识别是否是重复的信息、两次接收到的 SCI Report 中是否有 SCI 信息丢失，以及 SCS 是否是合法的接收端等。

步骤 S74、SCS 收到 SCI Report 后，对其中的 SCI 进行有效性检查，确认其是否正确、有效，并按照安全策略进行关联分析。例如 SCS 可以将 SCI Report 中的相关信息与本地 SDB 中存储的信息进行比对，例如 SCA ID、消息序列号、SCS ID 等是否正确有效，SCS ID 是否准确等。

关联分析包括单用户各类信息的关联分析和多用户相似信息的关联分析，分别分析一个移动台和一个网内多个移动台的安全情况，从而分析网络整体安全状态。安全策略由系统预先定义并存储在 SCS 的 SDB 中。

步骤 S75、SCS 根据移动台的 SCI 和关联分析结果与 SCS 存储在 SDB 中的 SCI 信息进行比对，对 SDB 进行更新，以保持 SDB 中存储移动台最新的 SCI。

步骤 S76、SCS 根据关联分析结果，确定是否对移动台的网络接入控制策略或应用服务控制策略进行更新。如果不需要更新，就直接转到步骤 S79；如果需要更新，转到步骤 S77。

步骤 S77、移动台的网络接入控制或应用服务控制策略，则 SCS 通过安全信息传送通道向 NAC 或 ASC 发送安全控制策略更新请求，携带被控制的移动台的 SCA ID、用户 ID 以及更新后的安全控制策略信息等信息。安全控制策略更新请求通过 SCS 和 NAC/ASC 之间的安全信息传送通道中加密传输，该安全信息传送通道可以利用现有的安全机制，例如传输层安全协议（Transport Layer Security，TLS）、通用开放策略服务协议（Common Open Policy Service Protocol，COPS）等，也可以是 CRS 自建的安全机制。

步骤 S78、NAC 或 ASC 通过安全信息传送通道向 SCS 返回安全控制策略更新响应，反馈移动台的安全控制策略的更新结果情况。

步骤 S79、SCS 根据关联分析结果和安全控制策略的更新情况，选择向 SCA 反馈的 SCI Response 的内容。

作为本发明的一个实施例，SCS 也可以不在每次收到 SCA 上报的 SCI Report 后都向 SCA 发送 SCI Response，例如 SCA 定期向 SCS 上报 SCI Report，且 SCS 进行关联分析后认为不需要进行安全控制策略更新和软件

更新，此时 SCS 可选择发送一个 SCI Response 来响应 SCA 上报的几个 SCI Report。

步骤 S710、SCS 通过安全信息传送通道向 SCA 发送 SCI Response，携带 SCS 对 SCA 反馈的安全控制信息，例如移动台操作系统需要安装的补丁及其下载地址、移动台安全软件的升级地址、SCS 对 SCA 的安全策略要求（包含 SCA 向 SCS 上报 SCI Report 的安全报告策略）或者移动台的安全控制策略更新信息等。

对于终端操作系统、SCA 以及安全应用软件等软件的升级更新，SCS 针对升级更新的不同安全级别可以定义各种策略，例如立即安装更新，安装更新前取消或者限制网络访问或者服务访问权限；在某一个特定时间点或者时间段之前安装更新，否则逾期将取消或者限制网络访问或者服务访问权限等。上述两种情况中，移动台访问更新相关的升级服务器的权限一直存在。

作为本发明的一个实施例，SCA 可以依据收集的移动台的 SCI 和 SCS 向 SCA 返回的 SCI Response 消息的内容生成移动台安全状态报告，供移动台用户查询，并可在 SCI 更新过程中，向用户提供相应的安全提示信息，例如在安装 SCA 过程中，给用户提示许可协议信息，当用户的网络访问或者服务访问被限制、取消或者重新开通时，向用户提示相关信息等。

作为本发明的一个实施例，在上述过程结束后，移动台可以按照 SCI Response 消息中的内容或者指示，发起 SCA 软件或者其他安全应用软件、移动台操作系统的更新，例如 SCA 从 SCS 的 SCI Response 中，获取需要更新的软件内容，以及更新内容的地址，从而进行相应的软件更新。软件更新完成后，则可能还需要再重复一次或者多次上述 SCI 更新流程，以便 SCS 更新移动台的接入控制、服务控制或者确认软件更新的效果，此时 SCA 向 SCS 上报的 SCI Report 中所包含的内容可以仅仅是 SCA 和 SCS 之间关于软件更新效果的确认信息。

如图 8 所示，本发明提供的关联响应系统的另一实施例包括网络侧和移动台。

所述的网络侧包括第一消息发送接收模块 811 和判断模块 812，所述

的第一消息发送接收模块 811 用于向所述的移动台发送安全关联代理探测请求消息，并用于接收所述的移动台发送的探测响应消息；所述的判断模块 812 用于根据所述的探测响应消息判断所述的移动台是否应安装安全关联代理；

所述的移动台包括第二消息发送接收模块 821，用于接收所述的安全关联代理探测请求消息，并向所述的网络侧发送探测响应消息。

所述的移动台还包括下载安装模块 822，用于当所述的判断模块判断所述的移动台需要安装安全关联代理时，下载并安装所述的安全关联代理。

其中，所述的网络侧的第一消息发送接收模块 811 和判断模块 812 可以在网络接入控制器内或安全关联服务器内。

本发明的关联响应系统可以应用于各种移动网络，例如 GSM、CDMA、WCDMA（Wideband Code Division Multiple Access，宽带码分多址）TD-SCDMA，CDMA2000 或者 WLAN 等，移动台可以是通过空中接口与移动网络连接通信移动电话或 PDA（Personal Digital Assistant，个人数字助理）等。

以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，凡在本发明的精神和原则之内所作的任何修改、等同替换和改进等，均应包含在本发明的保护范围之内。

权 利 要 求

1、一种实现移动台安全更新的方法，其特征在于，包括:

关联响应系统中的实体与移动台进行信息交互;

当根据所述信息交互确认需要安全更新时，所述关联响应系统的网络侧向移动台下发安全更新控制信息;

根据所述安全更新控制信息完成移动台的自动安全更新。

2、根据权利要求 1 所述的方法，其特征在于，所述关联响应系统与移动台进行信息交互为：关联响应系统的网络接入控制器向移动台发送安全关联代理探测请求消息，该消息中携带安全关联代理的初始化配置信息;

所述当根据所述信息交互确认需要安全更新时，所述网络侧向移动台下发安全更新控制信息为：如果移动台未响应所述探测请求消息，则判定移动台需要安装安全关联代理；所述网络接入控制器触发移动台启动安全关联代理的下载安装;

所述完成移动台的自动安全更新为：将安全关联代理下载并安装到移动台。

3、根据权利要求 2 所述的方法，其特征在于，所述移动台未响应所述探测请求消息包括：所述网络接入控制器在定时内未收到移动台的探测响应，或者网络接入控制器发送安全关联代理探测请求消息的次数超过设定门限。

4、根据权利要求 2 所述的方法，其特征在于，还包括：当移动台安装有安全关联代理且工作正常时，移动台的安全关联代理提取并保存所述安全关联代理探测请求消息中的初始化配置信息，并向网络接入控制器返回安全关联代理探测响应消息。

5、根据权利要求 4 所述的方法，其特征在于，所述安全关联代理探测响应消息中包含移动台不需要安装安全关联代理的通知信息、安全关联代理的标识和/或 IP 地址信息。

6、根据权利要求 1 所述的方法，其特征在于，所述关联响应系统与移

动台进行信息交互为：关联响应系统的安全关联服务器向移动台发送安全关联代理探测请求消息，该消息中携带安全关联代理的初始化配置信息；

所述当根据所述信息交互确认需要安全更新时，所述网络侧向移动台下发安全更新控制信息为：如果移动台未响应所述探测请求消息，则判定移动台需要安装安全关联代理；所述安全关联服务器触发移动台的下载安装操作；

所述完成终端的自动安全更新为：将安全关联代理下载安装到移动台。

7、根据权利要求 6 所述的方法，其特征在于，所述移动台未响应所述探测请求消息包括：所述安全关联服务器在定时内未收到移动台的探测响应，和/或安全关联服务器发送安全关联代理探测请求消息的次数超过设定门限。

8、根据权利要求 6 所述的方法，其特征在于，所述关联响应系统的安全关联服务器向移动台发送安全关联代理探测请求消息之前，还包括：关联响应系统的网络接入控制器向安全关联服务器发送移动台连接报告。

9、根据权利要求 8 所述的方法，其特征在于，在所述判定移动台需要安装安全关联代理时，安全关联服务器发送移动台连接响应 A 类消息给网络接入控制器，通知网络接入器所述移动台需要安装安全关联代理。

10、根据权利要求 6 所述的方法，其特征在于，还包括：当移动台安装有安全关联代理且工作正常时，移动台的安全关联代理提取并保存所述安全关联代理探测请求消息中的初始化配置信息，并向安全关联服务器返回安全关联代理探测响应消息。

11、根据权利要求 10 所述的方法，其特征在于，所述安全关联代理探测响应消息中包含移动台不需要安装安全关联代理的通知信息、安全关联代理的标识和/或 IP 地址信息。

12、根据权利要求 2 至 11 任一项所述的方法，其特征在于，所述将安全关联代理下载并安装到移动台，包括：

所述关联响应系统的网络接入控制器接收移动台的数据服务请求，将所述数据服务请求重定向到安全关联代理的下载地址；

移动台根据所述安全关联代理的下载地址下载安装对应的安全关联代理。

13、根据权利要求 12 所述的方法，其特征在于，所述安全关联代理的下载地址是由网络接入控制器确定的，包括:

所述网络接入控制器向移动台发送操作系统类型探测请求消息，请求获取移动台的操作系统/平台类型信息;

所述移动台向网络接入控制器返回操作系统类型探测响应消息，消息携带移动台的操作系统/平台类型信息;

所述网络接入控制器根据移动台的操作系统/平台类型信息确定与所述操作系统/平台类型信息对应的安全关联代理的下载地址。

14、根据权利要求 12 所述的方法，其特征在于，所述下载地址对应提供安全关联代理的下载服务器;

所述下载服务器根据与移动台连接过程中传递的参数判断移动台需要下载的安全关联代理。

15、根据权利要求 12 所述的方法，其特征在于，所述关联响应系统的网络接入控制器接收移动台的数据服务请求时，如果移动台尚未完成安全关联代理的下载或者网络接入控制器尚未获悉移动台需要安装安全关联代理，则网络接入控制器对移动台的数据服务请求进行安全处理。

16、如权利要求 2 至 11 任一项所述的方法，其特征在于，所述安全关联代理探测请求消息的目的地址为移动台的 IP 单播地址或者组播地址; 所述初始化配置信息包括安全关联服务器的 IP 地址或服务端口。

17、根据权利要求 1 所述的方法，其特征在于，所述关联响应系统与移动台进行信息交互为: 网络侧向移动台发送安全关联代理探测请求消息;

所述当根据所述信息交互确认需要安全更新时，所述网络侧向移动台下发安全更新控制信息为: 如果移动台未响应所述探测请求消息，则判定移动台需要安装安全关联代理; 所述网络侧触发移动台启动安全关联代理的下载安装;

所述完成移动台的自动安全更新为: 将安全关联代理下载并安装到移

动台。

18、根据权利要求 1 所述的方法，其特征在于，所述关联响应系统与移动台进行信息交互为：位于终端侧的关联响应系统的安全关联代理收集移动台的安全相关信息，上报给关联响应系统的安全关联服务器；

所述当根据所述信息交互确认需要安全更新时，所述网络侧向移动台下发安全更新控制信息为：所述安全关联服务器分析安全关联代理上报的安全相关信息，在需要时向安全关联代理返回安全相关信息响应；

所述完成终端的自动安全更新为：所述安全关联代理保存所述安全相关信息响应。

19、根据权利要求 18 所述的方法，其特征在于，所述位于终端侧的关联响应系统的安全关联代理收集移动台的安全相关信息，包括：

所述安全关联代理通过移动台的软件接口收集移动台的安全相关信息；

所述安全关联代理整理所述安全相关信息，选择向安全关联服务器上报的信息内容；

所述上报给关联响应系统的安全关联服务器为：所述安全关联代理通过与安全关联服务器之间的安全信息传送通道向安全关联服务器发送安全相关信息报告，携带所述选择后的信息内容。

20、根据权利要求 19 所述的方法，其特征在于，所述选择向安全关联服务器上报的信息内容为：安全关联代理选择其收集的移动台的安全相关信息的全部信息或者部分信息。

21、根据权利要求 19 所述的方法，其特征在于，所述发送安全相关信息报告的步骤为定期的、或者是由移动台的安全事件触发的，或者由安全关联服务器主动查询触发的。

22、根据权利要求 19 所述的方法，其特征在于，所述安全相关信息报告还包含可选的安全相关信息报告消息序列号、安全关联代理标识、安全关联服务器标识。

23、根据权利要求 18 所述的方法，其特征在于，所述安全关联服务器

分析安全关联代理上报的安全相关信息，在需要时向安全关联代理返回安全相关信息响应为：

所述安全关联服务器对安全关联代理上报的安全相关信息进行有效性检查；对所述安全相关信息进行关联分析；根据所述关联分析的结果更新本地保存的移动台的安全相关信息；

所述安全关联服务器根据所述关联分析的结果通过与安全关联代理之间的安全信息传送通道向安全关联代理返回安全相关信息响应，携带安全关联服务器向安全关联代理反馈的安全控制信息和移动台安全等级评估结果。

24、根据权利要求 23 所述的方法，其特征在于，所述关联分析为单用户信息关联分析和多用户相似信息的关联分析。

25、根据权利要求 23 所述的方法，其特征在于，在根据所述关联分析的结果更新本地保存的移动台的安全相关信息之后，还包括：

所述安全关联服务器根据所述关联分析的结果判断是否更新移动台的安全控制策略，是则通过与网络接入控制器或者应用服务控制器之间的安全信息传送通道向网络接入控制器或者应用服务控制器发送安全控制策略更新请求，携带安全关联代理标识、用户标识以及更新后的安全控制策略信息；

所述网络接入控制器或者应用服务控制器通过所述安全信息传送通道向安全关联服务器返回安全控制策略更新响应，通知安全关联服务器移动台的安全控制策略更新结果。

26、根据权利要求 25 所述的方法，其特征在于，所述安全关联服务器向安全关联代理反馈的安全控制信息中包含有移动台的安全控制策略更新信息。

27、根据权利要求 18 所述的方法，其特征在于，还包括：所述安全关联代理保存移动台最新的安全相关信息、安全相关信息报告内容、安全相关信息报告策略。

28、根据权利要求 18 所述的方法，其特征在于，还包括：安全关联代理根据收集的移动台的安全相关信息和安全关联服务器返回的安全相关信

息响应生成移动台安全状况评估报告或安全提示信息。

29、根据权利要求 18 所述的方法，其特征在于，还包括：所述安全关联代理根据安全关联服务器返回的安全相关信息响应更新移动台的安全应用软件或者给操作系统/平台打补丁。

30、根据权利要求 1 所述的方法，其特征在于，所述关联响应系统与移动台进行信息交互为：位于终端侧的关联响应系统的安全关联代理收集移动台的安全相关信息，上报给关联响应系统的安全关联服务器；

所述当根据所述信息交互确认需要安全更新时，所述网络侧向移动台下发安全更新控制信息为：所述安全关联服务器分析安全关联代理上报的安全相关信息，在所述移动台存在不安全因素时，向安全关联代理返回控制信息；

所述完成终端的自动安全更新包括：所述安全关联代理根据所述控制信息协助移动台修复不安全因素。

31、根据权利要求 30 所述的方法，其特征在于，所述完成终端的自动安全更新在网络侧设定的时段进行。

32、根据权利要求所述的方法，其特征在于，所述关联响应系统与移动台进行信息交互为：位于终端侧的关联响应系统的安全关联代理收集移动台的安全相关信息，上报给关联响应系统的安全关联服务器；

所述当根据所述信息交互确认需要安全更新时，所述网络侧向移动台下发安全更新控制信息为：所述安全关联服务器分析安全关联代理上报的安全相关信息，在所述移动台的安全关联代理需要更新时，向安全关联代理返回控制信息；

所述完成终端的自动安全更新包括：所述移动台从安全关联服务器下载软件，实现安全关联代理的自动更新。

33、根据权利要求 30 至 32 任一项所述的方法，其特征在于，还包括：在移动台自动安全更新而造成用户的服务受限时，安全关联代理将服务受限信息通知用户。

34、根据权利要求 1 所述的方法，其特征在于，所述关联响应系统与

移动台进行信息交互为：当移动台注册到网络后，如果终端侧的安全关联代理已经启动，则所述安全关联代理向安全关联服务器注册；

所述当根据所述信息交互确认需要安全更新时，所述网络侧向移动台下发安全更新控制信息为：如果安全关联代理没有启动或没有安装，则安全关联服务器提供下载安全关联代理所需的信息或发出安全关联代理使能指示；

所述完成终端的自动安全更新包括：将安全关联代理下载安装到移动台。

35、一种关联响应系统，与移动台进行信息交互，包括网络侧的安全关联服务器、与安全关联服务器相连的网络接入控制器和应用服务控制器，其特征在于：所述关联响应系统的安全关联服务器或网络接入控制器在根据所述信息交互确认需要安全更新时，向移动台下发安全更新控制信息；根据所述安全更新控制信息协助移动台实现自动安全更新。

36、根据权利要求 35 所述的系统，其特征在于，所述网络接入控制器用于向移动台发送安全关联代理探测请求消息，该消息中携带安全关联代理的初始化配置信息；如果移动台未响应所述探测请求消息，则判定移动台需要安装安全关联代理；触发移动台启动安全关联代理的下载安装。

37、根据权利要求 36 所述的系统，其特征在于，还包括位于移动台侧的安全关联代理，用于提取并保存所述安全关联代理探测请求消息中的初始化配置信息，并向网络接入控制器返回安全关联代理探测响应消息。

38、根据权利要求 35 所述的系统，其特征在于，所述安全关联服务器用于向移动台发送安全关联代理探测请求消息，该消息中携带安全关联代理的初始化配置信息；如果移动台未响应所述探测请求消息，则判定移动台需要安装安全关联代理；触发移动台启动安全关联代理的下载安装。

39、根据权利要求 38 所述的系统，其特征在于，所述网络接入控制器用于向安全关联服务器发送移动台连接报告。

40、根据权利要求 35 至 38 任一项所述的系统，其特征在于，还包括：安全关联代理下载服务器，用于在网络接入控制器重定向移动台的数据服务请求后，向移动台提供安全关联代理的下载服务。

41、根据权利要求 38 所述的系统，其特征在于，还包括位于移动台侧的安全关联代理，用于提取并保存所述安全关联代理探测请求消息中的初始化配置信息，并向安全关联服务器返回安全关联代理探测响应消息。

42、根据权利要求 41 所述的方法，其特征在于，所述网络接入控制器用于接收来自安全关联服务器在判定移动台需要安装安全关联代理时发送的移动台连接响应 A 类消息。

43、根据权利要求 35 所述的系统，其特征在于，还包括位于移动台侧的安全关联代理，用于收集移动台的安全相关信息，上报给关联响应系统的安全关联服务器；

所述安全关联服务器用于分析安全关联代理上报的安全相关信息，在需要时向安全关联代理返回安全相关信息响应。

44、根据权利要求 43 所述的系统，其特征在于，所述网络接入控制器和应用服务控制器用于接收安全关联服务器在根据分析结果判断需要更新移动台的安全控制策略时下发的安全控制策略更新请求，向安全关联服务器返回安全控制策略更新响应，通知安全关联服务器移动台的安全控制策略更新结果。

45、根据权利要求 41 至 44 任一项所述的系统，其特征在于，还包括：安全状态报告或安全提示信息生成单元，用于根据收集的移动台的安全相关信息和安全关联服务器返回的安全相关信息响应生成移动台安全状况评估报告或安全提示信息；所述安全状态报告或安全提示信息生成单元位于安全关联代理内。

46、根据权利要求 41 至 44 任一项所述的系统，其特征在于，还包括：更新单元，用于根据安全关联服务器返回的安全相关信息响应更新移动台的安全应用软件或者操作系统；所述更新单元位于安全关联代理内。

47、一种关联响应系统，包括网络侧和移动台，其特征在于，

所述的网络侧用于与移动台进行信息交互；当根据所述信息交互确认需要安全更新时，向移动台下发安全更新控制信息。

48、根据权利要 47 所述的关联响应系统，其特征在于，所述网络侧包括第一消息发送接收模块和判断模块，所述的第一消息发送接收模块用于

向所述的移动台发送安全关联代理探测请求消息，并用于接收所述的移动台发送的探测响应消息；所述的判断模块用于根据所述的探测响应消息判断所述的移动台是否应安装安全关联代理；

所述的移动台包括第二消息发送接收模块，用于接收所述的安全关联代理探测请求消息，并向所述的网络侧发送探测响应消息。

49、根据权利要求 48 所述的系统，其特征在于，所述的移动台还包括下载安装模块，用于当所述的判断模块判断所述的移动台需要安装安全关联代理时，下载并安装所述的安全关联代理。

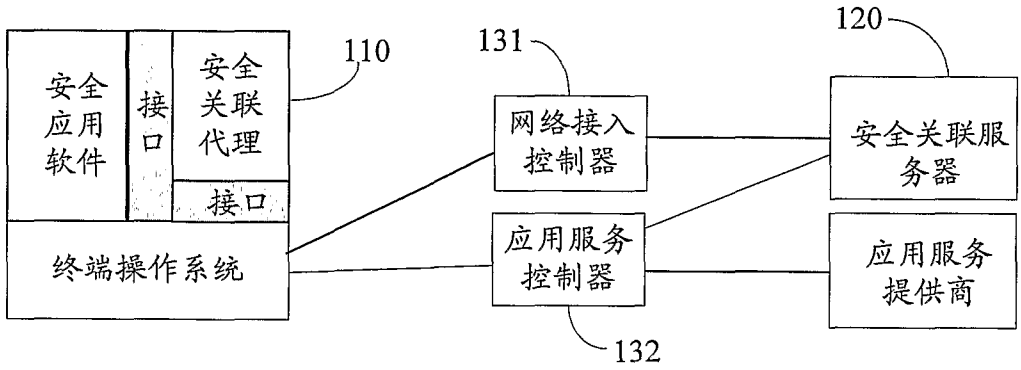

安全应用软件
接口
安全关联代理
接口
终端操作系统
110
131
网络接入控制器
应用服务控制器
132
120
安全关联服务器
应用服务提供商

图 1

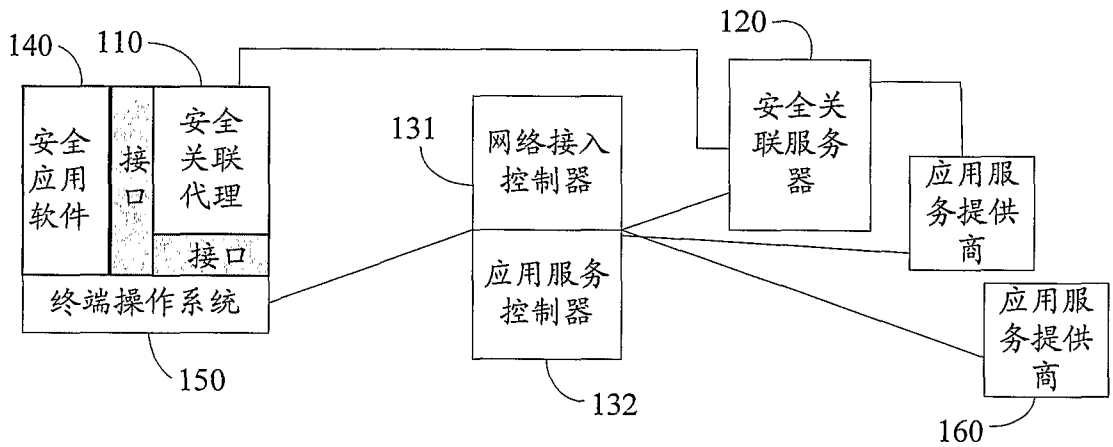

140
110
安全应用软件
接口
安全关联代理
接口
终端操作系统
150
131
网络接入控制器
应用服务控制器
132
120
安全关联服务器
应用服务提供商
应用服务提供商
160

图 2

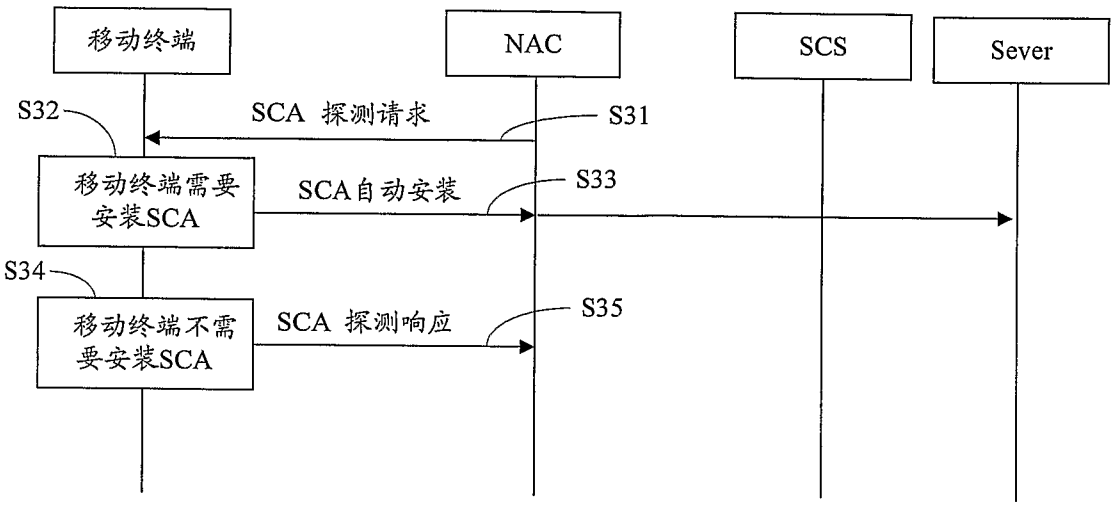

移动终端
NAC
SCS
Sever
S32
SCA 探测请求
S31
移动终端需要安装SCA
SCA自动安装
S33
S34
移动终端不需要安装SCA
SCA 探测响应
S35

图 3

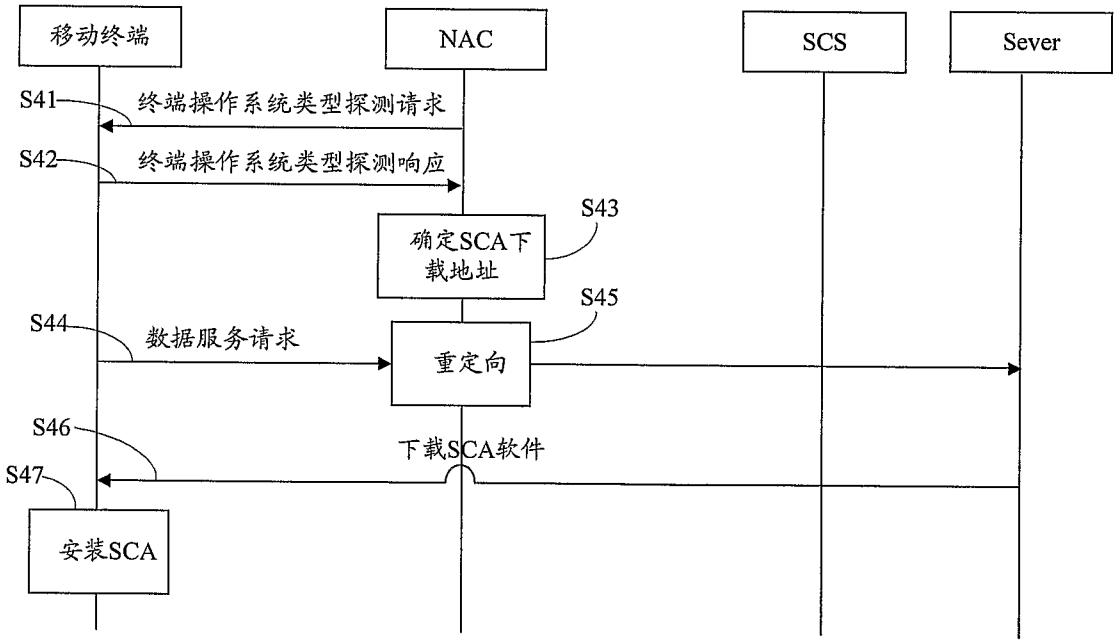

移动终端
NAC
SCS
Sever
S41
终端操作系统类型探测请求
S42
终端操作系统类型探测响应
S43
确定SCA下载地址
S45
S44
数据服务请求
重定向
S46
下载SCA软件
S47
安装SCA

图 4

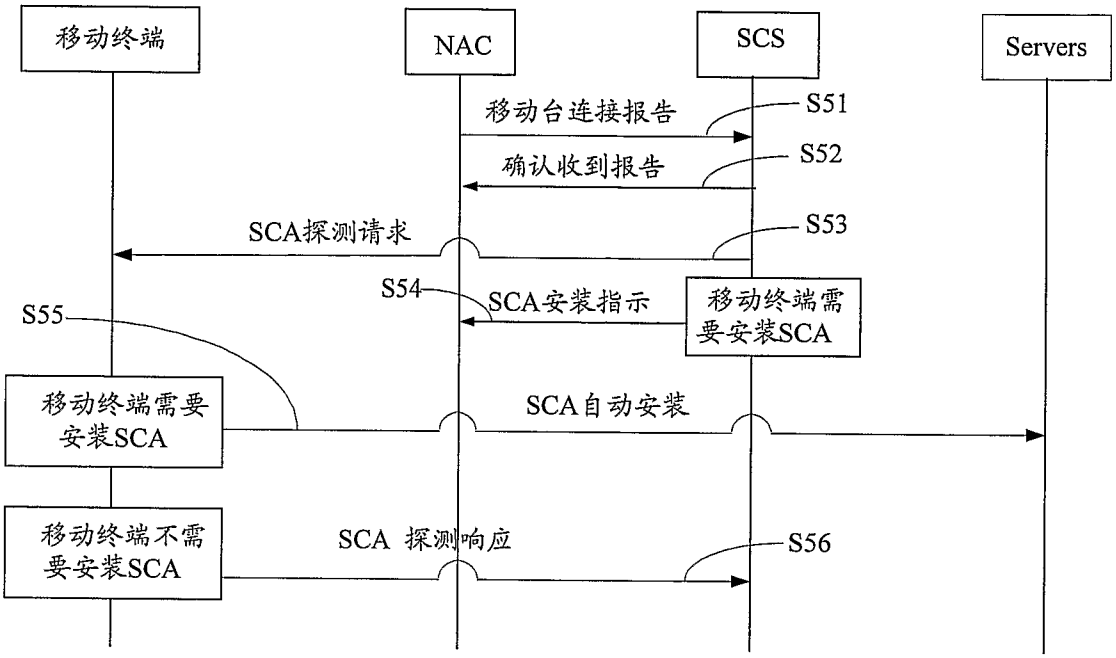

移动终端
NAC
SCS
Servers
移动台连接报告
S51
确认收到报告
S52
SCA探测请求
S53
S54
SCA安装指示
移动终端需要安装SCA
S55
移动终端需要安装SCA
SCA自动安装
移动终端不需要安装SCA
SCA 探测响应
S56

图 5

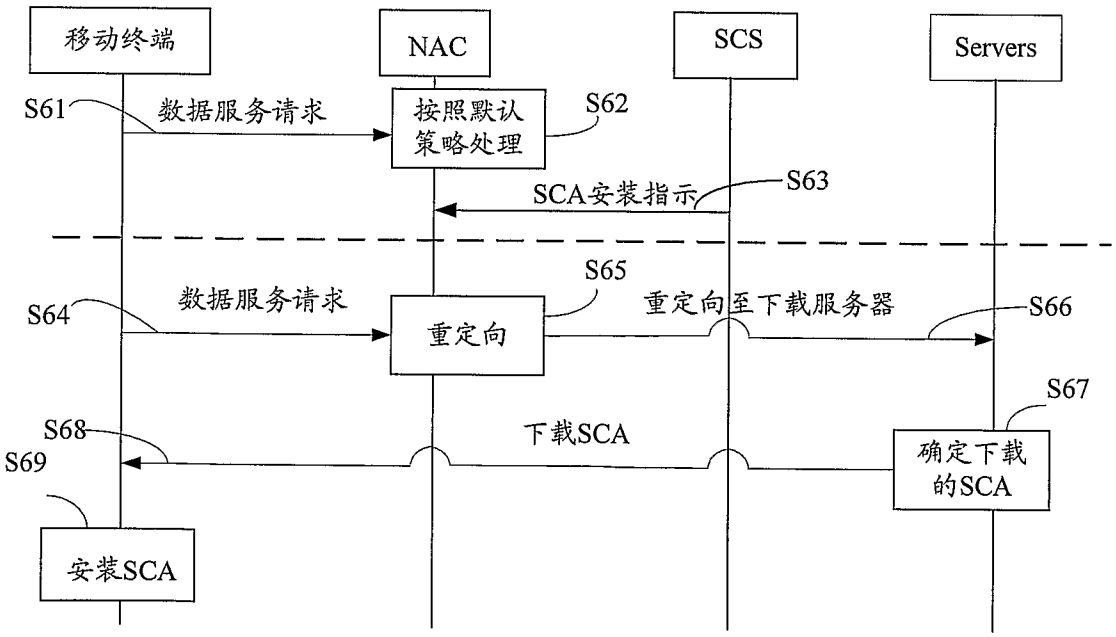

移动终端
NAC
SCS
Servers
S61
数据服务请求
按照默认策略处理
S62
SCA安装指示
S63
S64
数据服务请求
S65
重定向
重定向至下载服务器
S66
S67
S68
下载SCA
S69
确定下载的SCA
安装SCA

图 6

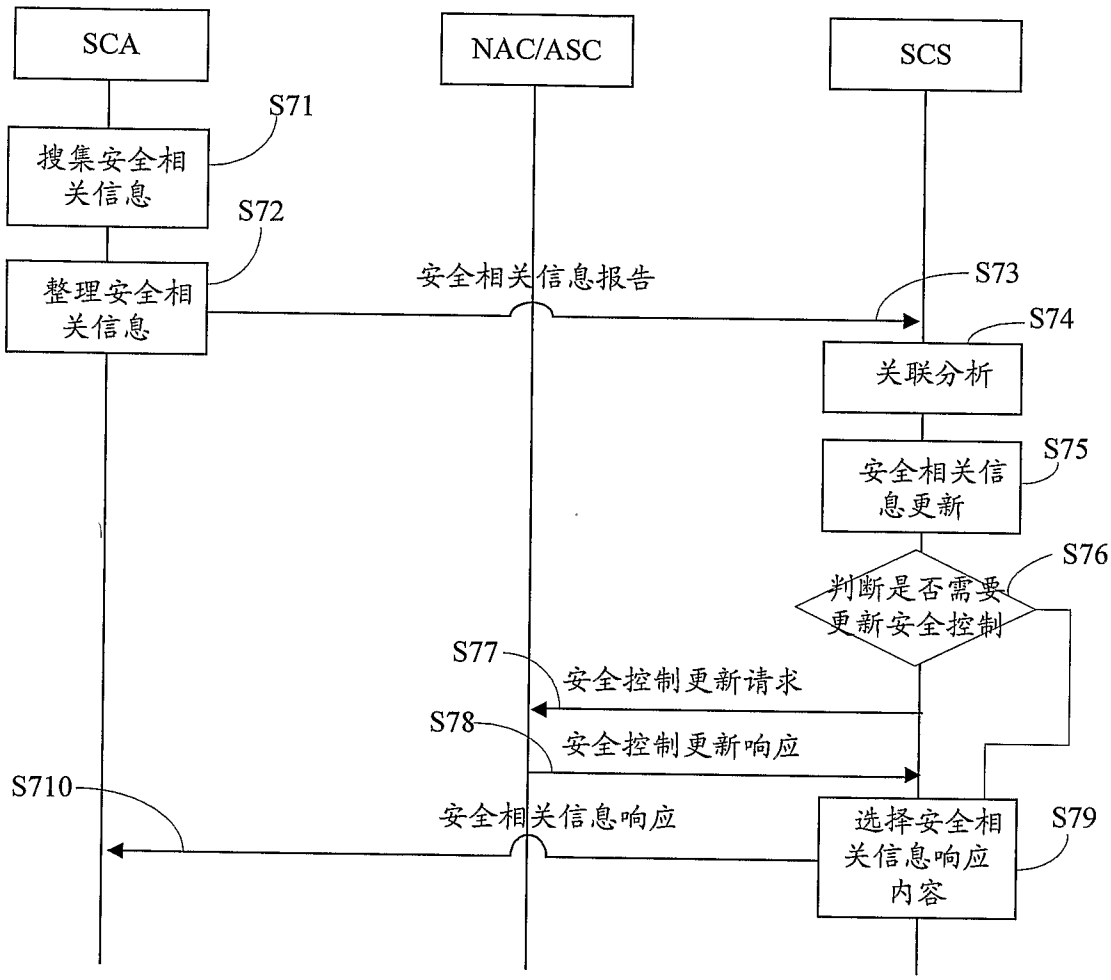

SCA
NAC/ASC
SCS
S71
搜集安全相关信息
S72
整理安全相关信息
安全相关信息报告
S73
S74
关联分析
S75
安全相关信息更新
S76
判断是否需要更新安全控制
S77
安全控制更新请求
S78
安全控制更新响应
S710
安全相关信息响应
选择安全相关信息响应内容
S79

图 7

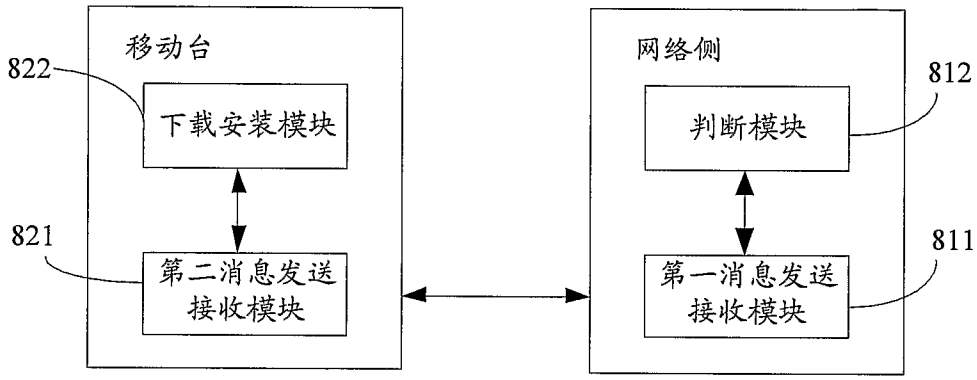


图 8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2006/002703

A. CLASSIFICATION OF SUBJECT MATTER

H04Q 7/32 (2007.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC[8] :H04Q 7/20, H04Q7/32, H04Q7/38, H04L 12/00, H04L 29/06

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI,EPODO,PAJ: CRS/correlative reacting system, secur+, updat+/download+/software/procedure?, terminal?/station?/phone?/device?, access+ control+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	ITU-T Security Standardization, Herb Bertine (2005.8.28-9.2) Pages 15-21	1-49
A	Mobile IPv6 Security Mechanism for Bingding Updates to Correspondent Nodes The whole documment.	1-49

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim (S) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&"document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 Jan. 2007 (10.01.2007)	01 FEB 2007 (01·02·2007)
Name and mailing address of the ISA/CN The State Intellectual Property Office, the P.R.China 6 Xitucheng Rd., Jimen Bridge, Haidian District, Beijing, China 100088 Facsimile No. 86-10-62019451	Authorized officer **Wang Chunyan** Telephone No. (86-10)62084581

Form PCT/ISA /210 (second sheet) (April 2005)

国际检索报告

国际申请号
PCT/CN2006/002703

A. 主题的分类

H04Q 7/32 (2007.01)i

按照国际专利分类表(IPC)或者同时按照国家分类和 IPC 两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

IPC[8] :H04Q 7/20, H04Q7/32, H04Q7/38, H04L 12/00, H04L 29/06

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用）)

WPI,EPODO,PAJ: CRS/correlative reacting system, secur+, updat+/download+/software/procedure?, terminal?/station?/phone?/device?, access+ control+

C. 相关文件

类　型*	引用文件，必要时，指明相关段落	相关的权利要求
A	ITU-T Security Standardization, Herb Bertine	1-49
A	移动 IPv6 注册通信对端绑定的安全保护机制　全文	1-49

☐ 其余文件在 C 栏的续页中列出。　　☐ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
10.1 月 2007（10.01.2007）	01 · 2月 2007 (01 · 02 · 2007)
中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路 6 号 100088 传真号：　(86-10)62019451	受权官员 王春艳 电话号码：(86-10)62084581