

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04Q 7/00 (2006.01)



[12] 发明专利说明书

专利号 ZL 01806096. X

[45] 授权公告日 2009 年 1 月 14 日

[11] 授权公告号 CN 100452887C

[22] 申请日 2001. 3. 5 [21] 申请号 01806096. X

[30] 优先权

[32] 2000. 3. 4 [33] GB [31] 0005173. 0

[86] 国际申请 PCT/EP2001/002455 2001. 3. 5

[87] 国际公布 WO2001/067785 英 2001. 9. 13

[85] 进入国家阶段日期 2002. 9. 4

[73] 专利权人 摩托罗拉公司

地址 美国伊利诺斯州

[72] 发明人 石 荣 马丁·约翰·埃利斯

马克·卡塔托

[56] 参考文献

US5842002A 1998. 11. 24

WO97/05551A1 1997. 2. 13

CN1212542A 1999. 3. 31

审查员 冉建国

[74] 专利代理机构 中原信达知识产权代理有限责
任公司

代理人 谢丽娜 张天舒

权利要求书 6 页 说明书 14 页 附图 2 页

[54] 发明名称

控制数据下载到用户设备的通信系统的结构
和方法

[57] 摘要

从不安全的网络(12)，比如因特网，被下载到节点(50)的代码被传送到一个支持节点(50)的仿真器的正常的检查站功能块(44)。只有经过将下载的代码在仿真器上运行(122-126)的交互操作性和兼容性检查之后，代码才被允许通过(116, 134)到达节点，以用于软件升级，应用程序扩增或内容检查等用途。系统操作员(或系统管理员)因此可以调节软件升级，以避免有潜在的可能会带来负面影响的灾难性的软件升级，比如移动单元操作。一旦代码被评估过了，它即可以被存储(108, 132)到代码和错误的库(46)中，以备将来相同的源于节点(50)的请求使用，或者可以将它在代码和错误的库(46)中丢弃掉和标记为不兼容的操作系统。

1. 一种蜂窝通信系统，包括：

到存储至少一份数据内容或代码的第三方数据库的接口；和
拥有用于请求从所述第三方数据库下载至少一份数据内容或代码的装置的节点；

本地代码和错误库，该本地代码和错误库用于存储所述下载的数据内容或代码以及如代码评估装置所确定的与所述下载的数据内容或代码相关的任何错误；以及

响应第三方数据库并连接到所述节点和本地库的正常的检查站功能块，所述正常的检查站功能块包括用于检查来自所述节点的下载请求是否用于先前评估并存储在本地库中的数据内容或代码的装置，其中

如果在本地库中存在该内容或代码，则所述用于检查的装置判断所述与该内容或代码相关的错误，并且将错误与可接受等级比较，其中

如果错误的等级是可以接受的，那么正常的检查站功能块操作来将数据内容或代码直接下载到请求节点，以及

如果错误的等级是不可以接受的，那么正常的检查站功能块拒绝来自该节点的下载请求；以及

如果在本地库中不存在该内容或代码，则所述正常的检查站功能块操作来响应请求下载的所述节点，截获从第三方数据库下载的至少一份数据内容或代码，所述正常的检查站功能块包括：

代表所述节点并与从第三方数据库下载的至少一份数据内容或代码进行交互作用的仿真器；

用于根据从第三方数据库数据下载的至少一份数据内容或代码与代表所述节点的所述仿真器的交互作用，评估所述仿真器运行状态的代码评估装置；

用于有选择地将至少一份数据内容或代码转发到所述节点的装置，该至少一份数据内容或代码被从符合对满足预定的运行状

态的运行状态的评估的第三方数据库下载。

2. 如权利要求 1 中所述的蜂窝通信系统，其中所述正常的检查站功能块包括用于评估从第三方数据库下载的数据内容或代码中的安全攻击以及数据内容或代码的兼容性中至少一个的装置。

3. 如权利要求 1 中所述的蜂窝通信系统，其中所述代码和错误库至少存储下述中的一些：

与连接到所述正常的检查站功能块的不同类型的节点相关的多种不同节点的仿真程序；以及

从识别的第三方数据库下载的数据内容或代码。

4. 如权利要求 3 中所述的蜂窝通信系统，其中所述用于检查的装置响应由请求下载的装置生成的第三方数据库的地址，用于在所述代码和错误库中寻找地址；和

数据内容或代码的到所述节点的直接下载与所述地址相关联。

5. 如权利要求 1 中所述的蜂窝通信系统，还包括：

包括所述正常的检查站功能块的到家庭网络的网关；和

到第三方数据库的专用安全链路；

其中所述家庭网络还包括：

用于响应对通过专用安全链路请求下载至少一份数据内容或代码的请求，选择性地禁止所述正常的检查站功能块操作的装置。

6. 如权利要求 5 中所述的蜂窝通信系统，还包括连接到所述家庭网络的访问网络，所述访问网络支持到主要附属于所述家庭网络的用户单元的通信，所述蜂窝通信系统还包括：

用于将所述访问网络中的用户单元发出的下载请求提交给所述家庭网络中的所述正常的检查站功能块的装置。

7. 如权利要求 1 中所述的蜂窝通信系统，其中所述节点由无线通信资源提供服务。

8. 如权利要求 1 中所述的蜂窝通信系统，还包括在所述第三方数据库和所述正常的检查站功能块之间连接的可被全球访问的网络。

9. 如权利要求 1 中所述的蜂窝通信系统，其中所述预定的运行状态具有完全可操作的通用性。

10. 一种用于控制数据下载的方法，其用于控制从存储至少一份数据内容或代码的第三方数据库到蜂窝通信系统的网络中的请求节点的数据下载，所述方法包括以下步骤：

存储接收的代码以及与其相关的任何错误；

检查来自所述节点的下载请求是否用于先前评估并存储的数据内容或代码，其中

如果存储了该内容或代码，则判断所述与其相关的错误，并且将错误与可接受等级比较，其中

如果错误的等级是可以接受的，那么将数据内容或代码直接下载到请求节点，以及

如果错误的等级是不可以接受的，那么拒绝来自该节点的下载请求；以及

如果未存储该内容或代码，则

响应请求下载的所述节点，截获从第三方数据库下载的至少一份数据内容或代码；

生成代表所述节点的仿真程序；

引发仿真程序与从第三方数据库下载的至少一份数据内容或代码之间的交互操作；

根据从第三方数据库下载的至少一份数据内容或代码与代表所述节点的仿真器之间的交互操作，评估仿真器的运行状态；

有选择地将对运行状态的评估满足预定的运行状态的、从第

三方数据库下载的至少一份数据内容或代码转发到所述节点。

11. 如权利要求 10 中所述的用于控制数据下载的方法，还包括评估从第三方数据库下载的数据内容或代码中的安全攻击以及数据内容或代码的兼容性中的至少一个。

12. 如权利要求 10 中所述的用于控制数据下载的方法，其中所述存储步骤包括在所述网络内的代码和错误库中至少存储下述中的一些：

与所述蜂窝通信系统内的不同形式的节点相关联的多个不同的节点仿真程序；和

从被识别的第三方数据库中下载的数据内容或代码。

13. 如权利要求 12 中所述的用于控制数据下载的方法，其中所述检查步骤包括：

在网络的代码和错误库中查找第三方数据库的地址；和

将与所述地址相关的数据内容或代码直接下载到所述节点。

14. 如权利要求 10 中所述的用于控制数据下载的方法，其中所述网络还包括通过专用安全链路连接到至少一个第三方数据库的网关，所述方法还包括步骤：

响应通过专用安全链路下载至少一份数据内容或代码，有选择地禁止生成仿真程序和评估运行状态。

15. 如权利要求 14 中所述的用于控制数据下载的方法，还包括步骤：通过家庭网络从访问网络中的用户单元发出下载请求。

16. 如权利要求 10 中所述的用于控制数据下载的方法，其中所述节点由无线通信资源提供服务。

17. 如权利要求 10 中所述的用于控制数据下载的方法，其中可被全球访问的网络连接第三方数据库和所述家庭网络。

18. 一种控制设备，用于调节从存储至少一份数据内容或代码的第三方数据库到蜂窝通信系统的网络中的请求节点的数据下载，所述控制设备包括：

用于存储所述下载的数据内容或代码以及如代码评估装置所确定的与该下载的数据内容或代码相关的任何错误的装置；以及

用于检查来自所述节点的下载请求是否用于先前评估并存储在用于存储的装置中的数据内容或代码的装置，其中

如果在所述用于存储的装置中存在该内容或代码，则所述用于检查的装置判断所述与该内容或代码相关的错误，并且将错误与可接受等级比较，其中

如果错误的等级是可以接受的，那么控制设备操作来将数据内容或代码直接下载到请求节点，以及

如果错误的等级是不可以接受的，那么控制设备操作来拒绝来自该节点的下载请求；以及

如果未存储该内容或代码，则所述设备进一步包括：

操作配置为响应节点的下载请求，截获从第三方数据库下载的至少一份数据内容或代码的装置；

代表所述节点，并与从第三方数据库下载的至少一份数据内容或代码进行交互的仿真器；

用于根据从第三方数据库下载的至少一份数据内容或代码与代表所述节点的仿真器的交互，评估所述仿真器运行状态的代码评估装置；和

用于有选择地将对运行状态的评估满足预定的运行状态的、从第三方数据库下载的至少一份数据内容或代码转发到所述节点的装置。

19. 如权利要求 18 中所述的控制设备，还包括用于评估从第三方数据库下载的数据内容或代码中的安全攻击以及数据内容或代码的兼

容性中的至少一个的装置。

20. 如权利要求 18 中所述的控制设备, 其中用于存储的装置包括代码和错误库, 其至少存储下述中的一些:

与连接到所述正常的检查站功能块的不同类型的节点相关的多个不同节点仿真程序; 和

从识别的第三方数据库下载的数据内容或代码。

21. 如权利要求 20 中所述的控制设备, 其中用于检查的装置包括: 用于响应由所述节点生成的第三方数据库的地址, 在代码和错误库中查找所述地址的装置; 和

用于从代码和错误库中将与所述地址相关的至少一份数据内容或代码直接下载到所述节点的装置。

22. 如权利要求 18 中所述的控制设备, 还包括:

用于响应通过进入控制设备的专用安全链路下载至少一份数据内容或代码的请求, 有选择地禁止仿真程序操作的装置。

控制数据下载到用户设备的通信系统的结构和方法

发明领域

本发明一般涉及控制数据下载到可编程的（adaptable）用户设备的通信系统，尤其是并且可与用于（但不排它）可下载终端（比如第三代无线通信设备）内的应用程序的调节。

背景技术

随着通信技术的发展，用户对于满足个人（或团体）要求的个性化用户设备功能的需求不断增长。这种用户设备可能具有多种形式，包括（但不限于）：i) 在第三代蜂窝系统中提出的所谓的软件无线，比如移动通信通用系统（UMTS）；和 ii) 可编程的终端设备，比如局域网（LAN）中的计算机。

在相当长的一段时期内，下载软件是一种愿望。现在，随着因特网访问和无线频率领域中数据包传输技术的发展，软件下载和终端编程已经变成现实。从服务器（或内容供应商）上下载的软件当然可以有多种形式，包括整个应用软件（比如更换移动专用固件）和用于寻址在代码初始版本发行之后被发现的某个特定技术缺陷的软件补丁。软件下载也可能是应内容供应商的要求而进行评估的特殊内容，并可能表现为一般的因特网信息，比如电子商务信息，网页，等等。此外，软件可以以用在用户设备中的附加的“插入式”内存扩展卡或 SIM 卡上的代码的形式提供。在下一代移动通信系统中，移动用户单元将能够通过分组交换集合信道，经过空中接口和有线或光纤网络直接访问因特网。此外，还面临着这样的问题，服务在未来将是与通信网络没有联系的，也就是说，网络操作者，服务提供者和制造者的角色可以被清楚的区分，并可由不相关的团体独立的支持。因此，理论上讲，可以从任何可访问源下载软件或内容。此外，应当理解，因特网的开

放性（尽管这是令人满意的）导致了网络是非常不安全的，其中的用户会因为不小心下载了不兼容的或蓄意制造的恶意代码而使自己的用户设备的功能的安全受到危及。在前一种情况下，在用户单元上同时运行下载的代码和已存在的软件/固件，可能仅仅会不小心地导致系统失效或系统崩溃。恶意制造的流氓程序，就是通常所指的“安全”攻击会蓄意地试图破坏或转移用户单元处理的数据，或者，更令人忧虑的是，通过永久的改写或禁用重要的功能或数据来破坏第三方设备。实际上，没有安全保护，安全攻击可相当容易地作用于特殊的通信分组或周期（在一次呼叫或因特网访问会话期间）和网络节点（比如用户单元和服务器）。

因此，对于用户设备的个性化，不幸的是，存在着固有的风险，这种风险除和用户设备所支持的应用软件的数量增加以及从（一般来讲）不安全的通信资源（比如因特网）上未受审查的数据库得到的代码更新或更换有关。

为了对付一些形式的安全攻击，病毒检查程序被（用于基于计算机的终端技术）开发出来以扫描蓄意制造出来的感染主机处理器的流氓软件。这种病毒检查程序必须被经常的更新以对付新的计算机病毒带来的问题。

至于安全攻击的类型，通常可以将它们归类为下列两个类别中的一种，即第一种类型，这种安全攻击试图偷偷地访问信息，和第二种类型的攻击，它进行破坏、改写或危及合法系统或用户单元的操作。

第一种类别的安全攻击包括下列构思：i) 探测用户请求，然后根据探测到的用户请求的重要性/相关性来拦截软件（或内容）；ii) “中间人”访问，其中一个实体拦截用户和权利认证机构之间认证请求，从而危及安全（例如，在电子商务环境中）；以及 iii) 中断下载。这些型式的安全攻击的通常思路是通过（比如）专门的通信路径的开

口直接访问信息。一个混合攻击机制与使用恶意代码有关，其中一个第三方实体（比如，一个恶意的雇员）通过检查全部安全认证背景的手段获得一个有效的“签名的证书”，但是随后第三方创建和签发恶意的内容。第一种类型的安全攻击不像基于提供一个安全通信连接这样容易处理。

第二种类型的安全攻击直接改变用户单元或主机处理器中（通过破坏代码来）的功能。这种破坏的形式有许多种，下面列出了主要的机制。首先，第三方在软件（或内容）下载到发出请求的用户单元或 LAN 服务器网关设备（比如网络服务器/节点）期间修改软件（或内容）。第二，被称之为特洛伊木马的攻击会导致处理系统看上去在进行/执行请求的程序，然而处理系统实际上在做一些罪恶的和追加于请求程序之上的事情，比如对用户单元的控制被有效地由与合法拥有者无关的第三方所接管。第三，用于软件下载的上行链路消息被截获，（由第三方）假冒的定址服务器导致将恶意或有敌意的代码下载到请求下载的处理器上。第四，关联的下载软件的用户单元或服务器可能因为伪代码而溢出。第五，在软件下载进程开始之前，第三方黑客可以通过修改服务器上的软件和内容来危及服务器的安全。

通常，如果地址服务器或数据库没有被适当的保护，黑客们就容易通过破坏其中存储的数据来危及服务器的安全。在这种情况下，没有外在的迹象表明服务器提供的数据被破坏了，因此，作为一个的受信任的真正好的服务器，服务器根据寻址节点（比如用户单元）和服务服务器本身之间传递授权证书，仍然可以被访问和交互操作。很明显，在这种情况下，用户单元可能不小心下载了具有恶意性质的被破坏的软件。事实上，如果被破坏的、有重要使命的可执行无线电软件（RF/IF 基带算法）被下载到移动单元，可能会导致移动单元的功能错误或过早结束功能；这是我们特别关心的内容。更具体的说，移动环境中被破坏的代码所带来的问题会由于用户单元（比如蜂窝电话或 UMTS 终端）固有的移动特性而加剧，因为与这个移动单元建立的联系会被切

断或阻止，并且这个联系不能被直接重新建立。因此，移动用户和服务提供者可能完全忘却任何电话/设备错误或故障。这样，从用户的立场看，没有丢失服务的明显迹象，然而，经营者将失去相关的服务收入。

很明显，现在应当理解，软件下载很容易被一个或多个安全攻击所攻击，通常强有力的安全机制被优选地用来保护软件下载不受安全攻击。

所谓的移动运行环境 (MExE) 已在 3GPP T2 中被建议用来提供应用程序、小程序和内容的自动安全传输。在 MExE 中实施的认证机制基于 CCITT X.509 数字认证，它可以使用户单元和服务器有效地互相认证。独立的加密机制被用于提供软件（或内容）下载的保密性。当前用于安全的软件/内容下载的 MExE 方法是用受“信任的认证机构”所授权的数字证书标记软件/内容。证书将唯一辨认服务器以向用户证明下载的软件/内容来自受信任的服务器；这种情况存在于如下情况：比如，服务器属于手机制造商。换言之，证书实质上包括一个设备唯一的数字签名，和一个为以后对在用户单元和服务器之间传输的数据分组（或类似的东西）解码的密钥。

不幸的是，这种在 MexE 中提供的安全机制只能防范某些安全攻击，主要是下载过程中修改软件这样的攻击。除了应用于 Java 沙箱的字节码验证之外，MexE 没有提供明显的安全保护以防止直接作用于始发服务器或通过欺骗手段获得的有效认证证书这样的安全攻击。

更详细地说，应当理解 Java 语言允许 Java 兼容的网络浏览器动态地下载代码片段，并在机器上运行这段代码。最初的 Java 安全机制利用沙箱，通过限制小程序的权利来加强对什么 Java 程序可以或不可以运行的进行严格的控制。除了赋予 Java 代码特殊的权利，Java 沙箱还控制下载的代码对系统资源的访问。

在计算机终端/工作站的上下文中，一旦代码被下载到工作站的沙箱中，Java 沙箱将执行一系列方式的验证，包括类（class）文件格式的检查和字节码的验证。在字节码验证中，字节码的运行依靠运行时间系统，也就是说，用于虚拟机指令集的仿真器。字节码验证器通过下述方法验证所有的字节码：i) 分析数据流来看看是否有违反堆栈溢出的情况；以及 ii) 直接访问寄存器。字节码验证器被安排来“调用”（也就是识别有潜在可能的破坏）那些例行程序和子例行程序，比如，它们获得了不适当的参数或获得了不适当的参数类型。可是，Java 沙箱字节码验证机制仅仅执行语言相关类型的检查，其作用是防止未批准的对本地资源的访问，并通过确保代码符合预先确定的限制条件上来防止破坏性操作。预先确定的限制条件能够确保不会发生堆栈的上溢或下溢，以及有正确的寄存器访问和存储。此外，字节码验证器看上去正确分配参数到所有字节码指令，并进而确保没有发生非法的数据转换。即使是如此复杂，Java 沙箱也不是足够安全，它不能解决黑客危及存储在服务器上的软件的安全，使用被截获的授权认证和特洛伊木马攻击这样严重的安全攻击。

作为对 Java 沙箱技术的适度概括，现在应当理解，Java 沙箱为 Java 代码提供了限制性的访问功能，从而防止访问与特定的 Java 小程序无关的存储器位置。因此，软件交互操作被提供绝对安全屏障的 Java 沙箱所限制。

在基于个人 Java 的 MExE 类标记 II 中，字节码验证被用于证明被下载的代码适合虚拟机的运行条件。然而，并没有要求制造商使用单一的代码格式，这样不是用 Java 语言编写的代码也可能被用在可下载环境中，例如可执行无线系统（或子系统）软件的情况。

当然，可以使用强力机制进行保护，由此，所有形式的功能个性化都受到了限制。比如，计算机系统被设计成通过防火墙/代理/缓存

进行操作。防火墙/代理可以通过过滤/阻止检索内容和最终得到的提取内容来为客户提供保护。这种用于因特网的防火墙/代理机制非常粗糙（比如，过滤所有的 javaScript，阻止所有对 <http://hackedcode.com> 的访问），不能满足今天发展中的通信环境中需要的各种途径。

发明内容

本发明的第一个方面，提供了一种通信系统，它的组成为：存储至少一份数据内容和代码的第三方数据库；具有请求从第三方数据库下载至少一份数据内容和代码的装置的节点；通信系统还包括：对第三方数据库进行响应并连接到节点的正常的检查站功能块；正常的检查站功能块用于响应请求下载的数据，截获从第三方数据库下载的至少一份数据内容和代码，正常的检查站功能块包括：代表节点并与从第三方数据库下载的至少一份数据内容和代码交互作用的仿真器；用于根据代表节点的仿真器与从第三方数据库下载的至少一份数据内容和代码之间交互作用，评价仿真器操作状态的代码评估装置；用于有选择地将对操作状态进行评估以满足预定的操作状态的、从第三方数据库下载的至少一份数据内容和代码转发给节点的装置。

在优选的实施例中，正常的检查站功能块包括用于评估从第三方数据库分别下载的数据内容和代码中，至少兼容性和安全攻击程度之一的装置。

优选地，代码和错误库与正常的检查站功能块连接，代码和错误库至少存储一些：多个连接到正常的检查站功能块的与不同形式节点相关的不同节点的仿真内容；从被识别的第三方数据库下载的数据内容、从被识别的第三方数据库下载的代码；适于下载到节点的曾经经过与被识别的第三方数据库相关的代码评估装置评估的数据内容和代码的指示（indication）。

在一个实施例中，正常的检查站功能块包括：对由请求下载的装

置产生的第三方数据库的地址做出响应、以在代码和错误库中寻找地址的装置；和在至少一份数据内容和代码存储在代码和错误库中并且使所述存储的数据内容和代码预先产生满足预定操作状态的仿真器操作状态时，直接从代码和错误库向节点下载与所述地址有关至少一份数据内容和代码的装置。

通信系统还可能包括：到包含正常的检查站功能块的家庭网络的网关；和到至少一个第三方数据库的专用的安全链路；其中家庭网络中还包括：用于响应请求通过专用安全链路下载至少一份数据内容和代码有选择地禁止正常的检查站功能块操作的装置。

访问网络可能被连接到家庭网络，同时访问网络支持对主要附属家庭网络的用户单元的通信。通信系统可能还包括：用于提交从访问网络中的用户单元下载到家庭网络中的正常的检查站功能块的请求的装置。

在第三方数据库和正常的检查站功能块之间一般连接可被全球访问的网络，例如因特网。

至于预定的操作状态，它的等级是任意设置的，但是可能要服从影响重要操作系统的程度。因此，在某些情况下要求有总的操作通用性，而在其它场合下在其后的节点操作中的微小错误可能是可以接受的（举例来说当节点（比如蜂窝电话）中的固件中存在已知问题，部分操作系统软件的升级可以表示操作功能的改善）。

本发明的第二个方面中，提供了一种用于控制数据下载到具有存储至少一份数据内容和代码的第三方数据库的通信系统网络中的节点的方法，该方法包括：在节点处，请求从第三方数据库下载至少一份数据内容和代码；方法还包括：响应节点下载请求，在网络中截获从第三方数据库下载的至少一份数据内容和代码；生成代表节点的仿真

程序；引发仿真程序和从第三方数据库下载的至少一份数据内容和代码之间的交互操作；根据从第三方数据库下载的至少一份数据内容和代码与代表节点的仿真程序之间的交互操作，评估仿真程序的操作状态；有选择地将符合对满足预定的操作状态的操作状态的评估的第三方数据库下载的至少一份数据内容和代码转发给节点。

本发明的另一个方面，提供了一种用于控制将数据下载到具有存储至少一份数据内容和代码的第三方数据库的通信系统网络中的节点的控制设备，控制设备包括：响应对节点下载请求，截获从第三方数据库下载的至少一份数据内容和代码的可操作配置的装置；代表节点和与从第三方数据库下载的至少一份数据内容和代码之间进行交互操作的仿真器；用于根据从第三方数据库下载的至少一份数据内容和代码与代表节点的仿真器之间的交互操作，评估仿真器操作状态的代码评估装置；用于有选择地将符合对满足预定的操作状态的操作状态的评估的第三方数据库下载的至少一份数据内容和代码转发给节点的装置。

本发明的另一个方面，提供了一种用于控制数据下载到具有存储至少一份数据内容和代码的第三方数据库的通信系统家庭网络中的节点的计算机程序产品，计算机程序产品包括：响应节点下载请求，指示控制器截获从第三方数据库下载的至少一份数据内容和代码的代码；指示控制器生成代表节点的仿真程序的代码；指示控制器引发仿真程序和从第三方数据库下载的至少一份数据内容和代码之间的交互操作的代码；指示控制器根据从第三方数据库下载的至少一份数据内容和代码与代表节点的仿真器之间的交互操作、评估仿真程序操作状态的代码；和指示控制器有选择地将符合对满足预定的操作状态的操作状态的评估的第三方数据库下载的至少一份数据内容和代码转发给节点的代码；其中的这些代码存储于可被计算机读取的媒体中。

优选地，当移动用户（比如）请求下载可能影响它的操作系统的代码时，不管移动用户在什么位置，这种代码总是被发送到正常的检查站功能块，以检查代码的兼容性。

本发明提供了一种机制，它有助于使系统操作员（或其它系统管理员）能够对由用户单元请求的，有潜在可能可疑的可下载代码执行清理检查，以使对用户的节点或通信设备中现存代码进行更新或扩增。考虑到本发明在移动无线通信设备环境中的应用后，系统操作员（或系统管理员）调节软件升级的能力减少了会给移动单元操作带来负面影响的潜在的灾难性的软件更新。更具体地说，本发明允许系统操作员否决会破坏和阻止各种对移动无线通信设备的系统访问（这里是说上行链路连接和下行链路连接）的软件下载。虽然本发明能够严格地控制软件下载，但基于系统操作员在用户访问站点或专用路径中拥有的信任等级，在控制方法上它能够选择。比如，如果用户访问安全的内部网络中的站点，软件（特别是应用代码，诸如交互的 Java 小程序）下载可以被立即批准，而不需要管理员审查和交互操作。相反地，如果用户访问被认为是不安全的站点（诸如通过多重网关进入广域网范围），管理员会采取更加严格的态度，由此，可下载的代码会被特殊地对待，并使其符合根据本发明中的原理的完整性/兼容性评估。

因此本发明提供一种用于软件的验证机制（作用是软件清理检查），这个机制可以在软件被下载和升级之前是可以动作的。因此，本发明致力于移动或其它用户单元或节点的个性化需求，同时防止有重要使命的软件被破坏。优选的实施例可以应用于通信系统中的一系列可选的节点上，并因此可以提供与 LAN（或类似的网络）相关的用户的服务调节，从而允许在多个用户单元或节点间共享验证机制。

本发明可以用于（比如）移动通信软件下载产品中；它可以用于增加 MExE 和软件定义的无线设备（SDR）的安全性。本发明还可以

查询（比如）3GPP TSG T2 MExE 标准、SDR 论坛和欧盟创建的第五框架 TRUST（透明的可重新配置的普遍存在的终端）项目中应用软件。

附图说明

现在将根据附图说明本发明中示例性的实施例，其中：

图 1 是本发明中优选的实施例的通信系统的方框图；和

图 2 是本发明中优选操作方法的流程图。

具体实施方式

参见图 1，它是本发明优选实施例的通信系统 10 的方框图。通信系统 10 中的许多组件采用传统的设计。

不安全的网络 12（比如因特网）提供（典型的）分组交换传输域，数据业务通过它，在家庭网络 13（可能是 LAN）和选择的外围实体 14-18 之间传输。通过实例（但不限于实例），外围实体可以采用包含基于应用程序的代码 20（即软件和固件）和帐单信息 22 的服务提供器的形式。作为变通，外围实体可以采用通常对电子商务 24 或信息 26 提供服务 and 访问的内容供应器 16 的形式。外围实体的第三种形式 18 可以是制造商的服务器，用该数据站点存储 Java 小程序或类似形式的固件 28。

关于与系统制造商相联系的任何服务器 18，尽管站点显示为通过不安全的网络 12 与家庭网络 13 互连的，但站点也可以通过专用的（被认为是安全的）链路 30，连接到服务器 18。通常，在与制造商相联系的服务器 18 和家庭网络 13 之间传输的信息将包含证书 32，以提供额外的安全保证（尽管本发明中有效地减少了证书的使用）。

由于提供了能够根据请求被下载的可访问代码或内容资源，被称为第三方数据库的各种外围实体是可以互相改变的。

关于家庭网络 13，网关 34 提供了家用网络 13 与不安全的网络 12 之间的物理接口。容易理解，网关 34 可能采用转换开关的形式，并通常提供某种形式的路由和/或交互操作的功能。因此网关 34 包括控制逻辑 35，并在数据网络 36 允许互连的家庭网络 13 中，又连接到数据网络 36（比如，基于分组的域）。网关 34，其可以是无线应用协议（WAP）网关，用于使消息无障碍地在通信端点间通过。

在蜂窝式环境中，数据网络 36 通常连接到基站控制器（BSC）38，以管理多个基站收发器（BTS）40-42。

数据网络 36 还提供通常还在处理器或类似的地方中实现的到正常的检查站功能块（sanity check-point function）44 的互连。在优选的实施例中，正常的检查站功能块 44 是基于代码的、代表至少一个与数据网络 36 互连的节点的仿真器。正常的检查站功能块 44 还连接到存储仿真代码和通过不安全网络 12 下载的内容和应用程序（比如软件和固件代码）的代码和错误库 46。代码和错误库 46 可能还包括由正常的检查站功能块 44 的仿真器以前进行的、与下载的代码和内容相关的仿真记录的结果缓存器。

数据网络 36 还可能是可以临时附属用户单元 50（通常与家庭网络 13 相关）的附加访问网络的分配点。用户单元可以是（比如）移动电话的形式。访问网络 48 的构造可能反映家庭网络 13，并通过图解显示为包括连接到家庭网络的数据网络 36 的数据网络（比如，支持因特网或类似的协议的基于分组的网络）52。此外，数据网络 52 通过专用线或光缆连接 56 连接到计算机 54。访问网络 48 的数据网络 52 用于提供通过访问 BSC58 和相关 BTS60-62 在外围实体 14-18 和比如说用户单元 50 之间传输信息的传输机制。

尽管本发明有更广泛的应用，本发明提供一种主要是用于抵御直接影响到外围实体中存储的代码的安全攻击的防护机制。家庭网络 13

中的正常的检查站功能块 44 内的仿真器用于代表用户单元请求从外围实体 14-18 下载内容或代码。指示网关确保从不安全的网络 12 下载的至少是有选择的代码或内容先被路由到和随后通常被保存（至少是临时性的）到代码和错误库 46 中。然后，代码或内容在仿真器上运行，通过与仿真结果的交互，评估代码或内容的兼容性和互操作性。更具体地说，正常的检查站功能块 44 将支持用于每一种被家庭网络 13 所支持的节点（比如 BSC, BTS 或用户单元或计算机）的用户单元仿真器。正常的检查站功能块 44 运行有敌意代码的检查程序，以探测安全攻击，诸如隐藏在下载的代码中的特洛伊木马，拒绝服务或其它形式的恶意（安全）代码攻击。仿真器模拟真实的发出请求的用户实体的准确功能（就像以前存储在代码和错误库 46 中的）。因此，只有当对代码或内容的兼容性评估完成了，它们才会被真正下载到发出请求的用户。如果代码被认为是不兼容的或有害的，那么代码将从仿真器和代码和错误库 46 中被清除，并且优选地在代码和错误库 46 中建立标记，使提供代码或内容的原始站点在将来将需要被特殊处理或总是不被考虑。这种第三方站点的标记会被家庭网络 13 周期性的重新审查，以处理第三方外围实体为解决有害或不兼容代码或内容而进行的合法化尝试。

正如将被理解的，仿真器对代码的兼容性和交互操作性的评估可以基于利用参数检查的技术，诸如变量，上溢或下溢，以及仿真器中寄存器的有效访问和存储。

优选地，正常的检查站功能块 44 属于家庭网络 13 所有，因为家庭网络总可以被认为是在网络-操作员-域中的受到良好保护的网络的受信任的一方。因此，家庭网络内部的网络节点（诸如 DSC 38, BTS 40-42, 和用户单元 50）通常是不受一般的源于因特网的安全攻击的。同样，家庭网络 13 对于附属用户单元的适当的操作和功能通常是可靠的，这意味着家庭网络 13 对确保下载到发出请求的用户单元的特殊用户软件在家庭网络中可以正常工作负有全部的责任，并提

供订购单元的全部功能。

参照流程图 2，所示为优选的用于本发明的操作方法。过程开始于由节点发出的用于从远程第三方站点下载代码或内容的请求（步骤 100）。可选地，一些形式的授权认证 102 可能会被用于增加安全。（从第三方站点）将代码和内容下载 104 到中间的工作正常的检查点函数 44，并可能请求将代码临时存储于代码和错误库 46 中。在进程的某些地方，代码和错误库 46 可能被检查（步骤 106-108）以识别寻址的（远程）第三方站点以前是否被访问过，以下载类似的或同样的代码或内容。如果是肯定的 109，本发明中的系统将访问（步骤 110）存储器以判断（步骤 112）这些以前被请求的代码或内容是否包含不多于一个的可接受等级的交互操作错误（此等级可能有零偏差）。判断块模 112 得出的肯定结果 114 会导致从代码和错误库 46 局部下载（步骤 116）代码或内容到发出请求的节点，从而大大减少区域业务流量。判断块模 112 得出的否定结果 114 会导致下载请求被拒绝，并因此通知（步骤 118）节点。

如果没有对第三方站点访问的记录，进程将按照从判断模块发出的第二条路径 120 进行，第二条路径导致调用（步骤 122）代表发出请求的节点（比如移动用户单元 50）的仿真器。从第三方站点下载的代码或内容在仿真器上运行（步骤 124），有敌意的代码检查程序识别（步骤 126-128）有害的，或节点不兼容的代码。如果仿真的结果似乎不受或明显不受下载的代码或内容影响（即，不严重的影响），流程将沿路径 130 继续进行下去，在这里下载代码的一条本地记录被优选地生成（步骤 132）（并存储在代码和错误库 46 中，供以后参考）。然后，通过提供下载的代码或数据内容来服务（步骤 134）于节点发出的代码或内容下载请求。如果模块 128 做出的判断是肯定的（137），那么系统优选地记录这个代码，而不是代码和错误库 46（即适合的数据库或存储设备）中至少是已存在的错误，并通知节点由于不兼容问题，下载被拒绝。

当然，如果（当请求下载时）系统能够访问（步骤 140）到寻址的外围实体的专用和安全的路径，那么可以立即进行（步骤 142）下载代码到发出请求的节点，并且不用进行仿真过程和相关的兼容性/有害性评估。

总之，正常的检查站功能块与代码和错误库 46 进行交互，来看看代码或内容以前是否被家庭网络 13 中的其它节点下载过。如果是这样，以前存储在代码和错误库 46 中的代码或内容就可以被下载到节点，以避免多余的仿真和 WAN 访问。否则，正常的检查站功能块调用与请求下载的节点类型相对应的仿真器，并在节点仿真器上运行下载的代码。有敌意的代码的程序探测可能的安全攻击。一旦下载的代码或内容通过了清理检查，它将被安置在代码和错误库 46 中以备其它类似节点以后访问使用。相反，如果探测到了重大的交互操作性错误/问题，下载的代码或内容（与相关的错误记录）一起将被存储到代码和错误库 46 中，以避免对今后相同节点或类似节点发出类似请求做出响应时，重复仿真过程。

当然，应当理解，前面的描述是通过举例进行的在本发明范围内可以对一些细节进行修改。比如，利用中间仿真设备的构思：通常为虚拟机的形式（在代码内被完全支持），可以被应用到供中心节点使用的所有软件或内容上。“第三方数据库”，“外围实体”或类似的术语应该被认为在更广泛的含义，包含（必需的或当上下文要求时）加载第三方 CD-ROM（或类似的东西）到中心节点，以用于后续的基于需求驱动的传播。因此，软件的可交互操作性可以被本发明评估，从而（通过在早期的，离线状态下识别潜在的不兼容的/有害的代码的能力）提供改善的软件升级。因此，用户在接收软件升级时可以有信心的认为，他们的定户单元与这个新软件是兼容的，并且所有的后续错误一般可以归咎于硬件功能错误。

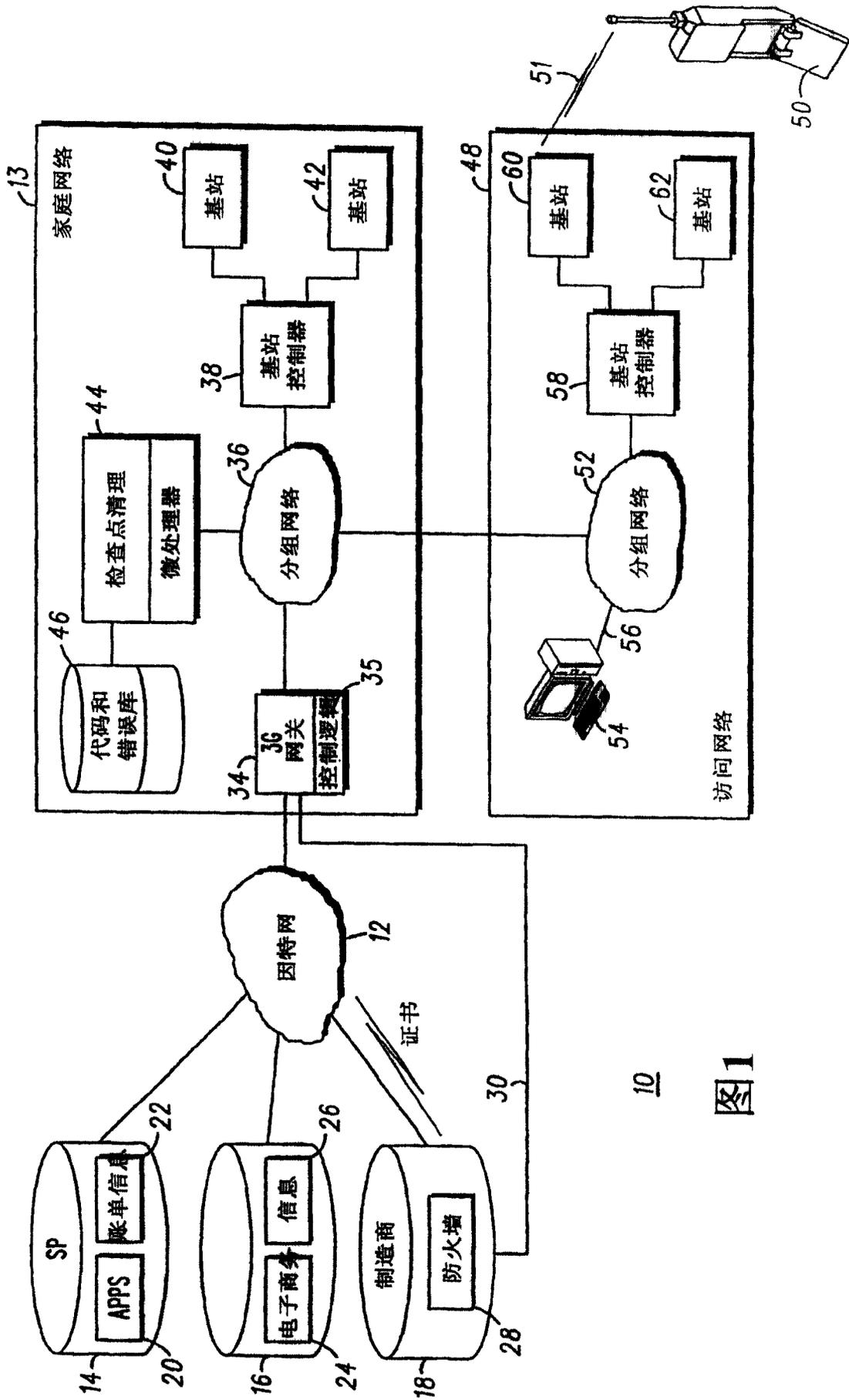


图1

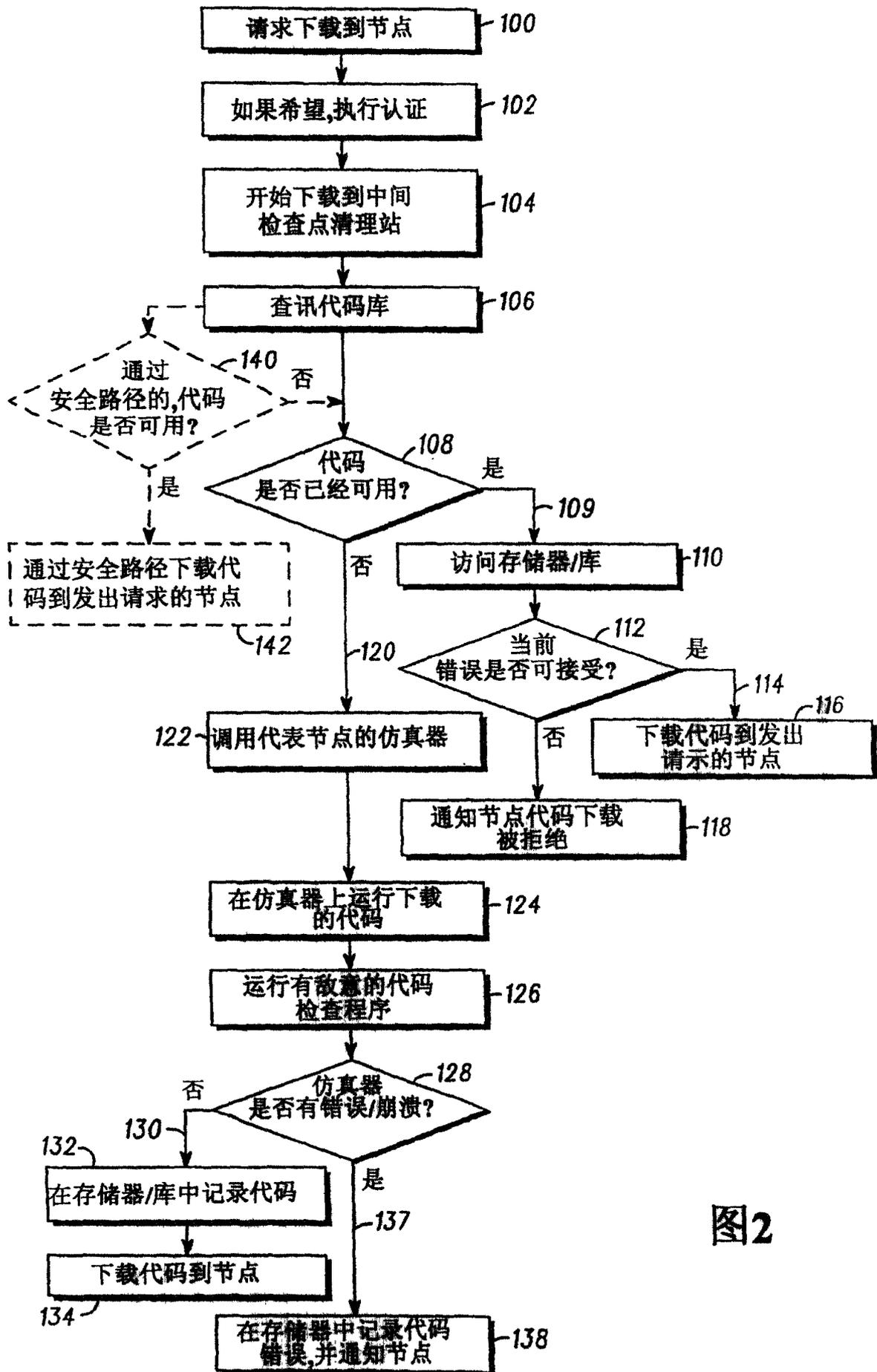


图2