(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 101822016 A
(43)申请公布日 2010.09.01

(21)申请号 200880109191.8

(22)申请日 2008.09.13

(30)优先权数据
102007045909.4 2007.09.26 DE

(85)PCT申请进入国家阶段日
2010.03.26

(86)PCT申请的申请数据
PCT/EP2008/007582 2008.09.13

(87)PCT申请的公布数据
WO2009/043435 DE 2009.04.09

(71)申请人 T-移动国际股份公司
地址 德国波恩

(72)发明人 M·罗伯克

(74)专利代理机构 中国国际贸易促进委员会专利商标事务所 11038
代理人 赵冰

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

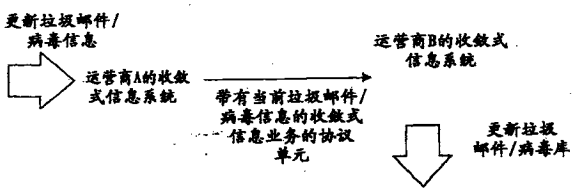
权利要求书 1 页 说明书 2 页 附图 1 页

(54)发明名称

在移动无线网中阻止病毒/垃圾邮件的方法

(57)摘要

本发明涉及一种用于在移动无线网中阻止病毒/垃圾邮件的方法，该移动无线网包含传输协议数据的收敛式信息业务，该方法的特征在于，在所述收敛式信息业务的协议中建立这样的功能：该功能允许在一个网络运营商或者不同网络运营商(A,B,C....N)的网络单元之间交换病毒和/或垃圾邮件信息。本发明的任务是提供一种用于收敛式信息系统的方法，其允许突破网络和平台的限制进行病毒和垃圾邮件信息的交换，以便在该处阻止病毒和垃圾邮件的大量发送。



CN 101822016 A

1. 一种用于在移动无线网中阻止病毒 / 垃圾邮件的方法，该移动无线网包含传输协议数据的收敛式信息业务，其特征在于，在所述收敛式信息业务的协议中建立这样的功能：该功能允许在一个网络运营商或者不同网络运营商 (A，B，C....N) 的网络单元之间交换病毒和 / 或垃圾邮件信息。

2. 根据权利要求 1 的方法，其特征在于，各个网络运营商 (A，B，C....N) 在其网络单元中连续地更新诸如病毒特征的关于病毒的信息和 / 或诸如发送方列表等的关于垃圾邮件的信息。

3. 根据权利要求 1 或 2 的方法，其特征在于，所述病毒和 / 或垃圾邮件信息被分配给自身的网络或其他运营商的所有成员系统或一部分成员系统。

4. 根据权利要求 1 至 3 中任一项的方法，其特征在于，接收方的系统根据由接收方所定义的特定标准判断所述病毒和 / 或垃圾邮件信息是否被记录在自身的病毒 / 垃圾邮件库中。

5. 根据权利要求 1 至 4 中任一项的方法，其特征在于，所述病毒和 / 或垃圾邮件信息通过发送该病毒和 / 或垃圾邮件信息的信息业务的中介功能被自动分配给所有与该功能相关的运营商。

在移动无线网中阻止病毒 / 垃圾邮件的方法

技术领域

[0001] 本发明涉及一种如权利要求 1 的前序部分所述的在移动无线网中阻止病毒 / 垃圾邮件的方法，该移动无线网具有收敛式信息业务，所述收敛式信息业务由“开放移动联盟 (Open Mobile Alliance)”标准化。

背景技术

[0002] 在今天的计算机网络、如互联网中，电脑病毒和垃圾邮件（大量发送接收方不希望收到的信息，如广告邮件）成为越来越严重的问题。由此，电子邮件业务的运营商以及互联网服务运营商试图通过本地解决方案来克服这样的问题。

[0003] 在未来的移动无线网中也很可能大量出现类似的问题，因为在今天的移动无线网中所提供的信息业务以及在不远的将来可能出现的信息业务（如收敛式信息系统）在功能范围方面越来越近似于互联网的业务范围。

[0004] 目前，前面所述的问题是专门针对特定的运营商或平台而解决的。但还没有跨网络运营商或跨平台的解决方案。

[0005] 由同一申请人所提交的德国专利申请 DE10226744B4 涉及一种用于在向和从移动通信网的用户终端设备传送信息时提供安全功能的方法和装置。在该移动通信网的网络节点中的一个装置内，执行对来自或发往用户终端设备的数据流的实时分析，其中数据通过事先由用户或者网络运营商 / 提供商所定义的内容而被识别和转发。由此使得该终端设备和连接在其上的用户设备受到保护，以免受到外部攻击。然而缺点在于，数据必须事先由用户或者网络运营商 / 提供商来规定，以确保可能实现的最佳保护。但为此需要附加的成本高昂的硬件 / 软件，另外，对此也不能立即识别出存在危险的数据（病毒 / 垃圾邮件），因此存在危险的数据可能在接收方的网络中以及经由接收方的网络和与之相连的网络而被传播。

发明内容

[0006] 本发明的任务是提供一种用于收敛式信息系统的方法，其允许突破网络和平台的限制进行病毒和垃圾邮件信息的交换，以便在该处阻止病毒和垃圾邮件的大量发送。

[0007] 权利要求 1 所述的特征用于解决所提出的问题。

[0008] 本发明的基本思想是基于在收敛式信息业务的协议中建立功能，该功能允许在一个网络运营商或者不同的网络运营商的网络单元之间交换病毒或垃圾邮件信息。

[0009] 通过使各个网络运营商在其网络单元中连续地更新关于病毒的信息（如病毒特征）和关于垃圾邮件的信息（发送者列表等），根据本发明，借助“收敛式信息业务”的协议单元，将这些信息分配给（自身网络或其他运营商的）所有成员系统或一部分成员系统。

[0010] 然后，接收方系统可以借助由接收方所定义的特定标准来判断该信息是否记录在自身的病毒 / 垃圾邮件库中。

[0011] 这种“相互结合”的优点在于，通过交换垃圾邮件 / 病毒信息，已经可以阻止病毒

/ 垃圾邮件在原网络中的传播，并避免其传输到其它网络中。

[0012] 另外，根据本发明建议：借助于相应的协议单元，上述病毒 / 垃圾邮件信息也可以通过所谓的中介功能 (broker function) 被自动分配给所有与该功能相关的运营商。

附图说明

[0013] 下面借助仅示出一种实施方式的附图详细描述本发明。这里由附图及其描述得出本发明的重要特征以及本发明的优点。

[0014] 如图所示：

[0015] 图 1 第一个收敛式信息系统 A 的垃圾邮件 / 病毒数据向第二个收敛式信息系统 B 的传送。

[0016] 图 2 第一个收敛式信息系统 A 的垃圾邮件 / 病毒数据借助“中介功能”向运营商 A，B，C...N 的多个收敛式信息系统的传送。

具体实施方式

[0017] 在图 1 中示出了运营商 A 的第一个收敛式信息系统的垃圾邮件 / 病毒向运营商 B 的第二个收敛式信息系统的传送，其中该传送通过收敛式信息业务的一个协议单元以当前的垃圾邮件 / 病毒信息来实现。

[0018] 随后，在运营商 B 的接收所述垃圾邮件 / 病毒信息的信息系统中，该垃圾邮件 / 病毒信息自动地或者经过特殊过滤后作为更新被记录在其垃圾邮件 / 病毒库中。

[0019] 在图 2 中示出了运营商 A 的第一个收敛式信息系统的垃圾邮件 / 病毒数据借助“中介功能”向运营商 B，C，D... 至 N 的多个收敛式信息系统的传送。

[0020] 该传送通过收敛式信息业务的一个协议单元以当前的垃圾邮件 / 病毒信息来实现，通过发送该垃圾邮件 / 病毒信息的运营商 A 的信息系统的中介功能被自动传送到所有连接在后的、接收该垃圾邮件 / 病毒信息的运营商 B，C，D... 至 N 的信息系统中。在所述中介功能中，接收垃圾邮件 / 病毒信息的运营商 B，C，D... 至 N 的信息系统详细定义了还应当将该垃圾邮件 / 病毒信息的那些部分发送给运营商 B，C，D... 至 N 的相应信息系统。

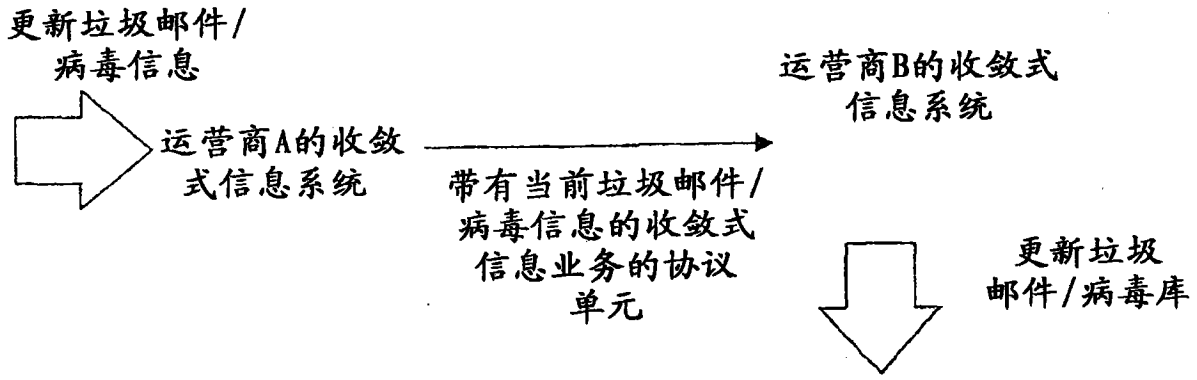

更新垃圾邮件/
病毒信息
运营商A的收敛
式信息系统
带有当前垃圾邮件/
病毒信息的收敛式
信息业务的协议
单元
运营商B的收敛式
信息系统
更新垃圾
邮件/病毒库

图 1

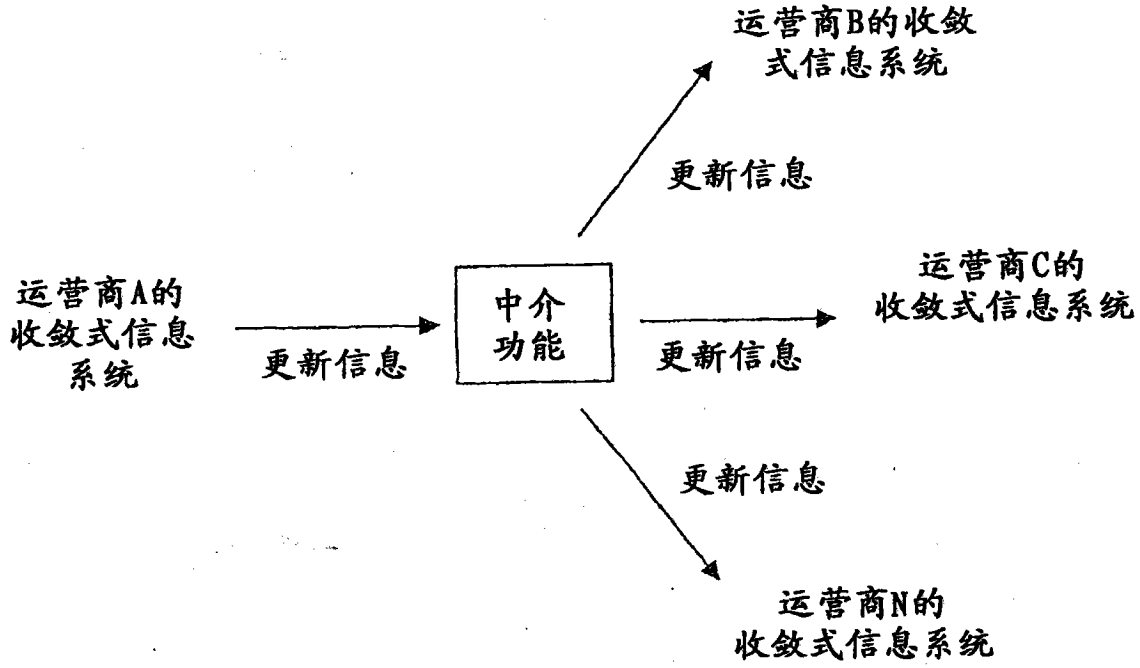

运营商B的收敛
式信息系统
更新信息
运营商A的
收敛式信息
系统
更新信息
中介
功能
更新信息
运营商C的
收敛式信息系统
更新信息
运营商N的
收敛式信息系统

图 2