(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 103139041 A
(43)申请公布日 2013.06.05

(21)申请号 201110375849.3

(22)申请日 2011.11.23

(71)申请人 中兴通讯股份有限公司
地址 518057 广东省深圳市南山区科技南路55号

(72)发明人 陈军 陶伟成 姚立哲

(74)专利代理机构 北京康信知识产权代理有限责任公司 11240
代理人 余刚 梁丽超

(51)Int.Cl.
H04L 12/58(2006.01)
H04L 29/06(2006.01)

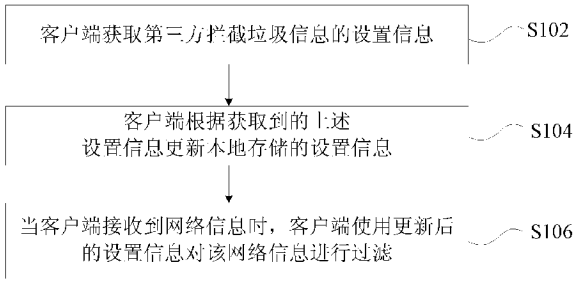
权利要求书3页 说明书12页 附图6页

(54)发明名称

信息过滤的方法、转发信息的处理方法、装置及系统

(57)摘要

本发明公开了一种信息过滤的方法、转发信息的处理方法、装置及系统。其中，该信息过滤方法包括：客户端获取第三方拦截垃圾信息的设置信息；客户端根据该设置信息更新本地存储的设置信息；当客户端接收到网络信息时，使用更新后的设置信息对该网络信息进行过滤。通过本发明，客户端根据获取到的第三方拦截垃圾信息的设置信息更新本地存储的设置信息，当接收到网络信息时，客户端使用更新后的设置信息对该网络信息进行过滤。解决了相关技术中过滤垃圾信息的效率较低的问题，该方式扩充了客户端的设置信息，提高过滤垃圾信息的成功率，提升用户体验。



CN 103139041 A

1. 一种信息过滤的方法，其特征在于包括：

客户端获取第三方拦截垃圾信息的设置信息；其中，所述第三方是除所述客户端以外的其他一个或多个设备；

所述客户端根据获取到的所述设置信息更新本地存储的设置信息；

当所述客户端接收到网络信息时，所述客户端使用更新后的所述设置信息对所述网络信息进行过滤。

2. 根据权利要求 1 所述的方法，其特征在于，所述其他一个或多个设备为服务器或指定客户端。

3. 根据权利要求 1 或 2 所述的方法，其特征在于，所述设置信息包括：黑名单和 / 或垃圾信息处理规则。

4. 根据权利要求 3 所述的方法，其特征在于，当所述设置信息为黑名单和垃圾信息处理规则时，所述客户端使用更新后的所述设置信息对所述网络信息进行过滤包括：

所述客户端检测所述网络信息的发送方是否在所述黑名单中，如果是，确定所述网络信息为垃圾信息；如果否，所述客户端检测所述网络信息中是否有与所述垃圾信息处理规则匹配的关键字；

如果有匹配的关键字，所述客户端确定所述网络信息为垃圾信息。

5. 根据权利要求 1 所述的方法，其特征在于，

所述客户端接收的所述网络信息为发送方转发的网络信息时，所述方法还包括：所述发送方或服务器将所述发送方标识和所述网络信息的原发送方标识添加在所述网络信息的信息头中；

所述客户端使用更新后的所述设置信息对所述网络信息进行过滤包括：所述客户端接收到来自所述发送方转发的网络信息时，使用所述客户端本地存储的设置信息对所述网络信息的信息头中的所述发送方标识和所述原发送方标识进行过滤。

6. 一种信息过滤的方法，其特征在于包括：

服务器接收来自客户端的获取设置信息的请求消息；

所述服务器将第三方拦截垃圾信息的设置信息添加到所述服务器本地的所述客户端对应的存储区；其中，所述第三方是除所述客户端以外的其他一个或多个设备；

所述服务器向所述客户端转发网络信息时，使用所述存储区中的设置信息对所述网络信息进行过滤。

7. 根据权利要求 6 所述的方法，其特征在于，所述请求消息为请求指定客户端的设置信息；所述服务器将第三方拦截垃圾信息的设置信息添加所述服务器本地的所述客户端对应的存储区包括：

所述服务器在所述服务器本地查找所述指定客户端对应的设置信息，将查找到的所述设置信息添加到所述服务器本地的所述客户端对应的存储区。

8. 根据权利要求 6 或 7 所述的方法，其特征在于，所述设置信息包括：黑名单和 / 或垃圾信息处理规则。

9. 根据权利要求 8 所述的方法，其特征在于，当所述设置信息为所述黑名单和所述垃圾信息处理规则时，所述服务器使用所述存储区中的设置信息对所述网络信息进行过滤包括：

所述服务器检测所述网络信息的发送方是否在所述黑名单中，如果是，确定所述网络信息为垃圾信息；如果否，所述服务器检测所述网络信息中是否有与所述垃圾信息处理规则匹配的关键字；

如果有匹配的关键字，所述服务器确定所述网络信息为垃圾信息。

10. 根据权利要求 6 所述的方法，其特征在于，

当所述网络信息为来自转发方转发的信息时，所述网络信息中携带有所述转发方的标识和原发送方的标识；

所述服务器使用所述存储区中的设置信息对所述网络信息进行过滤包括：所述服务器检测所述转发方的标识和 / 或所述原发送方的标识是否在所述设置信息中；如果所述转发方的标识和所述原发送方的标识中有一个在所述设置信息中，则确定所述网络信息为垃圾信息。

11. 一种转发信息的处理方法，其特征在于包括：

当发送方向接收方转发网络信息时，所述发送方或服务器将所述发送方标识和所述网络信息的原发送方标识添加在所述网络信息的信息头中，转发所述网络信息；

所述接收方接收到来自所述发送方转发的网络信息时，使用所述接收方本地存储的设置信息对所述网络信息的信息头中的所述发送方标识和所述原发送方标识进行过滤。

12. 一种信息过滤的客户端设备，其特征在于包括：

获取模块，用于获取第三方拦截垃圾信息的设置信息；其中，所述第三方是除所述客户端设备以外的其他一个或多个设备；

存储模块，用于根据所述获取模块获取的所述设置信息更新本地存储的设置信息；过滤模块，用于当接收到网络信息时，使用所述存储模块在本地存储的更新后的所述设置信息对所述网络信息进行过滤。

13. 根据权利要求 12 所述的客户端设备，其特征在于，所述获取模块还包括：

第三获取单元，用于获取第三方拦截垃圾信息的黑名单和 / 或垃圾信息处理规则，将所述黑名单和 / 或垃圾信息处理规则作为自身的设置信息。

14. 一种信息过滤的服务器，其特征在于包括：

请求消息接收模块，用于接收来自客户端的获取设置信息的请求消息；

设置信息添加模块，用于将第三方拦截垃圾信息的设置信息添加到所述服务器本地的所述客户端对应的存储区；其中，所述第三方是除所述客户端以外的其他一个或多个设备；

过滤模块，用于向所述客户端转发网络信息时，使用所述设置信息添加模块在所述存储区中添加的设置信息对所述网络信息进行过滤。

15. 根据权利要求 14 所述的服务器，其特征在于，所述请求消息接收模块包括：

请求消息接收单元，用于接收来自客户端的获取设置信息为黑名单和 / 或垃圾信息处理规则的请求消息。

16. 根据权利要求 14 所述的服务器，其特征在于，所述过滤模块包括：

检测单元，用于所述网络信息为来自转发方转发的信息，且所述网络信息中携带有所述转发方的标识和原发送方的标识时，检测所述转发方的标识和 / 或所述原发送方的标识是否在所述设置信息中；

确定单元，用于在所述转发方的标识和所述原发送方的标识中有一个在所述设置信息中的情况下，确定所述网络信息为垃圾信息。

17. 一种转发信息的处理系统，其特征在于包括：发送方装置和接收方装置；

所述发送方装置包括：标识添加模块，用于当向接收方装置转发网络信息时，将所述发送方装置对应的发送方标识和所述网络信息的原发送方标识添加在所述网络信息的信息头中；转发模块，用于将所述标识添加模块添加标识后的所述网络信息转发给所述接收方装置；

所述接收方装置包括：接收模块，用于接收到来自所述发送方装置转发的网络信息；过滤模块，用于使用所述接收方装置本地存储的设置信息对所述接收模块接收的网络信息的信息头中的所述发送方标识和所述原发送方标识进行过滤。

信息过滤的方法、转发信息的处理方法、装置及系统

技术领域

[0001] 本发明涉及通信领域，具体而言，涉及一种信息过滤的方法、转发信息的处理方法、装置及系统。

背景技术

[0002] 随着信息和通讯技术的迅速发展，各种终端可以随时随地的在网络中传播各种信息。在此背景下，垃圾信息也随之而来。这些垃圾信息包括了各种情色类的视频、图片、文学等“低俗内容”，赌博、造假、诈骗等各类违反道德、法律法规的内容以及对其他网络用户的诽谤、不良评价等。这些信息不但给广大人民群众的生活造成困扰，也造成人们精神上的损失。因此，解决网络中垃圾信息的问题已经刻不容缓。

[0003] 目前，处理垃圾信息的方法主要有两种，分别是基于用户黑名单过滤的方法以及采取关键词和特征匹配的方法。前者的主要策略是：用户事先记录垃圾信息的主体（比如垃圾信息的发起者），并将其列入限制名单的方式，但是这种方法是发生在垃圾信息已经成功发送之后，并且可能需要接收方反馈相应信息才能确定该信息为垃圾信息。另外由于单个用户的黑名单往往不全面，不具备对变更后的垃圾信息主体进行处理的能力。后者的主要策略是：预先建立一个垃圾信息的特征库，当接收到新的信息时提取信息中的关键词或者特征与特征库进行比对，以此来断定此信息是否为垃圾信息，这种方法的不足之处是准确性不高，容易造成误判且效率比较低。

[0004] 针对相关技术中过滤垃圾信息的效率较低的问题，目前尚未提出有效的解决方案。

发明内容

[0005] 针对相关技术中过滤垃圾信息的效率较低的问题，本发明提供了一种信息过滤的方法、转发信息的处理方法、装置及系统，以至少解决上述问题。

[0006] 根据本发明的一个方面，提供了一种信息过滤的方法，该方法包括：客户端获取第三方拦截垃圾信息的设置信息，该第三方是除客户端以外的其他一个或多个设备；客户端根据该设置信息更新本地存储的设置信息；当客户端接收到网络信息时，客户端使用更新后的上述设置信息对该网络信息进行过滤。

[0007] 上述其他一个或多个设备为服务器或指定客户端。

[0008] 上述设置信息包括：黑名单和 / 或垃圾信息处理规则。

[0009] 当设置信息为黑名单和垃圾信息处理规则时，客户端使用更新后的设置信息对网络信息进行过滤包括：客户端检测上述网络信息的发送方是否在黑名单中，如果是，确定该网络信息为垃圾信息；如果否，客户端检测该网络信息中是否有与垃圾信息处理规则匹配的关键字；如果有匹配的关键字，客户端确定该网络信息为垃圾信息。

[0010] 上述客户端接收的网络信息为发送方转发的网络信息时，上述方法还包括：发送方或服务器将该发送方标识和该网络信息的原发送方标识添加在该网络信息的信息头中；

相应地，上述客户端使用更新后的设置信息对网络信息进行过滤包括：客户端接收到来自该发送方转发的网络信息时，使用客户端本地存储的设置信息对该网络信息的信息头中的该发送方标识和原发送方标识进行过滤。

[0011] 根据本发明的另一个方面，提供了一种信息过滤的方法，包括：服务器接收来自客户端的获取设置信息的请求消息；服务器将第三方拦截垃圾信息的设置信息添加到服务器本地的客户端对应的存储区；其中，第三方是除客户端以外的其他一个或多个设备；服务器向客户端转发网络信息时，使用存储区中的设置信息对网络信息进行过滤。

[0012] 上述请求消息为请求指定客户端的设置信息；服务器将第三方拦截垃圾信息的设置信息添加服务器本地的客户端对应的存储区包括：服务器在服务器本地查找指定客户端对应的设置信息，将查找到的设置信息添加到服务器本地的客户端对应的存储区。

[0013] 上述设置信息包括：黑名单和/或垃圾信息处理规则。

[0014] 当设置信息为黑名单和垃圾信息处理规则时，服务器使用存储区中的设置信息对网络信息进行过滤包括：服务器检测网络信息的发送方是否在黑名单中，如果是，确定网络信息为垃圾信息；如果否，服务器检测网络信息中是否有与垃圾信息处理规则匹配的关键字；如果有匹配的关键字，服务器确定网络信息为垃圾信息。

[0015] 当网络信息为来自转发方转发的信息时，网络信息中携带有转发方的标识和原发送方的标识；上述服务器使用存储区中的设置信息对网络信息进行过滤包括：服务器检测转发方的标识和/或原发送方的标识是否在设置信息中；如果转发方的标识和原发送方的标识中有一个在设置信息中，则确定网络信息为垃圾信息。

[0016] 根据本发明的再一方面，提供了一种信息过滤的客户端设备，该客户端设备包括：获取模块，用于获取第三方拦截垃圾信息的设置信息；存储模块，用于将该设置信息存储在本地；过滤模块，用于当接收到网络信息时，使用本地存储的上述设置信息对该网络信息进行过滤。

[0017] 上述获取模块还包括：第三获取单元，用于获取第三方拦截垃圾信息的黑名单和/或垃圾信息处理规则，将黑名单和/或垃圾信息处理规则作为自身的设置信息。

[0018] 根据本发明的又一方面，提供了一种信息过滤的服务器，该服务器包括：请求消息接收模块，用于接收来自客户端的获取设置信息的请求消息；第一设置信息添加模块，用于将第三方拦截垃圾信息的设置信息添加到本地的客户端对应的存储区；过滤模块，用于向客户端转发网络信息时，使用上述存储区中的设置信息对该网络信息进行过滤。

[0019] 上述请求消息接收模块包括：请求消息接收单元，用于接收来自客户端的获取设置信息为黑名单和/或垃圾信息处理规则的请求消息。

[0020] 上述过滤模块包括：检测单元，用于网络信息为来自转发方转发的信息，且网络信息中携带有转发方的标识和原发送方的标识时，检测转发方的标识和/或原发送方的标识是否在设置信息中；确定单元，用于在转发方的标识和原发送方的标识中有一个在设置信息中的情况下，确定网络信息为垃圾信息。

[0021] 根据本发明的还一方面，提供了一种转发信息的处理方法，包括：当发送方向接收方转发网络信息时，该发送方或服务器将发送方标识和该网络信息的原发送方标识添加在该网络信息的信息头中，转发网络信息；接收方接收到来自发送方转发的网络信息时，使用接收方本地存储的设置信息对该网络信息的信息头中的上述发送方标识和原发送方标识

进行过滤。

[0022] 根据本发明的又一方面，提供了一种转发信息的处理系统，包括：发送方装置和接收方装置；其中，该发送方装置包括：标识添加模块，用于当向接收方装置转发网络信息时，将该发送方装置对应的发送方标识和网络信息的原发送方标识添加在网络信息的信息头中；转发模块，用于将标识添加模块添加标识后的网络信息转发给接收方装置；该接收方装置包括：接收模块，用于接收到来自发送方装置转发的网络信息；过滤模块，用于使用该接收方装置本地存储的设置信息对接收模块接收的网络信息的信息头中的发送方标识和原发送方标识进行过滤。

[0023] 通过本发明，根据第三方拦截垃圾信息的设置信息对网络信息进行过滤，能够比较准确地排除垃圾信息，加快了本地设置信息的更新速度，解决了相关技术中过滤垃圾信息的效率较低的问题，并提高过滤垃圾信息的成功率，因此，提升用户体验度。

附图说明

[0024] 此处所说明的附图用来提供对本发明的进一步理解，构成本申请的一部分，本发明的示意性实施例及其说明用于解释本发明，并不构成对本发明的不当限定。在附图中：

[0025] 图 1 是根据本发明实施例的信息过滤的方法的流程图；

[0026] 图 2 是根据本发明实施例的扩充的黑名单存储在本地的流程图；

[0027] 图 3 是根据本发明实施例的信息过滤的方法的另一种流程图；

[0028] 图 4 是根据本发明实施例的扩充的黑名单存储在服务器的流程图；

[0029] 图 5 是根据本发明实施例的信息过滤的客户端设备的结构框图；

[0030] 图 6 是根据本发明实施例的信息过滤的客户端设备的另一种结构框图；

[0031] 图 7 是根据本发明实施例的信息过滤的客户端设备的再一种结构框图；

[0032] 图 8 是根据本发明实施例的信息过滤的服务器的结构框图；

[0033] 图 9 是根据本发明实施例的信息过滤的服务器的另一种结构框图；

[0034] 图 10 是根据本发明实施例的信息过滤的服务器的再一种结构框图；

[0035] 图 11 是根据本发明实施例一的信息过滤的方法的流程图；

[0036] 图 12 是根据本发明实施例二的信息过滤的方法的流程图；

[0037] 图 13 是根据本发明实施例三的信息过滤的方法的流程图；

[0038] 图 14 是根据本发明实施例四的信息过滤的方法的流程图；

[0039] 图 15 是根据本发明实施例的转发信息的处理系统的结构框图。

具体实施方式

[0040] 下文中将参考附图并结合实施例来详细说明本发明。需要说明的是，在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互组合。

[0041] 本发明实施例考虑到基于用户自身的黑名单或过滤规则（也可以称为垃圾信息处理规则）对垃圾信息进行过滤的方式，容易造成误判且过滤垃圾信息的效率较低，提供了一种信息过滤的方法、转发信息的处理方法、装置（如客户端设备和服务器）及系统。下面通过实施例进行详细说明。

[0042] 本实施例提供了一种信息过滤的方法，该方法可以在客户端实现，如图 1 所示的

信息过滤的方法流程图，该方法包括以下步骤（步骤 S102- 步骤 S106）：

[0043] 步骤 S102，客户端获取第三方拦截垃圾信息的设置信息；其中，该第三方是除客户端以外的其他一个或多个设备；

[0044] 步骤 S104，客户端根据获取到的上述设置信息更新本地存储的设置信息；

[0045] 步骤 S106，当客户端接收到网络信息时，客户端使用更新后的设置信息对该网络信息进行过滤。

[0046] 通过上述步骤，客户端获取第三方拦截垃圾信息的设置信息并更新本地存储的设置信息，通常是添加到本地原先存储的设置信息中。当接收到网络信息时，客户端使用更新后的设置信息对该网络信息进行过滤，解决了相关技术中过滤垃圾信息的效率较低的问题，该方式扩充了客户端的设置信息，提高过滤垃圾信息的成功率，提升用户体验。

[0047] 步骤 S102 可以根据设定的周期进行获取设置信息，以达到周期的更新本地设置信息的目的，提高更新本地设置信息的效率。

[0048] 上述客户端获取到的第三方拦截垃圾信息的设置信息，可以是黑名单和 / 或垃圾信息处理规则。黑名单机制是对信息发送主体进行过滤，采用黑名单时，检测接收到的信息的发送方标识是否在黑名单中，以此来判断是否是垃圾信息。垃圾信息处理规则通常是对信息的内容进行过滤，垃圾信息处理规则可以是垃圾信息的过滤条件、垃圾信息的过滤规则、垃圾信息的判定条件。例如建立垃圾信息特征库（如关键性的文字、图形 / 图像、声音等），该特征库中存储有常见的垃圾信息特征 / 关键词，当客户端接收到新的信息时，客户端先提取该信息中的信息特征 / 关键词，再将该信息特征 / 关键词与特征库进行对比，以此来判断该信息是否是垃圾信息。或者客户端检测接收到的信息中是否包含垃圾信息特征库中的信息特征 / 关键词，以此来判断是否是垃圾信息。如果是垃圾信息，则对该垃圾信息进行过滤、拦截，不直接显示给用户，可以删除垃圾信息或存放在专门区域。

[0049] 上述客户端从其他一个或多个设备获取到设置信息，该其他一个或多个设备可以是服务器或指定客户端。客户端可以从服务器获取到第三方拦截垃圾信息的设置信息，该第三方可以包括以下至少之一：网络上的客户端、网络用户、网络上的服务器。例如，微博客户端通过微博服务器订阅了某个安全软件公司提供的垃圾处理规则，就可以获取这个安全软件公司服务器提供的垃圾处理规则并可定期更新。网络上的客户端可以是网络用户的业务客户端，比如 QQ 客户端、Email 邮件客户端、移动终端客户端等。客户端可以共享第三方拦截垃圾信息的设置信息。例如 QQ 用户通过客户端获取用户指定的 QQ 好友客户端的设置信息。

[0050] 客户端通过共享第三方的黑名单来扩充黑名单，通过扩充黑名单，从而更加全面的处理垃圾信息。客户端对垃圾信息处理规则的扩充方法与黑名单的扩充方法一样。扩充后的黑名单和 / 或垃圾信息处理规则可以存储在本地，扩充后的黑名单存储在本地的处理流程如图 2 所示：

[0051] 步骤 S202，客户端向服务器请求获取第三方黑名单；

[0052] 步骤 S204，服务器向客户端响应上述请求的第三方黑名单；

[0053] 步骤 S206，客户端将获取到的第三方黑名单添加到本地存储的扩充黑名单中。

[0054] 扩充后的黑名单可用来对垃圾信息进行过滤，过滤的具体方法可采用现有的技术方法来解决，这里不再赘述。同样的，扩充后的垃圾信息处理规则存储在本地的处理流程也

是如此，在此不再赘述。

[0055] 当上述存储在本地的设置信息为黑名单和垃圾信息处理规则时，客户端使用更新后的设置信息对接收到的网络信息进行过滤：首先，客户端检测该网络信息的发送方是否在黑名单中；其次，如果该网络信息的发送方在此黑名单中，则确定该网络信息为垃圾信息，如果该网络信息的发送方不在此黑名单中，客户端检测网络信息中是否有与上述垃圾信息处理规则匹配的关键字；再者，如果网络信息中有与上述垃圾信息处理规则匹配的关键字，客户端确定该网络信息为垃圾信息。对于不能确定是否是垃圾信息的网络信息，通常简单地按正常信息处理，或者提示用户处理，或者检测信息发送方是否在白名单中，以此判断是好友信息还是陌生信息。

[0056] 如果客户端接收到由转发方转发的网络信息，假设该网络信息的原发送方位于客户端的黑名单中，而转发方不在该黑名单中，此时很容易造成误判，没有过滤掉此垃圾信息，对于这种情况，可以在该网络信息中携带转发方的标识和原发送方的标识，客户端检测转发方的标识和 / 或原发送方的标识是否在客户端的黑名单中，如果转发方的标识和原发送方的标识中有一个在该黑名单中，则确定该网络信息的发送方在黑名单中，即可判定该网络信息是垃圾信息，并过滤掉该垃圾信息。

[0057] 如果客户端接收的网络信息为发送方转发的网络信息，上述方法还包括：发送方或服务器将发送方标识和网络信息的原发送方标识添加在网络信息的信息头中；相应地，该客户端使用更新后的设置信息对网络信息进行过滤包括：客户端接收到来自上述发送方转发的网络信息时，使用该客户端本地存储的设置信息对网络信息的信息头中的发送方标识和原发送方标识进行过滤。

[0058] 上述黑名单可以包括至少以下方式之一：电话号码、Email 地址、客户端 ID(identity，标识)，网络用户 ID、网络地址统一资源定位符 (Uniform Resource Locator，简称为 URL)、终端的媒体访问控制 (Media Access Control，简称为 MAC) 地址、终端网协 (Internet Protocol，简称为 IP) 地址、国际移动装备识别码 (International Mobie Equipment Identity，简称为 IMEI) 号、IMEI TAC(设备型号核准号码) 号、终端 user-agent(用户代理) 参数等标识。因此本发明适用于对语音呼叫、SMS、MMS、Email、多媒体邮件、及时消息、网络消息等网络信息进行过滤。

[0059] 本实施例还提供了一种转发机制，该转发机制中对转发信息的信息头进行了新的设置，下面以发送方向接收方转发网络信息为例进行说明：当发送方向接收方转发网络信息时，该发送方或服务器将发送方标识和网络信息的原发送方标识添加在该网络信息的信息头中，转发添加标识后的网络信息；接收方接收到来自上述发送方转发的网络信息时，使用接收方本地存储的设置信息对信息头中的发送方标识和原发送方标识进行过滤。其中，这里接收方本地存储的设置信息可以仅为其黑名单，当然接收方的黑名单也可以是通过上述方法扩充后的黑名单，即不仅包括接收方自身的黑名单，还可以包括从第三方获取的黑名单。

[0060] 上述网络信息的信息头中的发送方标识为该发送方对应的用户的标识，原发送方标识包括该发送方之前转发该网络信息的用户的标识和该网络信息的最初发送者的标识。因此，相对于当前的发送方而言，之前转发该网络信息的转发方均视作为该网络信息的原发送方。另外，上述发送方标识和网络信息的原发送方标识的添加可以由上述发送方完成，

也可以由发送方 / 接收方的服务器完成。

[0061] 本实施例还提供了另一种信息过滤的方法，该方法可以在服务器侧实现，如图 3 所示的是信息过滤方法的另一种流程图，该方法包括以下步骤（步骤 S302- 步骤 S306）：

[0062] 步骤 S302，服务器接收来自客户端的获取设置信息的请求消息；

[0063] 步骤 S304，服务器将第三方拦截垃圾信息的设置信息添加到服务器本地的客户端对应的存储区；其中，该第三方是除客户端以外的其他一个或多个设备；

[0064] 步骤 S306，服务器向客户端转发网络信息时，使用上述存储区中的设置信息对该网络信息进行过滤。

[0065] 通过本发明，服务器接收来自客户端的获取设置信息的请求消息后，将第三方拦截垃圾信息的设置信息添加到服务器本地的客户端对应的存储区，服务器使用该存储区中的设置信息对网络信息进行过滤，解决了相关技术中过滤垃圾信息的效率较低的问题，该方式扩充了客户端在服务器上的设置信息，提高过滤垃圾信息的成功率，提升用户体验。

[0066] 如果客户端想要获取另一指定客户端的设置信息，即上述请求消息为请求指定客户端的设置信息，服务器在本地查找该指定客户端对应的设置信息，将查找到的设置信息添加到客户端在服务器上的对应的存储区。或者服务器向指定客户端发送该设置信息的请求消息，并接收指定客户端的设置信息，再将设置信息添加到客户端在服务器上的对应的存储区。通过这种方式，客户端获取到指定客户端的设置信息，扩充了自身在服务器上的设置信息，为提高过滤垃圾信息的成功率提供了条件。

[0067] 当请求的设置信息是第三方服务器的设置信息时，服务器向第三方服务器转发该设置信息的请求消息，并接收第三方服务器的设置信息，将设置信息添加到客户端在服务器上的对应的存储区。

[0068] 与上述实施例相同，这里的设置信息也可以包括：黑名单和 / 或垃圾信息处理规则。

[0069] 客户端通过共享第三方的黑名单来扩充黑名单和 / 或垃圾信息处理规则，通过扩充黑名单和 / 或垃圾信息处理规则，从而更加全面的处理垃圾信息。扩充后的黑名单和 / 或垃圾信息处理规则可以如上所示存储在本地，也可以存储在服务器，扩充后的黑名单存储在服务器的处理流程如图 4 所示：

[0070] 步骤 S402，客户端在服务器上创建黑名单；

[0071] 步骤 S404，客户端向服务器发送获取第三方黑名单的请求消息；

[0072] 步骤 S406，服务器将第三方黑名单添加到上述客户端在服务器本地创建的黑名单中。

[0073] 扩充后的黑名单可用来对垃圾信息进行过滤，过滤的具体方法可采用现有的技术方法来解决，这里不再赘述。同样的，扩充后的垃圾信息处理规则存储在服务器的处理流程也是如此，在此不再赘述。

[0074] 当上述设置信息为黑名单和垃圾信息处理规则时，服务器使用存储区中的设置信息对要转发的网络信息进行过滤：首先，服务器检测要转发的网络信息的发送方是否在上述黑名单中；其次，如果该网络信息的发送方在黑名单中，则确定该网络信息为垃圾信息，如果该发送方不在黑名单中，服务器检测该网络信息中是否有与上述垃圾信息处理规则匹配的关键字；如果该网络信息中有与上述垃圾信息处理规则有匹配的关键字，服务器确定

该网络信息是垃圾信息。在服务器确定要转发的网络信息是垃圾信息之后，拦截该垃圾信息，以免该垃圾信息被发送至客户端。对于不能确定是否是垃圾信息的网络信息，通常简单地按正常信息处理，或者提示用户处理，或者检测信息发送方是否在白名单中，以此判断是好友信息还是陌生信息。

[0075] 如果服务器将要转发给客户端的网络信息是由转发方转发的信息时，假设该网络信息的原发送方位于服务器的黑名单中，而转发方不在该黑名单中，此时很容易造成误判，没有过滤掉此垃圾信息，对于这种情况，可以在该网络信息中携带转发方的标识和原发送方的标识，服务器检测转发方的标识和 / 或原发送方的标识是否在黑名单中 ；如果转发方的标识和原发送方的标识中有一个在黑名单中，则确定网络信息的发送方在黑名单中，由此可判定该网络信息是垃圾信息，服务器拦截该垃圾信息，防止将其发送至客户端。

[0076] 对应于上述在客户端实现的信息过滤的方法，本实施例提供了一种信息过滤的客户端设备，该设备用于实现上述实施例。图 5 是根据本发明实施例的信息过滤的客户端设备的结构框图，如图 5 所示，该客户端设备包括 ：获取模块 52、存储模块 54 和过滤模块 56。下面对该结构进行说明。

[0077] 获取模块 52，用于获取第三方拦截垃圾信息的设置信息 ；其中，该第三方是除所述客户端设备以外的其他一个或多个设备 ；

[0078] 存储模块 54，连接至获取模块 52，用于根据获取模块 52 获取的设置信息更新本地存储的设置信息 ；

[0079] 过滤模块 56，连接至存储模块 54，用于当接收到网络信息时，使用存储模块 54 在本地存储的更新后的设置信息对该网络信息进行过滤。

[0080] 通过上述客户端设备，存储模块 54 根据获取模块 52 获取到的第三方拦截垃圾信息的设置信息更新本地存储的设置信息，过滤模块 56 在接收到网络信息时，使用本地存储的更新后的设置信息对该网络信息进行过滤，解决了相关技术中过滤垃圾信息的效率较低的问题，该方式扩充了客户端的设置信息，提高过滤垃圾信息的成功率，提升用户体验。

[0081] 上述获取模块 52 可以从服务器或指定客户端获取第三方拦截垃圾信息的设置信息，如图 6 所示的信息过滤的客户端设备的另一种结构框图，该客户端设备除了包括上述图 5 中的各个模块之外，获取模块 52 还包括第一获取单元 522，用于从服务器获取第三方拦截垃圾信息的设置信息 ；或者，获取模块 52 包括第二获取单元，用于从指定客户端获取第三方拦截垃圾信息的设置信息，该方式未在图中示出。

[0082] 上述设置信息可以是黑名单和 / 或垃圾信息处理规则，对于这种情况，上述获取模块 52 还包括 ：第三获取单元，用于获取第三方拦截垃圾信息的设置信息为黑名单和 / 或垃圾信息处理规则的信息。

[0083] 当上述存储在本地的设置信息为黑名单和垃圾信息处理规则时，过滤模块 56 使用该设置信息对接收到的网络信息进行过滤 ：首先，检测该网络信息的发送方是否在黑名单中 ；其次，如果该网络信息的发送方在此黑名单中，则确定该网络信息为垃圾信息，如果该网络信息的发送方不在此黑名单中，检测网络信息中是否有与上述垃圾信息处理规则匹配的关键字 ；如果有匹配的关键字，确定该网络信息是垃圾信息，则拦截该垃圾信息，以达到过滤垃圾信息的目的。

[0084] 如果客户端接收到的网络信息是由转发方转发的信息时，上述客户端设备可以检

测该网络消息的转发方和原发送方是否在黑名单中，如图 7 所示的信息过滤的客户端设备的再一种结构框图，该客户端设备除了包括上述图 6 中的各个模块之外，过滤模块 56 还包括：黑名单检测单元 562 和确定单元 564。下面对该结构进行说明。

[0085] 黑名单检测单元 562，用于当设置信息包括黑名单时，如果网络信息为来自转发方转发的信息，且该网络信息中携带有转发方的标识和原发送方的标识，检测转发方的标识和 / 或原发送方的标识是否在黑名单中；

[0086] 确定单元 564，连接至黑名单检测单元 562，用于在转发方的标识和原发送方的标识中有一个在黑名单中的情况下，确定上述网络信息的发送方在黑名单中。

[0087] 对应于上述在服务器实现的信息过滤的方法，本实施例提供了一种信息过滤的服务器，该设备用于实现上述实施例。图 8 是根据本发明实施例的信息过滤的服务器的结构框图，如图 8 所示，该服务器包括：请求消息接收模块 82、设置信息添加模块 84 和过滤模块 86。下面对该结构进行说明。

[0088] 请求消息接收模块 82，用于接收来自客户端的获取设置信息的请求消息；

[0089] 设置信息添加模块 84，连接至请求消息接收模块 82，用于将第三方拦截垃圾信息的设置信息添加到本地的上述客户端对应的存储区；其中，该第三方是除客户端以外的其他一个或多个设备；

[0090] 过滤模块 86，连接至设置信息添加模块 84，用于向客户端转发网络信息时，使用设置信息添加模块 84 在存储区中添加的设置信息对该网络信息进行过滤。

[0091] 通过上述服务器，请求消息接收模块 82 接收来自客户端的获取设置信息的请求消息后，设置信息添加模块 84 将第三方拦截垃圾信息的设置信息添加到本地的客户端对应的存储区，过滤模块 86 使用该存储区中的设置信息对网络信息进行过滤，解决了相关技术中过滤垃圾信息的效率较低的问题，该方式扩充了客户端的设置信息，提高过滤垃圾信息的成功率，提升用户体验。

[0092] 请求消息接收模块 82 接收到的是来自客户端的请求消息，针对该客户端的请求消息是请求指定客户端的设置信息的情况，图 9 示出了信息过滤的服务器的另一种结构框图，该服务器除了包括上述图 8 中的各个模块之外，设置信息添加模块 84 还包括：设置信息查找单元 842 和设置信息添加单元 844。下面对该结构进行说明。

[0093] 设置信息查找单元 842，用于在请求消息为请求指定客户端的设置信息的情况下，在本地查找指定客户端对应的设置信息；

[0094] 设置信息添加单元 844，连接至设置信息查找单元 842，用于将设置信息查找单元 842 查找到的设置信息添加到本地的客户端对应的存储区。

[0095] 上述设置信息可以是黑名单和 / 或垃圾信息处理规则，对于这种情况，上述请求消息接收模块 82 还包括：请求消息接收单元，用于接收来自客户端的获取设置信息为黑名单和 / 或垃圾信息处理规则的请求消息。

[0096] 当上述存储在本地的设置信息为黑名单和垃圾信息处理规则时，过滤模块 86 使用该设置信息对接收到的网络信息进行过滤：首先，检测该网络信息的发送方是否在黑名单中；其次，如果该网络信息的发送方在此黑名单中，则确定该网络信息为垃圾信息，如果该网络信息的发送方不在此黑名单中，检测网络信息中是否有与上述垃圾信息处理规则匹配的关键字；如果有匹配的关键字，确定该网络信息是垃圾信息，则拦截该垃圾信息，以达

到过滤垃圾信息的目的。

[0097] 如果服务器将要转发的网络信息是由转发方转发的信息时，上述服务器可以检测该网络消息的转发方和原发送方是否在黑名单中，如图 10 所示的信息过滤的服务器的再一种结构框图，该服务器除了包括上述图 9 中的各个模块之外，过滤模块 86 还包括：检测单元 862 和确定单元 864。下面对该结构进行说明。

[0098] 检测单元 862，用于上述网络信息为来自转发方转发的信息，且该网络信息中携带有转发方的标识和原发送方的标识时，检测转发方的标识和 / 或原发送方的标识是否在上述设置信息（例如黑名单）中；

[0099] 确定单元 864，连接至检测单元 862，用于在转发方的标识和原发送方的标识中有一个在上述设置信息中的情况下，确定该网络信息为垃圾信息。

[0100] 下面结合优选实施例和附图对上述实施例的实现过程进行详细说明。

[0101] 实施例一

[0102] 在网络信息的接收方通过黑名单和 / 或垃圾信息处理规则（即设置信息）对接收到的网络信息进行拦截时，有时由于接收方的设置信息较少，不能拦截部分垃圾信息。对于这种情况，为了安全起见，接收方通过共享第三方黑名单和 / 或垃圾信息处理规则（即第三方拦截垃圾信息的设置信息）来扩充自己的黑名单和 / 或垃圾信息处理规则，再利用扩充的黑名单和 / 或垃圾信息处理规则对发送方发送的网络信息进行处理。扩充后的黑名单和 / 或垃圾信息处理规则可以存储在客户端本地也可以存储在服务器上，这两种存储方式的处理流程在前面已经进行了描述，在此不再赘述。

[0103] 对于上述场景，比如社交网用户拥有自己的黑名单 / 垃圾信息处理规则，并且该社交网用户在该社交网上有一群好友，其好友各自拥有他们自己的黑名单 / 垃圾信息处理规则，该社交网用户可以利用自己的黑名单 / 垃圾信息处理规则，以及好友的黑名单 / 垃圾信息处理规则和 / 或第三方黑名单 / 垃圾信息处理规则来在本地过滤接收到的网络信息。针对这种场景，本实施例提出的解决方法如图 11 所示，图 11 是根据本发明实施例一的信息过滤的方法的流程图，该方法包括如下步骤（步骤 S1102- 步骤 S1106）：

[0104] 步骤 S1102，社交网客户端向社交网服务器请求获取其社交好友的黑名单 / 垃圾信息处理规则，和 / 或第三方黑名单 / 垃圾信息处理规则；

[0105] 步骤 S1104，社交网服务器向社交网客户端提供其好友的黑名单 / 垃圾信息处理规则和 / 或第三方黑名单 / 垃圾信息处理规则；

[0106] 步骤 S1106，社交网客户端将服务器响应的黑名单 / 垃圾信息处理规则添加到在本地扩充的黑名单 / 垃圾信息处理规则库。

[0107] 通过上述方式，社交网客户端扩充了自身的黑名单 / 垃圾信息处理规则库。当有网络信息发送给该社交网客户端时，客户端根据扩充的黑名单 / 垃圾信息处理规则来对该网络信息进行处理，从而提高了过滤垃圾信息的成功率，提升了用户体验度。

[0108] 实施例二

[0109] 在上述实施例一中，社交网用户可以利用自己的黑名单 / 垃圾信息处理规则，以及好友的黑名单 / 垃圾信息处理规则和 / 或第三方黑名单 / 垃圾信息处理规则在本地过滤接收到的网络信息，本实施例介绍了在与上述实施例一相同场景下，社交网用户利用自己的黑名单 / 垃圾信息处理规则，以及好友的黑名单 / 垃圾信息处理规则和 / 或第三方黑名

单/垃圾信息处理规则在服务器过滤接收到的网络信息的方法，图12是根据本发明实施例二的信息过滤的方法的流程图，该方法包括如下步骤（步骤S1202-步骤S1208）：

[0110] 步骤S1202，社交网客户端在社交网服务器上创建黑名单/垃圾信息处理规则库。

[0111] 用户通过客户端可以在服务器上创建一个空的黑名单/垃圾信息处理规则库（便于以后添加扩充黑名单/垃圾信息处理规则）。社交网客户端还可以将本地存储的黑名单/垃圾信息处理规则发送到服务器并添加到服务器中该社交网客户端对应的黑名单/垃圾信息处理规则库中。

[0112] 步骤S1204，社交网客户端向社交网服务器请求获取其好友的黑名单/垃圾信息处理规则和/或第三方黑名单/垃圾信息处理规则。

[0113] 步骤S1206，社交网服务器将其好友的黑名单/垃圾信息处理规则库和/或第三方黑名单/垃圾信息处理规则添加到用户在社交网服务器创建的黑名单/垃圾信息处理规则库中。

[0114] 步骤S1208，社交网服务器利用黑名单/垃圾信息处理规则库对发送给社交网客户端的信息进行处理，然后将其发送给社交网客户端。

[0115] 通过上述方式，社交网客户端扩充了其在社交网服务器上创建的黑名单/垃圾信息处理规则库。当有网络信息发送给该社交网客户端时，社交网服务器根据扩充的黑名单/垃圾信息处理规则来对该网络信息进行处理，然后决定是否将该网络信息发送给社交网客户端，从而提高了过滤垃圾信息的成功率，提升了用户体验度。

[0116] 实施例三

[0117] 假设用户接收到的网络信息是由用户的好友转发的信息，而该网络信息对用户而言可能属于垃圾信息（比如该网络信息的原发送方位于用户的黑名单中），但是对于这种情况，基于现有的黑名单机制是不能对该网络信息进行拦截的。因此本实施例提出了一种信息过滤的方法，如图13所示的信息过滤的方法的流程图，该方法包括如下步骤（步骤S1302-步骤S1304）：

[0118] S1302，信息转发方将要转发的信息的原发送方标识添加到该信息中；

[0119] S1304，接收方根据转发方标识和/或原发送方标识来对信息进行过滤处理。

[0120] 通过这种发送，转发的信息包含转发方的标识和原发送方的标识，接收方接收到信息后，可以根据信息的转发方标识和/或原发送方标识来处理该信息。例如尽管转发方是用户的好友，但原发送方可能在用户的黑名单内，对于这种转发的信息，可以利用上述方式对其进行拦截，从而提高了过滤垃圾信息的成功率，提升用户的体验度。

[0121] 实施例四

[0122] 对于上述实施例三所描述的方法，假设网络用户拥有自己的黑名单和一群好友，当其好友向该网络用户转发信息时，由于好友不在其黑名单中，用户通常情况下不会过滤好友的信息，但是如果该信息对其好友来说不是垃圾信息，却有可能对该用户来说是垃圾信息，比如该信息的原发送方位于该用户的黑名单中，针对这种情况，本实施例将对接收方根据信息的转发方标识和/或原发送方标识来处理该信息的处理过程进行详细的描述，如图14所示的是信息过滤的方法的流程图，该方法包括如下步骤（步骤S1402-步骤S1404）：

[0123] 步骤S1402，信息转发方将要转发的信息的原发送方地址添加到该信息中。

[0124] 步骤S1404，接收方根据该信息中转发方地址和/或原发送方地址来对该信息进

行处理。

[0125] 例如：用户 B（邮件地址为：b@test2.com）的好友 C（邮件地址为：c@test 3.com）向用户 B 转发一封电子邮件（原发送方的地址为 a@test1.com），其中 a@test1.com 在用户 B 的黑名单内。假设现有的邮件格式（只给出了与本发明相关的部分域，具体的邮件头和邮件体格式可查阅相关的文档）如下所示：

[0126] From：" test3" <c@test3.com>

[0127] To：" test2" <b@test2.com>

[0128] Cc：

[0129] Subject：mail content

[0130] Date：Thu，25 Oct 2011 13:38:31-0800

[0131] MIME-Version：1.0

[0132] Content-Type：multipart/mixed；

[0133] Return-Path：c@test3.com

[0134] 对于这种情况，可以采用如下方式来实施，即在 From：域添加原发送方的邮件地址，则新的邮件格式为：

[0135] From：" test3" <c@test3.com>/" test1" <a@test1.com>

[0136] To：" test2" <b@test2.com>

[0137] Cc：

[0138] Subject：mail content

[0139] Date：Thu，25 Oct 2011 13:38:31-0800

[0140] MIME-Version：1.0

[0141] Content-Type：multipart/mixed；

[0142] Return-Path：c@test3.com

[0143] 当接收方用户 B（邮件地址为：b@test2.com）的服务器（test2）接收到该邮件后，提取 From：域" /" 后的原地址来与黑名单进行比较，以此来对接收到的信息进行处理，比如本实施例中经过比较可知原发送方的地址 a@test1.com 在用户 B 的黑名单内，则直接过滤并拦截该信息。

[0144] 另外，该步骤还可以采用如下方式来实施，即在邮件头中添加一个自定义域（以 X- 开头）。假如设定自定义域名为 X-Transmit，则新的邮件格式为：

[0145] From：" test3" <c@test3.com>

[0146] To：" test2" <b@test2.com>

[0147] X-Transmit：" test1" <a@test1.com>

[0148] Cc：

[0149] Subject：mail content

[0150] Date：Thu，25 Oct 2011 13:38:31-0800

[0151] MIME-Version：1.0

[0152] Content-Type：multipart/mixed；

[0153] Return-Path：c@test3.com

[0154] 当接收方用户 B（邮件地址为：b@test2.com）的服务器（test2）接收到该邮件后，

提取 X-Transmit :域中的邮件地址来与黑名单进行比较，比如本实施例中经过比较可知原发送方的地址 a@test1.com 在用户 B 的黑名单内，则直接过滤并拦截该信息。

[0155] 对应于上述实施例三和实施例四提供的方法，本发明实施例还提供了一种转发信息的处理系统，参见图 15 所示的转发信息的处理系统的结构框图，该系统包括 :发送方装置 150 和接收方装置 160 ；

[0156] 发送方装置 150 包括 :标识添加模块 152，用于当向接收方装置 160 转发网络信息时，将该发送方装置 150 对应的发送方标识和网络信息的原发送方标识添加在网络信息的信息头中 ;转发模块 154，与标识添加模块 152 相连，用于将标识添加模块 152 添加标识后的网络信息转发给接收方装置 160 ；

[0157] 接收方装置 160 包括 :接收模块 162，用于接收到来自发送方装置 150 转发的网络信息 ;过滤模块 164，与接收模块 162 相连，用于使用接收方装置 160 本地存储的设置信息对接收模块 162 接收的网络信息的信息头中的发送方标识和原发送方标识进行过滤。

[0158] 其中，网络信息的信息头中的发送方标识为该发送方装置 150 对应的用户的标识，原发送方标识包括该发送方装置 150 之前转发该网络信息的用户的标识和该网络信息的最初发送者的标识。因此，相对于当前的发送方而言，之前转发该网络信息的转发方均视作为该网络信息的原发送方。另外，上述发送方装置 150 对应的发送方标识和网络信息的原发送方标识的添加可以由上述发送方装置 150 完成，也可以由发送方装置 150 的服务器完成。

[0159] 其中，本系统中的设置信息与上述相同，为黑名单和 / 或垃圾信息处理规则。该设置信息也可以是采用上述实施例中的方式更新后的设置信息，具体更新方式这里不再赘述。从以上的描述中可以看出，针对相关技术中信息过滤方法的不足，本发明通过共享第三方黑名单和 / 或垃圾信息处理规则来扩充用户的黑名单和 / 或拦截规则来过滤垃圾信息，以及在转发信息时提供该信息的原发送方地址的方式来甄别垃圾信息，从而提高了垃圾信息的过滤成功率，提升了用户的体验。

[0160] 显然，本领域的技术人员应该明白，上述的本发明的各模块或各步骤可以用通用的计算装置来实现，它们可以集中在单个的计算装置上，或者分布在多个计算装置所组成的网络上，可选地，它们可以用计算装置可执行的程序代码来实现，从而，可以将它们存储在存储装置中由计算装置来执行，并且在某些情况下，可以以不同于此处的顺序执行所示出或描述的步骤，或者将它们分别制作成各个集成电路模块，或者将它们中的多个模块或步骤制作成单个集成电路模块来实现。这样，本发明不限制于任何特定的硬件和软件结合。

[0161] 以上所述仅为本发明的优选实施例而已，并不用于限制本发明，对于本领域的技术人员来说，本发明可以有各种更改和变化。凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

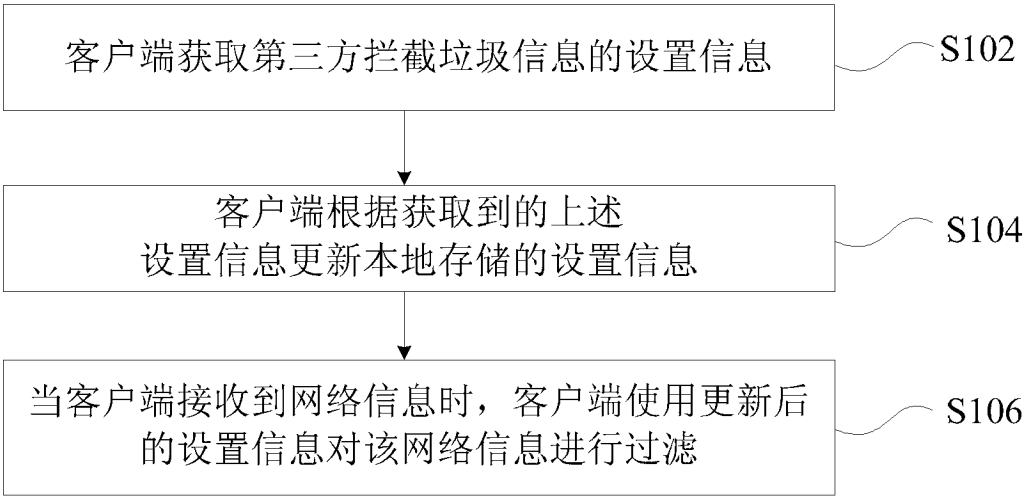

客户端获取第三方拦截垃圾信息的设置信息
S102
客户端根据获取到的上述
设置信息更新本地存储的设置信息
S104
当客户端接收到网络信息时，客户端使用更新后
的设置信息对该网络信息进行过滤
S106

图 1

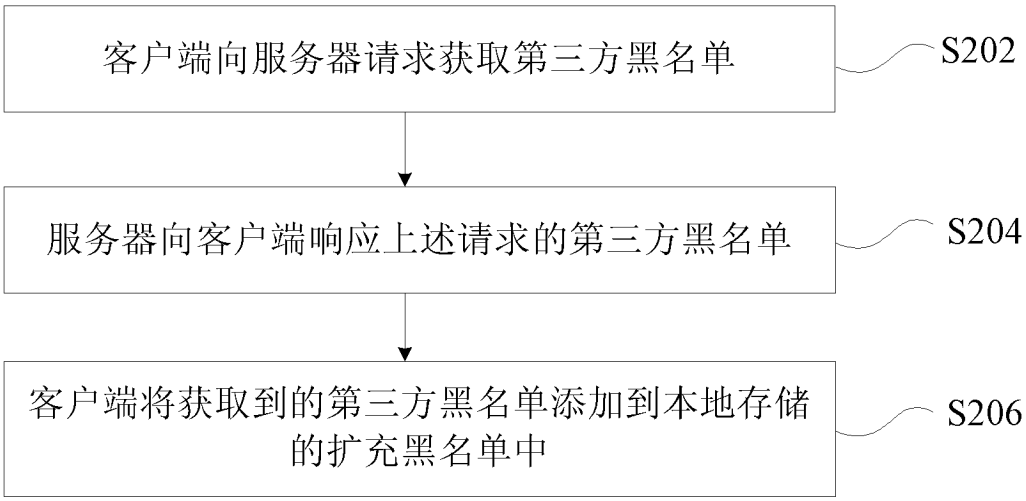

客户端向服务器请求获取第三方黑名单
S202
服务器向客户端响应上述请求的第三方黑名单
S204
客户端将获取到的第三方黑名单添加到本地存储
的扩充黑名单中
S206

图 2

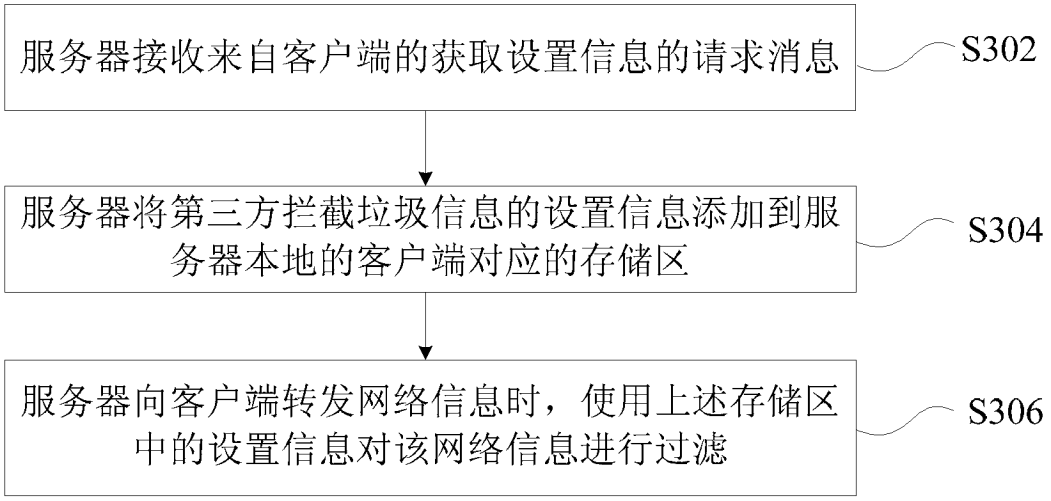

服务器接收来自客户端的获取设置信息的请求消息
S302
服务器将第三方拦截垃圾信息的设置信息添加到服务器本地的客户端对应的存储区
S304
服务器向客户端转发网络信息时，使用上述存储区中的设置信息对该网络信息进行过滤
S306

图 3

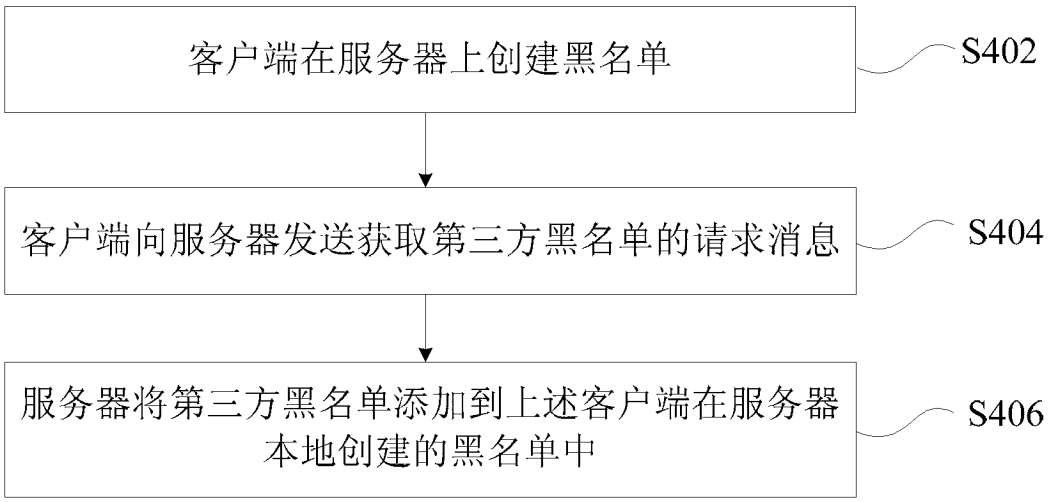

客户端在服务器上创建黑名单
S402
客户端向服务器发送获取第三方黑名单的请求消息
S404
服务器将第三方黑名单添加到上述客户端在服务器本地创建的黑名单中
S406

图 4

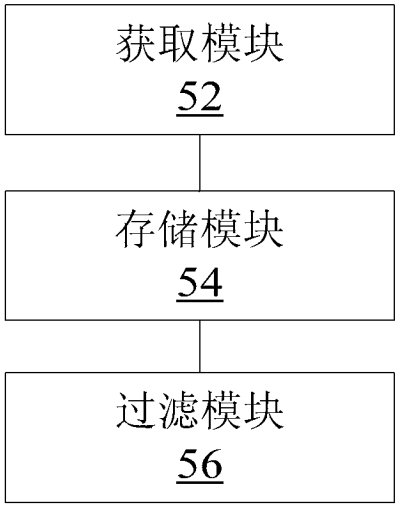

获取模块
52
存储模块
54
过滤模块
56

图 5

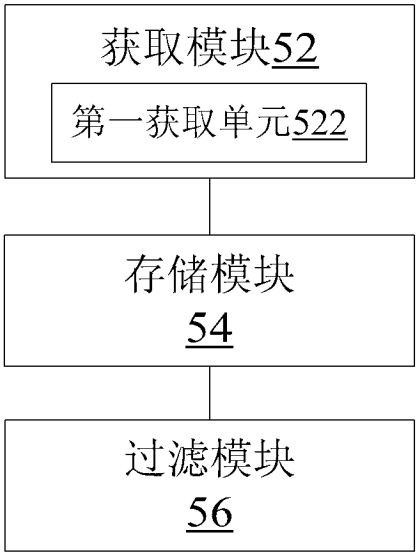

获取模块52
第一获取单元522
存储模块
54
过滤模块
56

图 6

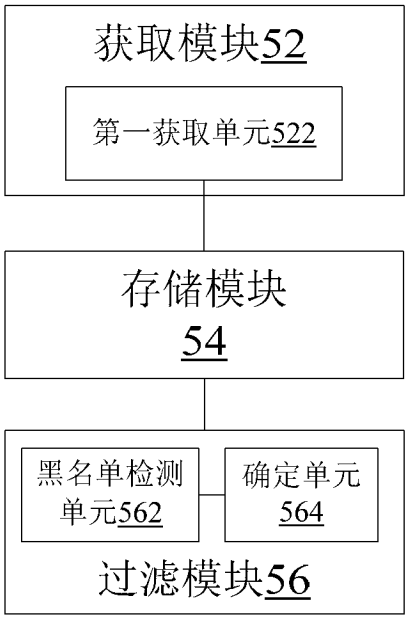

获取模块52
第一获取单元522
存储模块
54
黑名单检测单元562
确定单元
564
过滤模块56

图 7

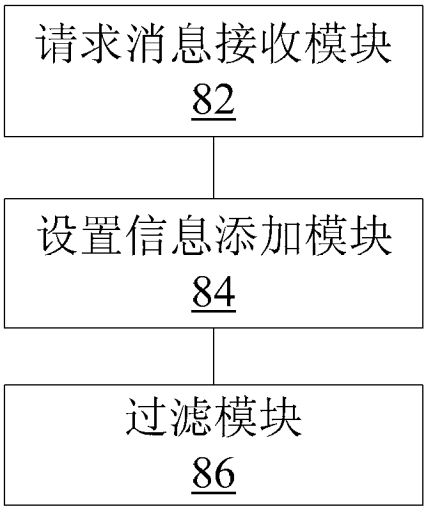

请求消息接收模块
82
设置信息添加模块
84
过滤模块
86

图 8

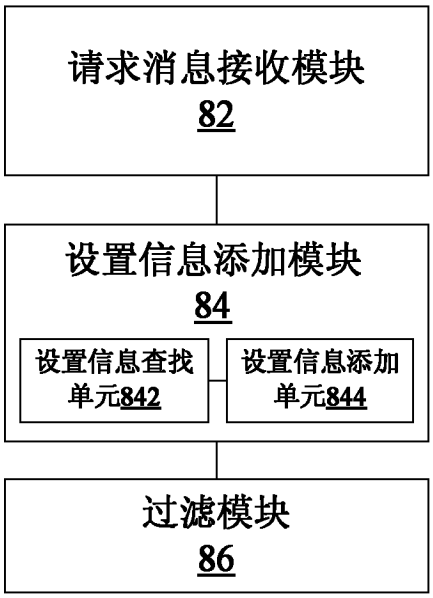

请求消息接收模块
82
设置信息添加模块
84
设置信息查找单元842
设置信息添加单元844
过滤模块
86

图 9

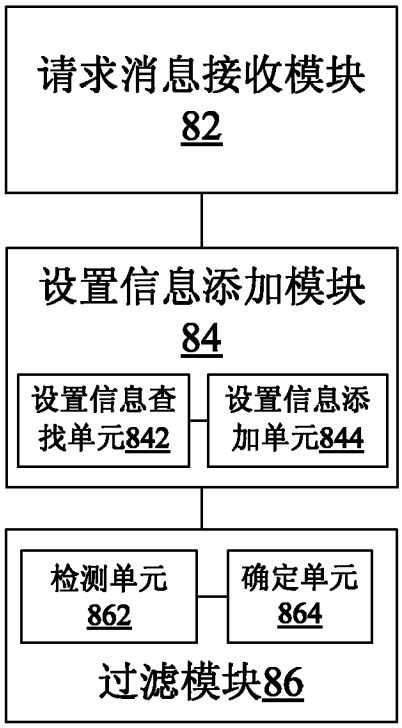

请求消息接收模块
82
设置信息添加模块
84
设置信息查找单元842
设置信息添加单元844
检测单元
862
确定单元
864
过滤模块86

图 10

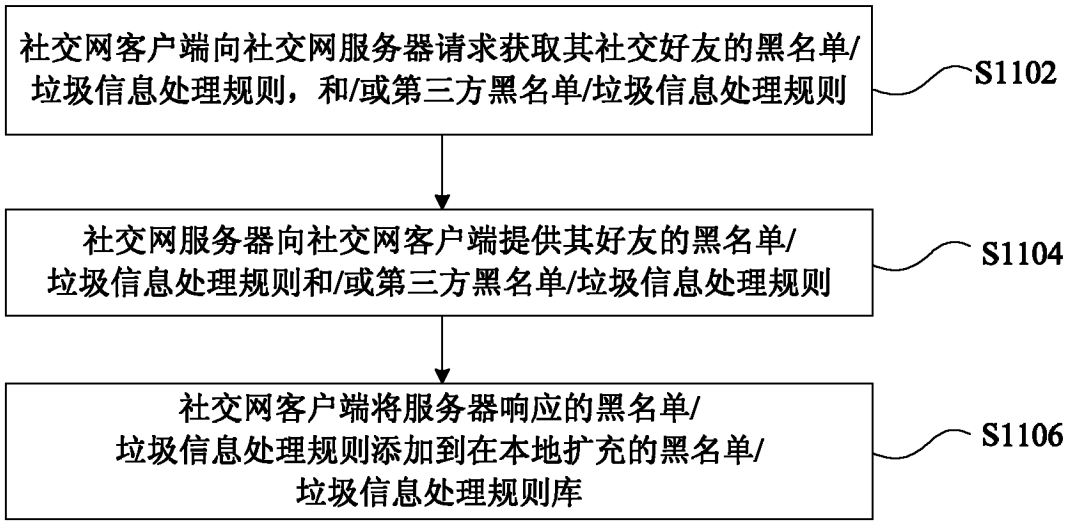

社交网客户端向社交网服务器请求获取其社交好友的黑名单/垃圾信息处理规则，和/或第三方黑名单/垃圾信息处理规则
S1102
社交网服务器向社交网客户端提供其好友的黑名单/垃圾信息处理规则和/或第三方黑名单/垃圾信息处理规则
S1104
社交网客户端将服务器响应的黑名单/垃圾信息处理规则添加到在本地扩充的黑名单/垃圾信息处理规则库
S1106

图 11

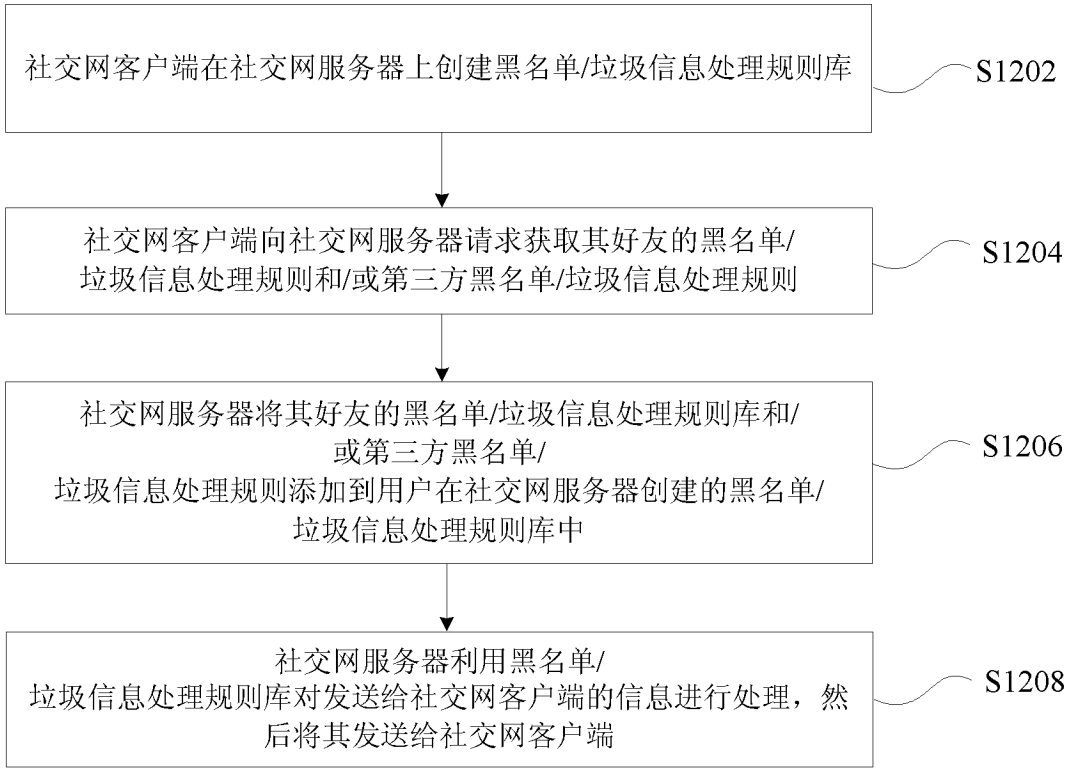

社交网客户端在社交网服务器上创建黑名单/垃圾信息处理规则库
S1202
社交网客户端向社交网服务器请求获取其好友的黑名单/
垃圾信息处理规则和/或第三方黑名单/垃圾信息处理规则
S1204
社交网服务器将其好友的黑名单/垃圾信息处理规则库和/
或第三方黑名单/
垃圾信息处理规则添加到用户在社交网服务器创建的黑名单/
垃圾信息处理规则库中
S1206
社交网服务器利用黑名单/
垃圾信息处理规则库对发送给社交网客户端的信息进行处理，然
后将其发送给社交网客户端
S1208

图 12

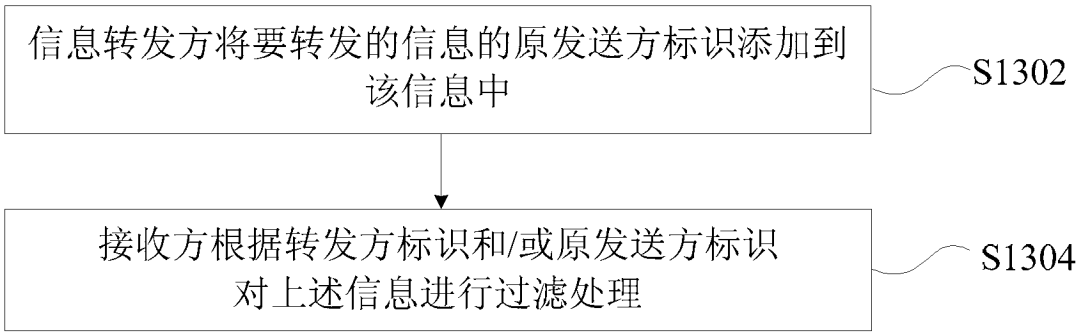

信息转发方将要转发的信息的原发送方标识添加到
该信息中
S1302
接收方根据转发方标识和/或原发送方标识
对上述信息进行过滤处理
S1304

图 13

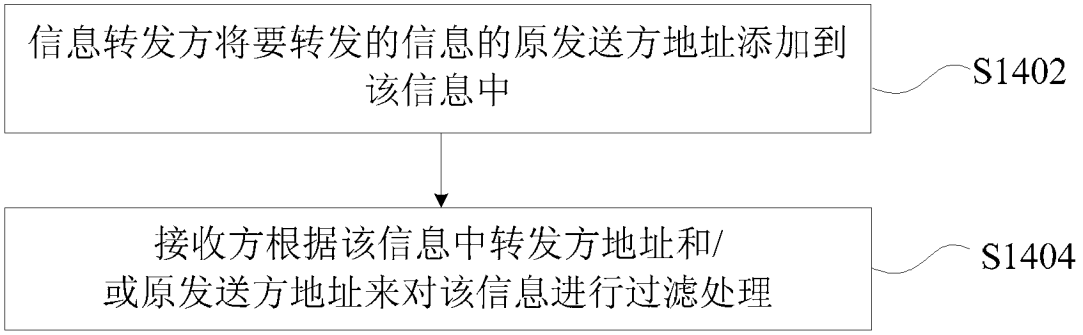

信息转发方将要转发的信息的原发送方地址添加到该信息中
S1402
接收方根据该信息中转发方地址和/或原发送方地址来对该信息进行过滤处理
S1404

图 14

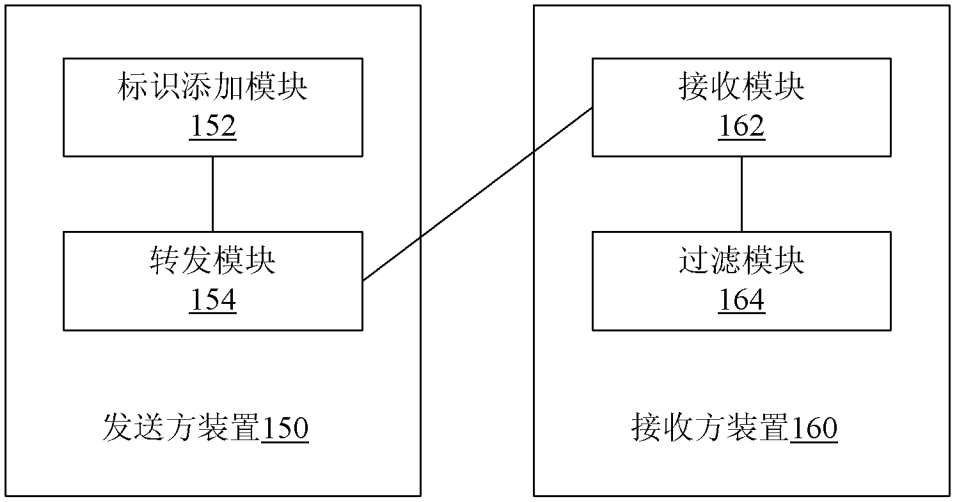

标识添加模块
152
转发模块
154
发送方装置150
接收模块
162
过滤模块
164
接收方装置160

图 15