(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 106850552 A
(43)申请公布日 2017.06.13

(21)申请号 201611190962.3

(22)申请日 2016.12.21

(71)申请人 恒安嘉新(北京)科技有限公司
地址 100089 北京市海淀区北三环西路25号27号楼五层5002室

(72)发明人 庞韶敏 高华 薛二彭 田野 何文杰 张震 金红 杨满智 刘长永 陈晓光

(74)专利代理机构 北京万慧达知识产权代理有限公司 11111
代理人 黄玉东 王荣

(51)Int.Cl.
H04L 29/06(2006.01)
H04M 1/665(2006.01)
H04M 3/436(2006.01)
H04W 4/16(2009.01)
H04W 12/12(2009.01)

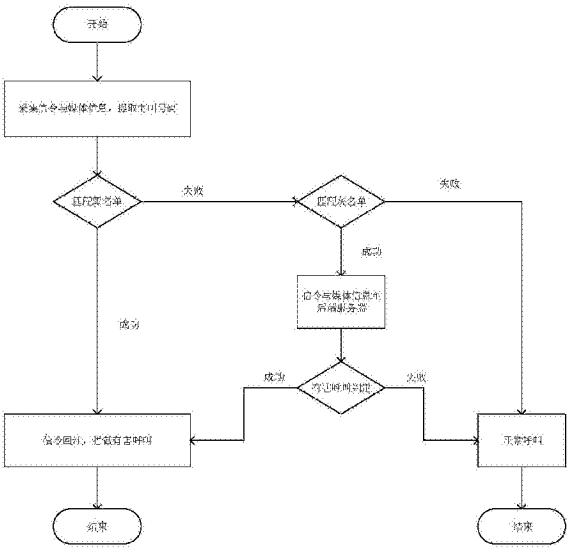
权利要求书1页 说明书4页 附图2页

(54)发明名称

一种基于信令回注实现有害呼叫拦截的方法

(57)摘要

本发明属于通信网络安全领域,公开了一种基于信令回注实现有害呼叫拦截的方法,该方法包括:前端设备采集信令与媒体信息,获取信令中的主叫信息,用该信息与数据库中的号码进行匹配,若为黑名单目标用户,则前端设备采用信令回注方式对该有害呼叫进行拦截;若为灰名单用户则将该呼叫的信令信息与媒体信息关联之后送入后端服务器,经后端服务器判定该号码为有害主叫,则下发命令至前端设备进行拦截,前端设备采用信令回注方式,实现对有害呼叫的拦截。本发明可对黑名单主叫的呼叫以及经过检测确认为有害的呼叫实现实时拦截。



CN 106850552 A

1.一种基于信令回注实现有害呼叫拦截的方法，其特征在于，所述方法包括：

前端设备采集信令与媒体信息，获取信令与媒体信息中的主叫号码信息；

用获取的主叫号码信息与数据库中主叫号码进行匹配，判定是否有害呼叫；其中，

若匹配为黑名单目标用户，则对该呼叫直接进行拦截；

若匹配不为黑名单用户，再次用该主叫号码与疑似有害呼叫灰名单库进行匹配，判定该号码是否为灰名单库所有，其中，

若匹配不为灰名单库所有，则允许其正常呼叫；

若匹配存在于灰名单库中，则将该呼叫的信令与媒体信息传至后端服务器经后端服务器判定该号码是否为有害主叫，若后端服务器判定为有害呼叫，则后端服务器下发命令至前端设备进行拦截，若后端服务器判定不为有害呼叫，则允许其正常呼叫。

2.如权利要求1所述的基于信令回注实现有害呼叫拦截的方法，其特征在于，前端设备通过对现网链路采用旁路并接模式实现采集，前端设备通过对媒体面信息进行采集并将采集到的媒体信息解码，完成信令与媒体的关联，采集方式包括镜像和分光。

3.如权利要求1所述的基于信令回注实现有害呼叫拦截的方法，其特征在于，前端设备将所有通话话单上报到后端服务器，后端服务器基于通话的外部输入特征、信令特征与行为特征进行分析，对疑似有害的呼叫生成灰名单并下发到前端设备的灰名单库中。

4.如权利要求1所述的基于信令回注实现有害呼叫拦截的方法，其特征在于，前端设备根据黑名单库的匹配结果以及后端服务器下发的命令，采用信令回注的方式生成释放呼叫的信令包，对有害呼叫实施拦截，其中所述信令回注包括构造相关的呼叫信息，将该消息发至网络，实现对有害呼叫的拦截。

5.如权利要求4所述的基于信令回注实现有害呼叫拦截的方法，其特征在于，对网络传输协议为SIP、BICC、ISUP中的控制信令，采用不同的回注信令实现拦截。

一种基于信令回注实现有害呼叫拦截的方法

技术领域

[0001] 本发明属于通信网络安全技术领域，尤其涉及一种基于信令回注实现有害呼叫拦截的方法。

背景技术

[0002] 近年来利用电话进行的诈骗方式呈爆发趋势，受骗面广，金额巨大，通信诈骗成为巨大的用户痛点。2013年，全国通信诈骗案30余万起，群众被骗100亿元；2014年，全国通信诈骗案40余万起，群众损失107亿元；2015年全国公安机关共立电信诈骗案件59万起，同比上升32.5％，造成经济损失222亿元。今年1月至8月，全国共立电信诈骗案件35.5万起，同比上升36.4％，造成损失114.2亿元。报告显示，近一年来，因个人信息泄露、垃圾信息、诈骗信息等原因，导致网民总体损失约805亿元，人均124元，其中约4500万网民近一年遭受的经济损失在1000元以上。这些损失的背后影射出了移动黑产，移动黑产是一条完整的链条，涉及到多个环节，仅仅靠某一方的力量，无法达到有效的打击目的，需要联合各方资源，一起发力。

[0003] 2013年至今，近10年来，我国电信诈骗案件每年以20％－30％的速度快速增长。全国共发生被骗千万元以上的电信诈骗案件104起，百万元以上的案件2392起。很多群众的“养老钱”“救命钱”被骗，倾家荡产、家破人亡；有的企业资金被骗，破产倒闭，引发群体性事件。

[0004] 鉴于上述电性诈骗案率频发，因此，如何从众多的电话号码中，分析出垃圾号码，圈出恶意号码，对那些疑似有害的呼叫进行拦截便成为了目前亟待解决的问题。

发明内容

[0005] 本发明的目的是，提供一种基于信令回注实现有害呼叫拦截的方法，以实现对通信中疑似有害呼叫的拦截。

[0006] 本发明采用的技术方案如下：

[0007] 一种基于信令回注实现有害呼叫拦截的方法，所述方法包括：

[0008] 前端设备采集信令与媒体信息，获取信令与媒体信息中的主叫号码信息；

[0009] 用获取的主叫号码信息与数据库中主叫号码进行匹配，判定是否有害呼叫；其中，

[0010] 若匹配为黑名单目标用户，则前端设备对该呼叫直接进行拦截；

[0011] 若匹配不为黑名单用户，再次用该主叫号码与疑似有害呼叫灰名单库进行匹配，判定该号码是否为灰名单库所有，其中，

[0012] 若匹配不为灰名单库所有，则允许其正常呼叫；

[0013] 若匹配存在于灰名单库中，则将该呼叫的信令与媒体信息传至后端服务器经后端服务器判定该号码是否为有害呼叫，若后端服务器判定为有害呼叫，则后端服务器下发命令至前端设备进行拦截，若后端服务器判定不为有害呼叫，则允许其正常呼叫。

[0014] 进一步地，前端设备通过对现网链路采用旁路并接模式实现采集，前端设备通过

对媒体面信息进行采集并将采集到的媒体信息解码，完成信令与媒体的关联，采集方式包括镜像和分光。

[0015] 进一步地，前端设备将所有通话话单上报到后端服务器，后端服务器基于通话的外部输入特征、信令特征与行为特征进行分析，对疑似有害的呼叫生成灰名单并下发到前端设备的灰名单库中。

[0016] 进一步地，前端设备根据黑名单库的匹配结果以及后端服务器下发的命令，采用信令回注的方式生成释放呼叫的信令包，对有害呼叫实施拦截，其中所述信令回注包括构造相关的呼叫信息，将该消息发至网络，实现对有害呼叫的拦截。

[0017] 进一步地，对网络传输协议为SIP、BICC、ISUP中的控制信令，采用不同的回注信令。

[0018] 与现有技术相比，本发明所提供的一种基于信令回注实现有害呼叫拦截的方法，通过与黑名单电话号码匹配，以及对灰名单用户的语音语义特征分析，可以实现对诈骗电话的识别。在识别出诈骗电话后，使用信令回注的方法对该呼叫进行实时拦截。本发明无需对现网进行较大改造，且不会影响现网中的正常通话。

附图说明

[0019] 图1是本发明实施例所述的基于信令回注实现有害呼叫拦截的方法的流程示意图；

[0020] 图2是本发明实施例所述的基于信令回注实现有害呼叫拦截的方法的系统架构图。

具体实施方式

[0021] 以下实施例仅用于更加清楚地说明本发明的技术方案，而不能以此来限制本发明的保护范围。如在说明书及权利要求当中使用了某些词汇来指称特定部件。本领域技术人员应可理解，硬件制造商可能会用不同名词来称呼同一个部件。本说明书及权利要求并不以名称的差异来作为区分部件的方式，而是以部件在功能上的差异来作为区分的准则。说明书后续描述为实施本发明的较佳实施方式，然所述描述乃以说明本新型的一般原则为目的，并非用以限定本发明的范围。本发明的保护范围当视所附权利要求所界定者为准。

[0022] 下面结合附图和具体实施例对本发明做进一步详细说明。

[0023] 本发明的目的是实现对黑名单号码的呼叫以及经过检测确认为有害的呼叫实现实时有效拦截。

[0024] 如图1、图2所示，本发明实施例所述的一种基于信令回注实现有害呼叫拦截的方法，包括如下步骤：

[0025] 前端设备采集信令与媒体信息，获取信令与媒体信息中的主叫号码信息；

[0026] 用获取的主叫号码信息与数据库中主叫号码进行匹配，判定是否有害呼叫；其中，

[0027] 若匹配为黑名单目标用户，则前端设备对该呼叫直接进行拦截；

[0028] 若匹配不为黑名单用户，再次用该主叫号码与疑似有害呼叫灰名单库进行匹配，判定该号码是否为灰名单库所有，其中，

[0029] 若匹配不为灰名单库所有，则允许其正常呼叫；

[0030] 若匹配存在于灰名单库中，则将该呼叫的信令与媒体信息传至后端服务器经后端服务器判定该主叫号码是否为有害呼叫，若后端服务器判定为有害呼叫，则后端服务器下发命令至前端设备进行拦截，阻止该呼叫继续，若后端服务器判定不为有害呼叫，则允许其正常呼叫。

[0031] 具体来说，本发明主要通过信令采集与媒体采集、有害呼叫判定以及有害呼叫拦截三步来确认。

[0032] 在信令的采集与媒体采集过程中，信令主要通过对现网链路采用旁路并接模式实现采集，采集方式为镜像或分光，或二者相结合的方式。媒体主要通过对媒体面信息进行采集，并将采集到的媒体信息解码，还原为音频文件。并通过对协议进行解码，完成信令与媒体的关联。旁路并接模式，前端设备与网络中设备为并接关系，优点在于前端设备出现故障不会影响到网络设备的正常运行，且无需对现网进行较大改造即可实现。镜像方式为，构造镜像链路，使网络设备中的信号除正常传送外，将其镜像传送至前端设备。分光方式则针对通过光网络进行信号传送的网络设备，构造分光链路，使网络设备中的光信号除正常传送外，将其分光传送至前端设备。

[0033] 在有害呼叫判定过程中，有害呼叫判定主要有两种方式。

[0034] 第一种判定方式为，前端设备设有黑名单库，前端设备对采集到的信令信息进行解码分析，获得信令中的主叫号码，用主叫号码与黑名单库进行匹配。判定该号码是否为黑名单库所有，若位于黑名单库中，则判定该呼叫为有害呼叫。

[0035] 第二种方式为，对信令信息解码分析获得的主叫号码没有位于黑名单库中，则用该主叫号码与疑似有害呼叫灰名单库进行匹配，判定该号码是否为灰名单库所有，若位于灰名单库中，则将该主叫号码的信令信息与媒体信息传至后端服务器，后端服务器对该呼叫做出判定是否为有害呼叫，后端服务器判定为有害呼叫，则拦截。

[0036] 其中，在有害呼叫的判定之前，前端设备将所有通话话单上报到后端服务器，后端服务器对外部输入特征、信令特征与行为特征进行单独或者综合分析，对疑似有害的呼叫生成灰名单下发到前端设备灰名单库，实现灰名单库的更新。后端服务器对认定为有害呼叫除了给前端服务器拦截的指令后，也同时可以生成黑名单下发到前端的黑名单库，实现黑名单库的更新。

[0037] 在有害呼叫拦截过程中采用信令回注方式，前端设备根据黑名单匹配结果以及后端服务器下发命令，生成释放呼叫的信令包，对有害呼叫实施拦截。信令回注即为构造相关的呼叫消息，将该消息发至网络，即可实现对有害呼叫的拦截。其中，信令回注消息的构造由前端设备完成。

[0038] 本发明针对不同网络采用不同的回注信令。

[0039] 根据黑名单拦截通话前呼叫，具体回注信令如下表所示：

[0040]

控制信令	控制承载	媒体承载	回注信令拦截控制
SIP	IP	IP	发送SIP 486消息
BICC	IP	IP	发送BICC REL消息
ISUP	TDM SS7	TDM	发送ISUP REL消息

[0041] 根据灰名单拦截通话后呼叫，具体回注信令如下表所示：

[0042]

控制信令	控制承载	媒体承载	回注信令拦截控制
SIP	IP	IP	发送SIP BYE消息
BICC	IP	IP	发送BICC REL消息
ISUP	TDM SS7	TDM	发送ISUP REL消息

[0043] 下面对三种信令传输协议进行简单介绍。

[0044] SIP(Session Initiation Protocol)是一个应用层的信令控制协议。用于创建、修改和释放一个或多个参与者的会话。

[0045] SIP独立于传输层,使用用户数据报协议(UDP)以及传输控制协议(TCP),将独立于底层基础设施的用户灵活地连接起来。

[0046] SIP BYE消息用于终止已建立的会话,可以通过向主叫方或被叫方发送此消息来结束会话。

[0047] BICC是Bearer Independent Call Control protocol的缩写,即与承载无关的呼叫控制协议。BICC是一个基于ISUP(ISDN User Part)的呼叫控制协议。既然是呼叫控制协议,BICC只负责建立、修改与终结呼叫。BICC是一个与承载无关的协议。REL是BICC的释放消息;REL也是ISUP的释放消息。

[0048] 本发明通过信令回注方式实现对有害呼叫的拦截,具体实现方式为在软交换局的现网链路采用旁路并接模式实施信令、媒体采集。前端设备将通话话单上报到后端服务器,后端服务器根据外部输入、信令特征与行为特征等生成黑名单和灰名单。前端设备对灰名单实现信令与媒体信息上报,后端服务器对上传的信息进行判定,若判定为有害呼叫则向前端设备发出拦截命令。前端设备通过信令回注的方式,实现对有害呼叫的拦截。

[0049] 本发明所述的方法在不影响现网中其它网络正常通话的基础上,无需对现网进行较大改造,即可实现对有害呼叫的有效拦截。

[0050] 值得注意的是,以上所述仅为本发明的较佳实施例,并非因此限定本发明的专利保护范围,本发明还可以对上述各种零部件的构造进行材料和结构的改进,或者是采用技术等同物进行替换。故凡运用本发明的说明书及图示内容所作的等效结构变化,或直接或间接运用于其他相关技术领域均同理皆包含于本发明所涵盖的范围内。

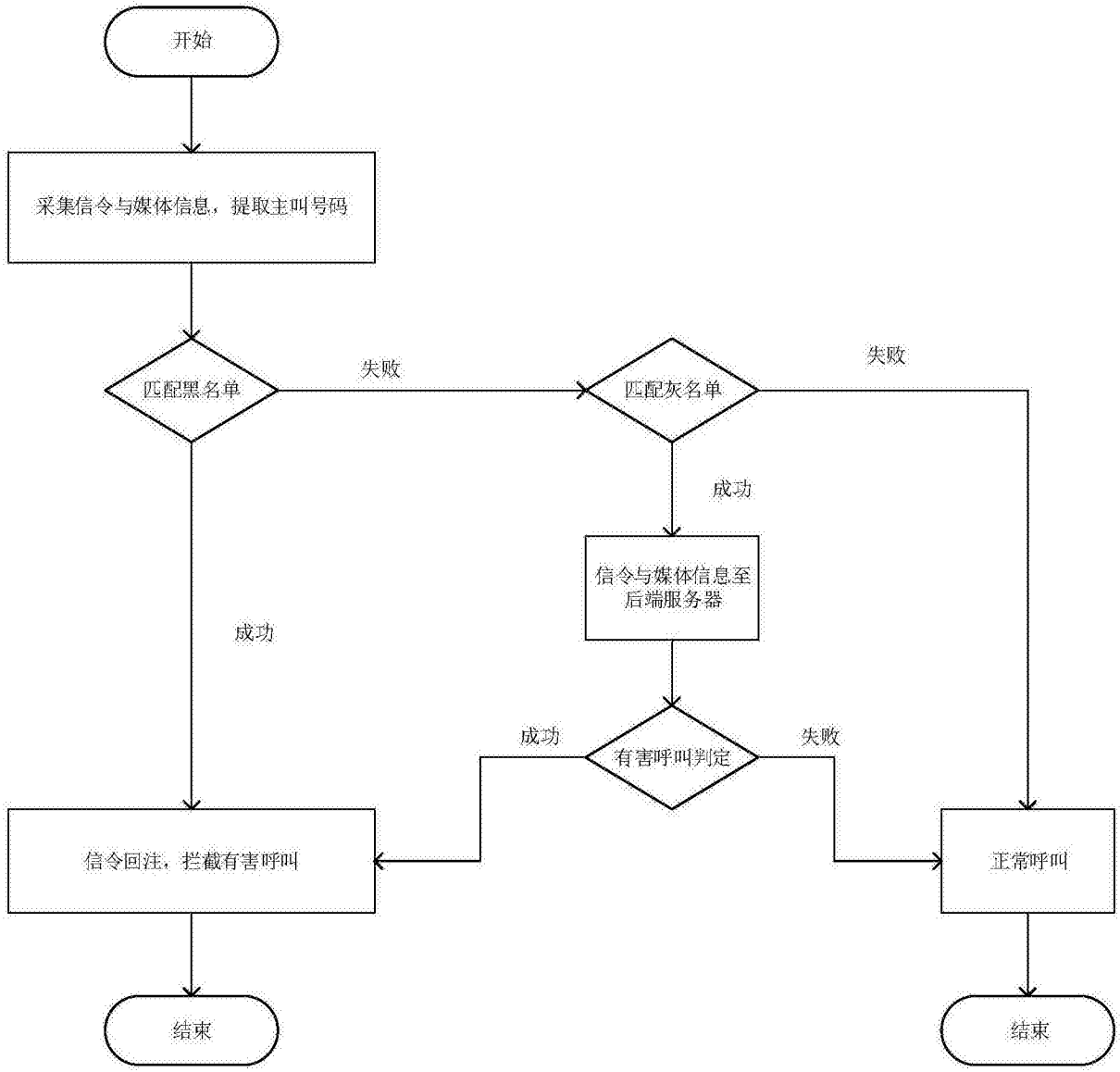

开始
采集信令与媒体信息，提取主叫号码
匹配黑名单
失败
匹配灰名单
失败
成功
信令与媒体信息至后端服务器
成功
成功
有害呼叫判定
失败
信令回注，拦截有害呼叫
正常呼叫
结束
结束

图1

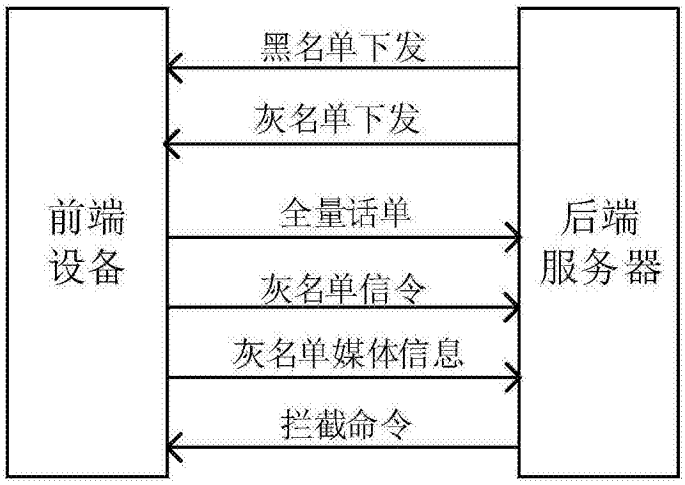


图2