



(12) 发明专利

(10) 授权公告号 CN 1942007 B

(45) 授权公告日 2012.08.22

(21) 申请号 200610105597.1

(22) 申请日 2006.07.19

(30) 优先权数据

60/701,222 2005.07.20 US

11/243,753 2005.10.04 US

(73) 专利权人 阿瓦雅技术有限公司

地址 美国新泽西州

(72) 发明人 迈克尔·J·克劳伯登斯

约翰·M·沃尔顿

(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 康建忠

(51) Int. Cl.

H04L 12/26(2006.01)

H04W 12/12(2006.01)

H04L 12/24(2006.01)

(56) 对比文件

CN 1411209 A, 2003.04.16, 全文.

US 2003/0145225 A1, 2003.07.31, 全文.

CN 1384639 A, 2002.12.11, 全文.

CN 1531254 A, 2004.09.22, 全文.

审查员 李燕

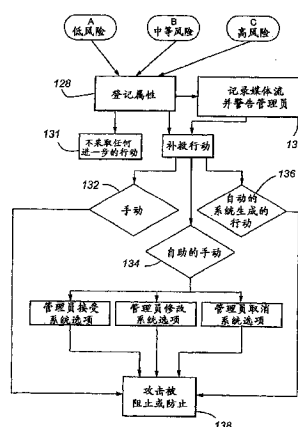
权利要求书 2 页 说明书 8 页 附图 5 页

(54) 发明名称

电话分机攻击检测、记录 and 智能防止

(57) 摘要

提供一种检测对通信企业进行的分机攻击并采取合适的补救行动来防止正在进行的攻击和未来的攻击的系统和方法。分析可疑呼叫的一个或多个属性,并将风险与每个分析的属性关联。其后,对分析的属性进行整体风险评估,登记攻击属性,并根据分析的呼叫属性,可触发一个或多个补救行动。补救行动可包括记录呼叫,通知管理员有可疑呼叫,或通过终止呼叫或关闭选择的通信终点来将通信企业与攻击隔离,从而防止正对分机进行的呼叫。可将规则应用于分析的属性,从而触发合适的补救行动。分析的呼叫属性可包括呼叫目的地、呼叫方向、呼叫类型、呼叫的时间、呼叫持续时间、呼叫源是否被欺骗,来自特定呼叫源的呼叫容量以及为可疑媒体流创建的散列值。



1. 一种保护通信企业的通信服务的方法,所述方法包括以下步骤:

检测以指向通信企业内的一个或多个分机的呼叫的形式的察觉的分机攻击,所述检测步骤包括分析呼叫的至少一个属性;

基于对所述至少一个属性的分析,对与呼叫关联的风险进行分类;以及

采取补救行动以根据与呼叫关联的风险来阻止察觉的攻击,

其中:所述检测步骤基于所述呼叫的媒体流随机性属性执行所述检测,并且包括:(i) 创建算法;(ii) 将算法应用于呼叫的第一媒体流;(iii) 生成反映第一媒体流内容的第一媒体散列值;(iv) 将算法应用于指向通信企业的随后呼叫的第二媒体流;(v) 生成反映第二媒体流的第二媒体散列值;(vi) 比较第一媒体散列值和第二媒体散列值;以及(vii) 如果第一媒体散列值和第二媒体散列值落入预先指定的范围,则采取补救行动。

2. 如权利要求 1 所述的方法,还包括以下步骤:

记录所述呼叫;以及

将与呼叫关联的类型以及风险警告给通信企业的管理员,使得管理员能够影响所采取的补救行动。

3. 如权利要求 1 所述的方法,其中:

所述检测步骤基于所述呼叫的呼叫源属性执行所述检测,并且包括以下步骤中的至少一个:(i) 对从呼叫源发送到企业的呼叫序列进行分析,如果呼叫序列与预定的不许可的呼叫序列匹配,则采取补救行动;(ii) 检测发送到企业内的未管理的号码的呼叫,并且如果对未管理的号码的呼叫的数量达到不许可的预定值,则采取补救行动;(iii) 分析呼叫源,并确定被呼叫的源是传真、语音还是调制解调器;(iv) 确定呼叫是否是从企业内的分机进行的;(v) 检测来自呼叫源的多个呼叫具有单个持续时间还是多个持续时间;(vi) 检测从呼叫源接收到的呼叫的数量,并确定所接收的呼叫的数量是否包括不许可的呼叫数量;以及(vii) 通过对欺骗呼叫的源 ID 属性与实际呼叫源 ID 进行比较来检测欺骗呼叫源,其中,执行查找或反向查找来确定实际呼叫源。

4. 一种保护通信企业的通信服务的设备,包括:

用于检测以指向通信企业内的一个或多个分机的呼叫的形式的察觉的分机攻击的装置,其包括用于分析呼叫的至少一个属性的装置;

用于基于对所述至少一个属性的分析,对与呼叫关联的风险进行分类的装置;以及

用于采取补救行动以根据与呼叫关联的风险来阻止察觉的攻击的装置,

其中所述用于检测以指向通信企业内的一个或多个分机的呼叫的形式的察觉的分机攻击的装置基于所述呼叫的媒体流随机性属性执行所述检测,并且包括(i) 用于创建算法的装置;(ii) 用于将算法应用于呼叫的第一媒体流的装置;(iii) 用于生成反映第一媒体流内容的第一媒体散列值的装置;(iv) 用于将算法应用于指向通信企业的随后呼叫的第二媒体流的装置;(v) 用于生成反映第二媒体流的第二媒体散列值的装置;(vi) 用于比较第一媒体散列值和第二媒体散列值的装置;以及(vii) 用于如果第一媒体散列值和第二媒体散列值落入预先指定的范围,则采取补救行动的装置。

5. 如权利要求 4 所述的设备,其中,

所述用于检测以指向通信企业内的一个或多个分机的呼叫的形式的察觉的分机攻击的装置包括以下中的至少一个:(i) 用于通过对欺骗的呼叫的源和实际呼叫源进行比较来

检测欺骗的呼叫源的装置,其中,执行查找或反向查找来确定实际呼叫源;(ii)用于指定至少一个规则的装置,所述至少一个规则应用于针对作为分机攻击而分析的呼叫的属性,所述属性包括呼叫持续时间、呼叫方向、呼叫类型、日的时间、呼叫目的地、欺骗的呼叫源、媒体散列值以及从呼叫的呼叫源接收到的呼叫的数量中的至少一个,所述规则与确定是否采取补救行动相关联;(iii)用于评估与呼叫关联的整体风险的装置,所述用于评估的装置包括分析呼叫的多个属性,所述属性包括媒体散列值、呼叫持续时间、呼叫方向、呼叫类型、日的时间、呼叫目的地、欺骗的呼叫源以及从呼叫的呼叫源接收的呼叫的数量中的至少一个;(iv)用于将察觉的攻击和与攻击关联的分配的风险通知给通信系统的管理员,从而使管理员能够干预所采取的补救行动的装置;以及(v)可执行编程指令模块,其被结合在通信企业内的通信服务器中,至少一个数据库与所述可执行编程指令模块相关联,其中,至少部分地基于先前发生的分机攻击的历史分析,所述可执行编程指令模块随时间而被修改以改变与攻击关联的风险的分配。

6. 如权利要求 5 所述的设备,其中:

所述用于评估的装置包括应用于所述呼叫属性中的至少一个并分配与至少一个分析的呼叫属性关联的风险的计算装置。

7. 如权利要求 5 所述的设备,其中,

所述用于通知的装置包括交互语音响应装置,所述交互语音响应装置被实现在所述通信服务器中,其中,在通过选择补救行动选项而生成适当的补救行动的过程中,将多个选项提供给管理员。

电话分机攻击检测、记录 and 智能防止

[0001] 相关申请的交叉引用

[0002] 本申请要求与 2005 年 7 月 20 日提交的美国临时申请 No. 60/701, 222 的优先权, 其全部公开在此引入作为参考。

技术领域

[0003] 本发明涉及保护通信系统不受分机攻击, 更具体地说, 本发明涉及一种用于检测分机攻击并采取合适的补救行动以防止正在进行的攻击以及攻击在未来发生的方法和系统。

背景技术

[0004] 许多商业和政府组织对通信安全性的关注正在增长。随着 VoIP 电话的出现和互联网的其它运用, 各个组织现在具有多种通信手段; 然而, 增长的通信能力也导致各个组织容易受到想要获得对该组织的通信系统的访问的黑客的攻击。发生许多电话分机攻击, 从而将多余消息提供给组织 (例如对各种商品和服务进行广告)。然而, 许多分机攻击可能是出于明显非法目的而启动的, 例如, 为了获得对机密的组织信息的访问。

[0005] 有很多可被启动的不同类型的电话分机攻击。对于 IP 电话来说, 互联网电话上的 SPAM(SPIT) 包括 IP 电话设备上广播的多余的大块消息。SPIT 与电子邮件 SPAM 和 SPIM(基于时消息收发的 SPAM) 是非常相关的。虽然 SPIT 不如 SPAM 盛行, 但电信产业预期 SPIT 将随着时间进展而出现更多问题。其它类型的分机攻击包括拒绝服务、战争式拨号 (war-dialing)、语音邮件口令暴力破解、分机口令暴力破解、长途话费欺诈 (toll fraud) 等。

[0006] 存在解决电话分机攻击的一些方案。当前可用的商用产品主要是基于规则的, 从而导致效率受限, 并且对于防止使用 IP 或呼叫者 ID 进行欺骗来掩盖攻击源的攻击尤其无效。两种公知的商用产品包括 **SecureLogix®** 生产的语音防火墙和语音侵入防止系统以及 **Sandstorm®** 生产的 **Sandtrap®**。

[0007] 虽然这些产品对于它们期望的目的来说是足够的, 但仍旧需要检测和防止与诸如 SPIT 的 IP 上的语音关联的新的、更复杂的攻击。更具体地说, 需要一种电话分机攻击解决方案, 该解决方案可检测、记录、警告并有效防止在传统电话 (电路交换) 和 IP 电话 (分组交换) 通信系统两者上发生的攻击。

发明内容

[0008] 本发明在于解决现有技术的上述问题和缺点。根据本发明的实施例, 提供一种方法和系统, 用于检测电话分机攻击, 记录攻击, 警告管理员或其他人有攻击, 其后提供补救能力以阻止正在进行的攻击并有效防止未来的攻击。

[0009] 根据本发明优选实施例, 本发明的方法和系统分析呼叫的多个属性以确定呼叫是否可能是电话分机攻击。一旦对呼叫属性进行分析, 就关于呼叫是否有可能是攻击而将风

险与每一个属性关联。可分析的呼叫属性包括：呼叫源、干线 (trunk) ID、呼叫者 ID 或 IP 地址 (如果是 VoIP 呼叫)、呼叫目的地、单向 (源) 媒体流随机性、呼叫持续时间、呼叫的时间、呼叫类型以及呼叫方向。此外,还可定义从特定源接收的呼叫的数量 (呼叫容量) 作为呼叫属性,并且从特定源接收的呼叫的数量对于在确定潜在的攻击中进行估计是重要因素。如果风险评估导致发现察觉的攻击,则正监控呼入呼叫的通信服务器或单机服务器选择性地对呼叫属性进行登记 (log), 对用于包括媒体流的可疑事件进行记录, 并警告管理员有察觉的攻击。

[0010] 通过基于借助于考虑呼叫属性而产生的风险的评估来合并一个或多个补救行动, 从而实现防止正在进行的攻击和未来的攻击。可按三种基本形式对补救行动进行分类, 所述三种基本形式即手动补救行动、自动补救行动以及自助补救行动。手动补救行动包括手动工作以禁闭通信系统或该系统中受影响的部分从而防止攻击。禁闭的示例将是断开调制解调器, 或改变用于接收呼入呼叫的限制的类别等。自动补救行动的示例包括指定应用于特定呼叫属性的一组规则, 其中, 如果呼叫属性满足规则的预置准则, 则通信系统自动禁闭整个系统或系统中受影响的部分以防止攻击。可响应于过去可能已经发生的攻击的历史分析随时间而改变指定的一组规则来包括对系统的精细调整, 从而在威胁风险的合适级别提供补救行动。对可疑呼叫属性进行登记, 从而提供历史基准以确定合适的补救行动。自助手动 (AAM) 补救行动是对手动和自动方法两者一起进行的选择性的混合, 从而提供对察觉的攻击的合适的响应。补救行动对于低风险攻击是更加基于规则的, 或通过组合人工影响和系统建议而对于较高的风险攻击是更加智能化的。可通过补救措施按多种形式将防止发送到用户 / 管理员, 所述多种形式包括电子邮件、文本消息或蜂窝电话呼叫。可通过使用具有菜单选择的用户接口屏幕、通过使用通信服务器 / 单机服务器中的交互语音响应 (IVR) 应用、或通过手动干预以隔离目标通信设备来实现对这些措施的激活。

[0011] 尤其当与以下附图一起进行讨论时, 本发明的其它特点和优点将变得更加清楚。

附图说明

[0012] 图 1 是描述结合第一实施例中的本发明的系统和方法的示例性通信系统的示意图;

[0013] 图 2 是描述第二实施例中的本发明的系统和方法以及示例性通信系统的示意图;

[0014] 图 3 是结合第二实施例中的本发明的通信设备的示意图;

[0015] 图 4 是描述结合第三实施例中的本发明的通信系统的另一示意图; 以及

[0016] 图 5A 和 5B 示出本发明的操作的一个示例实现。

具体实施方式

[0017] 图 1 示出适合于与本发明优选实施例关联使用的通信系统 10。通信系统 10 包括通信网络 12、通信服务器或网关 14、第一群组或第一类型的通信设备 18、以及第二群组或第二类型的通信设备 20。示出由本发明实现的功能被结合在通信服务器 14 中, 并被称为具有检测、记录和智能防止的电话分机攻击 (TEA-DRIP)。通信网络 12 可包括公共交换电话网络 (PSTN) 和 / 或可包括在其上根据互联网上的语音 (VoIP) 传送通信的分组数据网络。通信设备 18 和 20 可包括适合于用于与语音和数据通信连接的任意类型的通信设备。例如,

通常示出通信设备 18 为计算机,因此,通信设备 18 可代表 VoIP 电话、传真机、软 VoIP 电话和调制解调器等。示出通信设备 20 是表示传统电话和 / 或诸如蜂窝电话、PDA(个人数字助理)和 IP 台式电话机等无线语音通信设备。应当理解,通信服务器 14 可还表示专用交换分机(PBX)或任意其它相似的连接处理交换机或服务器,本发明不限于使用特定类型的通信交换机或服务器或相似的系统部件的配置。通信服务器 14 专用于一个或多个通信企业,诸如一个或多个商业或政府实体。通信网络 12 还可包括能够承载数据的一个或多个网络,所述数据可包括通信设备之间的实时数据,或数据分组源和通信设备中的一个或多个之间的实时数据。通信网络 12 还可包括计算机网络、其包括局域网、专用内部网或互联网。

[0018] 攻击源 22 例如可包括在黑客控制下的数据分组源,所述黑客发送恶意数据分组流,企图防止目标通信设备 18 或其它关联的设备执行期望的功能。因此,攻击源 22 可以与作为特定类型的分机攻击的拒绝服务(DoS)攻击相关联。攻击源还可与 SPIT(互联网电话上的 SPAM)、SPAM、战争式拨号、语音邮件口令暴力破解、分机口令暴力破解、长途话费欺诈等进行关联。战争式拨号指的是尝试通过使用由计算机所指挥的调制解调器来攻击进入通信系统,所述计算机顺序地或伪随机地拨打企业的多个分机号码以期确定是否存在调制解调器、传真机、语音邮件或其它与分机关联的通信设备。战争式拨号软件可用于允许黑客记录每次拨打的分机的结果。与当拨打时不生成响应的那些分机 / 号码相反,由调制解调器、传真机和语音邮件应答的那些号码 / 分机是稍后遭受攻击的设备。除了“暴力破解”术语意味着黑客尝试攻击进入通信系统的特定设备之外,语音邮件口令暴力破解和分机口令暴力破解与战争式拨号攻击相似。例如,黑客拨打号码序列以获得特定电话分机上的语音邮件的口令。语音邮件可包括专有和机密的组织信息,对语音邮件的未经授权的访问明显造成对组织的风险。长途话费欺诈指的是由已经访问企业的通信系统的某些人(例如雇员)进行未授权的长途电话呼叫或对通信系统的其它未授权的使用而进行的攻击。

[0019] 参照图 2 和图 3,关于示例性通信系统示出本发明的另一个实施例。具体地说,由本发明实现的功能被示出为结合在单独的服务器或网关 30 中,所述单独的服务器或网关 30 与特定企业的现有通信服务器 14 通信。作为单机通信设备 30,可按一个或多个数据库和 / 或一个或多个软件 / 固件应用的形式将服务器 30 描述为通常包括处理器 32、存储器 34、输入设备 36、输出设备 38、通信网络接口 40 以及数据存储器 31。所述应用可包括通信应用和下面将更充分地讨论的攻击防止应用。此外,可在数据存储器中存储操作系统程序和任意其它应用或作为服务器 30 的操作的一部分被存储的数据。就可执行程序指令而言,将本发明的功能描述为数据存储器 31 中的攻击防止应用 33。数据存储器的类型可包括磁存储设备、固态存储设备、光学存储设备、逻辑电路、或这些设备的任意组合。还应当理解,可在数据存储器 31 中维护的应用 / 程序可包括软件、固件或硬布线逻辑。通信总线 42 使得能够在各种组件之间进行通信。处理器 32 可包括用于执行应用程序或指令的任意通用可编程处理器或控制器。此外,处理器可包括特定配置的专用集成电路(ASIC)。处理器 32 一般作为运行实现由服务器 30 执行和 / 或实现的各种功能的程序代码,包括在此描述的各种检测、登记、记录、警告和补救行动。将这些功能中的每一种统称为攻击防止应用 33。可提供存储器 34 以与程序的执行一起使用,并用于临时或长期存储数据或程序指令。存储器 34 可包括诸如 DRAM 和 SDRAM 的固态存储器。其中,处理器 32 包括控制器,存储器 34 可集成到处理器。服务器 30 可包括一个或多个输入设备 36 和一个或多个输出设备 38。本领域技术人

员可理解,可提供的输入设备的示例包括数字键盘、键盘、指针设备等。本领域技术人员还可理解,输出设备 38 的示例包括扬声器、耳机、可视显示器等。提供通信网络接口 40 以将服务器 30 互连到通信网络 12。例如,通信网络接口 40 可包括以太网接口。与通信服务器 30 互连的通信网络的特定类型通常确定通信网络接口。

[0020] 参照图 4,关于示例性通信系统示出本发明的另一个实施例。在图 4 中,TEA-DRIP 服务器 30 位于通信服务器 14 的下游,服务器 30 仅服务于企业的选择的通信设备,诸如调制解调器 50。因此,可理解,本发明可被选择性地结合在通信企业的仅某些部分中。

[0021] 为了设置用于阻止进行中的攻击或防止未来的攻击的协议或方法,本发明提供对呼叫属性的全面分析,其后将风险分配给每一个属性。这些属性包括呼叫源、呼叫目的地、媒体流随机性、呼叫持续时间、呼叫时间、呼叫类型、呼叫容量和呼叫方向。对于每一个接收到的呼叫,可分析这些属性中的每一个,或可仅分析属性中的选择的一个。对于呼叫源,其包括干线 ID、呼叫方 ID 和 IP 地址(如果是 VoIP 呼叫)。攻击者可容易地对呼叫者 ID 或 IP 地址进行欺骗,或以更高的难度对呼叫者 ID 和 IP 地址两者进行欺骗。然而,甚至难以欺骗干线 ID。本发明的方法和系统还具有检测欺骗的呼叫方 ID 和 IP 地址的能力,尤其是声称来自企业内部但却从企业外部发源的那些欺骗的 ID 和地址。例如,可将来自 PSTN 或从 ISP 到达的但却具有来自企业内的地址的数据分组表征为欺骗的 ID 或地址。此外,可进行查找(或反向查找 SIP)以确定 IP 地址或呼叫者 ID 是否为欺骗的。检测欺骗的另一示例包括对从多个源发送的相同的媒体流进行检测。如以下进一步所描述的那样,对于结论为相同的媒体流是从多个源到达的,其媒体流随机性的分析表明呼叫为欺骗的概率很高。为了检测欺骗的干线 ID,可通过分析呼叫的 IP 地址和 / 或呼叫者 ID 来实现在某些情况下对这种欺骗类型的检测。此外,如果提供专用干线以仅处理特定呼叫类型,并且 ANI(自动号码识别)表明在不同干线上到达的呼叫类型,则其指示干线欺骗。如下进一步讨论,本发明的警告和防止方法可根据有多少这三种源属性被欺骗而变化。

[0022] 对于呼叫目的地属性,本发明的系统具有当对顺序分机号码(例如 8000、8001、8002 等)进行呼叫时进行检测的能力。如果攻击者对包括未管理的号码 / 分机的分机的范围进行呼叫,则由于未管理的号码未用于呼出呼叫或呼入呼叫,因此这些号码已经被呼叫的次数可表示可能的攻击。呼出系统消息可相对于管理的号码对攻击者标识未管理的号码。因此,战争式拨号可映射活的号码,包括具有用于稍后采用的语音邮件的那些号码。根据本发明,管理员可故意分配和管理一些未使用 / 未公布的分机号码,以对攻击呼叫设置陷阱。这些分机可被称为“蜜罐”分机。也可使用除了语音的诸如传真、调制解调器或其它呼叫类型的分机号码来监控攻击呼叫。例如,如果在公布的管理的号码范围之外来管理三个分机号码(诸如管理的蜜罐号码),则所有三个分机号码在短时间周期中具有呼叫,则因为在这些未公布的分机上接收任意呼叫的似然率极低,所以可将攻击的可疑或风险评定为高。

[0023] 对于媒体流随机性属性,由于语音通信在特性上是统计性随机的,因此,在不记录和应答呼叫的情况下,攻击者极难复制呼叫,也几乎不值得复制呼叫。因此,本发明可对可疑的呼入媒体流和先前接收的媒体流进行比较以检测唯一性。出于隐私权的原因,不是记录呼入媒体流并将其与其它呼入媒体流进行比较,而是可建立用于可疑呼入流的散列(hash)并且其后进行比较。可将散列定义为应用于呼入流的算法或数学运算,其导致值或

值的范围被分配给每一个接收的媒体流。散列也大大节省数据存储空间,并允许通过简单比较分配的值来进行简单的比较。

[0024] 对于呼叫容量属性,呼叫容量可随日、周、月而改变,但出现模式。如果呼叫容量高,则过多的容量的原因可能是战争式拨号攻击。

[0025] 对于呼叫持续时间属性,如果没有相同的呼叫持续时间,则自动的战争式拨号机器时常发送十分相似的准备好的消息。因此,简单地比较呼叫持续时间也可以是对于许多分机攻击的呼叫唯一性的良好测量措施。

[0026] 对于呼叫时间属性,接收呼叫的时间可以是关于是否已经发生攻击的指示符。尤其是如果企业不具有 24 小时运营,则良好地确定呼叫时间。在工作时间之后进行的呼叫更加被怀疑为攻击。与其它属性组合的工作时间之后的呼叫可帮助确定攻击是否正在进行,或是否正常在工作时间之后进行呼叫。

[0027] 对于呼叫类型属性,这是指呼叫是语音、调制解调器、传真或其它。例如,突然大量的多余的传真呼叫可表示攻击。

[0028] 对于呼叫方向属性,呼叫方向将确定例如是由雇员还是攻击者在企业内生成攻击,其中,攻击者已经获得对一个或多个电话设备的控制并将其用于攻击的目的。此外,如果攻击来源于内部,则可在检测长途话费欺诈尝试或其它潜在的非法使用中考虑呼叫目的地和日的时间。例如,如果在商务时间之后对资费号码进行呼叫,则出现长途话费欺诈。如果从企业外部生成攻击,则可采取其它警告和防止措施。

[0029] 一旦检测到可能的攻击,就能够登记呼叫属性,并通过记录选择的部分或整个媒体流来记录事件。分析呼入呼叫属性,将风险与属性中的每一个关联。分配整体风险或将其与可能的攻击关联,从而确定是否记录事件、警告管理员、并采取补救行动。可用多种方式来确定分配的整体风险,所述方式包括应用各种算法或对攻击签名(即在潜在的攻击上收集的数据)的其它数学关系。此外,可基于群组来分析呼叫,也就是说,可关于在特定时间周期中的呼叫的群组的属性来收集数据,其后,对于企业内的潜在的攻击来分析该群组。可以如何对和呼叫关联的风险进行分配的一个示例是简单三层(three-tier)分类系统,其中,基于一个或多个攻击属性或特征的出现而将属性标识为低、中或高风险。可将潜在的攻击分类以促使有合适的响应或补救行动的另一种方式为:简单地通过将数字值分配给在攻击签名中出现的特定属性,其后对所述值进行求和。如果所述值超过预定阈值,则触发一个或多个补救行动。

[0030] 应当理解,可根据尝试阻止潜在攻击的特定企业的特定需要而将为呼入呼叫所分析的属性与各种风险级别进行关联。此外,可能有自动导致生成高风险评估的某些类型的呼叫属性,因此促使采取合适的补救行动。在时间上,可修改本发明,从而企业可制订与企业的运营最匹配的风险评估和补救行动。可修改呼叫属性风险的一种方式是简单地提供用户接口输入,所述用户接口输入允许用户改变为确定风险级别而分配的任意值或算法,并允许另外操控关于呼叫属性而收集的数据。因此,本发明清楚地期望一种具有与基于规则的系统相比更大灵活性的“智能”系统,在基于规则的系统,用户没有修改风险评估以触发合适的补救行动的能力。当然,可通过修改补救或选择不执行补救而由人工交互来净化所有前述的补救。

[0031] 一旦呼叫或呼叫群组已经被分配有与呼叫关联的风险或整个分类,就关于是否应

该采取补救行动而作出确定。如果有与特定呼叫关联的低风险,则优选的选项可不采取进一步的行动。判断不采取进一步的行动说明,所需的行动仅是登记呼叫的属性,而不是其它所需的行动。因此,不发出告警,或不推荐补救行动。如果分配给特定呼叫的风险级别不为低,而是中或高,则可记录事件,和 / 或可关于攻击的出现而对系统管理员进行告警。可对管理员进行告警的形式可包括:语音邮件消息、电子邮件消息或对管理员的蜂窝电话生成的呼叫等。可指定通信设备 18、20、通信服务器 14 和 TEA-DRIP 服务器 30 登记呼叫属性并记录可疑呼叫。许多电话设备已经具有发送语音消息或拨打蜂窝电话或自动地使寻呼机振铃的内建能力。告警可以是基于风险级别或攻击的复杂级别的一个或多个预先选择的消息。可按最适合于特定企业的那样以实时、延迟或实时和延迟二者的方式来进行告警。在预测未来的攻击、防止未来的攻击以及帮助在跟踪和追踪攻击及攻击者过程中所需的法律执行的过程中,标识的攻击的历史是有用的。

[0032] 此外,可按表的形式将呼叫属性传递给管理员,在表中阐述分析的属性、分配的分类或与呼叫关联的风险以及可从收集的数据得到的其它结论中的每一个。例如,为了在确定将要采取的潜在的补救行动中减轻管理员的负担,传递给管理员的消息可包括用于已经接收到的特定类型的呼叫的一个或多个预定的推荐补救行动。其后,管理员可选择接受推荐的行动,或按照需要而对其进行修改。管理员可经由结合在通信服务器中的交互语音响应 (IVR) 应用选择一个或多个补救行动。如果对管理员告警,并且管理员已经访问系统计算机,则管理员可在告警中生成的用户接口屏幕上选择行动的过程。其后,该选择可使系统通过采取补救行动(例如断开一个或多个通信设备)来作出响应。IVR 功能应该需要来自攻击者的特征访问代码 (FAC) 或用于保持 IVR 访问安全的口令,所述攻击者可能反过来通过攻击 IVR 对通信系统进行控制。

[0033] 在已经对事件进行登记和 / 或记录并且已经告警管理员之后,采取合适的补救行动来防止继续攻击,并防止未来的攻击。补救行动可具有三种一般形式,即手动、自动或自助手动。可将手动补救行动描述为,诸如通过系统管理员的手动工作来禁闭或隔离通信系统或系统的目标部分从而防止正在进行的攻击。手动行动可包括从系统断开特定通信设备,改变限制的类别,并改变分机号码 / 地址。

[0034] 对于自动补救行动,可对系统编程以生成对察觉的攻击的响应,所述响应还可包括从系统断开一个或多个通信设备等。可基于唯一的一组呼叫属性特征或分配给呼叫的数字值的出现来触发自动补救行动。本发明还期望管理员能够基于对专用于特定企业的历史分析(登记)和其它唯一因素来制订这些自动补救行动。

[0035] 自助手动补救行动能力指的是对手动和自动补救行动进行混合的概念。这种类型的补救行动提供增强的功能的情况的一个示例是:如果第二天为母亲节,并且企业是鲜花递送公司,该公司在前一晚上在下班时间订单纷至沓来。异常数量的下班时间的呼叫正常地可触发不合适的自动响应,例如关闭一个或多个通信设备。明显地,由于将会拒绝许多消费者进行访问以订购第二天的鲜花,因此这将是灾难性的补救行动。相应地,管理员知道在这个特殊的夜晚将会有许多下班时间的呼叫,因此应该判断不采取行动。

[0036] 可以被采取以防止攻击或至少进一步分析潜在的攻击的补救行动的其它特定示例包括:(i) 记录事件但不采取防止措施;(ii) 以预先记录的警告消息来响应 SPAM 呼叫者以阻碍未来的呼叫;(iii) 将可疑的呼叫转发到运营商以寻求帮助,或由本地或长途提

供者进行其它分析；(iv) 对来自攻击源的呼叫进行速率限制以防止拒绝服务攻击。（理想地，速率被限制为随机间隔以防止攻击者将其攻击速率调整为与速率限制相匹配）；(v) 终止来自攻击源的呼叫。（传真的 SPAM 是不应该连接到传真机的呼叫的示例）；(vi) 通过暂时地阻塞来自一个源的所有呼叫达到一定时间周期来防止来自攻击源的未来的呼叫。（由于这个行动过程可允许攻击者通过欺骗攻击源而导致拒绝服务，因此该行动过程可能不是理想的；然而，可仅采取阻塞措施达到选择的预定次数，并用于诸如特定可疑的电话号码或 IP 地址的预先选择的呼叫源）；(vii) 记录呼叫以进行手动分析或呼叫追踪；以及 (viii) 请求用于回呼的电话号码 /IP 地址。（最后的措施至少保护企业不会有受欺骗的分机号码）。

[0037] 图 5A 和 5B 示出实现与本发明关联的功能的一个示例，所述功能包括：(i) 分析呼叫属性；(ii) 评估用于呼叫属性的风险；(iii) 记录事件；(iv) 对管理员进行告警；以及 (v) 采取补救行动。如图 5A 所示，生成呼叫作为 IP 或 PSTN 攻击 80。其后分析呼叫的多个属性 82。在分析属性之后，将风险评估 84 分配给呼叫属性。根据图 5A 的示例，为呼叫属性的每一个测量的或估计的特征分配低风险 86、中等风险 88 或高风险 90。返回各种呼叫属性 82，分析的属性可包括：来自源的呼叫的数量（容量）91，欺骗的呼叫源 92、呼叫目的地 94、日的时间 96、呼叫类型 98、呼叫方向 100、呼叫持续时间 102 以及媒体散列值 104。如所讨论的那样，可通过用于呼入媒体流的算法来确定媒体散列值。返回呼叫容量 91，分配风险的一种方式是对在商务时间期间或在商务时间之后发生的呼叫的数量进行分析。在该示例中，参照块 105，如果在商务时间从源接收到不期望的数量的呼叫，则分配低风险，而如果在商务时间之后接收到不期望的数量的呼叫，则分配中等风险。对于呼叫源欺骗的属性 92，如果 IP 地址 106 为欺骗的，则分配低风险。如果呼叫者 ID 为欺骗的，则分配低风险。然而，如果 IP 地址和呼叫者 ID 两者都为欺骗的，则分配中等风险。如果干线 ID 为欺骗的，则分配高风险。如果干线 ID 和任意其它 ID 为欺骗的，则仍旧分配高风险。对于呼叫目的地属性 94，如出现顺序呼叫目的地 112（例如拨打顺序的分机号码），则分配中等风险。对于未管理的号码 114，偶然呼叫或“命中 (hit)”那些号码构成低风险，而高频率地呼叫那些号码代表高风险。对于未管理的号码 116（故意未分配的并密切监控的那些号码），对这些蜜罐号码的呼叫代表高风险。对于日的时间属性 96，在块 118，呼叫关于是在商务时间接收的相对于是在非商务时间期间接收的而被分析。如果在商务时间期间进行呼叫，则分配低风险，而如果在商务时间之外进行呼叫，则分配中等风险。对于呼叫类型属性 98，如在块 120 所示，关于呼叫是语音、传真、调制解调器还是其它而对呼叫进行分类。通常可将调制解调器呼叫表征为高风险，与之相比，语音呼叫通常被表征为中等风险，诸如传真呼叫的其它呼叫通常可被表征为低风险。对于呼叫方向属性 100，在块 122，分析呼叫方向。呼叫向内方向的呼叫是从通信企业内的分机进行的那些呼叫，而呼叫向外方向的呼叫是从企业外部发源的那些呼叫。如果存在呼叫向内方向，则分配高风险，而对呼叫向外方向分配低风险。对于呼叫持续时间属性 102，在块 124 分析呼叫持续时间。如果在所比较的呼叫之间的呼叫持续时间相同，则分配高风险，而将低风险分配给多种呼叫持续时间。例外可应用作为出站呼叫中心的情况，其中，预先记录的消息导致相同的呼叫持续时间。对于媒体散列属性 104，在块 126，如果在所比较的呼叫之间媒体散列值相同，则将事件与高风险关联；而如果媒体散列值不同，则将低风险分配给事件。基于呼叫的单个属性或呼叫属性的组合，为了包括可应

用于特定呼叫的属性的任意数量的规则,确定整体风险评估 127。

[0038] 参照图 5B, 低的整体风险评估导致在块 128 登记选择的呼叫属性。取决于检测的属性, 提供三个选项中的一个, 即 (i) 在块 130 记录媒体流并警告管理员 (诸如通过电子邮件、寻呼机或蜂窝电话呼叫); (ii) 直接采取推荐的补救行动; 或 (iii) 如块 131 所示, 简单地不采取任何进一步的行动。如果分配整体中等风险, 则对选择的呼叫属性进行登记, 警告管理员, 记录媒体流, 其后采取合适的补救行动, 所述补救行动可包括没有任何进一步的行动。如果将高风险与特定呼叫关联, 则对选择的呼叫属性进行登记, 记录媒体流, 通知管理员, 其后采取合适的补救行动。对于高风险的情形, 通常不会不采取一些补救行动。如图 5B 所示, 为将要采取的补救行动提供三个一般选项, 包括手动响应 132、自助手动响应 134 和自动响应 136。对于自助选项 134, 管理员可接受系统提供的选项、取消系统提供的选项、或修改系统提供的选项。最终, 在块 138, 阻止或防止发生攻击。

[0039] 在本发明的另一方面中, 期望仅作为潜在的攻击来分析选择的呼叫。例如, 可以从被分析的呼叫的样本中检测具有在商务时间期间向外方向的语音呼叫, 因为当作为从攻击者发起的呼叫时, 这些类型的呼叫一般具有低风险。

[0040] 在本发明的另一方面中, 一旦已经发生确认的攻击并且标识出攻击源, 从相同攻击源进行的未来呼叫可导致绕开属性分析和风险评估并使补救行动发生或补救行动被推荐。相应地, 可为过去已经证明为攻击源的每一个 IP 地址或电话号码开发“黑名单”。在此情形中, 采取的补救行动可还包括自动记录某些部分或整个媒体流, 并其后终止该呼叫。可对所有攻击以登记的属性的形式维护历史数据, 并提供用于立即阻止或禁止来自所述的地址 / 号码的攻击的旁路指令。

[0041] 本发明的方法和系统具有许多优点。通过分析呼入呼叫的多个属性, 提供较大的灵活性以基于风险评估来生成合适的补救行动。风险评估不是静态的评估; 相反, 管理员可通过对确定属性是否应构成特定风险级别的规则进行操控而随时间来调整风险评估。详细的属性分析以及可修改的风险评估提供了一种“智能”模型, 该“智能”模型可针对特定的企业而被定制, 从而最佳地阻止或防止分机攻击。创建媒体散列允许本发明评估媒体流, 并仅记录媒体散列值, 而非整个媒体流, 从而节省了系统中的可用存储器空间, 并防止由于另外记录实际媒体流而不经意地侵犯隐私权。

[0042] 虽然已关于其优选实施例示出了本发明, 但应当理解, 在此处所附的权利要求的范围内可对本发明进行各种其它改变和修改。

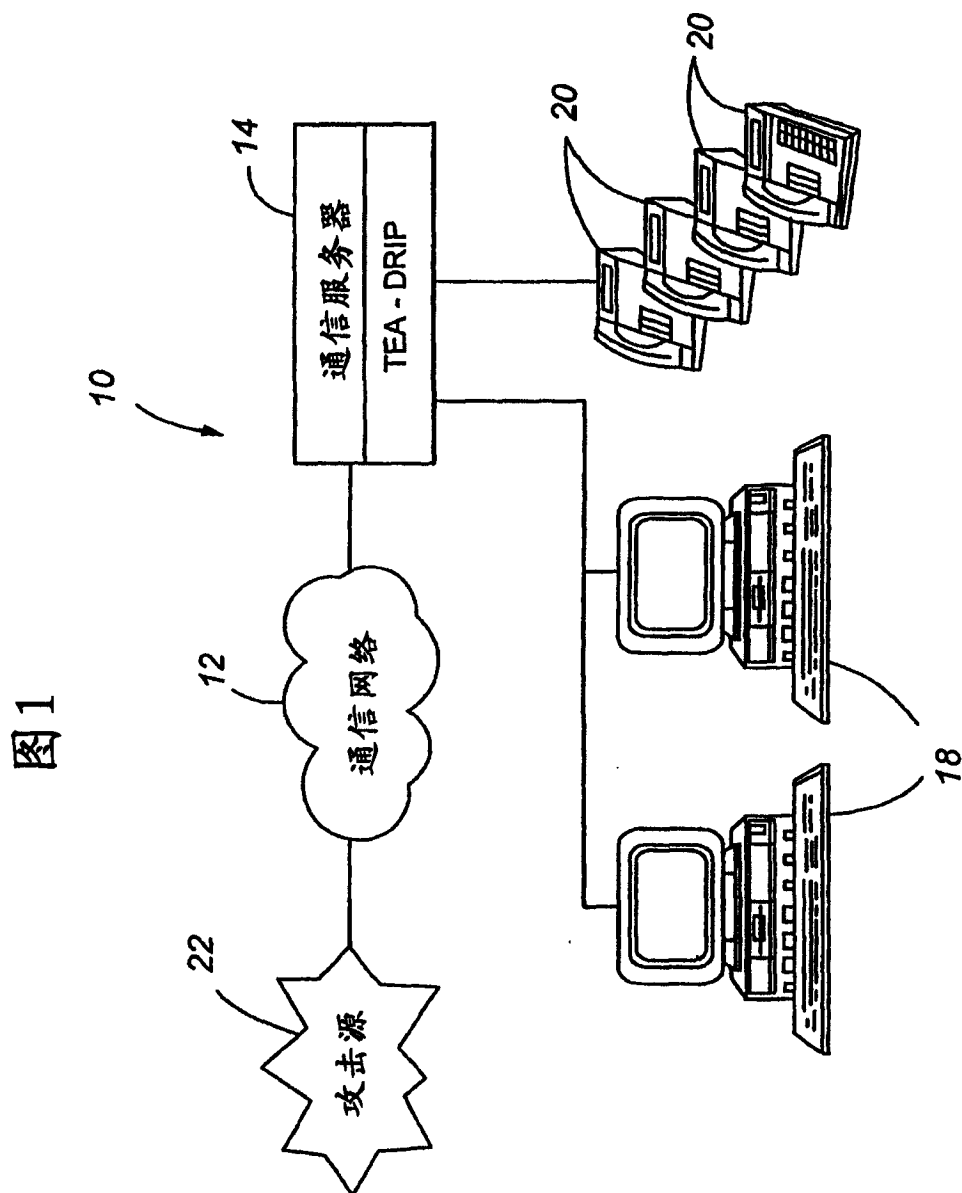


图2

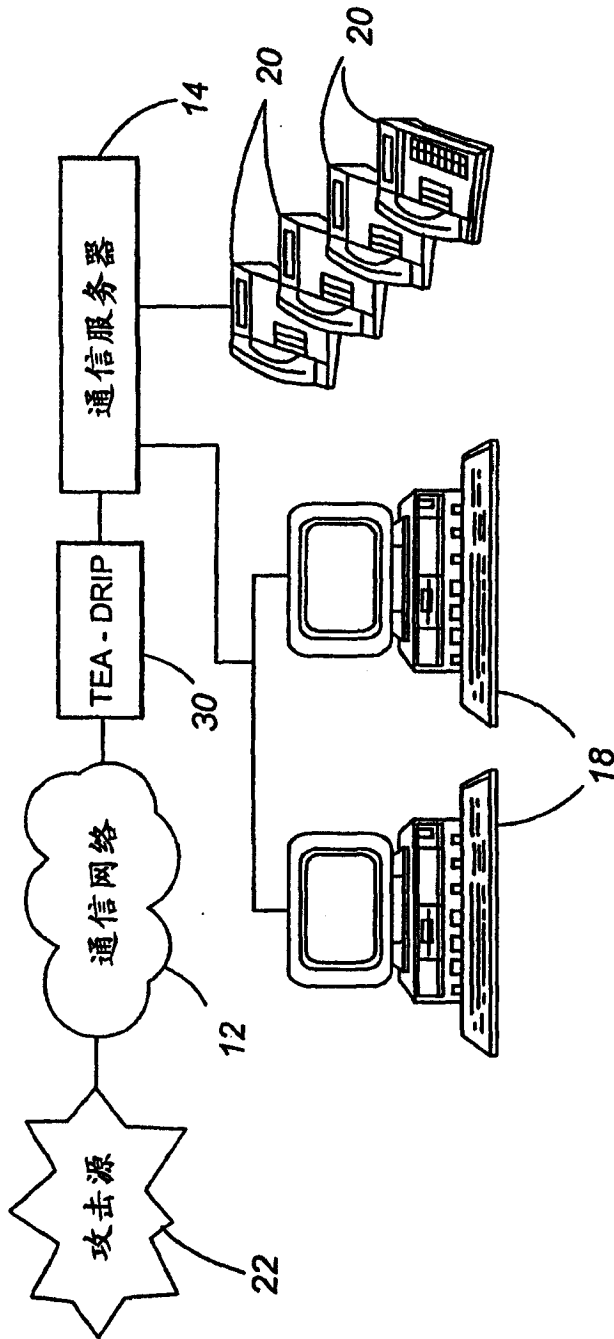


图3

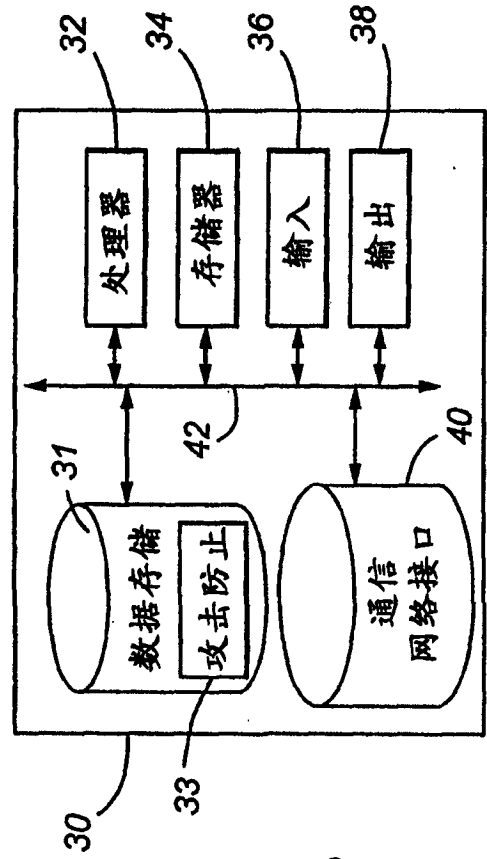


图 4

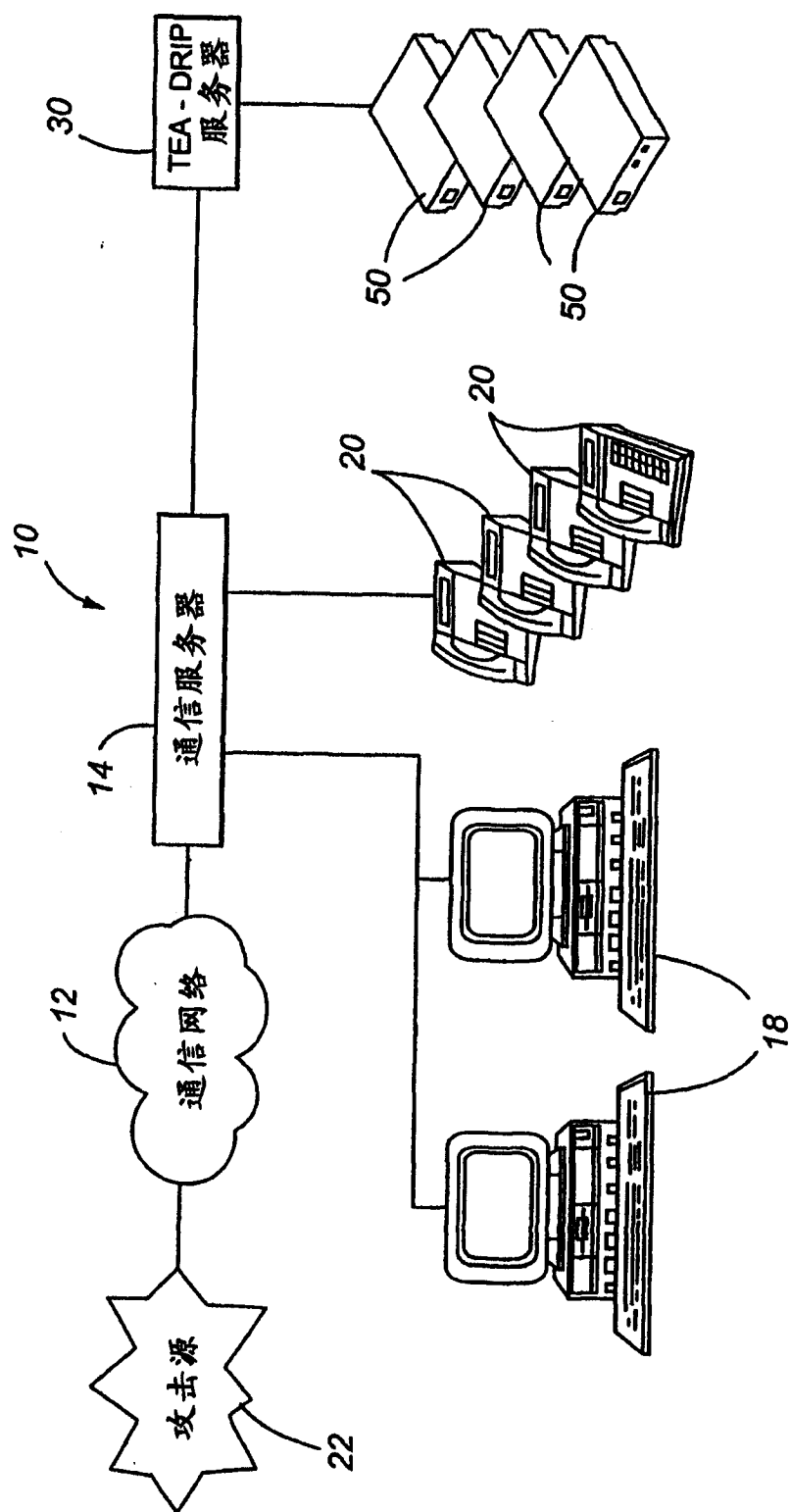
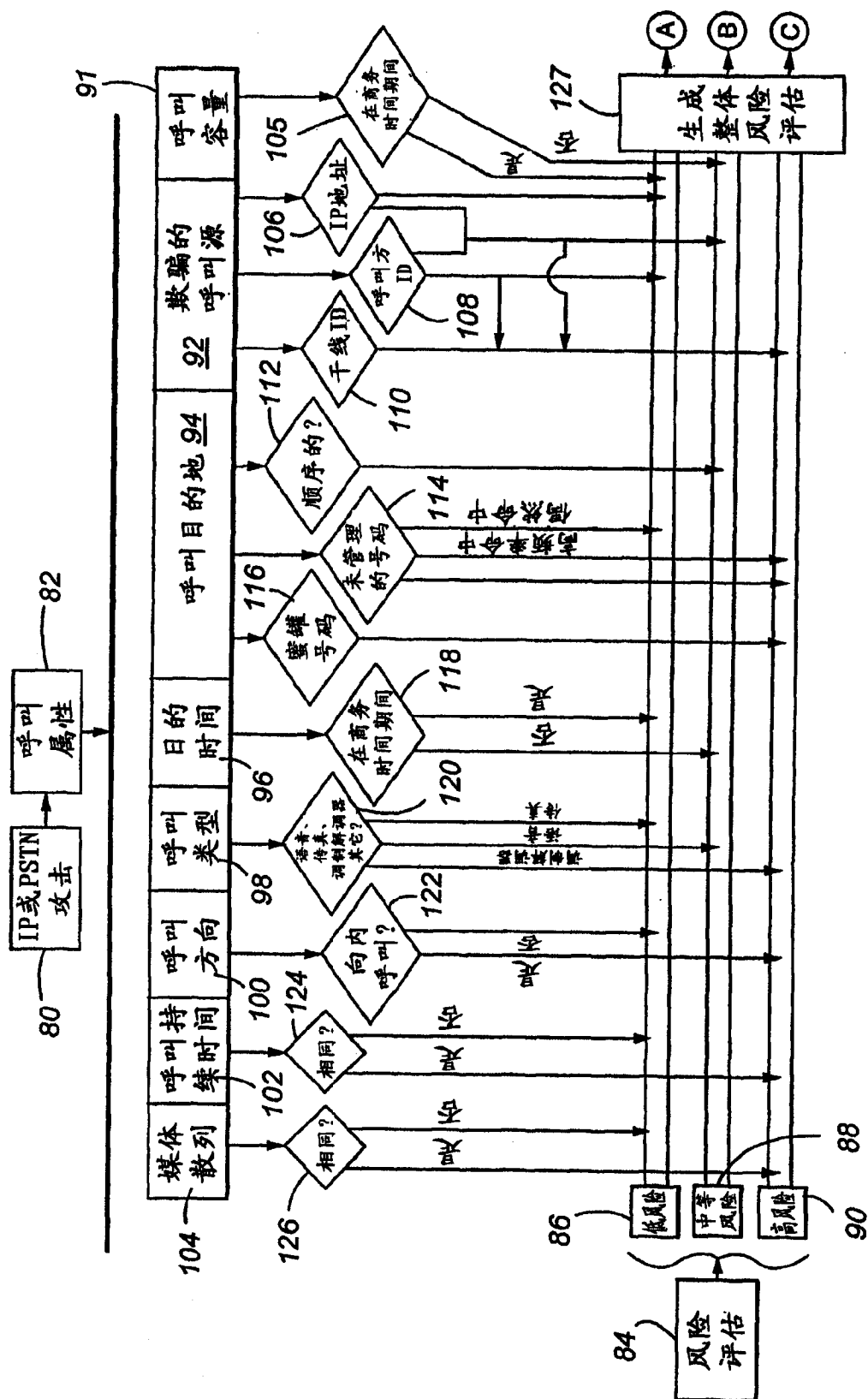


图 5A



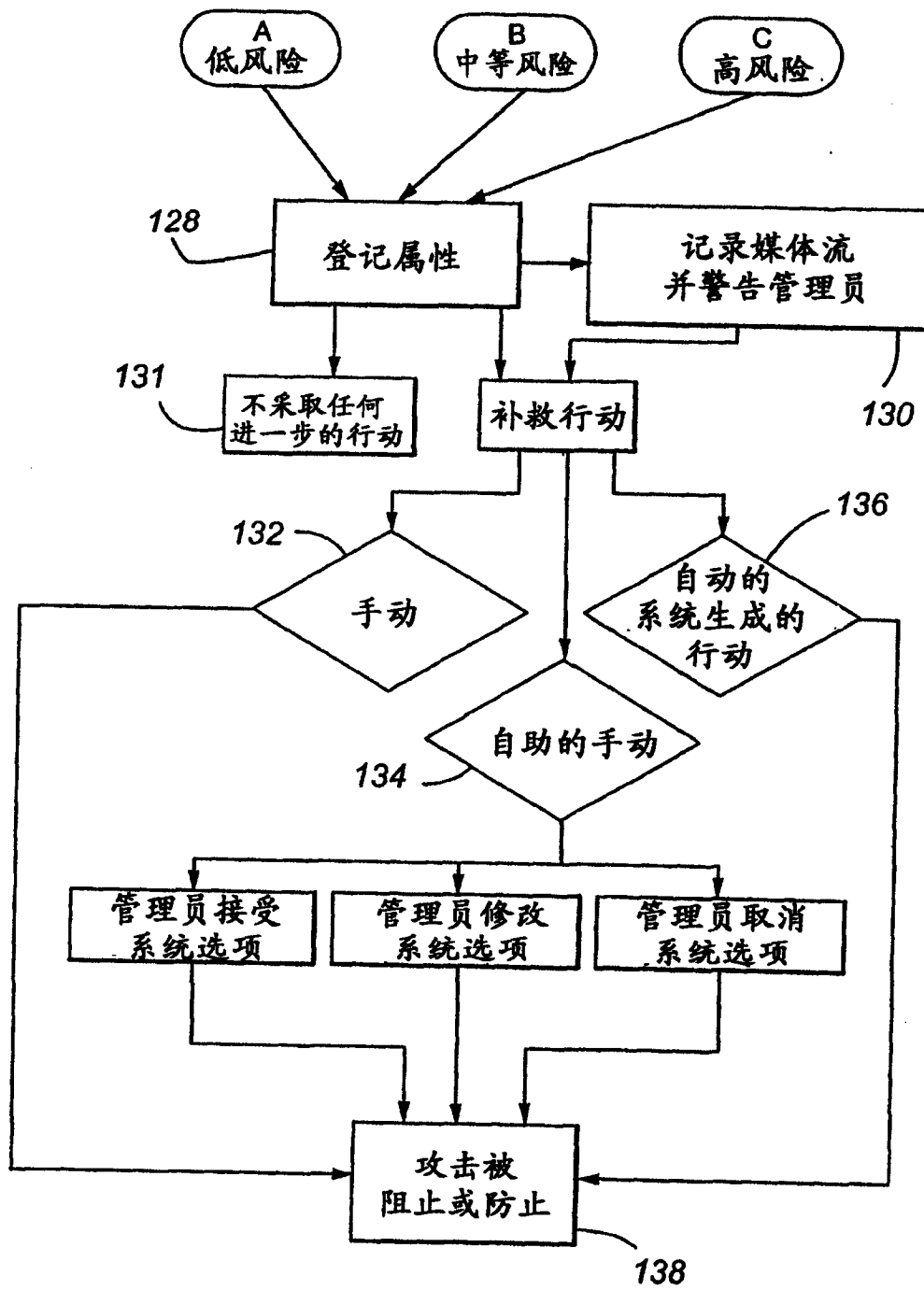


图 5B