(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 105933140 B
(45)授权公告日 2018.12.14

(21)申请号 201610216020.1

(22)申请日 2016.04.10

(65)同一申请的已公布的文献号
申请公布号 CN 105933140 A

(43)申请公布日 2016.09.07

(73)专利权人 广州金越软件技术有限公司
地址 510630 广东省广州市天河区五山路248号金山大厦1202-1204

(72)发明人 张天际

(74)专利代理机构 广州市深研专利事务所 44229
代理人 陈雅平

(51)Int.Cl.
H04L 12/24(2006.01)
H04L 29/06(2006.01)

(56)对比文件
CN 204349586 U,2015.05.20,
CN 101815059 A,2010.08.25,
CN 103327302 A,2013.09.25,
CN 104573914 A,2015.04.29,
CN 101764768 A,2010.06.30,
CN 103139058 A,2013.06.05,
蔡智立.政法业务协作平台研究与实现.《中国优秀硕士学位论文全文数据库》.2015,(第1期),

审查员 刘磊

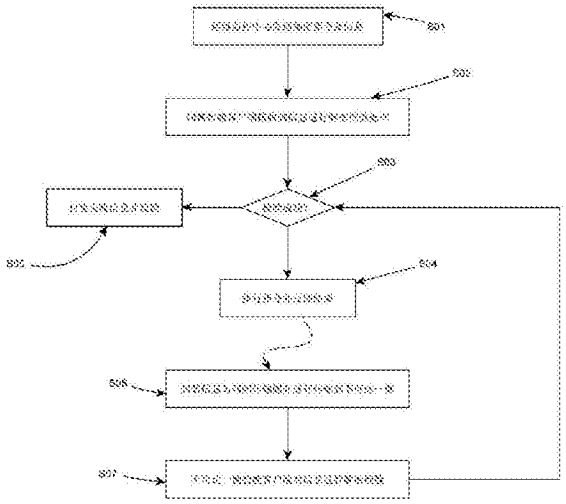
权利要求书1页 说明书4页 附图1页

(54)发明名称

一种智能化跨网络运维监控方法

(57)摘要

本发明公开了一种智能化跨网络运维监控方法，通过定义了一组针对跨网操作的指令格式，包括指令交换、指令解释和指令执行，以状态机形式描述各种操作，比如解释状态、执行状态和交换状态；利用状态机的状态迁移在上述状态之间进行转换，结合客户端消息传输机制完成跨网络信息采集和管理。本发明智能化跨网络运维监控方法在遵循政府部门安全要求的前提下，提升了整个网络的运维监控效率，即使跨网也能够快速有效地对系统或设备进行监控、报警和分析处理。



CN 105933140 B

1.一种智能化跨网络运维监控方法，定义了一组针对跨网操作的指令格式，包括指令交换、指令解释和指令执行，其特征在于，以状态机形式描述各种操作，比如解释状态、执行状态和交换状态；利用状态机的状态迁移在上述状态之间进行转换；状态之间的转换严格遵循指令定义，确保上述操作能够以正确顺序执行，在不同网络区域的内外两端各部署一套智能化客户端系统完成协议适配、信息采集、信息压缩、信息解压工作，跨网络运维监控步骤如下：将监控指令加密发送给可达一侧的智能化客户端；客户端接收到加密消息，解密并进行校验；验证通过，将消息连同元数据信息再次加密压缩，生成特定网闸能够传输的媒介；若校验失败，直接向运维监控中心发送反馈，网络不可达一侧的智能化客户端接收到该媒介，继续进行处理，步骤如下：对媒介进行解压缩和解密，提取出元数据信息和指令；对上述信息进行校验；校验通过则根据指令代替运维监控中心在不可达一侧进行监控操作；并将处理结果以相同机制封装完毕经网闸发送到另一端，由另一侧智能化客户端反馈到运维监控中心；校验失败的处理机制与上一步一致。

2.根据权利要求1所述的一种智能化跨网络运维监控方法，其特征在于，还提供了一种智能化客户端自动更新步骤，用于对智能化客户端进行版本更新，方案如下：运维监控中心将新版本的智能化客户端通过加密方式发送到网络可达一侧的智能化客户端，并提供特殊的加密指令表明进行升级更新；同一侧智能化客户端接收到加密信息，解密并校验，根据该特殊命令提取新版本文件予以执行，将执行结果加密发送到运维监控中心；同侧客户端同时会将该信息封装成网闸可识别媒介，发送到网络不可达一侧，由不可达一侧的智能化客户端解密、提取并进行更新，同时将更新结果以相同机制返回到运维监控中心一侧，避免重复进行更新操作。

一种智能化跨网络运维监控方法

技术领域

[0001] 本发明涉及计算机网络和文件传输技术领域，具体涉及一种如何有效且全面地对一个存在物理隔离区域的网络进行运维监控的策略方法。

背景技术

[0002] 近年来随着政府信息化项目建设的深入铺开，政府各部门间的业务需要将各自的系统关联起来相互协作，因而产生了大量的数据需要进行交换，这些数据一般都需要通过网络进行传输，但政府部门网络不会直接连接到外网，否则就会产生极大的安全隐患，一般做法是根据安全级别将网络划分为若干区域，关键区域和非关键区域之间不能直通而是隔离开来，这需要通过一种称为网闸的类似设备代为进行通信。

[0003] 但是这就会对网络及网络内部应用系统的运维监控带来障碍，传统的运维监控方案一般都要求所监控的网络到处可达，以便于其采集监控信息，隔离区域的出现，使得这种传统方式不再奏效，要么通过人工方式交换数据，要么只能在各个隔离开的网络区域内分开收集和处理这些数据，这就会导致运维管理效率低下，网络内部系统出现问题不能及时报警，从而影响到部门的正常工作。

[0004] 因此，如何在保障安全性的前提下，有效提升跨网络设备和系统的运维监控效率，就成为一个亟待解决的问题。

发明内容

[0005] 本发明的目的在于提供一种智能化跨网络运维监控方法，以解决上述背景技术中提出的问题。

[0006] 为实现上述目的，本发明提供如下技术：

[0007] 首先定义了一组针对跨网操作的指令格式，包括指令交换、指令解释和指令执行，以状态机形式描述各种操作，比如解释状态、执行状态和交换状态；其次利用状态机的状态迁移在上述状态之间进行转换；状态之间的转换严格遵循指令定义，确保上述操作能够以正确顺序执行；最后在不同网络区域的内外两端各部署一套智能化客户端系统完成协议适配、信息采集、信息压缩、信息解压工作。

[0008] 跨网络运维监控步骤如下：将监控指令加密发送给可达一侧的智能化客户端；客户端接收到加密消息，解密并进行校验；验证通过，将消息连同元数据信息再次加密压缩，生成特定网闸能够传输的媒介；若校验失败，直接向运维监控中心发送反馈，网络不可达一侧的智能化客户端接收到该媒介，继续进行处理，步骤如下：对媒介进行解压缩和解密，提取出元数据信息和指令；对上述信息进行校验；校验通过则根据指令代替运维监控中心在不可达一侧进行监控操作；并将处理结果以相同机制封装完毕经网闸发送到另一端，由另一侧智能化客户端反馈到运维监控中心；校验失败的处理机制与上一步一致。

[0009] 作为本发明的优选方案：本发明还提供了一种智能化客户端自动更新机制，用于对智能化客户端进行版本更新，确保跨网络自动化运维监控的稳定，方案如下：运维监控中

心将新版本的智能化客户端通过加密方式发送到网络可达一侧的智能化客户端，并提供特殊的加密指令表明进行升级更新；同一侧智能化客户端接收到加密信息，解密并校验，根据该特殊命令提取新版本文件予以执行，将执行结果加密发送到运维监控中心；同侧客户端同时会将该信息封装成网闸可识别媒介，发送到网络不可达一侧，由不可达一侧的智能化客户端解密、提取并进行更新，同时将更新结果以相同机制返回到运维监控中心一侧，避免重复进行更新操作。

[0010] 与现有技术相比，本发明的有益效果是：本发明智能化跨网络运维监控方法在遵循政府部门环境安全要求的前提下，提升了整个网络的运维监控效率，即使跨网也能够快速有效地对系统或设备进行监控、报警和分析处理。

附图说明

[0011] 图1是本发明的一具体实施例流程图，

[0012] 图2是本发明进行版本更新的实施例流程图。

具体实施方式

[0013] 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0014] 请参阅图1-2，一种智能化跨网络运维监控方法，定义了一组针对跨网操作的指令格式，包括指令交换、指令解释和指令执行，以状态机形式描述各种操作，比如解释状态、执行状态和交换状态；利用状态机的状态迁移在上述状态之间进行转换；状态之间的转换严格遵循指令定义，确保上述操作能够以正确顺序执行，在不同网络区域的内外两端各部署一套智能化客户端系统完成协议适配、信息采集、信息压缩、信息解压工作，跨网络运维监控步骤如下：将监控指令加密发送给可达一侧的智能化客户端；客户端接收到加密消息，解密并进行校验；验证通过，将消息连同元数据信息再次加密压缩，生成特定网闸能够传输的媒介；若校验失败，直接向运维监控中心发送反馈，网络不可达一侧的智能化客户端接收到该媒介，继续进行处理，步骤如下：对媒介进行解压缩和解密，提取出元数据信息和指令；对上述信息进行校验；校验通过则根据指令代替运维监控中心在不可达一侧进行监控操作；并将处理结果以相同机制封装完毕经网闸发送到另一端，由另一侧智能化客户端反馈到运维监控中心；校验失败的处理机制与上一步一致。

[0015] 本发明还提供了一种智能化客户端自动更新机制，用于对智能化客户端进行版本更新，确保跨网络自动化运维监控的稳定，方案如下：运维监控中心将新版本的智能化客户端通过加密方式发送到网络可达一侧的智能化客户端，并提供特殊的加密指令表明进行升级更新；同一侧智能化客户端接收到加密信息，解密并校验，根据该特殊命令提取新版本文件予以执行，将执行结果加密发送到运维监控中心；同侧客户端同时会将该信息封装成网闸可识别媒介，发送到网络不可达一侧，由不可达一侧的智能化客户端解密、提取并进行更新，同时将更新结果以相同机制返回到运维监控中心一侧，避免重复进行更新操作。

[0016] 本发明的工作原理是：本发明一实施例采用上述策略，对存在物理隔离的网络进

行跨网络监控，具体步骤如下：

[0017] 在网络可达一侧部署运维监控中心和智能化客户端，不可达一侧的智能化客户端只需要介质安装一次；

[0018] S01，运维监控中心发起指令采集全网各个监控设备或系统的相关信息；

[0019] 发起的指令包含以下信息：

[0020] 事件ID；

[0021] 发送方唯一标识符，包含发送方网络信息包括地址等；

[0022] 需要执行的指令；

[0023] 执行指令所需的数据信息；

[0024] 时间戳；

[0025] 关联事务ID；

[0026] 一个特殊的校验码，用于对该信息进行验证，该校验码包含运维监控中心的主要软硬件信息。

[0027] 信息经过对称加密后，使用特定协议，通过下面两种方式发送该信息：

[0028] 广播，适用于初始部署环境；

[0029] 根据运维监控中心已注册的智能客户端信息分别定向发送。

[0030] S02，可达网络一侧的智能客户端接收到该信息，首先对信息进行解密，得到原始的信息数据；利用校验码对信息数据进行校验，确保接收到的数据是由运维监控中心所发出。

[0031] S03，校验通过，根据指令及指令数据予以执行；执行后的结果，无论成功与否，都将封装到一个单一信息中，该信息包含以下属性：

[0032] 事件ID；

[0033] 发送方唯一标识符；

[0034] 指令；

[0035] 指令执行结果及数据；

[0036] 时间戳；

[0037] 关联的事务ID；

[0038] 校验码。

[0039] S04-S05，智能化客户端将该信息加密并根据原发送方唯一标识符将加密信息发送到运维监控中心，后者接收到反馈信息，解密后校验再进行进一步处理。

[0040] S06，可达网络一侧的客户端(称之为A)，还需要将接收到的信息处理后发送到网闸另一端，以便隔离网络一侧的客户端(称之为B)执行该指令，这需要进行以下步骤：

[0041] A在原有信息的基础上，增加一个转发标识；

[0042] A将该转发标识与原有信息一起加密，压缩生成网闸能够传输的媒介(一般为文件)；

[0043] 网闸将该媒介转移至B所在一侧；

[0044] S07，B接收到该信息，对获取到的媒介进行逆向处理；

[0045] 执行S03所表示的步骤。

[0046] 通过上述方式，即实现了对全网各设备和应用的监控。

[0047] 本发明的另一个实施例，是智能化客户端的版本自动更新，实施过程如下：

[0048] S08，运维监控中心发起指令对全网客户端进行版本更新；

[0049] 发起的指令包含以下信息：

[0050] 事件ID；

[0051] 发送方唯一标识符，包含发送方网络信息包括地址等；

[0052] 版本更新指令；

[0053] 更新版本文件；

[0054] 时间戳；

[0055] 关联事务ID；

[0056] 一个特殊的校验码，用于对该信息进行验证，该校验码包含运维监控中心的主要软硬件信息。

[0057] 使用广播或定向方式发送版本更新信息；

[0058] S09，可达网络一侧的智能客户端接收到该信息，首先对信息进行解密，得到原始的信息数据；利用校验码对信息数据进行校验，确保接收到的数据是由运维监控中心所发出。

[0059] S10，校验通过，注意此处与S03的不同，此时客户端将Fork出一个守护进程，用于监控版本更新状态；

[0060] S11，更新成功，守护进程将控制权转移给新更新的客户端，由后者发送反馈；

[0061] S12，更新失败，守护进程执行回滚操作，对原客户端进行还原，同时将控制权转移给还原后的客户端，并发送反馈；

[0062] S13，可达网络一侧更新后的客户端(称之为C)，还需要将接收到的信息处理后发送到网闸另一端，以便隔离网络一侧的客户端(称之为D)以进行版本更新，这需要进行以下步骤：

[0063] C在原有信息的基础上，增加一个转发标识；

[0064] C将该转发标识与原有信息一起加密，压缩生成网闸能够传输的媒介(一般为文件)；

[0065] 网闸将该媒介转移至D所在一侧；

[0066] S14，D接收到该信息，对获取到的媒介进行逆向处理；

[0067] 执行S10所表示的步骤。

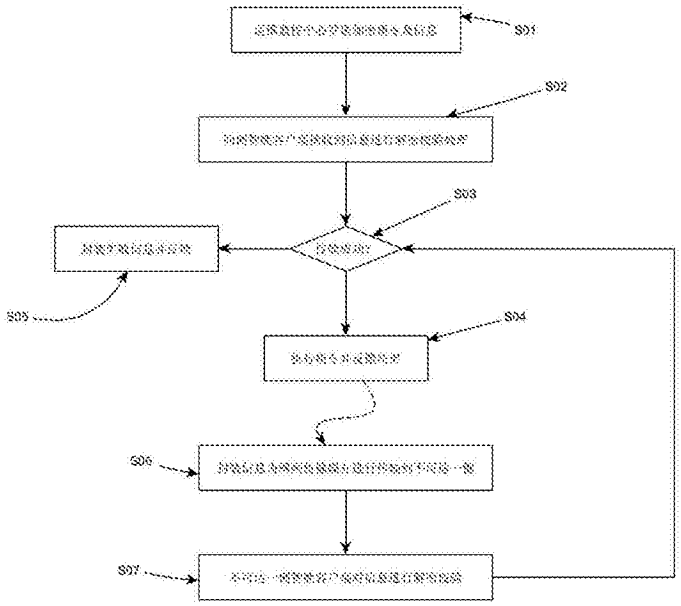


图1

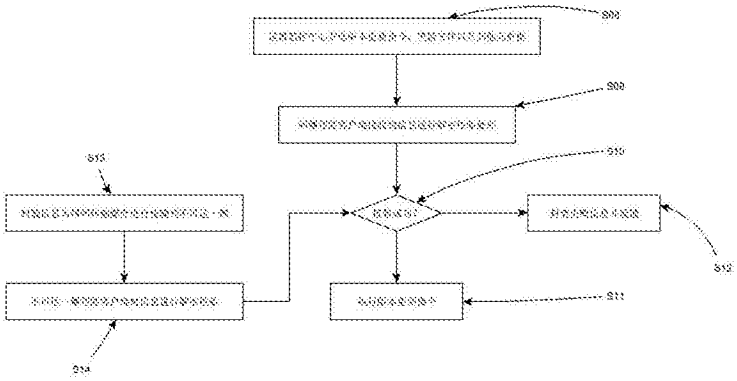


图2