(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 104113532 A
(43)申请公布日 2014.10.22

(21)申请号 201410308002.7

(22)申请日 2014.06.30

(71)申请人 公安部交通管理科学研究所
地址 214151 江苏省无锡市滨湖区钱荣路88号

(72)发明人 张捷 江海龙 吴晓东 陈学浩 全喜伟 李建民

(74)专利代理机构 无锡市大为专利商标事务所（普通合伙） 32104
代理人 曹祖良

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/08(2006.01)
H04L 9/32(2006.01)

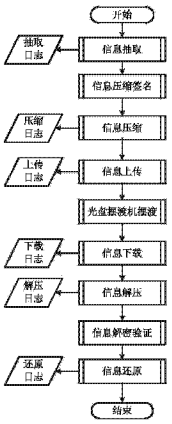
权利要求书2页 说明书4页 附图4页

(54)发明名称

物理隔离网络间信息自动安全交换的方法

(57)摘要

本发明提供了物理隔离网络间，在符合国家相关信息安全法规的基础上，进行不同网络间信息自动交换的一种实现方法。其能有效的提升不同网络间的信息交换效率，并大大缩短信息交换的延迟时间。其包括信息抽取、信息压缩、信息加密、信息传输、信息解密、信息解压、信息还原、信息交换监测等步骤，实现了完整闭环信息传输机制，使得信息交换实现了自动化。以光盘摆渡机的信息自动刻录、移动和读取动作代替了人工手动的光盘刻录拷贝动作，避免了效率低下、重复性工作多、容易出错等问题。本发明适用于公安或政府机构专网和公共信息网间的信息交换。



CN 104113532 A

1. 一种物理隔离网络间信息自动安全交换的方法，其特征在于，包括下述步骤：

步骤一．信息抽取：在物理隔离网络的两端，分别以定时任务方式读取配置信息，按照更新时间增量更新和以导出标记为条件抽取数据库中的信息，将配置的字段信息组织为XML文档；完成抽取后记录每条抽取记录的信息抽取日志信息；

步骤二：信息加密压缩，包括：

在物理隔离网络的两端，分别以定时任务方式读取抽取的XML文档，对XML文档以另一端服务器的公钥进行加密，并以本网服务器的私钥对加密后的XML文档进行签名后生成签名文件，将加密后的XML文档和签名文件压缩进一个有密码保护的文件中；完成压缩后记录每个操作的压缩日志信息；

在物理隔离网络的两端，分别以定时任务方式读取更新时间大于时间基线的文件服务器中文件，对读取的文件以另一端服务器的公钥进行加密，并以本网服务器的私钥对加密后的文件进行签名后生成签名文件，将加密后的文件和签名文件压缩进一个有密码保护的文件中；完成压缩后记录每个操作的压缩日志信息；

步骤三．信息传输，包括：

物理隔离网络的两端，分别以定时任务方式读写压缩文件，以Ftp协议将压缩文件传输到指定的Ftp服务器中；完成传输后记录每个操作的上传日志信息；

光盘摆渡机在物理隔离网络的两端的前置服务程序定时从本网端Ftp服务器上读取文件，读取的文件刻录到本网端的光驱的光盘中，待刻录完成后控制光驱和光盘摆渡机把光盘移动到另一网端的光驱中，另一网端的前置服务程序读取光盘中的内容把信息上传另一网端的Ftp服务器；

物理隔离网络的两端，分别以定时任务方式，以Ftp协议访问Ftp服务器下载文件信息；完成下载信息后记录每个操作的下载日志信息；

步骤四．信息解密和验证，包括：

物理隔离网络的两端，分别以定时任务方式读取下载的压缩文件，解压文件后获得加密文件和签名文件，以另一网端服务器的公钥对签名文件信息进行验证，并以本网端服务器的私钥对加密文件进行解密；

对解密后获取的普通文件按照配置要求传输到指定文件服务器，对解密后的XML文档存储到数据库中；完成解密和验证后记录每个操作的解压日志信息；

步骤五．信息还原，包括：

物理隔离网络的两端，分别以定时任务方式读取解密后的XML文档，对XML文档进行解析后按照配置以每一个子元素组为一条记录插入或更新指定数据库表；完成信息还原操作后记录每个操作的信息还原日志信息。

2. 如权利要求1所述的物理隔离网络间信息自动安全交换的方法，其特征在于：

所述步骤一中，组织XML文档时，将每条数据库记录为一个子元素组，XML文档中的每个字段以数据库记录中的字段名为子元素的属性。

3. 如权利要求1所述的物理隔离网络间信息自动安全交换的方法，其特征在于：

所述步骤二中，压缩格式为Zip格式。

4. 如权利要求1所述的物理隔离网络间信息自动安全交换的方法，其特征在于：所述步骤五之后还包括一个信息交换检测的步骤六：

物理隔离网络的两端，分别以定时任务方式读取时间基线后的解压日志和信息还原日志信息，并经过信息抽取、信息加密及签名、信息压缩、信息传输、信息解压、信息解密及验证、信息还原一系列步骤传送到另一网端，并更新另一网端对应的信息压缩日志和信息抽取日志信息；

物理隔离网络的两端，分别以定时任务方式检测信息压缩日志和信息抽取日志信息，对指定时间内未标记完成信息解压和信息还原操作的记录，更新相应标记，使这条记录重新进行信息加密及签名操作、信息压缩、信息传输、信息解压、信息解密及验证、信息还原一系列步骤传送到另一网端。

物理隔离网络间信息自动安全交换的方法

技术领域

[0001] 本发明涉及一种网络信息安全交换的方法，尤其涉及物理隔离网络间文件和数据库格式信息自动安全交换的实现方法。适用于公安或政府机构专网和公共信息网间的信息交换。

背景技术

[0002] 国家保密局《计算机信息系统国际联网保密管理规定》中要求“涉及国家秘密的计算机信息系统，不得直接或间接地与国际互联网或其它公共信息网络相连接，必须实行物理隔离”。按照要求，物理隔离网络间进行数据的交换，只能采用光盘刻录、拷贝的方式。这种方式存在效率低下、重复性工作多、容易出错等问题，不适应于信息连续性交换的要求。

发明内容

[0003] 本发明的目的在于提供一种物理隔离网络间信息自动安全交换的方法，对存储在不同网络环境下的信息经抽取成 XML 文档、加密压缩、Ftp 传输、解压解密、XML 信息解析等步骤进行自动交换，一方面保证了信息交换的安全性，另一方面提高了效率，避免了出错。本发明采用的技术方案是：

一种物理隔离网络间信息自动安全交换的方法，包括下述步骤：

步骤一．信息抽取：在物理隔离网络的两端，分别以定时任务方式读取配置信息，按照更新时间增量更新和以导出标记为条件抽取数据库中的信息，将配置的字段信息组织为 XML 文档；完成抽取后记录每条抽取记录的信息抽取日志信息；

步骤二：信息加密压缩，包括：

在物理隔离网络的两端，分别以定时任务方式读取抽取的 XML 文档，对 XML 文档以另一端服务器的公钥进行加密，并以本网服务器的私钥对加密后的 XML 文档进行签名后生成签名文件，将加密后的 XML 文档和签名文件压缩进一个有密码保护的文件中；完成压缩后记录每个操作的压缩日志信息。

[0004] 在物理隔离网络的两端，分别以定时任务方式读取更新时间大于时间基线的文件服务器中文件，对读取的文件以另一端服务器的公钥进行加密，并以本网服务器的私钥对加密后的文件进行签名后生成签名文件，将加密后的文件和签名文件压缩进一个有密码保护的文件中；完成压缩后记录每个操作的压缩日志信息；

步骤三．信息传输，包括：

物理隔离网络的两端，分别以定时任务方式读写压缩文件，以 Ftp 协议将压缩文件传输到指定的 Ftp 服务器中；完成传输后记录每个操作的上传日志信息；

光盘摆渡机在物理隔离网络的两端的前置服务程序定时从本网端 Ftp 服务器上读取文件，读取的文件刻录到本网端的光驱的光盘中，待刻录完成后控制光驱和光盘摆渡机把光盘移动到另一网端的光驱中，另一网端的前置服务程序读取光盘中的内容把信息上传另一网端的 Ftp 服务器；

物理隔离网络的两端，分别以定时任务方式，以 Ftp 协议访问 Ftp 服务器下载文件信息；完成下载信息后记录每个操作的下载日志信息；

步骤四．信息解密和验证，包括：

物理隔离网络的两端，分别以定时任务方式读取下载的压缩文件，解压文件后获得加密文件和签名文件，以另一网端服务器的公钥对签名文件信息进行验证，并以本网端服务器的私钥对加密文件进行解密；

对解密后获取的普通文件按照配置要求传输到指定文件服务器，对解密后的 XML 文档存储到数据库中；完成解密和验证后记录每个操作的解压日志信息；

步骤五．信息还原，包括：

物理隔离网络的两端，分别以定时任务方式读取解密后的 XML 文档，对 XML 文档进行解析后按照配置以每一个子元素组为一条记录插入或更新指定数据库表；完成信息还原操作后记录每个操作的信息还原日志信息。

[0005] 步骤六．信息交换检测：

物理隔离网络的两端，分别以定时任务方式读取时间基线后的解压日志和信息还原日志信息，并经过信息抽取、信息加密及签名、信息压缩、信息传输、信息解压、信息解密及验证、信息还原一系列步骤传送到另一网端，并更新另一网端对应的信息压缩日志和信息抽取日志信息。

[0006] 物理隔离网络的两端，分别以定时任务方式检测信息压缩日志和信息抽取日志信息，对指定时间内未标记完成信息解压和信息还原操作的记录，更新相应标记，使这条记录重新进行信息加密及签名操作、信息压缩、信息传输、信息解压、信息解密及验证、信息还原一系列步骤传送到另一网端。

[0007] 本发明的优点在于：

1）形成了经信息抽取、信息加密及签名、信息压缩、信息传输、信息解压、信息解密及验证、信息还原、信息交换监测出错后再返回到信息加密的完整闭环信息传输机制，使得信息交换实现了自动化。

[0008] 2）信息传输过程中基于公、私钥的信息安全加密机制。基于 RSA 算法生成 1024 位的密钥，在信息传输前对数据进行加密和签名操作，在接收信息后再进行验证和解密操作，保证信息传输过程中的安全性和完整性。

[0009] 3）基于光盘摆渡机的光盘自动刻录、移动和读取。以光盘摆渡机的信息自动刻录、移动和读取动作代替了人工手动的光盘刻录拷贝动作，避免了效率低下、重复性工作多、容易出错等问题。

附图说明

[0010] 图 1 为本发明的物理隔离网络间信息交换系统构成图。

[0011] 图 2 为本发明的物理隔离网络间信息交换流程图。

[0012] 图 3a 和图 3b 为本发明的物理隔离网络间信息交换监控流程图。

具体实施方式

[0013] 如图 1 所示，为物理隔离网络的结构组成示意图。A 网络和 B 网络都包含数据库、

文件服务器和FTP服务器。A网络和B网络之间是隔离的，依靠设置在两者之间的光盘摆渡机来沟通信息。光盘摆渡机具备刻录光盘、将光盘从一侧网络移动到另一侧网络、光盘读取的功能。

[0014] 本发明提出的物理隔离网络间信息自动安全交换的方法，包括下述步骤：

步骤一．信息抽取：

在物理隔离网络的两端，分别以定时任务方式读取配置信息，按照更新时间增量更新和以导出标记为条件抽取数据库中的信息，将配置的字段信息组织为XML文档，每条数据库记录(比如一个二维表格中的一行)为一个子元素组，XML文档中的每个字段以数据库记录中的字段名为子元素的属性。完成抽取后记录每条抽取记录的信息抽取日志信息。

[0015] 数据库的数据类型包括字符串、数字、时间等全部基本类型外还支持扩展的BLOB和CLOB等大字段数据类型。

[0016] 步骤二．信息加密压缩；包括对抽取的XML文档和文件服务器中的文件的信息加密压缩。

[0017] 在物理隔离网络的两端，分别以定时任务方式读取抽取的XML文档，对XML文档以另一端服务器的公钥进行加密，并以本网服务器的私钥对加密后的XML文档进行签名后生成签名文件，将加密后的XML文档和签名文件以Zip格式压缩进一个有密码保护的文件中。完成压缩后记录每个操作的压缩日志信息。

[0018] 在物理隔离网络的两端，分别以定时任务方式读取更新时间大于时间基线的文件服务器中文件，对读取的文件以另一端服务器的公钥进行加密，并以本网服务器的私钥对加密后的文件进行签名后生成签名文件，将加密后的文件和签名文件以Zip格式压缩进一个有密码保护的文件中。完成压缩后记录每个操作的压缩日志信息。

[0019] 此步骤中，加密采用RSA算法，公钥和私钥的长度都是1024位。文件服务器中的文件包括二进制和文本文件。

[0020] 步骤三．信息传输：

物理隔离网络的两端，分别以定时任务方式读写压缩文件，以PASV模式的Ftp协议下将压缩文件传输到指定的Ftp服务器中。完成传输后记录每个操作的上传日志信息。

[0021] 光盘摆渡机在物理隔离网络的两端的前置服务程序定时从本网端Ftp服务器上读取文件，读取的文件刻录到本网端的光驱的光盘中，待刻录完成后控制光驱和光盘摆渡机中的机械手把光盘移动到另一网端的光驱中，另一网端的前置服务程序读取光盘中的内容把信息上传另一网端的Ftp服务器。

[0022] 物理隔离网络的两端，分别以定时任务方式，以PASV模式的Ftp协议访问Ftp服务器下载文件信息。完成下载信息后记录每个操作的下载日志信息。

[0023] 此处作一简单说明，光盘摆渡机通常有两个光驱，其中一个光驱作为A网络前置机的连接设备；另一个光驱作为B网络前置机的连接设备。A网络前置机和B网络前置机都是服务器或者PC机，上面运行有前置服务程序；A网络前置机和B网络前置机是分设在两个隔离的A网络和B网络中的。

[0024] 步骤四．信息解密和验证：

物理隔离网络的两端，分别以定时任务方式读取下载的压缩文件，解压文件后获得加密文件和签名文件，以另一网端服务器的公钥对签名文件信息进行验证，并以本网端服务

器的私钥对加密文件进行解密。

[0025] 对解密后获取的普通文件按照配置要求传输到指定文件服务器，对解密后的 XML 文档存储到数据库中。完成解密和验证后记录每个操作的解压日志信息。

[0026] 步骤五．信息还原：

物理隔离网络的两端，分别以定时任务方式读取解密后的 XML 文档，对 XML 文档进行解析后按照配置以每一个子元素组为一条记录插入或更新指定数据库表。完成信息还原操作后记录每个操作的信息还原日志信息。

[0027] 步骤六．信息交换检测：

物理隔离网络的两端，分别以定时任务方式读取时间基线后的解压日志和信息还原日志信息，并经过信息抽取、信息加密及签名、信息压缩、信息传输、信息解压、信息解密及验证、信息还原一系列步骤传送到另一网端，并更新另一网端对应的信息压缩日志和信息抽取日志信息。

[0028] 物理隔离网络的两端，分别以定时任务方式检测信息压缩日志和信息抽取日志信息，对指定时间内未标记完成信息解压和信息还原操作的记录，更新相应标记，使这条记录重新进行信息加密及签名操作、信息压缩、信息传输、信息解压、信息解密及验证、信息还原一系列步骤传送到另一网端。

[0029] 本发明能有效的提升物理隔离网络间的信息交换效率，并大大缩短信息交换的延迟时间。

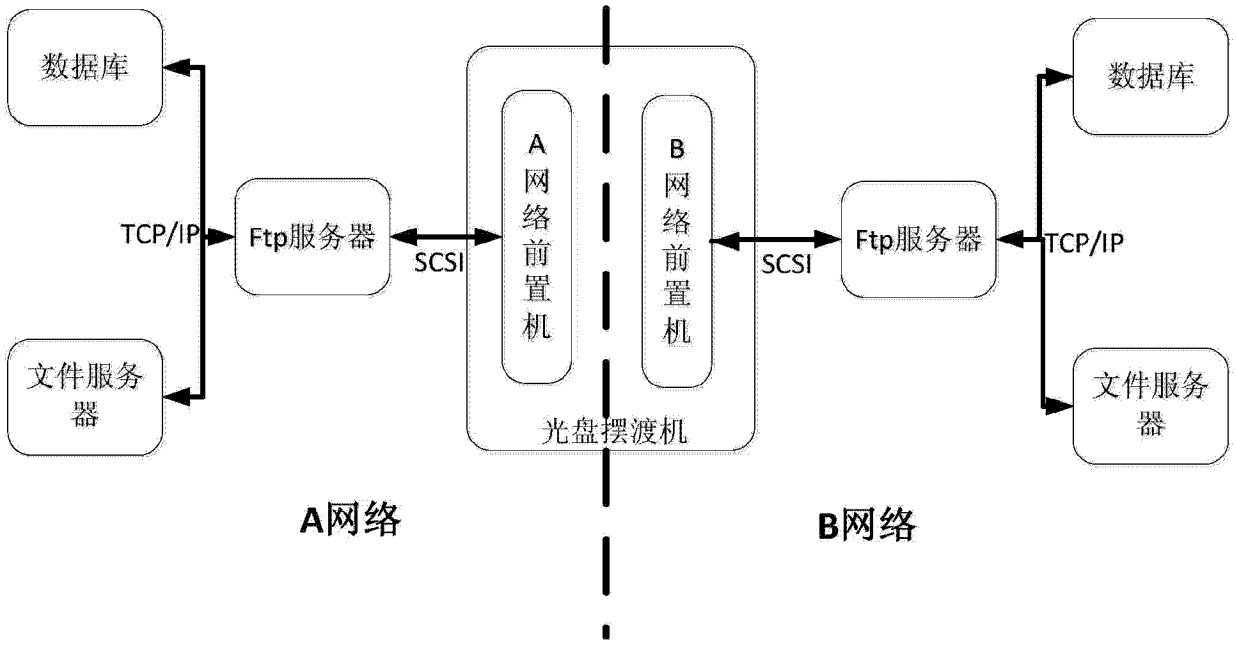

数据库
TCP/IP
Ftp服务器
SCSI
A网络前置机
B网络前置机
光盘摆渡机
SCSI
Ftp服务器
TCP/IP
数据库
文件服务器
文件服务器
A网络
B网络

图 1

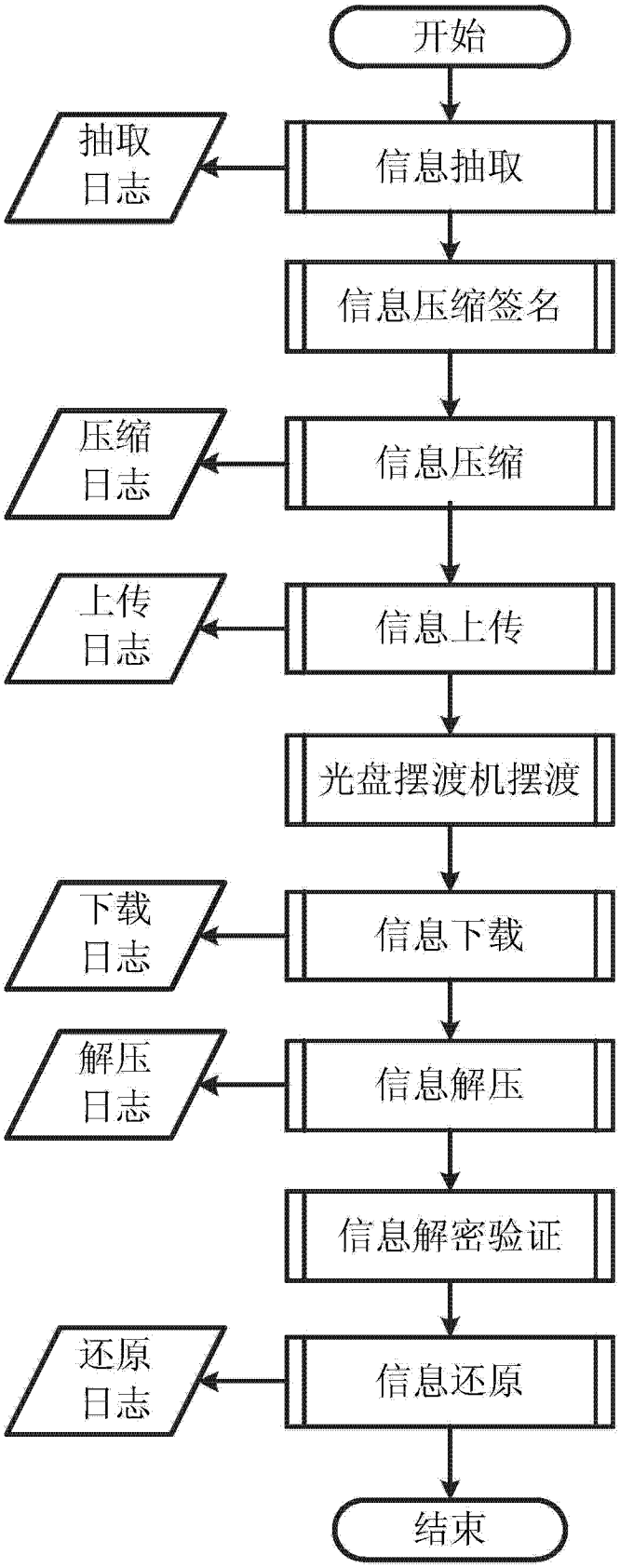

开始
信息抽取
抽取日志
信息压缩签名
信息压缩
压缩日志
信息上传
上传日志
光盘摆渡机摆渡
信息下载
下载日志
信息解压
解压日志
信息解密验证
信息还原
还原日志
结束

图 2

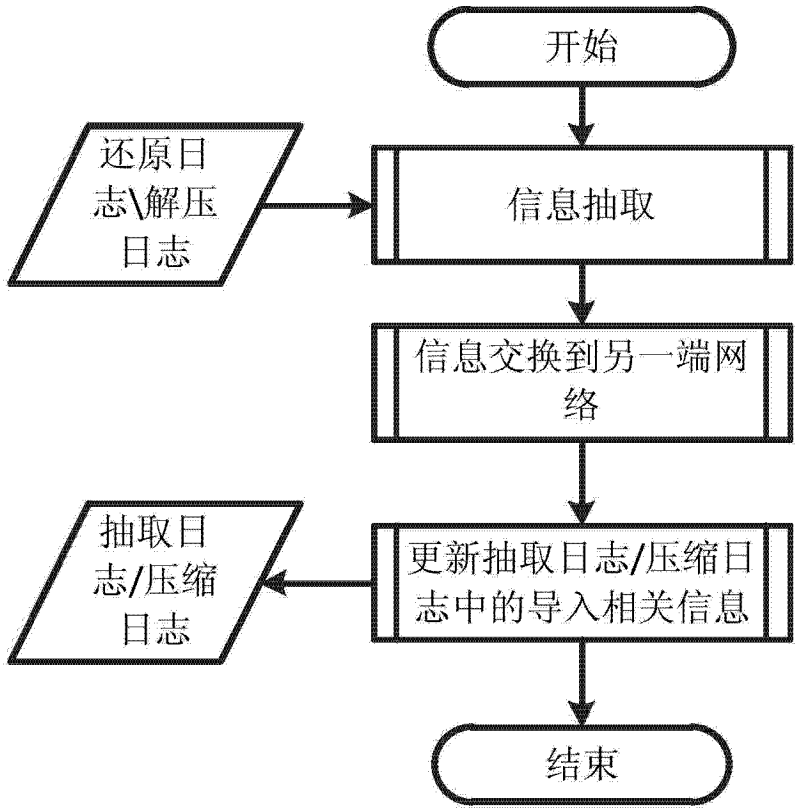

开始
还原日志\解压日志
信息抽取
信息交换到另一端网络
抽取日志/压缩日志
更新抽取日志/压缩日志中的导入相关信息
结束

图 3a

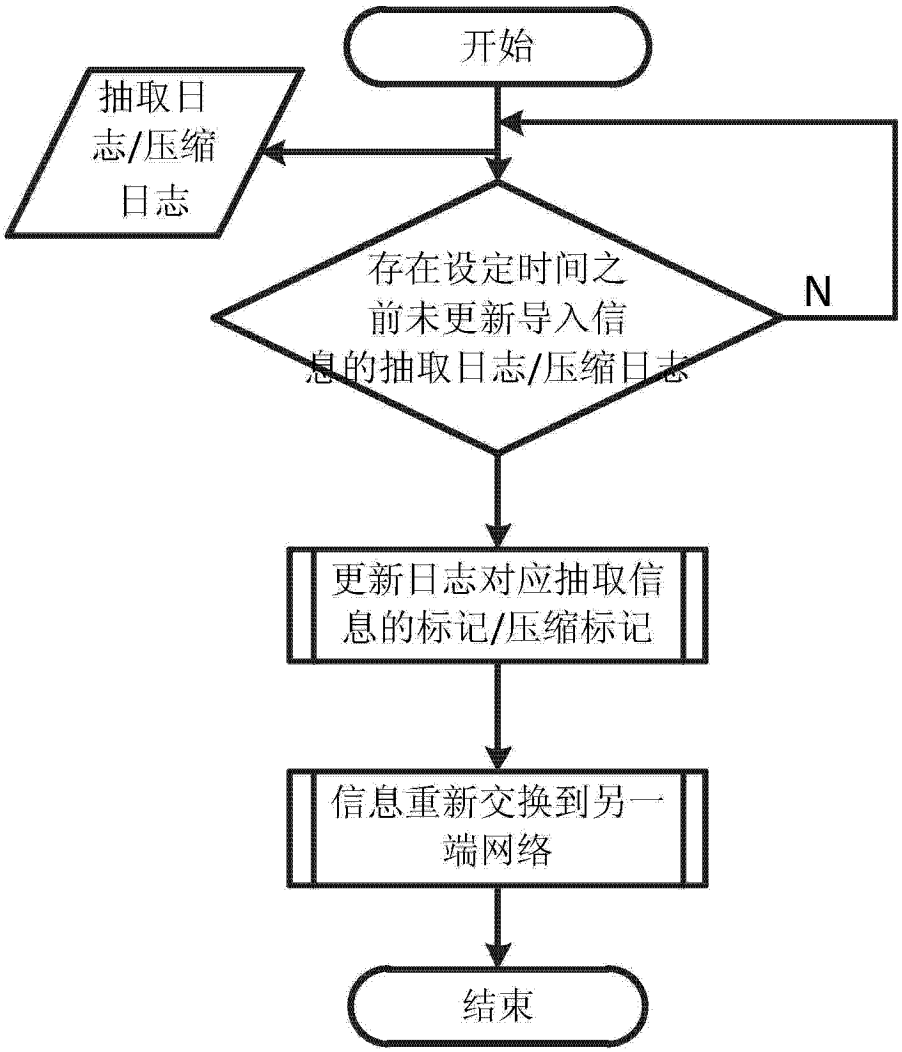

开始
抽取日志/压缩日志
存在设定时间之前未更新导入信息的抽取日志/压缩日志
N
更新日志对应抽取信息的标记/压缩标记
信息重新交换到另一端网络
结束

图 3b