文章编号:1671-4598(2021)02-0103-05 DOI:10.16526/j.cnki.11—4762/tp.2021.02.022 中图分类号:TP399 文献标识码:A

基于单向光的数据安全传输控制系统的设计与实现

樊志杰，胡正梁，熊已兴，芦 毅，刘 毅
（上海辰锐信息科技公司 研发中心，上海 200031）

摘要：对公安信息网与其他网络间的跨网络与跨信任域的安全数据交换进行了研究，提出了一种数据安全传输控制系统设计方案，底层硬件设计上基于光单向传输特点，保证数据的单向安全传输，实现网络间的物理隔离，上层系统软件通过采用完整性校验、数据加解密、数据重发、病毒扫描、内容过滤等多种技术保证系统传输数据的完整性、保密性、可靠性和内容合规性；整个系统由通道资源调度、通道资源上报、通道任务管理、队列任务管理以及主任务管理等模块组成，可实现设备信息注册、设备状态上报、通道任务管理、安全访问控制、监控与审计等功能，满足不同网络间文件数据、流数据、数据库数据、请求服务数据的安全、高效传输需求。

关键词：单向光；公安信息网；数据安全传输；完整性校验；数据加解密

Design and Implementation of Data Security Transmission Control System Based on One—way Light

Fan Zhijie, Hu Zhengliang, Xiong Yixing, Lu Yi, Liu Yi
(Research and Development Center, Shanghai Chenrui Information Technology Company, Shanghai 200031, China)

Abstract: The security data exchange model between the public security information network and other networks is studied, and propose a design scheme of data security transmission control system. The underlying hardware design is based on the characteristics of one—way light transmission, which can ensure the one—way safe transmission of data, and realize the physical isolation between networks. In order to ensure the integrity, confidentiality, reliability and content compliance of the transmission data, we adopt the integrity check, data encryption and decryption, data re—transmission, virus scanning, content filtering and other technologies in the upper system design. The whole system is composed of channel resource scheduling, channel resource reporting, channel task management, queue task management and main task management. It can realize the functions of device information registration, device status reporting, channel task management, security access control, monitoring and auditing. Meanwhile, the proposed system can meet the security and efficient transmission of file data, stream data, database data and request service data between different networks.

Keywords: one—way light; public security information network; data security transmission; integrity check; data encryption and decryption

0 引言

当前，出于信息安全防护的需求，全国公安机关的内部网络（公安信息网）必然需要和互联网等外部网络进行物理隔离，这样必然会造成内外网间数据交换的不便。在当下公安大数据和“互联网＋”战略的趋势下，以及一系列惠民便民政策的驱动下，公安机关急需要与其他部委和企事业单位之间进行数据交换，其中与互联网之间进行数据交换必不可少。另外，公安部门的便民服务大厅通常运行在互联网上，然而大多数公安核心业务系统在公安信息网内部运行，这样必然导致办理各类事项时需要公安信息网与互联网之间的数据进行安全交互[1-4]。

基于此，研究人员提出了一系列跨不同安全网域间数据传输交换的方案，其中公安部规定运用边界接入平台作为统一的标准，即通过在公安信息网与各类网络间构建出一道安全防护通道来保障不同网域间数据的安全、高效传输。相对而言，光纤因其在性能上的优势成为数据安全传输领域研究的热点。相关研究人员提出一种无需建立连接的单向传输协议，实现在不同网域间数据的传输交换，其基于单模光纤技术来设计单向传输设备[5-6]。目前涉及此方面的研究较多，但是大多实现技术仍存在传输不完整、传输无过滤、传输性能不高的问题，同时针对公安网边界的接入安全和公安业务应用数据交换共享需求，研发跨网络与跨信任域的数据安全传输系统十分必要。实现数据在不同网域、应用系统和数据源之间自动、快速、安全地交换，满足用户在各类平台、数据源及应用系统间的数据共享和聚合需求。

收稿日期:2020-12-06； **修回日期**:2021-01-05。
基金项目:国家重点研发计划(2018YFC0807105)。
作者简介:樊志杰(1982-)，男，山西朔州人，博士，研究员，主要从事信息与网络安全方向的研究。
引用格式:樊志杰，胡正梁，熊已兴，等.基于单向光的数据安全传输控制系统的设计与实现[J].计算机测量与控制，2021，29(2)：103-107，115.

鉴于此，本文提出一种基于单向光的数据安全传输控制系统，其作为公安网“统一边界平台”的公网安全接入链路，为两个不同安全域之间文件数据、数据库数据、请求服务数据的安全、高效传输和交换发挥着重要作用，并且能够实现对交换数据的全流程监控和审计。

1 系统结构及原理

本文提出的数据安全传输控制系统主要采用了单向传输技术和完整性检验技术，下面将对其进行概述。

1.1 单向传输技术

要做到真正意义上实现单向传输，不仅需要在软件方面做到逻辑上的数据单向传输，更重要的是在硬件上实现物理上数据单向传输。本系统依据光单向传输的特性，以及光纤的传输速度、稳定性等方面的综合考虑，设计了单向物理传输信道。该信道使用单向光纤网卡、单模光纤、分光器组成了数据传输的基础硬件结构[7-8]。

1）单向光纤网卡：光纤网卡多用于光纤以太网通信中，为快速以太网网络上的网络设备提供可靠的光纤连接，提高网络设备之间的数据传输速度。单向光纤网卡在硬件设计上实现收发不同向的两个光口，其中一个光口作为发送端只能发送光源，而另一个光口作为接收端则只能接受光源。本系统利用单向光纤网卡的特性，将一块光纤网卡的发送端与非信任网络进行连接，只负责发送数据；将另外一块光纤网卡的接收端和信任网络进行连接，只负责接收数据。

2）单模光纤：本系统设计的单向物理传输信道要求对数据进行高速传输，同时满足吞吐率高、误码率低的特征，因此该信道选用单模光纤。单模光纤的带宽一般可以达到千兆以上，比渐变型多模光纤的带宽高，而且单模光纤传输时信号损失较小。

3）分光器：分光器是一种在光纤通信系统中用来实现将光信号进行分支、耦合、分配的光纤汇接元器件。分光器的输入端和输出端在物理上是固定的，将光源正确地从输入端进入，输出端才能正确地将数据输出，而如果错误地将光源输入到输出端，则其他端口将无法获得正确数据。在本系统单向物理传输信道中引入单向光纤网卡、单模光纤和分光器，利用光传输特性，可实现物理通信信道的单向无反馈数据传输。

1.2 完整性检验技术

为了减少在数据传输中出错的概率，本文研究的数据安全传输系统采用了多种技术进行纠正及检测[9-12]，主要包括：

1）数据完整性校验：系统使用 zip 格式打包文件进行传输，当系统接收到 zip 文件后，对 zip 文件进行解压测试，凡是解压不成功的文件不会被传输。使用 zip 格式的原因是 zip 文件得到广泛支持，而且使用 zip 文件可以压缩文件的大小，节约网络的带宽，提高传输的效率。

2）数据加解密：系统能够对进行传输的文件数据进行加密、解密。

3）数据重发机制：在应用层我们将传输的每一个文件进行签名和验签，系统处于运行状态中时会对扫描到的文件不断进行传输，直至传输成功。

2 系统硬件设计

本文提出的数据安全传输控制系统由导入前置机、单向传输设备、导入服务器构成，导入前置机与导入服务器中存在硬件主板、操作系统平台及应用代理模块等。导入前置机与导入服务器之间通过光闸口与单向传输设备相连，组成数据单向导入通道。下面分别简述 3 个模块的原理：

1）导入前置机需要采集前端应用的数据，并对前端设备进行合规性检验，同时需要对前端采集的数据进行安全检查和格式过滤，最后将采集到的数据通过单向光技术传入到导入服务器中。另外，本系统设计时需要确保传输过程的全程审计。

2）单向传输设备利用光的不可逆性实现不同网络之间单向通讯，保证两个不同网络间的数据安全。同时，单向传输设备只负责导入前置机和导入服务器之间数据的安全传输。

3）导入服务器向公安信息网提供服务。公安信息网中的用户与导入服务器之间经过双向认证后，即可进行数据的请求和导入。

3 系统软件设计

本文提出的数据安全传输控制系统，软件层面主要包括通道任务管理、单向数据安全传输和通道资源上报 3 个模块。其中，通道任务管理模块用于创建数据交换任务；单向数据安全传输模块用于不同网域间数据的安全交换；通道资源上报模块用于对本系统运行状态进行监管。

3.1 通道任务管理

通道任务管理作为一个独立的模块，对外提供服务。供外、内服务区的资源调度模块调用，实现通道任务的创建、修改、删除、启停。其流程如图 1 所示。

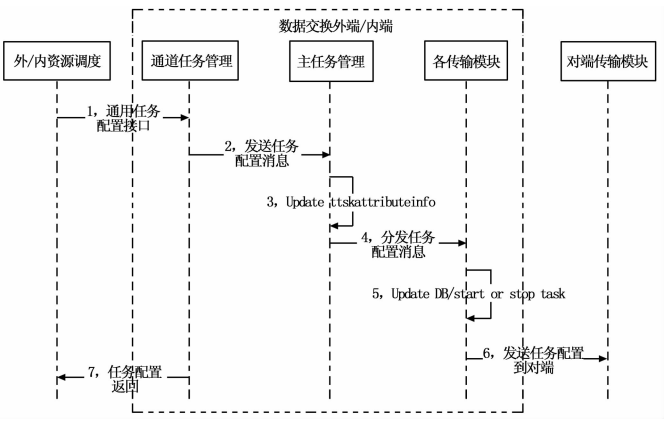

图 1 通道任务管理流程图

具体流程说明如下：

1）外、内资源调度模块调用通道任务管理模块对外提供的任务配置接口。

2）通道任务管理模块收到任务数据信息后，封装任务

配置消息报文发送到主任务管理模块。

3）主任务管理模块根据业务类型分发任务配置消息报文到各传输模块。

4）各传输模块根据任务配置报文类型更新数据库，执行相应动作。同时发送任务配置到对端。

5）通道任务管理模块返回资源调度模块调用信息。

3.2　单向数据安全传输

本系统单向数据安全传输模块间通讯结构如图 2 所示。

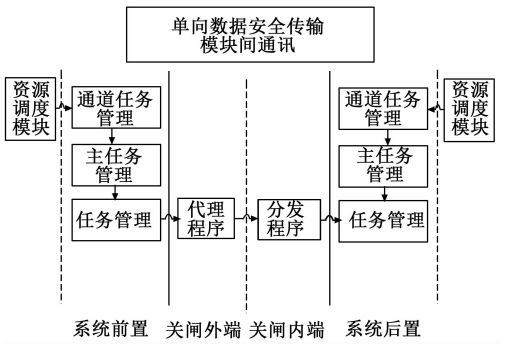

图 2　单向数据安全传输模块间通讯结构图

单向数据安全传输模块中任务管理具体实现任务的创建、修改、删除、启停。任务管理模块可以管理的任务类型有文件传输任务、数据库传输任务、MQ 消息传输任务等。任务管理模块从源服务器的指定位置读取数据后，直接通过单向光闸设备的代理、分发模块发往对端，对端任务管理模块再将数据转发至目标端服务器的指定位置，支持的数据类型有文件数据、数据库数据、MQ 消息数据。其流程如图 3 所示。

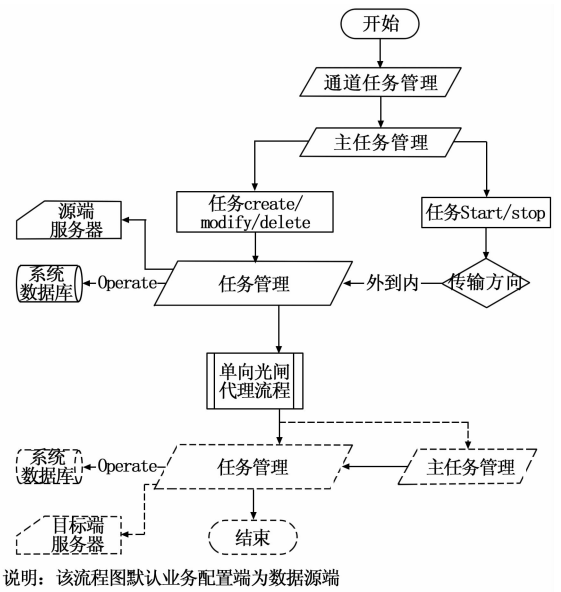

图 3　任务管理流程图

任务管理具体流程说明如下：

1）主任务管理模块根据任务配置报文类型，判断将其转发给任务管理模块中的文件传输任务、数据库传输任务、MQ 消息传输任务。

2）如果是任务 create/modify/delete，则转发给该端任务管理模块更新数据库即可。

3）如果是 start/stop，则先启动/停止数据源端的任务。

4）任务启动后，源端任务管理模块连接源端服务器获取等待传输的数据，传输至对端后，目标端任务管理模块将数据发送至目标端服务器。

本系统单向数据安全传输模块具备对传输数据的完整性校验、格式检查、病毒扫描、内容过滤等安全控制功能。

3.3　通道资源上报

3.3.1　设备信息注册

设备信息采用被动点击的方式进行注册。注册流程如下：

具体流程说明如下：

1）“系统”WEB 管理界面配置交换链路的唯一标识 devUID。

2）“系统”WEB 管理界面配置资源调度平台的 IP。

3）点击设备信息注册按钮。

4）后台通道资源上报模块收到设备信息注册消息，采集设备注册信息。

5）调用外、内服务区的资源调度模块对外提供的设备注册接口。

6）返回消息。

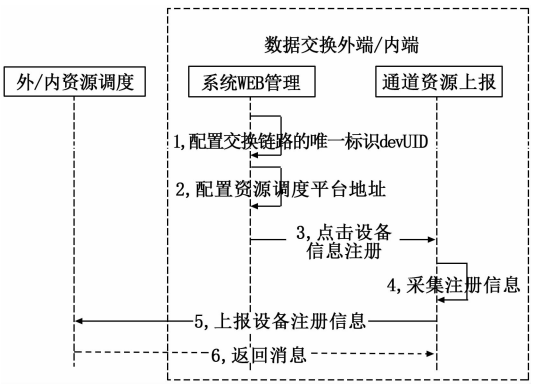

图 4　设备信息注册流程图

3.3.2　设备状态上报

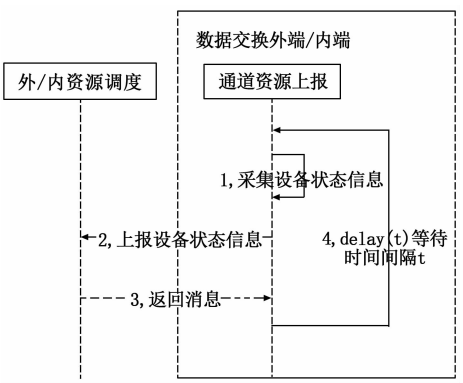

图 5　设备状态上报流程图

如图 5 所示，设备状态信息采用主动定时循环的方式

进行上报：

具体流程说明如下：

1）通道资源上报模块采集设备状态信息。

2）调用外、内服务区的资源调度模块对外提供的设备状态上报接口。

3）返回消息。

4）时间间隔 t 后再次上报。

4 系统主要功能

本系统的主要功能模块包括：文件数据单向传输、数据库单向传输、MQ 消息单向传输、安全控制、系统监控与审计等功能。

4.1 文件数据单向传输功能

Ftp 是文件传输协议，用于 internet 上控制文件双向传输；nfs 即网络文件系统，是 FreeBSD 支持的文件系统中的一种，它允许网络中计算机通过 TCP/IP 网络共享资源。

4.2 数据库单向传输功能

4.2.1 同构数据库同步

1）支持同构 Oracle 8i、9i、10G、11G、12C 数据库全量、增量数据同步。

2）支持同构 SQLServer2000、2005、2008 数据库全量、增量数据同步。

3）支持同构 MySQL5.6 及以下版本数据库全量、增量数据同步。

4）支持同步的字段类型主要以整型、字符串类型、日期类型、大字段类型等常用字段类型数据同步。

4.2.2 异构数据库同步

本系统同样支持 oracle、sqlserer、mysql 等异构数据库间的同步。

4.3 MQ 消息单向传输功能

MQ 消息队列中间件是分布式系统中的重要组件，在业务应用系统中解决应用解耦、异步消息时得到广泛的使用。本系统支持不同网域之间的 MQ 服务器上队列的中的数据同步功能。

4.4 安全控制功能

为了保障传输数据的安全性，本系统建立了安全防护体系，具体的安全控制功能包括[13-15]：

4.4.1 身份认证

数据安全传输控制系统的身份认证功能主要是指在管理员访问内置管理器时的身份认证。

4.4.2 设备认证

导入前置机负责对前端传输数据的设备进行身份认证，并通过相应的安全控制策略收集并传输前端的数据。导入服务器对各目标应用服务器进行设备认证，通过安全的协议，将文件传输到各目标应用服务器。

4.4.3 三权分立

支持安全管理员、系统管理员、系统审计员三级权限。

4.4.4 访问控制

本数据安全传输系统实现了从网络接口层到应用层的访问控制功能。

4.4.5 数据打包与校验

为了校验文件在传输过程中是否出错，系统使用 zip 格式打包文件进行传输。当系统接收到 zip 文件后，也会实现完整性检验，即对 zip 文件进行解压测试，凡是解压不成功的文件不会被传输。

4.4.6 MD5 文件完整性校验

支持对传输通过的文件做 MD5 文件完整性校验。

4.4.7 检查备份

支持 JPG 和 XML 格式检查，不满足检查条件的进行文件备份。

4.4.8 内容过滤

本数据安全传输系统的数据是无协议格式的上层应用数据，实现了对文本格式文件及数据库格式数据的内容审查。

4.4.9 流量控制

控制数据传输流量，保证数据平稳高效传输。

4.4.10 病毒扫描

对于包含有病毒数据的应用数据，单向安全传输系统阻止文件传输的同时对其进行日志记录，供安全管理员使用。

4.4.11 数据加解密

系统能够对进行传输的文件数据进行加密、解密，保证数据安全。

4.4.12 上报监管

本数据安全传输系统定时生成系统运行状态信息，日志更新日志文件，并支持日志上报监管系统功能。

4.5 系统监控与审计功能

为了检测数据传输的运行状态，本系统设计了系统监控与审计功能，主要包括：

4.5.1 系统监控

导入前置机、导入服务器系统提供对系统运行状态的实时监控功能。

4.5.2 流量监控

导入前置机上的流量监控进程间隔一定时间采集数据流量，并进行统计。

4.5.3 日志审计

本数据安全传输控制系统提供了强大的日志查询、日志存储和日志审计功能。

5 系统应用实施方案

本数据安全传输控制系统导入前置机、导入服务器与单向传输设备配套使用，对即将导入公安信息网的应用数据进行行业务处理，实现数据在不同密级网络之间的单向无反馈安全传输，支持文件、MQ 消息、数据库同步，根据不同的应用要求，配置不同类型的数据传输任务。下面以典型的文件传输应用场景为例，描述本系统应用实施方案。

5.1 文件同步应用模式 A

当外网没有专门的文件服务器时，可以在导入前置机

上建立 FTP 文件服务器，用户将文件上传到导入前置机的文件服务器，导入服务器通过单向传输设备接收到导入前置机传输来的文件后，将其上传到导入服务器网络的特定文件服务器上。

文件同步应用模式 A 的部署场景如图 6 所示。

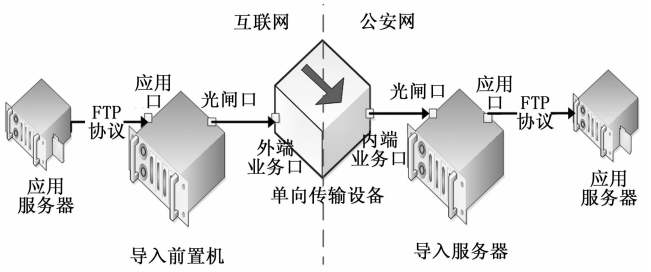

图 6　文件同步应用模式 A 部署图

通过配置导入前置机启用导入前置机的 FTP Server 服务。用户在外网中部署 FTP 客户端自动监控文件将其上传至导入前置机，在内网中部署 FTP 服务器来接收导入服务器主动上传来的文件。

5.2　文件同步应用模式 B

当内外网中均没有专门的文件服务器时，在导入前置机、导入服务器中分别建立 FTP 文件服务器，用户在将文件上传至导入前置机后，通过单向传输设备将其单向同步到导入服务器中，导入服务器接收到文件后向内网中的应用程序服务器发送文件到达通知，内网中的应用程序服务器接收到文件到达通知后主动连接单导入服务器并下载文件，完成文件的单向同步。

文件同步应用模式 B 部署场景如图 7 所示。

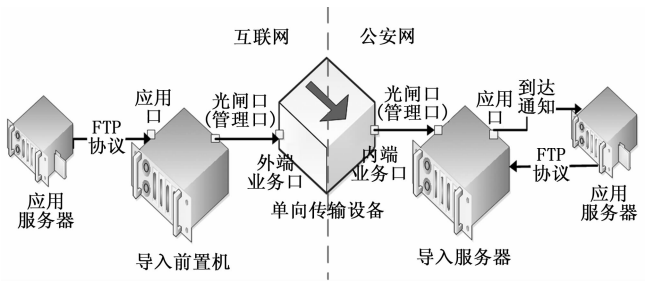

图 7　文件同步应用模式 B 部署图

通过配置单向安全传输系统分别启用导入前置机和导入服务器的 FTP Server 服务。用户在外网中部署 FTP 客户端自动监控文件将其上传至导入前置机，在内网中部署应用系统来接收文件到达通知并下载文件。

如果用户在外网没有专门的文件服务器，就可以文件同步应用模式 A 的方式进行文件传输。文件同步应用模式 A 也称外端推方式，是使用者将需要传输的文件从源端上传到导入前置机，然后由导入前置机上的处理程序，将文件封装并传输到导入服务器，由导入服务器处理程序接收并合并文件后，通过文件传输协议上传到目的端网络的特定文件服务器上。

如果外网有专门的文件服务器，就可以采用文件同步应用模式 B 进行文件传输。文件同步应用模式 B 也称外端拉方式，是指在导入前置机上的处理程序定期去源端文件服务器上获取需要传输的文件，然后再通过单向安全传输系统传输到导入服务器，导入服务器接收到数据报文合并成文件后，再上传。

综上所述，本系统上述两种文件同步模式都支持，用户根据具体应用场景来决定采用哪种文件同步运行模式。

6　结束语

本数据安全传输控制系统硬件上设计了基于单向光纤网卡、单模光纤、分光器为基础结构的单向物理传输信道；软件上设计了对传输数据的完整性校验、格式检查、病毒扫描、内容过滤等安全控制功能的单向数据安全传输模块，实现了数据在不同网域间的无反馈传输。无论是 UDP 协议，还是 TCP 协议的攻击要穿过本系统均是不现实的。

在当前公安大数据和“互联网＋”战略趋势以及一系列惠民便民政策的驱动下，公安机关与其他部委和企事业单位之间的数据交换需求日益增长，数据安全传输控制系统通过软硬件相结合，采用一系列安全技术，在公安信息网与各类网络间构建了一道安全防护通道，保障不同网域间数据的安全、高效传输，为各类公安业务的安全、高效开展提供了技术保障。光单向传输的特点一方面保证了数据的单向安全传输，另一方面也造成收端无法有效地向发端反馈各种确认和控制信息，如何有效地实现丢包重传、拥塞控制等功能都是需要继续完善和解决的技术问题。

参考文献：

[1] 田洪亮，张　勇，李　超，等. 云环境下数据库机密性保护技术研究综述 [J]. 计算机学报，2017，40 (10)：2245－2270.

[2] 沈昌祥，张大伟，刘吉强，等. 可信 3.0 战略：可信计算的革命性演变 [J]. 中国工程科学，2016，18 (6)：53－57.

[3] 张明德，郑雪峰，吕述望，等. 身份认证可信度研究 [J]. 计算机科学，2011，21 (11)：43－47.

[4] 石乐义，朱红强，刘祎豪，等. 基于相关信息熵和 CNN－BiLSTM 的工业控制系统入侵检测 [J]. 计算机研究与发展，2019，56 (11)：2330－2338.

[5] 赵伯听，李　飞，牟鹏至. 一种安全单向信息传输设备研究及设计 [J]. 计算机应用与软件，2010，23 (6)：98－99.

[6] 张雪亚. 计算存储数据安全访问控制机制研究 [J]. 计算机测量与控制，2018，26 (5)：242－244.

[7] 方　路，胡　勇. 基于 UDP 协议的文件单向传输系统 [J]. 网络安全技术与应用，2014 (12)：56－57.

[8] 王精丰. 基于单向光闸的传输控制系统的设计与实现 [D]. 北京：北方工业大学，2016.

[9] Ding Y L，Zhai Y Q. Intrusion detection system for NSL－KDD dataset using convolutional neural networks [A]. Proceedings of the 2018 2nd International Conference on Computer Science and Artificial Intelligence [C]. ACM，2018：81－85.

（下转第 115 页）