Computer Science and Application 计算机科学与应用, 2017, 7(11), 1125-1134
Published Online November 2017 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2017.711127

Hans汉斯

A Command Information Flow Reappearance System Based on Agents

Mengwei Li[1], Zhenghong Dong[2*], Zupeng Xiang[1], Lihao Liu[1]

[1]Department of Graduate Management, Space Engineering University, Beijing
[2]Department of Information Equipment, Space Engineering University, Beijing
Email: womengweiyi@163.com, *dzh.bj@163.com

Received: Nov. 10th, 2017; accepted: Nov. 23rd, 2017; published: Nov. 29th, 2017

Abstract

The reappearance of command information flow is to show the operational instructions generated by the military information system in a graphical way, so that users can observe the actual situation of information flow from different dimensions. This paper designs a kind of information flow reappearance system by using the multi-agents system and the Web graphical interface to display the information of the underlying business data of the military information system. The system obtains the militarycommand information system business message by using the port mirroring method and the jpcap function library, obtains the system network node information by analyzing the system deployment file and using the ping tool monitoring network, and uses the Web technology to display the results of the information collection and analysis, reappearance the information flow. Experiments in the actual environment show that the system provides an effective method for users to understand the flow of information in the typical business of military information system in a timely and accurate way.

Keywords

Command Information, Information Flow, Reappearance, Multi-Agents

一种基于代理的指挥信息流复现系统

李梦伟[1]，董正宏[2*]，向祖鹏[1]，刘立昊[1]

[1]航天工程大学研究生管理大队，北京
[2]航天工程大学信息装备系，北京
Email: womengweiyi@163.com, *dzh.bj@163.com

收稿日期：2017年11月10日；录用日期：2017年11月23日；发布日期：2017年11月29日

*通讯作者。

文章引用：李梦伟，董正宏，向祖鹏，刘立昊. 一种基于代理的指挥信息流复现系统[J]. 计算机科学与应用，2017, 7(11): 1125-1134. DOI: 10.12677/csa.2017.711127

摘　要

指挥信息流的复现即是把军事信息系统工作过程中产生的指挥业务信息以图形化的方式展现出来，方便用户从不同的维度去观察信息流的实际情况。以军事信息系统底层业务数据报文为数据源，结合多代理系统和Web图形化界面展现，设计了一种信息流复现系统。该系统采用端口镜像方式利用jpcap函数库获取军事信息系统业务报文，通过解析系统部署文件和使用Ping工具监测网络相结合的方法获取系统网络节点信息，利用Web技术对信息采集分析结果进行展示，并对信息流进行复现。在实际环境下的试验表明，该系统为用户及时、准确地了解军事信息系统典型业务的信息流提供了一种行之有效的方法。

关键词

指挥信息，信息流，复现，多代理

1. 引言

军事信息系统的信息流指的是军事信息系统在实际工作过程中产生的业务信息流。目前对于军事信息系统信息流还没有一个较好的采集、分析以及复现的工具，研究军事信息系统的指挥信息流，对于信息化战场上的演练分析具有重要意义。

军事信息系统是分布式系统，各节点通过计算机网络进行通信。由于分布式系统的物理和逻辑资源的分散性以及系统异构网络的复杂性，采集各个分布式单元的底层报文信息并对其信息进行整合分析就比较困难[1]。代理技术作为下一代分布式计算技术，具有强大的灵活性和代理功能，能够有效地解决分布式信息系统底层信息分析所面临的问题。近年来，随着军事信息系统的建设和代理技术的发展，国内外学者开展了大量的研究和实践。文献[2]通过代理 Agent 对指挥信息系统各作战单元进行仿真，但此 Agent 缺少对作战单元业务数据的采集和分析；文献[3]提出了大数据技术在指挥信息系统中的应用，但没有对平台数据采集技术和数据可视化技术进行具体研究；文献[4]对分布式系统的数据采集和检测提出了 Manager/Agent 模型的代理结构，融入了数据采集模块独立化的思想，但系统没有实现采集数据的共享机制，采集与检测的框架不够完善；

针对以上研究存在的问题，本系统以 JADE 作为代理开发平台，通过设计代理，将信息流业务记录的采集、分析以及复现任务分解到多个代理，通过各个代理分解复现的数据处理和运算工作，减少了服务器过量的处理负担。结合 Web 技术，把军事信息系统工作过程中产生的业务记录以图形化界面的方式展现出来，方便用户从不同的维度去观察信息流的实际情况。

2. 系统设计

2.1. 系统体系架构

本系统以 Eclipse 平台作为开发环境，利用 Java 语言编写军事信息系统信息流的复现系统。系统以数据包分析为基础，通过端口镜像的方式与军事信息系统相连，利用数据包捕获函数库(jpcap)函数库捕

获数据包，完成对军事信息系统业务信息的采集。通过解析军事信息系统部署信息的 XML 文件，获取各节点的层级、军用车类型和 IP 地址这些信息，并辅以 ping 工具完成对系统拓扑结构监控。在此基础上，对采集的数据进行分析并通过 Web 图形化形式完成对信息流的复现。

系统分为数据采集层、数据分析层、数据应用层三个层次。系统体系架构图如图 1 所示。各层次所实现的主要功能：

数据采集层：负责采集军事信息系统底层业务报文数据包并分析报文信息，并将其信息发送到数据分析层；

数据分析层：负责将获取采集层传递来的信息，将采集层中军事信息系统各部分的报文信息进行去重和匹配处理。分析军事信息系统的拓扑结构，并对系统拓扑结构的网络节点状态进行周期性监控保证拓扑信息的正确性；

数据应用层：负责与用户直接交互，维护军事信息系统业务交互信息以及指挥系统网络拓扑结构的数据库，作为信息流复现系统的服务器，接收用户在客户端的浏览器上的操作，将服务器处理结果以 Web 图形界面的方式呈现给用户。

2.2. 系统功能模块

系统包括用户管理、数据采集与处理、业务记录操作、信息流复现四个模块，如图 2 所示，具体如下。

用户管理模块：包括增加用户和删除用户功能。为了保证信息流复现系统的安全性，系统设置了三种用户类型：超极管理员、管理员、普通用户。每种不同类型的用户具有不同的系统使用权限。超极管理员具有添加、删除管理员以及普通用户的权限，具有查询、删除业务记录的权限，管理员具有查询、删除业务记录的权限，普通用户只具有查询业务记录权限。

数据采集与分析模块：在用户登录系统后，选择数据采集即启动所有的数据采集代理，选择数据分析则启动数据分析代理完成对采集数据的分析，并将分析后的结果发送到服务端代理存储到业务记录数据表中。

业务记录操作模块：业务记录操作模块包括业务记录查询和业务记录删除两个功能。在完成对业务信息的数据采集和分析后，业务记录查询能够查看数据采集模块采集到业务记录，业务记录按时间先后

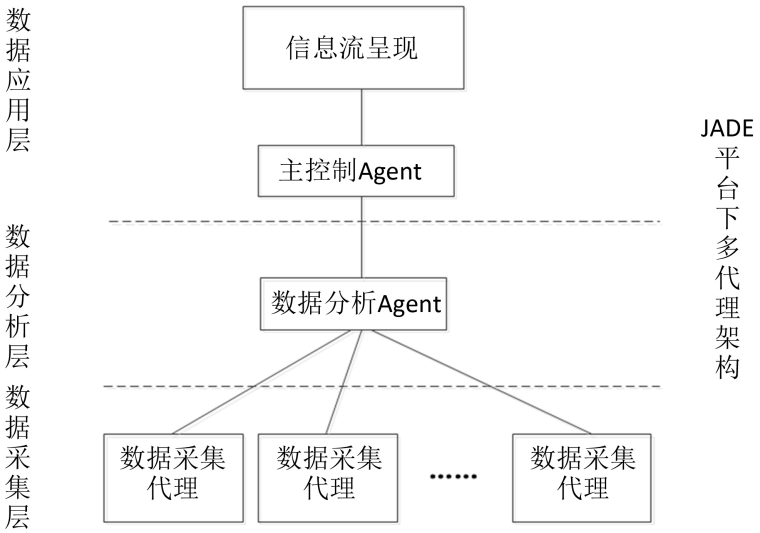

Figure 1. System architecture
图 1. 系统体系架构

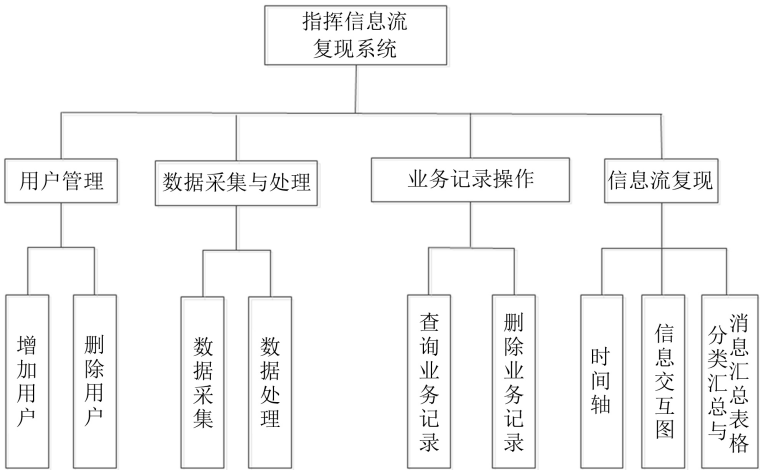

Figure 2. Function modules of system
图 2. 系统功能模块

进行排序。并能够按照搜索条件对业务记录进行搜索，搜索条件包括收方、发方、业务类型、时间段，方便用户对特定业务收方、发方、业务类型以及时间段的业务进行关注。业务记录删除能够按照特定业务收方、发方、业务类型以及时间段对业务记录进行删除。业务记录操作模块的操作的数据来自于业务记录数据表。

信息流复现模块：用户完成对业务记录的操作后，选择信息流复现，把信息流表中的信息流进行复现。Web 界面展示图的主要形式包括三个组件：① 时间轴组件、② 信息交互图组件、③ 业务信息表格组件。

3. 多代理系统

3.1. JADE 平台实现多代理系统

多代理系统是指多个独立自主的代理组成的系统，每个代理都是一个智能的实体，它们交互协作共同解决一个复杂的问题。通过对现有代理平台的对比分析，本系统采用 JADE 来开发多代理系统，实现分布式军事信息系统信息流的复现[5] [6]。

在 JADE 平台中，每一个代理相当于一个实施特定任务的主体，其任务的内容是代理中的 Behaviour。每一个代理通过 addBehaviour()方法将 behaviour 加入代理中执行，JADE 平台有三种主要的 Behaviour，分别是 OneshotBehaviours，Cyclic Behaviours 和 GenericBehaviours。在本系统中，对数据包的捕获分析、利用 Ping 工具对网络状态的探测都使用了 CyclicBehaviours，能够保证不断地执行任务。CyclicBehaviours 的 action()方法会不断的执行，直到代理执行 Behaviour 结束，它的 done()方法返回假，表示任务未完成[7]。

各代理之间采用基于同步的 socket 通信，把有用的信息封装在 XML 文档中，数据信息的传输通过 XML 文件的传输来实现。

3.2. 系统中代理的开发

根据信息流实时复现的过程和特点，系统将任务分解为多个子任务，每个子任务由一个代理或多个代理互相协作来完成。这些代理包括数据采集代理、数据分析代理、服务端代理。系统各层次中代理的功能图如图 3 所示。

从整个系统来说，系统中各个代理相互关联，互相合作完成信息流的智能复现，它们各自的功能定义如下：

1) 数据采集代理

在军事信息系统工作过程中，上下级节点之间会产生不同类型的交互数据。通过采集军事信息系统底层数据包，分析数据包报文信息即可得到的业务记录信息。考虑到在军事信息系统上部署数据包捕获程序可能会影响军事信息系统工作性能，为了不影响信息系统正常工作，数据采集代理采用交换机端口镜像的方式将流经网卡的数据包复制到镜像端口，在镜像端口利用数据包采集工具(jpcap 函数库)对数据包进行采集，并根据军事信息系统各业务报文的协议格式对采集到的数据包进行协议解析，将解析得到的报文信息映射到相应的 XML 文档，报文信息包括收方 IP 地址、发方 IP 地址、业务类型、时间这些信息，此 XML 文件通过套接字 socket 发送到数据分析层的数据分析代理。

2) 数据分析代理

数据分析代理接收多个数据采集代理发送的包含报文信息的 XML 文件，将 XML 文件解析后的业务记录信息存储到本地数据库。一条正常的业务指令会在两个数据采集代理中都有记录。因此，数据分析代理通过对比数据库中业务记录的源地址、目的地址、数据类型以及时间，完成对所有业务记录信息的去重和匹配。

在军事信息系统进行部署时会产生一个 ResourceList.xml 文件，它包括了系统拓扑结构信息。数据分析代理解析此 XML 文件，获得军事信息系统网络节点的层级、军用车类型、IP 地址这些信息，并将其写入到本地数据库中。利用解析 XML 文件可以获取到规划的军事信息系统拓扑结构信息，但在实际使用过程中，受外部因素以及系统自身的稳定性影响，军事信息系统局部节点可能会出现网络中断。实时的信息流复现时需要网络拓扑进行实时监测，判断网络节点是否出现故障，更新指挥网络节点状态。数据分析代理利用 ping 工具开启多个线程，探测数据库中各 IP 地址所代表的网络节点是否能够正常通信，通过周期性监控判断网络监控代理所解析到的系统拓扑结构信息是否发生变化，如果某 IP 地址不能正常通信，则将该 IP 地址所代表的网络节点在数据库中的属性改为异常。

在完成对数据库中业务记录和网络节点状态的分析后，数据分析代理将数据库中的信息映射到 XML 文件，通过套接字 socket 发送到数据应用层的服务端代理。

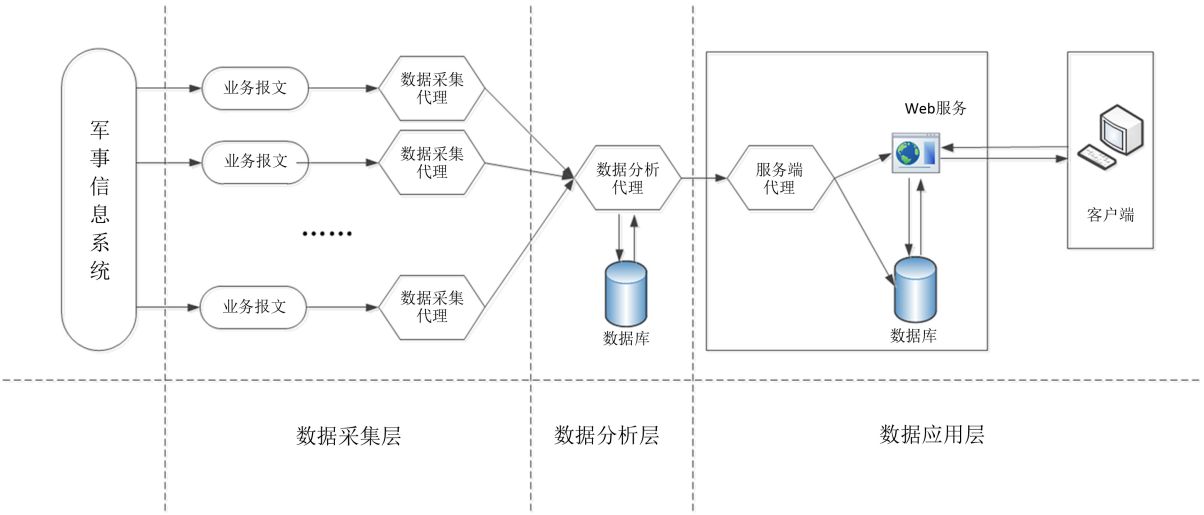

Figure 3. The functions of agents at all levels of the system
图 3. 系统各层次中代理的功能

3) 服务端代理

接收来自数据分析代理的 XML 文档，把文档解析后获取的信息写入相应地数据库中。启动 Web 服务与客户端进行交互，将数据采集、分析的结果以及复现的信息流以 Web 形式展现给用户，并提供与用户交互的接口。

4. 信息采集与分析

4.1. 指挥业务信息采集

本系统采用Java语言来设计，利用数据包捕获函数库(Jpcap)来完成对镜像端口数据包的捕获和分析[8]。

在利用 Jpcap 捕获数据包时，通过 getDeviceList()获取网络接口列表，通过 openDevice()选择用于捕获数据包的网络接口，利用回调函数 processPacket()捕获数据包，调用 Jpcap.handlePacket()函数来分析捕获的数据包，这时可以根据通信协议和业务协议获取数据包中的信息，如源地址、目的地址、指令类型、时间等信息。

4.2. 网络节点信息采集

要对信息流进行复现，首先要能够获取到指挥系统的网络拓扑结构，其次才能在网络拓扑上表示出信息流的走向。ResourceList.xml 文件中包含了指挥系统各节点的信息，通过解析此 XML 文件，可以得到指挥系统拓扑结构。

本系统采用 XML 文件解析的 API (DOM4J)来解析 XML 文件。DOM4J 是一个开源的 Java 解析 XML 文件的 API，同时还具有性能优异、功能强大和易用的特点。利用 DOM4J 解析 XM 时，在 OneShotBehaviour 的 action()中调用 XML 解析函数(DOM4J)，通过 SAXReader 下的 read()方法读入 XML 文件，获得 Element 元素，通过 getRootElement()得到 XML 文件的 Root 节点，在读取节点后，采用 Iterator 枚举遍历节点，即可获得各节点的属性。

4.3. 系统网络节点监测

利用 ping 工具开启多个线程，探测系统拓扑结构信息的各 IP 地址所代表的网络节点是否能够正常通信，通过周期性监控判断网络监控代理所解析到的系统拓扑结构信息是否发生变化[9]。网络监测流程图如图 4 所示。

监测程序创建 10 个探测线程和统计线程，在探测线程中周期性向所有数据库中网络节点的 IP 地址方向发送 ICMP 探测包，对其链路状态进行监测；在统计线程中通过分析 ICMP 响应包判断网络节点是否能够正常通信。通常情况下，响应时间大于 1 s 的网络是不可用网络，属于严重堵塞或中断状态。当收到响应的时延大于 1 s 的时候，记录该 ICMP 响应包的发送 IP 地址，将该 IP 地址所代表的网络节点在数据库中的属性改为异常。在完成对数据库中业务记录和网络节点状态的分析后，数据分析代理将数据库中的数据写入到 XML 文件，通过套接字 socket 发送到数据应用层的服务器代理。

5. 数据库设计

数据应用层的数据库结构图如图 5 所示。军事信息系统信息流的复现系统采 MySQL 数据库，通过 java 数据库连接 API (JDBC)来完成对数据库的操作。

数据库包括用户数据表、业务记录数据表、网络节点数据表以及信息流数据表。用户数据表中存放着系统的用户信息，用户实体的属性包括用户名、密码以及用户权限，在初始条件下，用户数据表中只有一个默认用户名和密码均为 admin 的超级管理员用户。业务记录数据表中存放着业务记录信息，业务

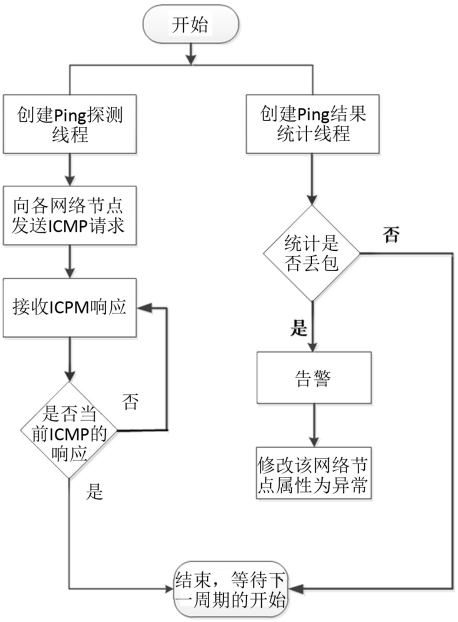

Figure 4. Monitoring the network nodes
图 4. 网络节点监测

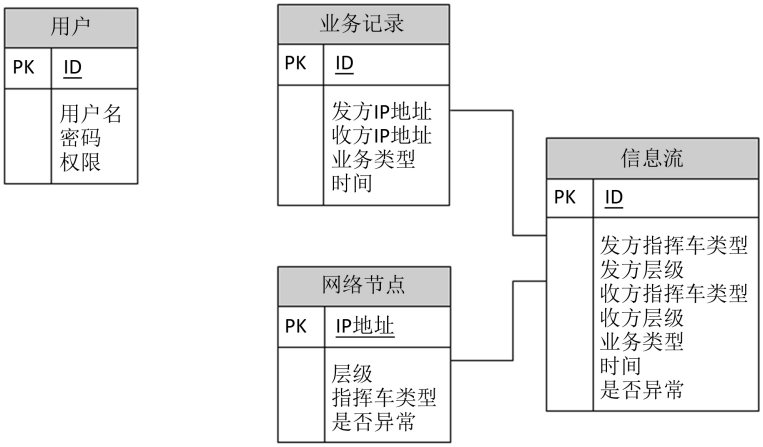

Figure 5. Database design
图 5. 数据库设计

记录实体的属性包括发方 IP 地址、收方 IP 地址、业务类型、时间。

网络节点数据表中存放着军事信息系统网络节点信息，网络节点实体的属性包括层级、军用车类型、IP 地址、是否异常。服务端代理接收数据分析代理利用套接字 socket 发送的业务记录 XML 文件以及网络节点 XML 文件，通过 DOM4j 对两个 XML 进行解析，分别将业务记录和网络节点信息存入本地的业务记录数据表和网络节点数据表。在用户完成对业务记录的操作，进行信息流复现时，根据 IP 地址对业务记录数据表和网络节点数据表的进行关联，通过数据库语句

INSERT INTO Info_flow (`senderIP`, `send_vichelType`, `receiverIP`, `receive_vichelType`, `type`, `time`, `isNormal`)

SELECT c.senderIP,a.vichelType,c.receiverIP,b.vichelType,c.type,c.time,a.isNormal|b.isNormal

FROM node AS a,node AS b,record1 AS c

WHERE a.ipAddress = c.senderIP AND b.ipAddress = c.receiverIP;

将关联结果写入信息流数据表，信息流数据表中包含信息流信息，信息流实体的属性包括发方军用车类型、发方层级、收方军用车类型、收方层级、业务类型、时间、是否异常。根据这些信息即可对军事信息系统的指挥信息流进行复现。

6. 信息流复现的图形化展示

信息流复现的目标是以图形化界面方式展示对军事信息系统底层业务报文数据的采集分析结果，并根据获取到的网络拓扑结构信息，在网络拓扑图中对业务信息流的走向进行模拟复现[10]。

Web 界面展示图的主要形式包括三个组件：① 时间轴，在时间轴上表示某时刻范围内业务报文信息[11]；② 信息交互图，表示军事信息系统之间信息交互的业务信息流走向；③ 分类汇总和消息汇总表格，表示设置的时间范围内业务报文信息的分类统计信息和每一条报文信息的具体收发方、时间、业务类型。图形界面如图 6 所示。

信息流复现的图形化展示界面的设计采用 MVC 设计模式，以主代理生成的数据库表为信息源，通过 JavaScript 实现图形的绘制，绘制图形用到的基础技术有 SVG、Echarts、D3.js 等。

时间轴组件通过 Echarts 中的堆叠柱状图构建，它的底层依赖与轻量级的 Canvas 类库 ZRender，能够提供形象、可交互的数据可视化图表，在此图中的一个柱体中通过颜色的不同可以表示该时间范围内所包含的业务报文类型以及这些业务类型的数量多少。

信息交互图组件通过 D3.js 和 SVG 构建。SVG 支持对矢量图形的缩放和平移而不失真。通过 D3 绘制出不同的军事信息系统的军用车，构建出各层级军用车之间拓扑关系展现图，根据数据库中的业务记录实现对信息流的复现。

业务信息表格组件表示的是设置时间范围内的业务报文的统计和将具体信息，其内容是不断刷新的，为保证数据刷新时界面的连续性，利用 Ajax 实现网页的异步更新。后台根据前端请求的字段从数据库中查询信息，返回 json 格式的信息，在对 json 格式信息解析后，在前端进行渲染，实现表格消息的刷新。

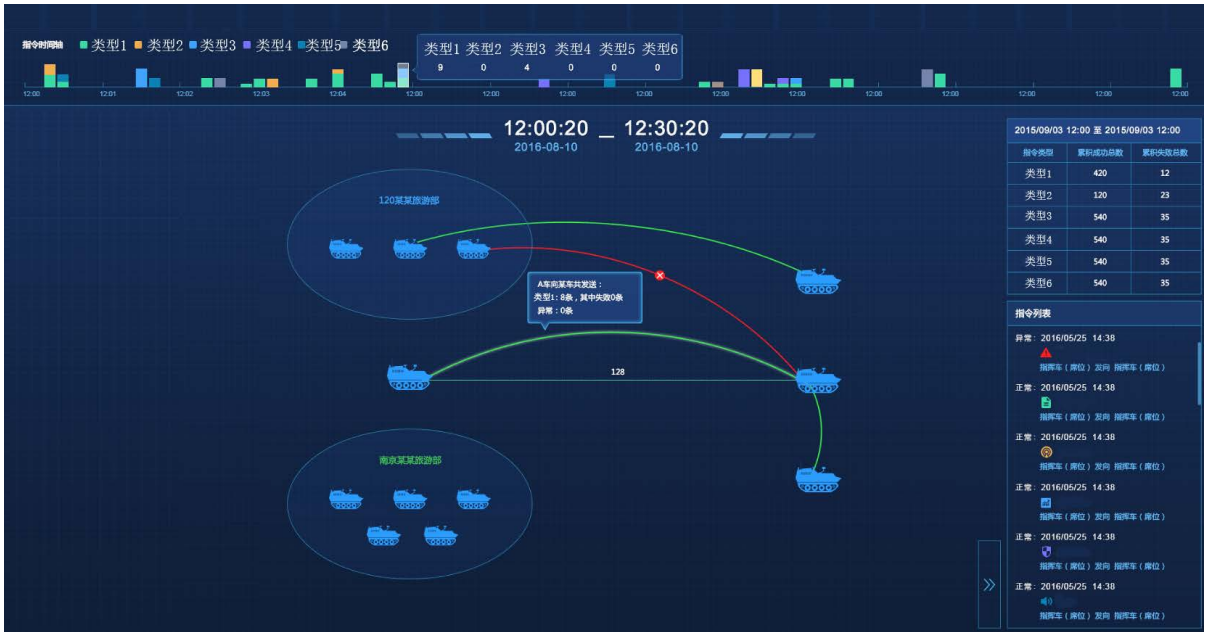

Figure 6. Graphic display interface
图 6. 图形展示界面

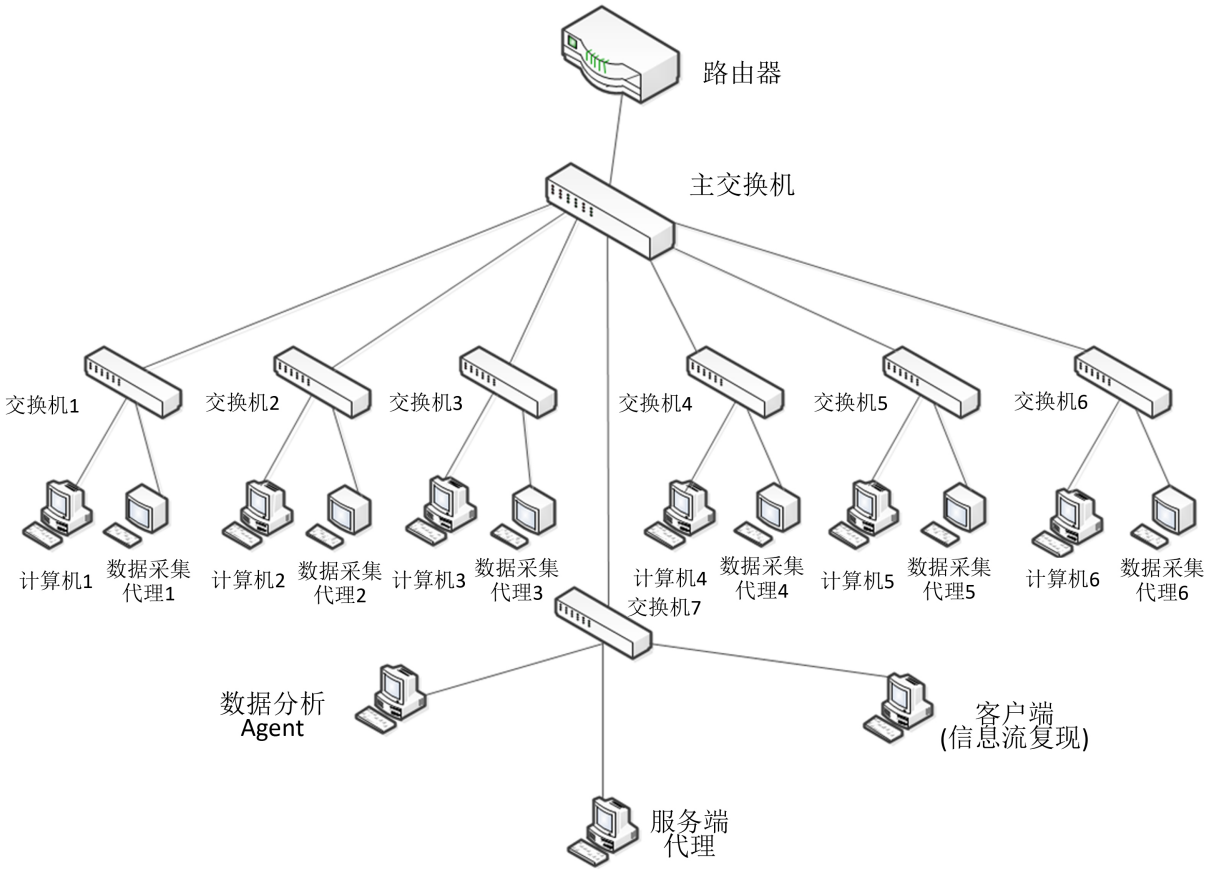

Figure 7. System deployment diagram
图 7. 系统部署图

7. 系统应用情况

在实验室搭建了指挥系统环境以及 JADE 代理运行环境，并对系统进行了部署应用。系统部署图如图 7 所示，使用一台 H3C s5000 系列的路由器和七台华为 s5700s 系列的二层交换机搭建了一个小型的局域网，此局域网通过单臂路由的方式连接，除主交换机外，其余各交换机以及与其相连接的主机代表一个网段，军事信息系统的主机与各自的数据采集代理处于局域网的同一网段之中，不同的数据采集代理处于不同的网段，但它们能够互相通信。数据包捕获代理通过交换机与军事信息系统主机相连，它所在主机的网口连接在做了端口镜像设置的交换机的监控端口上，能够获取到军事信息系统主机之间通信的底层数据包。

通过该系统的应用，能够帮助用户从收发方、业务类型、时间段等角度分析军事信息系统发送的典型业务信息，为用户分析军事信息系统指挥流程，研究新的打法战法提供了有效的数据支持。

8. 结束语

在人们对信息化时代耳熟能详的今天，人工智能时代已经初现端倪。军事信息系统产生的底层业务报文数据，价值巨大，对于其信息的获取、分析和利用会成为军事信息系统下一步发展的方向。本文以数据采集分析为基础，基于 JADE 平台的多代理系统，设计实现了信息流复现系统。同时，对下一步要开展的工作也做了思考：1) 根据信息流的分析结果，开展对军事信息系统网络故障的诊断，后续可以结合军事信息系统故障库一起研究；2) 利用对指挥业务流程复现的数据，结合神经网络技术进行自学习，为指挥员使用军事信息系统提供辅助决策。

参考文献 (References)

[1] 付华峥, 陈翀, 向勇, 等. 分布式大数据采集关键技术研究与实现[J]. 广东通信技术, 2015, 35(10): 7-10.

[2] 杨萍, 翟世梅, 刘虎. 基于信息系统的体系作战仿真系统[J]. 兵工自动化, 2015(2): 59-62.

[3] 王宏, 康建平, 李春林, 等. 大数据技术在指挥信息系统中应用[J]. 指挥信息系统与技术, 2015, 6(2): 10-16.

[4] 王金伟. 分布式数据采集与监测系统的设计、实现及应用[D]: [硕士学位论文]. 北京: 中国科学院研究生院(计算技术研究所), 2006.

[5] 赵东见, 杨奕飞, 翟江涛. 基于 JADE 的多 Agent 协同仿真系统设计[J]. 江苏科技大学学报(自然科学版), 2017, 31(3): 316-320.

[6] 刘骥. 基于 Agent 技术的互联网在线拍卖系统设计与实现[D]: [硕士学位论文]. 大连: 大连理工大学, 2016.

[7] 于卫红. 基于 JADE 平台的多 Agent 系统开发技术[M]. 北京: 国防工业出版社, 2011.

[8] JpcapTutorial. https://zh.scribd.com/document/45327270/JPcapTutorial

[9] Khan, R., Khan, S.U., Zaheer, R., *et al*. (2013) An Efficient Network Monitoring and Management System. *International Journal of Information Engineering and Electronic Business*, **3**, 122-126.

[10] 陈文艺, 宋亚红, 李晓伦. 基于物联网开放平台的设备数据显示方案[J]. 西安邮电大学学报, 2016, 21(6): 108-113.

[11] Echarts. http://echarts.baidu.com/examples.html