DOI: 10.7667/PSPC151254

基于 OPNET 的电网 SCADA 系统通信建模与仿真

胡春潮[1]，侯艾君[1]，马 凯[1]，蔡泽祥[2]，黄成巧[2]，席 禹[2]，潘天亮[2]

(1. 广东电网有限责任公司电力科学研究院，广东 广州 510080；2. 华南理工大学电力学院，广东 广州 510640)

摘要：为有效分析电网 SCADA 系统通信网络性能，提出基于 OPNET Modeler 建立电网 SCADA 系统通信网络关键对象模型和多场景仿真的方法。根据 SCADA 系统通信实际情况，在充分分析 SCADA 系统建模需求的基础上，深入研究 SCADA 系统通信建模方法，构建符合 SCADA 系统工程实际的网络性能仿真平台，实现了 SCADA 系统网络性能的多场景仿真。所提出的基于 OPNET 的电网 SCADA 系统通信建模与仿真方法，为 SCADA 系统通信网络性能分析提供直接而有效的工具，也为 SCADA 系统事故预演、设备选型、网络规划等提供了有力的分析与参考依据。

关键词：SCADA 系统；通信网络；建模；仿真；OPNET

Communication modeling and simulation of SCADA system of power grid based on OPNET

HU Chunchao[1], HOU Aijun[1], MA Kai[1], CAI Zexiang[2], HUANG Chengqiao[2], XI Yu[2], PAN Tianliang[2]

(1. Electric Power Research Institute of Guangdong Power Grid Co., Ltd., Guangzhou 510080, China;
2. School of Electric Power Engineering, South China University of Technology, Guangzhou 510640, China)

Abstract: In order to analyze the performance of SCADA system communication of power grid in an effective way, this paper proposes a method of building key models and multi-scenario simulation of SCADA system communication based on OPNET Modeler. According to the actual conditions of SCADA system communication, this paper researches the modeling method of the SCADA system based on sufficient analysis on the modeling demand of SCADA system. It also establishes a network performance simulation platform that adjusts to the engineering practices of SCADA system, realizing the aim of examining the network performance through the simulation of multi-device and multi-scenario. It is a direct and effective tool that the communication modeling and simulation method of SCADA system of power grid based on OPNET to analyze on SCADA system communication network. It also provides an effective tool and practical reference for fault preview, equipment selection and network planning of SCADA system communication.

Key words: SCADA system; communication network; modeling; simulation; OPNET

0 引言

电网数据采集与监视控制系统(SCADA)是能量管理系统 EMS 最重要的子系统，担负着电气设备远程监视和控制的重任，其承载业务的可靠性是调度中心对厂站端进行远程控制的关键[1]。目前，SCADA 系统业务信息通过电力调度数据网传输，通信网络作为 SCADA 信息传输的载体，其性能的优劣直接影响系统调度控制功能的实时可靠实施[2]，因此，研究 SCADA 系统通信网络、开发精准可靠的网络性能分析方法显得十分必要。

然而，当前在 SCADA 系统设计和运行过程中，通信网络性能分析多依赖于工程估算或者现场实测，分析投入成本高、准入门槛高而准确性差[3-4]。因此，本文提出基于 OPENT 仿真的 SCADA 系统网络性能分析方法[5-6]，通过结合使用 OPNET 标准模型整定与自定义建模两种方法，建立 SCADA 系统通信网络关键对象与场景模型，进一步构建 SCADA 系统仿真平台，实现基于 SCADA 系统实际的多场景网络性能仿真分析。仿真结果在准确性和实用性上都具备明显优势，本文设计的系统建模与仿真方法为 SCADA 系统规划设计、故障预言等提供了新的思路。

1 建模需求分析

SCADA 系统通信仿真主要用于电力系统稳态

或故障状态时信息传输的流量大小、延时等网络性能分析，其在业务类型、所用协议以及网络构建方式上与普通网络不同，本节具体从 SCADA 系统通信网络、通信业务、通信规约和仿真场景四方面对系统建模需求进行分析。

1.1 SCADA 系统通信网络建模需求

通信网络是 SCADA 系统信息传输的通道，承担信息寻址、交换与控制功能，通信网络建模内容主要包括以下几个方面：

1) 信源与信宿模型。通常意义上，厂站端远动装置与各级调度中心 SCADA 系统服务器在功能上作为信源与信宿，需要建立反映远动装置和 SCADA 服务器工作方式与处理过程的模型。

2) 信息交换模型。SCADA 系统交换机、路由器与通用交换设备存在差异，体现在其不仅需要承担业务信息的存储转发功能，还需要具备 VLAN、优先级、VPN 等网络管控策略，需要在已有模型上进一步开发。

3) 网络安全与访问控制模型。根据《电力二次系统安全防护技术规范》，SCADA 系统位于安全区Ⅰ，为保证其他安全区业务不对 SCADA 系统进行干扰，需要建立具有数据流向识别和过滤功能的防火墙模型。

4) 电力调度数据网模型。一般来说，电力调度数据网采用分层组网结构设计，是具有核心层、汇聚层、接入层三层的专用网络[7-8]。调度数据网模型需要体现网络结构以及和核心层、汇聚层及接入层的布置方法与组织形态。

1.2 SCADA 通信业务建模需求

SCADA 系统中基本业务包括：遥测、遥信、遥控和遥调四类，这四类业务是实现 SCADA 系统对电气设备监视和控制功能的基础。基于 OPNET 进行 SCADA 系统业务建模需要体现各类业务的运行特性和发送规律，各类业务的发送规律如表 1 所示。

表 1 SCADA 系统业务发送规律

Table 1 Transmission regular of services of SCADA system

SCADA 系统业务		发送规律
初始化过程(104 规约启动过程)		链路未连接时触发
总召唤	周期性遥信	每隔 10 min
	周期性遥测	周期性重复
变位遥信(随机性遥信)		随机触发
变位遥测(随机性遥测)		随机触发
遥控		随机触发
遥调		随机触发

如表 1 所示，遥信、遥测分为周期性和随机性两种，周期性遥信、遥测在总召唤时触发；随机性遥信、遥测也称为变位遥信、变位遥测，通常在电力系统的开关状态改变或测量的模拟信号出现异常时触发；遥控、遥调根据调度中心的需求而触发，属于随机性业务；SCADA 系统在链路未连接时需通过初始化过程业务建立主子站间连接，属于随机性业务；总召唤是主站召唤遥信、遥测数据时使用的业务，属于周期性业务。

1.3 SCADA 系统通信规约建模需求

IEC 60870-5-5 规约定义了 13 种 SCADA 系统通信的基本应用模式，其中 SCADA 系统实际使用的包括：(1)站初始化；(2)总召唤-子召唤；(3)循环数据传输；(4)采集事件过程；(5)命令传输过程[9-11]。IEC 60870-5-5 规定了各类应用模式中数据传输的顺序、数量等规则，如表 2 所示，列出 SCADA 系统业务与应用模式之间的映射关系。

表 2 SCADA 系统业务与基本应用模式映射表

Table 2 Mapping table between basic application model and services on SCADA system

SCADA 系统业务	对应的基本应用模式
初始化过程(104 规约启动过程)	①站初始化 ②总召唤
总召唤	总召唤-子召唤
遥测(周期性)	循环数据传输
遥信(周期性)	循环数据传输
变位遥测	采集事件过程
变位遥信	采集事件过程
遥控	命令传输过程
遥调	命令传输过程

如表 2 所示，详细列出了 IEC 60870-5-5 与 SCADA 系统各类业务的映射关系，在 OPNET 仿真建模过程中需建立满足规范的应用层协议，符合应用模式运行特性。

1.4 仿真场景建模需求

与通用网络服务不同的，SCADA 系统通信网络具有高可靠性、高专用性特征，为保证系统在各种工况下的可靠运行，有必要建立反映系统在不同运行工况下网络性能的多种仿真场景。仿真场景应包括电力系统稳定运行、一次系统故障和 SCADA 系统故障等三类，其中电力系统稳态工况仿真，可为研究现有 SCADA 系统正常活动时网络性能提供参考资料；电力系统故障工况仿真，可用于分析 SCADA 系统业务活动频繁时网络压力情况，而 SCADA 系统故障情况则反映系统自身抗风险能力。

2 SCADA 系统对象建模

2.1 OPNET 建模思路

OPNET 为用户自定义建模提供了便利的途径，本文使用 OPNET Modeler 自定义模型建立业务信息流，其开放式的建模机制满足 SCADA 系统建模仿真需要。OPNET Modeler 中包含面向通用网络通信仿真的标准模型，通过对标准模型参数合理地整定，能够完成实体设备、网络拓扑和仿真场景的建模，本文建模对象及建模内容如表 3 所示。

表 3 建模对象及方法

Table 3 Modeling objects and methods

类别	建模对象	建模方法
实体设备	工作站与远程终端单元	参数整定
	交换机	参数整定
	防火墙	参数整定
	路由器	参数整定
业务数据	业务信息流	自定义建模
网络拓扑	电力调度数据网	参数整定及自定义建模
仿真场景	正常情况	参数整定及自定义建模
	故障情况	参数整定及自定义建模

2.2 实体设备建模

1) 工作站与远程终端单元模型

OPNET Modeler 中提供通用的工作站与服务器模型，工作站加载封装成型的自定义 SCADA 系统业务模型来模拟 SCADA 系统业务信息的生成和发送过程；同样的，服务器模型加载配套的业务模型来模拟 SCADA 系统业务信息的接收、响应和处理过程。

2) 交换机模型

交换机模型使用 OPNET Modeler 中标准模型，除了需要体现一般交换机存储转发的功能外，还建立提供 VLAN 的网络流量控制策略。VLAN 的配置采用每个端口绑定一个 VLAN ID 的方法，同时把双方之间通信的端口加入“支持 VLAN”列表属性中。

3) 防火墙模型

本文使用防火墙模型的代理服务器功能实现网络隔离与访问控制的能力。防火墙模型通过启用或禁用代理服务器功能实现对特定信息流的放行或阻隔等网络隔离与访问控制，对特定业务的阻隔与访问控制和数据的延时是防火墙模型需要整定的参数。

4) 路由器模型

当前 SCADA 系统通常采用 IP 路由器进行组网，OPNET Modeler 中包含多类厂家的多类 IP 路由器型号，建模过程中选取合理 IP 路由器信号，并配置开放式最短路径优先(Open Shortest Path First, OSPF)路由协议，使网络能够根据链路状态选择传输路线，并在链路异常或故障而致使路由不可达时，能够以较短收敛时间重新选择合适的数据传输路径。

2.3 业务及通信规约建模

业务建模要根据 SCADA 系统基本应用模式的通信特征，通过配置数据交互字节的大小、发送规律，进而把关键业务与其对应的基本应用模式进行映射，并在业务模型中设置业务的发送规律，最终实现关键业务信息流的建模。

IEC 60870-5-5 传输规约定义的基本应用模式给出了相应的主子站交互序列图，并根据 SCADA 系统实际情况配置交互的数据大小，如双点遥控命令可以定为 16 字节。本文使用 OPNET Modeler 中自定义任务模型(Task Definition)对数据包的大小、发包周期、传输方向等数据包特性进行配置，从而把自定义任务和基本应用功能数据包特征形成对应关系。下面本文以遥控业务及其对应的基本应用模式中的命令传输过程为例说明建模方法。

如图 1 所示为命令传输交互过程图。如图 1 中，主子站之间的信息交互共包括 7 个阶段，第一阶段是由主站发起的，主站为主动方，子站为被动方，主动方在 TCP 协议中是处于客户机模式，由它发送第一次握手过程。第一阶段是主站发送的“选择命令”信息，数据包为 1 个，该数据包字节大小为 16 字节，数据源是主站，数据目的地是子站。第二阶段是子站向主站回答第一阶段信息而发送的“选择信息”，数据包为 1 个，该数据包字节大小是 16 字节，数据源为子站，数据目的地为主站。如此类推建立 7 个阶段从而完成“命令传输过程”的自定义建模。

当基本应用模式通过自定义任务模型建立后，要将其映射并修改为对应的 SCADA 系统业务。本文依据表 1 把对应的基本应用模式通过 OPNET Modeler 中的应用模型(Application Definition)映射并修改成 SCADA 系统业务。进一步，将业务分别加载至 SCADA 系统服务器和远动装置中，并在其中配置包括初次触发的时间，业务重复的次数、间隔和顺序等运行规律。本文设定所有业务在仿真初始阶段开始第一次触发，其他设定如表 4 所示。

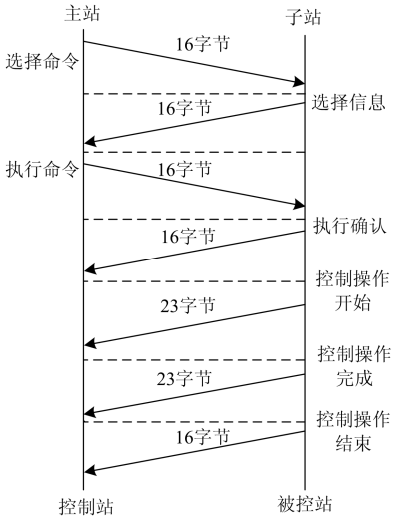


图 1　命令传输交互过程图

Fig. 1 Interactive process diagram of command transmission

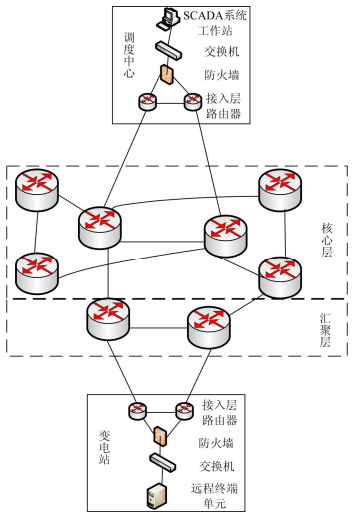


图 2　网络拓扑

Fig. 2 Network topology

表 4　SCADA 系统业务触发规律配置

Table 4 Toggle rule of services on SCADA system

SCADA 系统业务	触发规律
初始化过程	系统启动后运行 1 次
总召唤	每 10 min 周期性重复触发
变位遥信(随机性遥信) 变位遥测(随机性遥测)	服从[0, 3 600]上的均匀分布
遥控 遥调	服从[10, 3 600]的均匀分布，且每两次间隔不少于 10 s。

2.4　网络拓扑建模

网络拓扑依据电力调度数据网的三层结构设计，核心层为网状结构，汇聚层中两个路由器为一组承接于核心层与接入层之间，拓扑图如图 2 所示。

如图 2 中所示，网络拓扑图的上方子网代表“调度中心”，下方子网代表“变电站端”。调度中心和变电站内接入层路由器采用双星型连接，负责网络安全的防火墙接于路由器下游用于数据过滤，交换机接于防火墙后进行站内信息转发，工作站或远程终端可采用星型结构与交换机连接。

3　SCADA 系统网络性能仿真应用案例

3.1　正常运行场景流量仿真

本文根据图 2 所示网络拓扑结构设计 SCADA 系统流量仿真场景，以验证所建模型与预期结果是否吻合。本场景考察 SCADA 系统的业务信息流特征，模拟场景为电力系统处于稳定状态时信息流特征，依据上文所建模型，SCADA 系统的业务信息流流量大小的仿真结果如表 5 所示。

表 5　SCADA 系统业务仿真结果

Table 5 Simulation results of services of SCADA system

类型 / 传输方式	业务数据流量最大峰值/kbps	周期性业务数据流量峰值/kbps
SCADA 系统工作站到远程终端单元的流量	4.23	2.687
远程终端单元到 SCADA 系统工作站的流量	5.487	3.779

无论是从 SCADA 系统工作站到远程终端单元的流量，还是从 SCADA 系统远程终端单元到工作站的流量都在仿真的初始阶段达到最大值，符合上文设计在仿真开始阶段所有业务开始第一次触发的特征。业务数据流量最大值从远程终端单元到工作站的流量为 5.487 kbps，而由于 TCP/IP 协议的传输规定使得从工作站到远程终端单元的流量也达到 4.23 kbps。总召唤设定为每 10 min 周期性触发一次，从第 10 min 开始，每隔 10 min 系统中出现一个峰型流量，从远程终端单元到工作站的流量为 3.779 kbps，而从工作站到远程终端单元的流量也达到 2.687 kbps。变位遥测、变位遥信触发时间服从[0，3 600] s 上的均匀分布，而遥控、遥调触发时间设定为服从[10，3 600] s 上的均匀分布，结果中会出现另外的峰值小于 1 kbps 的峰型流量。从仿真结果上看，SCADA 仿真模型网络性能指标符合预期。

3.2　非法用户接入场景流量仿真

本文通过对比防火墙开启与未开启后 SCADA 系统流量变化情况，对防火墙模型的模型有效性进行验证，仿真验证所用网络拓扑如图 3 所示。图 3 所示仿真平台由 SCADA 系统工作站、数据库询问工作站、远程终端、防火墙、交换机、路由器等实

体设备模型组成，其中数据库询问计算机仿真系统外非法接入客户端，用于验证防火墙能否阻隔特定数据通过。图 4 为数据库询问工作站流量、远程终端单元出站流量仿真结果对比。

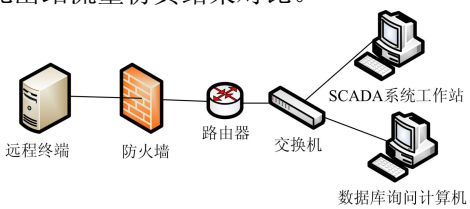
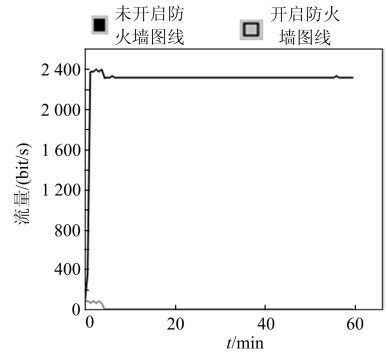
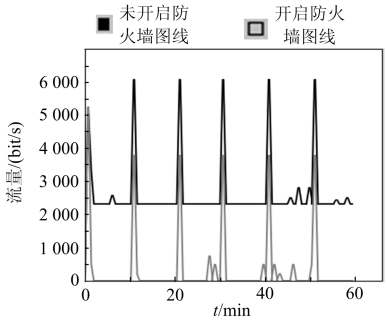


图 3 防火墙有效性验证场景的网络拓扑

Fig. 3 Topology of networks for verification scene of availability



(a) 数据库询问工作站流量对比



(b) 远程终端单元出站流量对比

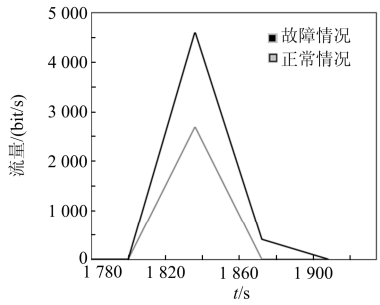
图 4 有无防火墙时的流量对比

Fig. 4 Comparison in traffic of the presence or absence of firewall

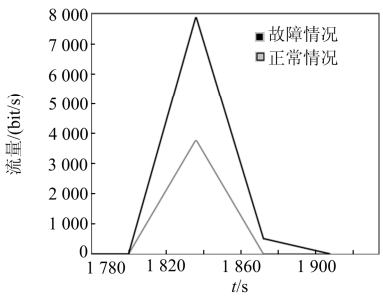
如图 4(a)所示，在未启用防火墙功能前，数据库询问计算机访问业务没有受到阻隔，询问流量达到稳定的 2.35 kbps，远程终端单元因受到非法的询问导致出站流量被抬高；防火墙开启后后，用于模拟非法的数据库访问的业务受到阻拦，非法数据库询问工作站只剩下网络初始化的流量。如图 4(b)所示，由于防火墙对非法数据的阻隔，远程终端单元出站流量比未开启防火墙前下降了 2.35 kbps，即为非法数据访问流量，防火墙模型满足建模预期。

3.3 故障运行场景仿真

应用建立的 SCADA 系统仿真模型，本文构造如图 2 所示网络仿真平台，用于仿真电力一次系统出现故障情况下，SCADA 系统通信网络动态运行特性。具体仿真电网开环馈线发生单相接地故障时，线路保护在重合闸失败而导致三相跳闸过程中 SCADA 系统网络性能变化情况。将故障设置仿真开始后 30 min，此时 SCADA 系统中变位遥信、遥测业务会在短时间内重发，设为发送共计 3 次，变位遥测点数设为 96 个(通过发送 48 个带两个信息体的 28 字节数据包传输)，变位遥信点数单相跳闸与单相合闸为 1 个，三相跳闸为 3 个，遥控、遥调业务在三相跳闸后触发一次。SCADA 系统网络性能仿真结果对比如图 5 所示。



(a) 主站出站流量对比



(b) 子站出站流量对比

图 5 主、子站出站流量对比

Fig. 5 Comparison in outbound traffic of master-salve station

从图 5 的结果对比可以得出，在电力系统故障时 SCADA 系统业务信息流链路峰值流量比正常活动的链路峰值流量有所增大，本应用案例中主站出站峰值流量为 4.595 kbps，相对正常运行情况增加了 1.908 kbps；子站出站峰值流量为 7.871 kbps，相对稳态运行情况增加了 4.092 kbps。因而在此情况下，网络传输的峰值流量不大于 10 kbps，并不会对数据的网络传输造成过大压力。为了评价网络的数据传输的实时性，下面对比两场景的 IP 数据包端到端延时，仿真结果如表 6 所示。

从结果可看出，一次系统正常运行情况与故障情况下 SCADA 系统网络延时上相差在 40 μs 以内，IP 数据包端到端延时在正常运行情况和故障运行

情况下均小于 1 s，延时在标准限定范围内。此外，从仿真结果中还可以看出，由于子站向主站方向传输的数据量相对较大，子站向主站方向比主站向子站方向的延时会相对较大，为主站出口网络设计和相关设备选型提供了借鉴依据。

表 6 IP 数据包端到端延时仿真结果

Table 6 Simulation result of IP packet end to end delay

传输方向	平均延时/ms		仿真 30 min 时刻延时(对应电力系统发生故障瞬时)/ms	
	正常情况	故障情况	正常情况	故障情况
主站到子站端到端	1.223	1.237	1.223	1.256
子站到主站端到端	1.237	1.264	1.241	1.267

4　结论

为建立有效且实用的 SCADA 系统通信网络性能分析方法，本文在深入研究 SCADA 系统建模需求基础上，利用 OPNET 仿真平台建立了 SCADA 系统网络关键对象模型。进一步通过构建 SCADA 系统不同运行场景，验证了所建模型的有效性，结果显示本文所建模型能够支撑 SCADA 系统多设备、多场景的网络性能分析需求，并能够真实仿真 SCADA 系统动态运行情况。本文建立基于 OPENT 的 SCADA 系统通信网络性能仿真模型和方法，为 SCADA 系统通信网络性能分析提供直接而有效的工具，也为 SCADA 系统事故预演、设备选型、网络规划等提供了有力的分析与参考依据。

参考文献

[1] 张永健. 电网监控与调度自动化[M]. 北京: 中国电力出版社, 2004.

[2] 曾瑛, 李伟坚, 陈媛媛, 等. 基于业务优先级的电力调度数据网拥塞规避算法[J]. 电力系统保护与控制, 2014, 42(2): 49-55.
ZENG Ying, LI Weijian, CHEN Yuanyuan, et al. A congestion avoidance algorithm based on the service priority for electric power dispatching data network[J]. Power System Protection and Control, 2014, 42(2): 49-55.

[3] 刘昊昱, 左群业, 张保善. 智能变电站过程层网络性能测试与分析[J]. 电力系统保护与控制, 2012, 40(18): 112-116.
LIU Haoyu, ZUO Qunye, ZHANG Baoshan. Process level network performance testing and analysis in smart substation[J]. Power System Protection and Control, 2012, 40(18): 112-116.

[4] 熊小萍. 电力系统广域通信网络可靠性分析及优化设计[D]. 南宁: 广西大学, 2014.
XIONG Xiaoping. Reliability analysis and optimal design of wide area communication network in power system[D]. Nanning: Guangxi University, 2014.

[5] 秦川红, 王宁, 任宏达, 等. 采用虚拟局域网的数字化变电站数据通信仿真研究[J]. 电力系统保护与控制, 2013, 41(2): 126-131.
QIN Chuanhong, WANG Ning, REN Hongda, et al. Simulation and study on data communication in digital substation based on virtual local area network[J]. Power System Protection and Control, 2013, 41(2): 126-131.

[6] 王海柱, 蔡泽祥, 邵向潮, 等. 智能变电站过程层网络关键对象建模与仿真[J]. 中国电力, 2013, 46(6): 80-84.
WANG Haizhu, CAI Zexiang, SHAO Xiangchao, et al. Key object modeling and performance simulation of process level networks in smart substation[J]. Electric Power, 2013, 46(6): 80-84.

[7] 李高望, 鞠文云, 段献忠, 等. 电力调度数据网传输特性分析[J]. 中国电机工程学报, 2012, 32(22): 141-148.
LI Gaowang, JU Wenyun, DUAN Xianzhong, et al. Transmission characteristics analysis of the electric power dispatching data network[J]. Proceedings of the CSEE, 2012, 32(22): 141-148.

[8] 罗汉武, 李昉, 张栋. 安全数据网的构建及其在河南电力调度数据网应用[J]. 电力自动化设备, 2007, 27(1): 65-67.
LUO Hanwu, LI Fang, ZHANG Dong. Construction of secure power data network and its application in Henan power data network[J]. Electric Power Automation Equipment, 2007, 27(1): 65-67.

[9] 郭晋洋. 基于 IP 宽带网的远动系统实时数据传输的研究[D]. 保定: 华北电力大学, 2004.
GUO Jinyang. The research of the telecontrol realtime data transmits on IP wideband network[D]. Baoding: North China Electric Power University, 2004.

[10] 贺平. 计算机网络——原理、技术与应用[M]. 北京: 机械工业出版社, 2013.

[11] GB/T 18657.5-2002 远动设备及系统第 5 部分: 传输规约第 5 篇: 基本应用功能[S].
GB/T 18657.5-2002 telecontrol equipment and systems-part 5: transmission protocols-section 5: basic application functions[S].

收稿日期：2015-07-20；　修回日期：2015-09-25

作者简介：

胡春潮(1984-)，男，通信作者，硕士研究生，工程师，从事继电保护、数字化变电站研究工作；E-mail：huchunchao@139.com

侯艾君(1986-)，女，硕士研究生，工程师，从事继电保护、数字化变电站研究工作；E-mail: 13503081530@139.com

马　凯(1985-)，男，硕士研究生，工程师，从事继电保护、数字化变电站研究工作。E-mail: 13600009565@139.com

（编辑　魏小丽）