火电工控系统网络安全防护方案设计*

张大松,姜洪朝,吴云峰
(中国电子信息产业集团有限公司第六研究所,北京 100083)

摘　要:针对火电工控系统的网络安全问题进行了研究,对当前火电工控系统的网络架构、安全挑战、防护现状、风险来源等网络安全问题进行了分析总结,按照电力系统的安全防护总体原则及相关标准规范,针对电力生产网络的特点及安全要求,提出了以数据探针为组成单元的能够覆盖电厂工控网络各个层级并配置监测中心的安全防护架构,能够对多种工控协议进行深度解析,对已知和未知危险流量进行识别和学习,并将宏观网络态势以可视化的方式展示出来,实现了对电厂工控系统多层次、立体化、智能化的安全防护,能够深度有效的保护电厂生产网络系统。

关键词:电厂安全;工控安全;安全防护;流量识别;协议解析
中图分类号:TP399　　**文献标识码**:A　　DOI: 10.19358/j.issn.2096-5133.2020.03.004
引用格式:张大松,姜洪朝,吴云峰. 火电工控系统网络安全防护方案设计[J]. 信息技术与网络安全,2020,39(3):17-22.

Design of network security protection scheme for thermal power industrial control system

Zhang Dasong, Jiang Hongchao, Wu Yunfeng
(The 6th Research Institute of China Electronics Corporation, Beijing 100083, China)

Abstract: The network security of thermal power industry control system is studied. The network architecture, security challenges, protection status and risk sources of thermal power industry control system are analyzed and summarized. According to the general principles and related standards of power system security protection, and in view of the characteristics and security requirements of power production network, the proposed security protection architecture is based on data probe component unit, covers all levels of the power plant industrial control network and is configured with a monitor center. It can deeply analyze various industrial control protocols, identify and learn known and unknown dangerous flows, and visualize the macro network situation. It realizes the multi-level, three-dimensional and intelligent security protection of the power plant industrial control system with deep and effective protection for power plant production network system.

Key words: power plant security; industrial control security; security protection; flow identification; protocol analysis

0　引言

电力工业是国家的重要基础工业,电力系统作为国民生产生活的关键基础设施具有举足轻重的地位。随着中国经济建设的蓬勃发展,能源供应质量成为直接关系工业生产稳定的决定因素。电力作为一种优质能源具有极大的市场需求,并且需求量随经济增长而逐年增长。

在高速经济增长的推动下,电力系统两方面的矛盾十分突出。一方面,随着中国工业的快速发展,特别是《中国制造 2025》及工业化和信息化深度融合的推进,电力安全生产的标准逐年提高,特别是安全保障方面的要求十分迫切。另一方面,随着工业化和信息化以及能源互联网的实际应用,电力系统从相互相对独立且完全与外网隔离发展为网络化连接和信息化管理,并且逐步向互联网开放。电力系统的信息化扩大了传统内部网络风险的发生范围和传递通路,而开放化则引入了全面的无时不在的互联网风险。

面对电力系统建设两个方面的矛盾,提高系统的安全防护能力是同时解决两方面矛盾的最佳选择。当前中国工业网络安全基础设施建设落后、安全系统脆弱、安全体系单薄,同时主观上安全意识

* 基金项目:北京市科技计划项目(No. Z181100005118005)

淡泊,因此加强网络信息安全建设、提高工业的安全防护能力成为当务之急。本文以电力行业工控系统网络安全为例,提出多层次立体防护体系架构,并应用于实际的电力工控网络系统中,保障电力生产安全。

1 火电工控系统

1.1 火电工控网络架构

大型火力发电厂一般都是全厂采用基于以太网的多层次大型网络架构,实际网络结构比较复杂。按照网络层次一般分为以下几层:

(1)现场控制层

控制层主要负责生产流程的过程控制,主要包括各种 DCS 分布式控制系统、工业控制器、数字量及模拟量数据采集模块、动力驱动系统、现场总线设备、以及各种显示操作仪器仪表等。控制层主要完成对系统设备的实时调节控制、顺序控制、设备检测、系统测试诊断、数据采集、状态监控、信号转换等功能。

(2)现场监控层

监控层主要负责对生产操作控制过程的状态监控、系统组态维护、现场仪器设备管理等工作。监控层一般布置负责各个分装置的工程师站及操作员站,负责生产现场的管控。在小型电厂中,只需控制层和监控层就可以满足电力生产的控制需求。对于大型电厂,由于有更高的生产过程智能化和信息化要求,一般会布置更高层级的网络层级。

(3)厂级 SIS 层

SIS 层主要作用是对生产过程的厂级综合管理和控制,向下连接全厂各种 DCS、PLC 等过程控制计算机系统,向上连接 MIS 管理信息系统,在整个网络层级中起到承上启下的作用。SIS 系统能够实现整个电厂的资源共享、信息互通,提高资源和信息的使用效率,达到管控一体化的厂级综合管控能力。

(4)MIS 层

MIS 层主要作用是对企业资源的综合管理,能够提供生产系统的宏观信息、建立统一的管理平台、整合各个系统资源、协调全厂信息资源的综合调度。MIS 层能够提供一些高级功能,通过历史数据,建立生产过程的优化模型和故障诊断模型,对生产过程进行优化指导、参数调优和智能故障诊断。

现有火电厂生产系统的典型网络结构如图 1 所示。

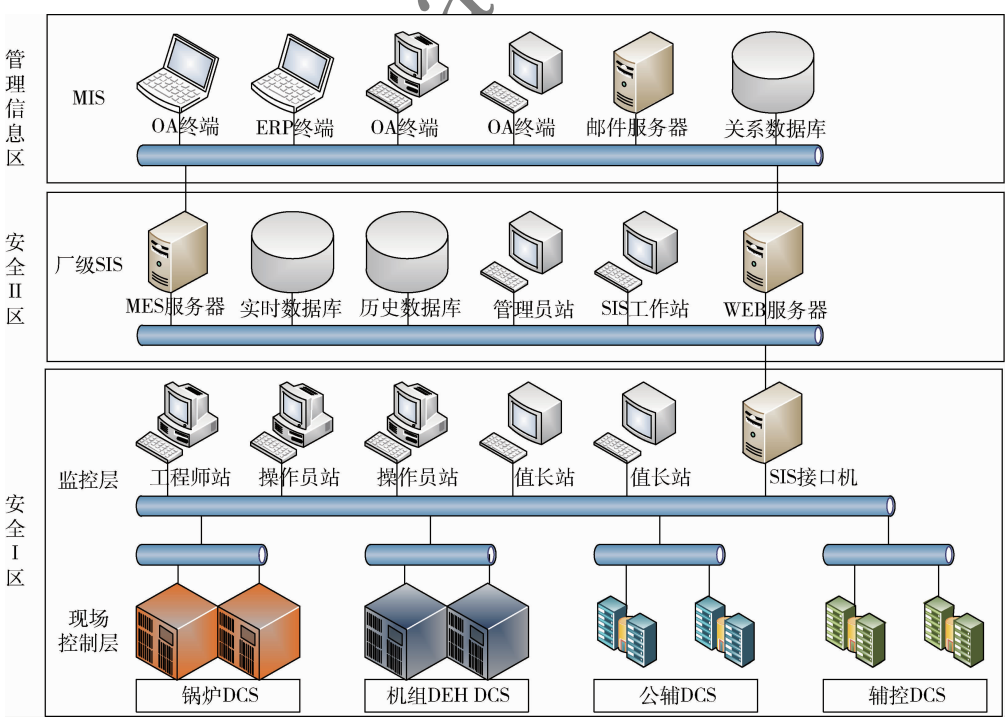

图 1 火电厂工控网络架构

1.2 火电工控网络层级安全挑战

根据火电工控网络架构,火电工控网络安全层级可以划分为控制层、网络层、应用层、数据层等四个层级,每个层级都面临不同的网络安全风险。四个层级的网络安全风险挑战分析如下:

(1)控制层安全挑战:PLC、DCS、SCADA 等工业控制系统,在控制平台、控制协议、控制软件设计之初,主要考虑实时性和可靠性,一方面因为核心元件大多是国外厂家生产,存在后门、漏洞等风险;另一方面诸如完整性校验、身份认证、授权、加密等信息安全功能都被忽略。随着信息技术(IT)和操控技术(OT)的融合,打破了传统的安全可信控制环境,网络攻击可从 IT 层渗透至 OT 层,但目前还缺乏有效应对高级持续威胁(APT)攻击检测和防护的手段。

(2)网络层安全挑战:涵盖工业网络、无线网络、商业互联网。网络融合消除了原有的工业环境内外部安全边界,将互联网、信息系统的安全风险引入工控网络,包括网络传递过程中常见的拒绝服务(DoS)、中间人攻击等,以及传输链路上的软硬件安全,无线网络防护边界模糊等安全风险。

(3)应用层安全挑战:企业信息化管理涉及的门户网站、ERP、PDM、CRM 以及云平台等,除面临传统 IT 安全挑战中的病毒、木马、漏洞等威胁外,还面临云平台服务虚拟化中的违规接入、内部入侵、多租户风险、跳板入侵等威胁。

(4)数据层安全挑战:指企业内部生产管理数据、生产操作数据以及企业外部数据,不管是大数据存储还是分布式服务器存储,都面临数据丢失、窃取、篡改等安全风险。

2 火电工控网络安全形势

2.1 火电工控网络安全现状

当前运行中的火力发电厂工控系统普遍存在以下安全隐患:

(1)核心设备和系统严重依赖进口:在火电厂的主控和辅控系统中,国外设备仍然处于主流地位,主要有艾默生、ABB、西门子、施耐德等国际品牌,国产品牌在一些机组上也有一定应用,主要以国电智深、和利时、浙江中控为主。设备层和控制层的网络风险从根本上一直存在。

(2)网络安全软件和设备功能不足:布置在各现场车间的网络监控层与厂级 SIS 层通讯多采用 OPC 协议,按照有关标准要求,需要添加工业防火墙用作逻辑隔离。然而,当前很多电厂采用的防火墙并不支持 OPC 协议的动态端口机制,也就无法配置安全策略,导致防火墙的隔离功能形同虚设。

(3)应用软件及操作系统维护不力:上层网络的操作系统长期不更新的情况大量存在,导致大量漏洞无法及时封堵,甚至长期缺乏相关维护人员。一些网络设备存在严重的系统漏洞,包括应用软件的漏洞,很容易被攻击者发现和利用,在未授权的情况下访问或破坏设备系统。

(4)工控网络各层互联加深:当前 MIS 与厂级 SIS 两层网络之间的互联程度加深,上层信息网的安全威胁渗入下层控制网络的机会大幅增加。

(5)安全管控不够全面:电厂经常发生外部电脑、存储设备接入内部网络的造成危险的事件,都是因为配套的安全技术措施和管理措施相对缺乏或者不够完善,由此导致病毒进入内部系统中而造成破坏。

(6)网络拓扑结构不清晰:在系统出现故障后,无法及时了解实际网络状况,不能对故障的来源进行追踪定位,无法对网络入侵行为、病毒、业务访问异常等问题进行细致分析处理。

2.2 火电工控网络安全风险来源

(1)工控设备通信防护脆弱

电厂工控系统中普遍采用的标准工控协议,如 Modbus TCP、ProfiNet、Ethernet IP、ControlNet、OPC 等协议,基本没有加密措施,很容易被解析。工控系统在实时运行时,系统维护、组态操作等功能缺乏认证、完整性、审计方面的管理控制,DoS、IP-Spoofing 等攻击手段很容易侵入系统内部。设备之间的网络通信没有加密认证机制,通信数据中的重要数据、工艺过程、控制参数等信息很容易被攻击者获取,甚至关键代码及数据被攻击者修改。

(2)工控系统入口管理疏忽

电厂工控系统中存在各种口令:操作系统账号、SCADA/HMI 等应用账号、PLC 读写口令、工业交换机/防火墙等网络设备配置账号、无线 AP 接入口令等,未设置口令、默认口令、弱口令、共享口令等现象大量存在,很容易成为系统的安全脆弱点,成为攻击的入口。最常见的弱口令问题相当于门户大开,攻击者很容易由此渗透至电厂内部网络,接管系统之后可操控执行任何命令,获取核心控制权之后可轻易使得整个工控系统崩溃。

(3)网络边界隔离措施不足

电厂不同的功能区域之间缺少必要的网络边界隔离措施,网络边界接入缺少严密的防护、认证过程,为非法接入或错误接入提供了可能。尤其是远程接入内部网络时,存在极大的远程控制和远程维护方面的安全风险。无线接入同样存在 IWLAN、GPRS 方面的安全风险。由于边界访问控制的缺乏,工控网络极易受到来自外部网络的攻击,且受到攻击后无法进行追踪。

(4)系统安全漏洞修复滞后

电厂工控系统中存在各种安全漏洞,操作系统、工业软件、控制器、网络设备等都会存在一些漏洞,以及不能及时修复的问题,对电厂生产系统的安全带来了极大隐患。漏洞不能及时修复的具体原因有:工控系统有严格的实时性、可用性要求,不能随意停机进行系统维护;漏洞修复之后可能导致系统兼容性问题;漏洞修复可能带来的不良影响无法预估;在修复漏洞时可能给系统带来新的病毒、蠕虫等恶意程序。

(5)安全事件监控响应欠缺

安全事件的监控、管理与响应机制不够完善和全面,无法实现对整个电厂网络的安全感知与管控。安全日志及其监控、审计措施缺乏,在发生安全问题后无法对整个电厂网络的风险来源及发生过程进行分析和追溯。安全事件的响应及时性问题也大量存在。

3 火电工控网络多层次立体防护设计

3.1 需求分析

火电厂防护设计需求分析:

(1)满足《电力监控系统安全防护总体方案》(36 号文)合规性要求。

(2)安全防护单元采用模块化设计、分布式部署,能够根据需要灵活布置在电厂网络的各个层级。

(3)具备集中式监测管控中心,能够对电厂网络整体安全态势进行展示、管理和监测。

(4)安全防护单元具备电厂网络各个层级的数据采集能力、协议深度解析能力、攻击流量识别能力。

(5)安全防护单元具备对所在网络的安全管理配置能力。

3.2 防护体系架构

根据电厂的实际工控网络架构,该电厂网络结构可以划分为:现场控制层、现场监控层、厂级 SIS 层、MIS 层等四层。由于各个层面的网络功能任务不同,各层的数据探针部署需要根据该层网络数据流量的特点进行方案设计,特别是该层网络协议特点需要先进行分析。

在现场控制层,协议类型主要是各种工业控制网络的私有协议,通常为实时控制数据流,特点是周期性传输、传输周期短、传输帧长简短。考虑到不影响该层网络协议的实时性,采用旁路部署的方式,将数据采集探针部署在各网络节点交换机的镜像口。通过镜像口将该网络节点的所有流量数据复制出来,只接收网络数据,不会向网络节点注入任何流量,因此不会对控制层网络产生任何影响,不会影响正常的生产工艺过程。

在现场监控层,协议类型主要是向下的控制命令和向上的状态反馈信息,有一定的实时性要求,控制命令数据简短、发送间隔不固定,状态反馈信息一般发送周期固定、数据量适中。为了不影响该层的现有工作过程,将数据采集探针部署在环网核心交换机的镜像口,通过镜像口将该网络节点的所有流量复制出来。

在 SIS 层,协议类型比较混杂,既有工控协议,也有 TCP/IP 协议,对协议数据的实时性要求进一步降低,传输数据量较大,尤其在历史累计数据需要传输的时候。同样,将数据采集探针部署在核心交换机的镜像口复制所有网络流量。

在 MIS 层,协议类型主要是以太网 TCP/IP 协议,数据传输量大,带宽高,实时性要求低。同样,将数据采集探针部署在核心交换机的镜像口。

除了各层部署数据采集探针之外,在电厂工控网络中心需要部署一台数据服务器作为安全监测中心,将分布式架构部署的各个层级的数据采集探针进行集中管理。同时,通过安全监测中心能够对所有安全设备进行统一管理和配置。火电厂安全态势防护体系架构如图 2 所示。

3.3 数据探针

在电厂工控网络的每个层级都会部署数据探针,数据探针负责本层级网络的安全防护。数据探针主要由服务器硬件和功能软件组成,功能软件主要包括高速镜像数据采集模块、网络协议深度分析及解析模块、攻击流量智能识别及分类模块、网络态势可视化分析及展示模块、管理配置模块等。通过各个功能模块的综合处理分析,可以实现对本层网络的网络风险识别、分析和处理。

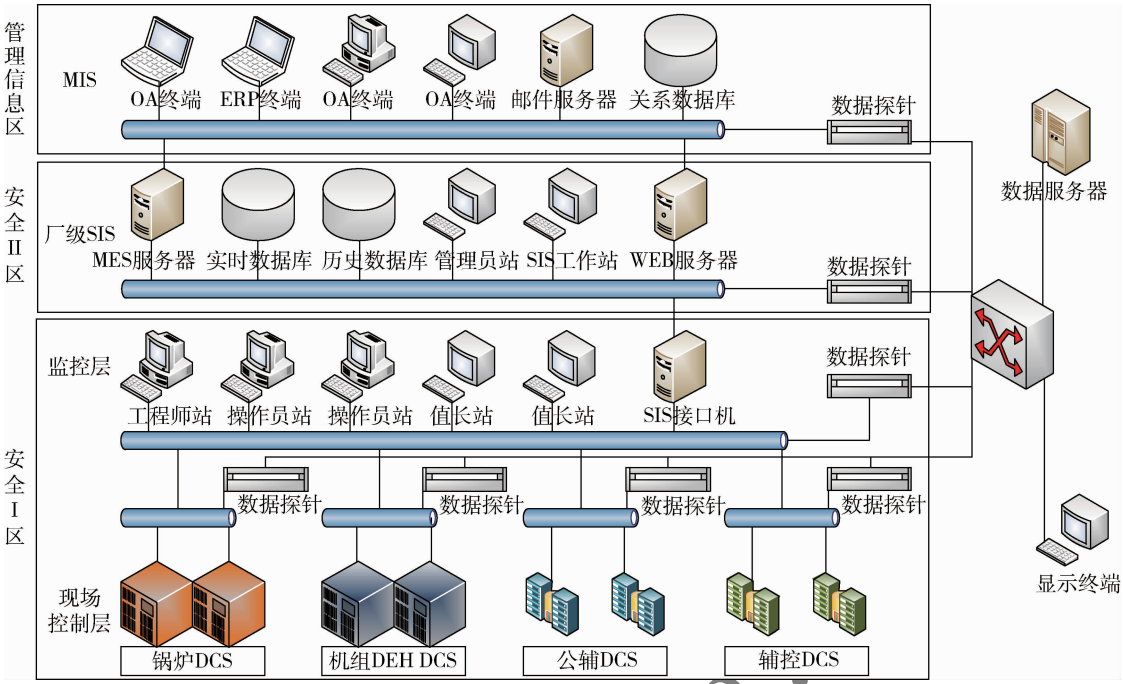

图 2　火电厂安全态势防护体系架构

3.3.1　数据采集

网络流量数据采集模块能够采集数据链路层及以上的流量数据,对于常规网络协议能够直接进行解析,主要包括 Web 相关协议(HTTP)、Mail 相关协议(SMTP、POP3、IMAP)、文件相关协议(FTP、Samba)等。对于基于以太网的工控网络协议及其他特殊协议则是借助于网络协议深度分析及解析模块进行解析,比如 POWERLINK、EtherNet/IP、OPC、S7、Modbus、Profinet、EtherCAT、SERCOS III、IEC 等主流工控协议。

3.3.2　网络协议深度分析及解析

网络协议深度分析及解析模块借助于数据包深度解析引擎,能够识别和解析当前主流工控协议,对于常用工控协议能够实现指令级检测和审计。目前,数据包深度解析引擎能够支持 10 多种主流工控协议。在保证电厂工控系统可用性与完整性的基础上,对数据包的网络标识、时间历程、有效数据特征、负荷数据类型等进行进一步检测分析,并将分析结果处理成易于人类理解的内容,便于人工辅助判断。

对于常规协议也能够进行深度分析,对于 HTTP、SMTP、POP3、RPC、TELNET、FTP、TFTP、SNMP、SNTP 等传统网络通信协议进行深度解析后,能够深度还原网络通信设备之间的通信内容。

对于深度解析后的重要网络通信事件能够进行记录,并全流量保存原始数据,便于用户对安全事件进行各种有针对性的安全回溯查询。

3.3.3　攻击流量智能识别及分类

攻击流量智能识别及分类模块基于网络协议深度解析的结果,进行危险流量的检测判定及危险类型和等级分类。该模块采用单分类支持向量机建立针对探针所在层级网络特点的攻击识别及分类机器学习模型,实现主机、通信、会话、指令、内容、工艺等各种环境的攻击流量检测,建立多层次、多维度的安全网络环境,为网络中的通信事件提供安全风险分析依据。

通过智能化的机器学习模型,能够有效识别、告警已知危险流量,对于未知危险流量,能够通过学习建立未知危险流量的特征,同时进行识别。通过智能化机器学习建立的危险流量特征比较稳定和显著,能够极大地降低误报率,同时提高了系统运行的有效性、稳定性。基于多个层级的流量特征监测和分析有利于掌控整个电厂生产控制网络的安全态势,及时调整和部署有效的安全策略,以达到消除网络系统中安全隐患的目的,实现网络全系统的持续安全运营和智能化的网络安全管理。

3.3.4　网络态势可视化分析及展示

可视化分析及展示模块能够对当前网络态势

的监测结果进行宏观分析和展示,根据内置的数据模型能够对系列安全事件进行智能化分析,包括事件聚类分析、样本聚类分析、时间序列历程分析、时间序列相关分析等。展示内容包括攻击来源、攻击目标、攻击类型、攻击时间等详细的事件记录信息。

3.3.5 管理配置模块

管理配置模块能够对数据探针的工业协议库、协议解析参数、攻击信息库、行为模型库、用户权限和行为范围等进行管理和配置。该模块能够自动监控所在网络的接入设备,根据设备的通信特征识别各种类型的控制器、服务器,自动生成网络拓扑。

4 结论

本文通过对电力行业的工控网络架构、安全风险、防护现状等网络安全问题进行研究分析,按照电力系统的安全防护总体原则及相关标准规范,针对电力生产分区的特点及网络要求,提出了以数据探针为组成单元的能够覆盖电厂工控网络各个层级并配置监测中心服务器的安全防护架构,能够解析多种工控协议,对已知和未知危险流量进行识别和学习,并将宏观网络态势以可视化的方式展示出来。安全防护架构具有多层次、立体化、智能化的显著特点,能够深度有效的保护电厂生产网络系统。

参考文献

[1] 陈连栋. 电力行业网络安全态势感知研究[D]. 北京:华北电力大学,2015.

[2] 魏钦志. 工业控制系统安全现状及安全策略分析[J]. 信息安全与技术,2013(2):25-28.

[3] 吴莹辉. 网络安全态势感知框架中态势评估与态势预测模型研究[D]. 北京:华北电力大学,2015.

[4] 朱明露. 功能安全标准在电厂安全系统中的应用研究[J]. 中国仪器仪表,2015(9):29-31.

[5] 谭小彬,张勇,钟力. 基于多层次多角度分析的网络安全态势感知[C]. 全国计算机安全学术交流会论文集(第二十三卷)[A],2008.

[6] 崔艳娜,张红金,李继安. 工业控制系统漏洞的统计及其分析研究[J]. 电子产品可靠性与环境试验,2018(6):41-46.

[7] 龚正虎,卓莹. 网络态势感知研究[J]. 软件学报,2010年07期

[8] 王娟. 大规模网络安全态势感知关键技术研究[D]. 成都:电子科技大学,2010.

[9] 胡威. 网络安全态势感知若干关键性问题研究[D]. 上海:上海交通大学,2007.

[10] 陶耀东,贾新桐. 工业控制系统网络安全态势感知框架研究[J]. 信息技术与网络安全,2018(5):3-6.

[11] 白雪原. 工控系统安全威胁及防护应用探讨[J]. 中国信息化,2018(5):70-71.

(收稿日期:2019-11-01)

作者简介:

张大松(1985 -),男,博士,高级工程师,主要研究方向:信息安全、工控安全、机器学习、智能控制。

(上接第 9 页)

[11] 顾兆军,刘东楠. 一种面向廊桥 AP 的 ECC 身份认证方案[J]. 小型微型计算机系统,2019,40(1):98-103.

[12] KA A K. RMAC-A lightweight authentication protocol for highly constrained IoT devices [J]. International Journal on Cryptography and Information Security (IJCIS),2018,8(3):1-14.

[13] 张刚,石润华,仲红. 车载自组织网络中基于身份的匿名认证方案[J]. 计算机工程与应用,2016,52(17):101-106,122.

(收稿日期:2020-01-12)

作者简介:

李秋月(1992 -),女,硕士研究生,主要研究方向:网络与信息安全。

赵艳(1980 -),女,博士,主要研究方向:信息安全。

李世明(1976 -),男,硕士,副教授,主要研究方向:网络与信息安全、物联网技术、数据挖掘。

版权声明