国产化泛在物联网安全防护系统的设计与应用

曾 彬，苏亮源，文吉刚

（湖南友道信息技术有限公司，湖南 长沙 410080）

摘 要： 针对物联网的终端类型多、规模大、维护难度大、面对新型攻击缺乏应对手段等难题，以物联终端资产风险检测为核心，基于海光国产化硬件平台，融合物联网终端分类、异常检测、协议精细化识别、智能准入控制等手段，形成了一套高效的一体化物联网安全防护解决方案，实现物联网风险、性能、资产、流量等全网数据的态势感知分析与综合呈现，多维度、多视角监控物联网流量、全网风险、属性状态、资产异变等情况。

关键词： 物联网；安全防护；资产探测；威胁检测

中图分类号： TP391　　**文献标识码：** A　　**DOI：** 10.19358/j.issn.2096-5133.2021.09.007

引用格式： 曾彬，苏亮源，文吉刚. 国产化泛在物联网安全防护系统的设计与应用[J]. 信息技术与网络安全，2021，40(9)：38-43.

Design and application of localized ubiquitous Internet of Things security protection system

Zeng Bin，Su LiangYuan，Wen Jigang

(Hunan YouDao Information Technology Co.，Ltd.，Changsha 410080，China)

Abstract： Aiming at the problems of many types of IoT terminals，large scale，difficult maintenance，lack of response means in the face of new attacks，this paper takes IoT terminal asset risk detection as the core，based on Haiguang′s domestic hardware platform，integrates IoT terminal classification，anomaly detection，protocol fine identification，intelligent access and other means，and forms a set of efficient integration platform. The Internet of Things security protection solution realizes the situation awareness analysis and comprehensive presentation of the Internet of Things risk，performance，assets，traffic and other network wide data，and shows the Internet of Things traffic，network wide risk，attribute status，assets changes and other situations from multi-dimensional and multi perspective.

Key words： Internet of Things；security protection；asset detection；threat detection

0 引言

泛在电力物联网将电力用户、电网企业、发电企业、供应商及其设备，以及人和物连接起来，产生共享数据，为用户、电网、发电、供应商和政府社会服务[1]。然而，随着万物互联的应用在深度上和广度上不断扩展，物联网安全事件频发，物联网攻击导致设备被控、用户隐私泄露、云服务端数据被窃取以及影响基础通信网络正常运行等严重后果[2]。在物联网平台侧，依托已有成熟的安全防护标准规范，具备完善的安全防护技术体系和管理制度。但靠近边缘接入侧，各种物联代理装置、传感装置、物联终端等具有分布广、资源受限、数量众多、异质化严重等特点，成为泛在电力物联网安全防护的薄弱点[3-4]。物联环境存在连接海量、数据异构复杂、私有协议多等诸多挑战，而且针对物联网应用系统安全漏洞的新型攻击手段让传统防御手段难以满足要求。现有系统和研究缺乏场景化分析，更多停留在资产识别、脆弱性分析等方面，缺乏对流数据、元数据、包数据、事件数据等进行关联分析和攻击溯源，如事件调查、历史回溯、条件组合等的效果都有待提高，才能满足物联网场景下的融合分析需求[5-7]。近年来，伴随物联网防护技术的发展，物联网安全防护手段将由“被动防御”向“主动防护”转移，物联网空间资产安全监测与防护技术的应用

可有效规避、抵御物联网在电力等应用领域存在的安全威胁及风险[8-9]。

1 系统设计

本文针对电力物联网中的端-边防护场景进行研究，通过关键技术研究，实现对感知层终端安全检测准入、对终端安全身份认证及访问控制。平台整体原理如图 1 所示，轻量级边缘代理部署在物联网感知层，与物联终端级联并处于同一物理实体内。探针设备通过被动流量镜像、主动探测扫描、日志搜集等多元化手段实现数据包、指纹数据、异常信息等数据的集采分析。

设备支持虚拟化与模块化分布式部署，系统硬件的核心组件采用国产解决方案，融合海光正交化平台架构，采用高性能海光处理器和 FPGA 的集成互联方案，自主研制适配国产硬件的安全软件，适配麒麟、统信操作系统，形成安全可控、高性能的的软硬件架构。

系统数据架构包括五个层次，从探针获取的原始数据、主动探测数据经过每一层的数据分析，最后得到需要的维度分析数据。

(1)前端设备。数据采集层通过设备主被动协同，实现数据的集中获取，提供基础网络通讯的流量数据、各类设备的指纹数据、设备监控异常信息等。数据知识层主要为网络流量、资产信息、网络日志、索引等提供存储载体，作为数据知识层，可为后期的数据分析提供数据源，为数据知识层提供指标加工与扩维。数据接口层主要用于应用层与知识层之间的数据通信与二次调用分析，同时满足第三方数据分析系统的数据输出，在基于数据训练、深度挖掘分析的基础上实现数据的关联共享、场景分析与多维呈现的可视化效果。

(2)风控运维中心。数据应用层主要指部署在中心机房的风控运维中心，通过对多分布式的前端设备进行集中统一管理，实现子模块的接入管理、任务调度、综合数据关联，数据深度分析，场景事件发现分析、风险等级评估等功能。同时实现风险、性能、资产、流量等全网数据的态势感知分析与综合大屏呈现，以多维度、多视角、可视化方式整体展示

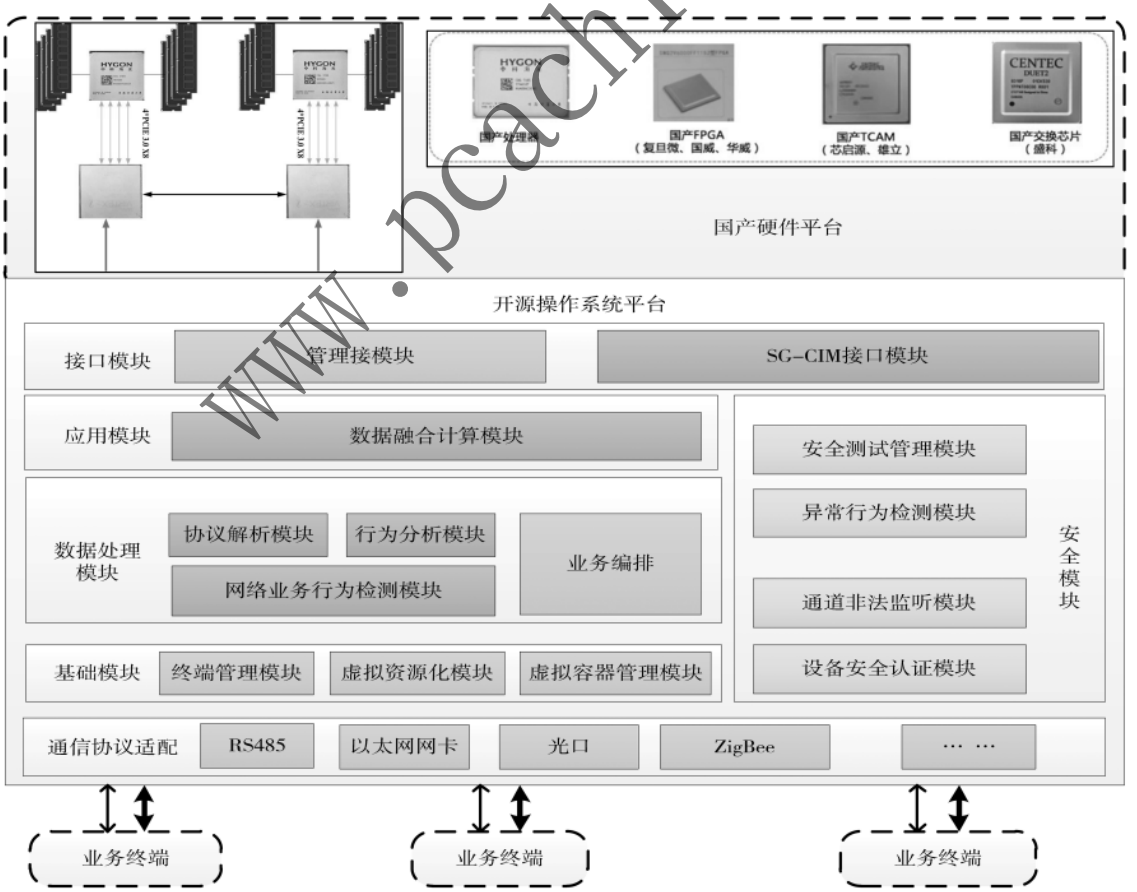

图 1 平台总体原理架构

物联网流量、全网风险、属性状态、物联网资产等异变情况，系统主要功能组成如图 2 所示。

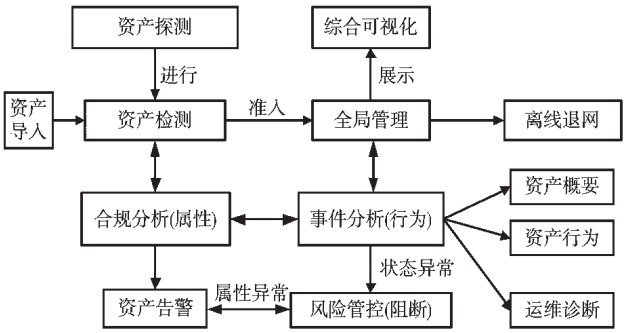

图 2 系统功能组成图

2 关键技术

2.1 主被动结合的异构数据采集及关联技术

借助于被动 DPI、主动测量/扫描、日志采集等方法，靠近终端接入层，获得丰富、细粒度的流量、性能、服务质量以及资产、安全相关的数据，实现对各物联资产设施，包括硬资源、软资源、以及应用资源等进行全面统一监控和可视化管理，如图 3 所示。同时流记录存储采用了多维分级索引技术，并实现了目录与源数据分离分级存储的技术[10]，以高速检索引擎为核心，基于流量日志广泛存在的半结构化特点，分离出结构化的日志数据，以此建立一级索引项；同时将日志的非结构化部分数据以文件形式存储至分布式文件系统中，并建立一级索引以便后续快速定位数据。同时，基于内网资产视角的告警汇聚，围绕以内网资产为核心梳理告警数据，将海量多源异构告警数据汇聚为风险事件，降低 99% 以上的冗余信息，协助用户更高效地梳理网络风险事件，有效解决物联网安全防护中的海量冗余告警问题。

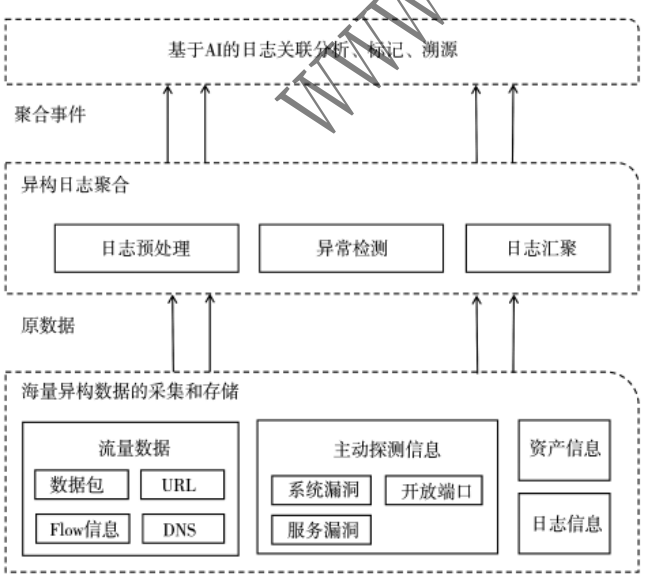

图 3 主被动结合的异构数据采集关联框架

2.2 物联终端协议特征提取身份标识技术

物联设备的协议异质性较高，海量异构终端的身份标识需要具有唯一性、可知性、可识别性[11]。因此需要在设备类型和协议不可知的情况下，对目标设备的可信终端身份标识进行提取，从而可以适用于各种不同的物联网设备类型，无需繁琐地收集设备类型或有关支持规范的协议特定知识活动识别任务。系统通过网络元数据拆解来标注物联设备的类型及属性，使用不同的功能粒度得到 IP 地址、端口号和 DNS 信息不能够实现对物联网设备活动推断的结论，又观察到客户端/物联网设备和服务器轮流以请求-回复通信方式进行，并由此可以推断物联网设备活动。单个请求和回复的数据包长度唯一地标识了设备事件的结论，也可以借鉴。通过高统计特征与其他特异性特征相结合的方法，利用当下研究结论显示最终分类结果。提取标识过程如图 4 所示。

2.3 基于国产化基础平台的数据包处理优化技术

电网的特殊环境要求必须发展自主化、安全可信的核心基础软硬件。近年来 CPU/FPGA 可重构混合体系架构取得长足发展，能够更方便快捷地提供更高层次的并行运算能力，满足海量物联设备连接的并发监测分析需求。系统采用海光国产硬件平台，业务板块采用业内独有的国产 FPGA+国产 CPU 异构处理方案。基于并行协同处理的硬件线程执行异构架构，实现对可重构资源的硬件线程加速方式利用。同时，原始数据存储使用并行处理方式，存储处理单元之间相互隔离，没有信息交互。软硬件线程通过共享数据存储方式进行多线程并行执行，共享数据结构，减少资源竞争，提升了线性的加速比。另外，最大化利用 CPU 和 FPGA 各自特性，既保障了设备的高性能，又为后期的灵活扩展升级留下了空间。

3 系统组成与实施

系统采用分布式监控、集中式管理的架构，核心子系统分为检测探针、准入探针和风控运维中心。“检测探针”从核心交换机的镜像端口获取原始流

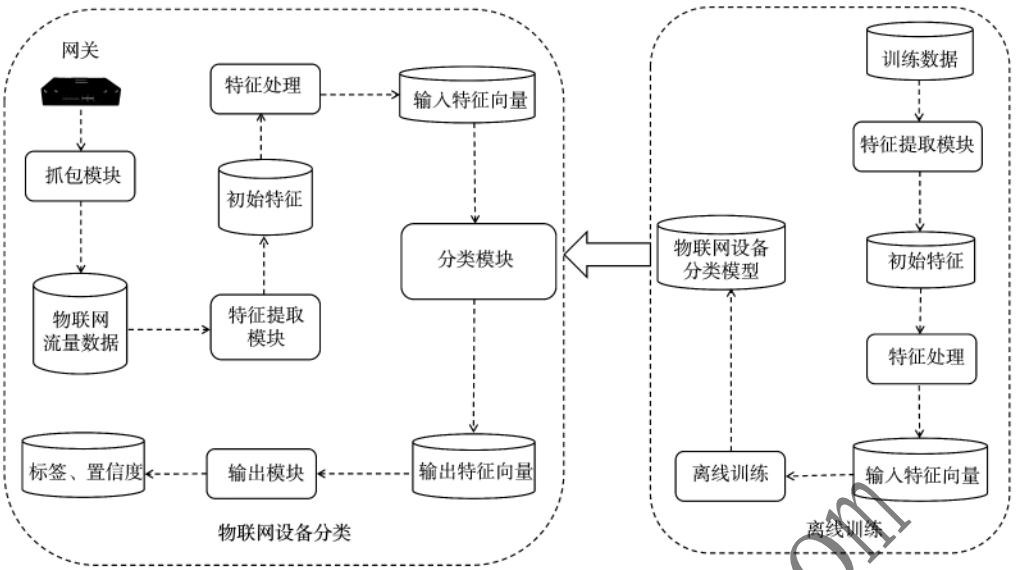

图 4 物联终端协议特征提取过程

量，对网络中的“真实生产数据”进行分析，从交换机的镜像端口获取原始流量。对复杂网络系统的监测需要在网络路径上的多个重要节点进行监测分析，因此可能引入 TAP，将各节点的数据进行合并以后，统一送到检测探针进行分析。“准入探针”一般旁入在接入侧交换机，对网络中的非法网络行为、非法接入设备进行主动探测与辨识，实现全方位的风险感知与智能管控。“风控运维中心”通常的情况下部署在核心数据中心，负责系统的全局管理、探针的策略集中管理和态势感知。系统的典型部署方式如图 5 所示。

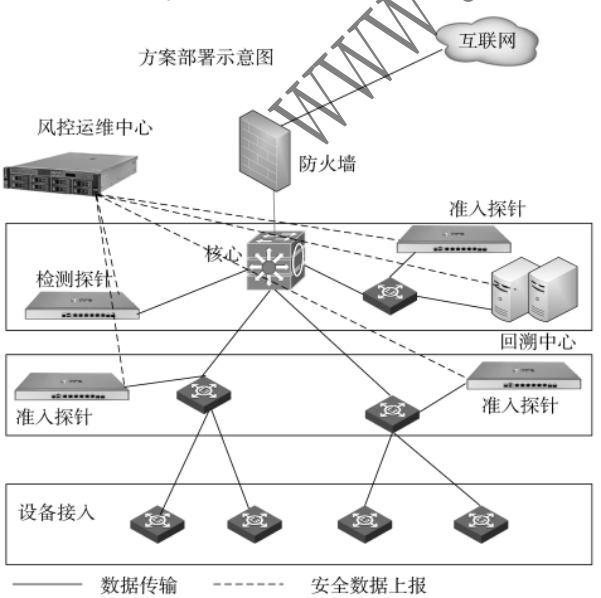

图 5 系统典型部署实施方案

(1)检测探针

针对信息系统的安全运维挑战，目前使用流量透视、回溯审计、性能监控、入侵检测、资产管理、漏洞扫描 6 位一体的检测探针，实现了网络流量分析、网络性能分析、风险事件分析、历史数据回溯分析四维一体的全网监控手段，为信息系统网络管理提供全新的解决方案与全方位的数据分析。

检测探针基于信息系统各个区域中心节点的采集数据，通过流量、性能、风险三方面的指标数据复合分析、建模分析。解决信息系统网络资产梳理及风险评估、流量异常问题、物联网设备运维问题、攻击检测判定、非法外联与 CC 远控、溯源分析、行为审计等需求。

(2)准入探针

准入探针是解决现存于物联网及传统网络中的终端安全问题设计的专用产品，兼容物联网及传统网络应用场景，可有效识别针对传统 PC、服务器、哑终端、智能设备等多种终端，对识别物联网终端进行有效准入控制，解决海量 IP 设备的接入认证和安全管控问题，帮助用户构建安全可控的物联网网络。

(3)风控运维中心

风控运维中心为集中管理平台，实现子系统的接入管理、任务调度、综合数据关联、数据深度分析、场景事件发现分析、风险等级评估等功能。同时实现风险、性能、资产、流量等全网数据的态势感知

分析与综合大屏呈现，以可视化方式整体展示物联网流量、全网风险、准入管控、资产管理等异变情况，如图 6 所示。

4 系统实现与应用

通过多元化采集、大数据存储检索与 AI 智能分析，实现“检测、响应与处置”的一体化物联网综合、智能化安全监测防护解决方案。系统目前已经在电力/公安监所等行业实现了推广应用，在物联网环境下的资产识别准确度达到 90%以上，应用识别规则数量超过 3 000 种，准确度达到 95%(IPv4/v6)，覆盖 32 个大类 42 000 余种攻击行为，包含 6 万条以上的漏洞规则等；单台前置探针管控物联网设备数量在 1 000 以上，最大处理流量吞吐量达到 10 Gb/s，并发连接数监测超过 100 万条。

(1)资产集中管理

基于网络运维资产与物联网终端资产的集中发现管理，对如 PC、服务器、业务系统、数据中心等资产进行有效运维管控，同时建立针对于物联网资产的识别、管控机制。对接入客户视频监控网络的物联网资产(如网络摄像头、录像机、门禁系统、报警系统、对讲机等)进行有效识别，并利用系统实现自动化资产统计、档案管理(IP、MAC、品牌、型号等)、IP 地址管理。

(2)资产画像分析

物联系统资产感知梳理，发现无主设备、非法设备，能够无损、安全、准确地识别工控网络中的各类物联系统、设备、软件以及其他运行中的 IT 服务器、数据库和网络设备。支持漏洞扫描、风险评估。组织漏洞快速定位、整改，跟踪安全资产状态，保证资产良性运行，保证网络风险、脆弱性评估的准确性，保证对攻击行为的响应处置的即时性。

(3)智能准入控制

通过部署在客户网络节点的准入探针，主动对物联网资产发起扫描探测，基于 IP、MAC、设备指纹等多维度进行识别，判断设备身份。对于私接和仿冒行为，根据准入规则进行二层阻断或三层联动交换机阻断，合法设备主动准入。对于设备漏洞、设备弱口令、高危端口、私接仿冒、异常流量进行有效管理。

(4)运维故障诊断

通过在核心交换机、互联网出口或其他节点位置设置镜像口，在网络节点位置处将流量送入监测分析系统，进行单节点或多节点关联分析，实现网络性能服务路径的统一分析，支持网络环路、IP 冲

图 6 实际环境下的物联网资产风险评估数据

突、广播风暴、ARP 欺骗等日常网络运维管理分析。

(5)异常检测溯源

系统通过交换机端口镜像网络流量方式实现对所有在网资产的上下行流量包检测。全面实时监测网络中 2~7 层协议/应用的字节/数据包流量大小、构成、分布和变化情况,利用流量基线、行为基线等分析模型捕捉到流量突发异常点,并对异常点的流量进行深入跟踪与分析。支持外联风险分析,展示内网主机外连的总体情况,包括主机分布、外连地区排行、外连风险类型排行、异常时间外连等,并展示外连风险主机排行。

(6)高级威胁检测

通过 DGA、数据标记、数据训练、机器学习、行为分析模型与多维度复合数据分析等检测技术,对网络中的木马、病毒的攻击行为进行实时检测分析,支持对勒索病毒、挖矿等新型病毒以及新型的攻击方式和攻击工具的识别与预警,支持对攻击链还原的可视化展示,运维人员可以更直观地看到某一个攻击行为的攻击细节,也可看到某个风险事件在攻击链中所处的位置。

5 结论

本文依托现有物联网资产管理平台的数据优势,建立“物联网空间安全防护平台”,优化物联网风险运维管理流程,实现了重大风险线上线下互相监督、联动处置,缩短了响应时间,提高了响应质效,真正实现风险的立体防控。同时,对物联终端信息进行系统性管理,深入数据分析,提炼关键指标,及时进行风险管控,支持网络访问逻辑关系的自动生成,配合安全、性能等模块实现非正常连接判断与深度分析,实时掌握用户网络性能信息、业务访问信息、安全风险信息等,达到对物联网全感知的安全监控。

参考文献

[1] 黄立.泛在电力物联网建设技术构架及实现方案[J].物联网技术,2021,11(2):74-75.

[2] 鲁伦.泛在电力物联网主要特征分析及安全技术展望[J].电力安全技术,2020,22(9):8-10.

[3] 廖会敏,玄佳兴,甄平,等.泛在电力物联网信息安全综述[J].电力信息与通信技术,2019,17(8):18-23.

[4] 陈继兴,赵普,袁磊,等.物联网和大数据技术在电力安全管控中的应用[J].科技创新与应用,2020(35):171-172.

[5] YOUSUF O,MIR R N.A survey on the Internet of Things security:state-of-art,architecture,issues and countermeasures[J].Information and Computer Security,2019,27(2):292-323.

[6] IDRISSI I,AZIZI M,MOUSSAOUI O.IoT security with deep learning-based intrusion detection systems:a systematic literature review[C]//2020 Fourth International Conference On Intelligent Computing in Data Sciences(ICDS),2020.

[7] 田秀霞,刘天顺,牛晓宇,等.面向泛在电力物联网云端数据的轻型动态完整性审计方案[J].计算机学报,2020,43(12):2298-2314.

[8] 中商产业研究院.2020-2026 全球及中国物联网(IoT)安全技术行业发展现状调研及投资前景分析报告[R].2020.

[9] 张玉清,周威,彭安妮.物联网安全综述[J].计算机研究与发展,2017,54(10):2130-2143.

[10] 李艳,王纯子,黄光球,等.网络安全态势感知分析框架与实现方法比较[J].电子学报,2019,47(4):927-945.

[11] 马政朝,郑瑞娟,吴庆涛,等.一种物联网安全属性概念提取方法[J].计算机仿真,2014,31(3):303-307.

(收稿日期:2021-04-28)

作者简介:

曾彬(1979-),男,博士,高级工程师,主要研究方向:网络测试、网络安全、大数据分析。

苏亮源(1986-),男,硕士,主要研究方向:网络安全、网络性能管理。

文吉刚(1978-),男,博士后,主要研究方向:网络流量分析、网络性能管理,网络安全。

版权声明

经作者授权，本论文版权和信息网络传播权归属于《信息技术与网络安全》杂志，凡未经本刊书面同意任何机构、组织和个人不得擅自复印、汇编、翻译和进行信息网络传播。未经本刊书面同意，禁止一切互联网论文资源平台非法上传、收录本论文。

截至目前，本论文已经授权被中国期刊全文数据库（CNKI）、万方数据知识服务平台、中文科技期刊数据库（维普网）、JST 日本科技技术振兴机构数据库等数据库全文收录。

对于违反上述禁止行为并违法使用本论文的机构、组织和个人，本刊将采取一切必要法律行动来维护正当权益。

特此声明！

《信息技术与网络安全》编辑部

中国电子信息产业集团有限公司第六研究所