文章编号:1671-4598(2020)12-0117-05 DOI:10.16526/j.cnki.11—4762/tp.2020.12.025 中图分类号:TP393 文献标识码:A

异构环境下无线传感大数据跨域传输安全控制系统设计

徐 良[1,2]
(1. 华南理工大学 计算机科学与工程学院，广州 510006；
2. 青海警官职业学院 现代教育技术中心，西宁 810000)

摘要：在异构环境下无线传感大数据受到网络入侵影响，容易出现数据丢包率高且传输效率低的问题，因此设计了异构环境下无线传感大数据跨域传输安全控制系统；根据异构环境下无线传感网络结构，设计由数据采集模块、处理模块和显示模块组成的系统总体结构；选择SY AD 08T型号数据信号采集器，监控现场数据采集显示结果；使用Ryzen 3 2200G型号核心处理器支持自适应动态扩频，执行处理指令；通过控制电路中电压值范围，调节电流强度；软件设计部分利用高维数据空间降维改进算法，借助ELM分类器检测大数据跨域传输入侵情况，利用通信窃听方式添加噪声控制接收端信噪比上限，以此控制跨域传输噪声；融合信道编码纠错与密码流扰乱，限制数据解码时间，阻止非正常渠道窃听；在网络环境和配置清单支持下进行实验验证分析，由实验结果可知，该系统丢包率低于1.5%，大数据传输效率最高为98%，有效增强了大数据跨域传输安全性。

关键词：异构环境；无线传感；大数据；跨域传输；安全控制

Design of Cross—Domain Transmission Security Control System for Wireless Sensor Big Data in Heterogeneous Environment

Xu Liang[1,2]
(1. Computer Science and Engineering, South China University of Technology, Guangzhou 510006, China;
2. Modern Education Technology Center, Qinghai Vocational College of Police Officers, Xining 810000, China)

Abstract: In the heterogeneous environment, wireless sensor big data is affected by network intrusion, which is prone to problems of high data packet loss rate and low transmission efficiency. Therefore, a cross—domain transmission security control system for wireless sensor big data in a heterogeneous environment is designed. According to the structure of the wireless sensor network in a heterogeneous environment, the overall structure of the system composed of data acquisition module, processing module and display module is designed. Select the SY AD 08T model data signal collector to monitor the on—site data acquisition display results; use the Ryzen 3 2200G model core processor to support adaptive dynamic spread spectrum, execute processing instructions; adjust the current intensity by controlling the voltage value range in the circuit. The software design uses the improved algorithm of high—dimensional data space dimensionality reduction, uses the ELM classifier to detect the intrusion of large data cross—domain transmission, and uses communication eavesdropping to add noise to control the upper limit of the signal—to—noise ratio at the receiving end to control cross—domain transmission noise. Fusion of channel coding error correction and cipher stream disruption limits data decoding time and prevents abnormal channels from eavesdropping. The experimental verification analysis was carried out under the support of the network environment and configuration list. From the experimental results, it can be seen that the system's packet loss rate is less than 1.5%, and the maximum data transmission efficiency is 98%, which effectively enhances the security of large data cross—domain transmission.

Keywords: heterogeneous environment; wireless sensing; big data; cross—domain transmission; security control

0 引言

在异构环境下提供数据共享机制，用户能够随意访问信任区域中的信息，有效提升数据传输效率[1]。但异构环境中包含不同的操作系统及通信协议，很难实现资源统一，因此难以达到用户同时跨域安全传输的目的，还会影响传输过程中的数据完整性。因此，异构环境下的无线传感大数据传输成为当前大数据研究领域重要问题之一[2]。

目前已有相关学者对异构环境下的数据安全传输机制做出了研究，其中，最常见的包括非合作博弈控制系统和数据跨域传输任务完成度量化控制系统。非合作博弈控制系统采用斯坦伯格功率模型控制大数据分布式功率，控制通信双方均衡传输。采用该系统虽然能在异构环境下保证大数据传输安全性，但难以满足实时性传输需求；数据跨域传输任务完成度量化控制系统引入通信任务完成机制，通过构建量化评估模型，深入分析大数据跨域传输判定因素，给出数据安全传输策略。该系统虽然有效均衡数据跨域传输任务，但无法保证大数据传输安全性。基于此，提出了异构环境下无线传感大数据跨域传输安全控制系统设

收稿日期:2020-04-23； **修回日期**:2020-05-19。

作者简介:徐 良(1988-)，男，青海海东人，大学本科，讲师，主要从事网络管理、信息网络安全、数据库(大数据)方向的研究。

计，对数据跨域传输要求较低，能够适应复杂异构环境。

1 异构环境下无线传感网络结构

异构环境下无线传感网络结构是由网络节点和各个基站组成的，其中传感网络节点具有感知物理信息、处理信息能力，其结构如图 1 所示。

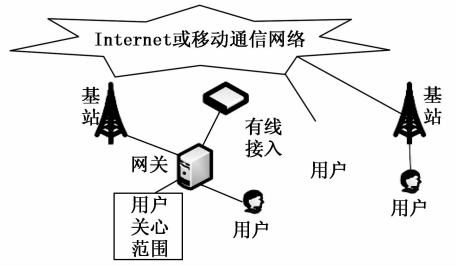

图 1 异构环境下无线传感网络结构

异构环境下的网络结构主要包括 CVR－100UC 型号物理信息采集器，主要感知需要数据，同时对采集数据转换；i5 9400F 型号处理器负责整个传感节点操作；无线通信模块负责与其他基站进行无线通信，交换采集到的数据；能量供应模块为传感节点提供所需能量，该能量一般是由 CR－2032 型号电池提供的[3]。异构环境下无线传感网络节点由于电池供电原因，具有通信能力有限的缺点，需要不断更换电池，并在户外难以保护节点，容易遭到不法分子入侵[4]。

2 系统结构设计

采用 SY AD 08T 型号数据信号采集器大数据跨域传输控制系统硬件主要分为 3 个模块，分别是数据采集模块、处理模块和显示模块[5]。其中采集模块具有多个采集节点，保证数据完整采集，避免数据丢失[6]。使用 FPGA 转换器接口采集数据时，需通过 Ryzen 3 2200G 型号核心处理器处理采集到的数据，剔除冗余数据，之后将处理好的数据传送给 SDRAM 进行数据存储，由 LG 25UM58－P 25 英寸显示器显示控制结果[7]。系统总体结构如图 2 所示。

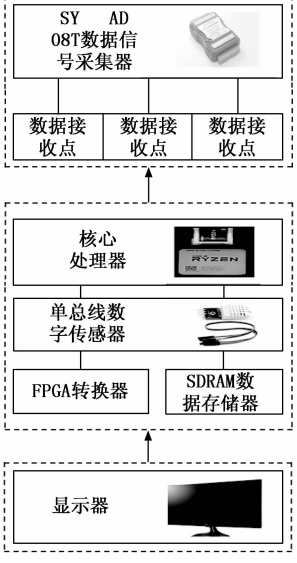

图 2 系统总体结构

控制系统的数据采集节点传感器为 Risym DHT22 型号单总线数字传感器，具有三根外部引脚[8]。为保证电源稳定，数据采集模块分别使用外接电源和内设电池两种方式，允许通过电压为 1.2～15 V。针对多通道数据并行传输信号特点，应及时调整微处理器芯片所需的电压或电流数值[9]。

2.1 数据信号采集器

选择 SY AD 08T 型号数据信号采集器具有成本低、体积小的优势，安装极为方便，用户可根据现场数据采集显示结果进行监控[10]。该采集器可实现传感器和主机之间信号安全隔离、采集、转换、监控与传输，其内部具有 RS－485 串行通信模块，每个模块串口最多可接 256 个 SY AD 系列模块，能与其他控制模块挂在同一 RS－485 总线上，方便主机控制与编程[11]。该采集器如图 3 所示。

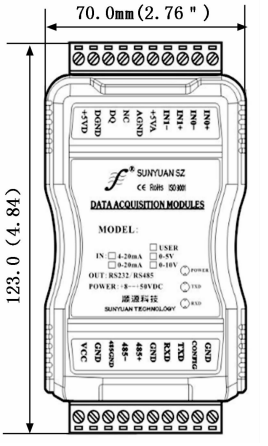

图 3 SY AD 08T 型号数据信号采集器

SY AD 08T 型号数据信号采集器可以测量两路或四路不会互相干扰的电流或电压信号，支持 ASCII 字符协议和 MODBUS RTU 通讯协议，响应时间小于 100 ms。根据需要设置校验和，该采集器内部含有瞬态抑制二极管，能够抑制浪涌脉冲，也可抑制来自网络的工频干扰。

2.2 核心处理器

核心处理器又称为内核处理器是 CPU 重要组成部分，其是以单晶硅生产工作制造而成的，所有执行命令都是通过该核心完成的[12]。选择 Ryzen 3 2200G 型号核心处理器具有 4 核线程，3.5 GHz 基频，支持自适应动态扩频，配置 Radeon Vega^8 Graphics 显卡和 AM4 主板。

CPU 从内核中去除指令，由存储器对指令译码，并将其分解成一系列微操作，并发出控制命令，进而完成一套指令的执行。

2.3 控制电路

对控制系统中电源单元的信号来说，重点控制的是电压值范围，应保持单次电压输入稳定性，进而保证控制系统信号采集稳定性。控制电路如图 4 所示。

电源输出信号稳定与数据控制精度有关，因此，数据节点传感器引脚与电源输出端直接连接，电压输出值也会

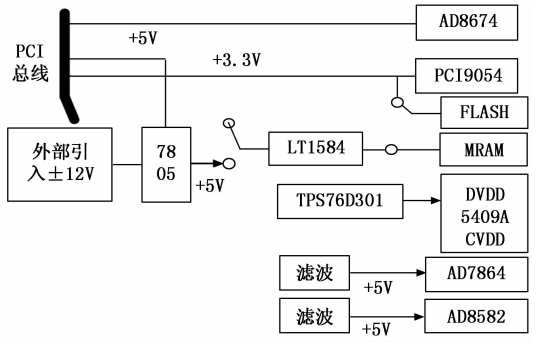

图 4　控制电路

影响电源单元电流输出强度，如果通道引脚输出的是电流信号，那么调节电流强度可以采用增减高精度电阻方式来实现。

3　软件部分设计

软件系统主要功能设计包括入侵检测和控制方案两个部分，其中入侵检测需要数据传输、存储与显示功能的支持，而控制方案需要远程控制功能的支持，系统软件框架及功能如图 5 所示。

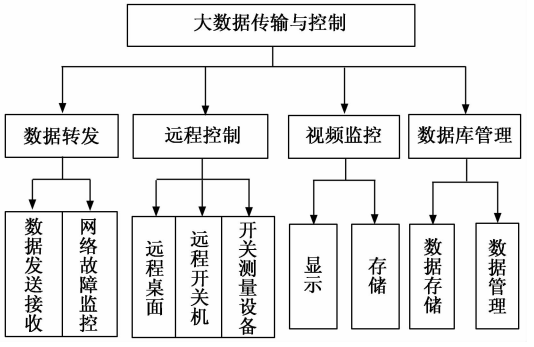

图 5　系统软件框架及功能

依据图 5 所示的各部分功能，对入侵检测和控制方案展开分析。

3.1　入侵检测

使用高维数据空间降维改进算法，结合相似性度量函数，利用 ELM 分类器实现异构环境下无线传感大数据跨域传输入侵检测，如图 6 所示。

图 6 中的各个元素依次为：$\boldsymbol{X}$ 为总样本特征矩阵、Y 为输入量输入分类器、T 为期望输出、N 为训练样本、H 为隐层节点的输出矩阵、n_i 为代表 i 类样本数、c 为样本种类、d 为样本特征维数、m 为特征向量维数、L 为隐藏层节点数。

将训练数据降维处理后生成转换矩阵形式，并将转换矩阵输入 ELM 分类器之中，由此获取隐层节点与输出层节点之间的输出权重。将测试后数据输入 ELM 分类器中进行分类处理，并输出检测结果。

步骤一：使用 0 均值标准化方式处理大数据，具体计算公式如下所示：

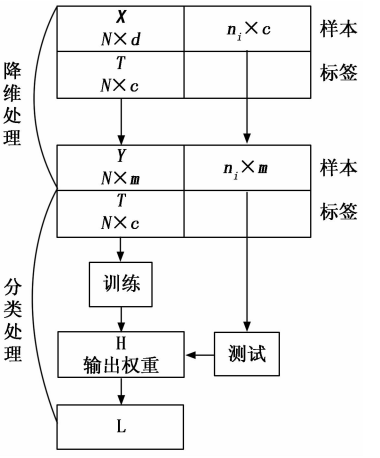

图 6　检测流程图

$$p = \frac{a - z}{s^2} \tag{1}$$

公式（1）中，a 表示原始输入量；p 表示预处理后输出数据；z 表示原始数据集各个维数均值；s^2 为方差。

步骤二：根据公式（2）得到累计散度矩阵 $\boldsymbol{Q}$：

$$\boldsymbol{Q} = \sum_{i=1}\sum_{j=i+1}\omega_{ij} n_i n_j (\beta_i - \beta_j)(\beta_i - \beta_j)^T \tag{2}$$

公式（2）中，ω_{ij} 表示数据空间相似性度量函数；n_i、n_j 分别表示第 i 和第 j 类样本数；β_i、β_j 分别表示第 i 和第 j 类在 T 维上均值。

步骤三：依据上述公式构建目标函数，并分解特征问题，获取特征值和向量；

步骤四：选取最大特征值所对应特征向量作为转换矩阵，并确定训练样本数据集；

步骤五：将降维后数据集作为分类器输入数据集，同时产生分类器输入权重；

步骤六：将上述获取的转换矩阵作为输入量输入分类器，由此获取检测集所对应的隐藏层输出矩阵；

步骤七：利用步骤六获得输出权重，并计算检测数据分类结果。

依据上述步骤，完成入侵检测。

3.2　控制方案设计

控制方案设计框架如图 7 所示。

在图 7 所示的框架下，对添加噪声控制和添加编码纠错与密码流扰乱控制进行详细分析。

3.2.1　添加噪声控制

利用通信窃听方式添加噪声控制接收端信噪比上限，使系统在异构环境下精准检测跨域传输信道编码参数缺陷，并通过主动添加方式，实现对跨域传输接收端信噪比上限精准控制。

在异构环境中，应先分析跨域发送端向接收端发送的敏感数据，由此获取接收端接收时的信号信噪比。在传送端添加跨域传输条件下的敏感数据时，应保证接收端噪声

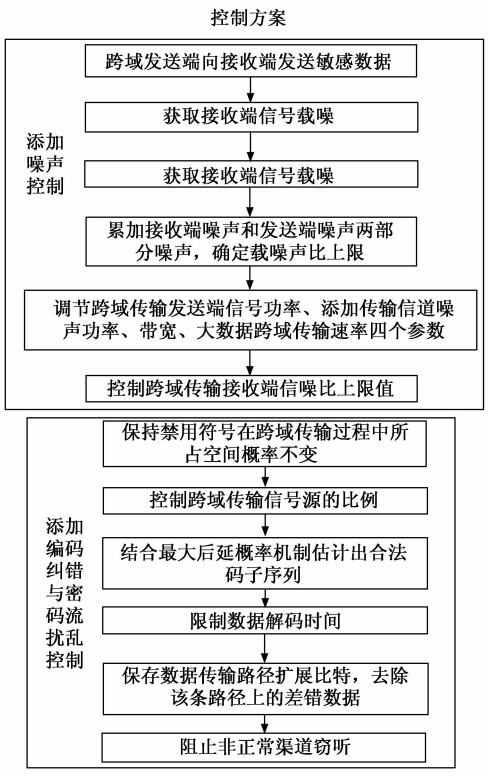

图 7 控制方案设计框架

和发送端噪声之间没有关联性，才能在跨域传输数据接收端出累加两部分噪声，确定信噪比上限。大数据跨域传输发送端通过对跨域传输发送端信号功率、添加传输信道噪声功率、带宽、大数据跨域传输速率 4 个参数调节，精准控制信噪比上限值。

3.2.2 添加编码纠错与密码流扰乱控制

引入映射控制算术码内映射的多个禁用符号，融合跨域传输信道编码纠错与密码流扰乱，能够阻止跨域传输发送端精准码流的获取，减小噪声影响。

保持禁用符号在跨域传输过程中所占空间概率不变，通过混沌映射生成密码流，控制跨域传输信号源的比例。预估存留在数据传输路径上的数目，限制数据解码时间。在迭代阶段，保存数据传输路径扩展比特，去除该条路径上的差错数据。入侵者在没有敏感数据密钥支持情况下，很难精准获取跨域的传输数据，有效阻止了非正常渠道的窃听。

综上所述，异构环境下无线传感大数据跨域传输安全控制系统软件功能分为入侵检测与控制方案设计两部分。引入高维数据空间降维改进算法及相似性度量函数获取入侵数据特征，利用 ELM 分类器得到输出权重，完成入侵数据检测及分类；通过调整传输信道噪声功率、带宽及传输速率控制信噪比上限值，通过映射控制算术码去除差错数据，控制了入侵数据的传输，完成了构环境下无线传感大数据跨域传输安全控制系统设计。

4 实验分析

通过设置实验来验证异构环境下无线传感大数据跨域传输安全控制系统设计合理性。

4.1 网络环境设置

无线传感网络中节点在基站协助下，形成一个网络拓扑结构，以此作为实验环境。当网络中节点感知到监测区域信息后，通过路由将数据传输到各个基站之中，并对来自节点数据信息进行预处理。

网络环境设置如图 8 所示。

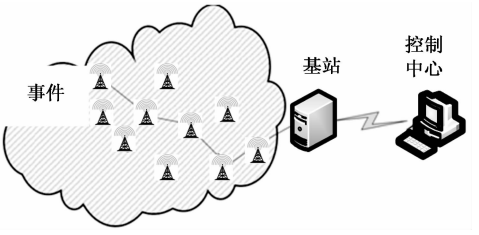

图 8 网络环境设置

依据图 8 所示网络环境设置实验配置参数，如表 1 所示。

表 1 配置清单

处理器	I5 9400 六核六线程
散热器	塔式双铜管散热器
主板	GA－B365M－Power
显卡	GeForce GTX1660 6GD
内存	8G DDR4 2666
硬盘	256GB M.2 固态硬盘
机箱	HALO
电源	400W 电源

4.2 网络安全威胁设置

针对无线传感网络受到安全威胁设置，需将网络与其它网络融合时受到的入侵设置为主要威胁方式。这种威胁方式为在融合前就已经存在，由于网关是整个网络传输中心部分，同时也是网络提供服务的唯一接口，因此，可认为网关是整个网络的安全瓶颈。恶意程序对秘密信息访问如图 9 所示。

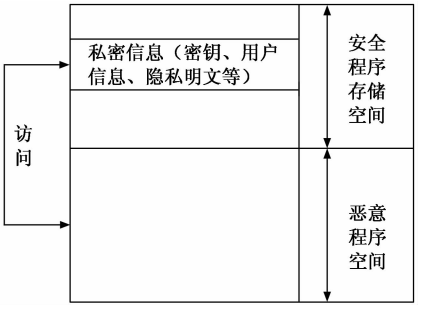

图 9 恶意程序对秘密信息访问

针对网关使用拒绝式攻击时，会导致整个网络失败，

这类攻击一般是通过相关协议进行防御的，因此，对动态用户认证协议作出修改。

4.3　实验结果与分析

将全部控制节点更新为 sink 节点，以此观测不同阈值范围内及不同节点数量规模下，传统系统与异构环境下控制系统大数据跨域传输过程中的丢失情况，需进行两组实验。第一组实验验证的是数据丢包率，第二组实验验证的是大数据传输效率。

4.3.1　数据丢包率

两种系统数据丢包率对比结果如图 10 所示。

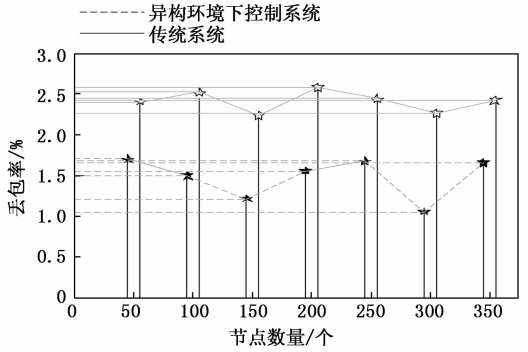

图 10　两种系统的数据丢包率对比分析

随着节点数量增加，使用传统系统始终处于高丢包率情况之中，而采用异构环境下的控制系统始终处于低丢包率情况之中，且在节点数量分别为 150 个和 300 个时，丢包率都低于 1.5%，说明这两个节点数量情况下都具有良好传输效果。因此，可以看出异构环境下的控制系统始在数据传输过程中减少数据丢失具有重要作用。

4.3.2　大数据传输效率

依据实验 1 组得到的节点数量分别为 150 个和 300 个时丢包率低的情况，分别将传统系统与异构环境下控制系统的大数据传输效率进行对比分析，结果如图 11 所示。

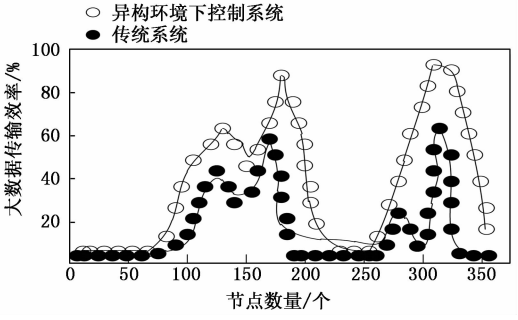

图 11　两种系统的数据传输效率对比分析

使用异构环境下控制系统大数据传输效率始终高于传统系统大数据传输效率，且在节点数量为 300 个时，大数据传输效率达到最高为 98%，而传统系统的大数据传输效率最高为 66%。针对两种系统在节点数量分别为 150 个和 300 个时丢包率低的情况，大数据传输效率却与之相反，出现这种现象的主要原因是该时段网络受到攻击较小，且异构环境下控制系统抵抗入侵能力较强，由此出现传输效率高且丢包率低的现象。

通过上述内容，验证了异构环境下无线传感大数据跨域传输安全控制系统丢包率低、传输效率高，具有良好的传输效果。

5　结束语

针对异构环境下无线传感网络节点存储特点，对其安全控制问题进行详细分析。以入侵检测为切入点设计有效控制系统，保证大数据能够在安全环境进行有效传输，在保证网络较长生命周期的同时具有良好入侵性能，从而保障大数据传输安全。实验结果表明，所设计系统的丢包率较低，传输效率高，证明该系统的传输效果好，具有实际应用价值。

此外，所设计系统在设计应用过程中还存在一些不足之处。所设计系统一般适用于地面异构无线传感网络，在其他领域存在局限性。因此，在未来研究中应针对不同应用背景对大数据跨域传输安全控制系统作出研究，进一步完善异构环境下无线传感大数据跨域传输安全控制系统。

参考文献：

[1] 江泽涛，时　晨. 混合云环境下基于异构系统的跨域身份认证方案 [J]. 计算机工程，2019，6 (10)：13－18.

[2] 孙永祺，龚会莲. 大数据驱动下破解跨域公共危机治理碎片化难题的理路探析 [J]. 领导科学，2019，5 (18)：7－11.

[3] 钟凤艳，王　艳，李念爽. 异构环境下纠删码的数据修复方法综述 [J]. 计算机应用研究，2019，10 (8)：2241－2249.

[4] 焦一鸣，周　川，郭　健，等. 异构计算环境下一种新型的多 DAG 任务调度算法 [J]. 计算机工程，2019，5 (7)：1－5.

[5] 薛开平，周焕城，孟　薇，等. 天地一体化网络无缝切换和跨域漫游场景下的安全认证增强方案 [J]. 通信学报，2019，10 (6)：138－147.

[6] 余承其，张照生，刘　鹏，等. 大数据分析技术在新能源汽车行业的应用综述——基于新能源汽车运行大数据 [J]. 机械工程学报，2019，55 (20)：3－16.

[7] 陈宇翔，郝　尧，赵　越，等. 面向制造大数据的安全存储交换技术 [J]. 电子技术应用，2019，5 (12)：38－41.

[8] 朱国康，陈奇志，徐　琨. 档案大数据安全面临的挑战与对策研究 [J]. 北京档案，2019，3 (5)：40－42.

[9] 薛　哲，郭大波，马识途. 基于 PEG 算法的连续变量量子密钥分发多维数据协调 [J]. 量子光学学报，2019，7 (2)：145－151.

[10] 闪顺章，吴　超，王从陆，等. 大数据视域下循证安全管理模式研究 [J]. 中国安全科学学报，2018，6 (6)：7－12.

[11] 王静宇，栾俊清，谭跃生. 基于数据敏感性的大数据访问控制模型研究 [J]. 计算机工程与应用，2019，8 (23)：70－77.

[12] 庄海燕. 大数据分析技术的无线通信网络安全风险预测 [J]. 微电子学与计算机，2019，4 (8)：97－100.