单位代码： 10293 密 级：



硕 士 学 位 论 文



论文题目： 无线传感器网络中的蠕虫检测

与异常数据检测方案研究

1016041018

学号

姓名

导 师

学 科 专 业

研 究 方 向

申请学位类别

论文提交日期

郑文添

吴蒙

信息安全

无线传感器网络安全

工学硕士

Security of Wireless Sensor Network

Thesis Submitted to Nanjing University of Posts and Telecommunications for the Degree of

Master of Engineering



By

Wentian Zheng

Supervisor: Prof. Meng Wu

February 2018

南京邮电大学学位论文原创性声明

本人声明所呈交的学位论文是我个人在导师指导下进行的研究工作及取得的研究成果。尽我所知，除了文中特别加以标注和致谢的地方外，论文中不包含其他人已经发表或撰写过的研究成果，也不包含为获得南京邮电大学或其它教育机构的学位或证书而使用过的材料。与我一同工作的同志对本研究所做的任何贡献均已在论文中作了明确的说明并表示了谢意。

本人学位论文及涉及相关资料若有不实，愿意承担一切相关的法律责任。

研究生学号：\_\_\_\_\_\_\_\_\_\_\_ 研究生签名：\_\_\_\_\_\_\_\_\_\_\_\_ 日期：\_\_\_\_\_\_\_\_\_\_\_\_

南京邮电大学学位论文使用授权声明

本人授权南京邮电大学可以保留并向国家有关部门或机构送交论文的复印件和电子文档；允许论文被查阅和借阅；可以将学位论文的全部或部分内容编入有关数据库进行检索；可以采用影印、缩印或扫描等复制手段保存、汇编本学位论文。本文电子文档的内容和纸质论文的内容相一致。论文的公布(包括刊登)授权南京邮电大学研究生院办理。

涉密学位论文在解密后适用本授权书。

研究生签名：\_\_\_\_\_\_\_\_\_\_\_\_ 导师签名：\_\_\_\_\_\_\_\_\_\_\_\_ 日期：\_\_\_\_\_\_\_\_\_\_\_\_\_

摘要

随着物联网技术和无线通信技术的不断发展，无线传感器网络广泛运用于现实世界中的数据采集和分析中。无线传感器网络是典型的Ad-hoc网络，由数目众多的传感器节点加上基站构成基本的网络架构，传感器节点负责收集数据，与基站通信，它们体积小，能量和内存有限。无线传感器网络需要获取实时可靠的数据来做出决策，然而由于各个节点部署在无人看守的野外环境中，节点的能量受限，会引起一系列的数据安全问题。

目前传感器网络安全的研究主要分为两个方向。一方面，如何在网络中识别和清除恶意节点，保证网络的健壮性尤为重要。无线传感器网络通常部署在无人值守的野外环境中，传感器节点极易被攻击者捕获，攻击者通过捕获节点制造恶意节点注入网络中窃取网络的数据，破坏网络的通信，夺取网络的控制权。目前针对移动节点攻击和副本节点攻击的方案已经很成熟了，但是对于蠕虫节点攻击相关的研究却非常少。蠕虫攻击对网络的损害是最大的，能够迅速感染传感器节点，使网络迅速瘫痪。另一方面，为了基站能够做出准确无误的判断，需要传感器节点能够传输可靠的数据值。因此，需要检测并剔除网络中由噪声或者传感器节点内部错误等原因引起的异常数据。然而，受限于传感器节点的计算资源和内存资源，相关的检测方案并不能在资源和检测效率上得到折衷的效果。

本文针对以上两点，进行了相关的研究。以序贯概率比检验(Sequential Probability Ratio Test,SPRT)为基础，结合偏向采样和随机值采样提出了SPRT-Biased-Random蠕虫检测方案来检测传感器网络中的蠕虫节点。实验结果表明该方案能够在5~18个时隙内检测到所有蠕虫节点，并使得传感器网络最终受感染的节点维持在2%~5%之间。针对网络中的异常数据检测，以PCA算法为基础结合马氏距离提出改进型分布式主成分异常数据检测(Improved Distributed PCA-Based OutlierDetection Method, IDPCA)方案，提高了模型的检测性能并降低了网络中的通信资源开销。实验结果表明该模型能够达到96%-97%的异常数据检测率并维持2%的异常数据误报率，同时该方案能够对异常数据进行溯源，让网络管理者能够快速定位网络问题。为了克服IDPCA方案无法很好地对线性不可分数据进行检测的缺陷，提出了基于马氏内核函数的分布式核主成分异常数据检测模型(Improved Distributed Kernel Principal Components Analysis,IDKPCA)。该方案将监测数据集映射到高维空间，能够很好地对线性不可分数据进行分类。通过使用马氏距离衡量数据向量到中心节点的距离，利用测量数据维度之间的相关性并训练最优的核参数，IDKPCA异常数据检测模型对线性不可分的数据能够达到近乎98%的异常数据检测率和2%的数据误报率。

关键词: 恶意蠕虫节点检测，异常数据检测，序贯概率比检验，PCA算法, 异常数据溯源

Abstract

With the continuous development of Internet of Things and wireless communication technology, wireless wensor networks are widely used in data collection and analysis in the real world. Wireless sensor network is a typical ad hoc network, which is composed of a large number of sensor nodes and base stations. Sensor nodes are responsible for collecting data measurments and communicating with base stations, they are small and have limited energy and memory. Wireless sensor networks need to acquire real-time and reliable data to make decisions. However, due to the deployment of harsh enviroment, the limited energy, there exist a series of data security problems.

At present, the research of wireless sensor network security is mainly divided into two parts. On the one hand, how to identify and remove malicious nodes in the network and ensure the robustness of the network is particularly important. Due to the unattended field environment, sensor nodes are easily compromised by attackers . Then, they may inject malicious nodes into the network to steal network data, destroy network communication and seize control of the network. Up util now, the schemes for mobile compromised node and replica compromised node attack in WSN are very mature, but few researchs on worm compromised nodes have been taken. Worm attacks can quickly infect sensor nodes and paralyze the network which have the greatest damage to the network. On the other hand, in order for the base station to make an accurate judgment, it is necessary for the sensor node to transmit reliable data. Therefore, it is necessary to detect and eliminate outliers caused by noise or internal errors of sensor nodes in the network. However, due to the limitation of computing resources and memory resources of sensor nodes, the related detection schemes cannot well meet the high detection rate and low false alarm rate of outlier detection.

In view of the above two points, this article has carried on the related research. Based on the SPRT worm detection model, the SPRT-Biased-Random worm detection scheme has been proposed combined with the random value sampling scheme and biased sampling scheme to detect worm nodes in network. Simulation results show that the schme can detect all worm nodes in 5 to 18 time slots and keep the infected nodes in the sensor network between 2% and 5%. For oulier detection in the network, based on PCA algorithm and Mahalanobis distance, an Improved Distributed PCA-Based Outlier Detection Method has been proposed, which improves the detection performance of the model and reduces the communication overhead in network. The experimental results show that the model can achieve an outlier detection rate of 96 % - 97 % and maintain an abnormal data false alarm rate of 2 %. At the same time, the scheme can track the source of outliers and enable network managers locate network problems quickly. In order to solve the problem that IDPCA scheme cannot be well applied to non-linear data measurements detection, this paper proposes an improved distributed kernel principal components analysis based on Mahalanobis kernel function, which can well detect non-linear ouliers by mapping the data measuments to high-dimensional space. The Mahalanobis distance is used to measure the distance from the data vector to the center, by leveraging the correlation among the measured data dimensions and a proper kernel parameter, about 98% outlier detection rate and 2% false alarm rate can be achieved by IDKPCA model.

Key words: worm compromised nodes detection, outlier detection, wireless sensor network, Sequential Probability Ration Test, Principal Components Analysis

目录

[目录 III](#_Toc535145100)

[第一章 绪论 1](#_Toc535145101)

[1.1 研究背景及意义 1](#_Toc535145102)

[1.2 国内外研究现状 2](#_Toc535145103)

[1.2.1 无线传感器网络恶意节点检测相关研究 2](#_Toc535145104)

[1.2.2 无线传感器网络异常数据检测相关研究 6](#_Toc535145105)

[1.3 研究内容及创新点 10](#_Toc535145106)

[第二章 无线传感器网络安全及相关算法概述 12](#_Toc535145107)

[2.1 无线传感器网络异常行为检测 12](#_Toc535145108)

[2.1.1 传感器网络中的恶意节点类型 12](#_Toc535145109)

[2.1.2 蠕虫传播模型 13](#_Toc535145110)

[2.1.3 序贯概率比检验 13](#_Toc535145111)

[2.2 静态无线传感器网络模型 14](#_Toc535145112)

[2.3 主成分分析与核主成分分析 15](#_Toc535145113)

[第三章 基于SPRT算法的恶意蠕虫节点检测方案 17](#_Toc535145114)

[3.1 引言 17](#_Toc535145115)

[3.2 网络拓扑结构和攻击者模型 18](#_Toc535145116)

[3.3 SPRT-Biased-Random蠕虫节点检测方案 19](#_Toc535145117)

[3.3.1 网络预处理阶段 20](#_Toc535145118)

[3.3.2 通信模式收集存储 20](#_Toc535145119)

[3.3.3 SPRT蠕虫检测 21](#_Toc535145120)

[3.4 安全性分析 24](#_Toc535145121)

[3.4.1 蠕虫节点检测率 25](#_Toc535145122)

[3.4.2 蠕虫节点感染的上限 27](#_Toc535145123)

[3.5 性能分析 28](#_Toc535145124)

[3.5.1 决策平均采样样本数 28](#_Toc535145125)

[3.5.2 通信资源开销和内存资源开销 30](#_Toc535145126)

[3.6 实验分析 31](#_Toc535145127)

[3.6.1仿真环境设定 31](#_Toc535145128)

[3.6.2仿真结果说明 32](#_Toc535145129)

[3.7 本章小结 34](#_Toc535145130)

[第四章 改进型分布式PCA异常数据检测方案 35](#_Toc535145131)

[4.1 引言 35](#_Toc535145132)

[4.2 网络拓扑结构假设 36](#_Toc535145133)

[4.3 IDPCA异常数据检测模型 37](#_Toc535145134)

[4.3.1 IDPCA异常数据检测模型训练 37](#_Toc535145135)

[4.3.2 IDPCA异常数据检测 39](#_Toc535145136)

[4.3.3 异常数据源检测 40](#_Toc535145137)

[4.3.4 模型更新 41](#_Toc535145138)

[4.4 性能分析 42](#_Toc535145139)

[4.4.1 通信资源开销 42](#_Toc535145140)

[4.4.2 计算资源开销 43](#_Toc535145141)

[4.4.3 性能仿真分析 44](#_Toc535145142)

[4.5 仿真分析 46](#_Toc535145143)

[4.5.1 仿真环境设定 46](#_Toc535145144)

[4.5.2 仿真结果分析 48](#_Toc535145145)

[4.6 本章小结 50](#_Toc535145146)

[第五章 基于马氏内核的分布式KPCA异常数据检测方案 51](#_Toc535145147)

[5.1 引言 51](#_Toc535145148)

[5.2 网络模型与马氏内核函数 51](#_Toc535145149)

[5.3 IDKPCA异常数据检测模型 53](#_Toc535145150)

[5.3.1 IDKPCA异常数据检测模型训练 53](#_Toc535145151)

[5.3.2 IDKPCA异常数据检测 55](#_Toc535145152)

[5.3.3 固定时间窗口模型更新 56](#_Toc535145153)

[5.4 性能分析 58](#_Toc535145154)

[5.5 仿真分析 59](#_Toc535145155)

[5.5.1 仿真环境设定 59](#_Toc535145156)

[5.5.2 仿真结果分析 60](#_Toc535145157)

[5.6 本章小结 62](#_Toc535145158)

[第六章 总结与展望 63](#_Toc535145159)

[6.1文章总结 63](#_Toc535145160)

[6.2未来工作展望 63](#_Toc535145161)

[参考文献 65](#_Toc535145162)

[附录1 攻读硕士学位期间撰写的论文与专利 70](#_Toc535145163)

[附录2 攻读硕士学位期间参加的科研项目 71](#_Toc535145164)

[附录3 IDPCA算法伪代码 72](#_Toc535145165)

[致谢 74](#_Toc535145166)

# 

# 绪论

* 1. 研究背景及意义

无线传感器网络(Wireless Sensor Network,WSN)因其能够部署在各种恶劣环境下完成任务，越来越受到专家和学者的关注。它们往往用于执行人类很难执行的任务，例如火山检测，生物危害检测和森林火灾防控等。除此之外，WSN还广泛运用于战场监视、边境监控、核攻击和化学攻击检测、入侵检测等场景[1]. 为了执行各种任务，需要在监测环境中部署基站和一组小型传感器设备。具体而言，传感器设备间形成自组织网络，相互协作以感测与分配的任务相关联的现象，然后将感测数据发送到基站[2]。监控者通过分析在基站收集的数据获得任务相关信息。为了帮助传感器节点高效地执行任务，研究人员提出了各种网络服务和通信协议。目前，已经为网络服务提出了节点定位、区域覆盖、数据压缩和聚合等协议。从物理层到传输层的各种网络协议也已经被提出用于传感器节点之间的通信。

然而，传感器网络通常以无人值守的方式部署，这些协议中的大多数都面临各种攻击，例如拒绝服务攻击、路由中断和虚假数据注入攻击、网络服务中断攻击[ 3、4、5 ]等。为了保护无线传感器网络免受各种攻击，许多学者给出了相应的解决方案。文献[ 4、6、7 ]提出了安全路由方案来减轻传感器网络中的路由中断攻击，文献[ 8、9]通过信任节点计算信任值来检测虚假数据注入攻击，文献[10]通过贝叶斯检验方案来预测虚假数据注入攻击。安全数据聚合协议[ 11、12、13、14、15 ]用于防止攻击者破坏传感器节点对数据的聚合。以上这些方案偏向于使无线传感器网络协议具有抵御攻击的能力，而不是消除攻击源。这些方案减轻了对网络服务和通信协议的威胁，但是需要大量的时间和精力来根据新类型攻击不断增强协议的健壮性。此外，由于很难预测新类型的攻击，协议只有在被新类型的攻击破坏后才能增强。因此，我们需要尽快发现和移除攻击源，以大幅降低采用攻击弹性方法所产生的成本和损失。各种攻击的主要来源来自被俘获的传感器节点，即攻击者可以利用无线传感器网络无人值守的特性来俘获传感器节点，从而对网络进行任何恶意活动。因此，无线传感器网络中的恶意节点监测和移除对于无线传感器网络的健壮性至关重要。

另一方面，WSN 在许多领域的应用通常需要高效、准确、实时的分析，以便于实时决策。准确的分析和决策主要依赖于传感器数据的质量，在监测过程中，传感应用会产生大量数据集，在处理大型数据集时，一个值得关注的问题是异常值问题[16]。在WSN中，异常值不可避免地会出现在几乎所有的数据集中，原因有两个:监控区域中的“罕见”事件以及由于WSN资源有限、软件或者硬件故障和恶劣的部署环境导致的感应错误。同时，在WSN中，环境条件可能会随着时间的推移而变化，因此，预定义的异常数据检测模型不一定能够对未知数据进行异常检测。因此，异常数据检测中的一个关键点是以可接受的检测精度动态检测异常值，同时将通信开销和能耗降至最低[17]。

在数据挖掘、数据库和统计等领域中，异常值检测问题已经被很好的解决了，在大型数据集中检测和消除异常值的技术也已经非常成熟。然而，这些解决方案并不适用于无线传感器网络。WSNs由大量小型自组织节点组成，CPU、带宽和能量资源有限。由于这些资源限制，来自其他领域的解决方案不能直接应用，因为它们可能会造成极高的通信损耗和计算损耗[18]。在WSN中，每个传感器节点拥有大数据集的一小部分，并与其邻居节点保持通信，以检测整个网络中的异常值。WSN中最耗费节点能量的行为是节点之间的通信，因此，我们研究的重点将放在尽可能的减少网络中的通信资源开销的同时，仍然能够高精度地检测异常数据并维持一个较低的异常数据误报率。

* 1. 国内外研究现状

1.2.1 无线传感器网络恶意节点检测相关研究

为了检测传感器网络中被捕获的恶意节点，文献[19][20][21][22][23]提出了多种检测方案。例如，文献[19][20]中提出了基于信誉值的信任管理方案，该方案的核心思想是根据单个节点的活动来管理其信任值，通过信任值来判读节点是否被俘获。虽然这些方案可以识别恶意节点，但是存在相当大的节点误报情况。事实上，所有基于信誉值的检测方案都存在误报率，当信任管理方案被重复应用于网络中的节点时，很大一部分良性的节点可能会被误认为是恶意节点，直接清除这些节点将带来非常昂贵的代价。

检测传感器网络中恶意节点的另一种方法是软件认证[21][23]。该方案的核心思想是：传感器节点通常会运行存储在闪存中的同一份可执行代码，通过验证在节点上运行的代码与预期的代码是否相同，可以检测被破坏的代码。这种方法几乎不存在误报，这意味着良性节点不会被无故地从网络中删除。然而，为了保证恶意节点的高检测能力，这些方案要求每个传感器节点都需要进行周期性的软件认证。因此，这种软件认证方案会给整个网络带来巨大的通信开销和计算开销。

为了克服上述两种方案的缺点并结合两种方式的优点，文献[24]结合软件认证方案提出了一种基于区域信誉值的信任管理方案。该方案的核心思想是将整个传感器网络分为不同的区域，然后对每一个区域设置信誉值，通过序贯概率比检测(Sequential Probability Ratio Test,SPRT)来检测非信任区域。最后，在这一部分区域运行软件认证方案，检测恶意节点并移除。通过这种区域性检测方案，能够快速定位非信任区域并运行软件认证方案，相比无条件的软件认证方案，该方案能够快速的检测网络中的异常节点并移除同时能够大大减小软件认证的节点数量，大量的减少网络的资源消耗。但是文献[24]提出的这种方案有一些极端情况，如果每个区域都存在不信任节点，也即每个区域都是不值得信任的区域，那么该情况下每个节点都需要进行软件认证，计算开销和通信开销也非常大。针对这种情况，文献[25]提出了仅仅基于非信任节点的软件认证方案，在保证恶意节点检测率的同时，大大降低了网络的计算资源消耗和通信资源消耗。

然而，基于区域信誉值的信任管理方案是针对静态恶意节点的，如果恶意节点在网络中处于移动状态，那么会造成大量恶意节点漏报。检测移动恶意节点的最简单方法是在网络部署前，在每个传感器节点中预分配其邻居节点列表，并让每个节点拒绝与其列表中未包含的节点通信。这能够防止移动恶意节点移动到其他区域与该区域内的节点通信。然而，这种方案需要网络管理者在部署阶段做更多的工作，因为网络的拓扑结构必须事先确定。此外，由于使用自动部署时总是存在部署错误，因此实际情况下每个节点的邻居节点很可能与预分配的邻居列表不同，导致许多良性节点与邻居节点通信失败，导致网络的大范围瘫痪。文献[26]表明，使用这种简单的方法会导致严重的网络连接问题。

文献[ 27、28、29、30]提出的位置区分方案能够有效检测移动恶意节点。在这些方案中，接收器基于接收信号强度( RSSI )或临时无线链路签名来识别无线网络中发送者的位置变化。然而，攻击者可以在移动过程中关闭节点的无线电，每次移动足够远的距离，以防止任何一个接收器监听到恶意节点从两个不同的位置发送数据包。文献[31]提出了一种分布式检测方案，通过利用SPRT算法来识别和移除移动恶意节点。该方案的核心思想是：静态传感器节点能够频繁的与邻居节点通信并建立邻居节点表，而移动恶意节点因为节点位置会实时变化并不会每次都和同一个节点进行通信，当节点发现其邻居表中有不与它通信的节点时，可以将该节点标记为可疑的移动恶意节点。该方案能够很好地解决传感器网络中的移动节点攻击。

文献[32][33]中通过椭圆曲线加密算法对网络之间传递的数据进行认证，防止恶意数据的注入，检测恶意节点。这种方案建立在公私钥加密算法的前提下，如果一个节点的密钥材料被攻击者获取，那么攻击者可以通过该节点进行任意合法的操作，该攻击称之为副本节点攻击。上述的方案能够很好的解决静态恶意节点和移动恶意节点的检测，然而针对大规模的副本节点攻击却无能为力。副本节点攻击是指攻击者从捕获的节点中获取节点的通信密钥材料和节点的ID，生成大量共享节点密钥材料和ID的攻击者控制的副本，然后将这些副本散布在整个网络中。通过捕获单个节点，攻击者可以创建尽可能多的副本节点。将这些副本节点注入网络所需的时间和精力要比捕获和破坏同等数量的原始节点所需的时间和精力少得多。副本节点由攻击者控制，但有密钥材料，使它们看起来像网络中的授权参与者。用于安全传感器网络通信的协议将允许副本节点与其他节点和基站创建成对的共享密钥，从而使节点能够加密、解密和认证其所有通信，它们就像是原始捕获的节点一样。

通过副本节点攻击，攻击者可以轻松地监控通过这些节点的大部分网络流量或者轻易地干扰良性节点的有效信号，注入伪造的数据来破坏传感器的监控操作。更具攻击性的攻击者可能会破坏常见的网络协议，包括集群形成、本地化和数据聚合，从而导致网络操作的持续中断。通过这些方法，拥有大量副本节点的对手可以轻松击败部署网络的主要任务。

检测副本节点攻击的一个直接解决方案是通过为移动节点配备防篡改硬件来防止对手从移动节点中提取秘密密钥材料。然而，尽管防篡改硬件会使从捕获的节点中提取密钥材料变得更加困难和耗时，但如果有足够的时间和充分的专业知识，攻击者仍有可能在少数节点中绕过防篡改。由于攻击者可以从单个捕获的节点生成许多副本，这意味着副本攻击相对于其他类型的恶意节点来说更加危险，因此基于软件的方案来保护移动传感器网络免受副本节点攻击非常重要。文献[34][35]针对静态传感器网络提出了几种基于软件的副本节点检测方案。这些方案使用的主要方法是让节点报告位置声明，以识别它们的位置。如果同一个ID的节点发送的位置报告中显示它们的位置不一致，那么判断该节点为一个副本节点。整个网络对该节点进行通信限制，移除副本节点。在静态网络中，该方案能够高效快速地检测副本节点，但是由于这种方法需要固定的节点位置，因此当节点需要移动时，就不能使用它。因此，对于移动传感器网络该检测方案并不适用。

针对该缺陷，文献[36]提出了一种基于SPRT的副本节点攻击检测方案来检测移动传感器网络中的副本节点攻击。该方案的核心思想认为一个良性移动节点的移动速度永远不应该超过系统配置的最大速度。因此，只要我们采用误差率低的速度测量系统，良性移动传感器节点的测量速度至多是系统配置的最大速度。然而，副本节点的移动速度会比良性节点快得多，因为它们需要同时位于两个(或更多)不同的位置，因此它们的测量速度可能会远远超过系统配置的最大速度。所以，如果我们观察到移动节点的测量速度超过系统配置的最大速度，那么网络中很有可能存在至少两个具有相同身份的节点，即该节点很有可能就是副本节点。通过该特性结合SPRT检验，该方案能够快速并准确的检测移动网络中的副本节点攻击。

然而，通过物理捕获大量传感器节点需要花费很多时间和精力，并且可能会使攻击者面临被发现的风险。对于攻击者来说，一个更好的选择是只捕获和破坏几个节点，然后使用自传播恶意代码(即蠕虫)来感染网络中的其他节点。通过简单地将受感染的节点重新引入网络，蠕虫会迅速传播并感染大量传感器节点，让攻击者获取整个网络的控制权。

尽管无线传感器网络中蠕虫节点的检测和预防十分重要，但是相关方面的研究却很少。由于传感器网络缺乏相应的硬件资源设施，已有的互联网蠕虫检测和预防方案[37][38][39][40]并不能直接应用于传感器网络。文献[37]和[39]中的签名检测算法通过对传感器节点发送的包进行签名认证，识别网络中的恶意蠕虫代码。该方案需要大量的计算开销来生成和维护签名，这不适用于资源受限的传感器网络。文献[38]中介绍了互联网中蠕虫检测的常见方案，这些方案中结合了贝叶斯网络模型、神经网络模型来做蠕虫识别，需要大量的计算资源开销并不适用于无线传感器网络。杨等人提出了基于软件多样性技术的方案来防止蠕虫传播[41]，该方案的核心思想是将整个网络分成一系列的网格单元，然后在每一个节点中分配不同的闪存程序，这样的话，邻居节点之间的闪存程序也不一样。当攻击者通过某个闪存程序的漏洞捕获某个节点之后，由于节点之间使用的是不一样的闪存程序，那么很大概率的情况下，蠕虫将无法进行传播。上述机制能够工作的前提条件是，每个节点的闪存程序漏洞是不一样的，否则无法阻止蠕虫节点的传播。文献[42]扩展了文献[41]中的思路，能够以较小的计算开销阻止相邻两个节点之间的蠕虫传播，进而阻断整个网络的蠕虫传播。然而，实际上很难做到使闪存程序的不同版本具有不同的漏洞，如果我们能够发现闪存程序的漏洞就可以主动修复它们，而不需要再等待蠕虫节点来感染。另一方面，如果在两个或更多版本的代码中发现不同的漏洞，蠕虫代码可以利用所有漏洞进行编程。这种蠕虫可以首先感染一个节点，然后切换漏洞，感染相邻的一个节点，从而在网络中传播。文献[ 43 ]研究了当节点的活动状态周期由随机节点调度确定时，使用软件多样性技术对传感器节点预防蠕虫感染的影响。文献[ 44 ]提出了一种软件多样性技术结合基于角色的图像着色方案来检测蠕虫节点。因为这些方案都是基于软件多样性技术的，所以它们的缺陷也和文献[41][42]所提出的相同。如果蠕虫传播不容易被中断，那么可以通过检测蠕虫节点然后移除来保证传感器网络的安全。文献[45],[46],[47],[48],[49]引入了远程软件认证方案有效的检测蠕虫节点。远程软件认证方案的核心思想是在软件或者硬件的基础上证明节点程序的完整性，由于任何节点都可以针对其他节点进行软件认证，并且无需使用专用硬件即可检测出受损节点，因此远程软件认证方案在资源受限的传感器网络中检测蠕虫节点有很大的优势[49]。但是，如果周期性地使用软件认证方法来检测传感器网络中的恶意节点，那么会给网络带来大量的通信资源开销。文献[50]中提出了一种适用于无线传感器网络的软件认证方案，其主要思想是让每一个节点在每一个时隙中随机选择一组节点来进行认证，当该节点收到这组节点发送的数据包时，对它们进行远程认证，从而检测被蠕虫感染的节点。尽管这种方法能够在一定程度上检测网络中的蠕虫节点，但是由于无法检测未包含在随机选择的集合中的感染节点导致检测能力下降。因此，寻找一种高效的蠕虫节点检测方案检测并剔除恶意蠕虫节点至关重要。

1.2.2 无线传感器网络异常数据检测相关研究

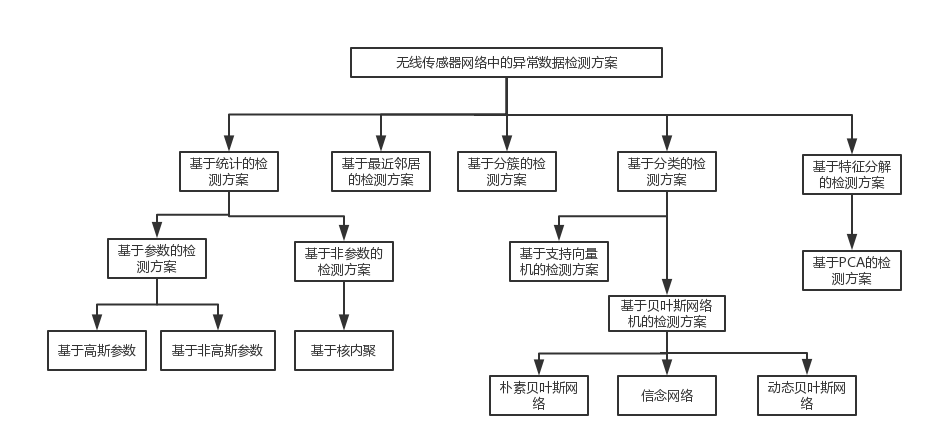
在无线传感器网络中，异常数据定义为与正常的监测数据模式差别较大的数据[51]。低成本和低质量的传感器节点具有严格的资源限制，例如能量(电池功率)、内存、计算能力和通信带宽。有限的资源使得传感器节点产生的数据不够可靠和准确，特别是当电池电量耗尽时，产生错误数据的概率将迅速增长[ 52 ]。另一方面，传感器节点易受环境影响,大规模高密度无线传感器节点部署在恶劣的环境下(多达数百甚至数千个节点)，在这种环境中一些传感器节点不可避免地会出现故障，这可能会导致噪声、故障、丢失和冗余数据。此外，传感器节点容易受到恶意攻击，如拒绝服务攻击、黑洞攻击和窃听[53]等，在这些攻击中，传感器监测的数据将被攻击者操纵或者窃取，导致网络数据的泄露或者大规模失真。

无线传感器网络已经广泛运用于各种生活场景，例如农业灌溉，医疗手术，森林火灾防控等。这些场景需要根据监测的数据来进行实时的状态分析，因此要求传感器网络传递的数据值足够可靠。为了保证基站接收数据的可靠性，必须对无线传感器网络中的异常数据进行剔除。检测异常数据最简单的方法就是对正常的监测数据集进行建模，然后将模型应用于新的监测数据，如果新到达的监测数据和所建模型的偏差超过一定的阈值，那么可以将该测量数据定义为异常数据进行丢弃。目前，已经有相当多的学者针对无线传感器网络中异常数据检测提出了解决方案，但是受限于传感器节点的资源限制，很多研究结果并不能在资源和检测效率上得到折衷的效果。另一方面，如何根据异常数据来追踪引起异常数据发生的原因这一问题亟待解决。本文旨在寻找一种有效的方案使得传感器网络在满足指定的异常检测率下，尽可能少地降低传感器节点消耗的资源，并对引起传感器节点数据异常的原因进行分析、溯源。

**A 异常数据检测的相关研究**

异常数据检测方案主要分为两种类型：集中式异常数据检测方案和分布式异常数据检测方案。在集中式异常数据检测方案中，各个节点将数据发送到基站统一处理，由基站进行数据的异常检测和剔除。这种方案会给整个网络带来巨大的通信开销，同时网络的故障率会大大提高，一旦基站因为数据处理崩溃或者直接被攻击者攻击，那么整个网络将崩溃。分布式异常数据检测方案中，数据的检测由各个节点自身完成，这种方案的优点是每个节点都能参与检测，网络的容错率高，能够大大降低节点之间的通信损耗。但是这种方案的缺点也很明显，每个节点单独运行检测算法会给节点的计算资源和内存资源带来消耗，加速传感器节点的能量耗尽，但是正常情况下，节点之间的通信能耗要远远大于计算能耗，所以主流的研究方向偏向于分布式检测方案。

根据是否需要标签训练样本，检测算法分为监督算法，半监督算法和无监督算法。监督算法和半监督算法训练模型的时候需要将训练数据按照标签分为正常数据和异常数据，而无监督算法不需要对数据进行分配标签，通过给定数据进行模型训练。在现实场景中要获取标签数据是相对困难的，会增加额外的工作量。文献[18]详细地归纳了机器学习算法在传感器网络异常数据检测中的运用，图1.1给出了传感器网络中异常数据检测方案的大致研究成果。



**图 1.1 无线传感器网络异常数据检测方案综述**

基于数据统计的异常检测方案是最早被提出来用于处理异常数据检测问题的方案。该类检测方案的核心是根据已知数据进行统计建模，生成一个概率模型表征数据的产生规律，如果一个数据值在该模型下的生成概率特别小，那么将该数据归为异常数据，否则归为正常数据，这是一类无监督的检测算法。文献[54]提出了一种基于高斯分布的概率统计模型来检测异常数据，该检测模型并没有利用节点数据的时域相关性因而异常数据的检测率较低。文献[55]提出了一种基于核函数的概率密度统计模型，该模型能够很好地检测高维异常数据，然而这种方法需要定义一个合适的门限值作为异常数据值的区分标准，找到该门限值非常难。如果能够建立合适的概率模型表征数据的生成规律，那么基于统计模型的检测方案能够很好地检测出异常数据。然而现实场景下，数据的统计分布模型是很难预估的，这是该方案最大的缺点。

基于最近邻居的方法是数据挖掘和机器学习社区中最常用的分析数据实例的方法。该方案使用明确的距离概念来计算两个数据实例之间的相似度。具体方案是通过计算当前节点的数据向量同邻居节点的数据向量的距离来判断当前节点数据是否为异常值，对于单个变量通常使用欧式距离描述，对于多元变量通常使用马氏距离来描述。文献[56][57]中详细介绍了最近邻居方案，文献[58][59]使用最近邻居检测方案来检测异常数据，但是给网络带来了比较大的通信开销和计算开销。对于多元数据而言，反复计算节点数据之间的相似度是一个计算量比较大的工作，同时如何确定相似度的阈值也是一个复杂的工作，因此最近邻居检测方案在WSN中并不常用。

基于聚类的方法是数据挖掘领域中用于将相似的数据实例分为同一个分组的常见方案。如果某个数据实例不属于某个分组，或者某个分组的大小明显小于其他分组，则它们被认定为异常数据值，通常使用欧式距离来衡量某个数据向量到中心向量的距离。文献[60]中使用k均值聚类的方法将训练数据集分成k类，对监测数据进行异常检测。该方案下异常数据的检测率是变化的，随着k值和每个组的组距变化，性能也大不相同，如何选取k值和分组组距使得检测模型的性能达到最佳非常困难，需要耗费大量的计算资源。

基于分类的异常检测方法是数据挖掘和机器学习领域中重要的学习算法。通过使用一组数据实例训练分类模型(训练)，并将一个未知实例分类到一个学习过的(正常/异常)类别中。无监督的分类算法不需要标签数据进行训练，一类非监督学习算法通过寻找正常值和异常值的边界来进行异常数据的检测。目前主流的分类算法主要包括两种类型：基于支持向量机( SVM )和基于贝叶斯网络的分类方法。文献[61,62,63,64]中通过SVM算法去计算正常数据和异常数据的分界面（超平面或者超曲面，超椭圆面）进行数据的检测，这种方案的计算复杂度过高，而且需要选取合适的内核函数进行高维空间映射，实现比较复杂。不仅如此，这些文献中提出的DQSSVM,CQSSVM,EOOD,EAOD方案只有在各自特定的数据类型下才能保持高效地检测，例如QSSVM方案适用于按照球面分布的数据的检测，而EOOD方案适用于数据类型是椭球形分布的数据检测。文献[65,66]中通过训练数据集来得到贝叶斯分类器，对数据进行检测。通过分类器能够很好地检测异常数据，但是训练合适的贝叶斯分类器需要大量的数据向量和计算资源开销。

以上的方案中仅仅考虑了传感器节点之间的空间相关性和节点内部数据的时域相关性，并没有考虑数据向量之间的维度相关性，这导致了多余的计算复杂度并且在一定程度上降低了异常数据检测效率。同时以上这些方案并没有考虑到数据维度较大的情形，这在分布式检测方案中会引入巨大的通信资源开销。最后，以上这些方案并没有很好地利用传感器节点的空间相关性来解决异常数据源的分析。

主成分分析（Principal Component Analysis,PCA）是数据降维的重要方法，广泛地运用于模式识别的领域。该方法的核心思想是找到一个变换使得坐标系旋转能够将数据的主要信息集中在少数几个维度上。基于PCA的异常检测模型不仅能够很好地处理低维数据向量而且也非常适用于高维的数据向量。文献[68]中介绍了PCA算法在无线传感器网络中异常节点检测和异常数据检测中的运用，实验结果表明基于PCA算法的异常数据检测方案能够很好地检测异常数据，但是该方案基于基站来建立模型属于集中式检测方案，会给网络带来巨大的通信开销，我们将该方案称之为CPCA方案。文献[69]中提出了一种基于固定组距的分布式PCA异常数据检测方案(DPCA)，该方案下每个传感器节点通过训练数据集进行QR分解将R矩阵发送给簇头节点计算全局的主成分值并计算判决门限值发送给各个节点。该方案的异常数据检测效率能够达到94%以上，但是网络中的通信资源消耗依然很大。文献[70]在计算完主成分分量之后并不使用欧式距离来计算判决门限值而是使用自定义的非相似度来判定异常数据，该方案的异常数据检测率能够达到90%以上，但是如何获取最佳门限值是限制该方案的主要因素。基于PCA算法的检测模型在处理线性可分的数据时性能非常好，但是在非线性可分数据模型下往往不能找到最佳的映射坐标轴来反映原数据的特征，因此引入了基于核函数的主成分分析法(Kernel Principle Components Annlysis,KPCA)将数据映射到高维空间中寻找最佳的映射坐标达到最好的检测效果。文献[71][72]说明了KPCA检测方案在非线性系统中能够达到非常好的检测效果。文献[73]对KPCA方法进行了详细地描述，文献[74][75]给出KPCA方案在传感器网络中的应用并提出了集中式KPCA检测方案，能够有效地检测网络中的异常数据，但是引入了大量的通信开销。

**B 异常数据源检测的相关研究**

由于无线传感器网络的资源限制和部署环境复杂，很难确定是什么导致了异常数据的产生。传统的异常数据检测方案并不区分异常数据产生的原因，这往往会导致网络的管理者无法获悉一些恶意事件的发生。传感器网络的异常数据主要由4个原因引起(1)部署环境中的噪声影响(2) 传感器节点内部发生错误，比如节点的能量不足或者节点损坏(3)恶意事件发生(4)传感器节点的恶意攻击[76]。环境噪声对数据的影响是随机的，这意味着一个传感器节点检测到的数据是一个非连续的异常数据值，那么它有可能是一个噪声引起的。如果某个传感器节点从某个时隙开始侦测的数据一直都是异常值，那么它有可能是节点内部异常引起的。如果一个组中的节点在连续的时隙内，节点产生的数据都是异常数据，那么有可能是网络中出现了恶意事件。文献[53]中提出了一种OPTICS的异常数据检测方案能够有效地区分异常数据源为恶意事件或者非恶意事件，但是不能确定非恶意事件发生的具体原因。文献[52]提出了一种ODS方案能够有效地检测恶意事件和恶意攻击，但是不能识别由节点损坏或者噪声引起的异常。综上所述，异常数据源的追溯至关重要。但是相关的研究却不能很好地区分引起异常数据产生的原因，本文提出的IDPCA方案能够很好地解决该问题。

* 1. 研究内容及创新点

本文针对无线传感器网络中的恶意节点检测和异常数据检测提出了新的解决方案，论文的主要工作如下：

1. 以往的无线传感器网络恶意节点检测方案中并没有很好地解决蠕虫节点感染问题。本文利用蠕虫节点传播的特性，以SPRT蠕虫检测模型为基础，结合偏向采样方案加速蠕虫节点的检测。同时为了更好地解决蠕虫节点的慢传播问题，结合随机值采样方案，提出了SPRT-Biased-Random蠕虫检测方案。方案能够在5~18个时隙内检测到蠕虫节点，并使得传感器网络最终受感染的节点维持在2%~5%之间。
2. 在PCA算法的基础上提出了一种改进型分布式PCA异常数据检测模型(Improved Distributed PCA-Based OutlierDetection Method, IDPCA)。通过充分利用传感器节点间监测数据的空间相关性和节点内数据的时域相关性我们提出双重检测机制（本地检测和全局检测）进行异常数据的检测和异常数据溯源。该模型充分考虑了数据维度之间的相关性，利用马氏距离来衡量数据间的相似度。对于网络中的异常数据检测率能够达到96%-97%并且整个网络的通信资源相对以往的分布式检测方案要小，同时能够很好地识别异常数据发生的原因。
3. 在IDPCA异常数据检测模型的基础上提出了一种基于马氏内核函数的主成分异常数据检测模型(Improved Distributed Kernel Principal Components Analysis,IDKPCA)，该方案能够很好地处理线性不可分的数据集。通过马氏内核函数将线性不可分的监测数据集一一映射，该模型能够很好的将数据在高维空间中进行区分。为了克服IDPCA异常数据检测模型中频繁地数据模型更新，引入艾宾浩斯遗忘曲线来实现固定窗口模型更新。实验表明IDKPCA异常数据检测模型能够达到近乎98%的异常数据检测率和2%的数据误报率，同时该模型下网络中的通信资源消耗趋近于常量级别，有利于延长整个传感器网络的寿命。

本文组织结构

本文由六个章节组成，各个章节的主要内容如下：

第一章介绍了研究背景和意义，简述了国内外对无线传感器网络中的恶意节点检测和异常数据检测的的各种方法，重点对蠕虫节点检测和异常数据检测技术进行了分析介绍。同时简单介绍了一下本文的研究方法和研究内容。

第二章我们针对本文用到的一些基础算法和网络的模型结构给出了详细的说明，如节点的预分配方案，SPRT检测算法，蠕虫模型等。

第三章我们研究了无线传感器网络中针对恶意蠕虫节点的检测方案，我们详细地阐述了SPRT-Biased-Random检测方案。该方案能够快速的检测网络中的蠕虫节点位置，并通过软件认证方案快速的将蠕虫节点移除，能够使得网络受到的影响最小。

第四章我们研究了无线传感器网络中异常数据的检测方案以及异常数据溯源。如何在合理利用传感器网络能量的同时，对网络中的异常数据和恶意事件进行准确的侦测，我们以主成分分析法为基础提出IDPCA异常数据检测方案，能够在较小的通信资源开销下，准确的侦测传感器网络中的异常数据和寻找异常数据源。

第五章对第四章中PCA算法无法很好地处理线性不可分的数据这一缺陷做出弥补，提出基于马氏内核函数的分布式主成分异常数据检测模型IDKPCA，能够很好地对线性数据和非线性数据进行异常数据的检测。同时引入了固定窗口模型更新策略，减小模型的更新频率，降低节点的计算资源消耗。

第六章对整篇文章的工作进行了概述和总结，针对文章中方案的不足之处提出了未来的研究方向。

# 无线传感器网络安全及相关算法概述

无线传感器网络已经广泛运用于各种生活场景，例如农业灌溉，医疗手术，森林火灾防控等[59]。这些场景需要根据监测的数据来进行实时的状态分析，因此要求传感器网络传递的数据值足够可靠。然而无线传感器网络部署在无人监控的野外，传感器节点很容易被攻击者捕获，攻击者通过捕获节点仿造数据值达到欺骗基站的目的，同时传感器节点能量有限，网络发送数据时极易受到环境中噪声的影响，造成数据的失真。无线传感器网络中的安全问题主要分为两种类型，第一种为传感器节点的异常行为检测即传感器节点遭受攻击，第二种类型为传感器节点异常数据的检测。本章节讨论传感器网络安全的两种情形并讨论文章中使用的一些算法。

* 1. 无线传感器网络异常行为检测

无线传感器网络因其部署在无人监控的野外环境中而极易受到攻击者的攻击，通过捕获传感器节点在网络中注入恶意数据，感染整个网络。攻击者侵入无线传感器网络的最直接方式是通过物理捕获节点，提取节点的密钥信息，将密钥信息复制到恶意节点中，让其在网络中冒充为良性节点，之后通过恶意节点发动一系列攻击，感染整个网络。恶意节点可以监听流经该节点的信息，也可以向其他节点传播恶意的数据，最糟糕的情况下，恶意节点会破坏其他传感器节点的聚簇算法，路由算法和数据聚合算法等，使整个网络崩溃。

2.1.1 传感器网络中的恶意节点类型

攻击者在捕获传感器节点之后为了能够尽量多的感染其余节点，避免自己被检测，会让恶意节点在网络中移动，这就是所谓的移动节点攻击。这种攻击可以通过事先在节点中预置邻居节点的方式来检测[36]。攻击者通过物理捕获节点之后，通过某些方法获取传感器节点的id和通信密钥，然后注入相同id和密钥的恶意节点到网络中进行攻击，这种方式为复制节点攻击方式，文献[26]针对复制节点攻击进行了分析。为了尽量多的感染整个传感器网络，复制节点会选择在网络间移动，这种攻击方式称为移动复制节点攻击，文献[34]对该种攻击方式进行了分析，并提出了相应的检测方案。然而，通过大量的去捕获真实环境中的传感器节点需要花费很高的代价，最有效的方式是通过捕获少量的节点，通过节点传播蠕虫病毒去控制整个网络的节点，这种方式即为恶意蠕虫节点。

2.1.2 蠕虫传播模型

流行病传播模型能够很好地预估网络中受感染节点的数量和感染率，被广泛的运用于互联网蠕虫传播建模中，本文也同样采用该模型来模拟传感器网络中的蠕虫传播。在文献[36]中给出了离散时间下的简单流行病传播模型(在不同时隙下，而非连续时间),式2-1给出了该模型下的蠕虫感染率：

|  |  |
| --- | --- |
|  | (2-1) |

蠕虫病毒的感染数量随时间的变化关系如式2-2所示，其中时间t是以每一个时隙为单位。

|  |  |
| --- | --- |
|  | (2-2) |

代表时刻网络中受感染的节点数量，代表网络中的总节点数量，代表传感器节点彼此之间的感染率[36], 代表初始的蠕虫节点的数量，第个时隙中受感染的节点为。

2.1.3 序贯概率比检验

序贯概率比检验(Sequential Probability Ration Test,SPRT)是一种统计决策方案[76],该方案也被称作序列化假设检验。该方案和其他假设检验模型的区别在于序贯概率比检验的采样数在检验前是不固定的，它根据检验的结果动态增加采样样本数，换句话说在SPRT算法中采样的样本数目是随机的。这一特点使得SPRT检测算法能够在满足给定的误报率和漏报率的条件下更快的结束检测。文献[6,7]中将SPRT检测算法描述成具有上限值和下限值的一维随机游走策略，在该策略开始时先定义空假设对应下限值，定义选择性假设对应上限值。SPRT算法在上下限区间的某个值开始逐渐向上限值或者下限值靠拢，如果新到达的样本值使得SPRT计算的值低于下限值那么SPRT结束检验，接受空假设。如果新到达的样本值使得SPRT计算的值大于上限值，那么SPRT结束检验接受选择性假设。否则，需要再增加一个样本值进行检验。

我们以故障半导体设备检验为例，详细阐述SPRT检测方案，在该情形中我们认为故障机器产生故障半导体的概率要远远大于非故障机器产生故障半导体的概率。令为设备生成的第个半导体，即为SPRT算法中的一个样本，令为随机伯努利变量，定义为：



伯努利分布为1的概率定义为：。如果小于一个预定义的门限值，那么该设备很有可能不是一个故障设备，反之，如果那么该设备很有可能是一个故障设备。判断半导体设备是否为故障设备的问题可以归结为和的假设检验问题，然而假设检验的结果有可能出错，我们需要指定能够承受的最大容错率。因此将上面的假设检验模型修改为时接受空假设，当时接受选择性假设。当时如果我们接受选择性假设那么定义为误报，当时我们接受空假设那么定义为漏报。我们通过自定义配置最大容错的误报率为，最大容错的漏报率为。

为了进一步理解SPRT算法如何检测，我们演示设备如何通过个采样样本进行决策。我们首先假设设备没有故障为空假设，假设设备有故障为选择性假设。定义为个采样样本下的对数概率比，定义如式2-3所示：

|  |  |
| --- | --- |
|  | (2-3) |

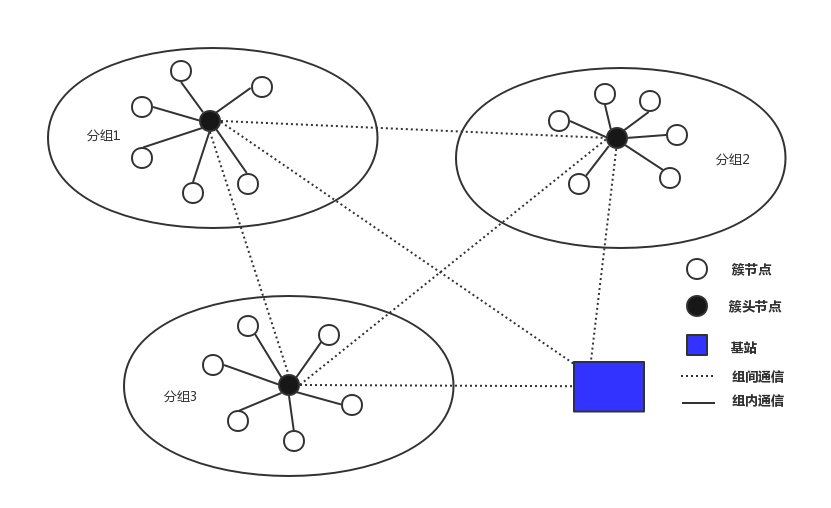
根据对数概率比，SPRT检测算法接受假设和假设的规则如下：



* 1. 静态无线传感器网络模型

本小节我们将介绍静态传感器网络的分簇结构和位置分布函数。

我们提出的方案利用了传感器网络的分簇结构[77],该结构示意图如图2.2所示。如该图所示，每一个集群拥有一个集群头和若干个邻居节点，集群头能够和邻居节点间通信也能和其余的集群头节点(包括基站)进行数据通信，基站监控和管理着整个传感器网络。传感器节点的异常数据检测需要经过双层节点检测即节点本身的局部检测和集群头的全局检测，通过集群头节点来寻找异常数据发生的原因，如果节点遭受了恶意攻击或者监控区域发生了恶意事件，那么集群头向基站发出警报，基站做出相应的处理。除此之外，集群头节点还能够进行数据聚合，重复数据剔除，节省与基站间的通信带宽。



**图2.2 网络的分簇结构**

我们将传感器节点按照分组进行部署，采用的分组策略是将节点按照二维高斯分布分散在区域中，所满足的二维高斯分布密度函数满足式2-4。其中是每个传感器分组的组头节点，为标准差。

|  |  |
| --- | --- |
|  | (2-4) |

2.3 主成分分析与核主成分分析

主成分分析（Principal Component Analysis,PCA）是降维的重要方法，该方法的核心思想是找到一个变换使得坐标系旋转能够将数据的主要信息集中在少数几个维度上。每一个主成分都是数据在某一个方向上的投影，在不同的方向上这些数据方差的大小由其特征值决定。一般我们会选取最大的几个特征值所在的特征向量，这些方向上的信息丰富，能够包含数据向量的绝大部分信息。由[78]我们可知求解最大主成分分量即求解最优化问题：，其中为向量间的协方差矩阵，通过拉格朗日乘数法有：

|  |  |
| --- | --- |
|  | (2-5) |

上式对求导有：

|  |  |
| --- | --- |
|  | (2-6) |

所以求解主成分分量相当于求解，从而得到的特征值对角阵和对应特征向量也即新的投影坐标方向。假设我们的训练样本是，每个样本值是维向量，那么训练样本的协方差矩阵为式2-7所示，我们需要求解该矩阵的特征向量矩阵。

|  |  |
| --- | --- |
|  | (2-7) |

在核主成分分析(Kernel PrincipalComponents Analysis,KPCA)方法中，认为原有数据有更高的维数，可以在更高维的空间（Hilbert Space）中做PCA分析（即在更高维空间里，把原始数据向不同的方向投影）这样做的优点在于：对于在通常线性空间难于线性分类的数据点，我们有可能再更高维度上找到合适的高维线性分类平面。方案的核心还是求解协方差矩阵的特征值和特征向量，但是协方差矩阵是高维空间下的协方差矩阵，具体可参考文献[78].

|  |  |
| --- | --- |
|  | (2-8) |

# 基于SPRT算法的恶意蠕虫节点检测方案

* 1. 引言

在WSN中，攻击者可以很容易的通过物理手段来俘获传感器节点，然后通过俘获的节点发动各种攻击。然而寻找和俘获大量的传感器节点需要大量的时间和精力，同时会让攻击者很容易暴露。因此，对于攻击者而言，更好的选择是仅仅俘获几个节点，并向这些节点注入自我传播的恶意代码（即蠕虫）来感染这些节点。通过简单的方式，将受感染的节点重新引入网络，蠕虫可以在网络中迅速传播，感染网络中绝大部分的良性节点，让攻击者获取网络的控制权。

蠕虫病毒传播是传感器网络安全的一个主要问题。正如我们在互联网中看到的那样，蠕虫可以迅速传播并且造成巨大的破坏。在传感器网络中，攻击者只需要捕获几个传感器节点就能进行大范围的蠕虫攻击，因此蠕虫节点应该尽快的被检测出来并剔除以减小对网络的最大伤害。尽管防止和检测蠕虫传播攻击对于阻止传感器网络中的节点被大量俘获至关重要，但是相关方面的研究却很少。杨等人提出了基于软件多样性技术的方案来防止蠕虫传播[41].大多数传感器节点在闪存中运行它们的主要软件程序，称之为闪存程序。杨等人提出的方案的核心思想是将整个网络分成一系列的网格单元，然后在每一个节点中分配不同的闪存程序，这样的话，邻居节点之间的闪存程序也不一样。当攻击者通过某个闪存程序的漏洞捕获某个节点之后，由于节点之间使用的是不一样的闪存程序，那么很大概率的情况下，蠕虫将无法进行传播。上述机制能够工作的前提条件是，每个节点的闪存程序的漏洞是不一样的，否则无法阻止蠕虫节点的传播。如果蠕虫传播不容易被中断，可以通过检测蠕虫节点然后移除，保证传感器网络的健壮性。文献[45],[46],[47],[48],[49]引入了远程软件认证方案有效的检测蠕虫节点。远程软件认证方案的核心思想是在软件或者硬件的基础上证明节点程序的完整性，由于任何节点都可以针对其他节点进行软件认证，并且无需使用专用硬件即可检测出受损节点，因此远程软件认证方案在资源受限的传感器网络中检测蠕虫节点有很大的优势。文献[50]中提出了一种适用于无线传感器网络的软件认证方案，其主要思想是让每一个节点在每一个时隙中随机选择一组节点来进行认证，当该节点收到这组节点发送的数据包时，对它们进行远程认证，从而检测被蠕虫感染的节点。尽管这种方法能够在一定程度上检测网络中的蠕虫节点，但是由于无法检测未包含在随机选择的集合中的感染节点导致检测能力下降。

为了解决以上方案中的缺陷，我们提出了一种基于序列概率比检验(Sequential Probability Ratio Test, SPRT)的蠕虫传播检测方案SPRT-Biased-Random，该方案结合随机采样策略和偏向采样策略，能够大大的提高蠕虫节点的检测效率。该方案基于以下事实：蠕虫节点以逐跳方式传播，会产生一条链式的通信链路, 因此当一个蠕虫节点传播时我们可以观测到一条“蠕虫链”慢慢增长，该链路连接了传感器网路中的多个节点。相较而言，良性节点之间的通信模式偏向于多对一的通信模式，多个数据源节点向一个数据聚合器发送数据，在这种模式下很难观测到“链式”通信模式，因此在正常的网络通信模式中我们会很难发现包重传现象。基于以上的理论，SPRT检测方案以网络中是否有包重传现象作为采样样本，根据样本类型动态地配置最低阈值和最高阈值。我们定义空假设为蠕虫没有在网络中传播，选择性假设为蠕虫在网络中传播，当SPRT检测到当前的网络中“包重传”数量低于最低阈值时，接受空假设。当“包重传”现象数量高于最高阈值时，接受选择性假设。本章采用偏向采样方案，加速了蠕虫检测传播的速度，减少了网络中受感染的节点数量。同时我们采用一种随机采样方案，有效地提高了慢蠕虫的检测率。

本章提出的SPRT-Biased-Random蠕虫传播检测方案的优势在于能够快速地检测出网络中的蠕虫节点，该方案相对于其他方案更加健壮可靠，对基本上的蠕虫类型都有效，因为该方案的核心思想是针对包重传这一个现象进行分析的。通过理论分析和仿真实验对所提出的方案进行评估表明该方案能够高效地检测传感器网络中的蠕虫节点，极大地限制攻击者。实验结果表明，我们所提出的方案至多需要5个采样值就能侦测出蠕虫节点，同时能够限制网络中被蠕虫感染的节点在2%-5%之间。本章的随后部分主要包括模型的假设，模型的具体描述，模型的分析和仿真。

* 1. 网络拓扑结构和攻击者模型

在本小节，我们提出了本方案下无线传感器网络的拓扑结构和攻击者模型。

A 网络拓扑结构

假设传感器网络是静态网络，其中的传感器节点在部署完成之后位置不会再发生改变。同时节点之间是双向链路，能够彼此通信，彼此监听。一个传感器节点要被蠕虫感染，需要接收多个数据包。在当前的传感器网络结构中，最大的网络分组包的大小为28比特，因此想要注入一个恶意的代码，一个分组包的数据量是远远不够的[79]。根据文献[79]中的实验结果，一个自传播的恶意蠕虫代码至少需要1024比特大小，当蠕虫代码在网络中传播时需要大约50-100的分组来传送数据包。

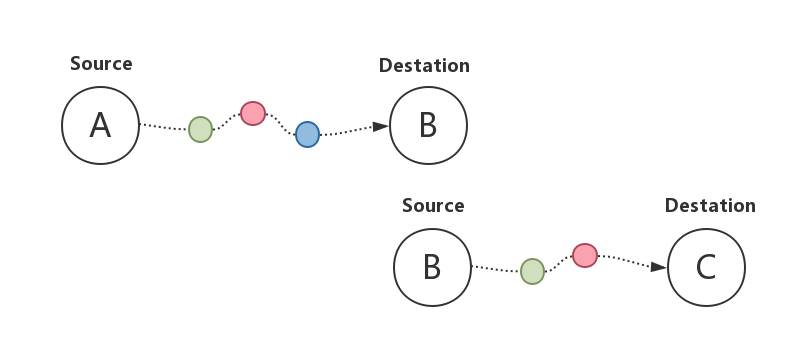
B 攻击者模型

假设攻击者能够捕获传感器网络中的一些传感器节点，同时将这些节点设置为蠕虫病毒的发起者在网络中传播蠕虫。通过这种方式，在不被检测到的情况下尽可能多的控制网络中的节点。本文中，我们假设一个传感器节点只有两种状态:易感染和已感染。所有传感器节点最初都处于易感染状态，除了已感染的蠕虫发起者。一旦易感染节点被蠕虫病毒感染，它的状态就会变成已感染。我们不仅要模拟蠕虫节点传播的速度，同时还要模拟蠕虫如何通过网络传播。我们假设攻击者采用逐跳传播策略，每个感染节点将蠕虫传播到其相邻的易感节点。传感器网络通常使用本地化协议进行聚类、数据聚合和其它活动，任意多跳对等通信在传感器网络中是非常少见的。如果蠕虫没有以邻居到邻居的方式传播，不会表现出和正常本地流量的共同特点，那么蠕虫节点就很容易被检测到。因此，为了降低被检测到的机率，攻击者将依赖逐跳传播策略，使得蠕虫病毒传播看起来更像是正常的本地流量。然而，当这种逐跳传播策略与流行病模型一起使用时，可能无法满足给定时隙内感染节点数的增长，因为感染节点在某个时隙内的邻居节点可能已经都已经是感染节点了。在这种情况下，我们假设感染节点通过从网络中随机选择敏感节点并将蠕虫传播给它们来维持感染率。由于传感器网络通常有密集的节点部署来确保网络互联和区域覆盖，因此每个节点基本上都有足够的邻居节点使得逐跳传播策略优于随机传播策略，从而大大降低蠕虫节点被检测的机率。

* 1. SPRT-Biased-Random蠕虫节点检测方案

在本小节中，我们详细的阐述所提出的蠕虫检测方案。该方案的核心思想在于，蠕虫节点之间的通信模式异于正常节点的通信模式，我们假设在传统的传感器网络应用中，传感器节点之间不会彼此发送大量的数据包。因为如果节点之间频繁的通信，会使得节点的能量快速的消耗，缩短整个网络的寿命。

考虑这样一个场景，蠕虫节点A向易感染节点B发送大量的蠕虫包进行感染，当B节点被感染了之后，它会将蠕虫包传递给C节点进行感染。因此如果我们对A发送到B的蠕虫包和B发送到C的蠕虫包进行抽样检测的话，我们不难发现肯定有包是重复发送的。我们定义这种传播模式为“链”，“链”和多跳通信模式的区别在于“链”的每两个节点都是一组源和目标节点，而多跳通信则是一组源节点和目标节点通过多个中间节点进行通信。图3-1描述了“链”和多跳模式通信的区别，其中A-B-C“链“有两组源节点和目的节点，A-B通过三个中间节点进行通信，属于多跳通信模式。



**图3.1多跳通信模式和“链“通信模式示意图**

* + 1. 网络预处理阶段

在传感器网络部署前需要对每一个传感器节点分配唯一的ID号同时分配私钥进行节点之间的通信。通过密钥管理方案可以防止源节点伪造，当一个节点接收到另一个节点发来的分组包时，首先通过密钥验证节点之间是否可以通信，如果认证不通过那么丢弃分组，通过这种方式可以防止蠕虫病毒仿造节点ID增加蠕虫检测的误报率。在节点部署完成之后，每个节点需要找到自己的邻居节点并以的概率周期性地将自己选举为监控节点，因此一个组中的节点有可能依次成为监控节点。通过周期性地选举监控节点可以让攻击者无法精确掌握监控节点因而无法准确攻击，另一方面可以让每个节点依次成为监控节点，节约每个节点的能量。

* + 1. 通信模式收集存储

每当节点接收到来自节点的数据包，节点检查分组包的目的地址是不是自身，节点是不是自身节点的邻居节点，如果满足上述条件，那么节点将分组包的源节点ID和目标节点ID以概率广播发送给它的邻居节点。我们将称作通信模式，节点的邻居节点在接收到通信模式的时候，如果该邻居节点是监测节点那么该节点接收并保存该通信模式，否则丢弃该通信模式。包预处理(Packet Preprocessing Unit,PPU)的伪代码如表3-1所示,该算法工作在MAC层。

表3-1 分组包预处理单元算法

|  |
| --- |
| 输入：接收到的数据包packet |
| **If pkt.destination==u and pkt.source==u’s neighbor then** |
| **Broadcast  to neighbors with probability** |

每个监测节点以一定概率接收邻居节点广播的通信模式，进行蠕虫检测。更进一步，节点将整个检测时域分成一系列的时隙，在每一个时隙中保存通信模式信息。每当节点接收到一个通信模式，首先检测和是否是其邻居节点，如果是的话节点在内存中存储，否则将其丢弃。接着监测节点检测内存中是否已经存在，其中或者，那么可以组合成融合通信模式或者，同时对计数器M进行加一操作。其中计数器M用于统计融合通信模式的合成次数，在每一个时隙开始时M初始化或重置为0，每当有通信模式融合计数器加一。我们以节点中是否存在融合通信模式来作为数据包重复传输的重要理论依据。在正常的网络中，监测节点基本上不可能产生融合通信模式，因此M计数器很大概率的值为0。而在蠕虫节点传播下监测节点会有大量的融合通信模式产生，因此M的值至少大于1。因此每一个时隙中M的值都可以作为节点的邻居区域是否有蠕虫传播的依据。在每一个时隙中，如果M=0，我们就直接接受空假设网络中没有蠕虫传播，如果M>1那么我们根据M值的大小选取M个采样值来加速接受网络中有蠕虫传播，我们把该方案定义为偏向采样方案。偏向采样方案的优势在于，能够产生更多的样本加速SPRT算法接受假设，因此能够快速的监测到网络中的蠕虫传播区域。

* + 1. SPRT蠕虫检测

SPRT算法是一种统计决策算法，它并不预先规定观测样本群的数目，而是在检测过程中不断地增加数据，一直到满足某个门限值时终止算法。我们假设蠕虫没有在网络中传播为空假设，蠕虫在网络中传播为选择性假设。在本节中我们首先结合偏向采样方法定义SPRT蠕虫检测方案。我们假设为第个时隙时检测节点的计数器M的值。我们通过定义伯努利随机变量如式(3-3)所示。

|  |  |
| --- | --- |
|  | (3-3) |

伯努利随机变量成功的概率为，也即网络中有融合通信模式出现的概率如式3-4所示：

|  |  |
| --- | --- |
|  | (3-4) |

因为假设和假设在整个样本空间中是独立的，所以我们得到式3-5：

|  |  |
| --- | --- |
|  | (3-5) |

如果单独考虑的话，可得式3-6,由该式我们可以推出随着减小而增大，随着的减小而增大，这意味着蠕虫节点的检测率越高那么漏报率就越低。给定预定义的两个门限值和，如果监测节点运行SPRT算法检测到那么很可能网络中并没有蠕虫传播，如果检测到那么很有可能网络中发生了蠕虫传播。所以判断传感器网络中是否有蠕虫传播可以归结成一个假设检验问题，问题的空假设为，选择假设为。

|  |  |
| --- | --- |
|  | (3-6) |

基于该问题的描述，我们给出检测节点如何通过个样本结合SPRT算法做出决策，其中被视为一个采样样本，SPRT的对数概率比计算方法如式3-7所示：

|  |  |
| --- | --- |
|  | (3-7) |

因为每个时隙间产生融合通信模式是互相独立的，我们假设每个样本之间是独立同分布的，那么可以改写为式3-8：

|  |  |
| --- | --- |
|  | (3-8) |

定义为个采样样本中的情况，因此可以推出式3-9,其中。

|  |  |
| --- | --- |
|  | (3-9) |

基于对数概率比, SPRT的运算规则如下：



其中代表用户配置的最大容许的误报率，代表用户配置的最大容许的漏报率，根据式3-9，令分别为3-10和3-11所示：

|  |  |
| --- | --- |
|  | (3-10) |
|  | (3-11) |

那么SPRT算法的运算规则可以修改为如下：



如果SPRT算法接受了假设，那么监测节点重启SPRT算法继续监测。如果接受假设那么监测节点向邻居节点发送广播说明本地可能有节点被蠕虫感染。然后监测节点和其邻居节点使用软件认证方案[49,80]分别对其邻居节点进行蠕虫检测，在检测到蠕虫节点之后使网络中的节点不再与该节点进行通信。

虽然基于偏向采样的SPRT蠕虫检测算法能够快速准确地检测蠕虫攻击，但是在一些特殊的场景下蠕虫检测将会失败，比如说蠕虫病毒可以动态地改变其在网络中的节点感染率快慢，导致SPRT算法出现大量的漏报。具体来说，如果一个蠕虫节点感染邻居节点的速率较慢，那么在网络中就不会频繁地出现融合通信模式，这样一来很多蠕虫节点会被当做是良性节点。为了解决这个问题，我们需要动态地改变采样样本的门限值。由上面给出的定义我们知道代表网络中没有蠕虫病毒传播，但是监控节点出现了融合通信模式的概率。该概率也即代表了传感器节点在判断网络中没有蠕虫病毒传染的时候能够最大承受的监控节点有融合通信模式发生的概率，如果蠕虫病毒能够掌握这个信息，那么它可以动态地改变自己的成对感染率，将自己伪装成良性节点。因此我们引入随机参数动态修改该概率值，即将替换成，很明显参数的值应该大于1 也即，这意味着我们对样本值为假设的样本信任权重较低，接受假设的概率降低，能够在慢蠕虫传播的情况下加速SPRT决策向假设靠近检测蠕虫。如果SPRT决策接受假设那么网络中基本不可能出现融合通信模式(由良性节点构成融合通信模式的概率非常小)，这样的话即使是慢蠕虫传播也能检测出来。我们假设参数服从的均匀分布，在每一个时隙运行SPRT算法时随机选取值，使得攻击者无法动态改变蠕虫的成对感染率，在一定程度检测蠕虫病毒的慢传播。在该假设下SPRT的对数概率比扩展为式3-12所示：

|  |  |
| --- | --- |
|  | (3-12) |

因此SPRT的修改规则相应的修改为：



其中如下所示：

|  |  |
| --- | --- |
|  | (3-13) |
|  | (3-14) |

* 1. 安全性分析

在本小节，我们首先分析了所提出方案的蠕虫节点检测率，接着我们给出当SPRT算法终止时传感器网络中受感染节点的数量。

* + 1. 蠕虫节点检测率

假设分别代表实际场景下蠕虫节点的误报率和漏报率。定义为SPRT接受假设而实际情况是的概率，定义为SPRT接受假设而实际情况是的概率，根据文献[72]有如下关系式：

|  |  |
| --- | --- |
|  | (3-15) |

代表用户配置的最大容许的误报率，代表用户配置的最大容许的漏报率。由式(3-15)可得单个检测节点的蠕虫检测率的下限值为：

|  |  |
| --- | --- |
|  | (3-16) |

由3-16可知，和配置的值越小，单个节点的检测率就越高。如果网络中有个监测节点，那么传感器网络的蠕虫检测率如式3-17所示：

|  |  |
| --- | --- |
|  | (3-17) |

接着，我们探究监测时隙个数对单个节点蠕虫检测率的影响。在每个检测时隙，我们首先随机选取值来防止蠕虫节点的慢传播，针对单个检测节点我们提出定理1。

定理1：假设在前个时隙检测中选取的值分别是，同时假设SPRT算法终止时检测了个样本，那么蠕虫节点在第个时隙前检测到的概率。其中为每一轮时隙中蠕虫未被检测到的最大概率，如式3-18所示：

|  |  |
| --- | --- |
|  | (3-18) |

证明：在每一轮时隙中，SPRT算法在的时候接收假设，检测到蠕虫传播。因此在每一轮的时隙中，蠕虫不被检测到的概率为：

=

如果蠕虫节点在个时隙前的任意一个时隙中检测到，那么蠕虫节点将被检测到，所以蠕虫节点在前个时隙被检测到的概率为，由于因此有：



定理1证明完毕。

我们首先给出了随检测节点变化的关系，从1个节点逐渐增加到5个节点，，结果如图3.2所示。由图3.2分析可知，传感器网络中蠕虫节点的检测率随着的减小而增大，这与所分析的结论一致。同时整个网络的蠕虫检测率随着网络中监测节点的数量增加而增大，且在较小数量的监测节点下依然能保持高的蠕虫检测率。

**图3.2 网络中监测节点个数和检测率的关系** **图3.3 检测时隙个数和检测率的关系**

图3.3描述了蠕虫检测率随着检测样本数和检测时隙的变化关系。在该仿真中为了方便讨论蠕虫检测率的性能，我们假设在每一轮时隙中值相等，令，那么就有，同时我们令。由仿真结果可知随着采样样本数目的增加和检测时隙的增加，蠕虫检测率都随之增加，且只需要通过5个时隙的检测就能达到0.8的检测率，这说明了方案的高效性。

* + 1. 蠕虫节点感染的上限

在这一节中，我们讨论所提出的SPRT检测方案当检测到蠕虫节点时能够控制的网络中受感染节点的数量。

定理2：令为监测节点个通信模式采样样本中由蠕虫节点引起的融合通信模式的比例，那么监测节点w在其邻居节点至少被感染个时，能够检测出蠕虫节点。其中如式3-19所示：

|  |  |
| --- | --- |
|  | (3-19) |

证明：因为代表融合通信模式在个通信模式采样样本中的个数，那么有。根据SPRT算法的终止条件有：，那么可以重写为，如式3-19所示。值得注意的是一个融合通信模式的出现代表有一个节点被感染，为了简单起见，我们假设蠕虫节点之间不会在彼此传染。因此，有个融合通信模式出现，说明就有个节点被感染，那么当监测节点w的邻居节点至少有个被感染时，w能监测出该区域有蠕虫节点。



**图3.4 参数对****节点检测出蠕虫节点所需要的最小感染节点数的影响**

根据定理2，图3.4描述了参数与监测节点检测出蠕虫节点所需要的最小感染节点数的关系。我们令，可以发现最小感染节点的数量与采样数成正比，这说明需要检测的时间越久，网络中受感染的节点就会越多。因此如果能够通过尽量少的采样样本检测蠕虫节点的话，对传感器网络的影响会最小，与此同时我们发现参数越大，传感器节点最后受到感染的节点越少，这是因为参数越大,SPRT算法接受假设的概率越大，可以加速对蠕虫节点的检测。

* 1. 性能分析

在本小节，我们首先给出了SPRT蠕虫检测模型决策需要的样本均值，接着讨论了整个方案中产生的通信开销和内存开销。

3.5.1 决策平均采样样本数

我们将定义为SPRT算法做出决策的样本数目，是一个随机变量，该变量由样本类型决定，由文献[72]有：

|  |  |
| --- | --- |
|  | (3-20) |

由3-20我们可以计算如式3-21所示：

|  |  |
| --- | --- |
|  | (3-21) |

结合引入的随机参数，可以改写为如式3-22所示：

|  |  |
| --- | --- |
|  | (3-22) |



**图 3.5. 和采样均值的关系** **图3.6 值和的关系**

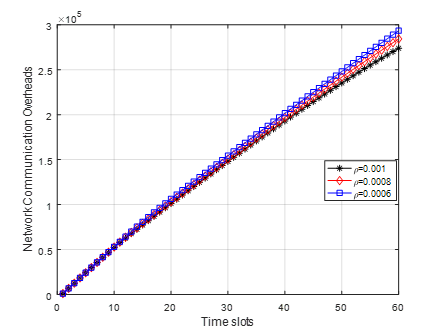
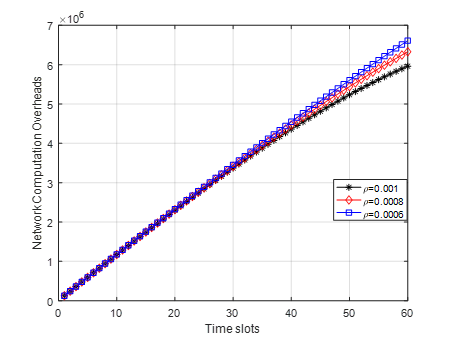


**图3.7 值和的关系**

图3.5展示了与采样样本均值的关系，通过结果图我们可以发现越大SPRT算法所需要的决策样本数目就越少，越大所需要的决策样本数就越高。同时由图进一步分析我们可知较小时，当逐渐增大时两者之间的差距渐渐缩小，最终。这表明越小，SPRT检测算法能够通过少量样本，迅速检测出蠕虫节点。图3.6和3.7分别展示了值和、的关系，在该仿真中我们假设，从0.0逐渐增加至0.30。由仿真结果分析可知，随着的增大，平均采样值都有所增加，且随着增大，平均采样样本逐渐减少，这是因为，该值越小SPRT算法决策所需要的平均样本数就越少。

3.5.2 通信资源开销和内存资源开销

我们定义SPRT检测算法中的通信损耗为每个时隙中节点间发送和接收的平均通信模式量。假设整个传感器网络中有个节点，那么整个网络在一个时隙中有个监测节点，为监测节点的选举概率。假设节点拥有个邻居节点，同时每个时隙中平均有个数据包的目的地址为节点，如果该节点为非监测节点，那么该节点在每个时隙中将会发送个数据包，其中为数据包的抽样概率，为包的源节点为节点的邻居节点的概率。如果该节点为监测节点那么它在每个时隙中最多需要接收个数据包，对于整个传感器网络而言每个时隙中，监测节点的数量为，非监测节点的数量为，那么一个时隙中整个网络的最大通信开销为。我们定义SPRT检测算法中的内存资源开销为每个时隙中监测节点需要存储的通信模式的平均值。在最坏的情况下，每一个监测节点最多需要存储的样本数目为，网络中的监测节点数量为，那么网络中总的最大内存资源开销为。在本文中我们讨论通信资源开销和计算资源开销随检测时隙增加的累计和。需要注意的是每个时隙中被检测出的蠕虫节点不在进行通信，因此逐渐减小。



**图3.8 不同感染率下检测时隙和通信资源的关系** **图3.9不同感染率下检测时隙和计算资源的关系**

图3.8和图3.9分别描述了不同感染率下传感器网络的通信资源和计算资源随检测时隙的变化关系。很明显，随着时隙的增加整个网络的计算资源和通信资源都在增加，但并不是呈现简单的线性增加关系而是增长率慢慢下降的趋势，这是因为随着检测时隙的增加，网络中能够通信的节点减少（被检测到的蠕虫节点不在通信），总的通信量增长减小。同时我们发现感染率越大，相对的资源开销越小，这是因为感染程度越高，蠕虫节点检测速度加快，总体资源开销下降。

* 1. 实验分析

在本小节，我们首先给出了仿真环境的设定，然后给出相应的仿真结果，分析方案的性能。

3.6.1仿真环境设定

我们通过简单的仿真实验来评估所提出模型的性能。在我们的仿真实验中，500个传感器节点部署在的方形区域内，传感器节点的通信半径为。在之前的分析中我们将传感器节点按照分组进行部署，采用的分组策略是将节点按照二维高斯分布分散在区域中，所满足的二维高斯分布密度函数满足式3-23。其中是每个传感器分组的组头节点，为标准差，在仿真实验中和通信半径相同，我们将500个传感器节点分成20组，每一组25个传感器节点，其它仿真参数设计如下：，

监测节点的自我选举概率，分组包随机广播的概率。

|  |  |
| --- | --- |
|  | (3-23) |



**图 3.10 不同感染率下感染节点随时隙的变化**

假设每个节点要么只单独传播良性的分组包，要么就仅仅传送蠕虫节点包。在良性传播的情形下，我们假设正常的网络流量生成满足泊松分布，包发送的间隔时间满足参数为的指数分布。对于蠕虫节点而言，假设它在每个时隙中发送的分组包为50字节以感染其他节点，文献[79]对这一假设进行了合理的分析。同时我们假定蠕虫节点以逐跳方式进行传播，在感染一个节点之后将恶意代码继续传播给下一个节点，假定蠕虫的传播模型为2.1.3节中讨论的离散型蠕虫传播模型，我们讨论蠕虫的感染率从0.0002变化到0.001的实验结果。对于每一组的性能指标，我们取1000次实验结果的均值作为最后结果进行比较。

3.6.2仿真结果说明

我们通过以下几个性能指标来评估文章所提出的SPRT蠕虫检测方案（原始方案和为随机值方案）。

**i** SPRT蠕虫检测算法决策所需要的平均采样样本数

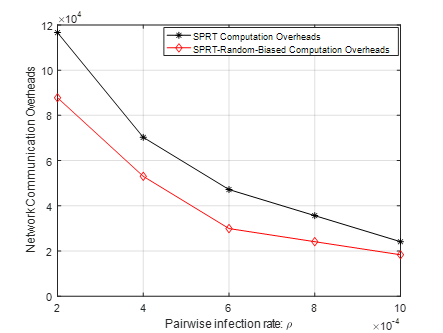
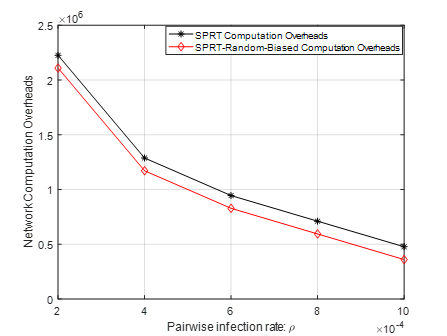
**ii** SPRT蠕虫检测算法决策所需要的平均时隙数

**iii** 检测到蠕虫病毒传播时，网络中被感染的节点数

**iv** 通信资源和内存资源消耗

****

**图3.11 不同感染率下所需检测时隙比较 图3.12 不同感染率下所需的平均采样数比较**

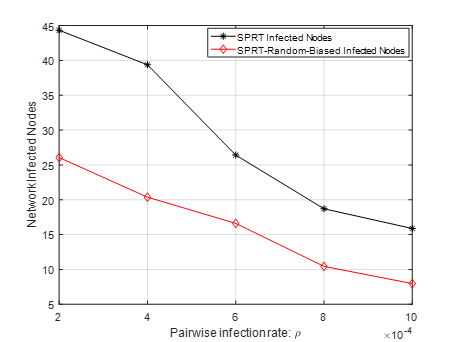
****

**图 3.13 不同感染率下网络的通信资源比较 图3.14 不同感染率下网络的计算资源开销**

图3.11描述了不同感染率下SPRT蠕虫检测算法和SPRT-Random-Biased蠕虫检测算法的所需检测时隙数的。由3.11分析我们可知随着蠕虫病毒感染率的增长，整个网络的检测时隙逐渐减少，这是因为蠕虫节点的感染率增高，网络中的蠕虫包传送频繁，会出现大量的包重传现象加速了SPRT检测算法对蠕虫的检测。同时，我们可以很明显的发现SPRT-Random-Biased算法相比SPRT算法能够有效的降低所需检测的时隙数，更早的检测到蠕虫节点。蠕虫的感染率越低，SPRT-Random-Biased的检测时隙数相对于SPRT算法的效果就越好，这突出了所提方案的优越性。

图3.12展示了不同感染率下SPRT蠕虫检测算法和SPRT-Random-Biased蠕虫检测算法检测并清除网络中的蠕虫节点所需要的平均样本数。随着感染率的增加，两种算法下检测样本数目都在减少，这是因为蠕虫感染率增加，网络中大量的发生包重传现象，网络中的大量样本为有效样本能够加速蠕虫节点的检测。同时我们可以知道SPRT-Random-Biased算法需要的平均样本数要小于SPRT蠕虫检测算法，可以简单理解为需要的检测时隙少，所需要的平均样本值相对较少。且当蠕虫的感染率为0.001时，SPRT-Random-Biased算法只需要约为5的样本值进行蠕虫检测。

图3.13和3.14分别描述了不同感染率下整个网络的通信资源损耗和计算资源损耗。随着感染率的增加，通信资源和计算资源都逐渐降低。这是因为随着感染率的增加，网络对蠕虫节点的检测加快，所需要的时隙数减少，网络间的通信开销和计算资源开销随之降低，具体可以参考3.5.2中的分析。同时SPRT-Random-Biased算法在各个传染率下的资源消耗要比SPRT算法低，这也是所提方案的优越性所在。

****

**图 3.15 不同感染率下传感器网络检测到蠕虫节点时受感染的节点数量**

图3.15展示了两种方案在不同感染率下传感器网络检测到蠕虫节点时受感染的节点数量，由图分析我们可知，蠕虫节点的感染率越高，就越容易被侦测到，其在网络中感染的节点就会相对更少。我们也可以看到所提出的SPRT-Random-Biased检测方案能够有效的限制感染节点的比例在2%~5%左右，比SPRT检测方案要更加优越。

* 1. 本章小结

在本章中，我们基于SPRT算法构建了蠕虫检测模型，并在其基础上构建了有效解决慢蠕虫传播的SPRT-Random-Biased蠕虫检测模型。通过进一步的分析和实验，我们提出的模型能够有效地检测传感器网络中的蠕虫节点，极大的限制蠕虫传播给网络带来的影响。实验结果说明我们提出的SPRT-Random-Biased检测方案能够通过尽可能少的时隙和采样样本数量来检测到蠕虫节点，该检测方案能够将蠕虫感染节点限制在2%~5%之间，同时该方案能够减少网络中的通信损耗和计算损耗，可以高效地排查传感器网络中的蠕虫节点。

然而，在该研究中我们并没有研究恶意节点既传播良性数据又传播恶意代码的情况，如果蠕虫节点能够既发送良性数据又发送蠕虫包，那么它完全有可能将自己伪装成良性节点进行隐藏。在本章中并没有对这一个情况进行考虑，这是值得研究的一个方向点。

# 改进型分布式PCA异常数据检测方案

* 1. 引言

WSN要求网络传递的数据值足够可靠。然而无线传感器网络部署在无人监控的野外，传感器节点很容易被攻击者捕获，攻击者通过捕获节点仿造数据值达到欺骗基站的目的，同时传感器节点能量有限，网络发送数据时极易受到环境中噪声的影响，造成数据的失真。因此为了保证基站接收到数据的可靠性，必须对异常数据进行剔除。上一章中我们针对蠕虫节点进行检测剔除，文献[24]中针对移动恶意节点进行检测，文献[26]针对复制节点进行检测，文献[34]针对移动复制节点进行检测,通过恶意节点检测能够很大程度上减小网络被攻击的概率，本章我们将重点放在由传感器内部的错误或者数据传播过程中噪声引起的异常数据检测。

在WSN中，异常数据定义为与正常的监测数据特征差别较大的数据。因此检测异常数据最简单的方法就是对正常的监测数据进行建模，然后将模型应用于新的监测数据，如果新到达的监测数据和模型的偏差超过一定的阈值，那么可以将该监测数据定义为异常数据进行丢弃。文献[68],[81]详细地概述了无线传感器网络中的异常数据检测方案, 然而这些方案普遍存在以下的缺点：一方面，这些方案很多是集中式方案，会给部分节点带来巨大的资源开销，同时会给整个传感器网络带来巨大的通信开销。另一方面，所给出的方案往往并不能在资源和检测效率上得到折衷的效果，这对实时数据检测精度要求高的应用而言是非常致命的。最后，以上这些方案中仅仅解决了如何识别传感器网络中的异常数据，却并没有提及如何追溯异常数据发生的原因，对于网络的管理者而言，仅仅知道网络中是否有异常数据发生是不够的，掌握异常数据发生的原因有助于网络管理者更好地保护网络的安全性。

主成分分析法(Principal Componnets Analysis,PCA)被广泛运用于模式识别领域，是一类非常高效的模式识别算法[82]。本章基于PCA算法，对数据向量进行降维之后使用马氏距离来衡量数据向量之间的相似性，提出了改进型分布式主成分异常数据检测(Improved Distributed PCA Outlier Detection,IDPCA)方案。该方案下异常检测分为本地检测和全局检测，大大地提高了网络的检测性能。我们将传感器网络进行分组，每个组拥有一个簇头节点，在每一个分组中节点都运行IDPCA检测算法识别网络中的异常数据。同时充分利用传感器网络的空间相关性，本章创造性的提出了异常数据源检测方案，主要检测网络中的异常数据是由恶意事件引起的还是由传感器节点内部错误或者噪声引起的。通过拟合数据和英特尔伯克利实验室侦测的数据进行仿真分析，仿真结果说明IDPCA异常数据检测方案能够达到96%~97%的异常数据检测率和2%的数据误报率，能够有效地识别网络中异常数据发生的原因并且降低网络的整体通信资源消耗。

* 1. 网络拓扑结构假设

在本部分，我们对传感器网络的部署规则进行相应的说明以及假设。我们假设整个传感器网络是一个静态网络，节点部署完成之后不再改变位置，节点之间可以进行双向通信且节点之间的密钥对已经提前匹配，非合法密钥之间的节点无法进行通信。整个网络部署在无人看守的野外环境下，传感器节点之间彼此同步。将节点按照组分散开来，每个组有一个组节点，假设同一个组中的节点监测的数据值是相近的，且都在组节点的通信范围内，这就是我们说的传感器节点之间的空间相关性。令代表一组以节点为组节点的一组传感器节点集合。在每一个时隙间隔，集合中的每一个节点测量一组数据值，令分别代表各个节点测量的数据向量。每一个数据向量拥有维的数据：。图4.1展示了一个以为中心节点的邻居节点关系图。



**图4.1以****为中心节点的邻居节点**

根据不同的应用场景，异常数据可以分为全局异常数据和局部异常数据。局部异常数据代表的是每一个节点根据自身的测量值和检测算法检测出的异常数据。全局异常数据是指通过一组节点中各个节点的共同作用，检测出的异常数据值。我们的目的在于当某个节点检测到一个新的数据测量值，通过局部检测和全局检测对该数据进行实时的检测。另外，通过充分利用传感器节点之间的空间相关性，我们进一步研究了异常数据产生的原因，追踪异常数据源。

* 1. IDPCA异常数据检测模型

在本节中，我们详细介绍IDPCA异常数据检测方案，该方案主要包括四个部分：模型训练阶段、异常数据检测阶段、异常数据源检测阶段、模型更新阶段。

4.3.1 IDPCA异常数据检测模型训练

模型训练阶段旨在为每一个节点单独地建立起正常数据模型。假设是传感器节点在个时隙窗口中收集到的个检测数据向量，可以表示为式(4-1)所示。

|  |  |
| --- | --- |
|  | (4-1) |

其中每一个有维分量。节点首先将中每一个向量值进行标准化，然后计算以列为中心的矩阵：

|  |  |
| --- | --- |
|  | (4-2) |

为每一列的均值向量，为长度的向量。接着我们计算协方差矩阵如式4-3所示：

|  |  |
| --- | --- |
|  | (4-3) |

求解协方差矩阵对应的特征值和特征向量，对应的特征向量即为主成分分量，其中特征值按照从大到小排列，最大特征值对应的特征向量为第一主成分分量定义为。

|  |  |
| --- | --- |
|  | (4-4) |

节点计算所有测量向量值到第一主成分的投影距离式4-5所示，示意图如图4.2所示。

|  |  |
| --- | --- |
|  | (4-5) |



图4.2 测量向量值到第一主成分的投影距离.

然而欧式距离在计算数据向量的相似度时并不会考虑数据维度之间的相关性，马氏距离在计算数据向量的相似度时结合数据向量维度之间的相关性更加适用于多元数据向量的相似度分析[62]。同时，在最大主成分方向上的投影并不能完全地反应数据的原有特征，因此我们采用新的距离计算方案来建立模型。令为特征值的的总和，即：

 (4-6)

为了能够获取数据的绝大部分特征，使用主成分分量的得分来确定选择的主成分个数。实验表明当主成分的得分大于0.9时，新的映射坐标能够代表原数据的特征，主成分个数的获取由式4-7确定。

|  |  |
| --- | --- |
|  | (4-7) |

这也就意味着当我们将数据进行PCA处理之后原来的维数据将变成的维数据向量。定义映射后的数据向量的协方差矩阵为，均值，那么各个数据向量到数据中心的马氏距离计算如式4-8所示：

|  |  |
| --- | --- |
|  | (4-8) |

定义了各个向量投影之后到中心节点的特征距离，能够很好的定义数据之间的相似度。定义为邻居节点中数据向量距离数据中心最大的马氏距离。以六元组作为节点的本地异常检测模型。

当一个数据向量在本地被检测为异常数据时需要再次进行全局的异常检测，全局异常检测由邻居节点的簇头节点负责检测，该节点的异常检测模型是由邻居节点共同作用获得的。每个邻居节点将训练得到的三元组发送给簇头节点，簇头节点根据特定的融合算法[83]来建立全局异常检测模型，模型的计算规则如式4-9所示。

|  |
| --- |
|  |
| (4-9) |
|  |
|  |

综上所述，IDPCA异常数据检测模型的伪代码如表4.1所示。

**表4.1 异常检测模型的建立**

|  |
| --- |
|  |

4.3.2 IDPCA异常数据检测

在密集分布的传感器网络中，充分利用传感器节点之间的数据相关性，每个节点都能够提供充足的数据来进行异常检测。检测阶段分为局部检测和全局检测。初始化阶段，每个传感器节点通过它在个时间窗口中获得的监测数据计算主成分向量和主成分个数进一步计算最大马氏距离。接着每个节点将它的三元组广播到其相邻的簇头节点中，簇头节点根据各个邻居节点发送的三元组通过融合算法来计算。当一个新的数据向量到达节点 ,节点首先运行本地异常检测算法。根据其六元组计算当前数据向量到数据中心的马氏距离，然后比较和。如果，那么当前数据向量被认为是一个正常的数据。否则，该数据向量被标记为可疑数据，节点将降维之后的数据发送到簇头节点并根据三元组计算相似度与进行比较，如果，那么最终被认为是一个异常数据，否则将其可疑标记去除，认为其是一个正常数据。因此，最终的异常数据判别函数如式(4-10)所示:



|  |  |
| --- | --- |
|  | (4-10) |

根据式(4-10)，如果的最终结果等于-1，那么该数据被认为是一个异常数据,否则该数据为正常数据。

 (4-6)

异常数据检测的伪代码如表4.2所示。

**表4.2 异常数据的检测流程**

|  |
| --- |
|  |

4.3.3 异常数据源检测

区分是何种原因引起了网络中的异常数据是一项非常重要的工作。无线传感器网络中，引起数据异常的原因主要包括以下几种：通信链路中的环境噪声、传感器内部节点错误、真实的事件发生和恶意攻击。本方案着重讨论如何区分异常数据是由简单的噪声或者内部错误引起还是由真实事件导致。主要思路如下：簇头节点中维护初始变量，当邻居节点监测数据为异常数据时,当所有邻居节点都检测完毕，如果,那么当前网络中有真实的事件发生(比如森林火灾发生时，会有一大批异常数据同时发生)。否则，当前的异常数据只是由单纯的噪声或者内部错误引起的，在这种情况下节点收集随之而来的个时隙窗口中的个数据向量，计算其到数据中心的平均马氏距离。如果，那么此时的数据异常是由噪声引起的，否则是由于传感器节点内部异常导致的数据异常。



异常数据可以由传感器内部的异常和通信链路中的噪声引起，为了便于分析我们假设这两者的产生概率相同为，的值理论上应该是一个非常小的数，否则传感器网络将无法正常运行，是每个簇中产生异常数据的节点数量。异常数据源归结为恶意事件的条件满足，这意味着有一半以上的节点的数据为异常数据，所以如果异常数据源被虚报为恶意事件的话，那么一个簇节点中至少有的节点被误报为异常数据。假设异常数据的误报率为，那么异常数据源被误报为恶意事件的最大概率为：。假设某个节点周围发生了恶意事件，我们假设一个簇中的节点检测的数据都是异常数据，这个时候如果没有检测出有异常事件发生，说明至少有一半以上的节点漏报了异常数据，也即假设异常数据的检测率为，那么漏报率为，至少有一半以上的节点漏报，所以异常数据源为恶意事件的最小检测概率为。异常数据源的检测算法伪代码如表4.3所示:

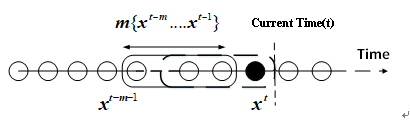
**表4.3 无线传感器网络异常数据源检测**

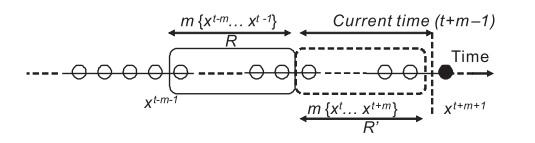
|  |
| --- |
|  |

4.3.4 模型更新

随着无线传感器网络部署环境的变化，监测数据实时变化(温度的变化)，因此异常数据检测模型需要进行实时的更新。令代表当前的时间窗口，为了更新全局检测模型，每个传感器节点都需要根据当前时间窗口的前个时间窗口中的正常数据重新计算六元组。具体的数据模型更新过程如图4.3所示。异常数据检测模型的更新，能有效的提高异常数据的检测效率，该方案的核心思想是减少对旧数据的依赖性，根据实时的数据来提高模型的精确性。







**图4.3 异常数据检测模型的更新过程，黑色节点代表当前的检测窗口**

根据以上分析，给出完整的IDPCA算法检测的伪代码见附录3。

* 1. 性能分析

本节我们讨论IDPCA异常数据检测模型的通信资源消耗和计算资源消耗。

4.4.1 通信资源开销

我们假设通信资源开销为异常模型检测时，网络中因为PCA检测方案而引起的额外的通信开销。为了便于分析，我们以数据的维数为单位衡量通信的开销，例如传播一个数据向量需要的通信开销。在所提出的IDPCA方案中,每一个传感器分组拥有个邻居节点，每个邻居节点在计算完成六元组之后将发送给簇头节点进行全局异常模型的建立。其中的维度是，的维度为，但是由于它是一个对称矩阵，所以其有效的维度可以认为是，的维度为1。所以，对于邻居节点而言其通信损耗为，而簇头节点为。如果任意一个邻居节点本地异常检测未通过那么节点将当前向量值计算的发送到簇头节点进行全局检测，这个过程中最坏的情况下每一个邻居节点需要额外增加通信损耗，簇头节点需要额外增加。因此在所提出的方案中邻居节点的通信损耗最多为为,簇头节点的通信损耗为，总的通信损耗为。文献[68]提出的集中式PCA检测方案中，各个邻居节点将个时隙窗口中收集到的个数据向量集中发送到簇头节点，簇头节点根据这些数据向量建立检测模型，在异常数据检测时，每个节点将自己的数据向量值发送到簇头节点进行检测。因此在这种模式下邻居节点的通信量，簇头节点的通信量为，总的通信损耗为。文献[69]提出的分布式PCA检测方案中，每个邻居节点的通信量为，簇头节点的通信量为，总损耗为。文献[62]中提出的基于SVM的分布式EOOD和EAOD方案在网络中的通信损耗为，其中传递协方差矩阵的通信损耗为，传递均值矩阵和半径的通信损耗为。其中。



4.4.2 计算资源开销

我们假设通信资源开销为异常模型检测时，网络中因为PCA检测方案而引起的额外的计算资源开销。在所提出的IDPCA检测方案中，模型建立阶段每个邻居节点需要对数据向量进行标准化，这个过程的计算资源耗费为，接着计算协方差矩阵并通过特征值分解获取主成分分量，同时通过主成分得分值计算所需主成分分量的个数，这个过程的计算资源耗费为。最后，再得到主成分分量之后需要计算坐标映射后的向量矩阵和其协方差矩阵并计算最大马氏距离值，这个过程的计算损耗为，所以邻居节点的计算资源总消耗为。对于簇头节点而言，它需要额外的计算这部分的计算开销为，所以簇头节点的计算开销为，所以总的计算开销为。文献[68]中的集中式PCA检测方案，邻居节点的计算开销可视作为0，簇头节点的计算开销为。文献[69]中的DPCA异常数据检测模型中邻居节点的计算开销为，簇头节点的额外计算开销为，所以簇头节点的计算开销为，所以总的计算开销为：。文献[62]中提出的基于SVM的分布式EOOD和EAOD方案在网络中的计算损耗分为协方差矩阵计算和均值计算，总的计算损耗为。

4.4.3 性能仿真分析

本部分我们讨论不同方案下异常数据检测模型消耗资源对比，其中我们认为邻居节点个数为常量值不超过50，具体如表4.5所示。

**表4.5 各个方案的通信性能损耗和计算资源损耗**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **网络中通信损耗** | **邻居节点的计算损耗** | **簇头节点的计算损耗** |
| **CPCA异常检测模型** |  | **-** |  |
| **DPCA异常检测模型** |  |  |  |
| **IDPCA异常检测模型** |  |  |  |
| **EOOD异常检测模型** |  |  |  |
| **EAOD异常检测模型** |  |  |  |



由表4.5可知IDPCA异常数据检测模型在所给方案中拥有较小的通信损耗，且计算资源损耗和其它方案相近。为了细致比较各种方案的资源消耗，我们比较一个簇中总的计算资源开销和通信资源开销，如图4.4,4.5,4.6所示。



**图4.4 监测数据维度和通信资源开销的关系**



**图4.5 监测数据维度和计算资源开销的关系 图4.6 训练数据集和计算资源开销的关系**

图4.4描述了5种异常数据检测模型下，通信资源开销随测量数据向量维度变化的关系，集中式PCA检测方案的通信开销远远超过了其余方案的通信开销，随着监测数据维度的增加各种方案下网络的通信量都慢慢增加，IDPCA异常数据检测模型下网络的通信资源受数据维度变化的影响较小，拥有所给方案中最低的通信资源消耗。图4.5和图4.6展示了无线传感器网络中计算资源开销与模型训练数据集和监测数据维数的关系，随着两个参数的增大，总体计算资源消耗增长，且EAOD和EOOD异常数据检测模型下，整个网络拥有最低的计算资源消耗，DPCA方案和IDPCA方案的计算资源消耗几乎相等，IDPCA稍微高一点。值得说明的是，在传感器网络中通信消耗的能量值要远大于计算消耗的能量，因此IDPCA方案能够很好的节省传感器节点的能量，延长网络的寿命。



**图4.7 异常数据误报率和恶意事件误报率的关系图 4.8 异常数据检测率和恶意事件检测率的关系**

图4.7描述了单节点的异常数据误报率和异常数据源为恶意事件的误报率，由图分析可知网络中恶意事件的误报率随着单节点的误报率增大而增大，但是始终维持在一个非常小的值，说明方案对网络中的恶意事件存在极小的误报情况，一旦网络中发现恶意事件应该马上处理。图4.8描述了网络中恶意事件的检测率随每个节点异常数据检测率变化的关系，由图分析我们可知恶意事件的检测率随着节点异常数据检测率增加而增加且当节点的异常数据检测率为0.7以上就能够达到0.9的恶意事件检测率，当节点的检测率超过0.9之后，恶意事件的检测率趋近于1，这说明如果我们的方案能够达到90%以上的异常数据检测率那么我们能够很准确的判断网络中是否有异常事件发生。

* 1. 仿真分析

在本小节，我们首先给出了仿真环境的设定，然后给出相应的仿真结果，分析方案的性能。在WSN中，我们通常选取两个指标来衡量检测模型的性能，即：异常数据的检测率(Detection Rate，DR),误报率(False Alarm Rate, FAR)。异常数据的检测率指的是检测模型检测到的异常数据占总的异常数据的比例，误报率指的是检测模型将正确的数据误判为异常数据的比例，异常数据的检测率越高，误报率越低，检测模型的性能就越好。

同时在很多文献中以接收者操作曲线(Receiver Operating Characteristic,ROC) 来衡量异常数据检测模型的优劣性，ROC曲线描述的是FAR和DR之间的关系，理论上该曲线和坐标轴所围面积最大为1。评估某个检测方案是否足够好可以通过ROC曲线所围面积是否趋近于1来判断和比较。在本节我们通过比较不同PCA方案的ROC曲线和基于SVM异常数据检测模型的ROC曲线来说明所提出模型的优越性，ROC曲线与坐标轴所围面积(AUC)越大，该检测模型的性能就越好。

4.5.1 仿真环境设定

I**拟合数据集**

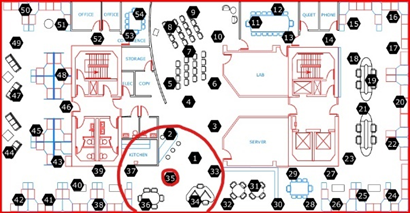
在拟合数据集合中我们以一组节点进行仿真分析，簇头节点拥有20个邻居节点，每个检测的数据为3维数据，每个维度的数据值服从高斯分布，方差为0.03，均值为(0.3,0.35,0.4)中的随机值。每个节点中的异常数据定义为某个维度上的数据值服从均匀分布，取值范围在[0.5,0.7]。我们选取四个时间窗口中的1000正常数据来训练异常检测模型，接着在每个时间窗口中选取200个正常数据值和50个异常数据值，分析每一个时间窗口中，检测模型的异常数据检测率和误报率。拟合的数据集合如图4.9所示。



**图4.9 训练数据集和待检测数据集**

**II IBRL数据集**

英特尔伯克利实验室采集的传感器数据集(IBRL)是评估无线传感器网络中异常数据检测模型性能的主要数据源。该网络测量的数据包括：环境温度，湿度，光照强度和电压，在本节中我们使用湿度值和温度值两个属性进行仿真分析。该网络每隔31秒收集一次数据，我们的仿真数据来源于图4.10中以节点35为簇头节点的一组节点，其邻居节点为1，2，3，34，36，37。



**图4.10 IBRL无线传感器网络模型**

我们使用2004年2月28号上午9点到下午5点的数据进行模型训练，如图4.11所示，2月29号到3月3号的检测数据进行检验。为了更好的评估模型的性能，我们随机选取50个数据向量，对其温度值加上值进行仿真实验，如图4.12所示。同时，为了直观的比较三种模型下异常数据的误报率，我们对正常数据引入高斯白噪声，高斯白噪声的强度由信噪比(SNR)表征。

****

**图4.11 IBRL训练数据集 图 4.12 IBRL测试数据集**

4.5.2 仿真结果分析

这一小节中我们首先给出了拟合数据集下，IDPCA异常数据检测模型的DR和FAR随时间窗口的变化，接着讨论实际环境中不同方案的性能比较。



**图4.11 拟合数据集下IDPCA异常数据检测率 图4.12 拟合数据集下IDPCA数据误报率**

图4.11和4.12展示了IDPCA异常检测模型在不同的时间窗口中的DR和FAR。由图4.11我们可知IDPCA算法能够将DR稳定在93%以上，平均的异常检测率为96%左右。由图4.12我们可知IDPCA检测模型能够同时达到一个较小的FAR，基本能够维持在2%左右，是一个较小的误差值。

**** 

**图4.13 IBRL数据集合下异常数据检测率对比 图4.14 IBRL数据集合下异常数据误报率对比**

图4.13的结果说明了本方案所采用的异常检测模型能在实际场景中取得很好的效果，它能够达到近乎96%-97%的异常数据检测率，比已提出的DPCA方案和CPCA方案达到的效果要更好，EAOD方案使用的是基于SVM的异常检测方案，该方案的异常数据检测模型最高能够达到99%的检测率，然而这并不能说明该方案的检测性能最优。另一方面，从图4.14我们可以看出，通过本方案提出的双重检测机制和模型更新策略，IDPCA检测模型能够有效的降低异常数据的误报率，比已经提出的DPCA和CPCA方案更加的可靠,而EAOD方案虽然拥有最高的异常数据检测率，但是其异常数据的误报率在方案中也是最大的。由4.4.3小节分析结合本节实验结果我们可知ICDPCA方案能够很好地检测网络中的恶意事件（DR>0.9）并且几乎不会出现误报的情况。



**图4.15 不同PCA方案的ROC曲线对比 图4.16 IDPCA方案同SVM方案的ROC曲线对比**

图4.15展示了IDPCA方案下ROC曲线和DPCA,CPCA的对比图，我们能够很轻易地看出IDPCA方案的性能要优于其余两种方案，它能在较低的误报率下保持较高的检测率, 更加的符合实际场景。图4.16展示了IDPCA方案和EAOD方案[62]的ROC曲线对比，由图分析可知IDPCA方案能够在保证高检测率的同时保持低的误报率，它的检测性能要优于基于SVM的检测方案。综上所述，本方案在继承原有PCA异常检测模型的基础上，提高了模型的异常数据检测率、降低了误报率，同时对网络中的恶意事件能够很好地识别，该方案的可靠性更高，更加适合于实际场景。

* 1. 本章小结

本章在已有的PCA异常数据检测模型的基础上提出了IDPCA异常数据检测模型，该模型充分利用传感器节点之间的空间相关性、节点数据间的时域相关性以及数据向量之间的维度相关性能够达到较高的异常数据检测率，同时维持较低的数据误报率。另外，通过提出的双重检测机制，我们能够很好地区分异常数据的起因，针对网络中的恶意事件能够很好地识别。最后为了满足检测数据的实时变化，我们动态更新检测模型来保证模型的可用性。然而根据4.4节的分析我们可以发现IDPCA异常数据检测模型的计算步骤比较繁杂，而且网络中的通信消耗并不能达到常量级别，因此需要寻求更加高效地方案来解决该问题。同时针对部分线性不可分的数据集而言，PCA算法并不能找到最佳的映射空间来反映数据的特征。针对以上问题我们在下一章中引入基于KPCA算法的分布式异常数据检测方案来检测传感器网络中的异常数据。

# 第五章 基于马氏内核的分布式KPCA异常数据检测方案

5.1 引言

在第四章中，我们提出了基于PCA算法的IDPCA异常数据检测模型，该模型能够很好的检测出传感器网络中的异常数据并检测异常数据产生的原因。然而PCA检测算法只有在数据集为线性可分时能够达到的效果最好，而对于线性不可分的数据向量PCA算法往往找到的映射坐标轴并不能达到最优。因此在PCA算法的基础上使用核主成分分析法(Kernel Principal Components Analysis,KPCA)来处理监测数据为非线性可分的情况。KPCA使用核函数将原始数据向量映射到高维特征空间，也就是把当前低维空间转换成高维空间，并在这个空间中计算特征向量。我们忽略特征值很低的向量，然后在这个变换的空间中训练模型。与PCA相比，KPCA计算量大，耗时长得多。KPCA中训练样本数目远高于PCA，因此，需要估计的主成分分量也要大得多。与线性PC分析方法相比，KPCA方法在处理非线性系统[71][72]时具有非常大的优势,文献[73]中详细介绍了KPCA算法的原理。在本章中我们将基于马氏内核的KPCA方案用于无线传感器网络中的异常数据检测。为了检测异常值，我们使用马氏距离来衡量数据向量之间的相似度，通过模型训练得到最大的非相似度。如果新数据点的非相似度高于最大非相似度，观察值将被视为异常值。同时，借鉴第四章中的思路我们提出IDKPCA异常数据检测方案，最后通过固定时间窗口模型更新策略来更新异常检测模型，有效地降低模型的更新频率，减小了传感器节点的计算开销。实验结果表明：在英特尔伯克利实验室的数据下，IDKPCA的异常数据检测率能够达到98%且误报率在2%左右，其检测效率要高于IDPCA方案和EAOD方案[62]，这是因为这些检测的数据并不是线性可分的，而KPCA检测方案对于线性不可分的数据有更好的检测效果。

5.2 网络模型与马氏内核函数

假设整个传感器网络是一个静态网络，节点部署完成之后不再改变位置，节点之间可以进行双向通信且节点之间的密钥对已经提前匹配，非合法密钥之间的节点无法进行通信。整个网络部署在无人看守的野外环境下，传感器节点之间彼此同步。将节点按照组分散开来，每个组有一个组节点，假设同一个组中的节点监测的数据值是相近的，且都在组节点的通信范围内，这就是我们说的传感器节点之间的空间相关性。令代表一组以节点为组节点的一组传感器节点集合。在每一个时隙间隔，集合中的每一个节点测量一组数据值，令分别代表各个节点测量的数据向量。每一个数据向量拥有维的数据：。通过寻找合适的核函数能将低维空间中线性不可分的数据映射到高维空间中进行线性分类，图5.1给出了KPCA的原理示意图。



**图5.1 KPCA原理示意图**

经典的核函数包括径向基核函数(RBF)、多项式核函数等。然而马氏内核的应用并不广泛，马氏内核函数通过利用测量数据间数据值的相关性，将数据映射到高维空间中，马氏内核如式5-1所示：

|  |  |
| --- | --- |
|  | (5-1) |

令为节点的个维数据向量，我们定义数据中心为和协方差矩阵如式5-2所示：

|  |  |
| --- | --- |
|  | (5-2) |

某个数据节点到数据中心的马氏距离为：

|  |  |
| --- | --- |
|  | (5-3) |

我们定义马氏内核函数如式5-4所示:

|  |  |
| --- | --- |
|  | (5-4) |

其中为一个正半定矩阵，当，，为单位矩阵时，马氏内核可以看作是特殊的RBF内核函数，在实际场景中马氏内核一般定义为式5-5所示:

|  |  |
| --- | --- |
|  | (5-5) |

径向基核函数RBF也称为高斯核函数，其表达式如式5-6所示：

|  |  |
| --- | --- |
|  | (5-6) |

马氏内核与高斯内核的不同之处在于，它为输入空间数据的每个维度定义了一个特定的深度值或权重。这使得计算出的判定边界相对于数据点的中心具有非球形形状。

5.3 IDKPCA异常数据检测模型

本节我们详细介绍所提出的IDKPCA异常数据检测方案，该方案主要分为四个阶段。异常数据检测模型训练阶段、异常数据检测阶段，异常数据源检测阶段、异常数据模型更新阶段。其中异常数据源的检测与第四章中的思路一致，本节不在单独提出。

5.3.1 IDKPCA异常数据检测模型训练

模型训练阶段旨在为每一个节点单独地建立起正常数据模型。假设传感器节点在个时隙窗口中收集到的个监测数据向量。在高维空间中我们定义映射，这里表示Hibert泛函空间，通过该映射每个监测数据映射为,它们的维数理论上可以是无穷的，在这个新的空间中协方差矩阵可以定义为式5-7所示：

|  |  |
| --- | --- |
|  | (5-7) |

令,那么，如果需要求解特征值的话那么需要计算矩阵的特征值，但是由于映射函数是未知的所以无法计算，根据KPCA的推导我们有如下的结果：

|  |  |
| --- | --- |
|  | (5-7) |
|  | (5-9) |

其中是由核函数确定的内积值矩阵，如式5-10所示. 为高维空间中向量向方向的投影值。

|  |  |
| --- | --- |
|  | (5-10) |

在模型训练开始时，对数据向量进行归一化，保留数据均值和标准差，接着计算矩阵并求出对应的和。令为矩阵特征值的的总和，即：

 (5-11)

在高维空间中主成分个数比低维空间中要多，为了能够获取数据的绝大部分特征值，我们参照主成分分量的得分来确定选择的主成分个数。实验表明当主成分的得分大于0.9时，新的映射坐标能够代表原数据的特征，主成分个数的获取由式5-12确定。

|  |  |
| --- | --- |
|  | (5-12) |

构建模型的主成分分量个数由参数决定，确定之后紧接着通过计算每个训练样本的非相似度[70]并找出其中最大的非相似度值来定义异常检测模型阈值,非相似度的定义如式5-13所示：

|  |  |
| --- | --- |
|  | (5-13) |

最后，节点通过保留六元组来构建本地异常数据检测模型。对于簇头节点，上一章使用相应的融合算法对协方差矩阵和均值进行了重构得到全局的异常检测模型。这种方案计算步骤比较繁琐而且涉及到协方差矩阵的传输，并没有对网络中的通信资源进行最合理的优化。因此，结合文献[84]中的思路,令每个邻居节点将各自的发送到簇头节点中，然后簇头节点计算全局最大非相似度=来定义全局异常数据检测模型。

**表5.1 IDKPCA异常数据检测模型的建立**

|  |
| --- |
|  |

5.3.2 IDKPCA异常数据检测

检测阶段分为局部检测和全局检测。初始化阶段，每个传感器节点通过它在个时间窗口中获取的训练数据计算六元组。接着每个节点将它能容忍的最大非相似度广播到其相邻的簇头节点中，簇头节点根据各个节点发送的最大非相似度计算全局最大非相似度，通常情况下该全局最大非相似度取的是各个节点最大非相似度的中位数[84]。当一个新的数据向量到达节点,节点首先根据其将当前的数据向量标准化，然后通过核函数计算PC Score得到，接着比较和。需要特别注意的是的计算，此处先进行标准化得到。由式5-1、5-9和5-13得到式5-14:

|  |  |
| --- | --- |
|  | (5-14) |

如果，那么当前数据向量被认为是一个正常的数据，否则该数据向量被标记为可疑数据，并将其发送到簇头节点中和进行比较，如果，那么最终被认为是一个异常数据，否则将其可疑标记去除，认为其是一个正常数据。因此，最终的异常数据判别函数如式(5-15)所示:

|  |  |
| --- | --- |
|  | (5-15) |

根据式(5-15)，如果的最终结果等于-1，那么该数据被认为是一个异常数据。

|  |  |
| --- | --- |
|  | (5-16) |

表5.2给出了IDKCPA异常数据检测模型下，异常数据的检测流程：

**表5.2 IDKPCA异常数据检测流程**

|  |
| --- |
| ; |

5.3.3 固定时间窗口模型更新

随着无线传感器网络部署环境的变化，异常数据检测模型需要进行相应的的更新。异常数据检测模型的更新，能有效的提高异常数据的检测效率，该方案的核心思想是减少对旧数据的依赖性，根据数据的实时性来提高模型的精确性。在上一章中我们采用实时更新策略来保证模型的可靠性，在每个时间窗口中接受到新数据时根据新数据是否是异常数据来更新模型。一般情况下，网络中的正常数据值占的比例很大，这意味着模型更新的速度非常频繁，这会给网络带来大规模的计算资源开销。为了降低模型更新的速度且不影响模型的性能，我们提出了固定时间窗口模型更新策略，如图5.2所示。



**图 5.2 固定时间窗口模型更新策略**

其中表示经过个时间窗口对模型进行更新，即重新计算全局的六元组。为了确定合适的值，我们引入艾宾浩斯遗忘曲线。艾宾浩斯遗忘曲线揭示了人们在学习中的遗忘是有规律的，遗忘的过程并不是呈现简单的线性关系而是处于一种非均衡的变化。将艾宾浩斯遗忘曲线应用于机器学习中来舍弃旧数据，寻找合适的时间窗口间隔来进行模型更新，其表达式如式5-17所示。

|  |  |
| --- | --- |
|  | (5-17) |

其中代表的是记忆强度，代表记忆时间，代表记忆量。图5.3给出了记忆量与记忆时间窗口的关系，当时我们对模型进行更新。



**图5.3 记忆量与记忆时间窗口的关系**

5.4 性能分析

本节中我们分析IDKPCA模型建立需要花费的通信资源和计算资源。由以上的小结分析，IDKPCA方案下的通信资源消耗和IDPCA方案的通信资源消耗相同，但是IDKPCA方案下的计算资源要比IDPCA大，我们着重讨论该模型的计算资源消耗。

我们假设计算资源开销为IDKPCA检测方案运行时，网络中因为IDKPCA检测方案而引起的额外的计算资源。模型建立阶段每个邻居节点需要对数据向量进行标准化，这个过程的计算资源耗费为(为节点的训练样本数)，接着通过计算矩阵进行特征分解得到PC Score计算，这个过程中通过核函数计算得到矩阵的资源耗费为，马氏内核中的协方差矩阵的计算复杂度为，最后在得到主成分分量之后需要计算值，这个过程的计算损耗为，所以邻居节点的计算资源总消耗为。对于簇头节点而言，它需要额外的计算这部分的计算开销为，所以簇头节点的计算开销为，所以总的计算开销为。

在所提出的IDKPCA方案中,每一个传感器分组拥有个邻居节点，每个邻居节点在计算五元组之后将发送给簇头节点进行全局的计算，对于邻居节点而言其通信损耗为1，而簇头节点为。如果任意一个邻居节点本地异常检测未通过那么节点将当前向量值计算的发送到簇头节点进行全局检测，这个过程中最坏的情况下每一个邻居节点需要额外增加1通信损耗，簇头节点需要额外增加。因此在所提出的方案中邻居节点的通信损耗为,簇头节点的通信损耗为，总的通信损耗为。

各个方案下的资源消耗如表5.3所示，其中为常量值代表邻居节点的个数且不超过50。IDKPCA方案下异常数据检测模型的通信损耗是最少的达到了常量级别，虽然该方案的计算步骤简洁但是引入的计算资源开销却随着训练样本的增加而大幅度增加。为了克服频繁地模型更新带来的巨大计算资源开销，我们提出了5.3.3节中的策略有效地降低模型的更新频率。

**表5.3 IDKPCA方案的资源消耗同其它方案的比较**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **网络中通信损耗** | **邻居节点的计算损耗** | **簇头节点的计算损耗** |
| **CPCA异常检测模型** |  | **-** |  |
| **DPCA异常检测模型** |  |  |  |
| **IDPCA异常检测模型** |  |  |  |
| **EOOD异常检测模型** |  |  |  |
| **EAOD异常检测模型** |  |  |  |
| **IDKPCA异常检测模型** |  |  |  |

5.5 仿真分析

本节我们分析所给出的IDKPCA方案的DR和FAR随核函数参数变化的关系，接着我们比较IDKPCA方案和IDPCA、EAOD方案的异常数据检测率，最后比较了这三种方案的ROC曲线和曲线所围面积(Area Under Curve,AUC)。

5.5.1 仿真环境设定

本节我们依旧使用英特尔伯克利的实验数据来进行模型分析，该测量数据值包括测量温度(temperature),环境湿度(humidity)，光照强度和传感器电压(Voltage)。在上一章中仅仅使用了环境温度和湿度来进行模型的性能分析，然而传感器节点的电压值也是一个很重要的因素，通过电压值异常能够检测出无效节点。传感器节点测量电压值的正常范围在[2,3]之间且其变化和环境中的温度密切相关[85],在本节中我们使用温度值、湿度值和传感器电压来进行模型的训练和检测。我们使用2004年2月28号上午9点到下午5点的1200个训练数据进行模型训练，如图5.4所示。为了突出IDKPCA方案的优势我们在测试数据集中随机选取50个数据向量插入电压异常值服从均匀分布，同时选取50个数据向量(和电压异常向量不重复)温度值加上值进行仿真实验，如图5.5所示。令。为了寻找最佳的核参数使得模型的DR和FAR达到最佳，我们令的值从1逐渐递增到2001，观察参数对模型性能的影响。



**图5.4 IBRL训练数据集** **图5.5 IBRL测试数据集**

5.5.2 仿真结果分析

****

**图5.6 参数****与模型检测率的关系** **图5.7 参数****与模型误报率的关系**

图5.6展示了基于高斯径向核函数的KPCA检测方案和基于马氏内核函数的KPCA检测方案异常数据检测率随参数值的变化关系。由图分析可知，基于RBF高斯径向核函数当很小的时候模型的检测性能很差，而基于马氏核函数的异常数据检测方案的性能受该参数的影响较小，模型的异常检测率维持在90%以上。同时，由图我们能发现基于马氏内核的KPCA检测方案的异常数据检测性能要优于基于RBF内核的KPCA检测方案，该方案的异常检测率要比RBF-KPCA平均高0.01到0.02左右，同时发现在参数内出现检测率的峰值。

图5.7给出了基于高斯径向核函数的KPCA检测方案和基于马氏内核函数的KPCA检测方案异常数据误报率随参数值的变化关系。由该图分析可知，两种内核函数下的异常数据检测模型都能够达到很小的数据误报率，基本能维持在3%以下，平均误报率在1.5%左右。结合异常数据的检测率的峰值在[800,1000]的区间中出现，我们取参数值来进行其余实验，在该参数下基于马氏内核的KPCA检测方案的平均检测率为98%，平均误报率为1.4%。。

****

**图 5.8 不同模型下异常数据检测率的比较 图5.9 PCA模型的ROC曲线比较**

图5.8给出了时IDKPCA方案和IDPCA等方案的异常数据检测率对比图。由图分析可知在不同的时间窗口中IDKPCA方案下模型的异常数据检测率稳定在97%-98%之间，是一个非常可靠的检测效率。同时，IDPCA方案的异常数据检测率在94%~95%之间，相比于线性可分的数据集而言，其检测效率下降了一些。EAOD方案的异常数据检测率最高,达到了98%~99%,但是这并不能说明该方案的检测效率是最好的。图5.9给出了IDKPCA、IDPCA和EAOD异常检测模型的ROC曲线，由图可知EAOD方案下模型的异常数据检测率高的同时异常数据的误报率也相对较大，而IDKPCA方案和IDPCA方案能够保证异常数据的检测率在95%以上且数据的误报率维持在2%左右，且在相同的误报率下IDKPCA方案的异常数据检测率要高于IDPCA方案。图5.10进一步给出了三种异常检测模型下方案的ROC曲线所围面积在每个时隙中的平均值，AUC越大模型的检测性能越好。由图5.5我们可知，IDKPCA方案下模型的AUC值在0.94-0.95之间，IDPCA方案的AUC值在0.90-0.94之间，EAOD方案的AUC值在0.87~0.88之间。因此在检测性能这一方面，IDKPCA方案能够达到最好的效果。

****

**图 5.10 不同模型下ROC曲线所围面积的的比较**

5.6 本章小结

本章在第四章的基础上，为了解决线性不可分的异常数据检测，提出了基于马氏内核的IDKPCA异常数据检测模型，该方案能够很好地检测线性不可分的异常数据，达到98%的异常数据检测率的同时能够维持异常数据的误报率在2%左右。同时，我们改进了第四章中全局异常检测模型的训练，有效地减少了网络中的通信资源消耗并且引入了固定时间窗口更新机制，大大降低了模型更新的频率，减小了每个节点的计算资源消耗。然而KPCA方案引入了核函数的计算并且需要计算最佳的核参数，这在一定程度上也加大了计算的复杂度。未来仍需要继续探究如何进一步的减小节点的计算复杂度。

# 第六章 总结与展望

6.1文章总结

文章针对传感器网络中的蠕虫节点检测和异常数据检测提出了新的解决方案。

首先，无线传感器网络中的恶意节点是威胁传感器网络安全的最严重的问题，一旦网络中存在恶意节点那么整个网络都将处于危险状态，已有的研究解决了很大一部分恶意节点的检测，但是对于蠕虫恶意节点并没有提出有效地解决方案。本文以SPRT算法为基础，结合偏向采样方案和随机值采样方案提出的SPRT-Biased-Random方案能够有效地检测传感器网络中的蠕虫节点，并在5-18个时隙内完全检测并移除传感器网络中的蠕虫节点，整个网络受感染的节点维持在2%到5%之间，计算方式简单，所需存储资源和通信资源也相对较少。

其次，在第四章我们提出了IDPCA异常数据检测方案来检测传感器网络中的异常数据。方案的核心是通过PCA来寻找数据的最大特征方向，使用最大距离值来衡量数据的相似度。同时我们充分的利用了传感器节点之间的空间相关性，通过本地检测和全局检测来提高模型的检测精度和降低数据的误报率。同时我们通过上述方案来有效地识别传感器网络中的异常数据源，同时针对网络中最敏感的恶意事件我们做出了详细地分析，分析表明在单个节点的异常数据检测率达到90%以上时，能够对网络中发生的恶意事件进行很好地检测。总结而言，基于IDPCA的异常数据检测方案能够降低网络中的通信负载，同时相比于其它方案IDPCA方案能够提高异常数据的检测率，降低数据的误报率。

最后在第五章中我们基于IDPCA异常数据检测方案无法对非线性可分的数据进行最佳地检测，提出了基于马氏内核的IDKPCA异常数据检测方案。实验结果表明：IDKPCA方案能够有效地检测非线性数据和线性数据，异常数据的检测性能要较优于IDPCA方案，但是IDKPCA中引入了核函数，计算复杂度要比IDPCA方案高，在精确度要求达到95%以上的场景中，IDPCA会更加适合，如果需要检测精度大于98%以上的，那么需要牺牲节点的计算资源来换取高的异常检测率。

6.2未来工作展望

虽然无线传感器网络安全的相关研究已经相当成熟。本文对针对无线传感器网络中的蠕虫节点检测和异常数据检测提出了新的方案，为了进一步提高无线传感器网络的安全，未来的工作可以从以下几个方面进行研究。

1. 本文针对的是静态传感器网络中的蠕虫节点检测，但是并没有针对移动传感器网络进行检测。移动传感器网络中的蠕虫节点始终在移动，一旦定位之后，如果继续移动的话那么本文的方案并不能实时地去除该恶意节点，这样的话有可能蠕虫节点会持续感染整个网络使得网络变得不可用。
2. 本文提出的基于PCA的异常数据检测方案基于矩阵的特征分解，计算复杂度相对较高。另外通过充分利用了节点之间的空间相关性和时域相关性本文中的方案能够达到高的检测性能，但是如果节点移动之后，检测数据的时域性和节点间的空间相关性就会大大改变，这样的话，本文所提出的模型就不再适合了。需要将模型扩展到移动网络中。

到目前为止，无线传感器网络安全的研究成果主要集中在理论分析和仿真分析。其中仿真软件像NS2,OMNET操作复杂，而且仿真的效果并没有很强。目前缺乏高效地仿真平台能够很好地

# 参考文献

[1] Yessembayev, A., et al. (2018). "Detection of Good and Bad Sensor Nodes in the Presence of Malicious Attacks and Its Application to Data Aggregation." IEEE Transactions on Signal and Information Processing over Networks 4(3): 549-563.

[2] Padmaja, P. and G. V. Marutheswar (2017). Detection of milicious node in wireless sensor networks. 2017 International Conference on Computer Communication and Informatics (ICCCI).

[3] Osanaiye, O. A., et al. (2018). "Denial of Service Defence for Resource Availability in Wireless Sensor Networks." IEEE Access 6: 6975-7004.

[4] Wang, Y., et al. (2017). An information-centric multiple-source routing scheme for wireless sensor networks. 2017 IEEE International Conference on Smart Energy Grid Engineering (SEGE).

[5] Tariq, M., et al. (2018). Detection of False Data in Wireless Sensor Network Using Hash Chain. 2018 International Conference on Applied and Engineering Mathematics (ICAEM).

[6] Hoang, T., et al. (2017). Adaptive routing in wireless sensor networks under electromagnetic interference. 2017 International Conference on Information Networking (ICOIN).

[7] Ahmed, A., Bakar, K.A., Channa, M.I. et al. Peer-to-Peer Netw. Appl. (2017) 10: 216.

[8] Sreevidya, B. and M. Rajesh (2018). False Data Injection Prevention in Wireless Sensor Networks using Node-level Trust Value Computation. 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI).

[9] López-Valcarce, R. and D. Romero (2017). Defending surveillance sensor networks against data-injection attacks via trusted nodes. 2017 25th European Signal Processing Conference (EUSIPCO).

[10] Liu, X., et al. (2018). "Bayesian Test for Detecting False Data Injection in Wireless Relay Networks." IEEE Communications Letters 22(2): 380-383.

[11] Thompson, S. A. and B. K. Samanthula (2017). Optimized Secure Data Aggregation in Wireless Sensor Networks. 2017 15th Annual Conference on Privacy, Security and Trust (PST).

[12] Karthikeyan, B., et al. (2017). Energy efficient data compression and aggregation technique forwireless sensor networks. 2017 International Conference on Nextgen Electronic Technologies: Silicon to Software (ICNETS2).

[13] Wang, T., et al. (2017). An Efficient and Secure Itinerary-Based Data Aggregation Algorithm for WSNs. 2017 IEEE Trustcom/BigDataSE/ICESS.

[14] Nehra, P. and A. Nagaraju (2017). Fault Tolerance using Quadratic-Minimum Spanning Tree (Q-MST) with Secure Data Aggregation in Wireless Sensor Networks. 2017 14th IEEE India Council International Conference (INDICON).

[15] Mukartihal, P. P. and D. I. Hatti (2017). Client Puzzle Approach for Securing Aggregated Data in Wireless Sensor Network. 2017 IEEE 7th International Advance Computing Conference (IACC).

[16] Ayadi, A., et al. (2017). Outlier detection based on data reduction in WSNs for water pipeline. 2017 25th International Conference on Software, Telecommunications and Computer Networks (SoftCOM).

[17] İ, K. and T. Ercan (2018). Anomaly Detection in Wireless Sensor Networks Data by Using Histogram Based Outlier Score Method. 2018 2nd International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT).

[18] Dwivedi, R. K., et al. (2018). A Study on Machine Learning Approaches for Outlier Detection in Wireless Sensor Network. 2018 8th International Conference on Cloud Computing, Data Science & Engineering (Confluence).

[19] Zhang, W., et al. (2018). "A novel trust management scheme based on Dempster–Shafer evidence theory for malicious nodes detection in wireless sensor networks." The Journal of Supercomputing 74(4): 1779-1801.

[20] Amudha, G. and P. Narayanasamy (2018). "Distributed Location and Trust Based Replica Detection in Wireless Sensor Networks." Wireless Personal Communications 102(4): 3303-3321.

[21] Zeiser, M. and D. Westhoff (2016). Re-visited: On the Value of Purely Software-Based Code Attestation for Embedded Devices. Innovations for Community Services, Cham, Springer International Publishing.

[22] Lee, J. and T. Kwon (2016). "Secure dissemination of software updates for intelligent mobility in future wireless networks." EURASIP Journal on Wireless Communications and Networking 2016(1): 250.

[23] Y. Yang, X. Wang, S. Zhu, and G. Cao. Distributed software-based attestation for node compromise detection in sensor networks. In IEEE SRDS, October 2007.

[24] Jun-Won, H., et al. (2012). "ZoneTrust: Fast Zone-Based Node Compromise Detection and Revocation in Wireless Sensor Networks Using Sequential Hypothesis Testing." IEEE Transactions on Dependable and Secure Computing 9(4): 494-511.

[25] Thaile, M. and O. B. V. Ramanaiah (2016). Node Compromise Detection based on NodeTrust in Wireless Sensor Networks. 2016 International Conference on Computer Communication and Informatics (ICCCI).

[26] J. Ho, D. Liu, M. Wright, and S.K. Das. Distributed detection of replica node attacks with group deployment knowledge in wireless sensor networks. In Elsevier Ad Hoc Networks Journal, 7(8):1476–1488, 2009

[27] Rahman, M. U., et al. (2017). Lightweight detection of malicious nodes in mobile ad hoc networks. 2017 International Conference on Communication Technologies (ComTech).

[28] Z. Li, W. Xu, R. Miller, and W. Trappe. Securing wireless systems via low layer enforcements. In ACM WiSe, Pages:33–42, September 2006

[29] N. Patwari and S. K. Kasera. Robust location distinction using temporal link signatures. In ACM MobiCom, Pages:111–122, September 2007.

[30] J. Zhang, M. Firooz, N. Patwari, and S. K. Kasera. Advancing wireless link signatures for location distinction. In ACM MobiCom, Pages:26–37, September 2008.

[31] J.-W. Ho, ‘‘A framework for robust detection and prevention of wide-spread node compromise in wireless sensor networks,’’ Doctoral dissertation, Dept. Comput. Sci. Eng., Univ. Texas Arlington, Arlington, TX, USA, 2010.

[32] Al-Riyami, A., et al. (2016). "An Adaptive Early Node Compromise Detection Scheme for Hierarchical WSNs." IEEE Access 4: 4183-4206.

[33] Geedhabhanu, S. and P. Latha (2015). Excluding compromised node by tracing false data injected messages in Wireless Sensor Network. International Confernce on Innovation Information in Computing Technologies.

[34] M. Conti, R.D. Pietro, L.V. Mancini, and A. Mei. A Randomized, Efficient, and Distributed Protocol for the Detection of Node Replication Attacks in Wireless Sensor Networks. In ACM Mobihoc, pages:80-89, 2007.

[35] K. Xing, F. Liu, X. Cheng, and H.C. Du. Real-time Detection of Clone Attacks in Wireless Sensor Networks. In IEEE ICDCS, pages:3-10, 2008

[36] Jun-Won, H., et al. (2011). "Fast Detection of Mobile Replica Node Attacks in Wireless Sensor Networks Using Sequential Hypothesis Testing." IEEE Transactions on Mobile Computing (TMC) 10(6): 767-782.

[37] Rasheed, M. M., et al. (2017). Detecting and optimizing internet worm traffic signature. 2017 8th International Conference on Information Technology (ICIT).

[38] Koganti, V. S., et al. (2016). Internet worms and its detection. 2016 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT).

[39] J. Newsome, B. Karp, and D. Song, ‘‘Polygraph: Automatically generating signatures for polymorphic worms,’’ in Proc. IEEE Symp. Secur. Privacy, May 2005, pp. 226–241.

[40] Ahmad, M. A., et al. (2016). Early containment of fast network worm malware. 2016 3rd National Foundation for Science and Technology Development Conference on Information and Computer Science (NICS).

[41] Y. Yang, S. Zhu, and G. Cao, ‘‘Improving sensor network immunity under worm attacks: A software diversity approach,’’ in Proc. ACM MobiHoc, May 2008, pp. 149–158

[42] Y. Yang, S. Zhu, and G. Cao, ‘‘Improving sensor network immunity under worm attacks,’’ Ad hoc Netw., vol. 47, no. 1, pp. 26–40, Sep. 2016

[43] N. Gui, E. Zhai, J. Hu, and Z. Chen, ‘‘SWORDS: Improving sensor networks immunity under worm attacks,’’ in Proc. Web-Age Inf. Manage. (WAIM), Jul. 2010, pp. 86–96.

[44] Y. Liu, W. Zhang, S. Bai, and C. Wang, ‘‘Defending sensor worm attack using software diversity approach,’’ in Proc. IEEE Int. Conf. Commun. (ICC), Jun. 2011, pp. 1–5

[45] T. Abuhmed, N. Nyamaa, and D. Nyang, ‘‘Software-based remote code attestation in wireless sensor network,’’ in Proc. IEEE GLOBECOM, Nov. 2009, pp. 1–8.

[46] X. Kovah, C. Kallenberg, C. Weathers, A. Herzog, M. Albin, and J. Butterworth, ‘‘New results for timing-based attestation,’’ in Proc. IEEE Symp. Secur. Privacy, May 2012, pp. 239–253.

[47] Yang, P. and S. Yen (2017). "Memory attestation of wireless sensor nodes through trusted remote agents." IET Information Security 11(6): 338-344.

[48] Fu, D. and X. Peng (2016). "TPM-based remote attestation for Wireless Sensor Networks." Tsinghua Science and Technology 21(3): 312-321.

[49] Ahmed, N., et al. (2018). Program-flow attestation of IoT systems software. 2018 15th Learning and Technology Conference (L&T).

[50] Distributed Software-Attestation Defense against Sensor Worm Propagation,(2015)

[51] Haque, M. A. and H. Mineno (2018). Contextual Outlier Detection in Sensor Data Using Minimum Spanning Tree Based Clustering. 2018 International Conference on Computer, Communication, Chemical, Material and Electronic Engineering (IC4ME2).

[52] Patil, S. D. and B. P. Vijayakumar (2017). A Novel Outlier Detection Scheme (ODS) in Wireless Sensor Networks. Computing and Network Sustainability, Singapore, Springer Singapore.

[53] Abid, A., et al. (2017). "Outlier Detection in Wireless Sensor Networks Based on OPTICS Method for Events and Errors Identification." Wireless Personal Communications 97(1): 1503-1515.

[54] W. Wu, X. Cheng, M. Ding, K. Xing, F. Liu, and P. Deng, Localized Outlying and Boundary Data Detection in Sensor Networks, IEEE Trans. Knowl. Data Eng., Vol. 19, No. 8, pp. 1145-1157, 2007.

[55] T. Palpanas, D. Papadopoulos, V. Kalogeraki, and D. Gunopulos, Distributed Deviation Detection in Sensor Networks, ACM Special Interest Group on Management of Data, pp. 77-82, 2003

[56] E. Knorr and R. Ng, Algorithms for Mining Distance-Based Outliers in Large Data Sets, International Journal of Very Large Data Bases, pp. 392-403, 1998

[57] S. Ramaswamy, R. Rastogi, and K. Shim, Efficient Algorithms for Mining Outliers from Large Data Sets, ACM Special Interest Group on Management of Data, pp. 427-438, 2000.

[58] J. Branch, B. Szymanski, C. Giannella, and R. Wolff, In-Network Outlier Detection in Wireless Sensor Networks, Proc. IEEE ICDCS, 2006.

[59] K. Zhang, S. Shi, H. Gao, and J. Li, Unsupervised Outlier Detection in Sensor Networks using Aggregation Tree, Proc. ADMA, 2007

[60] Andrade, A. T. C., et al. (2016). Outlier detection using k-means clustering and lightweight methods for Wireless Sensor Networks. IECON 2016 - 42nd Annual Conference of the IEEE Industrial Electronics Society.

[61] Shahid, N., et al. (2015). "One-class support vector machines: analysis of outlier detection for wireless sensor networks in harsh environments." Artificial Intelligence Review 43(4): 515-563.

[62] Zhang, Y., et al. (2013). "Distributed online outlier detection in wireless sensor networks using ellipsoidal support vector machine." Ad Hoc Networks 11(3): 1062-1074.

[63] Shahid, N., et al. (2012). Quarter-Sphere SVM: Attribute and Spatio-Temporal correlations based Outlier &amp; Event Detection in wireless sensor networks. 2012 IEEE Wireless Communications and Networking Conference (WCNC).

[64] Rajasegarar, S., et al. (2010). "Centered Hyperspherical and Hyperellipsoidal One-Class Support Vector Machines for Anomaly Detection in Sensor Networks." IEEE Transactions on Information Forensics and Security (TIFS) 5(3): 518-533.

[65] Hao, Y., et al. (2015). A Distributed Bayesian Algorithm for data fault detection in wireless sensor networks. 2015 International Conference on Information Networking (ICOIN).

[66] Titouna, C., et al. (2015). "Outlier Detection Approach Using Bayes Classifiers in Wireless Sensor Networks." Wireless Personal Communications 85(3): 1009-1023.

[67] Feng, H., et al. (2017). "Distributed outlier detection algorithm based on credibility feedback in wireless sensor networks." IET Communications 11(8): 1291-1296.

[68] V. Chatzigiannakis and S. Papavassiliou, " Diagnosing anomalies and identifying faulty nodes in sensor networks," IEEE Sensors J., vol. 7, pp. 637–645, 2007

[69] Livani, M. A. and M. Abadi (2010). Distributed PCA-based anomaly detection in wireless sensor networks. 2010 International Conference for Internet Technology and Secured Transactions.

[70] Rassam, M. A., et al. (2012). One-Class Principal Component Classifier for anomaly detection in wireless sensor network. 2012 Fourth International Conference on Computational Aspects of Social Networks (CASoN).

[71] K, Kapitanova, S.H , Son and K. D, Kang. Event Detection in Wireless Sensor Networks. Second International Conference, ADHOCNETS 2010, Victoria, BC, Canada, August 2010.

[72] Y, Zhang, N, Meratnia, P. J.M, Havinga. Distributed online outlier detection in wireless sensor networks using ellipsoidal support vector machineǁ. Ad Hoc Networks , December 2012

[73] Y, Zhang, N.A.S, Hammb, N, Meratnia, A, Steinb, M, Voorta. And P.J.M , Havinga. Statistics-based outlier detection for wireless sensor networksǁ, Volume 26, Issue 8, April 2012

[74] Fernandes Jr, G., et al. (2015). "Autonomous profile-based anomaly detection system using principal component analysis and flow analysis." Applied Soft Computing 34: 513-525.

[75] Ghorbel, O., et al. (2015). A Novel Outlier Detection Model Based on One Class Principal Component Classifier in Wireless Sensor Networks. 2015 IEEE 29th International Conference on Advanced Information Networking and Applications.

[76] A. Francillon and C. Castelluccia. Code Injection Attacks on HarvardArchitecture Devices. In ACM CCS, Pages:15–26, October 2008

[77] Patil SD, Vijayakumar BP (2016) Clustering in mobile wireless sensor networks. In: International conference on innovations in computing and networking

[78] <https://blog.csdn.net/baimafujinji/article/details/79376378>

[79] C. Zou, L. Gao, W. Gong, and D. Towsley, ‘‘Monitoring and early warning for Internet worms,’’ in Proc. ACM CCS, Oct. 2003, pp. 190–199

[80] T. Park and K. G. Shin. Soft tamper-proofing via program integrity verification in wireless sensor networks. In IEEE Trans. Mob. Comput., 4(3):297–309, 2005

[81] McDonald, D., et al. (2015). "A Survey of Methods for Finding Outliers in Wireless Sensor Networks." Journal of Network and Systems Management 23(1): 163-182.

[82] Haque, M. A. and H. Mineno (2018). Contextual Outlier Detection in Sensor Data Using Minimum Spanning Tree Based Clustering. 2018 International Conference on Computer, Communication, Chemical, Material and Electronic Engineering (IC4ME2).

[83] P. Kelly, An Algorithm for Merging Hyperellipsodial Clusters, Technical report, Los Alamos National Laboratory, 1994.

[84] Yang, Z., et al. (2008). An online outlier detection technique for wireless sensor networks using unsupervised quarter-sphere support vector machine. 2008 International Conference on Intelligent Sensors, Sensor Networks and Information Processing.

[85] http://db.csail.mit.edu/labdata/labdata.html

[86] Zheng W., Yang L., Wu M. (2018). An Improved Distributed PCA-Based Outlier Detection in Wireless Sensor Network. In: Sun X., Pan Z., Bertino E. (eds) Cloud Computing and Security. ICCCS 2018. Lecture Notes in Computer Science, vol 11067. Springer, Cham；

[87] Sun, Q.-y., et al. (2018). "Study on fault diagnosis algorithm in WSN nodes based on RPCA model and SVDD for multi-class classification." Cluster Computing.

[88] Antonopoulos, C., et al. (2017). Event Identification in Wireless Sensor Networks. Components and Services for IoT Platforms: Paving the Way for IoT Standards. G. Keramidas, N. Voros and M. Hübner. Cham, Springer International Publishing: 187-210.

# 附录1 攻读硕士学位期间撰写的论文与专利

1. Zheng W., Yang L., Wu M. (2018) An Improved Distributed PCA-Based Outlier Detection in Wireless Sensor Network. In: Sun X., Pan Z., Bertino E. (eds) Cloud Computing and Security. ICCCS 2018. Lecture Notes in Computer Science, vol 11067. Springer, Cham；
2. Zheng, W., et al. (2017). "3D MIMO Kronecker channel modeling based on three types of typical attena arrays." Xi Tong Gong Cheng Yu Dian Zi Ji Shu/Systems Engineering and Electronics 39(6): 1366-1373.
3. “适用于无线传感器网络的异常数据检测方法”，公开号：­CN108650649A

# 附录2 攻读硕士学位期间参加的科研项目

(1)国家自然科学基金，面向上下文感知数据的流计算复杂事处理技术研究(61572262)；

(2)国家电网通信项目，能源互联网中的通信路由传输；

(3)国家电网安全项目，能源互联网中的通信安全。

# 附录3 IDPCA算法伪代码

|  |
| --- |
| 1. letbe the max Mahalanobis distance of node; |
| 2. letbe the global Mahalanobis distance of ’s neighboring nodes; |
| 3. letbe the amount of data measurements for learning |
| 4. letbe a new data measurement arrive at; |
| 5. letbe the data vectors arriving at’s neighboring nodes at the same time interval |
| 6. letbe the Mahalanobis distance of at nodein time windows t; |
| 7. let be the Mahalanobis distance of at nodecompute by group node |
| 8. procedure learning  ①each node collects  data measurements for learning its ownby PCA, then broadcasts to its group node ;  ②each group node computes  ③initiate IsOutlier() for each node;  return; |
| 9. procedure IsOutlier() for |
| 11. procedure SourceOfOutlier(); |
| 12. procedure Updating training model |

# 致谢

时间荏苒，岁月如梭，不知不觉，三年的研究生时光就接近了尾声，回想这三年，我经历了很多，也成长了很多，从入学时的迷茫，到毕业时的坚定。想到在学校的时光即将结束，心里充满了对学校，对老师，对同学的不舍与感激。

首先我要感谢我的导师吴老师和杨老师在这三年里对我的谆谆教诲，在科研和生活中都给了我很大的帮助。吴老师严谨的治学态度和渊博的知识一直是我学术生涯的榜样，而杨老师对学术研究的激情和创新精神则激励着我成长。在两位导师的指导下，我飞速成长，在学术领域取得了不错的成果，还养成了主动学习，独立思考的良好习惯，学会了发现问题并努力从实践中解决，为以后的人生之路打下了坚实的基础，没有虚度研究生的时光。

此外，还要感谢同教研室的师兄师姐，感谢他们慷慨地与我分享学术过程中的经验和教训，并教会我很多实践过后才能掌握的小技巧，让我少走了很多弯路。感谢教研室的师弟师妹，一起学习一起成长，互相讨论难题，交流学术，在教研室营造了浓厚的学术氛围。感谢我的室友谢豪、竺殊荣、张彦轩在生活中对我的帮助，和你们一起生活的时光非常开心。感谢我的小伙伴王慧健、吴警、孟阳、在我遇到困难挫折时候对我的安慰和鼓励。还要感谢陪伴了我上半生的篮球、感谢在学校陪我打了7年篮球的各位球友。

我要感谢我的父母，感谢他们对我的培养、教育以及无私的关怀，在父母的鼓励、引导和支持下，我才能顺利的完成学业。