单位代码： 10293 密 级：



硕 士 学 位 论 文



论文题目： 无线传感器网络安全研究

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。这种技术源于美国军方，广泛运用于诸如火山检测，森林火灾防控，海啸监控等任务。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，传感器节点负责监测数据，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可靠的数据，然而由于各个节点部署在野外，节点的能量受限，会引起一系列的安全问题，目前传感器网络安全的研究主要分为两个方面：

随着移动通信技术的不断发展，各种无线终端都能够自由的在各个通信网中进出，由于无线信号在网络内部的广播特性，如果存在恶意的无线终端，那么网络内传输的信息就很有可能被窃听。并且最关键的是，目前的无线网络中的安全主要都是基于传统的加解密算法的高层安全。然而，在有线网络中非常有效的方法，却在无线通信中存在很多缺陷。首先，无线网络中都是小型的无线终端，因此如果加密太过复杂，设备的电量和计算能力很有可能无法支撑解密过程。其次，加解密算法的安全性大多是基于现有的计算机无法在短时间内对其进行破解，随着计算机计算能力的不断发展以及量子计算机的出现，很多传统的加密方法都有可能会被破解。

因此，基于物理层的信息安全技术成为一种重要的解决方案被人们所重视。它们利用信道自身的物理层特性来提高无线通信的安全性，其本质就是利用信道的噪声和多径特性的不确定性来加密发送信息。物理层安全技术通常作为上层加密方法的补充或替代，使得窃听者几乎不能获得发送信号的信息。在本文中我们研究了使用中间节点来对抗窃听攻击的方法。其中，中间节点可以表现为干扰节点或者中继节点。干扰节点通过广播人工噪音来对窃听者进行干扰，而中继节点则接收源发送的信息并且将其转发给预定的目的节点。我们研究的目的是找出在给定的约束条件下，系统所能获得的最大安全容量。

在本文中，我们利用博弈论来对中间节点的功率分配进行分析：

(1)提出了对主信道提供帮助的友善干扰节点是具有自私性特性的，因此这些干扰节点优先最大化自身的收益，并且它们的价格都可以任意变化。我们应用伯特兰德博弈对问题进行建模分析，并找出干扰节点收益的最优值。

(2)为了解决主信道信号过弱的问题，提出了一个干扰节点和中继节点协作的方法。首先从多个中间节点中选出一个友善干扰节点和一个中继节点，然后获得干扰和中继节点的功率、价格关系，最终应用伯特兰德博弈获得一个最优的功率分配策略，在此情况下，干扰和中继节点的自身收益最大，并且此时主信道的安全容量也是当前条件下的最大值。

(3)我们针对对干扰器并不总是善意的，它更可能是试图最大化破坏性影响的恶意干扰器的问题，提出了利用干扰节点和窃听节点的目的不同，使用恶意干扰者来干扰恶意窃听者。最终能够利用攻击者之间的内在矛盾来提高通信系统的安全性，显著提高主信道的安全容量。

关键词: 物理层安全，窃听攻击，博弈论，干扰节点，保密容量

Abstract

Wireless communications are vulnerable to eavesdropping attacks due to their broadcast nature. To deal with their emerging challenge of physical layer security, we study the anti-eavesdropping problem in the presence of intermediate nodes. The intermediate nodes can act as jammer or relay. The jammer node is used to broadcast artificial interference noise on the eavesdropper. Meanwhile, the relay node acts as a traditional relay and retransmits source signal from the source to the intended destination. This thesis studies the security problem in wireless networks, cooperative networks and wireless communication process. The goal is to obtain the optimal power allocation strategy in order to achieve the maximum secrecy capacity on the basis of Shannon information theory. The contributions of this thesis are as follows. First, we study the anti-eavesdropping problem in the presence of selfish jammers, who desire to achieve the maximum profit of themselves. When the cost of friendly jammers is considered in previous works, the cost is either set fixed or a same variable to all jammers. Since this treatment is not realistic, we propose the communication systems including selfish jammers with different costs. Second, we propose a relay and jammer selection strategy which selects the jammer and relay nodes from intermediate nodes to enhance the security of the malicious eavesdropper. For achieving the maximum secrecy capacity by the selected nodes, we introduce a power allocation approach based on price competition. Finally, we consider the transmission process in the presence of jamming attacks and eavesdropping attacks. With the existence of jamming attacks, we maximize the secrecy capacity of the main channel. We perfectly study the anti-eavesdropping problem in the presence of intermediate nodes under various wireless communication settings. In addition, game theory is applied to analyze these optimization problems.

Key words: Physical layer security, eavesdropping attacks, game theory, jammer, secrecy capacity

目录

[第一章 绪论 1](#_Toc510960099)

[1.1 研究背景及意义 1](#_Toc510960100)

[1.2 国内外研究现状 1](#_Toc510960101)

[1.3 研究内容及创新点 6](#_Toc510960105)

[1.4 本文组织结构 7](#_Toc510960106)

[第二章 无线传感器网络安全和相关算法概述 8](#_Toc510960107)

[2.1 无线传感器网络恶意节点检测 8](#_Toc510960109)

[2.1.1 传感器网络中恶意节点类型 8](#_Toc510960110)

[2.2.2 蠕虫传播模型及蠕虫节点分析 11](#_Toc510960111)

[2.2.3 SPRT算法 11](#_Toc510960111)

[2.2 无线传感器网络异常数据检测 11](#_Toc510960112)

[2.2.1 异常数据类型 11](#_Toc510960113)

[2.3.2 异常数据检测模型 12](#_Toc510960114)

[2.3.3 无线传感器网络聚簇算法概述 13](#_Toc510960115)

[2.3 机器学习算法在无线传感器网络异常数据检测中的应用 16](#_Toc510960116)

[2.3.1 PCA算法 16](#_Toc510960117)

[2.3.2 KPCA算法 17](#_Toc510960118)

[2.4 本章小结 21](#_Toc510960120)

[第三章 无线传感器网络中蠕虫节点检测方案 26](#_Toc510960124)

[3.1 引言 26](#_Toc510960125)

[3.2 网络拓扑结构和攻击者模型 27](#_Toc510960126)

[3.3 SPRT检测方案 29](#_Toc510960129)

[3.4 安全性分析 30](#_Toc510960130)

[3.4.1 恶意节点的检测率 30](#_Toc510960131)

[3.4.2 恶意节点的错报率 32](#_Toc510960132)

[3.5 性能分析 33](#_Toc510960133)

[3.5.1恶意节点检测所需采样样本期望 33](#_Toc510960134)

[3.5.2通信资源和内存资源 33](#_Toc510960135)

[3.6 性能仿真 36](#_Toc510960136)

[3.6.1 仿真环境设定 39](#_Toc510960131)

[3.6.2 仿真结果分析 40](#_Toc510960131)

[3.7 本章小结 40](#_Toc510960141)

[第四章 改进型PCA算法在无线传感器网络异常数据检测中的运用 40](#_Toc510960142)

[4.1 引言 40](#_Toc510960143)

[4.2 网络拓扑结构假设 40](#_Toc510960144)

[4.3 改进型PCA异常数据检测方案 42](#_Toc510960147)

[4.3.1 模型训练 42](#_Toc510960148)

[4.3.2 异常数据检测 43](#_Toc510960149)

[4.3.3 异常数据源检测 44](#_Toc510960148)

[4.3.4 模型更新 45](#_Toc510960148)

[4.4 安全性及性能分析 45](#_Toc510960150)

[4.4.1 异常数据的检测率 46](#_Toc510960151)

[4.4.2 异常数据的误报率 47](#_Toc510960152)

[4.4.3 通信和存储资源消耗 48](#_Toc510960152)

[4.5 性能仿真 49](#_Toc510960153)

[4.5.1 仿真环境设定 49](#_Toc510960131)

[4.5.2 仿真结果分析 39](#_Toc510960131)

[4.6 本章小结 39](#_Toc510960141)

[第五章 改进型KPCA算法在无线传感器网络异常数据检测中的运用 47](#_Toc510960154)

[5.1 引言 47](#_Toc510960155)

[5.2 网络拓扑结构假设 47](#_Toc510960155)

[5.3 IKPCA异常数据检测模型 47](#_Toc510960155)

[5.4安全性分析 47](#_Toc510960155)

[5.5 性能分析 47](#_Toc510960155)

[5.6 仿真分析 47](#_Toc510960155)

[5.6.1 仿真环境设定 49](#_Toc510960131)

[5.6.2 仿真结果分析 49](#_Toc510960131)

[5.7 本章小结 47](#_Toc510960155)

[第六章 总结与展望 47](#_Toc510960154)

[6.1 文章总结 47](#_Toc510960155)

[6.2 未来工作展望 48](#_Toc510960156)

[参考文献 49](#_Toc510960157)

[附录1 攻读硕士学位期间撰写的论文 52](#_Toc510960158)

[附录2 攻读硕士学位期间参加的科研项目 53](#_Toc510960159)

[致谢 54](#_Toc510960160)

# 

# 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[2]. 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。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[ 84 ]。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[ 25、43、75 ]。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。例如，文献[ 43、54、59 ]提出了安全路由方案来减轻路由中断攻击，文献[ 81、86、91 ]通过使用认证方案来减轻虚假数据注入攻击。安全数据聚合协议[ 8、18、38、60、78 ]用于防止攻击者破坏聚合。但是，这些方案中的大多数关注于使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，无线传感器网络( WSN )在许多领域的应用通常需要高能效、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。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测量错误。同时，在WSN中，环境条件可能会随着时间的推移而变化，因此，预定义的正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。

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，从大型数据集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以简单的方式应用，因为它们可能会造成极高的通信损耗和计算损耗。在WSN中，每个传感器节点拥有大数据集的一小部分，并与其邻居节点进行战略性通信，以检测整个网络中的异常值。值得注意的是，WSN中最耗费节点能量的行为是：一个无线节点向下一个无线节点发送数据。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. 无线传感器网络恶意节点检测

为了检测传感器网络中被捕获的恶意节点，文献[1][6][13][15][17][19][23]提出了多种检测方案。例如，文献[6][13][19]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，但是由于误报的风险，它们不容易被清除。事实上，所有基于信誉值的检测方案都有很小的误报率，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。

处理传感器网络中恶意节点的另一种方法是软件认证[1][15][17][23]。该方案利用了这样一个事实，即传感器节点通常运行存储在闪存映像中的同一份可执行代码，并且在没有来自基站的明确指令的情况下不应改变。这些方案验证了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地软件认证。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[4]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，然后在再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。

然而，基于区域信誉值的信任管理方案是针对静态的恶意节点的，如果恶意节点在网络中会移动，那么恶意节点就能够不被检测到。如果攻击者能够创建移动恶意节点，他将受益于节点移动带来的攻击路径多样化。例如，如果攻击者希望对基站发起DDoS攻击，他可以使用一组移动恶意节点，这些节点移动到尽可能多的不同位置，并向每个位置的基站发送洪泛数据包。这些数据包可以在本地进行身份验证，但在基站无法进行身份验证，需要某种形式的追溯来识别每个攻击者。如果攻击者不以基站为目标，而是旨在破坏分布式自组织协议，如路由协议和聚簇协议，他可以通过移动相对较少的节点来实现。当移动恶意节点在网络中移动时，一部分移动恶意节点可以一次性在一个区域内中断这些操作，从而产生路由黑洞、或者由于时间同步和定位错误导致的协议失败，以及其他形式的破坏。综上，移动恶意节点攻击对网络的影响将比静态恶意节点攻击更加危险，对于移动的恶意节点也需要相应的检测方案对其进行检测和移除。

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，这种方案需要网络运维人员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[ 35 ]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、47、57、87 ]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[5](博士论文)提出了一种分布式检测方案，通过利用顺序概率比检验( SPRT )来识别和移除移动恶意节点。该方案利用静态传感器节点能够频繁的与邻居节点通信并被侦测到而移动恶意节点的邻居节点时刻在更新不能保持时刻通信的特点，并结合SPRT算法能够快速检测和撤销移动恶意节点。

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，上述的方案却无能为力。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，只要他有硬件可以生成。副本节点不必是移动节点，唯一的要求是它们有相同的ID和密钥材料在网络中通信，所有这些都可以从捕获的节点中获得。将这些复制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。副本节点由对手控制，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复制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，虚招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[3][9][12]中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[3]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，文献[3]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。

我们首先描述了无线传感器网络中静态恶意节点检测的一些研究。基于软件认证的方案用来检测传感器节点被破坏的软件模块[ 55、62、64、79 ]。在文献[ 55、62、64 ]中，基站通过执行内存代码的一部分或全部来检查内存代码是否被恶意更改。在文献[79]中，传感器节点的内存代码由其邻居节点进行认证。上述这些方案都需要定期验证每个传感器节点，因此在通信和计算方面会产生大量开销。我们的静态节点泄露检测方案不需要定期证明，而是针对不可信区域的一次性证明。

由于高层的安全防护技术比如加密技术[1]在计算能力飞速发展的今天越来越有可能被破解，为了弥补这一缺陷，物理层安全技术被提出作为一种有效的底层安全防护技术来弥补高层技术的不足。

无线网络具有两个基本特征，即广播性和叠加性，这两个特征使得在存在恶意用户的情况下对信息传输可靠性和安全性方面提出了多种挑战。其中无线通信的广播性质使得发送者难以防止非预期接收者窃听保密信息，而叠加性质可能导致接收端的多个信号发生重叠。考虑到这两种情况，恶意用户通常被建模为(1)试图从正在进行的传输中提取信息而未被检测到的未经授权的恶意窃听节点，或(2)试图降低目标接收端接收信号的恶意干扰节点。

反恶意窃听节点和反恶意干扰的物理层策略一直是人们长期以来关心的问题，特别是在军事网络等传输高度机密信息的网络中。传统情况下，数据传输的安全性通过网络层的基于秘钥的加密技术来实现，然而，在现代的动态无线网络中，存在着对称密码系统的密钥分配和非对称密码系统的高计算复杂度等问题。并且，最重要的是，所有的加密措施都基于不知道密钥的情况下对它们进行破译在计算上是不可行的这一前提，然而这一前提在数学上还未被证实，而且由于计算机计算能力的不断增长，过去被认为几乎完全安全的加密方法不断被破解。因此，许多现在常用的加密方案被认为并不是牢不可破，我们需要找到一种更加可靠或者能够对加密方法进行补充的方法，因此物理层安全作为一个可行的研究方向被专家广泛研究。

物理层安全是指利用物理信道本身的特性，如唯一性和互异性等，来实现信息加密，主要是作为一种上层安全的补充方法出现，能够极大地增强系统整体的安全性能。通常物理层安全的研究都是以窃听信道模型为基础，包含信道编码、秘钥协商、协作干扰等多种技术。物理层安全的理论基础是Shannon在他的经典论文“保密系统的通信理论”中证明的保密通信系统模型和信息论，通过“一字一密”的方式进行加密[2]。Wyner则引入了窃听信道的模型[3]，证明不使用高层加密技术也可以获取一个近似完全安全的传输环境。即在离散无记忆信道中，如果合法接收信道的质量优于窃听信道时，总会存在一个大于零的速率能够保证信息传输的完全安全性，即窃听者无法送收到的信号中获取任何信息。而这样的保密方式的码率存在一个上限，他把这个上限定义为保密容量。Leung则证明了AWGN信道的保密容量实际上就是合法信道的信道容量与窃听信道的信道容量之差[4]。在随后的研究中，这个结论被扩展到高斯窃听信道[4]、瑞利衰落信道[5]和广播信道[6]中。

如果主信道的信道容量不比窃听信道大，则不存在一个大于零的保密容量，因此，我们很难实现安全通信，并且现实生活中很容易出现这种情况。因此Casiszar将安全通信问题推广到一个更为一般的情况，即不需要窃听信道比主信道质量差，仍能保证安全通信[7]。之前的研究已经提出了很多方法[8,9]，其中一种可行的方法是在无线网络中应用友善的干扰节点。友善的干扰节点广播干扰信号，通过降低窃听信道的质量以使主信道优于窃听信道来提高信道的安全性。在此基础上，以恶化窃听信道信道条件为出发点的人工干扰技术成为国际上的研究热点。Carleial在文献[10]中讨论了Wyner模型的一个特地，即主信道无噪音，而文献[4]则考虑了AWGN的衰落窃听信道，证明了只有当主信道的信道容量大于窃听信道时才能保证非零的保密容量。另外，文献[11]研究了一种更普遍的情况，发送方将非保密信息广播传输给接收节点和窃听节点，而仅仅将保密信息发送给接收节点。

然而，我们需要注意的是，如文献[12,13]所述，主通道的传输质量并不总是优于窃听信道。因此我们需要解决这个问题，友善干扰节点传输人工噪音技术被认为是一个有效的方法，它通过向恶意窃听节点传送人为噪声降低窃听信道的信道质量来提高保密能力。而通过提高主信道传输质量的中继节点技术也被广泛研究。文献[9,14,15,16]就采用了这两种方法尝试最大化系统的保密容量。

* + 1. 干扰节点和窃听节点的协同

此外，中继节点技术也被广泛的研究。该技术就是在发送节点与接收节点之间增加了一个或多个中继节点，对发送节点传输的信号接收并转发给接收节点，即无线信号需要经过多次转发才能到达接收节点。以较简单的两跳中继为例，就是将一个发送-接收信道分割为发送-中继信道和中继-接收信道，从而可以把一个传输质量较低的信道替换为两个传输质量较好的信道，以获得更高的信道容量及更大的传输范围, 物理层安全技术中则通过提高主信道传输信号的质量来提高信道的保密容量。文献[14]引入了一个具有实际物理层网络编码方案的四终端中继-窃听信道，并且提出了几种中继节点相互合作的策略。在[15]中假设了一个双向中继网络，其中两个源节点通过放大和转发的中继节点相互发送消息。此外，他们还考虑了一个拥有多个中继节点的网络，并获得了最佳的中继方案。文献[16]也假设了一个存在窃听威胁的双向中继网络，通过对多个中继节点的相互影响进行研究，提出了三种不同的功率控制方案来最大化保密速率。文献[17]则研究了车联网并提出了一种用于存在多个源节点和中继车辆的VANET的中继车辆选择算法，并且建立了一个合作博弈模型以实现最大合作收益。文献[18]将物理层安全方法应用于车辆通信，并试图实现可靠的通信链路。文献[9]则考虑了一个具有多个中继的协作无线网络来提高安全性，他们提出了一个最佳的中继选择方案来防御窃听攻击并最大化保密能力。

在之前研究的基础上，单独的中继或者单独的干扰技术都是一种有效的方法，然而如何将它们结合起来使得两者的效率都显著提升也是一个很有价值的研究点。干扰节点通过降低窃听信道的信道质量来提高主信道的保密容量，而中继节点则通过提高主信道的信道容量来提高主信道的保密容量，它们通过不同的角度来达成相同的目的，因此它们可以相互合作而提高双方的效率。文献[19]提出了一个由两个信源组成的双向中继系统，一个是恶意窃听者，一个是中继节点，另一个是友好的干扰节点。它们提出了一种功率控制方案来实现主信道上的最大保密容量。而考虑到一些保密性约束，文献[8]研究了协作系统中的中继和干扰选择，最终提出了一种在实现最大保密容量的同时在干扰节点和非干扰节点之间切换的混合方法。文献[13]提出了一种通过对中间节点进行选择来增强通信安全性的方案。而文献[20]则研究了在协作中继和干扰的帮助下如何实现了无线自组网的安全协作通信，保密容量最大化问题被转化为一个优化问题，并提出一个算法来解决它。

虽然友善干扰节点技术被广泛用作一种可行的方法来提高系统的安全性，但恶意干扰节点也会存在于无线通信中[21,22,23]，这个问题不能被忽视。文献[22]研究了无线网络中存在一个试图干扰主信道信息传输过程的智能干扰节点，它能够在知道源节点传输功率的情况下调整自身的干扰功率来最大限度地发挥破坏效果。文献将干扰节点和源节点的功率控制问题看做一个优化问题进行研究，并将问题建模为斯塔科尔伯格博弈。文献[23]研究了CPS系统中移动终端的干扰攻击，这些攻击可能会降低通信质量。

* + 1. 博弈论在物理层中的应用

作为一种高效的数学分析工具，博弈论[24]被应用于研究智能决策者之间的相互作用作为一种有效的方法[25]，博弈论主要应用于经济学，政治学和心理学，以及逻辑学，计算机科学和生物学[26]。具有竞争或对抗性质的行为都可以称为博弈行为。在这类行为中，参加竞争的各方都拥有不同的目标。为了达到它们各自的目标，每个参与竞争的个体都必须考虑对手的各种可能的行动方案，并根据对手的方案选取相应的对自己最有利的相应行动方案。比如日常生活中的下棋，打牌等。博弈论就是研究博弈行为中是否存在一组对各方来说都是最合理的行动方案，以及如何找到这个合理的行动方案的数学理论和方法。最初，它的研究只涉及零和游戏，即其中一个人的收益必将导致其他参与者的损失。但是随着研究的深入，现在博弈论适用于各种行为关系，现在是人类，动物和计算机中逻辑决策科学的一个总称。

博弈论由三个要素组成：参与者、策略和收益。参与者是拥有决定自身策略的决定权。存在两个参与者的博弈被称为“双人博弈”，而存在多个参与者的博弈被称为“多人博弈”。策略则是参与者的的行为。在一场博弈中，参与者将会有一整套完整的行动计划，所有的参与者只会从它自身的策略组中选择一个相对最优的策略。而收益则是指在一场博弈中参与者的得失情况，每个参与者总是会想要最大化自身的收益，但是它们的收益并不仅仅和自身的策略有关，还有可能会被其他参与者的策略所影响，所以需要对自身的策略进行调整来得到更多。

博弈论可以分为很多类型。合作博弈是指由于外部的某些条件而使得某些参与者为了提高它们的收益不得不进行合作，而非合作博弈则是每个参与者都不可能进行合作，它们始终都是相互竞争的关系，比如零和游戏。静态博弈是所有参与者同时选择他们的策略，而动态游戏是指参与者的选择有先后顺序，并且后选择参与者会观察到先选择的参与者的策略，并据此来选择它自身的策略。

在大多数博弈中，它们都会存在均衡。纳什均衡就是一个非合作博弈的解决方案概念，其中包含两个或更多参与者，其中每个参与者被假定知道其他参与者的均衡策略，并且没有任何参与者能够通过仅仅改变它自身的策略而不影响其他参与者。当每个参与者都选择了一个策略，并且任何一个参与者都没有动力改变自身的策略，即无论如何变化都会降低自身的收益，那么当前的策略选择和相应的最大收益构成了纳什均衡，纳什均衡是博弈论中的基本概念之一。

博弈论作为一种研究独立博弈者之间复杂相互关系的有效数学工具，也被被广泛应用于通讯研究领域。

随着博弈论的应用，文献[27,28]研究了在干扰节点和中继节点帮助下如何对窃听节点进行防御。文献[29]研究了多输入多输出(MIMO)高斯瑞利衰落信道，在信道中有权访问信道的干扰节点可能会造成与未经通信许可的干扰节点一样多的损坏。文献[30]也研究了MIMO高斯信道并利用博弈论分析了MIMO广播信道和多址接入情况下高斯干扰的性质，得到了纳什均衡。文献[31]则在合作干扰的帮助下提供了可实现的保密率，使窃听者从观察中获得几乎为零的信息。

文献[32]在由单天线源节点、多天线目的节点和多天线窃听者组成的无线网络中，借助于全双工干扰节点的协作研究了最佳保密率。他们提出了一种新的自我保护方案来防御窃听并应用博弈论获得最佳的干扰协方差矩阵。文献[33]研究了合作干扰节点存在情况下的安全情况。通过对协作节点之间的关系进行建模并我们可以获得一组均衡协作干扰方案能够得到最大的总收益。[34]则应用了博弈论研究了源节点和友善干扰节点之间的相互作用，源节点需要付给干扰节点一定的收益，运用斯塔科尔伯格博弈对之间的关系进行了分析并求得均衡值。讨价还价的博弈[35]也被用来研究在合作的干扰节点的存在情况下下实现最大的保密能力。纳什谈判解决方案(NBS)被引入作为这个问题的有效方法，并且实现了基于NBS的方案。文献[36]则研究了一个使用分布式拍卖博弈的合作无线网络并基于博弈关系提出了一个基于拍卖的方案来提高保密容量。

本文应用的伯特兰德博弈和斯塔科尔伯格博弈。伯特兰德博弈描述了一个参与者的收益受其他参与者价格策略影响并且所有参与者的价格策略同步变化的系统。文献[37]在认知无线电网络中应用了伯特兰德博弈进行带宽分配和定价，最终得到一个称为伯特兰德均衡的最优结果，并通过仿真验证。斯塔科尔伯格博弈则描述了一个领导者首先选择策略的情况，追随者根据领导者的选择而选择最优的应对策略。文献[22]假设存在一个智能的干扰者，他可以在获知源节点的发射功率后，快速调整发射功率以最大限度地对主信道进行破坏。基于这个假设，他们研究了一个智能干扰器存在的最佳功率控制问题。问题被建模为斯塔科尔伯格博弈并最终求得了一个斯塔克尔伯格均衡。

文献[38]对可以应用于提高CPS系统网络安全性的博弈论框架进行了总结和分类。文献[39]选择了一个包含一个控制器、一个估计器和一个来自CPS的检测器的系统，提出了一个混合随机博弈模型来模拟这个系统，并提出了一个移动视界方法来求解这个博弈。文献[40]研究了一种无线供电网络，用户可以通过该网络向能源提交能量需求以获得其发射功率。在这个系统中，他们考虑一个窃取能量来干扰用户信息传输的恶意节点。然后，提出了一个博弈论模型来分析攻击者与用户之间的关系，最后设计了一个迭代算法来获得这个博弈的纳什均衡。

* 1. 研究内容及创新点

本文从提高无线网络传输安全性的角度，研究无线网络中各个节点的功率选择和控制问题。论文主要的主要工作如下：

1. 以往的大部分研究都优先考虑主信道的收益，而不是友善的干扰节点的收益。然而，移动设备在通信系统中扮演的角色并不固定。考虑到它们的流动性和自由性，它们可以自由的加入和退出通信系统并选择自己扮演的角色。因此，我们使用以干扰节点收益为主要考虑因素的通信模型，对各个节点的价格都自由变化的情况进行了研究，并使用了伯特兰德博弈来对问题进行分析来求得最大的干扰节点收益和相对最大的主信道保密容量。仿真结果表明干扰节点能够获得最大的收益。
2. 提出了一种干扰节点和中继节点合作的方法来对抗窃听节点。首先我们从多个中间节点中选择出一组最优的干扰-中继节点组，无论传输的功率以及价格如何变化，这一对干扰-中继节点组总是能够获得最大的保密容量。其次，我们对选定的节点组的传输策略进行了研究，不同于以往干扰节点和中继节点的价格都固定或成比例变化，我们给定它们可以自由的变化它们的策略，在此基础上对它们的价格、功率和它们之间的相互关系进行研究，并使用伯特兰德博弈分析它们之间的关系。仿真结果表明算法能够获得最大的中间节点收益和相对最大的主信道保密容量。
3. 我们考虑到干扰节点并不总是善意的而提出了干扰攻击和窃听攻击同时存在的情况下如何提高系统的安全性。由于恶意干扰节点是智能节点，它可以选择最佳的功率策略，以最大限度地降低主信道的信道容量，而窃听节点它的目的是最大限度的窃听到主信道的信息，考虑到它们之间目的的矛盾性，我们利用了它们之间的冲突来提高系统的保密容量。我们使用了斯塔科尔伯格博弈来分析干扰节点和传感器之间的策略关系，利用恶意干扰来对抗窃听攻击，最终得到一个最大的保密容量，并且恶意干扰节点也会认为它对主信道进行了足够大的干扰。仿真结果表明主信道的保密容量有了显著的提升。
   1. 本文组织结构

本文由五个章节组成，各个章节的主要内容如下：

第一章介绍了研究背景和意义，简述了国内外对于抗窃听攻击所提出的各种方法，重点对干扰节点技术和中继节点技术进行了分析介绍，并简要介绍了一下博弈论的应用。同时简单介绍了一下本文的研究方法和研究内容。

第二章我们研究了存在自私干扰节点的通信系统，它由源节点，目的节点，干扰节点和恶意窃听者组成。我们使用伯特兰德模型进行建模，研究如何在主信道取得最大保密容量的情况下，最大化自私干扰节点的收益。

第三章我们研究了干扰-中继节点组的最优选择策略，并研究了在选定干扰-中继节点组的情况下，如何对它们的价格和功率策略进行调整来获取最大的中间节点收益。

第四章我们研究了在干扰攻击和窃听攻击同时存在的情况下如何利用它们之间的冲突来提高系统的安全性。我们使用了斯塔科尔伯格博弈来对问题进行分析。

第五章对全文进行了总结并指出了未来可行的研究方向。

# 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[4](博士论文)。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[5]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[6]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[2]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[2], 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[72],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2-1所示：

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

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. 无线传感器网络异常数据检测

# 基于SPRT算法的无线传感网蠕虫节点检测方案

* 1. 引言

在无线传感器网络中，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[26]。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[23].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[1],[11],[15],[17],[22]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[8]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，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。

本章提出的基于SPRT的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1%-3%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[28],因此这个假设是非常合理的。根据文献[28]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. 基于SPRT的蠕虫节点检测方案

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。

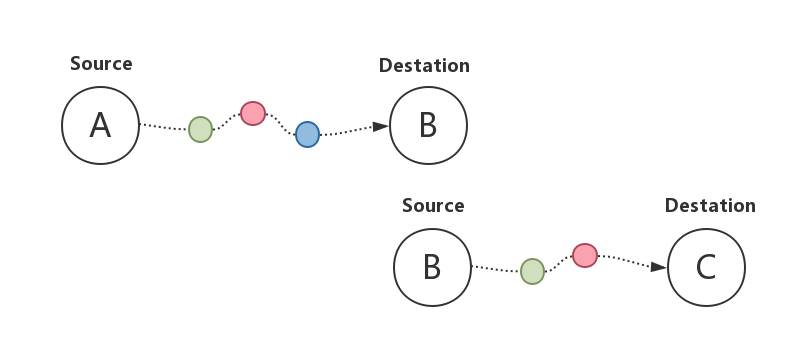


图3.1. 多跳通信模式和“链“通信模式示意图

**3.3.1** 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。

**3.3.2** 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[55,79]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，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w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) |

结合引入的随即参数可以改写为如式3-21所示：

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



**图 3.5. 和采样均值的关系**  **图3.6 值和的关系**

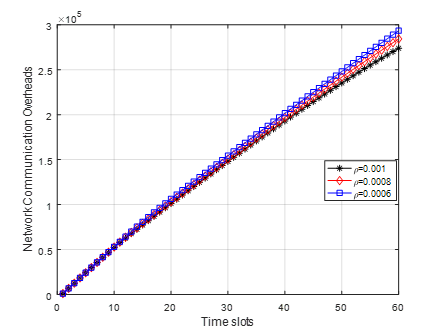
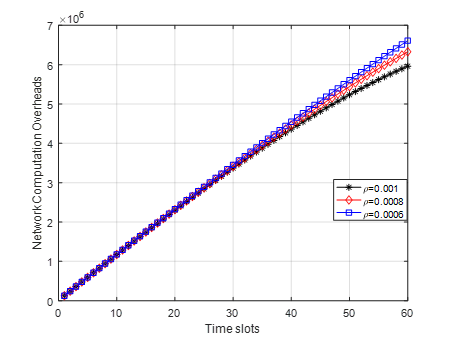


**图3.7 值和的关系**

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小越大SPRT算法所需要的决策样本数目就越少，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跟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，1000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1000个传感器节点分成20组，每一组50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以感染其他节点，文献[28]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样本数，平均采样样本数

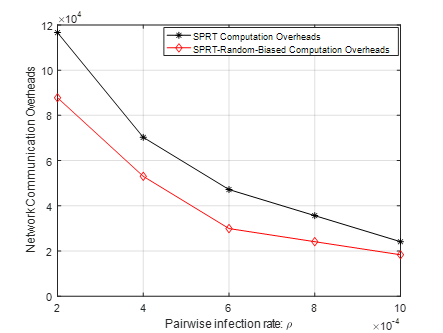
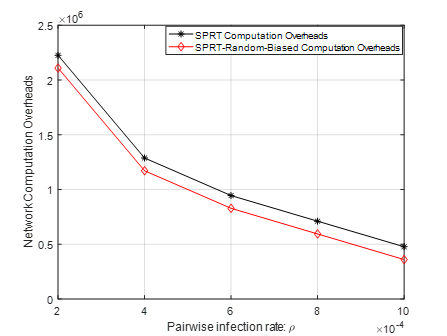
**ii** 检测到有蠕虫传播时所需要的时隙数，平均时隙数

**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**

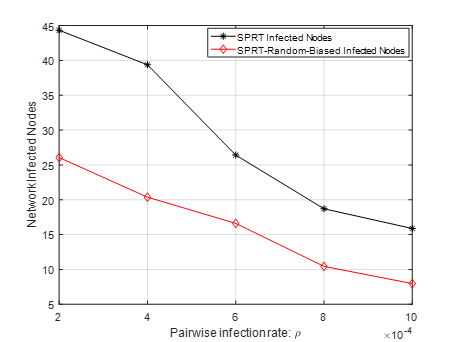
****

**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1%~3%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1%~3%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。

# 基于PCA算法的无线传感器网络异常数据检测方案

* 1. 引言

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，必须对非正常数据进行剔除。上一章中我们针对蠕虫节点进行检测剔除，文献[60]中针对移动节点进行剔除，文献[61]针对复制节点进行检测，文献[62]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，我们将重点放在由于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。基于以上原因，建立合适的异常数据检测模型对传感器网络中的数据进行监测，保证基站接收数据的可靠性，同时要尽可能保证消耗较小的能量以保证传感器网络的可用性至关重要[63]。

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[64]。因此检测异常数据最直观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[65],[66]详细地概述了无线传感器网络中的异常数据检测方案，主要包括以下几种类型的方案：基于统计模型的检测方案、基于聚簇的检测方案、基于最近邻居的检测方案、基于分类的检测方案，基于频谱分解的方案。然而这些所给出的方案普遍存在以下的缺点：一方面，这些方案很多是集中式的方案，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，所给出的方案往往不能保证数据检测率和传感器节点的能量令人满意的效果。

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[67]。通过坐标轴重新映射，PCA 算法将数据映射到最能代表数据分布的坐标轴上，在本文中通过计算第一主成分来近似代表数据的分布，我们提出一种新的检测方案，改进型分布式PCA异常数据检测方案(Improved Distributed PCA Outlier Detection,IDPCA)。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自身或者噪声引起的。通过拟合数据和伯克利实验室侦测的数据进行仿真分析，仿真结果说明我们所提出的方案能保证较高的异常数据检测率和较低的异常数据误报率，同时降低网络的整体通信负载。

本章的剩余部分如下所示：第二部分网络的结构假设，第三部分方案描述，第四部分性能分析，第五部分仿真实验。

* 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，我们详细介绍改进型分布式PCA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 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标准化为[0,1]区间上的值，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。矩阵的主成分可以通过对进行奇异值分解(SVD):

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

和都为正交矩阵。又矩阵的特征向量构成，代表矩阵的主成分分量值由的特征向量构成。定义为由矩阵的特征值由大到小排列的对角矩阵。矩阵的第一主成分分量定义为，然后节点计算所有测量向量值到第一主成分的投影距离,示意图如图4.2所示。

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

所有测量向量值到第一主成分的投影距离最大值定义为，最后我们使用三元组来定义异常数据检测模型。



图4.2 测量向量值到第一主成分的投影距离.

异常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 异常数据检测阶段**

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正确数据计算最大主成分分量和最大投影距离。接着每个节点将它的最大投影距离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投影距离计算全局最大投影距离，通常情况下该全局最大投影距离取的是各个节点最大投影距离的中位数。当一个新的数据向量到达节点 ,节点首先根据其三元组计算当前数据向量到第一主成分的距离，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，否则的话，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(4-5)所示:

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

根据式(4-5)，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。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 异常数据源检测阶段**

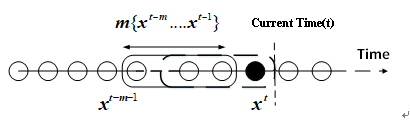
区分是何种原因引起了网络中的异常数据是一项非常重要的工作。无线传感器网络中，引起数据异常的原因主要包括以下几种：通信链路中的环境噪声、传感器内部节点错误、真实的事件发生和恶意攻击。本方案着重讨论如何区分异常数据是由简单的噪声或者内部错误引起还是由真实事件导致。主要思路如下：簇头节点中维护初始变量，当邻居节点监测数据为异常数据时,当所有邻居节点都检测完毕，如果,那么当前网络中有真实的事件发生(比如森林火灾发生时，会有一大批异常数据同时发生)。否则，当前的异常数据只是由单纯的噪声或者内部错误引起的，在这种情况下异常数据节点收集随之而来的个时隙窗口中的个数据向量，计算其到第一主成分分量的平均距离。如果，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。异常数据源的检测算法流程如表4.3所示:

**表4.3 无线传感器网络异常数据源检测**

|  |
| --- |
|  |

**4.3.4 模型更新阶段**

随着无线传感器网络部署环境的变化，监测数据实时变化，所以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，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。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**

根据以上分析，给出完整的IDPCA算法检测的伪代码如表4.4所示。

**表4.4 IDPCA算法伪代码**

|  |
| --- |
| 1. letbe the max projection distance from the first pc of node; |
| 2. letbe the median projection distance of ’s neighboring nodes’; |
| 3. letbe the median projection distance of the set ; |
| 4. letbe the amount of data measurements for learning theand first pc; |
| 5. letbe a new data measurement arrive at ; |
| 6. letbe the data vectors arriving at’s neighboring nodes at the same time interval |
| 7. let be the projection distance from the first pc at node in time windows t; |
| 8. let  be the median projection distance offrom their own first pc in time windows t; |
| 9. procedure learning and first pc  ①each node collects  data measurements for learning its own first pc and compute, then broadcasts the distance information to its group node ;  ②each group node computesand;  ③initiate IsOutlier(,) for each node;  return; |
| 10. procedure IsOutlier(,) for  when arrives at ,computes ;  if (>&&>)  indicates an outlier;  SourceOfOutlier(,,,) for;  else  indicates a normal one;  endif  return; |
| 11. procedure SourceOfOutlier(,,,);  ①collects the projection distance from its neighbor respectfully and compute the median projection distance;  ②if (>&&>)  if (>&&>)  may indicates an event;  else  may indicates an erroneous data measurement;  endif;  else  may indicates an erroneous data measurement;  endif;  return; |
| 12. procedure Updating global maximum projection distance using the newly m time windows |
|  |

* 1. 性能分析

在本节中我们讨论所给出模型的通信资源消耗和计算资源消耗，同时讨论异常数据源检测效果。

**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三元组之后将发送给簇头节点，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。如果数据向量没有通过全局异常检测即数据被检测为异常数据，假设这个概率为，那么启动异常数据源的检测。此时，各个邻居节点将发送至簇头节点，每个邻居节点增加1通信开销，簇头节点增加开销。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。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。

**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，这个过程的计算资源耗费为，最后在得到第一主成分之后需要计算值，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。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：。

**4.4.3 恶意事件源检测效率**

这一部分我们分析引起异常数据源为恶意事件的情形。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较小的数，否则传感器网络无法正常运行。我们假设异常数据检测率为，由4.3节可知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且引起异常的原因不是由于传感器内部节点或者噪声。假设节点之间的检测概率彼此独立，我们。。。。。待续分析



**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描述了三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分布式PCA方案和IDPCA方案下的，IDPCA异常数据检测模型下通信资源不受数据维度影响，拥有三种方案下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CPCA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。需要明白一点，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。

* 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。在无线传感器网络中，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高好。

**4.5.1 仿真环境设定**

I**拟合数据集仿真**

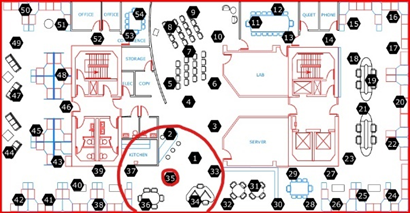
在拟合数据集合中我们以一组节点进行仿真分析，簇头节点拥有20个邻居节点，每个检测的数据为3维数据，每个维度的数据值服从高斯分布，方差为0.03，均值为(0.3,0.35,0.4)中的随机值。每个节点中的异常数据定义为某个维度上的数据值服从均匀分布，取值范围在[0.5,0.7]。我们选取四个时间窗口中的1000正常数据来训练异常检测模型，接着在每个时间窗口中选取200个正常数据值和50个异常数据值，分析每一个时间窗口中，检测模型的异常数据检测率和误报率。拟合的数据集合如图4.7所示。



**图4.7 训练数据集和待检测数据集**

**II 4.2 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。该网络每隔31秒收集一次数据，我们的仿真数据来源于图4.8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。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，2月29号到3月3号的检测数据进行检验。因为IBRL数据集中的收集数据都是正常数据，为了更好的评估模型的性能，我们随机选取1000个数据向量，对其温度值加上值进行仿真实验，在很多文献中都有这一操作。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4.8 IBRL无线传感器网络模型**

**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异常数据检查测模型的异常数据检测率和误报率随时间窗口的变化，接着讨论实际环境中不同方案的性能比较。



**图4.9 拟合数据集下IDPCA异常数据检测率 图4.10 拟合数据集下IDPCA数据误报率**

****

**图4.11 IBRL数据集合下异常数据检测率对比 图4.12 IBRL数据集合下异常数据误报率对比**

# 参考文献

[1] 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

[2] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. Wireless sensor networks : a survey. Computer Networks 38(4):393–422, March 2002

[3] Jun-Won, H., et al. (2009). Fast Detection of Replica Node Attacks in Mobile Sensor Networks Using Sequential Analysis. 28th Annual IEEE International Conference on Computer Communcations (INFOCOM).

[4] 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.

[5] 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.

[6] J. Jung, V. Paxon, A.W. Berger, and H. Balakrishnan. Fast port scan detection using sequential hypothesis testing. In IEEE Symposium on Security and Privacy, Pages:211–225, May 2004

[7] M. Xie, H. Yin, and H. Wang. An effective defence against email spam laundering. In ACM CCS, Pages:179–190, October 2006.

[8]Krikidis I, Thompson J S, Mclaughlin S. Relay selection for secure cooperative networks with jamming[J]. IEEE Transactions on Wireless Communications, 2009, 8(10):5003-5011.

[9]Zou Y, Wang X, Shen W. Optimal Relay Selection for Physical-Layer Security in Cooperative Wireless Networks[J]. IEEE Journal on Selected Areas in Communications, 2013, 31(10):2099-2111.

[10]Carleial A B, Hellman M E. A note on Wyner''s wiretap channel[J]. IEEE Transactions on Information Theory, 1977, 23(3):387-390.

[11] 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

[12]Hui H, Swindlehurst A L, Li G, et al. Secure Relay and Jammer Selection for Physical Layer Security[J]. IEEE Signal Processing Letters, 2015, 22(8):1147-1151.

[13]Chen J, Zhang R, Song L, et al. Joint Relay and Jammer Selection for Secure Two-Way Relay Networks[J]. IEEE Transactions on Information Forensics & Security, 2012, 7(1):310-320.

[14]Lai L, Gamal H E. The Relay–Eavesdropper Channel: Cooperation for Secrecy[J]. IEEE Transactions on Information Theory, 2008, 54(9):4005-4019.

[15] A.-R. Sadeghi, S. Schulz, and C. Wachsmann, ‘‘Lightweight remote attestation using physical functions,’’ in Proc. ACM WiSec, Jun. 2011, pp. 109–114

[16]Wang H M, Yin Q, Xia X G. Distributed Beamforming for Physical-Layer Security of Two-Way Relay Networks[J]. IEEE Transactions on Signal Processing, 2012, 60(7):3532-3545.

[17] A. Seshadri, A. Perrig, L. van Doorn, and P. Khosla, ‘‘SWATT: SoftWarebased attestation for embedded devices,’’ in Proc. IEEE Symp. Secur.Privacy, May 2004, pp. 272–282

[18]Cho W. Physical Layer Issues in Vehicular Communications[J]. Journ. Korea Inst. Electron. Commun. Sci, 2012, 7(5):1229-1234

[19]Zhang R, Song L, Han Z, et al. Physical Layer Security for Two-Way Untrusted Relaying With Friendly Jammers[J]. IEEE Transactions on Vehicular Technology, 2012, 61(8):3693-3704.

[20]Han B, Li J, Su J, et al. Secrecy Capacity Optimization via Cooperative Relaying and Jamming for WANETs[J]. Parallel & Distributed Systems IEEE Transactions on, 2015, 26(4):1117-1128.

[21]Rawat R, Sharma D. Impact of jamming attack in vehicular ad hoc networks[J]. Int. Journ. Adv. Res. Comput. Commun. Eng, 2015, 4(4):457-461.

[22] Y. Yang, X. Wang, S. Zhu, and G. Cao, ‘‘Distributed software-based attestation for node compromise detection in sensor networks,’’ in Proc. IEEE SRDS, Oct. 2007, pp. 219–230

[23] 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.

[24]Fudenberg D, Tirole J. Game Theory[J]. Mit Press Books, 2010, 1(7):841-846.

[25]Gibbons, Robert. A primer in game theory[M]// A primer in game theory /. Harvester Wheatsheaf, 1992.

[26] 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

[27]Chen H, Li Y, Jiang Y, et al. Distributed Power Splitting for SWIPT in Relay Interference Channels Using Game Theory[J]. Wireless Communications IEEE Transactions on, 2015, 14(1):410-420.

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

[29]Kashyap A, Basar T, Srikant R. Correlated jamming on MIMO Gaussian fading channels[C]// IEEE International Conference on Communications. IEEE, 2004:458-462 Vol.1.

[30]Brady M H, Mohseni M, Cioffi J M. Spatially-Correlated Jamming in Gaussian Multiple Access and Broadcast Channels[C]// Information Sciences and Systems, 2006, Conference on. IEEE, 2006:1635-1639.

[31]Tekin E, Yener A. The General Gaussian Multiple-Access and Two-Way Wiretap Channels: Achievable Rates and Cooperative Jamming[J]. IEEE Transactions on Information Theory, 2008, 54(6):2735-2751.

[32]Zheng G, Krikidis I, Li J, et al. Improving Physical Layer Secrecy Using Full-Duplex Jamming Receivers[J]. IEEE Transactions on Signal Processing, 2013, 61(20):4962-4974.

[33]Tekin E, Yener A. The Gaussian multiple access wire-tap channel: wireless secrecy and cooperative jamming[J]. 2007, 54(12):404-413.

[34]Han Z, Marina N, Debbah M, et al. Physical Layer Security Came: How to Date a Girl with Her Boyfriend on the Same Table[C]// International Conference on Game Theory for Networks, 2009. Gamenets. IEEE, 2009:287-294.

[35]Duan B, Cai Y, Zheng J, et al. Cooperative jammer power allocation — A Nash bargaining solution method[C]// International Conference on Wireless Communications & Signal Processing. IEEE, 2015:1-6.

[36]Zhang R, Song L, Han Z, et al. Improve physical layer security in cooperative wireless network using distributed auction games[C]// Computer Communications Workshops. IEEE, 2011:18-23.

[37]Martyna J. Oligopoly Bertrand model for price competition in cognitive radio networks[C]// International Symposium on Communication Systems, Networks & Digital Signal Processing. IEEE, 2014:227-231.

[38]Roy S, Ellis C, Shiva S, et al. A Survey of Game Theory as Applied to Network Security[C]// Hawaii International Conference on System Sciences. IEEE, 2010:1-10.

[39]Miao F, Zhu Q. A moving-horizon hybrid stochastic game for secure control of cyber-physical systems[C]// Decision and Control. IEEE, 2015:517-522.

[40]Niyato D, Ping W, Dong I K, et al. Game theoretic modeling of jamming attack in wireless powered communication networks[C]// IEEE International Conference on Communications. IEEE, 2015.

[41]Kapetanovic D, Zheng G, Rusek F. Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks[J]. Communications Magazine IEEE, 2015, 53(6):21-27.

[42]Brown A, Pearcy C. An introduction to analysis /[M]. Springer-Verlag, 1995.

[43]Granville V, Krivanek M, Rasson J P. Simulated annealing: a proof of convergence[J]. IEEE Transactions on Pattern Analysis & Machine Intelligence, 2002, 16(6):652-656.

[44]Kirkpatrick S, Jr G C, Vecchi M P. Optimization by simulated annealing.[J]. Readings in Computer Vision, 1983, 220(4598):606-615.

[45]Malatras A, Coisel I, Sanchez I. Technical recommendations for improving security of email communications[C]// International Convention on Information and Communication Technology, Electronics and Microelectronics. IEEE, 2016:1381-1386.

[46]Abdallah W, Hamdi M, Boudriga N. A public key algorithm for optical communication based on lattice cryptography[C]// Computers and Communications, 2009. ISCC 2009. IEEE Symposium on. IEEE, 2009:200-205.

[47]Wang T, Giannakis G B. Mutual Information Jammer-Relay Games[J]. IEEE Transactions on Information Forensics & Security, 2008, 3(2):290-303.

[48]Liu W, Tan D, Xu G. Low complexity power allocation and joint relay-jammer selection in cooperative jamming DF relay wireless secure networks[C]// IEEE International Conference on Anti-Counterfeiting, Security and Identification. IEEE, 2013:1-5.

[49]Li L, Yu L. Pricing models based on Bertrand game under Dual-channel Environment[C]// International Conference on Business Management and Electronic Information. IEEE, 2011:669-672.

[50]Bletsas A, Shin H, Win M Z. Cooperative Communications with Outage-Optimal Opportunistic Relaying[J]. IEEE Transactions on Wireless Communications, 2007, 6(9):3450-3460.

[51]Lee S, Han M, Hong D. Average SNR and ergodic capacity analysis for opportunistic DFrelaying with outage over rayleigh fading channels[J]. IEEE Transactions on Wireless Communications, 2009, 8(6):2807-2812.

[52]Mariappan R, Reddy P V N, Wu C. Cyber Physical System Using Intelligent Wireless Sensor Actuator Networks for Disaster Recovery[C]// International Conference on Computational Intelligence and Communication Networks. IEEE, 2016:95-99.

[53]Gungor V C, Hancke G P. Industrial Wireless Sensor Networks: Challenges, Design Principles, and Technical Approaches[J]. IEEE Transactions on Industrial Electronics, 2009, 56(10):4258-4265.

[54]Zhang Y, He S, Chen J. Data gathering optimization by dynamic sensing and routing in rechargeable sensor networks[C]// Sensor, Mesh and Ad Hoc Communications and Networks. IEEE, 2013:273-281.

[55] 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

[56]Orojloo H, Azgomi M A. Evaluating the complexity and impacts of attacks on cyber-physical systems[C]// Real-Time and Embedded Systems and Technologies. IEEE, 2016:1-8.

[57]Yue J, Yang B, Guan X. Fairness-guaranteed pricing and power allocation with a friendly jammer against eavesdropping[C]// International Conference on Wireless Communications & Signal Processing. IEEE, 2013:1-6.

[58]Kim T S, Kim S L. Random power control in wireless ad hoc networks[J]. IEEE Communications Letters, 2005, 9(12):1046-1048.

[59] 1. Shahid, N.: Energy efficient outlier detection in WSNs based on temporal and attribute correlations. In: 7th International Conference on Emerging Technologies, pp. 1-6. IEEE, Islamabad (2011).

[60] 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.

[61] Jun-Won, H., et al. (2009). Fast Detection of Replica Node Attacks in Mobile Sensor Networks Using Sequential Analysis. 28th Annual IEEE International Conference on Computer Communcations (INFOCOM).

[62] 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.

[63] Ghorbel, O., Snoussi, H.: A Novel Outlier Detection Model Based on One Class Principal Component Classifier in Wireless Sensor Networks. In: 29th International Conference on Advanced Information Networking and Applications, pp. 70-76. IEEE, Gwangiu (2015).

[64] Zhang, Y., Meratnia, N., Havinga, P.: Adaptive and Online One-Class Support Vector Machine-Based Outlier Detection Techniques for Wireless Sensor Networks. In: International Conference on Advanced Information Networking and Applications Workshops, pp. 990-995. IEEE, Bradford (2009).

[65] Zhang, Y., Meratnia, N., Havinga, P.: Outlier Detection Techniques for Wireless Sensor Networks: A Survey. IEEE Communications Surveys & Tutorials 12(2), 159-170(2010).

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

[67] Ahmadi, M., Abadi, M.: An energy-efficient anomaly detection approach for wireless sensor networks. In: 5th International Symposium on Telecommunications, pp.243-248. IEEE, Tehran (2010).

[68] V. Chatzigiannakis and S. Papavassiliou, "Diagnosing anomalies and identifing faulty nodes in sensor networks," IEEE Sensors Journal, vol. 7, no. 5, pp.637-645, May 2007

[69] Livani, M. A. and M. Abadi (2011). A PCA-based distributed approach for intrusion detection in wireless sensor networks. 2011 International Symposium on Computer Networks and Distributed Systems (CNDS).

[72] A. Wald. Sequential analysis. Dover Publications, 2004

[79] Y. Yang, X. Wang, S. Zhu, and G. Cao. Distributed software-based attestation for node compromise detection in sensor networks. In IEEE SRDS, Pages:219–230, October 2007

# 附录1 攻读硕士学位期间撰写的论文

(1)L. Yuan, K. Wang, T. Mizayaki, S. Guo, and M. Wu, ”Optimal transmission strategy for sensors to defend against eavesdropping and jamming attacks”, Proc. 2017 IEEE ICC, pp. 1-6, Jul. 2017.；

# 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。

# 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王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，而王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。感谢教研室的立秋、糜俊等同学，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。感谢我的室友王星、周昊、周祺华和金俊杰在生活中对我的帮助，和你们一起生活的时光非常开心。感谢我的小伙伴薛四猛、朱琦、金石、顾焕钊、马悦和赵莲在我遇到困难挫折时候对我的安慰和鼓励。还要感谢卢卢在我迷茫的时候对我的陪伴，给了我战胜困难的勇气。

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。