申请上海交通大学硕士学位论文

基于无线传感器网络的分布式估计及安全机制设计

论文作者 米 士 超

学　　号 1120329048

指导教师 关新平 教授

专　　业 控制科学与工程

答辩日期 2015 年 1 月 16 日

Submitted in total fulfilment of the requirements for the degree of Master in Control Science and Engineering

Distributed Estimation and Security Mechanisms for Wireless Sensor Networks

Shichao Mi

Supervisor

Prof. Xinping Guan

Department of Automation

School of Electronic, Information and Electrical Engineering

Shanghai Jiao Tong University

Shanghai, P. R. China

Jan. 16th, 2015

上海交通大学
学位论文原创性声明

本人郑重声明：所呈交的学位论文，是本人在导师的指导下，独立进行研究工作所取得的成果。除文中已经注明引用的内容外，本论文不包含任何其他个人或集体已经发表或撰写过的作品成果。对本文的研究做出重要贡献的个人和集体，均已在文中以明确方式标明。本人完全意识到本声明的法律结果由本人承担。

学位论文作者签名：米士超

日　期：2015 年 1 月 16 日

上海交通大学
学位论文版权使用授权书

本学位论文作者完全了解学校有关保留、使用学位论文的规定，同意学校保留并向国家有关部门或机构送交论文的复印件和电子版，允许论文被查阅和借阅。本人授权上海交通大学可以将本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和汇编本学位论文。

保　密□，在_____年解密后适用本授权书。

本学位论文属于

不保密☑。

（请在以上方框内打“✓”）

学位论文作者签名：朱士超　　指导教师签名：

日　期：2015年1月16日　　日　期：2015年1月16日

基于无线传感器网络的分布式估计及安全机制设计

摘 要

无线传感器网络由于具有成本低、易于部署、自组织等特点受到了广泛的关注，并在军事、环境、家居和工业监测等方面得到很好的应用。由于传感器节点大多部署在开放的环境中，很容易受到来自外部环境或者恶意的攻击，加之节点自身的存储能力、计算能力以及能量等资源的限制，使无线传感器网络的轻量级安全机制设计面临很大的挑战。

无线传感器网络中的典型攻击包括：通过扰乱路由信息，导致信息无法正常传输降低网络性能；通过大量消耗节点的能量造成网络瘫痪；通过数据篡改影响传感器节点的感知结果。论文针对网络中的数据篡改攻击，设计确保网络感知精确度的安全防御机制，并针对入侵检测问题，提出了基于移动传感器网络的安全防护方法，具体的研究成果简述如下：

（1）无线传感器网络的分布式估计及其安全机制设计。本文针对无线传感器网络中的数据篡改攻击，尤其是隐蔽的恶意数据注入攻击，基于加权平均一致性方法设计了分布式安全机制。传感器节点在感知过程中，根据邻居节点的感知数据与自身数据的差值与预先设定的阈值做比较，以此来检测恶意节点，并对其余的节点基于加权平均算法进行一致性估计以得到准确的感知数据，数值仿真表明该算法可以有效地抵御数据篡改攻击。

（2）异构传感器网络的分布式估计及其安全机制设计。本文针对大规模无线传感器网络，设计了由传感器感知主节点与中继节点组成的异构传感器网络的分布式一致性安全算法。该算法通过阈值检测网络中的恶意节点，在一致性算法中，通过调节相关参数，来自适应地调节传感器节点在算法中所占的权重。该算法既避免了误判精度较低的节点为恶意节点，同时提高了无线传感器网络一致性估计的安全性。

（3）基于移动无线传感器网络的入侵搜索与安全防护。论文针对诸如大型场馆等室内环境的入侵检测问题，利用移动传感器网络来对入侵者进行跟踪和捕获。由于室内环境中存在障碍物，移动传感器节点的移动速度受限。论文利

用图论方法构建拓扑图，通过树分解得出了一个能够成功围捕入侵者所需的最少传感器节点的数量，并设计了一种基于树分解的围捕策略，以确保对入侵者的捕获。

关键词： 无线传感器网络 分布式估计 安全机制 数据篡改攻击 图搜索

Distributed Estimation and Security Mechanisms for Wireless Sensor Networks

ABSTRACT

With features of low-power, low-cost, easy to deploy and self-organization, wireless sensor networks (WSNs) have been widely used monitoring of sensitive information in diverse fields such as military, environment, household and industrial. But a wireless sensor network is vulnerable since it is deployed in harsh environments. In addition, WSNs suffer from a lot of constraints, including small memory, low computation capability and limit energy source. Thus, secure wireless sensor network is facing great challenges.

Attacks in wireless sensor networks include the following common situation. The attacker may disrupt routing protocols to reduce network performance, or consume a large of network energy to make the network paralysis, or inject false data to change the final result. In this thesis, we deal with the secure problems of distributed consensus of WSNs and we study the security of the monitored environment for WSNs. We focus on the following three challenging works.

1. A secure distributed consensus scheme for wireless sensor networks. Considering data falsification attack, especially covert false data injection attacks, we present a distributed detection mechanism in which sensor node compare deviation with the threshold to detect abnormal nodes is presented. And a weighted averaging consensus scheme is proposed. Simulation results illustrate the effective of the proposed secure scheme.

2. A distributed consensus-based secure scheme for heterogeneous sensor networks. For large-scale field environment, we consider a heterogenous WSNs composed of two types of sensors: sensor nodes and relay nodes. A asymptotically unbiased consensus scheme with adaptive local consensus parameters is proposed. The algorithm

allows lower precision nodes to attend the consensus while improves the security of the network.

3. Indoor intrusion detection and security for mobile wireless sensor networks. Mobile sensor networks can complete dangerous task instead of human beings. There are obstacles in indoor environment, the speed of sensor nodes is limited. By using the concepts of graph theory, the indoor environment dispersed into finite graph. We establish an upper bound of sensor nodes that can capture the intruders. A hunting strategy based on tree decomposition is proposed to ensure the safety of the indoor environment.

KEY WORDS: Wireless Sensor Networks, Distributed Estimation, Security Mechanism, Data Falsification, Graph Search

目　　录

插图索引

第一章 绪论

1.1 研究背景及意义

无线传感器网络（Wireless Sensor Networks，简称 WSNs）的出现为人类感知世界提供了新的工具。近年来，随着微机电系统、无线通信技术、传感器技术和现代网络等技术的迅速发展，无线传感器网络得以迅速发展并引起了广泛关注 [1–3]。无线传感器网络作为一种新的信息获取以及信息处理技术，融合了数据采集、分布式处理、嵌入式计算和无线通信技术等，极大地扩展了信息获取的能力，将物理世界、计算机世界与人类社会联系起来，为人们提供最真实、最有效、最直接的信息。

无线传感器网络是由不同类型的传感器节点组成的网络系统，这些传感器节点部署在监测区域，以协作的方式对周围的环境进行实时地监测和感知，并对所采集的信息进行处理，然后通过相应的网络协议来实现数据传输和信息融合。传感器节点具有低成本、易于部署、自组织性等特点，可以在危险区域、恶劣环境以及边远地区等不适合人工操作的地区进行监控，完成战场监测、定位、工业监控等任务，具有广泛的应用前景，在军事国防、智能交通、工业生产、环境监测、现代农业、智能家庭等很多领域都有潜在的应用价值 [4–8]。

与传统的网络相比，无线传感器网络具有低成本、扩展性强、高度灵活性等特点 [9]，有着巨大的优势和发展前景。由于传感器节点一般部署在开放的甚至是比较恶劣的环境中，很容易受到恶意干扰或者攻击。另一方面，传感器节点由于自身计算能力不高、存储容量有限、电池能量有限等因素，无法加载类似防火墙的安全防护手段和协议。如果传感器网络受到了攻击，错误的数据可能导致网络信息的泄漏或者使网络得到错误的结果，引起严重的后果，因此无线传感器网络的安全机制设计问题尤为重要。

鉴于无线传感器网络中的安全机制设计的重要性，本文面向传感器网络的感知功能需求，设计了基于一致性算法的安全机制。并基于移动传感器网络研究了入侵检测安全防护问题，分别以恶意节点的检测和分布式安全估计（感知算法）为研究切入点，以提高网络的安全性、降低网络整体感知数据的差异并降低数据计算冗余性为目标，同时减少节点之间不必要的数据通信为目标，以

节省网络能量。论文的研究工作不仅面向网络感知能力的提升设计了具体的安全机制，而且为无线传感器网络技术的具体应用提供了重要的技术支持，因此，具有非常重要的理论指导意义和实际应用价值。

1.2 无线传感器网络概况

无线传感器网络被认为是二十一世纪最重要的新兴技术之一，其发展和应用有着广泛的前景。大量的传感器节点通过人工放置、飞行器撒播或者火箭弹射等方式随机散落在被监测区域内部或者附近，而后节点以自组织的方式构成网络。如果监测区域有事件发生，传感器节点将感知到的数据，通过多跳的方式，并借助临时建立的链路传送给终端。

无线传感器网络主要包括传感器节点、汇聚节点以及管理节点。每个传感器节点主要由四个基本部分组成：传感器单元、数据处理单元、通信单元以及电池单元，有些传感器节点可能包含额外的应用相关的组件，例如发电机、定位装置或者移动装置等，如图 1–1所示。传感器单元通常由传感器和模数转换器（ADC）组成。模数转换器将传感器感知的模拟信号转化为数字信号。数据处理单元通常包含一个小的存储器用来管理该传感器节点与网络中其它节点的协作。通信单元使得节点与网络连通。电池单元是传感器节点中非常重要的一部分，为其它各个部分提供能源，而电池的能量是有限的。大部分传感器网络应用中的路由技术或者感知任务需要位置信息，因此传感器节点中可能包含一个定位装置，另外有些应用中需要传感器的移动来完成任务，因此有些传感器节点包含移动装置。

传感器节点的协议在传感器节点中的应用很多，其中在物理层、数据链路层、网络层、传输层和应用层中的主要作用如下：

- 物理层：负责选频，产生载波频率，信号的偏转，调制和数据加密；
- 数据链路层：负责数据帧检测，数据流复用，媒体访问和错误控制，并保证可靠的点到点、点到多点的传输；
- 网络层：负责数据包的转发和地址分配；
- 传输层：负责数据包的可靠传输；
- 应用层：负责数据如何请求，为传感器节点和用户终端之间提供服务。

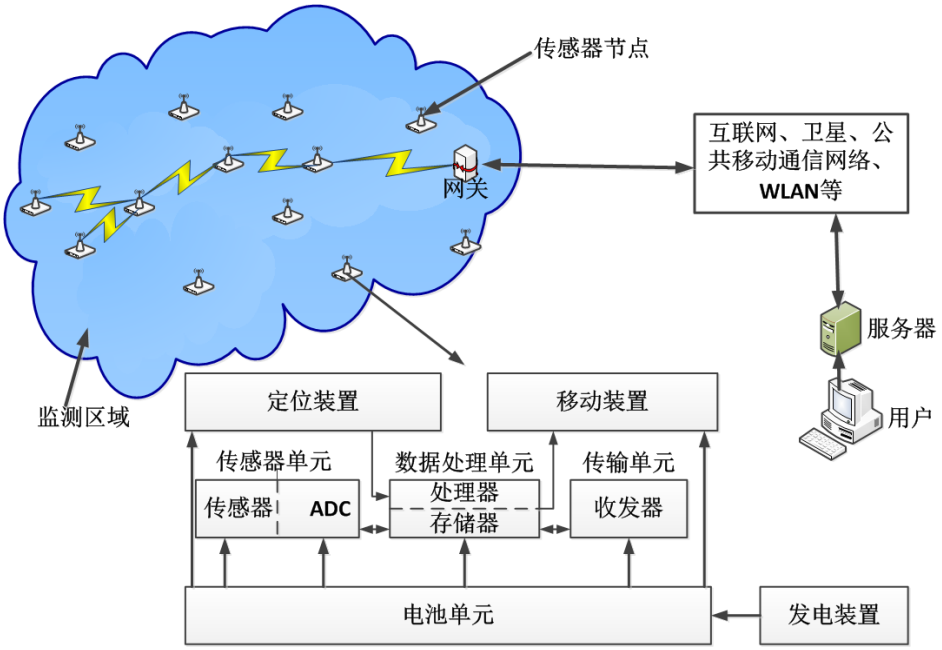


图 1–1: 无线传感器网络结构

Fig 1–1: Structure of WSNs

1.2.1 无线传感器网络的特点

无线传感器网络是一种基于应用的网络 [10]，除了有自组网络的一般特性外，还有自身的一些特点：

- 节点数量多，分布密集。为了对一个区域进行准确的监测，一方面通常需要大量的传感器节点部署到该区域，数量之多可能达到成千上万；另一方面传感器节点部署比较密集，使得网络具有强连通性，保证了监测区域网络的抗毁性。

- 自组织。无线传感器网络中，网络的布设以及自组织不需要依赖其他的网络设备，传感器节点通过拓扑控制机制、分层协议、分布式算法等各自协调行为，这样节点可以自动地快速组成无线网络。

- 动态拓扑。无线传感器网络中的节点可能因为故障或者电池电量用完而退出网络，也可能因为一些需求而被添加到网络中，这都会使网络的拓扑发生变化。另外无线通信链路的变化也会引起网络拓扑的变化，因此无线传感器网络具有动态的可重构性。

- 无中心。由于无线传感器网络中所有的节点都是随机部署的，所有的节点既是感知节点又是小的融合中心，是一个对等的网络。每一个节点知道自己以及邻居节点的信息，可以利用相邻节点之间的通信以及协作来完成信号的处理以及通信，具有很好的协作性。

- 节点资源有限。传感器网络在应用中通常是大规模部署，而且成本较低，能量受限，计算能力、通信能力以及电池能量有限。

- 安全问题突出。由于传感器网络一般部署在未受保护的区域，传感器节点自身资源受限，又采用无线多跳的通信方式，使得节点很容易被攻击者捕获或者对感知数据进行篡改，使网络暴露在多种类型的攻击下，降低网络的安全性能。

无线传感器网络的上述特点降低了数据传输的安全性。例如由于传感器节点体积小、低成本、资源有限、无线信道通信等，使得 WSNs 更容易受到拒绝服务的攻击。无线传感器网络中的攻击通过扰乱路由信息降低网络性能；或者通过大量消耗网络的能量造成网络瘫痪；或者通过数据篡改影响网络的最终结果。如果传感器网络部署在恶劣的环境中或者敌对的环境中，信息的传输过程中会出现阴影衰落、多径衰减等不可避免的因素，这就使得网络获取的信息不准确，如果将这些数据传给用户，可能造成非常严重的后果。因此，我们需要对节点获得的数据进行一定的处理，通过节点间的协同合作来获得对环境准确的一致性描述，并设计相应的安全机制来抵御恶意节点的攻击，保障网络感知数据的安全性。

1.2.2 无线传感器网络分布式估计

无线传感器网络的估计问题可以分为基于集中式估计和分布式估计两类。集中式估计中，通常网络中存在一个信息处理能力很强的数据融合中心，所有的数据汇集到融合中心后，融合中心对其进行处理，得出用户所需要的数据。分布式估计中的节点都是对等的，每个节点通过与邻节点进行通信，对数据进行局部处理，通过迭代的方式完成对状态的估计。相比与集中式估计，分布式估计具有更好的鲁棒性和可扩展性。近年来，分布式一致性问题受到了学者的广泛关注，并涌现出很多的研究，比如基于多智能体系统框架 (Multi-agent System) 的蜂拥和集群控制 [11–13]、编队控制 [14, 15]、覆盖控制 [16] 等。

分布式估计中，网络中的每个节点都作为一个小的数据处理中心，对感知信息进行处理。网络中的每个节点对周围环境进行感知，并将感知到的数据发送给邻居节点，每个节点对这些信息进行相应的处理，得到自身的一个估计结果。分布式估计不需要所有的节点都将信息发送给融合中心，整体上减少了系统能耗，延长了网络的寿命。另外，采用分布式的估计方式，提高了网络的可靠性，通过把工作负载分散到网络，当一个节点故障时，其它节点不会受到影响。

1.2.3 无线传感器网络中的安全问题

由于传感器节点大多数部署在开放的环境中甚至是敌方区域，很容易被攻击者进行攻击，因此传感器网络的安全问题亟待解决。网络攻击通过扰乱路由信息，降低网络的性能，或者通过大量消耗网络的能量造成网络瘫痪，或者通过数据篡改影响网络的最终结果。加之传感器网络的一些特点使得其安全问题的研究具有相当的复杂性，如传感器节点的资源限制使跳频扩频、对称密钥加密等能量消耗大的安全机制不适用；无线多跳通信的特点使得一些攻击方式如窃听、干扰等更加容易实施。另外，网络中缺乏有效的安全机制是阻碍传感器网络应用的主要因素。而最常见的分类方式是按照协议栈层次，下面按照网络协议栈层次对攻击方式进行分析：

- 物理层攻击

  1）拥塞攻击（Jamming attack）。网络传输中，节点在发送和接收数据时在同一频段上进行通信，如果两个节点在同一频段同时发送信号，会引起信号干扰，使两个发送端均无法正常可靠地发送数据。拥塞攻击中攻击者利用该特点，在传感器节点周围发射功率较强的无线电波，对正常的通信进行干扰 [17]，破坏网络正常的通信能力，如图 1–2所示。在单频段的通信中，该攻击非常有效。

  2）数据篡改。由于大多数无线传感器网络部署在开放的环境中，传感器节点暴露在外面，而且节点的安全机制有限，其脆弱性使得攻击者可以轻易的俘获节点，并对节点的感知信息进行篡改，或者对其植入恶意代码使传感器节点变为恶意节点，并进行进一步的攻击。

  3）耗尽攻击。恶意节点持续不断的向网络中发送数据包，消耗所有转发

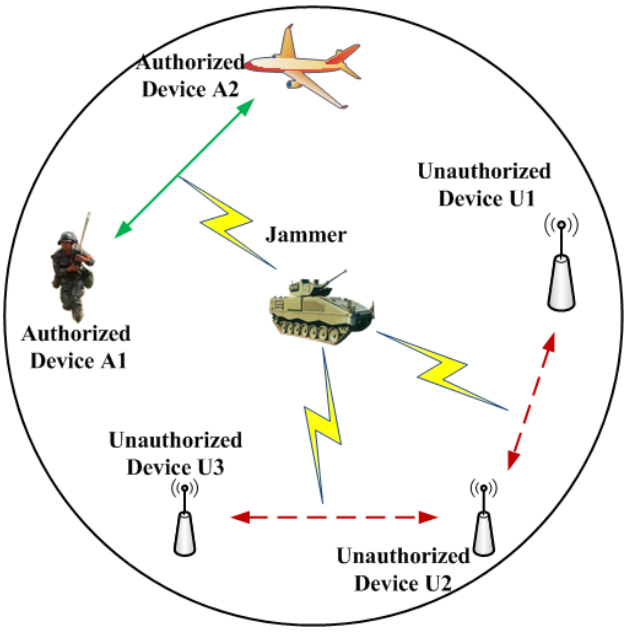


图 1–2: 拥塞攻击

Fig 1–2: Jamming attack

和接收该数据包的节点的能量，使其一直处于忙碌的接收转发中直至能量耗尽。

- 网络层攻击。

1）拒绝服务（Denial of Sevice，简称 DoS）攻击。DoS 攻击中攻击者通过发送恶意数据，引起多余的网络流量，这会对网络带来两方面的影响[18]。一方面，恶意的网络流量会抢占信道，造成网络堵塞并严重影响数据的正常传输；另一方面大量恶意网络流量的传输使节点一直出于工作状态，扰乱节点的正常休眠，减小了网络寿命。另外，该攻击方式可以与其它攻击方式联合，比如拥塞攻击等，扩大对网络的破坏力。DOS 攻击示意图如 1–3所示。

2）路由信息篡改攻击。攻击者通过对网络的监听，篡改和伪造路由信息表从而影响网络中数据的传输路径。虚假的路由信息会延长正常的信息传输路径，或者会造成环状路由，导致信息无法正常到达基站，而且造成网络中大量的能量耗费，甚至使网络瘫痪。

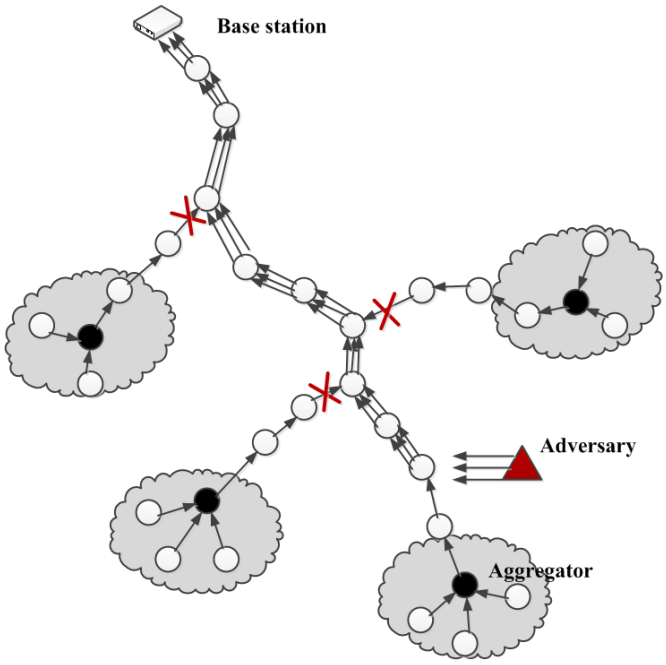


图 1–3: 拒绝服务攻击

Fig 1–3: Dos

3）选择转发攻击。攻击者对接收到的数据进行选择性的转发，而丢掉其它的部分。最常见的选择性转发方式有两种：一种是随机转发，即攻击者按照一定的概率丢掉其所接收到的数据包；另一种是攻击者丢弃掉所有接收到的数据包。如果网络中的关键节点遭到攻击，将会对网络造成明显的破坏。

4）基站黑洞攻击。攻击者伪造一个恶意节点，并通过伪造路由使其成为信息传输中的最佳路由节点，使恶意节点周围的节点将数据包发送给此恶意节点。此攻击使得选择转发攻击更加易于实施，并使网络中大量的数据包流向恶意节点。

5）Sybil 攻击。恶意节点以多个身份在网络中虚拟成多个节点，与网络中的其它节点进行通信。这种攻击会给容错算法、分布式存储以及网络拓扑维护带来严重的影响。

6）虫洞攻击。攻击者通过重复播放的方式使网络中的两个节点建立一条低延迟的通信链路，从而欺骗其它节点到此链路的路由，并使其将数据

包发送过来。

7）Hello 洪泛攻击。无线传感器网络中，大部分路由协议都通过发送 HELLO 报文来更新链路并维护其邻居列表。攻击者通过使用较大的功率来广播 HELLO 报文，从而骗取较多的传感器节点成为其邻居节点。如果攻击者将上级路由广播到基站，则所有的节点将会把数据包转发给攻击者。

- 传输层攻击

1）洪泛攻击。传输层主要保证端到端的连接。洪泛攻击中，攻击者反复做出新的连接请求直到一端的能量被耗尽或者攻击者忽略合法的连接请求，使得网络中的连通受到影响。

2）不同步攻击。不同步攻击是指攻击者对现有连通状态进行破坏。攻击者通过反复向主机发送欺骗的消息，造成该主机对并不存在的错过的信息要求重传。有些情况下，攻击者可能减小或者毁坏主机交换数据的能力，并导致主机不停的修复并不存在的错误而消耗能量。

近年来对传感器网络的安全技术有一定的研究，但是没有任何的安全机制可以应对所有的攻击问题，传感器网络的安全没有形成完善的体系，仍然存在着巨大的安全隐患。因此，如何设计低能耗、高效率的安全算法以及机制以保障网络的安全存在巨大的挑战。

1.2.4 移动无线传感器网络

移动无线传感器网络（Mobile Wireless Sensor Networks，简称 MWSNs）是指传感器节点可以移动的网络，移动的传感器节点可以在任何需要的地方快速部署，为很多问题的研究提供了新的解决方案，并得到了广泛的应用，比如健康状况监测、追踪、空间探索、灾难救援等等。MWSNs 中节点可以根据需求到任意地点采集数据，完成了很多静态网络不能完成的任务，在应急情况下，MWSNs 可以自组织的构建应急相应网络，并自动实施有效方案。比如在战场环境监测中，手持监测设备、车载监测设备、飞行器监测设备都是移动的传感器节点，可以快速组建覆盖整个战场区域的监测网络。移动节点根据战场需要到指定的位置感知数据，或者作为中继节点进行通信，并将所采集到的数据发送给指挥中心，指挥中心通过分析这些数据做出决策，如图 1–4所示。

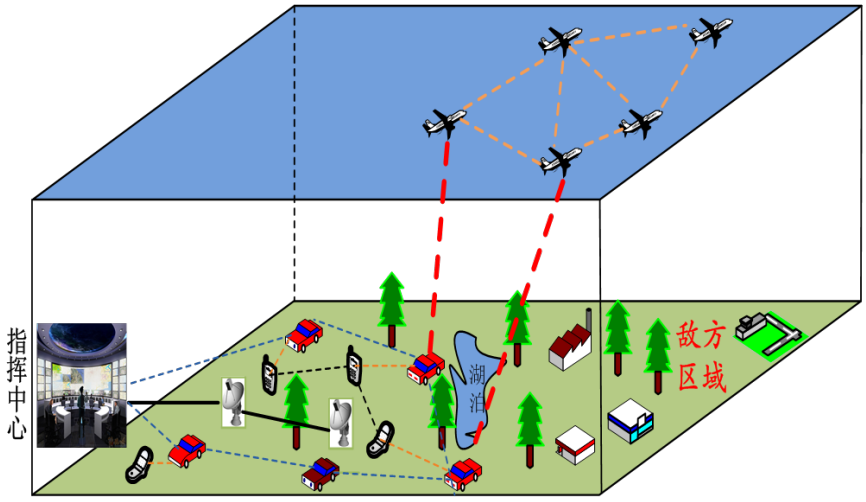


图 1–4: 战场监测中的移动传感器网络

Fig 1–4: Battlefield monitoring mobile sensor networks

1.3 相关研究

在无线传感器网络中，分布式一致性估计可以提高估计的准确性和有效性，并得到越来越多的关注。但是在分布式一致性估计中也存在安全问题，比如恶意节点可能在网络中注入错误的数据，影响网络的感知精度。数据篡改攻击非常容易影响分布式一致性计算的结果，例如，一个恶意节点在分布式一致性估计的过程中重复播放某一常值，整个网络将会收敛到这一常值 [19]。此外，数据篡改攻击还可能造成网络的不收敛、增大传输损耗、减小网络寿命等。因此，本文主要侧重于针对网络中数据传输和融合过程中的数据篡改攻击，提出分布式的安全机制，提高网络的可靠性计算。

近年来，分布式网络中针对恶意节点数据攻击的安全机制已经出现了一些研究成果。其中大部分异常值检测都是通过设定阈值来区分恶意节点和正常节点的，文 [20] 提出了一种自适应偏差容错的安全机制，该机制容许网络中感知数据偏差较大的节点参与一致性算法，减少了安全机制误判节点为恶意节点的概率，同时提高了网络的安全性。文 [21] 中在连续时间的系统中提出了一种平均子序列降低（Mean Subsequence Reduce）的算法，该算法可以抵御网络中有 F 个恶意节点的情况并实现渐近一致性。另外，一部分检测算法通过状态估计的残差来进行异常值的检测。Franco[22] 基于离散的卡尔曼状态估计设计了一

种分布式的异常值检测和分离算法；Pasqualetti[23] 基于未知输入观测为线性一致性网络设计了一种入侵检测算法。上述基于残差的检测方法理论性比较强，检测结果也很准确，但是只考虑了网络中只有一个恶意节点的情况，若网络中有多于一个恶意节点，则这些算法将会失效。

在网络安全的研究中，网络拓扑也是一个很重要的因素，文 [24] 针对网络中恶意节点上届的问题做了研究，并证明了在一个 $2k+1$ 连通图中，如果有少于 k 个恶意节点，则网络可以检测出恶意节点。文 [25] 根据有向图的连通度和节点度的特性定义了图的鲁棒性，在某些边从图中去掉后这种鲁棒性也可以保证，此研究中还给出了不同有向图的鲁棒性的比较方法，在网络中检测并去除掉恶意节点后，网络的拓扑发生变化，网络的鲁棒性依然可以描述。

从上面可以看出，针对分布式网络中恶意节点的研究已经有很多，当前的研究主要分为两类，一类检测算法是根据一个阈值来辨别恶意节点和常规节点；另一类检测算法主要通过计算估计残差的 2 范数来判断此节点是否为恶意节点。然而，如果攻击者足够隐蔽的话，当前的算法无法检测出恶意节点。Pathan[26] 指出信息传输过程中存在很多的攻击，比如数据篡改、伪造、重复播放或者数据包丢弃等，并且由于无线通信本身存在劣势，攻击者很容易对网络传输流量进行监控并且对信息进行拦截、阻断、修改或者伪造数据包，因此错误的信息很容易注入网络并发送给用户。文 [19] 中根据分布式算法的特点提出了一种隐蔽的自适应数据注入攻击。错误数据注入攻击（false data injection attacks）[27] 是根据现有检测算法的弱点提出的一种可以逃过基于残差的检测方法的新的攻击形式。

1.4 本文研究研究内容及结构

1.4.1 研究内容

根据上面的分析，本文针对网络中攻击，重点分析了数据篡改攻击，研究了恶意节点的检测算法，并研究了减小恶意节点影响的一致性算法。本文的主要贡献如下：

（1）无线传感器网络的分布式估计及其安全机制设计

大多数无线传感器网络在应用中，由于监测环境恶劣，又采用无线信道、有限电源以及分布式计算等，存在很多安全问题，比如节点信息被篡改、拥塞

攻击、拒绝服务等，会给网络带来很大的影响。针对无线传感器网络中的数据篡改攻击，基于加权平均提出一种分布式的安全算法来减小网络中的恶意节点对网络的影响。该算法中，节点根据邻居节点数据与自身数据差值与预先设定的阈值做比较，来判断邻居节点是否为恶意节点，当判断出邻居节点为恶意节点时，则把恶意节点排除网络，并对其余的节点进行一致性估计。针对阈值分离不出的恶意节点，我们设计了一种基于加权平均的一致性算法来减小恶意节点对一致性结果的影响。并通过仿真实例验证了算法的有效性。

(2) 异构传感器网络的分布式估计及其安全机制设计

针对大规模无线传感器网络，部署由主节点与中继节点组成的异构传感器网络来对区域进行监测。针对网络中的数据篡改攻击，本文提出了基于自适应阈值的检测方法判断网络中正确的以及错误的节点，并基于此设计基于无偏估计的分布式一致性算法。一致性算法中，为了避免把偏差较大的诚实节点误判为恶意节点排除网络，通过减小错误节点的一致性系数使其参与一致性过程来减小恶意节点对网络带来的影响。该算法既能使得网络中精度较低、与邻居节点感知结果相差较大的节点能够参与一致性过程，同时又提高了网络的安全性。

(3) 基于移动无线传感器网络的入侵搜索与安全防护

室内环境很像现实生活中的办公室，室内移动的传感器网络可以解决很多在室内危及安全或者是人类束手无策的危险问题。它可以代替人进行搜索和救援、安保等等工作。但是由于室内环境的特殊性，使传感器节点的移动速度受限。针对此种情况，我们利用图论知识，将室内环境离散化为图并对其进行树分解。在此基础上得出了一个能够成功围捕入侵者所需的传感器节点的最少数量，并提出了一种基于树分解的围捕策略，以保证室内环境的安全。

1.4.2 本文结构

本文共分为五章，其具体的结构如下:

第一章是绪论，主要介绍了本文的选题背景及其研究意义，概述了无线传感器网络及其特点，按照网络协议层次分析了其存在的安全问题，然后介绍了与本课题有关的研究工作，最后阐述了研究内容并介绍了取得的成果。第二章针对无线传感器网络中的数据篡改攻击，提出了基于加权平均的分布式估计安全算法来减小网络中的恶意节点对网络的影响。第三章主要设计了异构传感器

网络中的安全机制以及算法实现，提出了基于自适应阈值的检测方法，并设计了基于无偏估计的分布式一致性算法，避免了误判网络中的诚实节点为恶意节点，并提高了网络的安全性。第四章利用图论的知识对室内环境中的安全进行研究，得出了一个能够成功围捕入侵者所需的传感器的最少数量，并提出了一种基于树分解的围捕策略。第五章对全文的工作进行了总结，并展望未来研究工作。

第二章　无线传感器网络的分布式估计及其安全算法设计

2.1　引言

低成本、高性能的嵌入式设备以及网络的发展，推动了工程系统由集中式向分布式的转变，同时促进了大规模网络中，端到端的路由向网络计算的转变。分布式的网络计算在缩减等待时间、减小通信开销、增强节点的鲁棒性以及处理链路故障方面有更好的优势。而分布式计算中存在一个基本的挑战就是只使用局部信息对网络进行计算，也就是每个节点通过自己通过感知、计算以及跟邻节点的通信来获得的信息。而大规模的分布式网络中存在很多自身的弱点以及外部的威胁。

无线传感器网络在应用时，由于监测环境的特殊性，又采用采用无线信道、有限电源以及分布式控制等，存在很多的安全问题，比如节点信息被篡改、拒绝服务、Sybil 攻击等，因此无线传感器网络的安全是必须要考虑的问题。我们可以通过算法设计来减少网络中的恶意攻击对传感器网络带来的影响。

本部分主要针对无线传感器网络中的数据篡改攻击，设计了一种分布式估计的安全算法来减小网络中恶意节点的影响。该算法中，节点根据邻居节点数据与自身数据差值与预先设定的阈值的比较，来判断邻居节点是否为恶意节点，当判断出邻居节点为恶意节点时，把恶意节点排除网络，并对剩余节点进行一致性估计。针对阈值分离不出的恶意节点，我们设计了一种基于加权平均的一致性算法来减小恶意节点对一致性结果的影响。仿真实例验证了算法的有效性。

2.2　问题描述

2.2.1　网络模型

考虑由 $\mathcal{N}$ 个节点组成的无线传感器网络，对某一区域进行参数估计。为了便于理论分析，我们将节点以及节点间的通信拓扑建模为一个无向图

$\mathcal{G}=(\mathcal{N},\mathcal{E})$，其中 $\mathcal{N}=\{1,2,\ldots,\mathcal{N}\}$ 为所有节点的集合，$\mathcal{E}\in\mathcal{N}\times\mathcal{N}$ 为节点之间所有通信链路的集合。如果满足 $(i,j)\in\mathcal{E}$ 并且 $i\neq j$，则节点 j 是节点 i 的邻居。设邻居节点的集合为 $\mathcal{N}_i=\{j|(j,i)\in\mathcal{E}\}\subset\mathcal{N}$，$|\mathcal{N}_i|$ 表示节点 i 的邻居的数量。如果 $\mathcal{G}$ 中任意两个节点之间都有一条通路，则为连通图。

图 $\mathcal{G}$ 的拉普拉斯矩阵 $\mathcal{L}=(l_{ij})_{n\times n}$ 为

$$l_{ij}=\begin{cases}|\mathcal{N}_i|, & \text{if } j=i\\ -1, & \text{if } j\neq i, j\in\mathcal{N}_i\\ 0, & \text{otherwise}\end{cases}\tag{2–1}$$

图的拉普拉斯矩阵的定义为

$$\mathcal{L}=D-A\tag{2–2}$$

其中 D 为图 $\mathcal{G}$ 的度矩阵，$D=diag(d_1,d_2\cdots d_n)$，$d_i=\sum_{j\neq i}a_{ij}$。$A$ 为图 $\mathcal{G}$ 的邻接矩阵。

在无线传感器网络进行监测的初始阶段，每个传感器节点 i 在环境中感知到一个参数值，用 $x_i(0)$ 表示，一致性估计的目标是通过节点间信息的通信以及数据融合，最终共同得出该参数准确的估计值。通信时，节点 i 只能跟在其传输范围内的节点进行通信，这些节点我们称为该节点的邻居节点。在信息融合的过程中，采用迭代的方式进行一致性估计，每一次迭代，节点 i 都会根据自己的感知到或者估计的状态值以及接收到的数据更新自己当前的状态，并将更新的状态值发送给邻居节点。

Olfati-saber 在文 [28] 中介绍了一种离散时间的分布式一致性估计算法：

$$x_i(k+1)=x_i(k)+\epsilon\sum_{j\in\mathcal{N}_i}a_{ij}(x_j(k)-x_i(k))\tag{2–3}$$

式中，$x_i(k)$ 为迭代过程中第 k 步节点 i 的状态值，a_{ij} 表示信号从节点 i 传输到节点 j 的信号衰减幅度，$\mathcal{N}_i$ 表示能与节点 i 进行通信的所有节点（即邻居节点) 的集合，$\epsilon\in(0,1/\Delta]$，$\Delta=\max_i(\sum_{j\neq i}a_{ij})$。该算法收敛速度跟 ϵ 的选取有关，最终收敛结果为所有节点初始状态的平均值，本文中我们称此经典的一致性算法为 Olfati 一致性算法。

本文中我们假设网络在离散的时间中进行的，在第 k 步迭代过程中，节点 i 的状态更新方程为：

$$x_i(k+1)=w_{ii}x_i(k)+\sum_{j\in\mathcal{N}_i}w_{ij}x_j(k)\tag{2–4}$$

其中 w_{ij} 表示节点 j 的状态值在节点 i 的状态更新算法中所占的权重。由式 2–4可以看出每个节点的状态更新是节点自身状态和邻居节点状态的线性组合。在第 k 步所有节点的状态可以记为 $\mathrm{x}(k)=[x_1(k)\ x_2(k)\ ...\ x_n(k)]^T$，则整个网络的状态更新方程为

$$\mathrm{x}(k+1)=W\mathrm{x}(k) \tag{2–5}$$

其中 W 为权重矩阵，并且如果 $j\notin\mathcal{N}_i$，$w_{ij}=0$。

2.2.2　攻击模型

分布式一致性估计虽然有很多的优势，但是由于其协议暴露在环境中、采用分布式计算等，同时存在很多的弱点。本节中，我们介绍分布式一致性估计中存在的潜在的攻击。

无线传感器网络中的攻击方式分为内部攻击和外部攻击。一个外部攻击者可能会拦截节点的状态、注入虚假的状态、重复播放信息、伪装为诚实节点等，但是外部攻击者不具备有效的安全密钥。一个内部攻击者可能是被俘获的节点，并具备该节点内存储的安全密钥，并能够操纵该节点的感知状态，然后广播伪造的状态信息。还有一种攻击方式是由于传感器节点的软件或者硬件故障造成测量不准确。

大多数传感器网络部署在开放的环境中，而传感器节点的安全机制有限，攻击者可以轻易的俘获节点，对节点进行数据篡改攻击。因此数据篡改攻击是一种非常常见的攻击方式。而数据篡改攻击既可能发生在传感器节点感知数据的阶段，也可能发生在通信阶段或者数据融合阶段，能够长时间的影响网络，造成网络不收敛或者收敛到一个错误的值，带来非常严重的影响，因此本章中我们考虑数据篡改攻击。数据篡改攻击主要包括以下两种形式。

（1）常数据注入攻击

攻击者忽略网络中的更新算法，并在每一步更新过程中持续向网络中广播一个固定的常数值。在这种攻击方式下，若网络中只有一个攻击者，无论网络中传感器节点的初始状态如何，网络都会逐渐收敛到该常数值。若网络中有多与一个攻击者，并且向网络中广播不同的常数值，网络将不会收敛。并且这种攻击方式会延长网络的收敛时间。

（2）随机数据注入攻击

攻击者在迭代过程中向网络中注入随机的数据。这种攻击方式没有规律，我们可以用下面的模型进行分析。

假设网络没有被恶意节点控制，且通信链路可靠，数据融合过程中网络的拓扑保持不变。假设数据篡改中的恶意节点随机地在融合过程中注入错误的数据，我们可以得出节点 h 的状态更新方程

$$x_h(k+1) = w_{hh}x_h(k) + \sum_{j\in\mathcal{N}_h} w_{hj}x_j(k) + e_h(k) \tag{2–6}$$

其中 $e_h(k)$ 为第 k 步节点 h 注入邻居节点的恶意数据。如果 $e_h(k)$ 在任意一步不为 0，则节点 h 为恶意节点。在有恶意节点攻击的情况下，网络的状态更新方程为

$$\mathrm{x}(k+1) = W\mathrm{x}(k) + e(k) \tag{2–7}$$

攻击者可以选择任意的非零向量作为攻击向量，现有的检测方法一般计算状态估计残差的 2 范数来判断节点是否为恶意节点，然而如果攻击者采用错误数据注入攻击的方式，即注入的 e 为权重矩阵 W 列向量的线性组合，$e = Wc$，其中 c 为任意一个非零向量，则这种攻击非常隐蔽，即可以不被阈值检测算法检测到，也不会被基于状态估计残差 2 范数的检测方法检测出来，而这种攻击会对网络造成很大的破坏 [27]。随机数据攻击会通过造成网络不收敛或者收敛到一个错误的值破坏一致性算法。

针对数据篡改攻击，尤其是上述攻击方式，我们设计了一种基于加权平均的分布式一致性安全算法，减小恶意节点对网络的影响。

2.3 基于加权平均的一致性分布式安全估计算法

2.3.1 基于自适应阈值的分布式检测方法

检测算法的目标就是检测并排除掉网络中的异常节点，一致性算法中，网络中的节点大的状态值逐渐减小，而小的状态值逐渐增大直到所有的节点收敛到同一个结果。因此状态值之间的差值逐渐减小至 0，基于此，我们设计了一种基于自适应阈值的分布式检测方法。

复杂的环境中，节点的对环境的测量值各不相同，我们采用增大阈值的方法来避免把偏差较大的正常节点误判为恶意节点。首先每个节点感知周围环境

中的参数得到初始值 $x_i(0)$，第一步迭代中，为了使每个节点参与迭代过程，每个节点按照下述公式计算阈值：

$$\lambda_i(0) = \max_{j\in\mathcal{N}_i}\{x_i(0) - x_j(0)\} \tag{2–8}$$

数据融合过程中，随着一致性估计算法的进行，邻居节点之间的状态差值会越来越小，我们采用下面的算法来自适应的调整阈值。

$$\lambda_i(k+1) = \frac{\sum\limits_{j\in\mathcal{N}_i}|x_j(k+1) - x_i(k+1)|}{\sum\limits_{j\in\mathcal{N}_i}|x_j(k) - x_i(k)|}\lambda_i(k) \tag{2–9}$$

每次融合过程中，节点 i 将自身节点信息与收到的邻居节点信息 j 的差值 $|x_i(k) - x_j(k)|$ 与 $\lambda_i(k)$ 做比较，如果 $|x_i(k) - x_j(k)| > \lambda_i(k)$，则节点 i 认为节点 j 为恶意节点，并将其排除在外，节点 i 的后续一致性算法中不再考虑此节点。一致性过程中，邻居节点之间的状态值之差会减小，直到达到一致性差值变为 0，$\lambda_i(k)$ 也会减小至 0。

2.3.2　基于加权平均的一致性算法

数据篡改是一种易于实施但是却难以检测的攻击，特别是当攻击者注入的数据满足 $e(k) = Wc < \lambda(k)$ 时，上述基于自适应阈值的分布式检测算法不能检测出这种攻击，但是这种攻击方式可以对网络造成长时间的攻击并带来严重的影响。在 $\lambda(k)$ 的限制下，若 $e(k)$ 随着迭代的进行逐步减小，并始终保持 $e(k) < \lambda(k)$，则这种攻击方式变得更加隐蔽，能躲过几乎所有的检测方法。尽管对此种攻击方式不能很好的检测，而在分布式估计中，我们可以把 $e(k)$ 看作噪声，并且加权平均的收敛方法对处理噪声具有很好的效果。基于此，为了减小恶意节点未被检测出来前对网络的影响，我们提出了一种基于加权平均的一致性算法（Weighted Averaging-based Consensus Scheme）。

首先，我们先介绍加权平均的预备知识。假设 H 为实希尔伯特空间，并且 $L = H^N$ 为其向量空间。记 H 空间的内积为 $\langle\cdot,\cdot\rangle$，$||\cdot||$ 为相应的范数，序列 x 的第 k 个元素记为 $(x)_k$，$x \to P$ 表示 x 收敛到 P，且 $P \in H$。则实序列 $a = \{a_k\}$ 的加权平均算法 $\mathcal{A}_a : L \to L$ 定义为

$$(\mathcal{A}_a x)_k = \begin{cases} a_1 x(1), & \text{if } k = 1 \\ (1 - a_k)(\mathcal{A}_a x)_{k-1} + a_k x(k), & \text{otherwise} \end{cases} \tag{2–10}$$

其中 $x=\{x(k)\}\in L$。如果 $x\in L$, 则 $\mathcal{A}_a x$ 为 x 的加权平均算法，序列 a 为相应的加权平均算法的平均序列。

引理 2.1. *[29]* 如果实系列 $a=\{a_k\}$ 满足 $a_1=1$ 并且当 $k\geq 2$ 时，$0<a_k<1$; 定义实序列 $\{\beta_k\}$、$\{\gamma_k\}$ 分别为

$$\beta_k=\begin{cases}1, & k=1\\ \prod\limits_{m=2}^{k}\frac{1}{1-a_m}, & otherwise\end{cases} \tag{2–11}$$

$$\gamma_k=a_k\beta_k \tag{2–12}$$

则以下条件成立

1.$\beta_k=\sum_{m=1}^{k}\gamma_m$;

2. 对于任意的 $x=\{x(k)\}\in L$ 有 $(\mathcal{A}_a x)_k=(1/\beta_k)\sum_{m=1}^{k}\gamma_m x(m)$

假设 x 为未知参数 x^* 的估计序列，则使用加权平均算法可能会得到下面两种情况:

1. 如果 x 没有收敛到 x^*，但是序列有一定的特殊性，则 x 可能会加权收敛到 x^*;

2. 如果 x 收敛到 x^* 但是收敛速度很慢，则加权平均算法可能会加快 x 的收敛速度。

随机逼近算法对于处理噪声有很好的效果，而当噪声收敛时，随即逼近算法可以转化为噪声的加权平均算法，同样对于处理噪声有很好的效果。我们可以通过以下随机逼近算法考虑未知线性函数 $Ax-b$, $A:H\to H$，$b\in H$ 的递归估计问题。

$$x(k+1)=x(k)-a_kA_kx(k)+a_kb(k)+a_ke(k) \tag{2–13}$$

其中 $x_1\in H$ 可以是任意序列，A_k、b_k 分别为 A、b 的估计值，$e(k)$ 为噪声序列。步长值 $\{a_k\}$ 为非负的实数序列，并且满足 $a_1=1$, 当 $k\geq 2$ 时 $a_k<1$，$a_k\to 0$ 且 $\sum_{k=1}^{\infty}a_k=\infty$。假设 A_k，b_k 满足下列条件:

(i). $\inf\{Re\lambda:\lambda\in\sigma(A)\}>0$, 其中 $\sigma(A)$ 为 A 的谱.

(ii). $\limsup_{k\to\infty}(1/\beta_k)\sum_{m=1}^{k}\gamma_m||A_m||<\infty$.

(iii). $||(1/\beta_k)\sum_{m=1}^{k}\gamma_m A_m - A|| \to 0$.

上一节的检测算法可以通过阈值来检测出网络中的恶意节点，但是如果在数据融合过程中，攻击者采用隐蔽的错误数据注入攻击模型，每一步注入一个误差，且该误差为权重向量中列向量的线性组合，误差大小都在阈值范围之内，即 $e = Wc < \lambda(k)$，则如果采用 1.2.2所描述的 Olfati 一致性算法，式 2–14，整个网络将会收敛到一个与真实值偏差较大的结果。

$$x(k+1) = x(k) - \epsilon\mathcal{L}x(k) \tag{2–14}$$

其中 $0 < \epsilon < (\max_i |\mathcal{N}_i|)^{-1}$。

由于隐蔽的错误数据注入攻击难以检测，为了减小攻击者对整个网络的影响，我们提出了一种基于加权平均的一致性安全算法。这种算法能够使整个网络在有恶意节点存在的情况下仍然收敛到理想值。下面我们介绍此算法。

首先，网络中的每个节点独立的从周围环境中感知一个状态值，并传输给周围邻居。然后，每个节点按照上一节的检测算法，对周围邻居进行恶意节点的检测。根据检测算法得出的恶意节点排除后，节点 i 根据自己的状态以及剩余邻居节点的状态，按照下面的算法对自身状态进行更新

$$x_i(k+1) = x_i(k) + \epsilon(k)\sum_{j\in\mathcal{N}_i}(x_j(k) - x_i(k) + e_j(k)) \tag{2–15}$$

$$x(k+1) = x(k) - \epsilon(k)(\mathcal{L}x(k) - e(k)) \tag{2–16}$$

其中 $\epsilon(1) = 1$，$\epsilon(k) < 1$（$k \geq 2$），$\epsilon(k) \to 0$ 并且 $\sum_{k=1}^{\infty}\epsilon(k) = \infty$。由于 $\epsilon(k)$ 在每一步都是可变的，因此 $x_i(k)$ 的估计过程中邻居节点对估计结果的影响也是可变的，可以通过调整 $\epsilon(k)$ 的大小来调整邻居节点在 $x_i(k)$ 估计过程中所占的权重。采用这种一致性算法，可以使 $x(k)$ 收敛到平均值 $(1/n)\sum_i x_i(0)$，并减小恶意节点对整个网络的影响。我们利用如下的定理来证明此算法的可行性，并可以收敛到理想值。

定理 2.2. ：*$x(k)$ 收敛到平均值 $(1/n)\sum_i x_i(0)$，当且仅当 $e(k)$ 加权平均收敛到 0.*

证明. 根据攻击模型，我们可以得到如下一致性算法

$$\mathrm{x}(k+1) = \mathrm{x}(k) - \epsilon(k)\mathcal{L}\mathrm{x}(k) + \epsilon(k)e(k) \tag{2–17}$$

上式可以变换为如下形式

$$\mathrm{x}(k+1)=\mathrm{x}(k)-\epsilon(k)\mathcal{I}\mathrm{x}(k)+\epsilon(k)(\mathcal{I}-\mathcal{L})\mathrm{x}(k)+\epsilon(k)e(k) \tag{2–18}$$

其中 $\mathcal{I}_{n\times n}$ 为单位阵，则我们可以得到如下结论

(1). $\sigma(\mathcal{I})=1$, 则 $\inf\{Re\lambda:\lambda\in\sigma(\mathcal{I})\}>0$.

(2). $||\mathcal{I}_{n\times n}||=1$, 则有

$$\begin{aligned}&\limsup_{k\to\infty}(1/\beta_k)\sum_{m=1}^{k}\gamma_m||\mathcal{I}||\\ =\ &\limsup_{k\to\infty}(1/\beta_k)\sum_{m=1}^{k}\gamma_m\times 1\\ =\ &\limsup_{k\to\infty}(1/\sum_{m=1}^{k}\gamma_m)\sum_{m=1}^{k}\gamma_m\\ =\ &1<\infty\end{aligned} \tag{2–19}$$

(3).

$$\begin{aligned}&||(1/\beta_k)\sum_{m=1}^{k}\gamma_m\mathcal{I}-\mathcal{I}||\\ =\ &||(1/\sum_{m=1}^{k}\gamma_k)\sum_{m=1}^{k}\gamma_m\mathcal{I}-\mathcal{I}||\\ =\ &0\end{aligned} \tag{2–20}$$

根据自适应阈值的分布式检测方法，阈值逐渐收敛至 0，若异常值检测时 $e(k)$ 未被检测出来，则 $e(k)$ 逐渐减小至 0。若 $e(k)$ 没有随着 $\lambda(k)$ 的减小做出相应的调整，则相对应的节点会被检测为恶意节点排除网络。故 $e(k)$ 加权收敛至 0。根据一致性算法我们可以得到

$$\begin{aligned}\mathbf{1}^T\mathrm{x}(k)=\ &\mathbf{1}^Tx(k-1)-\mathbf{1}^T\epsilon(k-1)\mathcal{L}\mathrm{x}(k-1)\\ &+\mathbf{1}^T\epsilon(k-1)e(k-1)\end{aligned} \tag{2–21}$$

由于 **0** 是拉普拉斯矩阵的特征向量，**1** 是特征向量对应的特征根，所以有 $\mathcal{L}\mathrm{x}(k)=0$。故下面的公式成立

$$\begin{aligned} & \mathbf{1}^T\mathrm{x}(k) \\ = \ & \mathbf{1}^T x(k-1)+\mathbf{1}^T\epsilon(k-1)e(k-1) \\ = \ & \cdots \\ = \ & \mathbf{1}^T x(0)+\mathbf{1}^T(\epsilon(0)e(0)+\epsilon(1)e(1) \\ & +\cdots+\epsilon(k-1)e(k-1)) \end{aligned} \tag{2–22}$$

由于 $e(k)$ 加权收敛到 0，所以有 $\epsilon(0)e(0)+\epsilon(1)e(1)+\cdots+\epsilon(k-1)e(k-1)$ 收敛至 0。假设网络最终收敛到 P，即当 $k\to\infty$ 时，$x_i(k)=P$，由上式我们可以得到

$$\mathbf{1}^T\mathrm{x}(k)=\mathbf{1}^T\mathrm{x}(0) \tag{2–23}$$

则有

$$nP=\mathbf{1}^T\mathrm{x}(0) \tag{2–24}$$

$$P=\frac{1}{n}\mathbf{1}^T\mathrm{x}(0) \tag{2–25}$$

故有 $\mathrm{x}(k)$ 收敛到平均值 $(1/n)\sum_i x_i(0)$ □

根据以上分析，WACS 算法过程如下

Algorithm 1: 基于加权平均的分布式估计算法

Require: 网络离散化为 $\mathcal{G}=(\mathcal{V},\mathcal{E})$, 网络中有 n 个传感器节点

1: 每个传感器节点对周围环境进行感知并得到初始感知状态 $x_i(0)$, 传感器节点将其感知状态 $x_i(0)$ 发送给邻居节点
2: **for** 整个网络未实现一致性 **do**
3: **for** 对于任意的 $n_i\in\mathcal{N}$ **do**
4: **for** 对于任意的 $n_j\in\mathcal{N}_i$ **do**
5: **if** $|x_i(k)-x_j(k)|>\lambda_i(k)$ **then**
6: $w_{ij}(k)=0$
7: **else**

8: $w_{ij}(k) = \epsilon(k) l_{ij}(k)$
9: **end if**
10: **end for**
11: $x_i(k)$ 进行状态更新
12: $x(k+1) = x(k) - \epsilon \mathcal{L} x(k)$
13: $\lambda_i(k)$ 进行更新
14: $\lambda_i(k+1) = \frac{\sum_{j \in \mathcal{N}_i} |x_j(k+1) - x_i(k+1)|}{\sum_{j \in \mathcal{N}_i} |x_j(k) - x_i(k)|} \lambda_i(k)$
15: $k = k + 1$
16: **end for**
17: **end for**

2.4 仿真结果研究

本节中，我们通过仿真实例来验证了基于自适应阈值的分布式检测方法以及基于加权平均的一致性分布式安全估计算法的有效性，仿真中比较了在有恶意节点存在的情况下，Olfati 一致性算法和我们提出的算法所表现出来的性能，并对两种算法的方差进行了比较。

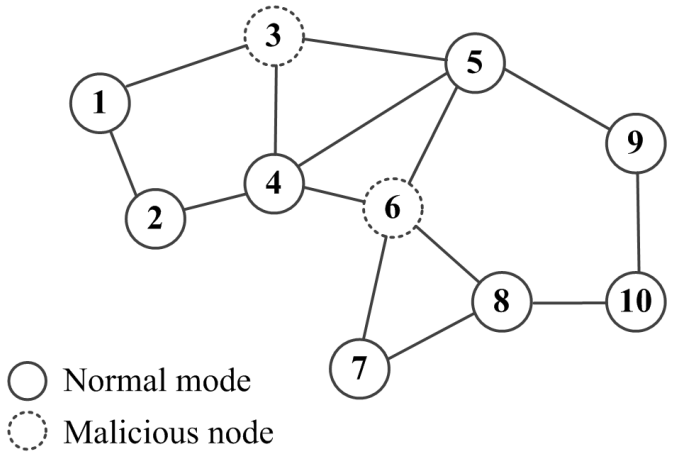


图 2–1: 含 2 个攻击者和 8 个节点的传感器网络拓扑

Fig 2–1: A network with two attackers and 8 normal nodes.

为了便于仿真，我们做如下假设，如图 2–1所示，假设传感器网络由

10 个节点组成 $\mathcal{N} = \{1, 2, ...10\}$，并且节点 $i \in \mathcal{N}$ 感知的初始值为 $x_i(0)$ 且 $\mathrm{x}(0) = [3\ 5\ 9\ 7\ 13\ 8\ 7\ 4\ 6\ 8]^T$，攻击者在数据融合过程中随机的注入错误数据。为了便于计算，我们选取一致性参数 $\epsilon(1) = 1$，$\epsilon(k) = (1/k), k \geq 2$，攻击者注入的误差向量为 $e = (\mathcal{I} - \epsilon(k)\mathcal{L})c \times \lambda(k)$，其中 $c = [2\ 1\ 3\ 1\ 0\ 1\ 0.5\ 2\ 0.3\ 1]$，假设网络中只有两个恶意节点，节点 3 采用数据篡改攻击，而节点 6 采取隐蔽的错误数据注入的攻击方方式，即 $e_6 < \lambda(k)$，因此恶意节点 6 可能不会被检测算法检测出来。如果没有攻击者网络将会收敛至 7。

在有恶意节点攻击的情况下，先对网络采用检测算法进行恶意节点的检测，然后采用一致性算法。首先，对检测算法进行仿真。下图 2–2中可以看出，检测算法只检测到一个恶意节点 3 并将其排除网络，采用隐蔽的错误数据注入攻击的节点 6 没有被检测算法检测出来。其中图 2–2 采用的是 Olfati 一致性算法，根据仿真结果，我们可以看出系统收敛至 8，偏差为 14.2%。而采用 WACS 算法时如图 2–3，可以看出系统大致收敛至 7，如果一致性算法足够长的话，系统将会收敛至 7，算法减小了恶意节点带来的影响。故所提出的 WACS 一致性算法对恶意节点具有很好的抵御性。

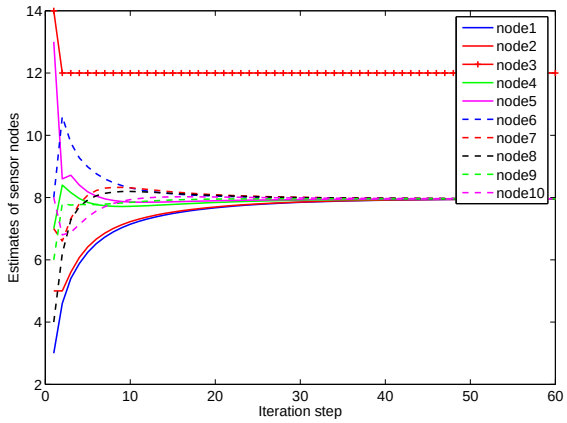


图 2–2: Olfati 一致性算法的收敛结果

Fig 2–2: The Olfati consensus scheme on the network.

此外，我们对 Olfati 一致性算法和 WACS 算法进行了方差和标准差的比较，如图 2–4所示，我们可以看出，WACS 算法的方差和标准差在数据融合开始阶段比较大，随着融合过程的进行逐渐减小，然而 Olfati 一致性算法的标准差和方差相对比较大。所以 WACS 算法可以使网络收敛到一个比较理想的值，如果

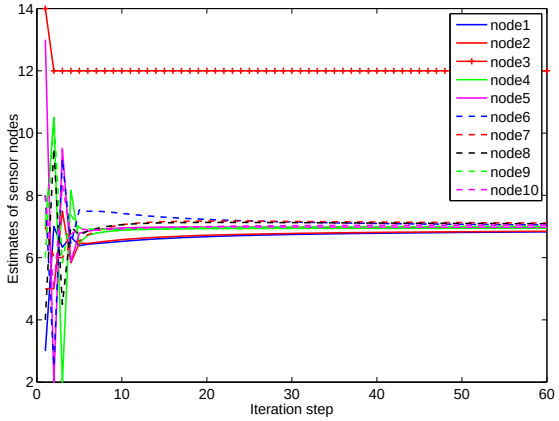


图 2–3: 加权平均算法的收敛结果

Fig 2–3: A secure scheme with weighted averaging on the network.

网络中有不止一个恶意节点，WACS 算法也可以使网络收敛到一个理想值，算法具有很好的扩展性。

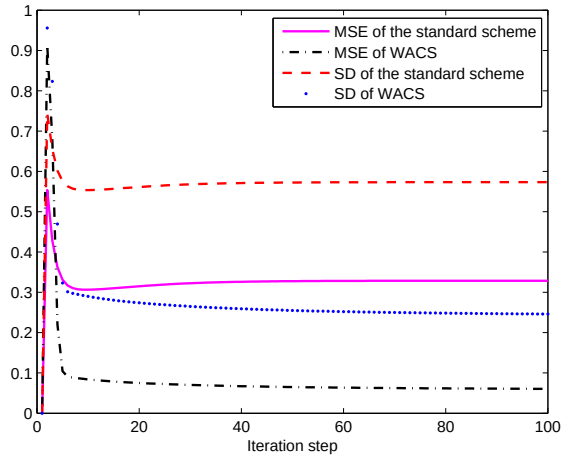


图 2–4: 两种算法 MSE、SD 比较

Fig 2–4: Comparison of the MSE and SD for the Olfati and WACS scheme.

2.5 本章小结

本章研究了无线传感器网络中数据篡改攻击下的检测算法以及安全机制。首先我们介绍了无线传感器网络分布式计算中存在的潜在攻击，并对其进行建模。针对这些攻击，我们首先提出了一种自适应阈值的检测方法，检测方法中，节点根据邻居节点与自身节点的状态差值与阈值 $\lambda(k)$ 做比较。若差值大于 $\lambda(k)$ 则认为该邻居节点为恶意节点，并将其排除网络；若差值小于 $\lambda(k)$，则认为该邻居节点为诚实的节点。阈值 $\lambda(k)$ 根据节点及其邻居节点状态的大小确定，并随着一致性估计的进行也逐渐更新直至减小至 0。这种检测算法可以检测网络中的大部分恶意节点，而对于检测算法不能检测出来的恶意节点，即隐蔽的恶意数据注入攻击方式，我们提出了一种基于加权平均的分布式一致性估计算法，将攻击注入的恶意数据看作网络中的噪声，采用加权平均的方法进行去噪，算法中通过对一致性参数大小适当的选取来调节算法的收敛速度以及收敛结果。然后通过定理证明了算法的收敛效果和收敛结果，网络可以收敛到所有节点初始状态的平均值。仿真结果验证了该算法具有较好的收敛效果，对于网络中的数据篡改攻击有很好的抵御作用。

第三章　基于异构传感器网络的分布式估计及其安全算法设计

3.1　引言

无线传感器网络的覆盖范围比较广，传感器节点通过适当的部署来协作完成对整个环境的监测。但是对于大范围的监测环境，长距离的信息交互将会耗费传感器节点大部分的能量，并且可能会导致传感器网络的分裂甚至是部分节点的孤立。针对这种情况，一种常用的方法就是通过部署中继节点来连通网络中孤立的部分，保证网络的连通性并且延长监测网络的寿命，由不同种类的传感器节点组成的网络为异构传感器网络。然而异构传感器网络的分布式计算也存在着一定的挑战，比如，在感知阶段，数据传输阶段以及数据融合阶段会出现链路的失效或者恶意节点的攻击，给监测网络造成很大的影响，尤其是在外部环境或者复杂的工业环境中，极其影响用户的决策。因此异构传感器网络中的安全问题是非常必要且有挑战性的。

无线传感器网络中的分布式估计问题已经有很多研究，如文 [30–35]，但是大多数研究都是针对同构网络的，即网络中的传感器有相同的硬件以及感知、通信、计算能力，但是这并不适用于多类传感器并存的大多数无线传感器网络。异构传感器网络中存在不同种类的传感器节点，可以延长网络的寿命并完成更多的任务。近年来，异构传感器网络的分布式估计也已经被众多的学者所研究 [36–41]，文 [42] 提出了一种基于非对称链路的分布式概率路由协议，以保证在簇头较少的情况下达到所要求的传输速率并保证该路由协议在异构传感器网络中的有效性和可靠性。文 [43] 基于流量包的特殊结构提出了一种新的跨层的 MAC 协议（Cross-Layer MAC protocol），该协议可以有效的处理网络中的多跳、多流量以及多数据包的情况。Zhu[41] 提出了一种异构传感器网络中的分布式估计模型，并设计了网络部署策略来支持该模型的实现。文 [**?**] 研究了工业无线网络中不同的多类传感器节点共存的分布式估计问题，提出了一种低通的分布式估计算法，并建立了算法稳定性的充分条件。上述的研究中，传感器节点在分布式估计中按照一定的方式进行融合，但是分布式估计中存在很多的

安全问题，如果一个节点被攻击，可能增大传输损耗、减小网络寿命、造成感知不准确等。尤其是在异构传感器网络中，如果一个传感器节点被攻击，可能会对其它种类的传感器造成影响，给网络带来很大的破坏。随着信息物理系统（Cyber-physical systems）的发展，其安全问题也成为非常重要且有挑战性的问题。

本章节主要解决异构无线传感器网络中的安全问题，考虑网络中存在两种节点的情况：传感器节点、中继节点。传感器节点有较强的计算能力，而中继节点只能对数据进行转发。针对网络中的数据篡改攻击，采用自适应阈值的检测方法判断网络中正确的以及错误的节点，并基于此设计基于无偏估计的分布式一致性算法（Asymptotic Unbiased Consensus Scheme，简称 AUCS）。一致性算法中，为了避免把偏差较大的诚实节点误判为恶意节点排除网络，通过减小其一致性系数使之参与一致性过程来减小恶意节点对网络带来的影响。

3.2 问题描述

3.2.1 网络模型

无线传感器网络中，传感器节点通过协作进行环境感知和数据融合。大规模的监测环境中，长距离的信息交互会耗费传感器节点大部分的能量，并且可能会导致部分传感器网络的孤立。为了保证网络的连通性并且延长监测网络的寿命，我们考虑在网络中加入中继节点。本部分我们考虑连通的异构传感器网络，网络由两种节点组成：传感器节点（主节点）、中继节点。

考虑由 N 个节点组成的异构传感器网络，对大范围的环境进行监测，其中包括 M 个传感器节点，$N-M$ 个中继节点，分别用 $\mathcal{I}_S=\{1,2,...,M\}$、$\mathcal{I}_R=\{M+1,M+2,...N\}$ 来表示。每个主节点可以感知环境中的参数，而中继节点由于硬件条件的限制不能对环境进行感知，只能对信息进行接收和转发。我们把网络离散化为连通的无向图 $\mathcal{G}=(\mathcal{V},\mathcal{E})$，其中 $\mathcal{V}$ 表示网络中所有节点的集合，且 $\mathcal{V}=\mathcal{I}_S\cup\mathcal{I}_R$ 为主节点和中继节点的并集。$\mathcal{E}\in\mathcal{V}\times\mathcal{V}$ 表示图中的边集，代表网络中节点之间通信链路的集合。如果节点 j 在节点 i 的通信范围之内，则代表这两个节点可以互相通信，我们在图中两个节点之间插入一条边。即如果满足 $(i,j)\in\mathcal{E}$ 并且 $i\neq j$，则节点 j 是节点 i 的邻居。记节点 i 的邻居集合为 $\mathcal{N}_i=\{j|(j,i)\in\mathcal{E}\}\subset\mathcal{V}$，$|\mathcal{N}_i|$ 表示节点 i 的邻居数量。如果 $\mathcal{G}$ 中任意两个节点之间都有一条通路，则 $\mathcal{G}$ 为连通图。

图 $\mathcal{G}$ 的拉普拉斯矩阵 $L=(l_{ij})_{N\times N}$ 为

$$l_{ij}=\begin{cases}|\mathcal{N}_i|, & \text{if } j=i\\ -1, & \text{if } j\neq i, j\in\mathcal{N}_i\\ 0, & \text{otherwise}\end{cases} \tag{3–1}$$

传感器节点对环境进行监测时，首先每个传感器节点 i $(i\in\mathcal{I}_S)$ 可以在环境中监测到一个初始参数数值 $x_i(0)$，而网络的目标是通过传感器节点的感知信息以及节点间信息的通信协作以及数据融合，最终共同得出参数值。在信息融合的过程中，每个传感器节点按照一定的算法进行数值的更新估计。然而异构传感器网络中，由于中继节点不能对环境进行感知，只能进行转发和信息融合，因此在信息融合时，中继节点没有初始值，我们用下列公式计算的值来表示中继节点的初始值。

$$x_i(0)=\frac{\sum\limits_{j\in\mathcal{N}_i}x_j(0)}{|\mathcal{N}_i|}, \text{if } i\in\mathcal{I}_R \tag{3–2}$$

这样，我们可以对每个节点的状态更新进行计算，由于主节点与中继节点感知能力不同，我们对它们的状态更新分别进行计算，主节点的状态更新方程为:

$$x_i(k+1)=x_i(k)+\epsilon\sum_{j\in\mathcal{N}_i}a_{ij}(x_j(k)-x_i(k)),\ \text{if } i\in\mathcal{I}_S, \tag{3–3}$$

中继节点的状态更新方程为:

$$x_i(k+1)=\sum_{j\in\mathcal{N}_i}\gamma_{ij}x_j(k),\ \text{if } i\in\mathcal{I}_R, \tag{3–4}$$

其中

$$0<\epsilon<(\max_i|\mathcal{N}_i|)^{-1}=\frac{1}{\Delta} \tag{3–5}$$

Δ 表示网络中节点度数的最大值，a_{ij} 表示信号从节点 i 传输到节点 j 的信号衰减幅度。γ_{ij} 表示权重并且满足 $\gamma_{ij}>0$ 并且 $\sum_{j\in\mathcal{N}_i}\gamma_{ij}=1,\forall i\in\mathcal{I}_R$。若 $j\notin\mathcal{N}_i$，则 $\gamma_{ij}=0$。我们可以看出节点 i 所有的邻居节点满足 $j\in\mathcal{N}_i$, $\sum_{j=1}^{N}\gamma_{ij}=1,\forall i\in\mathcal{I}_R$。从中我们可以看出，每个节点通过自身的状态以及邻居节点的状态的线性组合来更新自己的状态。

为了简化一致性的算法以及便于安全算法的设计，联合上述两个公式 (3–3) 和 (3–4)，得到主节点的状态更新公式

$$x_i(k+1) = x_i(k) + \epsilon \left[\sum_{j \in \mathcal{N}_i^S} a_{ij}(x_j(k) - x_i(k)) + \sum_{k \in \mathcal{N}_i^R} \sum_{j \in \mathcal{N}_k{}^S} a_{ik}\gamma_{kj}(x_j(k) - x_i(k)) \right] \tag{3–6}$$

式中 $\mathcal{N}_i^S$ 表示节点 i 的邻居中为主节点的集合，$\mathcal{N}_i^R$ 表示节点 i 的邻居中为中继节点的集合。式中我们可以看出主节点的更新过程的计算可以只跟网络中的主节点有关，减少了网络中的异构性给网络算法设计带来的复杂性。我们定义若 $\lim_{k\to\infty} E\{x_i(k)\} = \theta$，则序列 $\{x_i(k)\}$ 为 θ 的渐进无偏估计值。

3.2.2 攻击模型

本章节中我们考虑异构传感器网络中的数据篡改攻击，数据篡改攻击中攻击者在传感器节点的感知节点篡改感知结果或者在数据融合阶段注入错误的数据来攻击网络。由于这种攻击方式对网络的影响时间比较长，会带来很大的影响。我们根据攻击阶段的不同，把数据篡改攻击分为 3 种不同的类型。

- 感知阶段数据篡改攻击（Sensing Data Falsification（*SDF*）Attack)。这种攻击方式只发生在数据感知阶段，攻击者改变节点感知的初始值 $x_i(0), i \in \mathcal{I}_S$，并将错误的数据传输给邻居节点。而在数据融合阶段，攻击者正常进行数据更新以及与邻居之间的信息交互。在复杂的环境中，这种攻击方式易于实施，但是难以与监测数据偏差较大的恶意节点进行区分。为了避免把偏差较大的诚实节点误以为恶意节点，本章节中我们只减小此种攻击对网络的影响，并不将其排除网络。

- 融合阶段数据篡改攻击（Iteration State Falsification（*ISF*）Attack)。攻击者在数据感知阶段不对网络进行攻击，只在数据融合阶段，每一步迭代过程中注入错误的数据。这种攻击方式能够长时间的影响网络，所以会带来严重的后果。

- 随机数据篡改攻击（Random Data Falsification（*RDF*）Attack)。攻击者在感知阶段或者数据融合阶段随机的注入错误数据。这种攻击方式具有非常好的隐蔽性，难以检测。

上述的 3 种攻击方式比较隐蔽，但会给网络造成严重的影响，比如网络不收敛，或者收敛到一个偏差较大的错误数值。本文我们将设计一种基于无偏估计的分布式一致性安全算法（Asymptotically Unbiased-based Consensus Scheme，简称 AUCS）来减小数据篡改攻击对整个网络的影响。

3.3　异构传感器网络中的分布式安全估计算法

3.3.1　基于无偏估计的分布式一致性安全算法（AUCS）

一致性算法中，网络中节点状态值大的逐渐减小，而小的状态值逐渐增大直到所有的节点收敛到同一个结果。因此状态值之间的差值逐渐减小至 0。基于此，我们通过阈值来判断网络中的节点是否感知的数据偏差较大，并设计了基于无偏估计的分布式一致性算法来减小恶意节点给网络带来的影响，该算法允许网络中偏差较大的诚实节点来参与融合过程。

下面我们介绍 AUCS 算法的过程，假设网络并没有被攻击者控制，且通信链路可靠，并且数据融合过程中网络的拓扑保持不变。首先每个主节点 $i \in \mathcal{I}_R$ 感知环境中的参数然后将其发送给邻居节点；在迭代过程中，主节点 $i \in \mathcal{I}_R$ 将邻居节点与自身状态值的差值与阈值 $\lambda(k)$ 做比较，将 $|x_j(k) - x_i(k)| < \lambda_i(k)$ 的节点集合记为 $\mathcal{N}_i^T$，其个数记为 $\beta_i(k)$，将 $|x_j(k) - x_i(k)| \geq \lambda_i(k)$ 的节点集合记为 $\mathcal{N}_i^F$，其个数记为 $\alpha_i(k)$。若 $\beta_i(k) + 1 \geq \alpha_i(k)$ 则节点 $i \in \mathcal{I}_S$ 被判定为诚实的节点，其状态更新方程为

$$x_i(k+1) = x_i(k) + \sigma(k) \Bigg[\sum_{j \in \mathcal{N}_i^{ST}} a_{ij}(x_j(k) - x_i(k)) + \sum_{j \in \mathcal{N}_i^{SF}} \frac{a_{ij}}{a(k)}(x_j(k) - x_i(k)) + \sum_{k \in \mathcal{N}_i^R} \sum_{j \in \mathcal{N}_k{}^{ST}} a_{ik}\gamma_{kj}(x_j(k) - x_i(k)) + \sum_{k \in \mathcal{N}_i^R} \sum_{j \in \mathcal{N}_k{}^{SF}} \frac{a_{ik}}{a(k)}\gamma_{kj}(x_j(k) - x_i(k)) \Bigg] \tag{3–7}$$

其中 $\sigma(k) > 0$ 表示一致性参数，$\mathcal{N}_i^{ST}$ 表示 $\mathcal{N}_i^T$ 中的主节点的集合，$\mathcal{N}_i^{SF}$ 表示 $\mathcal{N}_i^F$ 中主节点的集合，$a(k)$（$a(k) \geq 1$）表示通过减小一致性算法中错误的节点相应的参数来减小恶意节点对整个网络的影响。算法中可以看出若 $a(k)$ 变大，则恶意节点对网络的影响会减小，我们通过调整 $a(k)$ 的大小来调节网络中的节点在一致性算法中占的比例。如果一个节点被持续检测为恶意节点则相应的 $a(k)$ 将持续变大，并最终把恶意节点排除网络，若节点被检测为正常的节点则相应的 $a(k)$ 将减小。我们对 $a(k)$ 采用 AIMD （Additive Increase

Multiplicative Decrease）的方法来确定其数值大小。若节点被检测为恶意节点，则令 $a(k+1)=a\times a(k)$，且 $a>1$。当一个恶意节点停止攻击网络时，其相应的系数 $a(k)$ 以 $a(k+1)=(1/a)\times a(k)$ 的方式减小直至 $a(k)=1$，当 $a(k)=1$ 时若节点继续表现正常则 $a(k)$ 保持为 1 不变。

根据式 3–7我们得到状态方程的拉普拉斯矩阵 $\hat{L}=[\hat{L_{ij}}]\in R^{M\times M}$ 且

$$\hat{L}_{ij}=\begin{cases}\sum\limits_{j\in\mathcal{N}_i^{ST}}a_{ij}+\sum\limits_{j\in\mathcal{N}_i^{SF}}\frac{a_{ij}}{a(k)}+\sum\limits_{j\in\mathcal{N}_k^{ST}}\sum\limits_{k\in\mathcal{N}_i^{R}}a_{ik}\gamma_{kj} \\ \qquad\qquad+\sum\limits_{j\in\mathcal{N}_k^{SF}}\sum\limits_{k\in\mathcal{N}_i^{R}}\frac{a_{ik}}{a(k)}\gamma_{kj}, \quad \text{if } j=i \\ -a_{ij}, \qquad \text{if } j\neq i, j\in\mathcal{N}_i^{ST}\backslash\mathcal{N}_k^{R}, k\in\mathcal{N}_i \\ -\frac{a_{ij}}{a(k)}, \qquad \text{if } j\neq i, j\in\mathcal{N}_i^{SF}\backslash\mathcal{N}_k^{R}, k\in\mathcal{N}_i \\ -a_{ik}\gamma_{kj}, \qquad \text{if } j\neq i, j\in\mathcal{N}_k^{RT}\backslash\mathcal{N}_i, k\in\mathcal{N}_i \\ -\frac{a_{ik}}{a(k)}\gamma_{kj}, \qquad \text{if } j\neq i, j\in\mathcal{N}_k^{RF}\backslash\mathcal{N}_i, k\in\mathcal{N}_i \\ -a_{ij}-a_{ik}\gamma_{kj}, \text{if } j\neq i, j\in\mathcal{N}_i^{ST}\cap\mathcal{N}_k^{R}, k\in\mathcal{N}_i \\ -\frac{a_{ij}}{a}-\frac{a_{ik}}{a(k)}\gamma_{kj}, \text{if } j\neq i, j\in\mathcal{N}_i^{SF}\cap\mathcal{N}_k^{R}, k\in\mathcal{N}_i\end{cases} \tag{3–8}$$

定义 $P(k)=I-\sigma(k)\hat{L}\otimes I$，则得到式 3–7相应的向量形式为

$$x(k+1)=P(k)x(k) \tag{3–9}$$

由于 $\mathcal{G}$ 是无向的连通图，故 $\hat{L}$ 所有的行和为 0，因此 0 是 $\hat{L}$ 的特征值，又由于 $\hat{L}\mathbf{1}=0$，因此 $\mathbf{1}=(1,1,\ldots,1)^T$ 是 0 特征值相对应的右特征向量，且 $I\hat{L}+\hat{L}^TI$ 是半正定的。

若节点满足 $\beta_i(k)+1<\alpha_i(k)$，则该节点被认为是恶意节点，其状态更新方程保持不变，也就是说，如果一个节点被检测为恶意节点，则它按照原来的方式进行状态更新。

我们通过下面的公式来确定节点 i 的检测阈值 $\lambda_i(k)$

$$\lambda_i(k)=\frac{1}{|\mathcal{N}_i|}\sum_{j\in\mathcal{N}_i}\left|x_j(k)-\frac{x_i(k)+\sum_{j\in\mathcal{N}_i}x_j(k)}{|\mathcal{N}_i|+1}\right| \tag{3–10}$$

从式 3–10可以看出阈值 $\lambda_i(k)$ 不包含任何节点的先验信息，只根据节点当前的状态值确定，在减少计算的同时保证了阈值的灵活性，随着网络分布式一致性的进行，$\lambda_i(k)$ 将最终收敛至 0。

考虑到恶意节点注入网络的恶意数据可能会引起节点状态偏差值较大，因此我们采用节点邻居跟自身状态值的差值跟阈值做比较的方法来检测网络中感知偏差较大的节点以及恶意节点。并采用 AUCS 的算法来减小恶意节点给网络带来的影响。AUCS 算法的如下所示

Algorithm 2: 基于无偏估计的分布式估计算法

Require: 网络离散化为 $\mathcal{G}=(\mathcal{V},\mathcal{E})$, M 个传感器节点, $N-M$ 个中继节点

设 $k=0$
for $i\in\mathcal{I}_S$ **do**
　设 $a(k)=1, a>1, \alpha_i=0,\ \beta_i=0$
　每个传感器节点对周围环境进行感知并得到初始感知状态 $x_i(0)$, 传感器节点将其感知状态 $x_i(0)$ 发送给邻居节点
end for
for $i\in\mathcal{I}_R$ **do**
　$x_i(0)=\frac{\sum_{j\in\mathcal{N}_i}x_j(0)}{|\mathcal{N}_i|}$.
end for
for 整个网络未实现一致性 **do**
　for $i\in\mathcal{I}_S$ **do**
　　$\lambda_i(k)=\frac{1}{|\mathcal{N}_i|}\sum\limits_{j\in\mathcal{N}_i}\left|x_j(k)-\frac{x_i(k)+\sum_{j\in\mathcal{N}_i}x_j(k)}{|\mathcal{N}_i|+1}\right|$
　　for $j\in\mathcal{N}_i$ **do**
　　　if $|x_i(k)-x_j(k)|>\lambda_i(k)$ **then**
　　　　$\alpha_i=\alpha_i+1$
　　　　if $a(k)=1$ **then**
　　　　　$a(k)=a$
　　　　else
　　　　　$a(k)=a\times a(k)$
　　　　end if
　　　else
　　　　$\beta_i=\beta_i+1$
　　　　if $a(k)>1$ **then**
　　　　　$a(k)=\frac{1}{a}a(k)$

else
  $a(k) = 1$
end if
end if
end for
if $\beta_i + 1 > \alpha_i$ **then**
  $x_i(k)$ 根据公式 (3–7) 更新自己的状态并将其状态估计值发送给邻居节点
  $\hat{L}_{ii}$ 进行更新并保证其每一行的行和为 1
end if
end for
$k = k + 1$
end for

3.3.2 AUCS 算法性质分析

本部分我们对 AUCS 的性质进行了分析，为了证明算法的收敛性定义每一个传感器节点 i 的估计误差变量为 $e_i(k) = x_i(k) - \theta$，则所有的传感器节点在分布式估计过程中第 k 步的估计误差变量为 $e(k) = [e_1(k), e_2(k), \cdots, e_M(k)]^T$。由于 $(\hat{L} \otimes I)(\mathbf{1} \otimes \theta) = 0$，在公式 3–9的两边分别乘以 $\mathbf{1} \otimes \theta$，得到如下公式

$$e(k+1) = P(k)e(k) \tag{3–11}$$

接下来我们通过对估计误差性质的分析来分析 AUCS 算法的性质。

由于网络中两个节点之间的通信是对等的，即图 $\mathcal{G}$ 为无向图，故分布式一致性算法中，传感器节点和中继节点的系数产生了 Hermitian 矩阵 $\hat{L}$。定义 $\hat{e}(k) = (I \otimes I)e(k)$ 用来代替 $e(k)$，则我们得到

$$\hat{e}(k+1) = CP(k)e(k) \tag{3–12}$$

其中 $C = \sqrt{P} \otimes I$。我们定义

$$\widetilde{H} = C(\hat{L} \otimes I)C^{-1} + C^{-1}(\hat{L}^T \otimes I)C \tag{3–13}$$

若图 $\mathcal{G}$ 为强连通图，则 $\widetilde{H}$ 为正定的。

定理 3.1.：如果图 $\mathcal{G}$ 中含有一个强连通分支包含所有的传感器节点，且序列 $\{\sigma(k)\}_{k\geq 0}$ 满足

$$\sum_{k=0}^{\infty}\sigma(k)=\infty,\ \sum_{k=0}^{\infty}\sigma^2(k)<\infty \tag{3–14}$$

则对于所有的传感器节点 i，序列 $\{x_i(k)\}$ 为 θ 的渐近无偏估计，即

$$\lim_{t\to\infty}E\{x_i(k)\}=\theta,\forall i\in\mathcal{I}_S \tag{3–15}$$

证明. 由于 C 是正定矩阵。对式 3–12两边分别求期望，可以得到如下公式

$$E\{\hat{e}(k+1)\}=CP(k)C^{-1}E\{\hat{e}(k)\} \tag{3–16}$$

对于 $k>k_0$，则有

$$E\{\hat{e}(k)\}=\prod_{s=k_0}^{k-1}CP(s)C^{-1}E\{\hat{e}(k_0)\} \tag{3–17}$$

对上式两边取二范数得到

$$||E\{\hat{e}(k)\}||\leq\prod_{s=k_0}^{k-1}||CP(s)C^{-1}||||E\{\hat{e}(k_0)\}||,\ \forall k>k_0 \tag{3–18}$$

令 $T=\hat{L}\otimes I, T_1=C^{-1}T^TC^2TC^{-1}, T_2(k)=\widetilde{H}-\sigma(k)T_1$，可以得到

$$C^{-1}T^TC+CTC^{-1}=C(\hat{L}\otimes I)C^{-1}+C^{-1}(\hat{L}^T\otimes I)C=\widetilde{H} \tag{3–19}$$

由于 $P(k)=I-\sigma(k)T$，于是可以得到下式

$$\begin{aligned}C^{-1}P^T(k)C^2P(k)C^{-1}&=I-\sigma(k)\tilde{H}+\sigma^2(k)T_1\\&=I-\sigma(k)T_2(k)\end{aligned} \tag{3–20}$$

由于矩阵 $\tilde{H}$ 以及 T_1 为半正定矩阵。因此有 $\lambda_{min}(\tilde{H}/2)>0$ 并有 $\lambda_{max}(T_1)>0$。根据式 3–14中的条件，当 $k\to\infty$ 时，$\sigma(k)\to 0$。因此存在 $k_1>0$ 满足 $\sigma(k)\lambda_{max}(T_1)\leq\lambda_{min}(\tilde{H}/2),\forall k\geq k_1$。且有当 $k\geq k_1$ 时，$T_2(k)$ 为正定矩阵。根据 Rayleigh-Ritz 定理 [44] 可以得到如下关系

$$\lambda_{min}(\tilde{H}/2)\leq\lambda_{min}(T_2(k))\leq\lambda_{max}(T_2(k))\leq\lambda_{max}(\tilde{H}),\forall k\geq k_1 \tag{3–21}$$

又由于 $\sigma(k) \to 0$, 存在 $k_2 > k_1$ 使得

$$\sigma(k) \leq \frac{1}{\lambda_{max}(H)}, \forall k \geq k_2 \tag{3–22}$$

因此我们可以得到如下关系式

$$\begin{aligned} ||CP(k)C^{-1}||^2 &= ||C^{-1}P^T(k)C^2P(k)C^{-1}|| \\ &= 1 - \sigma(k)\lambda_{min}(T_2(k)), \forall k \geq k_2 \end{aligned} \tag{3–23}$$

令 $k_0 = k_2$，则式 3–18可以转换为如下形式

$$||E\{\hat{e}(k)\}|| \leq \prod_{s=k_0}^{k-1} \sqrt{1 - \sigma(k)\lambda_{min}(T_2(k))}||E\{\hat{e}(k_0)\}||, \ \forall k > k_0 \tag{3–24}$$

根据式 3–21以及式 3–22可以得出若 $k > k_0$ 则有 $0 < \sigma(k)\lambda_{min}(T_2(k)) \leq 1$ 又由于 $\ln(1 - \sigma(k)\lambda_{min}(T_2(k))) \leq -\sigma(k)\lambda_{min}(T_2(k))$。则从式 3–21 到式 3–24，我们可以得到，对于任意的 $k > k_0$，则有

$$\begin{aligned} ||E\{\hat{e}(k)\}|| &\leq \exp(-\frac{1}{2}\sum_{s=k_0}^{k-1}\sigma(k)\lambda_{min}(T_2(k)))||E\{\hat{e}(k_0)\}|| \\ &\leq \exp(-\frac{1}{2}\lambda_{min}(\tilde{H}/2)\sum_{s=k_0}^{k-1}\sigma(k))||E\{\hat{e}(k_0)\}|| \end{aligned} \tag{3–25}$$

从前面的证明可知 $\lambda_{min}(\tilde{H}/2) > 0$ 以及 $\sum_{k=0}^{\infty}\sigma(k) = \infty$，则我们可以得到如下公式

$$\lim_{k\to\infty} ||(I \otimes I)E\{e(k)\}|| = \lim_{k\to\infty} ||E\{e(k)\}|| = 0 \tag{3–26}$$

且有

$$||(I \otimes I)E\{e(k)\}|| \geq \min_{1\leq i\leq M} ||E\{e(k)\}|| \tag{3–27}$$

公式 3–26以及 3–27中可以得出 $||E\{e(k)\}||$ 收敛至 0。所以系统收敛结果只跟节点状态的初始值有关系。 □

3.4 仿真结果研究

本部分我们通过仿真实例来验证了异构传感器网络中基于渐近无偏的分布式一致性算法的有效性，考虑 3 种不同类型的数据篡改攻击方式分别对网络进

行攻击，仿真中比较了在有隐蔽的恶意节点存在的情况下一般的一致性算法和AUCS 算法的性能。

为了便于仿真，我们做如下假设，如图 3–1所示，传感器网络由 12 个节点组成，其中有 9 个主节点以及 3 个中继节点，恶意节点对主节点进行攻击。为了简化仿真，我们不考虑节点之间进行通信时的路径衰减，即 $a_{ij}=1$ 时，节点 i 和节点 j 能进行可靠通信，$a_{ij}=0$ 时，节点 i 和节点 j 不能进行通信。假设传感器节点在分布式估计中所占的权重为 $\gamma_{ij}=a_{ij}/\Sigma_{j\in\mathcal{N}_i}a_{ij}=1/|\mathcal{N}_i|$，$\forall i\in\mathcal{I}_R$，一致性参数 $\sigma(1)=1$ 且当 $k>1$ 时 $\sigma(k)=1/(k-1)$。在进行分布式安全估计算法初始，每个传感器节点 $i\in\mathcal{I}_S$ 从周围环境中感知初始状态 $x(0)=[x_i(0)]^T$。假设网络中没有恶意节点是，传感器节点的初始感知数值在区间 [0，8] 中随机选取，$x_i(0)=[3.3626;8.4791;4.1553;6.5966;8.2043;1.9973;3.8923;4.2489;4.0636]^T$。

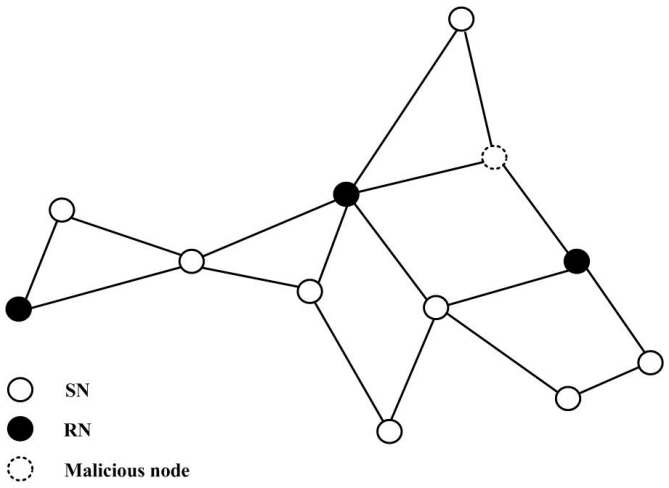


图 3–1: 8 个传感器节点、3 个中继节点、一个攻击者组成的异构传感器网络

Fig 3–1: A network with 8 honest sensor nodes, 3 relay nodes and one attacker.

首先对没有恶意节点存在的网络进行分布式估计的仿真，得到网络的收敛值为 5.0657。仿真结果如下图 3–2所示，通过分布式估计算法使初始状态不同的节点值经过协作通信、计算最终收敛到同一状态值。

考虑网络中存在一个恶意节点的情况，假设恶意节点为传感器节点 4，对网络进行 *SDF* 攻击的方式，即改变初始状态值 6.5966。若网络采用 Olfati 一致性算法，网络将会逐渐收敛值一个统一的结果 6.1493，可以看出由于恶意节点的影响，该结果与真实值偏差较大。仿真结果如图 3–3。然而若采用 AUCS

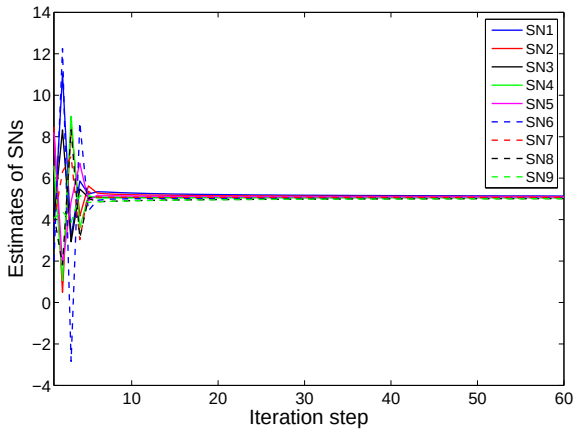


图 3–2: 无恶意节点时 AUCS 算法的收敛结果

Fig 3–2: Convergence of AUCS without attack.

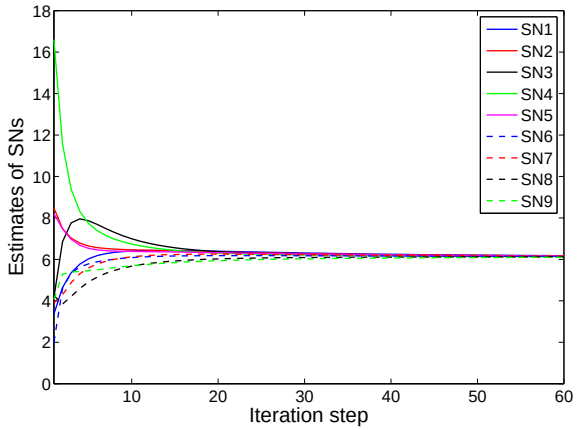


图 3–3: 一个 *SDF* 攻击节点时 Olfati 一致性算法的收敛结果

Fig 3–3: Convergence of Olfati consensus algorithm with one *SDF* attacker.

算法，得出的结果为 5.0657，仿真结果如图 3–4所示。可见 AUCS 算法减小了 *SDF* 攻击对网络的影响，提高了网络的安全性。

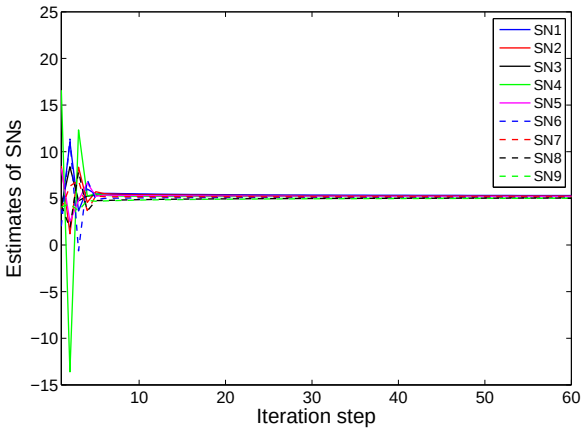


图 3–4: 一个 *SDF* 攻击节点时 AUCS 算法的收敛结果

Fig 3–4: Convergence of AUCS with one *SDF* attacker.

若网络中的恶意节点实施 *ISF* 的攻击方式，仿真中我们假设恶意节点在进行数据更新时，每一步迭代过程中都加入一个高斯白噪声，这种攻击方式会较长时间的对网络造成影响，当采用 Olfati 一致性算法时，仿真结果如图 3–5所示。而当采用 AUCS 算法时，仿真结果如图 3–6所示。

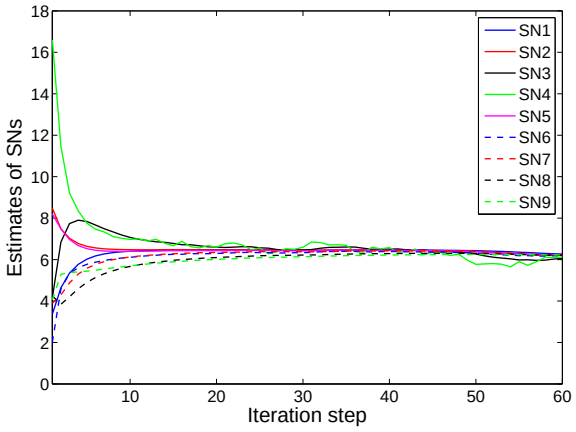


图 3–5: 一个 *ISF* 攻击节点时 Olfati 一致性算法的收敛结果

Fig 3–5: Convergence of Olfati consensus algorithm with one *ISF* attacker.

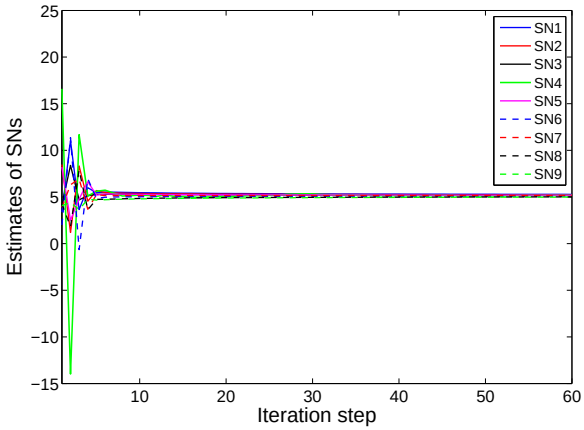


图 3–6: 一个 *ISF* 攻击节点时 AUCS 算法的收敛结果

Fig 3–6: Convergence of AUCS with one *ISF* attacker.

仿真中我们还考虑了参数 $a(k)$ 对一致性结果的影响，分别对 *SDF* 攻击、*ISF* 攻击以及 *RDF* 攻击三种攻击方式进行了仿真，如图 3–7所示。从仿真结果我们可以看出，当 $a(k)$ 变大时，恶意节点对网络的影响会逐渐减小。

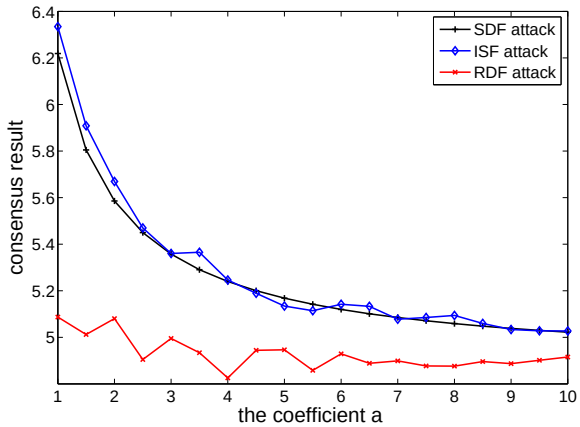


图 3–7: 不同攻击方式下的 AUCS 算法的收敛结果

Fig 3–7: Consensus results of AUCS under different attacks.

3.5　本章小结

本章节我们考虑了在大规模的传感器网络中，部署由主节点与中继节点组成的异构传感器网络来对环境进行监测。由于监测环境的复杂多变性，会给网络带来安全问题，针对网络中的数据篡改攻击，我们提出了基于自适应阈值的检测方法判断网络中正确的以及错误的节点，并基于此设计基于无偏估计的分布式一致性算法来减小网络中的恶意节点对网络带来的影响。本部分提出的安全机制充分利用一致性数据融合过程中信息对等交互的特点，改变数据融合中其他节点数据的权重，将其设置为自适应调整的动态阈值。每次融合过程中，节点 i 都将本次收到的邻居节点 j 的数据与自身的数据进行对比，如果他们的差值绝对值在阈值 $\lambda_i(k)$ 以外，我们的做法是将邻居节点的数据在融合中的权重降低。这一做法与直接将其排除在外不同，有的节点因为在环境中所处位置的不同或者探测精度的影响，会产生比较大的偏差。如果直接排除在外，容易将精度低但不存在数据篡改的节点错误地排除在外。本章节提出的算法基于如下一个基本规律，那就是空间分布临近的节点所探测到的环境参数类似，而且每个节点探测的误差服从零均值分布。如果该节点不是恶意节点，其结果不会长时间与别的节点差别很大。而且我们提出的自适应修改阈值 $\lambda_i(k)$ 的算法，使得精度较低、与邻居节点探测结果相差较大的节点能够逐渐恢复其在融合过程中的权重，同时提高了网络的安全性。

第四章　基于移动传感网的入侵搜索与安全防护

4.1　引言

无线传感器网络的应用中，在感知环境的基础上，人们还希望能够进一步影响环境。在工业控制、战场探测、应急救援等应用中，不仅需要传感器网络对环境进行监测，还需要通过传感器的移动对事件进行处理。近年来移动互联网高速发展，移动用户与周围环境交互的需求越来越高，移动无线传感器网络的研究应运而生 [45]。而随着人们对家庭和办公安全的重视程度越来越高，室内移动无线传感器网络的安全问题引起了越来越多的关注 [46–48]。比如在大型场馆内，如果有一个乱入的入侵者影响网络或者影响场馆，都会对场馆的安全带来隐患。因此我们需要对室内环境中的入侵者进行围堵并捕获，以保证被监控环境的安全。

关于监测环境的安全问题，一部分学者将其刻画为追逃游戏（Pursuit-Evasion Games，简称 PEGs）开展了具体的研究 [49–52]。Chen[53] 提出了一种以抽样的方法来计算入侵者性能界限的算法，并给出了一个传感器网络的 n 跳磁盘模型来模拟延迟和数据包丢失，用此模型设计了一个概率屏障，用来把追逃游戏的状态空间分为一个逃跑区和一个捕获区并基于此设计最优控制策略。Schenato[52] 提出了无线传感器网络下的追逃游戏的蜂拥协调控制，文中设置了一个分层控制结构通过联合集中和分散的实时控制算法来开发无线传感器网络的优势，并提出了一个追逐者的协调方案来利用最短的时间捕获逃逸者。Vieira 在文 [54] 中受到零和博弈理论的启发，基于机会成本函数提出了在 PEG 中基于最短时间来捕获逃逸者的算法。在研究追逃策略的同时，基于追逃策略的追逐者的数量（追逐者的数量是指在某一环境中存在一种策略使得最少数量的追逐者就可以成功围捕入侵者，最少的数量即为追逐者的数量）也逐渐引起研究者的重视 [55, 56]。如果网络中有过多的追逐者参与围捕策略，则两个或者更多的追逐者在追逐过程中很可能撞击到一起，并且过多的追逐者会增加成本，造成资源的浪费；但是如果追逐者的数量不足，很容易造成围捕的失败，攻击者在网络中没有被捕获，会对网络造成严重的影响。因此追逐者数量问题的研究，在实际应用中是一个非常重要的问题。Aigner[57] 证明了在一个可平

面图中追逐者的数量至多为 3。Lu[58] 证明了在一个 n 节点的有限图中，追逐者的数量至多为 $n2^{-(1-o(1))\sqrt{\log_2 n}}$ 。然而这些研究中都假设追逐者和入侵者的能力是相同的，它们有相同的速度，并且知道环境以及对手所有的信息，然而这些假设在一些情况下是不切实际的，例如入侵的速度可能比追逐者的速度大的多 [59–61]。

本章中我们对移动传感器网络监控下的室内环境的安全问题进行研究。由于室内环境的复杂性，存在障碍物等情况，传感器节点的感知范围以及移动速度受限。然而无线传感器网络的存在为传感器节点进行感知、计算、互相通信提供了保障，弥补了追逐者感知范围受限带来的不足。无线传感器网络为节点之间提供通信保障，使得传感器节点之间可以实现信息共享并能进行协同估计。针对上述情况，我们设计了基于移动 WSNs 的入侵搜索与安全防护，得出能够监测并排除入侵者所需要的最小传感器数量的上届，保证了网络的安全性。

4.2 问题描述

本节中，我们首先介绍树分解的一些知识，然后对监测环境进行数学刻画。

4.2.1 树分解

在图论中，树分解是一个图到一个树的映射，树分解可以加快在原有的图形上解决问题 [62]。直观的说，一个图的树的分解是指用树的子树来表示图中的节点集，当图中的节点相邻时则相应的子树交叉，每个子树都将图的节点和树的节点联系起来。本章节我们给出一个新的树分解的的定义，这种定义更加便于对移动 WSNs 监控下的室内环境安全策略进行设计。下面介绍树分解的定义：图 $\mathcal{G}=(\mathcal{V},\mathcal{E})$ 的一个树分解为 $(\mathcal{T},\mathcal{X})$，$\mathcal{X}=\{\mathcal{X}_i|i\in\mathcal{I}\}$，其中 $\mathcal{I}$ 是 $\mathcal{V}$ 的一个子集族，$\mathcal{T}$ 是指以 $\mathcal{I}$ 为顶点集的树，$\mathcal{T}$ 中的节点是 $\mathcal{X}$ 的子集，并且满足：

(i) $\bigcup\mathcal{X}_i=\mathcal{V}$;

(ii) 对每条边 $(u,v)\in\mathcal{E}$, 都存在 $i\in\mathcal{I}$ 满足 $\{u,v\}\subset\mathcal{X}_i$;

(iii) 对任意 $i,j,k\in\mathcal{I}$，若 k 处于树 $\mathcal{T}$ 中从 i 到 j 的唯一路中，则 $\mathcal{X}_i\bigcap\mathcal{X}_j\subseteq\mathcal{X}_k$ 对于至少有两个度为 1 的节点的图 G，为了后面的计算方便，我们对此类图 G 重新定义一种树分解。图 $\mathcal{G}=(\mathcal{V},\mathcal{E})$ 的一个树分解为 $(\mathcal{T},\mathcal{X})$, $\mathcal{X}=\{\mathcal{X}_i|i\in\mathcal{I}\}$。

路径 $\mathcal{L}$ 为连接图 $\mathcal{T}$ 中端点 v_1 到 v_K 的路径，路径中包含 K 个节点 $v_1, v_2, \ldots, v_K$，本文中定义的树分解具有一下特性：

(i) $\bigcup \mathcal{X}_i = \mathcal{V}$;

(ii) 对于任意的 $i \in \mathcal{I}$, $\mathcal{X}_i$ 至少包含一个 $v_i, 1 \leq i \leq K$;

(iii) 对于任意一条边 $(u, v) \in \mathcal{E}$，存在一个 $i \in \mathcal{I}$ 使得 $\{u, v\} \subset \mathcal{X}_i$;

(iv) 对于树的节点 $\mathcal{X}_i, \mathcal{X}_j$ 以及 $\mathcal{X}_k$，如果树节点 $\mathcal{X}_k$ 是树节点 $\mathcal{X}_i$ 到 $\mathcal{X}_j$ 路径上的一个树节点，则图 $\mathcal{G}$ 中存在一个节点属于 $\mathcal{X}_i \cap \mathcal{X}_j$ ，且有 $\mathcal{X}_i \bigcap \mathcal{X}_j \subseteq \mathcal{X}_k$.

在图的树分解中，有一个重要的概念：树宽 $\mathsf{tw}(\mathcal{G})$。树的宽度反映了在一棵最优树分解中任意一个树的节点在图中映射的点的个数。树的宽度首先是由 Robertson 和 Seymour 在建立图的 minor[63] 理论时提出的，其定义如下：

$$\mathsf{tw}(\mathcal{G}) = \min_{(\mathcal{T},\mathcal{X})} \max_{i \in \mathcal{I}} \{|\mathcal{X}_i| - 1\},$$

其中 $|\mathcal{X}_i|$ 表示 $\mathcal{X}_i$ 的基数。由上式可以看出，图的树分解的树宽表示的是图 $\mathcal{G}$ 所有可能的树分解中的最小宽度，通过树宽的计算可以更好的分析图的性质。

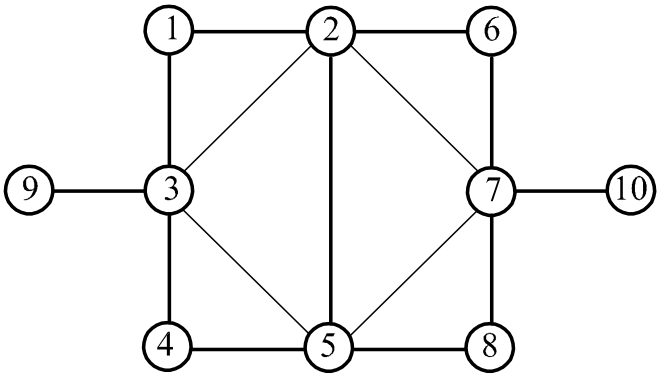


图 4–1: 有 10 个节点的图 $\mathcal{G}$

Fig 4–1: A graph $\mathcal{G}$ with ten vertices.

我们用例子来说明如何对图进行树分解以及求其树宽。图 $\mathcal{G}$ 的拓扑图如图 4–1所示，图 $\mathcal{G}$ 的一种树分解 (T, X) 如图 4–2所示。图 $\mathcal{G}$ 中有 10 个节点，路径 L 为 9-3-2-7-10。它的一种树分解后为一个有八个节点的树。图中的每一条边连接两个节点，这两个节点在树的节点上也列在一起。树中的每个节点都含有路径 L 中的节点。每个树的节点至多有 3 个点，所以这种分解的树的宽度为 2。

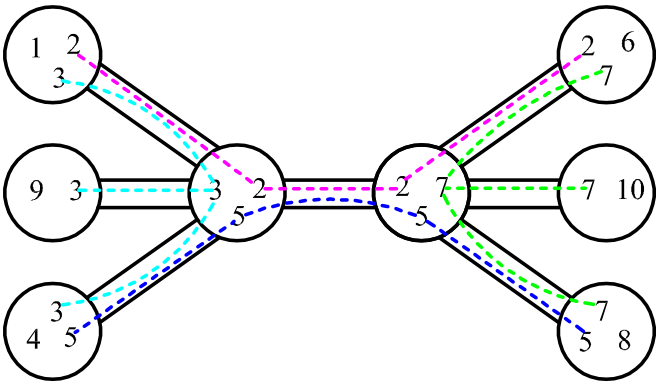


图 4–2: 图 $\mathcal{G}$ 的树分解

Fig 4–2: A tree decomposition of graph $\mathcal{G}$.

4.2.2 拓扑结构刻画

考虑到移动 WSNs 中攻击者可能非常强大，以及本文所考虑的室内环境，我们做以下假设：

1. 整个过程是在室内的环境中进行的，攻击者和移动传感器节点都不能离开室内环境；

2. 攻击者的能力很强，并且速度可以无限大，知道所有的环境信息以及传感器节点的位置信息；

3. 传感器节点知道室内环境的信息以及队友的位置信息，但是在感知范围之外，由于数据丢包等的影响，无法精确知道攻击者的位置信息，本文中我们假设传感器节点不知道攻击者的位置信息，并且传感器节点的移动速度是有限的；

4. 整个过程是在离散的时间中进行的，并且运动是顺序进行的，攻击者先移动一步，传感器节点再移动一步。

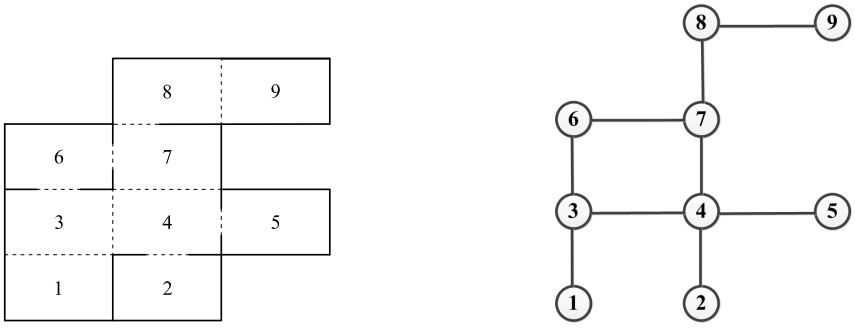
对于室内环境的描述，一种常见的方法就是将其离散化成有限图 [64–67]。本章节中，我们根据传感器节点的感知能力和移动速度对环境进行离散化：

1. 根据传感器节点的监测能力对环境进行离散化，使得每个传感器节点能够监测环境离散化后的每一个单元，若攻击者进入此单元，传感器节点能够及时对其进行捕获；

2. 用顶点来代替环境中的单元；

3. 在两个相邻的单位之间插入一条边。

例如下图 4–3所示，根据以上规则，如图 4.3(a)所示的环境可以用离散化为图 4.3(b)所示的图 $\mathcal{G}$。



(a) 室内环境　　(b) 离散化后的图 $\mathcal{G}$

图 4–3: 室内环境的刻画示意图

Fig 4–3: A Indoor Environment Decomposition.

$\mathcal{G} = (\mathcal{V}, \mathcal{E})$ 中，$\mathcal{V} = \{1, 2, \ldots, M\}$ 表示顶点集，$|\mathcal{V}|$ 表示图中顶点的个数，$\mathcal{E}$ 表示边集。顶点的度 deg 是指图中跟该顶点相连的所有的顶点的数目。若一个顶点的度为 1，则我们称该顶点为端点。图中长度为 K 的路径是指 K 个不同的顶点组成的一条路径 $(i_1, i_2), (i_2, i_3), \ldots, (i_{K-1}, i_K)$。若 $i_1 = i_K$，我们称此路径为环。

我们假设传感器节点的速度以及感知范围都是 1，也就是说传感器节点在图 $\mathcal{G}$ 中每一次至多移动一条边的距离，能够监测自己所在的节点以及距离为 1 条边的邻居节点。由于我们假设传感器节点以及攻击者的运动是顺序进行的，若攻击者一旦移动到传感器节点的监测范围内，下一步将会被传感器节点捕获。而我们假设攻击者的速度无限大，攻击者每一步可以移动 s 条边，$s \geq 1$。因此，当至少一个传感器节点跟攻击者在同一个节点上时，攻击者被捕获。

本文中我们的目的是确定成功捕获攻击者并有效保护网络所需要的最小的传感器节点的数量，经过一系列特定的移动，传感器节点逐渐把攻击者限定在越来越小的范围内，最终成功捕获。

4.3　基于移动 WSN 的入侵搜索与安全防护

4.3.1　传感器节点数的最少上界

本节中我们基于图的树分解得出了移动的 WSNs 中安全防护所需要的传感器节点的最小上界。其具体算法如下。

定理 4.1.：对于任意一个有限的、简单连通图 $\mathcal{G}$，如果 $\mathcal{G}$ 中至少含有两个端点，那么网络中所需的传感器节点的数量为

$$\lfloor tw(\mathcal{G})/2 \rfloor + 1 + \sum_{i=1}^{K} \sum_{l=1}^{m_i} n_{i,l}, \tag{4–1}$$

其中 $\lfloor \cdot \rfloor$ 为 *floor* 函数，且 $n_{i,l}$，$l = 1, 2, \ldots, m_i$，$i = 1, 2, \ldots, K$ 将会在证明中给出定义。

证明. 图 $\mathcal{G}$ 的最优树分解为 $(\mathcal{T}_{\mathcal{L}}, \mathcal{X})$，树分解中的树节点 $\mathcal{X}_{i,j}$, $j = 1, 2, \ldots, m_i$ 包含相应的 v_i，且 v_i 满足 $i \leq h, \forall v_h \in \mathcal{X}_{i,j}$。例如，$\mathcal{X}_{i,1}$ 包含相应的顶点 v_i，$i = 1, 2, \ldots, K$，其中 K 表示路径 $\mathcal{L}$ 的长度。图 $\mathcal{G}$ 的最优树分解如图 4–4所示。图的树分解中对于任意一个树节点 $\mathcal{X}_i$，至多需要 $\lfloor \mathsf{tw}(\mathcal{G})/2 \rfloor + 1$ 个传感器节点

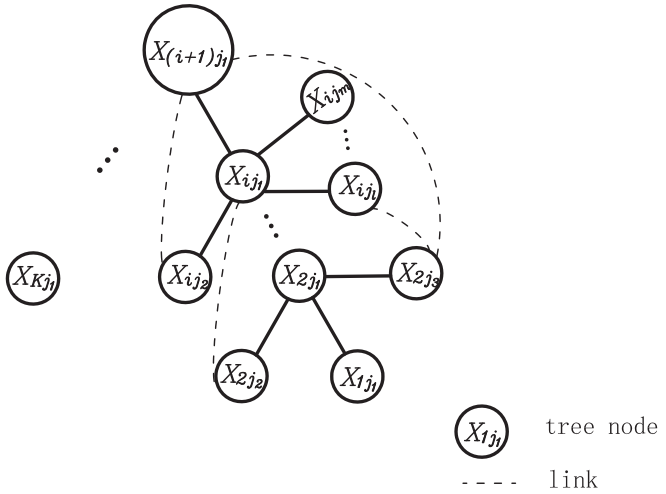


图 4–4: 图 $\mathcal{G}$ 最优树分解 $(\mathcal{T}_{\mathcal{L}}, \mathcal{X})$

Fig 4–4: The optimal tree decomposition $(\mathcal{T}_{\mathcal{L}}, \mathcal{X})$ of graph $\mathcal{G}$.

就可以对其进行监视和安全防护。令 $b_1, b_2, \ldots, b_q$ 表示 $\mathcal{X}_i / v_i$ 中的顶点，下面我

们介绍树节点 $\mathcal{X}_i$ 中的安全防护机制。首先，我们将 $\mathcal{X}_i$ 根据下面的规则重新构造为一个类似于二叉树的形状（见图 4–5）。

i) 令 v_i 为树中的第 0 层顶点；

ii) 将 v_i 的相邻顶点定义为第 1 层顶点；

iii) 依此类推，将第 h 层顶点的相邻顶点定义为第 $h+1$ 层顶点；

iv) 若为定义层数的顶点 j 的相邻顶点为 $j_1, j_2, \ldots, j_k$，且它们分别属于不同的层 $l_1, l_2, \ldots, l_k$，则定义顶点 j 为第 $\min\{l_1, l_2, \ldots, l_k\}+1$ 层的顶点。

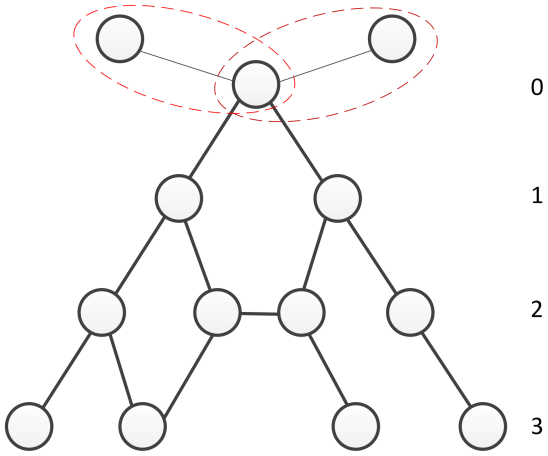


图 4–5: 树节点的重新构造示意图

Fig 4–5: A subtree rearrangement into a tree-like graph.

根据以上定义，令偶数层的顶点数量为 N。若 $N \leq q/2$，则我们考虑偶数层的顶点，若 $N > q/2$，则我们考虑奇数层的顶点。我们下面证明 N 个传感器节点可以对 $\mathcal{X}_i$ 进行监测以及安全防护。首先，令传感器节点 p_1 停留在顶点 v_i 处，剩余的 $N-1$ 个传感器节点对 $\mathcal{X}_i$ 进行搜寻，直到这些传感器节点停留在 $\mathcal{X}_i$ 的偶数层，搜寻过程中，传感器节点到达某一偶数层时，一些传感器节点停在该层的顶点上，其余传感器节点继续搜寻，直到 $\mathcal{X}_i$ 中所有的顶点都被监视。用这种方法，攻击者在有限步数后就会被限定到 $\mathcal{X}\backslash\mathcal{X}_i$ 的范围内。由于 $N \leq q/2$ 又根据树宽 $\mathsf{tw}(\mathcal{G})$ 的定义，因此 $\lfloor \mathsf{tw}(\mathcal{G})/2 \rfloor + 1$ 个传感器节点即可对节点 $\mathcal{X}_i$ 进行搜寻和监视。

传感器节点从顶点 v_1 开始沿着路径 $\mathcal{L}$ 进行搜索。从上述讨论中可以看出 $\lfloor \mathsf{tw}(\mathcal{G})/2 \rfloor + 1$ 个传感器节点就可以树节点 $\mathcal{X}_{i,1}$ 进行搜索以监视。为了对其相邻

的树节点进行搜索和监视，传感器节点按照下面的运动策略进行从 $\mathcal{X}_{i,1}$ 到 $\mathcal{X}_{i,2}$ 的移动。

- 对于监视 $X_{i,1}\bigcap\mathcal{X}_{i,j}$ 或者 $\mathcal{X}_{i,1}\bigcap\mathcal{X}_{k,j}$, $j=2,\ldots,m_i$, $k>i$ 的传感器节点，令其继续保持在相同的边不动；
- 对于监视 $b_{h'}b_h$，$b_{h'}\in\mathcal{X}_{i,1}\bigcap\mathcal{X}_{i,2}$ 且 $b_h\in\mathcal{X}_{i,1}\backslash\mathcal{X}_{i,2}$ 的传感器节点，令其沿着边 $b_{h'}b_h$ 移动到顶点 b_h，然后监视边 $b_hb_{h''}$，其中 $b_{h''}\in\mathcal{X}_{i,2}\backslash\mathcal{X}_{i,1}$；
- 对于其它的传感器节点，令它们监视 $\mathcal{X}_{i,2}\backslash\mathcal{X}_{i,1}$ 中未被监视的边。

按照上述方式，$\lfloor\mathsf{tw}(\mathcal{G})/2\rfloor+1+n_{i,1}$ 个传感器节点即可搜索和监视 $\mathcal{X}_{i,1}\bigcup\mathcal{X}_{i,2}$，$\forall\mathcal{X}_{i,2}$，其中 $n_{i,1}=|Y_{i,1}|$ 且 $Y_{i,1}=\sum_j\mathcal{X}_{i,1}\bigcap\left(\bigcup_{k>i}\mathcal{X}_{k,j}\right)$。重复上面的步骤，我们可以得出 $\lfloor\mathsf{tw}(\mathcal{G})/2\rfloor+1+\sum_{l=1}^{m_i}n_{i,l}$ 个传感器节点可以搜索和监视 $\bigcup_{l=1}^{m_i}\mathcal{X}_{i,l}$，其中 $n_{i,l}=|Y_{i,l}|$ 且 $Y_{i,l}=\sum_j\mathcal{X}_{i,l}\bigcap\left(\bigcup_{k>i}\mathcal{X}_{k,j}\right)$。

在所有的树节点 $\mathcal{X}_{i,j}$, $j=1,2,\ldots,m_i$ 都被搜索和监视后，令 $\sum_{l=2}^{m_i}n_{i,l}$ 保持对 $\bigcup_{l=2}^{m_i}\left(\mathcal{X}_{i,l}\bigcap\left(\bigcup_{k>i}\mathcal{X}_{k,j}\right)\right)$ 的监视。然后令传感器节点 p_1 移动到 v_{i+1} 进行监视。对于其它传感器节点的移动策略，我们需要考虑以下两种情况：

- 若存在 $2\leq l^*\leq m_i$ 使得 $\mathcal{X}_{i,l^*}\bigcap\left(\bigcup_{h<i}\mathcal{X}_{h,j}\right)\backslash\{v_i,v_{i-1}\}\neq\emptyset$，则令传感器节点通过 v_i 监视 $\left(\mathcal{X}_{i,l^*}\bigcap\left(\bigcup_{h<i}\mathcal{X}_{h,j}\right)\right)\backslash\{v_i,v_{i-1}\}$ to $\mathcal{X}_{i+1,1}$；
- 若 $\bigcup_{l=2}^{m_i}\left(\mathcal{X}_{i,l}\bigcap\left(\bigcup_{h<i}\mathcal{X}_{h,j}\right)\backslash\{v_i,v_{i-1}\}\right)=\emptyset$，则令 $\lfloor\mathsf{tw}(\mathcal{G})/2\rfloor+1$ 个传感器节点按照上面的方式并沿着 $\mathcal{X}_{i,1}$ 到 $\mathcal{X}_{i+1,1}$ 的最短路径搜索并监视 $\mathcal{X}_{i+1,1}$。

从上面的搜索监视过程，我们可以得出 $\lfloor\mathsf{tw}(\mathcal{G})/2\rfloor+1+\sum_{i=1}^{K}\sum_{l=1}^{m_i}n_{i,l}$ 就可以对图 $\mathcal{G}$ 进行搜索和监视。 □

4.3.2 基于树分解的搜索算法

我们根据定理（4.1）提出了基于树分解的搜索算法（Tree Decomposition based Graph Searching Algorithm，简称 TWGS），具体如下所示。

Algorithm 3: 基于树分解的搜索算法

Require: 图 $\mathcal{G}=(\mathcal{V},\mathcal{E})$，传感器节点的数量 n

所有的传感器节点移动到 v_1
$\mathcal{X}_i \leftarrow \mathcal{X}_{1,1}$
$i \leftarrow 1$
while $i < K$ **do**
　令一个传感器节点移动到树节点 $\mathcal{X}_i$ 的第 0 层顶点
　if $\mathcal{X}_i$ 中偶数层顶点的数量多于奇数层顶点的数量 **then**
　　令 $\lfloor \mathsf{tw}(\mathcal{G})/2 \rfloor$ 个传感器节点移动到 $\mathcal{X}_i$ 中奇数层的顶点上
　else
　　令 $\lfloor \mathsf{tw}(\mathcal{G})/2 \rfloor$ 个传感器节点移动到 $\mathcal{X}_i$ 中偶数层的顶点上
　end if
　$l \leftarrow 1$
　while $l < m_i$ **do**
　　令 $n_{i,l}$ 个传感器节点监视 $Y_{i,l}$，剩下的 $\lfloor \mathsf{tw}(\mathcal{G})/2 \rfloor + 1$ 个传感器节点搜索并监视 $\mathcal{X}_{i,l+1}$.
　　$l \leftarrow l + 1$
　end while
　令 $\sum_{l=2}^{m_i} n_{i,l}$ 个传感器节点监视 $\bigcup_{l=2}^{m_i} Y_{i,l}$.
　if $\bigcup_{l=2}^{m_i} Z_l = \bigcup_{l=2}^{m_i} \left(\mathcal{X}_{i,l} \bigcap \left(\bigcup_{h<i} \mathcal{X}_{h,j}\right) \setminus \{v_i, v_{i-1}\}\right) = \emptyset$ **then**
　　令 $\lfloor \mathsf{tw}(\mathcal{G})/2 \rfloor + 1$ 个传感器节点沿着 $\mathcal{X}_i$ 到 $\mathcal{X}_{i+1,1}$ 的最短路径监视并搜索 $\mathcal{X}_{i+1,1}$
　else if 存在 $2 \le l^* \le m_i$ 使得 $Z_{l^*} \neq \emptyset$ **then**
　　令传感器节点从 Z_{l^*} 经由 v_i 监视 $\mathcal{X}_{i+1,1}$
　end if
　$\mathcal{X}_i \leftarrow \mathcal{X}_{i+1,1}$
　$i \leftarrow i + 1$
end while

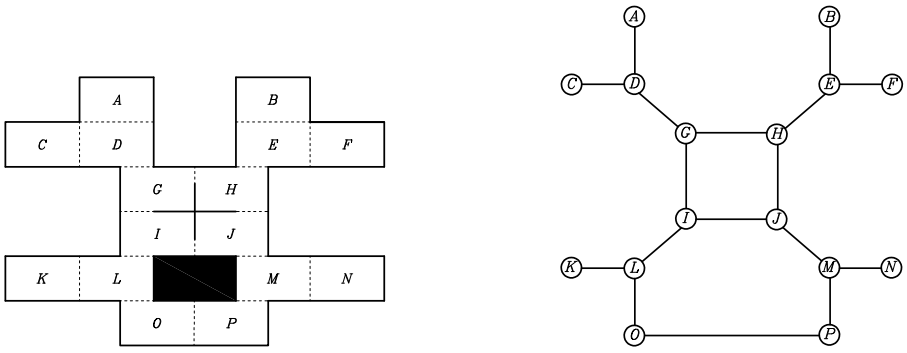
TWGS 搜索算法可以用于所有的有限的、简单连通图，对于没有端点或者只有一个端点的图，我们可以在图中合适的位置加入两个或者一个端点使得在图中可以找到连接两个端点的通路。因此 TWGS 算法对于移动 WSNs 的安全防护具有很好的扩展性。

4.4 仿真结果研究

本章节中，我们给出了两个室内环境中 TWGS 算法的例子，仿真中，假设攻击者的移动速度无限大，也就是说攻击者在一步移动中可以移动到距离传感器节点最远的位置。

4.4.1 数值仿真 1

数值仿真中我们所用的室内环境如图 4–6所示，环境中有一个障碍物。根据传感器节点的感知能力以及移动能力，室内环境 4.6(a)的一种离散化方式如图 4.6(b)所示。



(a) 数值仿真 1 的室内环境　　(b) 相应的离散化后的图 $\mathcal{G}_1$

图 4–6: 室内环境的刻画示意图

Fig 4–6: A Environment Decomposition.

对于图 $\mathcal{G}_1$，选择路径

$$\mathcal{L} = A - D - G - I - L - O - P - M - J - H - E - B$$

按照上面介绍的树分解的方式，可以得出图 $\mathcal{G}_1$ 的最优树分解如图 4–7所示。从图 4–7中我们可以看出每一个树的节点中包含两个顶点，因此 $\mathsf{tw}(\mathcal{G}_1) = 1$。从图中我们可以看出 $\mathcal{X}_{3,2} \bigcap \mathcal{X}_{10,1} = \{H\}$，$\mathcal{X}_{4,2} \bigcap \mathcal{X}_{9,1} = \{J\}$。根据定理 4.1，可以得出，室内环境图 4–6的入侵检测与安全防护所需要的传感器数量为 3。对其

使用 TWGS 算法后，3 个传感器 p_1，p_2，p_3 的移动策略为

$$\begin{bmatrix} A & D & G & H & H & H & H & H & H & H & H & E \\ A & D & G & I & J & J & J & J & J & J & H & E \\ A & D & G & I & L & O & P & M & J & H & E & B \end{bmatrix}.$$

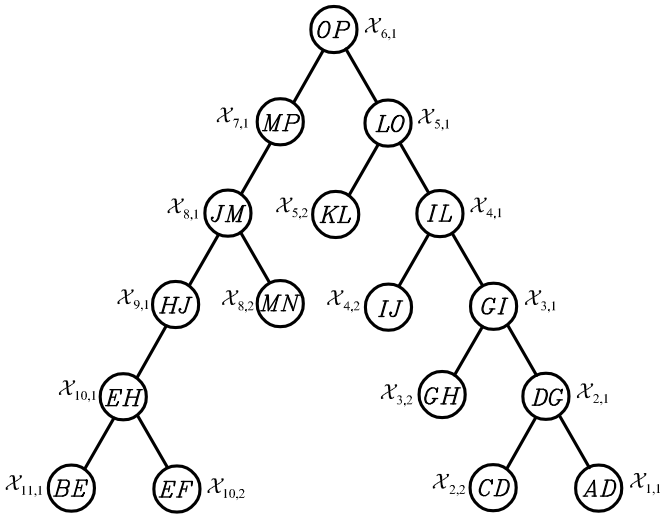


图 4–7: 图 $\mathcal{G}_1$ 最优树分解

Fig 4–7: The optimal tree decomposition of graph $\mathcal{G}_1$.

4.4.2　数值仿真 2

图 4–8为上海交通大学电信群楼某一层的平面图，其相对应的离散化后的图 $\mathcal{G}_2$ 如图 4–9所示，我们可以看出图 $\mathcal{G}_2$ 中含有很多个环。

在图 $\mathcal{G}_2$ 中选取路径

$$\mathcal{L} = 4-11-10-9-16-15-8-7-6-5-30-31-32-33-25-$$

$$26-35-36-37-28-29-22-21-19-12-13,$$

路径 $\mathcal{L}$ 中包含 26 个顶点。图 $\mathcal{G}_2$ 的最优树分解可以简化为如图 4–10所示，其中 $\mathcal{T}_1$，$\mathcal{T}_2$，$\mathcal{T}_3$ 分别表示最优分解树 $\mathcal{T}$ 中的 3 个子树，分别如图 4.11(a)，4.11(b)，4.11(c)所示。

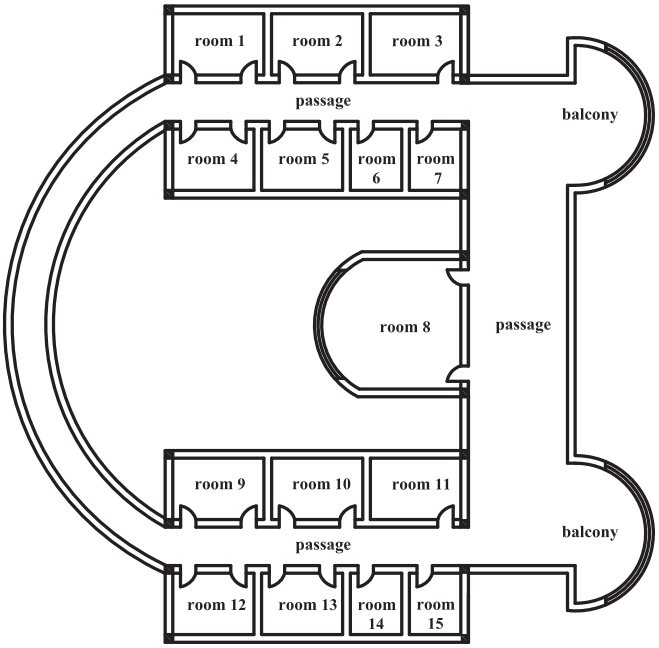


图 4–8: SJTU 某一层的平面图

Fig 4–8: The floor plan of an apartment of SJTU for the second example.

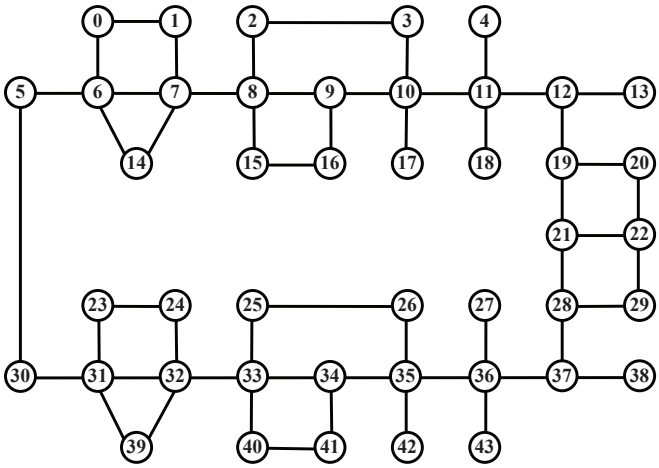


图 4–9: 室内环境离散化后的图 $\mathcal{G}_2$

Fig 4–9: the corresponding graph $\mathcal{G}_2$.

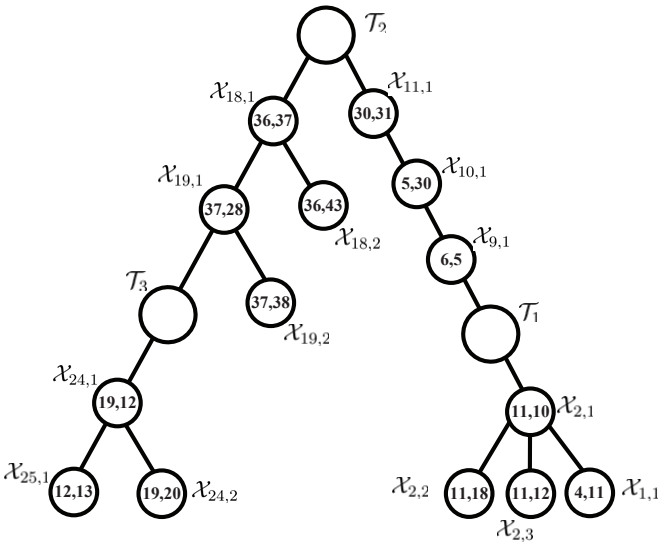


图 4–10: 图 $\mathcal{G}_2$ 最优树分解

Fig 4–10: The optimal tree decomposition of graph $\mathcal{G}_2$.

从以上图中我们可以看出，每个树的节点至多包含 4 个顶点，因此 $\mathsf{tw}(\mathcal{G}_2) = 3$。而且 $\mathcal{X}_{2,3} \bigcap \mathcal{X}_{24,1} = \{12\}$，$\mathcal{X}_{3,2} \bigcap \mathcal{X}_{4,2} = \{8\}$，$\mathcal{X}_{3,2} \bigcap \mathcal{X}_{6,1} = \{8\}$ 且有 $\mathcal{T}_1$ 中 $\mathcal{X}_{8,1} \bigcap \mathcal{X}_{8,2} \bigcap \mathcal{X}_{8,3} = \{6\}$；$\mathcal{T}_2$ 中 $\mathcal{X}_{12,3} \bigcap \mathcal{X}_{12,2} = \{32\}$，$\mathcal{X}_{14,2} \bigcap \mathcal{X}_{17,3} = \{34\}$；$\mathcal{T}_3$ 中有 $\mathcal{X}_{20,2} \bigcap \mathcal{X}_{22,1} = \{21\}$，$\mathcal{X}_{22,2} \bigcap \mathcal{X}_{24,2} = \{20\}$。根据定理 (4.1) 可以得出 4 个传感器就可以对图 $\mathcal{G}_{\in}$ 进行入侵检测及安全防护。假设初始时刻，令所有的传感器 p_1，p_2，p_3，p_4 都移动到顶点 4，对其使用 TWGS 搜索算法后，攻击者最终将在顶点 20 处被监测到并被捕获。传感器 p_1，p_2，p_3，p_4 的移动策略如下：

$$
\begin{bmatrix}
4 & 11 & 12 & 12 & 12 & 12 & 12 & 12 & 12 & 12 & 12 & 12 & 12 & 12 \\
4 & 11 & 10 & 3 & 2 & 8 & 8 & 7 & 1 & 0 & 6 & 5 & 30 & 31 \\
4 & 11 & 10 & 10 & 10 & 9 & 8 & 7 & 7 & 7 & 6 & 5 & 30 & 31 \\
4 & 11 & 10 & 9 & 16 & 15 & 8 & 7 & 7 & 7 & 6 & 5 & 30 & 31
\end{bmatrix}
$$

$$
\begin{bmatrix}
12 & 12 & 12 & 12 & 12 & 12 & 12 & 12 & 12 & 12 & 12 & 12 & 12 & 12 \\
23 & 24 & 32 & 33 & 40 & 41 & 34 & 35 & 36 & 37 & 28 & 21 & 21 & 21 \\
32 & 32 & 32 & 33 & 25 & 26 & 35 & 35 & 36 & 37 & 28 & 29 & 22 & 20 \\
32 & 32 & 32 & 33 & 33 & 33 & 34 & 35 & 36 & 37 & 28 & 29 & 22 & 21
\end{bmatrix}
$$

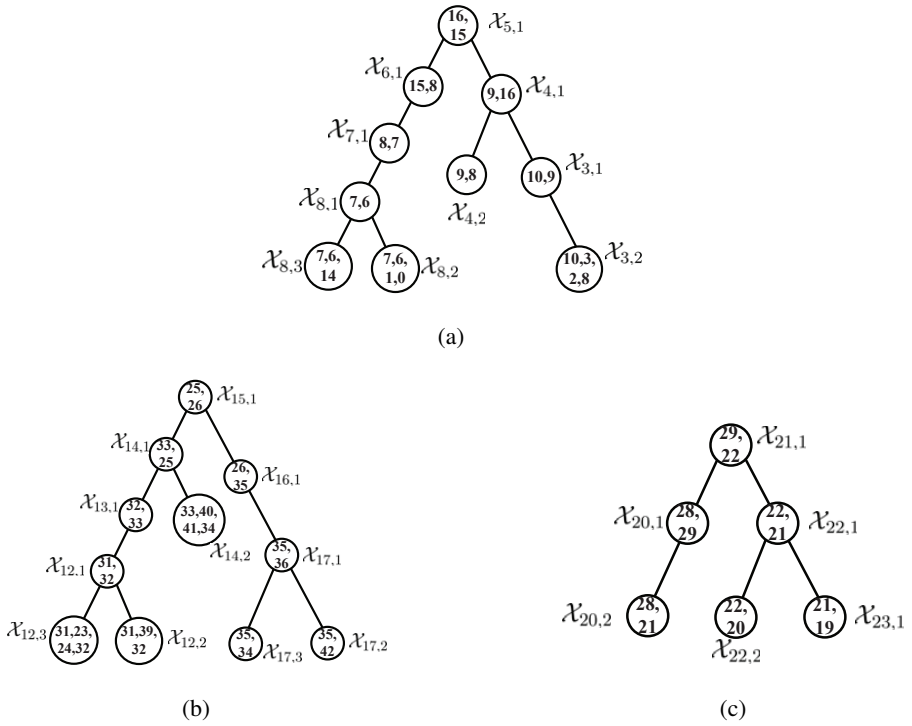


图 4–11: $\mathcal{T}_1$ (a)，$\mathcal{T}_2$ (b)，$\mathcal{T}_3$ (c) 的完整形式

Fig 4–11: The complete form of subtrees $\mathcal{T}_1$ (a), $\mathcal{T}_2$ (b) and $\mathcal{T}_3$ (c), respectively.

4.5 本章小结

本章中我们研究了基于移动传感器网络的室内环境的入侵搜索与安全防护。由于室内环境存在障碍物等具有复杂性，加之传感器节点的感知能力和移动速度有限，我们根据传感器节点的感知范围和移动速度将室内环境离散化为无向有限图。然后根据图的结构我们将图进行树分解，并基于图的树分解我们得出了一个能够成功围捕入侵者所需的传感器节点的最少数量。最后我们提出了一种基于树分解的围捕策略 TWGS，并通过两个数值仿真结果，验证了 TWGS 算法的有效性。室内 PEG 的提出是由于室内环境很像现实生活中的办公室，室内 PEG 可以解决很多在办公室里面人们无法解决的危险问题。它可以代替人进行搜索和救援、安保等等工作。本文虽然解决了室内 PEG 中关于追逐者数量的问题，还有很多问题值得进一步深入研究。

第五章 总结与展望

5.1 工作总结

对于无线传感器网络而言，安全性是其应用中最为关键的因素之一，它直接关系着无线传感器网络的应用能力和对环境的监测性能。但是由于传感器网络中节点存储能力、计算能力、能量有限以及采用无线通信等条件的限制，使得网络的安全机制设计成为一个亟待解决而又非常具有挑战的问题。论文对无线传感器网络中分布式计算的安全机制进行了研究，并利用移动传感器网络实现了对被监测环境的保护。本论文的主要贡献如下:

1. 针对无线传感器网络中的数据篡改攻击，尤其是隐蔽的恶意数据注入攻击，进行了建模，并提出了一种自适应的阈值检测算法，通过传感器网络的协同感知能力，基于加权平均一致性算法提出了一种分布式安全机制设计方法。算法中，节点根据邻居节点数据与自身数据的差值与预先设定的阈值做比较，若差值大于阈值则认为该邻居节点为恶意节点，并将其排除网络。基于加权平均分布式估计算法中，将攻击注入的恶意数据看作噪声，采用加权平均的方法进行去噪，通过定理证明了算法的收敛效果和收敛结果，网络收敛到节点初始状态的平均值。数值仿真表明该算法可以有效地抵御数据篡改攻击。

2. 论文讨论了大规模无线传感器网络中，部署由主节点与中继节点组成的异构传感器网络来加强网络的连通性，并延长网络寿命。针对网络中的数据篡改攻击，充分利用一致性数据融合过程中信息对等交互的特点，提出了基于无偏估计的分布式一致性安全算法。算法通过改变数据融合中节点数据的权重，并将其设置为自适应调整的动态阈值，来减小恶意节点的影响。自适应的动态阈值使得精度较低、与邻居节点探测结果相差较大的节点能够逐渐恢复其在融合过程中的权重，同时提高了网络的安全性。

3. 移动传感器网络可以解决很多环境中人们无法解决的危险问题。室内环境中由于空间封闭、视线有限等存在很多的安全问题。本文研究了基于

移动无线传感器网络的入侵搜索与安全防护。由于室内环境中存在障碍物等具有复杂性使得传感器节点的移动速度受限，而入侵者的能力可能很强大。针对此情况，本文利用图论知识，根据传感器节点的感知范围和移动速度，将室内环境离散化为图，并对其进行树分解，基于图的树分解得出了一个能够成功围捕入侵者所需的传感器节点的最少数量，并设计了一种基于树分解的围捕策略 TWGS，以保证室内环境的安全。

5.2 课题研究展望

本文针对无线传感器网络中的安全进行了研究，重点研究了数据篡改攻击下的安全机制设计。事实上，对于无线传感器网络的安全防御还处于起步阶段，还有很多的问题需要进一步解决。在接下来的工作中，主要从以下方面进行深入的研究：

1. 论文中的分布式估计问题假设节点间的通信是理想的，但是无线传感器网络的应用环境中，大部分环境恶劣且存在电磁干扰、阴影衰落等，节点之间的通信中会存在时延、丢包等。在这情况下的分布式估计问题，值得我们进一步研究。

2. 大多数检测算法对网络中的所有节点进行检测，没有对其受到攻击产生的影响来区分节点的重要性。这种检测算法的效率比较低，并且耗能较大。在大规模网络中，传感器节点的数量很多，整个网络的性能由于增加安全机制可能会降低。因此，如何辨别受到攻击概率较大的节点，如何有选择性的对节点进行检测，是接下来要研究的一个重要方向。

3. 论文中我们的检测算法都是针对静止的传感器网络，但是随着物联网的发展，移动的传感器节点（如已经普及的智能手机实际上已经成为一种典型的移动传感器网络）是未来网络发展的重要趋势，如何对移动的传感器网络进行安全检测是未来研究的迫切任务。

4. 针对被监测环境的安全问题，论文中我们得出了移动传感器节点最少数量的问题，但是安全问题是一个时间问题，需要进行快速解决，因此，如何利用最少的传感器节点进行最快速度的检测并捕获入侵者需要更加深入的研究。

参考文献

[1] Akyildiz I F, Su W, Sankarasubramaniam Y, et al. Wireless sensor networks: a survey[J]. Computer networks, 2002, 38(4):393–422.

[2] 孙利民. 无线传感器网络 [M]. 北京: 清华大学出版社, 2005.

[3] Yick J, Mukherjee B, Ghosal D. Wireless sensor network survey[J]. Computer networks, 2008, 52(12):2292–2330.

[4] Xu N. A survey of sensor network applications[J]. IEEE Communications Magazine, 2002, 40(8):102–114.

[5] 任丰原, 黄海宁, 林闯等. 无线传感器网络 [J]. 软件学报, 2003, 14(7):1282–1291.

[6] Gao T, Massey T, Selavo L, et al. The advanced health and disaster aid network: A light-weight wireless medical system for triage[J]. IEEE Transactions on Biomedical Circuits and Systems,, 2007, 1(3):203–216.

[7] Du R, Chen C, Yang B, et al. Effective urban traffic monitoring by vehicular sensor networks[J]. IEEE Transactions on Vehicular Technology, 2014. DOI:10.1109/TVT.2014.2321010.

[8] Zhu S, Xie L, Chen C, et al. Collective behavior of mobile agents with state-dependent interactions[J]. Automatica, 2014. DOI: 10.1016/j.automatica.2014.10.064.

[9] Buratti C, Conti A, Dardari D, et al. An overview on wireless sensor networks technology and evolution[J]. Sensors, 2009, 9(9):6869–6896.

[10] Chong C Y, Kumar S P. Sensor networks: evolution, opportunities, and challenges[J]. Proceedings of the IEEE, 2003, 91(8):1247–1256.

[11] Jadbabaie A, Lin J, Morse A S. Coordination of groups of mobile autonomous agents using nearest neighbor rules[J]. IEEE Transactions on Automatic Control, 2003, 48(6):988–1001.

[12] Chen C, Zhu S, Guan X, et al. Wireless sensor networks: Distributed consensus estimation[M]. Berlin, Germany: SpringerBrief, 2014.

[13] Olfati-Saber R. Flocking for multi-agent dynamic systems: Algorithms and theory[J]. IEEE Transactions on Automatic Control, 2006, 51(3):401–420.

[14] Ji M, Egerstedt M B. Distributed Coordination Control of Multi-Agent Systems While Preserving Connectedness[J]. IEEE Transactions on Robotics, 2007, 23(4):693–703.

[15] Yang P, Freeman R A, Lynch K M. Multi-agent coordination by decentralized estimation and control[J]. IEEE Transactions on Automatic Control, 2008, 53(11):2480–2496.

[16] Cortes J, Martinez S, Karatas T, et al. Coverage control for mobile sensing networks[C]. Proceedings of IEEE International Conference on Robotics and Automation(ICRA'02). Washington, DC, USA: IEEE, May. 11-15, 2002, 2:1327–1332.

[17] Mpitziopoulos A, Gavalas D, Konstantopoulos C, et al. A survey on jamming attacks and countermeasures in WSNs[J]. Communications Surveys & Tutorials, 2009, 11(4):42–56.

[18] Raymond D R, Midkiff S F. Denial-of-service in wireless sensor networks: Attacks and defenses[J]. Pervasive Computing, 2008, 7(1):74–81.

[19] Yan Q, Li M, Jiang T, et al. Vulnerability and protection for distributed consensus-based spectrum sensing in cognitive radio networks[C]. Proceedings of INFOCOM. Orlando, USA: IEEE, Mar. 25-30, 2012:900–908.

[20] Liu S, Zhu H, Li S, et al. An Adaptive Deviation-tolerant Secure Scheme for distributed cooperative spectrum sensing[C]. Proceedings of Global Communi-

cations Conference (GLOBECOM), 2012 IEEE. Anaheim, USA: IEEE, Dec. 3-7, 2012:603–608.

[21] LeBlanc H J, Koutsoukos X D. Consensus in networked multi-agent systems with adversaries[C]. Proceedings of the 14th international conference on Hybrid systems: computation and control. New York, USA: ACM, Apr. 12-14, 2011:281–290.

[22] Franco E, Olfati-Saber R, Parisini T, et al. Distributed fault diagnosis using sensor networks and consensus-based filters[C]. Proceedings of the 45th IEEE Conference on Decision and Control. San Diego, USA: IEEE, Dec. 13-15, 2006:386–391.

[23] Pasqualetti F, Bicchi A, Bullo F. Distributed intrusion detection for secure consensus computations[C]. Proceedings of the 46th IEEE Conference on Decision and Control. New Orleans, USA: IEEE, Dec. 12-14, 2007:5594–5599.

[24] Pasqualetti F, Bicchi A, Bullo F. Consensus computation in unreliable networks: A system theoretic approach[J]. IEEE Transactions on Automatic Control, 2012, 57(1):90–104.

[25] LeBlanc H J, Zhang H, Koutsoukos X, et al. Resilient asymptotic consensus in robust networks[J]. IEEE Journal on Selected Areas in Communications, 2013, 31(4):766–781.

[26] Pathan A, Lee H W, Hong C S. Security in wireless sensor networks: issues and challenges[C]. Proceedings of the 8th International Conference Advanced Communication Technology (ICACT'06). Phoenix Park, UK: IEEE, Feb. 20-23, 2006, 2:1043–1048.

[27] Liu Y, Ning P, Reiter M K. False data injection attacks against state estimation in electric power grids[J]. ACM Transactions on Information and System Security (TISSEC), 2011, 14(1):13.

[28] Olfati-Saber R, Fax J A, Murray R M. Consensus and cooperation in networked multi-agent systems[J]. Proceedings of the IEEE, 2007, 95(1):215–233.

[29] Wang I J, Chong E K, Kulkarni S R. Weighted averaging and stochastic approximation[J]. Mathematics of Control, Signals and Systems, 1997, 10(1):41–60.

[30] Stankovic S S, Stankovic M S, Stipanovic D M. Decentralized parameter estimation by consensus based stochastic approximation[J]. IEEE Transactions on Automatic Control, 2011, 56(3):531–543.

[31] Schizas I D, Ribeiro A, Giannakis G B. Consensus in ad hoc WSNs with noisy links—Part I: Distributed estimation of deterministic signals[J]. IEEE Transactions on Signal Processing, 2008, 56(1):350–364.

[32] Speranzon A, Fischione C, Johansson K H, et al. A distributed minimum variance estimator for sensor networks[J]. IEEE Journal on Selected Areas in Communications, 2008, 26(4):609–621.

[33] Olfati-Saber R, Shamma J S. Consensus filters for sensor networks and distributed sensor fusion[C]. Proceedings of the 44th IEEE Conference on Decision and Control & 2005 European Control Conference (CDC-ECC'05). Seville, Spain: IEEE, Dec. 12-15, 2005:6698–6703.

[34] Xiao L, Boyd S, Lall S. A scheme for robust distributed sensor fusion based on average consensus[C]. Proceedings of the 4th International Symposium on Information Processing in Sensor Networks (IPSN'05). Los Angeles, USA: IEEE, Apr. 25-27, 2005:63–70.

[35] Barbarossa S, Scutari G. Decentralized maximum-likelihood estimation for sensor networks composed of nonlinearly coupled dynamical systems[J]. IEEE Transactions on Signal Processing, 2007, 55(7):3456–3470.

[36] Chen C, Yan J, Lu N, et al. Ubiquitous monitoring for industrial cyber-physical systems over relay assisted wireless sensor networks.[J]. IEEE Transaction on Emerging Topics in Computing, 2014. DOI: 10.1109/TETC.2014.2386615.

[37] Zhu S, Chen C, Ma X, et al. Consensus based estimation over relay assisted sensor networks for situation monitoring.[J]. IEEE Transaction on Emerging Topics in Computing, 2014. DOI: 10.1109/JSTSP.2014.2375851.

[38] YAN J, CHEN C, LUO X, et al. Topology optimization based distributed estimation in relay assisted wireless sensor networks.[J]. IET Control Theory & Applications, 2014. DOI: 10.1049/iet-cta.2014.0163.

[39] ZHU S, CHEN C, GUAN X. Distributed optimal consensus filter for target tracking in heterogeneous sensor networks[C]. Proceedings of the 8th Asian Control Conference (ASCC). Taiwan: IEEE, May. 15-18, 2011:806–811.

[40] ZHU S, CHEN C, GUAN X. Consensus protocol for heterogeneous multi-agent systems: A Markov chain approach[J]. Chinese Physics B, 2013, 22(1):018901.

[41] ZHU S, CHEN C, GUAN X. Sensor Deployment for Distributed Estimation in Heterogeneous Wireless Sensor Networks.[J]. Ad Hoc & Sensor Wireless Networks, 2012, 16(4):297–322.

[42] CHEN X, DAI Z, LI W, et al. ProHet: a probabilistic routing protocol with assured delivery rate in wireless heterogeneous sensor networks[J]. IEEE Transactions on wireless communications, 2013, 12(4):1524–1531.

[43] HEFEIDA M S, CANLI T, KHOKHAR A. Cl-mac: A cross-layer mac protocol for heterogeneous wireless sensor networks[J]. Ad Hoc Networks, 2013, 11(1):213–225.

[44] HORN R A, JOHNSON C R. Matrix analysis[M]. Cambridge: Cambridge university press, 2012.

[45] AKYILDIZ I F, KASIMOGLU I H. Wireless sensor and actor networks: research challenges[J]. Ad hoc networks, 2004, 2(4):351–367.

[46] CHAN H, PERRIG A. Security and privacy in sensor networks[J]. Computer, 2003, 36(10):103–105.

[47] SMAILAGIC A, KOGAN D. Location sensing and privacy in a context-aware computing environment[J]. Wireless Communications, 2002, 9(5):10–17.

[48] YAN J, GUAN X, LUO X, et al. Formation control and obstacle avoidance for multi-agent systems based on virtual leader-follower strategy.[J]. International Journal of Information Technology & Decision Making, 2013:1–16.

[49] YAN J, GUAN X P, LUO X Y, et al. A cooperative pursuit-evasion game in wireless sensor and actor networks[J]. Journal of Parallel and Distributed Computing, 2013, 73(9):1267–1276.

[50] DU R, CHEN C, ZHANG X, et al. Path Planning and Obstacle Avoidance for PEGs in WSAN: I-ACO Based Algorithms and Implementation.[J]. Ad Hoc & Sensor Wireless Networks, 2012, 16(4):323–345.

[51] ALSPACH B. Searching and sweeping graphs: a brief survey[J]. Le matematiche, 2006, 59(1, 2):5–37.

[52] FOMIN F V, THILIKOS D M. An annotated bibliography on guaranteed graph searching[J]. Theoretical Computer Science, 2008, 399(3):236–245.

[53] CHEN P, SASTRY S. Pursuit controller performance guarantees for a lifeline pursuit-evasion game over a wireless sensor network[C]. Proceedings of the 45th IEEE Conference onDecision and Control. San Diego, USA: IEEE, Dec. 13-15, 2006:691–696.

[54] VIEIRA M A, GOVINDAN R, SUKHATME G S. Scalable and practical pursuit-evasion with networked robots[J]. Intelligent Service Robotics, 2009, 2(4):247–263.

[55] FRANKL P. Cops and robbers in graphs with large girth and Cayley graphs[J]. Discrete Applied Mathematics, 1987, 17(3):301–305.

[56] CHINIFOROOSHAN E. A better bound for the cop number of general graphs[J]. Journal of Graph Theory, 2008, 58(1):45–48.

[57] AIGNER M, FROMME M. A game of cops and robbers[J]. Discrete Applied Mathematics, 1984, 8(1):1–12.

[58] LU L, PENG X. On Meyniel's conjecture of the cop number[J]. Journal of Graph Theory, 2012, 71(2):192–205.

[59] Fomin F V, Golovach P A, Kratochvíl J, et al. Pursuing a fast robber on a graph[J]. Theoretical Computer Science, 2010, 411(7):1167–1181.

[60] Frieze A, Krivelevich M, Loh P S. Variations on cops and robbers[J]. Journal of Graph Theory, 2012, 69(4):383–402.

[61] Mehrabian A. Lower bounds for the cop number when the robber is fast[J]. Combinatorics, Probability and Computing, 2011, 20(04):617–621.

[62] Bollobás B. Graph theory[M]. Amsterdam: Elsevier, 1982.

[63] Robertson N, Seymour P D. Graph minors. II. Algorithmic aspects of tree-width[J]. Journal of algorithms, 1986, 7(3):309–322.

[64] Goldberg A V, Harrelson C. Computing the shortest path: A search meets graph theory[C]. Proceedings of the 16th annual ACM-SIAM symposium on Discrete algorithms. Philadelphia, USA: Society for Industrial and Applied Mathematics, Jan. 23, 2005:156–165.

[65] Kirousis L M, Papadimitriou C H. Interval graphs and seatching[J]. Discrete Mathematics, 1985, 55(2):181–184.

[66] Fomin F V, Golovach P A. Graph searching and interval completion[J]. SIAM Journal on Discrete Mathematics, 2000, 13(4):454–464.

[67] Chung T H, Hollinger G A, Isler V. Search and pursuit-evasion in mobile robotics[J]. Autonomous Robots, 2011, 31(4):299–316.

致 谢

值此论文完成之际，我的心中充满了喜悦和感激，谨向关心、支持、帮助我的人们致以最诚挚的谢意!

首先，感谢我的导师关新平教授。从课题的选择到项目的最终完成，关老师都始终给予我细心的指导和不懈的支持。他渊博的学识、卓越的眼光、敏捷的思维使我受益匪浅；另外他严谨的治学态度、科学的研究方法、忘我的工作激情以及对问题的高瞻远瞩，给予我无尽的启迪，是我终生为人为学的楷模。

感谢陈彩莲教授在学习和生活方面给我的关心和帮助。陈老师为人谦和，对待工作态度认真严谨。研究生期间取得的大部分科研成果都离不开陈老师的辛勤付出，在与陈老师的讨论中帮我理清了问题的思路，她宝贵的科研经验将让我受益无穷。

感谢课题组所有老师，为我提供的良好实验条件、浓厚的学术氛围。感谢实验室的朱善迎学长及其他学长、学姐在我的研究遇到困难时给予了指导和帮助，使我的研究能继续顺利地开展下去。同时也感谢实验室的同学们，给我创造了一个和谐融洽的学习氛围。感谢上海交通大学给我提供了一个风景秀美、学术氛围浓厚的环境，让我在这里得到成长。

感谢 B203292 班的全体同学，在共同的学习生活中与你们结下了深厚的友谊，并陪伴我度过了丰富多彩的硕士生活。感谢我的室友们，从遥远的家来到这个陌生的城市里，是你们和我共同维系着彼此之间姐妹般的感情，维系着寝室那份家的融洽。两年半过去了，仿佛就在昨天。两年半里，我们就像家人一样彼此理解与支持，共享快乐，同担困苦。各奔前程，大家珍重。

深切感谢父母多年来对我的无私抚育，他们给了我人生中最大的恩惠与财富。他们一直以来对我的培养、信任和无私地付出。在我人生的每一个转折点上，都有他们的默默支持，我的每一点成绩背后都有他们的鼓励和理解。

再一次感谢所有帮助过我的人，祝大家一切顺利!

攻读学位期间发表的学术论文目录

[1] Shichao Mi, Shanying Zhu, Cailian Chen and Xinping Guan, TWGS: A Tree Decomposition Based Indoor Pursuit-Evasion Game for Robotic Networks[C], *Proc. of 13th IFAC Symposium on Large Scale Complex Systems: Theory and Applications*, pp: 135-140, Shanghai, China. Jul.7-10, 2013.

[2] Shichao Mi, Hui Han, Shanying Zhu, Cailian Chen, Bo Yang and Xinping Guan, A Secure Distributed Consensus Scheme for Wireless Sensor Networks Against Data Falsification[C], *Proc. of the 11th World Congress on Intelligent Control and Automation (WCICA)*, pp: 3025-3030, Shenyang, China, Jun.29-Jul.4, 2014.

[3] Shichao Mi, Hui Han, Jianzhi Liu, Cailian Chen, Bo Yang and Xinping Guan, A Distributed Consensus-based Secure Scheme for Heterogeneous Sensor Networks Against Data Falsification[J], *International Journal of Distributed Sensor Networks (IJDSN)*, 2014 (under review).

攻读学位期间参与的项目

[1] 面向地空复杂电磁环境分布式协同监测的自组网技术研究，国家重点实验室开放性课题（CEMEE2014K0102A），2013.10–2014.10

[2] 基于认知无线电的工业无线网络理论与优化方法, 国家自然科学基金重点项目 (60934003)，2010.01-2013.12