分簇无线传感器网络内部安全关键技术研究

叶正旺　著

吉林大学出版社

分簇无线传感器网络内部安全关键技术研究

叶正旺 / 著

吉林大学出版社

图书在版编目（CIP）数据

分簇无线传感器网络内部安全关键技术研究 / 叶正旺著 .—长春 : 吉林大学出版社 , 2019.9
ISBN 978-7-5692-5657-4

Ⅰ . ①分… Ⅱ . ①叶… Ⅲ . ①无线电通信—传感器—计算机网络—安全技术—研究 Ⅳ . ① TP212 ② TP393.08

中国版本图书馆 CIP 数据核字 (2019) 第 219110 号

书　　名　分簇无线传感器网络内部安全关键技术研究
FENCU WUXIAN CHUANGANQI WANGLUO NEIBU ANQUAN GUANJIAN JISHU YANJIU

作　　者　叶正旺　著
策划编辑　张树臣
责任编辑　张树臣
责任校对　曲　楠
装帧设计　张沭沉
出版发行　吉林大学出版社
社　　址　长春市人民大街 4059 号
邮政编码　130021
发行电话　0431-89580028/29/21
网　　址　http://www.jlup.com.cn
电子邮箱　jdcbs@jlu.edu.cn
印　　刷　吉林省科普印刷有限公司
开　　本　787mm × 1092mm　1/16
印　　张　10.875
字　　数　180 千字
版　　次　2019 年 9 月　第 1 版
印　　次　2019 年 9 月　第 1 版
书　　号　ISBN 978-7-5692-5657-4
定　　价　68.00 元

目 录

第一章

第二章

第三章

第四章

第五章

第六章

第七章

第一章

DIYIZHANG

绪 论

随着嵌入式系统、无线通信、网络及MEMS等技术的快速发展，无线传感器网络(Wireless Sensor Network WSN)[1][2]已被广泛应用于不同环境和行业下进行监控和数据收集，随之带来的网络安全问题也日渐受到人们的重视，尤其是在军事、商业、医疗、公共安全、智能交通和工业等领域的应用。但是，由于传感器节点受能量、计算、存储等资源的限制，如何设计实现高效可用的无线传感器网络安全机制成为无线传感器网络的核心问题，尤其是妥协节点或捕获节点发起的内部安全威胁。目前，针对无线传感器网络安全的研究受到了国内外学者的广泛关注，已成为无线传感网络研究的热点。本书主要针对分簇无线传感器网络内部安全展开研究，对网络运行的各个阶段的功能需求和安全需求进行分析，从拓扑构建、节点通信、数据融合、路由等关键技术进行了深入研究并提出了相应的安全措施，以提高网络的安全性。本章作为绪论，首先简单介绍了无线传感器网络的应用以及研究背景。其次，阐述了本书研究的问题和意义，并概述了主要研究工作和创新点。最后，介绍了本书的组织结构。

第一节 研究背景

无线传感器网络技术是物联网信息感知体系的核心技术，是推进物联网应用的首要着力点。早在1999年，著名的美国商业周刊便将无线传感器网络列为21世纪最具影响的21项技术之一；2003年，MIT技术评论 Technology Review 在预测未来技术发展的报告中，将无线传感器网络列为改变世界十大新技术之一。

无线传感器网络是由大量具有通信和计算能力的微小传感器节点部

署在监控区域，通过无线通信方式形成一个多跳的自组织网络系统，其目的是协作感知、采集和处理网络覆盖区域中感知对象的信息，并发送给观察者。传感器、感知对象和观察者构成了传感器网络的三个要素[3]。一般来说，传感器节点具有灵活、方便、廉价且易于部署等特点并已经渗入到军事、医疗、工农业、环境监测等诸多领域[4][5]。在国防和军事领域，美陆军提出“灵巧传感器网络通信”计划，并在2005年开展了“无人值守地面9传感器群”项目，美海军确立了“传感器组网系统”研究项目[5]。美国国防部在C4ISR项目的基础上提出了C4KISR计划[6]，美国Sandia国家实验室与能源部合作确立开发检测有毒气体化学成分的化学传感器网络系统的反恐项目。美陆军在俄亥俄州开发用于战场探测的无线传感器网络系统项目——沙地直线(A Line In The Sand)项目[7][8]。美国BAE系统公司于2012年研发“狼群”地面无线传感器网络系统。在环境监测和气象研究领域，英国南安普顿大学在2003～2006年期间开展了GlacsWe系统项目[9]。日本宽带项目（WIDE）执行主席江崎浩教授（Hiroshi Esaki）于2005年启动Live-E！项目[10]。澳大利亚墨尔本大学和詹姆斯库克大学于2007年开始合作部署GBR无线传感器网络应用系统[11]。美国加州大学伯克利分校Intel实验室启动“in-situ”项目，欧洲电信开发和战略研究所于2011年完成了欧盟第七研究框架计划中的研究项目WSAN4CIP。在医疗卫生领域，美国范德比特大学于2007年开展了CareNet项目[12]用于远程医疗保健。与此类似的研究还有术后病人恢复监控系统HipGuard[13]项目、iCabliNET项目[14]、远程健康保健系统MOBiHealth[15][16]和基于环形传感器的移动健康监测系统MHMS[17]。欧洲开展了欧盟资助下的AmbulanceandEmergency-112项目，日本北海道大学的一个远程医疗研究小组成功研制了多种移动通信方式的远程监护系统。在智能交通领域，美国的马萨诸塞大学建立的UMass DieselNet智能公交系统，美国加州大学伯克利分校的ATMIS项目，美国哈佛大学和BBN公司于2007年开始在麻省剑桥部署的City Sense无线传感器网络系统[18]都是无线传感器网络在道路交通监测方面的应用。欧洲启动了由布鲁塞尔的ERTICO组织统筹的CVIS系统开发，日本启动了由NPA (National Police Agency)等5个相关部门和机构共同开发的UTMS 21系统，这是继20世纪90年代初UTMS系统以来的第2代交通管理系统。在工业领域，2004年，美国能源部（Doe）发

布“未来工业计划（IOF）”中指出，基于工业无线技术的低成本测控系统是实现到2020年美国工业整体能耗减低5%目标的主要手段，代表工业自动化系统技术的发展方向，将在石油天然气开采，石化，冶金，污水处理等高能耗，高污染行业有广泛的应用前景；美国总统科技顾问委员会在“面向21世纪的联邦能源研究与发展规划”中指出，工业无线技术的广泛应用将使工业生产效率提高10%，并使排放和污染降低25%。中国产业信息网（http://www.chyxx.com）发布的《2016～2022年中国无线传感器网络市场评估及市场发展趋势研究报告》中可以看到：随着工业4.0概念的逐渐推广，工业生产智能化成为未来工业转型的重要手段，作为工业智能化重要技术之一的无线传感器网络技术必将发挥越来越重要的作用，而工业无线传感器网络市场也将赢来更为广阔的发展机遇，行业增长速度有望稳定增长。数据显示，2014年我国工业无线传感器网络市场为6.2亿元，预计到2019年，其市场规模可达到24.2亿元，复合增长达31.31%。

随着无线传感器网络技术的广泛应用，网络的安全问题日渐受到人们的重视，尤其在军事、商业、医疗、公共安全、智能交通和工业等领域的应用，这些敏感信息的泄露或篡改将导致国家、企业和个人利益蒙受巨大损失。因此，无线传感器网络的安全性是其能否得到广泛应用的一个关键所在。

无线传感器网络的安全问题主要来源于其固有的特点：如无线传输、节点资源受限、网络规模大、节点部署密集、缺少固定的网络基础设施、拓扑动态变化、部署区域开放以及节点无人值守等。由于这些固有的特点使得无线传感器网络中的节点物理上是不安全的，节点易受到各种恶意攻击，如窃听攻击、数据篡改、重放攻击、伪造身份、拒绝服务和节点俘获等。根据恶意攻击的发起源不同，恶意攻击可以分为外部攻击和内部攻击两种类型[19]。

（1）外部攻击：是指攻击者部署在要攻击的无线传感器网络外部的恶意节点，该类节点由于无法获取网络内部的密钥信息和合法认证，因而无法建立与网络内合法节点的信任通信关系，只能对无线网络信道进行监听，对网络内部通信进行干扰。对于这些外部恶意节点引起的外部攻击的防范可以通过认证和加密机制来实现。

（2）内部攻击：是指攻击者已经突破加密、身份认证等方式设置的第一层安全防护，掌握了相应的安全加密方式，并已拥有的合法身份从网络运行过程中主动地发起有针对性的、蓄意的、串谋的攻击行为。这种拥有合法身份的内部恶意节点引起的内部攻击可参与数据采集、数据传输等网络关键服务，从而可以实现对转发数据的篡改、注入和丢弃等，这种攻击节点具有高度的隐蔽性，一般情况下难以被安全机制察觉，对网络造成的危害更加不可预期。

对于无线传感器网络安全研究，如果假定节点是可信的，那么，无线传感器网络安全机制的设计就与传统网络相似，只针对外部攻击做出安全策略，考虑能量、计算、存储等资源的限制构造以密钥为安全根基的网络安全体系是基本方向。但是，在现实中无线传感器网络节点极易遭受攻击变为妥协节点转变为内部攻击，导致其上的软件和秘密信息的物理安全也不能保证。例如基于密钥管理的安全机制[20][21][22]、基本安全服务CINA^{3}及隐私保护（Privacy-preserving）[23]等安全技术可以降低网络被恶意攻击的可能性，针对网络的外部攻击有较好的防御效果，但是都无法解决内部攻击问题。因为攻击者已经突破加密、身份认证等方式设置的第一层安全防护，以合法的身份从网络内部实施攻击，可以在网络的各个运行阶段发起恶意攻击，包括网络拓扑的建立、节点通信、数据融合和路由传输等。

因此，设计无线传感器网络安全机制需要考虑两部分工作，一部分是针对外部攻击的安全机制，另一部分是应对因物理节点受到攻击引发的内部攻击。在节点计算能力、存储能力和能量受限的无线传感器网络中，无线传感器网络的安全机制设计面临着严峻的挑战，如何实现高效、可靠的安全机制以保障网络的机密性、完整性、认证、授权、新鲜性和可用性等关键问题成为当今研究的热点之一。

第二节　问题的提出与课题的意义

一、问题的提出

由于无线传感器网络的应用环境与运行方式等特点，使得无线传感

器网络中的节点物理上是不安全的，极易受到危及节点物理安全的内部攻击，例如，节点俘获、节点复制攻击、Sybil攻击[24]、DoS攻击[25]、黑洞攻击、虫洞攻击[26]、选择性转发攻击[26]和Sinkhole攻击[25][27]等。这类拥有合法身份的内部恶意节点发起的内部攻击可参与网络运行的各个运行阶段发起不同的恶意攻击，并且具有较高的隐蔽性。在分簇网络拓扑建立阶段，内部恶意节点可以通过节点伪装、恶意征募、多重身份、发布虚假信息等方式破坏分簇协议的正常运行。其中分簇协议面临的各种安全威胁，包括簇首占据攻击、簇成员恶意征募攻击、多重簇成员身份攻击等。在节点通信阶段，成员节点将感知到的数据发送给簇头及其邻居节点，为进行下一步操作提供基础条件。在这个阶段，攻击者可以通过提供虚假信息、不转发信任请求消息或策略性攻击等方式破坏节点间的数据通信的准确性和合法性。其中节点通信评估面临的各种安全威胁，包括间歇性攻击（On-Off攻击）、诽谤攻击、篡改攻击、自攻击等。在数据融合阶段，对采集的信息打包成规定的报文格式，成员节点将数据发送给簇头之后，簇头节点进行融合处理，得到基本数据，在这个阶段，恶意节点攻击者可以通过伪造或篡改感知数据和中间计算结果，造成用户基于错误的网内数据处理结果而做出错误的决策。其中针对通信数据或消息的各种安全威胁，包括篡改攻击、伪造攻击、注入虚假信息、DOS攻击等。在数据传输阶段，通过多跳路由的方式把数据报文传输到基站，簇头节点将融合数据发送给Sink节点，在这个阶段，攻击者可以干扰路由包的转发情况，还可以通过攻击网内数据处理过程来干扰计算和数据传输过程、扩大攻击效果、破坏数据的可用性等。其中针对路由转发的各种安全威胁，包括黑洞攻击、灰洞攻击、虫洞攻击、女巫攻击、选择性攻击等。由以上分析此可知，无线传感器网络的内部安全威胁涉及到网络运行的各个阶段，并表现为多样性[28]，如不及时地检测出网络内部恶意节点，无线传感器网络中的拓扑协议、节点通信、数据融合机制、路由机制等都会受到破坏。因此，在受限的无线传感器网络中，如何从各个层面设计相应的安全机制来有效抵御内部攻击是无线传感器网络安全研究的关键问题之一。

目前，针对无线传感器网络内部安全的研究技术主要可以分为两类：异常检测机制[29][30][31]和基于信任管理的安全机制[32][33][34]。异常检测机

制是通过预定义正常的行为，发现异常的不符合预期的行为来推断异常的存在，该安全机制只针对某一个或者几个特定攻击行为建立攻击行为识别，该方法具有单一性。因此，异常检测机制不能很好地适应复杂攻击的环境。信任模型被认为是一种非常有效的无线传感器网络内部安全机制，该方法通过对网络中节点行为的可信度、能力、可靠性等指标进行评估，依靠主体与客体之间发生的交互行为构成的直接证据以及其他个体反馈的与该客体之间交互行为构成的间接证据进行评估，实现网络中恶意节点的识别，保障网络内部的安全。近年来，基于信任机制的无线传感器网络安全研究已成为国内外学者和科研机构研究的热点，基于信任机制已被应用于无线传感器网络中各个阶段进行安全策略设计，其中包括安全网络拓扑的建立、安全数据融合、安全路由等。虽然信任模型及相关的安全关键技术研究工作取得了一定的进展，但是仍存在很多不足，具体表现在以下几个方面：

（1）在网络拓扑结构中，基于分簇的网络拓扑凭借其简单、灵活、高能效、便于管理、可扩展性强等诸多优势，在现有各类无线传感器网络中得到广泛应用。由于无线传感器网络能量的受限性，目前，研究人员针对分簇拓扑组织下的通信能量有效性、负载均衡等网络性能优化问题提出了多种有效的成簇算法。但是，这些分簇协议设计没有考虑到无线传感器网络面临的安全问题，有一类内部恶意攻击专门针对分簇的拓扑协议进行攻击，使得分簇协议很容易被攻击者破坏和误用。因此，需综合考虑节点的能耗和安全威胁建立安全、高效的分簇拓扑结构。

（2）信任模型被认为是一种非常有效的无线传感器网络内部安全机制，对网络安全及安全、可靠数据传输的改善起到了很大作用，但仍存在以下不足，例如：有些信任评估[33][34][35]仅仅考虑节点之间的通信交互行为而并没有考虑其他信任评价因素，导致信任评估不够精确；信任评估在考虑多种因素计算信任值时，多因素的信任整合采用平均加权法进行整合[36-39]，得到的信任值具有主观性，影响信任决策的科学性和灵活性；现有的信任模型[40][41]中缺乏对网络环境动态性的考虑，影响了信任评估结果的准确性；还有些信任模型[33][38][40]没有考虑能量消耗对信任值的影响；另外，还有一类恶意节点专门针对信任评级进行攻击，通过提供虚假信息或策略性攻击行为影响信任评估。因此，现有的信任评估还存在

不够精确、缺乏动态性等不足，需要建立高效、动态的信任评估模型，实现高效、动态、精确的信任评估，应用于无线传感器网络安全设计。

（3）数据安全是无线传感器网络的基本保障，一切安全措施都是以数据的安全性为目标。但是，无线传感器节点常常被部署在开放环境下工作，极易被俘获、破坏或攻击，攻击者可以通过故意注入错误的数据或篡改数据等方式破坏数据的完整性。另外，传感器节点结构简单易发生故障，也将导致产生错误的数据。针对通信数据或消息的内部恶意攻击，仅仅依靠加密[42]、认证[43]等传统方法的安全算法并不能完全地保障无线传感器网络数据的安全需求[44]。基于信任机制的安全数据融合算法能够及时地、有效地识别俘获节点，有效地解决了内部攻击，实现安全的数据融合。但是，现有的安全数据融合算法也存在很多不足。如有些基于信任评价的安全数据融合算法[45][46]通过建立节点间的信任评估，能够识别发现多种类型的恶意节点攻击行为，有效保障了数据的安全融合。但不能有效抵御如On-Off攻击等策略性恶意节点引发的攻击；很多文献将簇头节点作为数据融合节点进行数据融合与传输，这个过程使簇头节点消耗很大的能量，极易造成簇头节点的能耗耗尽而死亡，影响网络的生命周期；另外，只考虑簇内恶意节点对数据融合安全的影响，并没考虑融合节点被捕获时对数据融合的影响。因此，针对数据的安全性问题，需建立安全的数据融合机制，有效抵御各种类型的恶意攻击，保障数据融合的安全性。

（4）可靠安全的路由协议是数据传输的有力保障，在无线传感器网络内部安全威胁中，专门有一类恶意攻击节点针对无线传感器网络中路由转发发起内部恶意攻击[47][48]，这类恶意攻击行为表现为：丢弃所有路由包或丢弃部分路由包、异常转发等，使数据包不能在节点之间正确转发。如黑洞攻击、灰洞攻击、虫洞攻击等。目前，国内外已经做了许多安全路由相关的研究[49][50]，基于信任的无线传感器网络安全路由的研究已经取得了很多研究成果[51]，但是很少文献[52][53][54]考虑针对信任模型的这类特殊的恶意攻击。另外，在考虑路由安全的同时，现有文献很少考虑由于节点或链路的故障导致数据丢失或重发的问题。因此，为了能够有效抵御各种内部恶意节点对路由发起的攻击，并能够保障节点失效情况下数据传输的可靠性，需要建立安全容错路由，实现无线传感器网络安