WUXIANCHUANGANQIWANGLUO
ANQUANJISHUYANJIU

无线传感器网络安全技术研究

张楠 著

西南交通大学出版社
Http://press.swjtu.edu.cn

无线传感器网络安全技术研究

张 楠 著

西南交通大学出版社
·成都·

内 容 提 要

本书针对无线传感器网络的安全问题，分析了无线传感器网络所面临的安全威胁及对应的安全策略，重点探讨了无线传感器网络的密钥管理、路由协议等问题，同时创新性地提出了基于混沌的密钥预分配技术、基于免疫的数据融合技术等。本书可供计算机、通信、电子和自动化领域的科研人员和工程技术人员参考，也可以作为相关专业本科高年级学生和研究生的参考书。

图书在版编目（CIP）数据

无线传感器网络安全技术研究 /张楠著. —成都：西南交通大学出版社，2010.8
ISBN 978-7-5643-0772-1

Ⅰ. ①无… Ⅱ. ①张… Ⅲ. ①无线电通信－传感器－安全技术 Ⅳ. ①TP212

中国版本图书馆CIP数据核字（2010）第149033号

无线传感器网络安全技术研究

张 楠 著

*

责任编辑 张宝华
封面设计 本格设计
西南交通大学出版社出版发行
（成都二环路北一段111号 邮政编码：610031
发行部电话：028-87600564）
http://press.swjtu.edu.cn
成都蓉军广告印务有限责任公司印刷

*

成品尺寸：146 mm×208 mm 印张：7.687 5
字数：214千字
2010年8月第1版 2010年8月第1次印刷
ISBN 978-7-5643-0772-1
定价：22.00元

内容提要

无线传感器网络是由大量传感器节点通过无线通信技术以自组织方式构成的网络，在军用和民用方面有着广泛的应用前景。本书针对无线传感器网络的安全问题，分析了无线传感器网络所面临的安全威胁及对应的安全策略，重点探讨了无线传感器网络的密钥管理、路由协议、入侵检测、认证等关键技术，对最新研究成果进行了总结。同时创新性地提出了基于混沌的密钥预分配技术、基于免疫的数据融合技术、任播路由技术及基于 Muti-Agent 的入侵检测技术等，为无线传感器网络安全提供了新的发展思路。本书可供计算机、通信、电子和自动化领域的科研人员和工程技术人员参考，也可以作为相关专业本科高年级学生和研究生的参考书。

目 录

1 绪 论

1.1 无线传感器网络概述

随着通信技术、嵌入式计算技术和传感器技术的日益成熟，微机电系统（Micro-electro-mechanism system, MEMS）、片上系统（SOC，System on chip）、无线通信和低功耗嵌入式技术得到了飞速发展，同时也孕育出无线传感器网络[1]（Wireless sensor networks, WSN），而且它正以其低功耗、低成本、分布式和自组织等特点带来了信息感知的一场变革。无线传感器网络是由部署在监测区域内大量的廉价微型传感器节点组成，通过无线通信方式形成的一个多跳自组织网络。它将大量具有传感器、数据处理单元及通信模块的智能节点散布在感知区域，通过节点间的自组织方式工作；它综合了传感器技术、嵌入式计算技术、分布式信息处理技术和无线通信技术，能够协同地实时监测、感知和采集网络分布区域内的各种环境或监测对象的信息，并对这些数据进行处理，获得详尽而准确的信息，同时将这些信息传送到需要这些信息的用户当中[2]。与传统中心处理方式相比，它具有鲁棒性高、准确性高、灵活性高及智能化强等优点，主要应用于空间探测、环境观测与预报系统、智能家居、工业生产、军事“智能尘埃”（Smart dust）、重要场所安全监控、

医疗护理、灾害监测、精细农业……，其广阔的应用前景掀起了国内外对无线传感器网络的研究热潮。1999 年和 2000 年美国《商业周刊》和 MIT《技术评论》在预测未来技术发展报告中，分别将 WSN 列为 21 世纪最有影响力的 21 项技术和改变世界的十大新技术之一。

由于无线传感器网络的巨大应用价值，它已经引起世界许多国家的军事部门、工业界和学术界的极大关注。2003 年，美国自然科学基金委员会制定了无线传感器网络研究计划，投资 34 000 000 美元，以支持相关基础理论的研究；美国国防部和各军事部门都对无线传感器网络给予了高度重视，提出了 C4ISRT（Command，Control，Communication，Computing，Intelligence，Surveillance，Reconnaissance and Targeting）计划，强调战场情报的感知能力、信息的综合能力和信息的利用能力，把无线传感器网络作为一个重要研究领域，设立了一系列的军事传感器网络研究项目；美国英特尔公司、美国微软公司等信息工业界巨头也开始了无线传感器网络方面的研究工作，纷纷设立或启动了相应的行动计划；日本、英国、意大利、巴西等国家也对无线传感器网络表现出极大的兴趣，纷纷展开了该领域的研究工作。

无线传感器网络是一种全新的信息获取平台，能够实时监测和采集网络分布区域内的各种检测对象的信息，并将这些信息发送到网关节点，以实现复杂指定范围内的目标检测与跟踪。它具有快速展开、抗毁性强等特点，有着广阔的应用前景。传感器网络、塑料电子学和仿生人体器官又被称为全球未来的三大高科技产业。

1.1.1 无线传感器网络的特点

无线传感器网络除了具有 AdHoc 网络的移动性、断接性、电源能力局限性等共同特征以外，还具有很多其他鲜明的特点。

（1）网络规模大，拓扑结构复杂。

为了获取准确信息，在监测区域内通常部署大量的传感器节点。

传感器节点数量可能达到成千上万，甚至更多。这样通过不同空间视角获得的信息具有更大的信噪比；通过分布式处理大量采集的信息能够提高监测的精确度，降低对单个节点传感器的精度要求；大量冗余节点的存在，使得系统具有很强的容错性能；大量节点能够增大覆盖的监测区域，减少洞穴或者盲区。

(2) 自组织网络。

通常情况下，在无线传感器网络应用中，传感器节点被放置在没有基础设施的地方。传感器节点的位置不能预先精确设定；节点之间的邻居关系也不能预先知道。如通过飞机将大量传感器节点撒播到面积广阔的原始森林中，或随意放置到人不可能到达或危险的区域，这就要求传感器节点具有自组织能力，能够自动进行配置和管理，通过拓扑控制机制和网络协议自动形成转发监测数据的多跳无线网络系统。在无线传感器网络的使用过程中，部分传感器节点由于能量耗尽或环境因素造成了失效；也有一些传感器节点为了弥补失效节点，提高监测精度而补充到网络中。这样无线传感器网络中的节点个数就会出现动态的增加或减少，从而使网络的拓扑结构随之也动态变化。而无线传感器网络的自组织性要能够适应网络拓扑结构的这种动态变化。

(3) 数据传输方向性强。

在无线传感器网络中，数据传输具有很强的方向性。通常，查询信息是通过广播或多播的方式从观察者向网络内传感器传输，而探测结果信息则是由分布在各处的传感器节点向查询点汇聚。

(4) 多跳路由。

网络中节点通信距离有限，一般在几十米到几百米范围内，节点只能与它的邻居直接通信。如果希望与其射频覆盖范围之外的节点进行通信，则需要通过中间节点进行路由。匿定网络的多跳路由需用网关和路由器来实现，而无线传感器网络中的多跳路由则由普通网络节点完成，没有专门的路由设备。这样每个节点既可以是信息的发送者，也可以是信息的转发者。

(5) 动态性网络。

无线传感器网络是一个动态的网络，节点可以随处移动。一个节点可能会因为电池能量耗尽或其他故障，退出网络运行；一个节点也可能由于工作需要而被添加到网络中。无线传感器网络的拓扑结构可能因为下列因素而改变：

① 环境因素或电能耗尽造成的传感器节点出现故障或失效；环境条件变化可能造成无线通信链路的带宽变化，甚至时断时通。② 无线传感器网络的传感器、感知对象和观察者这三个要素都可能具有移动性。③ 新节点的加入。④ 可靠的网络。

（6）以数据为中心，具备自组织能力。

传感器网络是一个任务型的网络，网络的布设和展开无需依赖任何预设的网络设施，节点通过各种协议算法协调自己的行为，节点开机后就可以快速、自动地组成一个独立的网络。传感器网络中的节点采用编号标识，节点编号是否需要全网唯一取决于网络通信协议的设计。由于传感器节点的随机部署，构成的传感器与节点编号之间的关系是完全动态的，表现为节点编号与节点位置之间没有必然的联系。用户使用传感器网络查询事件时，直接将所关心的事件通告给网络，而不是通告给某个确定编号的节点。网络在获得指定事件的信息后汇报给用户。这种以数据本身作为查询或者传输线索的思想更接近于自然语言交流的习惯。所以通常说传感器是一个以数据为中心的网络。

例如，在应用于目标跟踪的传感器网络中，跟踪目标可能出现在任何地方，对目标感兴趣的用户只关心目标出现的位置和时间，而不关心哪个节点监测到了目标。事实上，在目标移动过程中，必然是由不同的节点提供目标的位置信息。

（7）应用相关的网络。

传感器用来感知客观物理世界，获取物理世界的信息量。客观世界的物理量多种多样，不可穷尽，不同的传感器应用关心不同的物理量，因此对传感器的应用系统也有多种多样的要求。

不同的应用背景对传感器网络的要求也不同，其硬件平台、软件系统和网络协议必然会有很大的差异。所以传感器网络不能像

Internet 一样，有统一的通信协议平台。对于不同的传感器网络，其应用虽然存在一些共性问题，但在开发传感器方面有更高效的目标系统。针对每一个具体应用来研究传感器网络技术，是传感器网络设计不同于传统网络设计的显著特征。

无线传感器网络特别适合部署在恶劣环境或人类不宜到达的区域，使得传感器节点可能工作在露天环境中，遭受太阳的暴晒或者风吹雨淋，甚至遭到无关人员或动物的破坏。由于监测区域环境的限制以及传感器节点数量巨大，人工不可能“照顾”到每个传感器节点，网络的维护显得十分困难甚至不能维护。无线传感器网络的通信保密性和安全性也十分必要，要防止监测数据被盗取和获取伪造的监测数据。因此，无线传感器网络的软硬件必须具有鲁棒性和容错性。

此外，无线传感器网络也存在一定的局限性：

（1）传感器节点的通信能力有限。

传感器节点的数据传输率低、通信距离短，一般只有几十米到几百米，而且传感器往往工作在恶劣地区，因此难免受到环境的影响：一方面造成无线传感器之间的通信不可靠；另一方面可能使传感器出现长时间故障、甚至损坏。无线通信的能量消耗与通信距离的关系为

$$E = kd^n$$

其中参数 n 满足关系 $2 < n < 4$。n 的取值与很多因素有关：障碍物多、干扰大，n 的取值就大。天线质量对信号发射质量的影响也很大，随着通信距离的增加，能量消耗将急剧增加。

（2）电源能量受限。

传感器节点的体积微小，通常由能量有限的电池供电，而且通过更换电池来补充能量的方式不可取。

（3）计算机能力有限。

传感器一般采用嵌入式处理器和存储器，因此都具有计算能力，可以完成一些处理工作。但由于嵌入式处理器和存储器的能力和容量有限，使得传感器节点的处理能力十分有限。

1.1.2 传感器网络的关键技术

在传感器网络中，节点被任意散落在被监测区域内，以自组织形式构成网络，通过多跳（Multi-hops）中继方式将监测数据传到Sink节点，最后Sink节点借助卫星链路或临时建立的Sink链路将汇聚数据传送到远程中心进行集中处理。它通常包括分布式传感器节点、汇聚节点（Sink）、互联网和用户界面等。这些通过飞机布撒或人工布置等方式部署在感知对象内部或者附近的节点通过自组织方式构成无线网络，以协作的方式感知、采集和处理网络覆盖区域中特定的信息，可以实现对任意地点、在任意时间信息的采集、处理和分析。传感器节点监测的数据沿着其他传感器节点逐跳进行传输，在传输过程中可能被多个节点处理，经过多跳路由到汇聚节点（Sink），最后经过互联网或卫星到达任务管理节点。用户通过管理节点对传感器网络进行配置和管理，发布监测任务以及收集监测数据。

无线传感器网络因为上述特点及其与现有网络的区别，导致已有网络中的许多技术并不能直接应用到无线传感器网络中，无线传感器网络的研究领域还存在许多新的挑战。

1.1.2.1 MAC层技术

MAC层是无线传感器网络协议堆栈中的一个重要层次，它实现网络的自组织和节能。节点被随机放置后，MAC层协议实现节点间链路的建立，以保证所有的节点可以公平、有效地利用有限的带宽。另外，网络的节能也由MAC层实现。目前，研究者已经提出了很多MAC层设计的建议方案，大致可以划分为两大类：

（1）固定分配类。

固定分配类MAC层协议主要有频分多址接入（FDMA）、时分多址接入（TDMA）、码分多址接入（CDMA）三种；现在的MAC

协议主要有 SMACS、EAR、TRAMA、TDM-FDM、DE-MAC 等。SMACS 是一个分布式协议，节点可以发现自己的邻节点，并建立邻居列表，进而建立通信链路。SMACS 采用多信道，而且用中心调度方式对信道进行分配。节点的射频模块可以在不同的信道采用不同的频率，从而降低了冲突发生的概率。在此协议中还使用了随机唤醒机制，即没有通信任务时，节点进入睡眠状态，节省电源。EAR 协议用于固定节点和移动节点间的通信，它是 SMACS 协议的补充。采用 EAR 协议的无线传感器网络中，连接的建立和断开完全由移动节点来负责，并且以信噪比的值来决定是否要断开和连接。TRAMA 协议是基于能量的协议。在此协议中，时隙的分配是通过节点所携带能量的多少来决定的。该协议按照一定的规则选出能量最低的节点，为其分配时隙。在此时隙内，节点可以工作或睡眠。当某一节点携带的能量比选举出的节点具有的能量低时，它进入选举阶段。如此反复，各节点间的能量将会得到有效平衡，从而延长了网络的生存期。

（2）基于竞争类。

“竞争”的含义是，连接到信道上的节点遵循某种规则竞争信道，得到使用权的节点可以进行通信。基于竞争类的 MAC 层协议有 Sensor-MAC(S-MAC)、Timeout-MAC(T-MAC)、WiseMAC 和 B-MAC 等。S-MAC 协议沿用了 IEEE 802.11 协议的冲突避免方式。除此之外，还采用了工作/休眠策略，将时间分为帧，每一帧内分为工作阶段和休眠阶段：没有通信任务时，节点转入休眠状态，并缓存采集到的数据；进入工作阶段集中发送数据。因此 S-MAC 具有很好的节能特性，它满足了 MAC 层协议对各性能间平衡的要求，能量和时延之间可以根据流量来折中。T-MAC 协议与 S-MAC 协议的实现机制基本相同，也采用了帧的概念。它通过设置细微的超时间隔(Fine-grained timeouts)来动态地选择占空比，从而减少了闲时侦听信道所消耗的能量，延长了网络的生命期。WiseMAC 协议的特别之处在于，发送节点在收到数据确认包的同时可以获得接收节点下一次的信道侦听时间，由此发送节点可获得其所有邻居节点的信道侦

听时间，以简化唤醒机制的实现。

1.1.2.2 路由技术

路由发现和维护是无线传感器网络中的另一项关键技术，由网络层负责。它的主要任务是在传感器节点和 Sink 节点间建立路由，可靠地传递数据。无线传感器网络中资源严重受限，因此路由协议设计的首要原则是节省能量，延长网络系统的生存期。协议不能太复杂、不能在节点保存太多的状态信息、节点间不能交换太多的路由信息；同时应尽量避免发送冗余信息，减少能量的浪费。现已提出的路由协议可简单分为以下几个类别：

(1) 以数据为中心的路由协议。

Flooding、Gossiping、SPIN 协议等都属于以数据为中心的协议，这类协议的特点是基于数据查询。在传输过程中，有相同属性的数据进行融合，由此减少冗余数据的传输，以节省能量。与基于地址的路由协议相比，这种以数据为中心的路由协议更适合于以数据为中心的无线传感器网络。

Flooding 协议（洪泛协议）是最早最简单的路由协议，此协议中没有任何路由算法。节点向它的所有邻居节点广播所收到的数据，直到数据到达目的节点或达到数据报的最大跳数。Flooding 协议的缺点在于容易引起信息爆炸和重叠，造成网络拥塞，不能满足应用所需的网络 Qos。Gossiping 协议是针对 Flooding 协议的缺点而提出的。它与 Flooding 协议的不同之处在于，Gossiping 协议中节点随机选择一个邻居节点来转发数据，而不再向它的所有邻居节点广播要发送的数据。与 Flooding 协议相比，Gossiping 协议减少了网络拥塞；但由于转发数据的随机性，使得端到端的数据传输时延有所增加。SPIN 是基于协商的传感器网络路由协议，它采用三次握手机制。SPIN 中有三种类型的消息：ADV、REQ 和 DATA。当某个节点有数据需要发送时，它就向全网广播 ADV 消息；收到 ADV 消息且对要发送的数据感兴趣的邻居节点此时向发送节点发出 REQ 消息，表

示希望接收此数据；发送节点收到 REQ 消息后，用 DATA 消息封装数据，发送到目标节点。

（2）分层次的路由协议。

这类协议的设计思想是，将所有节点划分为若干簇，每个簇按照一定规则来选举一个簇头。各个节点采集的数据在簇头节点进行融合，再由簇头节点与 Sink 节点进行通信。这种分层设计可以大大减少网络流量，达到节约功耗的目的。此类协议包括 LEACH、TEEN 协议等。LEACH 协议是一个典型的分层次的路由协议。在该协议中，所有节点被分为若干簇，每个簇选举一个簇头，各个簇头还可以组成更高层次的簇。LEACH 协议的目标在于通过随机的选择簇头，将整个网络的能量负载平均分配到每个传感器节点中。TEEN 协议是改进的 LEACH 协议，它设立了软、硬门限值，只有在同时满足两个门限值时才发送数据。当检测值超过硬门限时，数据立即被发送出去，并把此次检测值作为新的硬门限；如果检测值与硬门限的差值超过了软门限，数据也立即被发送，并把这个差值作为新的软门限。

（3）基于位置的路由协议。

这类协议利用位置信息将数据传送到目标区域，从而不必为了寻找目标区域向全网广播数据，以减少能量的消耗。此类协议包括 MECN & SMECN、GAF、GEAR。

（4）基于网络流的路由协议。

这类路由协议在实现路由发现和维护的同时，还力求满足网络的 QoS 需求。一些协议在建立路由路径的同时，还考虑节点的剩余能量、每个数据包的优先级、估计端到端的时延，从而为数据流选择一条最合适的发送路线。这类协议有 SPEED、SAR 等。SPEED 协议是一个空分的、基于网络流的无线传感器网络协议。SPEED 协议中使用反馈机制来使 MAC 层性能达到最优；对于需要重新路由的分组，则采用临近反馈循环机制。与其他协议相比，SPEED 可以有效地平衡网络的流量负荷，延长网络的生存期。SAR 协议的路由过程是一个以网关的一跳邻居作为根节点的多棵树不断延伸的过