作集萃·理工学科

Research on Key Management Scheme for Wireless Sensor Networks

无线传感器网络密钥管理方案研究

余旺科 著

天津大学出版社
TIANJIN UNIVERSITY PRESS

博士学位论文优秀作集萃·理工学科

Research on Key Management Scheme for Wireless Sensor Networks

无线传感器网络密钥管理方案研究

余旺科 著

天津大学出版社
TIANJIN UNIVERSITY PRESS

内 容 提 要

无线传感器网络是一种集成了传感技术、微电技术、无线通信技术和分布式信息处理技术的新兴网络，其应用已经扩展到环境监测、交通管理及医疗卫生等诸多领域。由于传感器节点本身硬件能力的一些限制以及复杂的安全环境、多样的安全需求等因素的综合影响，无线传感器网络的安全受到严峻的挑战。而密钥管理在无线传感器网络的安全方面具有十分重要的意义，它是保障安全通信和安全路由的关键因素。本书对密钥管理的关键问题进行了深入的阐述，旨在能设计出安全高效的密钥管理方案。

本书关键词：无线传感器网络，密钥管理，密钥预分配，安全性，连通性

图书在版编目(CIP)数据

无线传感器网络密钥管理方案研究 / 余旺科著. —
天津 : 天津大学出版社, 2018.11
(学术理论研究著作集萃. 理工学科)
ISBN 978-7-5618-6268-1

Ⅰ. ①无… Ⅱ. ①余… Ⅲ. ①无线电通信－传感器－计算机网络－安全技术－研究 Ⅳ. ①TP212②TP393.08

中国版本图书馆 CIP 数据核字(2018)第 242350 号

WUXIAN CHUANGANQI WANGLUO MIYAO GUANLI FANGAN YANJIU

出版发行	天津大学出版社
地　　址	天津市卫津路 92 号天津大学内(邮编:300072)
电　　话	发行部:022-27403647　邮政部:022-27402742
网　　址	publish.tju.edu.cn
印　　刷	北京虎彩文化传播有限公司
经　　销	全国各地新华书店
开　　本	185mm×260mm
印　　张	6
字　　数	150 千
版　　次	2018 年 11 月第 1 版
印　　次	2018 年 11 月第 1 次
定　　价	36.00 元

目　录

第1章 绪 论

1.1 背景

无线传感器网络(Wireless Sensor Networks,WSN)集微电技术、传感器技术和通信技术于一体,可广泛应用于教育、军事、医疗及交通等诸多领域,拥有巨大的应用潜力和商业价值,引起了国内外广泛的关注和研究[1-5]。2003 年美国《技术评论》杂志认为,有 10 种新兴技术在不远的将来会产生巨大的影响[6],这些全新的技术很快就可以改变计算、医疗、制造、运输和能源基础设施等领域,而无线传感器网络就是 10 种新兴技术之一。

无线传感器网络的安全问题来源于:无线通信的特性,传感器节点的资源严格受限,传感器网络分布区域广而密集,缺少固定的网络基础设施,配置前无法获知网络的拓扑结构,部署区域的开放性。特别是当无线传感器网络部署在无人看护或容易受损的环境时,保证无线传感器网络的安全性更应是优先考虑的问题。以提供安全、可靠的保密通信为目标的密钥管理是无线传感器网络安全研究最为重要、最为基本的内容,有效的密钥管理机制也是其他安全机制,如安全路由、安全定位、安全数据融合及针对特定攻击的解决方案等的基础[7-12]。相对于传统网络,无线传感器网络更易受到包括被动窃听、数据篡改和重发、伪造身份、拒绝服务、节点俘获等安全威胁和攻击,因而这些研究成果一般不能直接应用于无线传感器网络。为满足无线传感器网络数据的安全需求,需要设计出更适用于无线传感器网络的密钥管理方案[13-16]。

1.2 密钥管理方案的安全问题

1.2.1 制约因素

由于无线传感器网络的特殊性,在安全研究中无线传感器网络会受到一些因素的制约,例如电源能量有限、计算与通信能力受限、安全定位问题、数据包延迟或丢失等。下面介绍无线传感器网络中的一些重要制约因素[18-21]。

1. 资源限制

传感器节点的资源有限特性导致很多复杂、有效、成熟的安全协议和算法不能直接使用。传感器节点采用电池供电,且大多数情况下不可更换。在选择和设计安全算法时,需要考虑尽可能地减少该算法在计算、数据存储和数据传输过程中的能耗,尤其是传输能耗的降低;尽可能地延迟网络的生命周期。虽然公私钥安全体系是目前商用安全系统最理想的认证和签名体系,但从存储空间上看,一对公私钥的长度达到几百个字节,而且计算速度非常慢,这对于存储

空间和计算能力有限的传感器节点来说是无法完成的。因此，如何降低传感器节点的存储开销、计算开销和通信开销是整个无线传感器网络安全研究中的重点。

2. 不可靠的通信

无线传感器网络中数据包传输是无连接的，因此是不可靠的。由于信道错误或者阻塞，有可能会损害数据包，造成数据包丢失；而信道衰弱或者传感器节点处于睡眠模式都会引起无线传感器网络的间歇性连接。

3. 物理安全无法保证

传感器节点被分布在开放的，甚至“敌对”的区域，其工作空间本身就存在不安全因素，节点很可能遭到物理或逻辑上的俘获，所以在传感器网络的安全设计中必须考虑及时撤销网络中被俘传感器节点的问题以及因为被俘传感器节点导致的安全隐患扩散问题。

4. 动态的拓扑结构

随着网络中关键传感器节点能量的减少，需要通过改变网络的拓扑结构来平衡网络中传感器节点的能量消耗。传感器节点的失效、被俘和新节点的加入都会导致无线传感器网络拓扑结构的动态变化。如果拓扑结构发生改变，邻居传感器节点的集合也会发生改变，因此密钥建立过程需要重新执行。

5. 组播认证

传感器网络作为一个整体来完成某项特殊的任务，每个传感器节点既是数据的采集者，又是路由的转发者。每个传感器节点在与其他传感器节点通信时存在信任度和信息保密的问题。当基站向全网发布查询命令时，每个传感器节点都能够有效地判定消息的确来自于有广播权限的基站，这对于资源有限的传感器网络来说是非常难的。

6. 延迟

传感器网络的多跳路由协议会因阻塞传感器节点处理数据而引起网络延迟。虽然延迟可能非常短，但是在安全服务中时间是非常重要的因素，延迟会带来同步问题。在一些重要的事件报告和密钥分发中，应该尽可能地减少时间延迟以保证数据的及时性。

1.2.2 主要攻击

无线传感器网络密钥管理方案受到的主要攻击如下[22-26]。

1. 欺骗、篡改或重发路由报文

攻击者向无线传感器网络中注入大量的欺骗路由报文；攻击者截获并篡改路由报文，把自己伪装成发送路由请求的汇聚传感器节点，使整个网络的报文传输被吸引到某一局域内，致使各传感器节点之间能量失衡，或者在网络内造成环形路由；攻击者重发以前收到的路由报文，以增加网络延迟。

2. 链路攻击

攻击者通过控制并侵占一个网络中的合法节点，使其产生错误的路由信息，实现对网络的破坏。该攻击可以使网络中的路由算法认为数据经过它时可以达到最优的路由，但实际上该节点已经被攻击者控制，因而恶意节点需要伪装出高可靠性，使自己安全地存在于数据链路上。

3. 选择性转发

恶意节点拒绝转发报文,但是为了防止被发现,可能会选择性地发一些报文或将一些报文修改后再转发。多路径路由能有效地减少这种攻击所造成的信息丢失。另外,邻居节点和基站能监视这种行为,降低向这种容易丢报文的节点转发报文的优先级。当选择转发的攻击点处于报文转发的最优路径上时,这种攻击危害较大。

4. 确认收到欺骗

该攻击方式充分利用了传感器节点无线通信的特性。如果有源传感器节点向某一邻居传感器节点发送数据报文,其他的邻居传感器节点也会收到同样的报文。当攻击点侦听到该邻居传感器节点处于非工作状态时,便冒充该邻居节点向源传感器节点反馈一个确认收到报文的信息,让源传感器节点误以为该传感器节点处于工作状态。

5. Flood 攻击

很多协议都需要节点向邻近的节点广播自身的信息,以声明自己是其他传感器节点的邻居传感器节点,但是一个较强的恶意传感器节点会以足够大的功率广播信息报文,收到信息包的传感器节点会误认为这个恶意传感器节点是它们的邻居传感器节点。在以后的路由选择中,这些传感器节点很可能会使用含有恶意传感器节点的路径,向恶意传感器节点发送数据报文。事实上,由于该传感器节点离恶意传感器节点的距离较远,所以它以普通的发射功率传输的数据报文根本无法到达目的地,从而造成这些数据报文丢失。

6. 黑洞攻击

攻击者引诱其他节点向其发送数据报文,从而创造一个以攻击者为中心的黑洞。比较典型的攻击方法是攻击者让其他节点根据路由算法相信它是最好的转发选择,从而吸引其他节点向其发送数据报文。例如,一个攻击者可以通过伪造或回放一个数据报文,以示它有高质量的路由到基站,等吸引到其他节点向其发送数据报文时,再进行其他攻击(如进行选择性转发攻击)。

7. Sybil 攻击

无线传感器网络中每一个传感器节点都应有一个唯一的标识符与其他传感器节点进行区分。当前具有容错功能的路由协议都是靠不同的传感器节点分布式地存储路由信息,从而在不同传感器节点之间实现从源传感器节点到目的节点的多路径路由。Sybil 攻击的特点是攻击点伪装成具有多个身份标识的传感器节点,当通过该传感器节点的一条路由遭到破坏时,网络会选择另一条自认为完全不同的路由。由于该传感器节点有多重“身份”,所以该路由实际上还是通过了该攻击点,因此 Sybil 攻击大大地降低了多路径路由的效果。

8. DoS 拒绝服务攻击

由于无线传感器网络是基于某一任务的合作团队,在无线传感器网络节点之间建立合作规则以达成默契,这需要彼此之间频繁地交换信息。进行攻击的传感器节点可以以不同的身份连续向某一邻居传感器节点发送路由或数据请求报文,使该邻居传感器节点不停地分配资源以维持一个新的连接状态。由于无线传感器网络节点资源有限,这种攻击危害很大。

1.2.3 安全目标

无线传感器网络密钥管理方案的安全目标[27-35]如下。

1. 可认证性

可认证性包括两个方面,即实现实体的认证和消息的认证。传感器节点应该能够核实消息的来源,即该消息是否是所期望的合法的传感器节点发送的,并且确实是该传感器节点在当前时刻的动作,而不是以往时刻行为的复制。另外,可认证性还要考虑基站向所有传感器节点发送消息过程中的组播认证。

2. 连通性

这里的连通性是指通过密钥管理方案产生的密钥连通图的安全连通性,即无线传感器网络中邻居节点能建立共享密钥的可能性。保持足够高的密钥连通概率是无线传感器网络发挥其应有功能的必要条件。需要强调的是,无线传感器网络节点几乎不可能与距离较远的其他节点直接通信,因此并不需要保证每一个节点与其他所有的节点保持安全连通,仅需确保相邻传感器节点之间保持较高的密钥连通概率即可。

3. 抗毁性

在无线传感器网络中,攻击者可以通过对俘获的传感器节点进行复制,然后再利用这些复制的节点侵入原有的网络。使用这种攻击手段,攻击者会增加网络中的传感器节点的数量,并使用复制的传感器节点来控制网络。针对这种攻击,无线传感器网络必须能够抵抗一定数量的传感器节点俘获攻击,保证网络的安全。所以,抗毁性是评估密钥管理方案优劣的一个重要指标,即当网络中的部分传感器节点被俘获之后,未被俘获传感器节点的密钥被暴露的概率。抗毁性越好,意味着安全链路受损的概率就越低。一个理想的密钥管理方案应该是在部分传感器节点被俘获之后,对其他正常传感器节点之间安全通信的影响几乎为零。

4. 负载

无线传感器的负载包括三种:通信负载、计算负载和存储负载。由于传感器节点电源能力的限制,要求密钥管理方案的耗电量尽可能的小。而通过实际比较发现,传感器节点之间通信操作消耗的电能远远大于计算操作所消耗的电能,因此要求密钥管理方案中的通信负载尽可能的小。传感器节点的物理特性决定了其有限的计算能力,一个需要复杂计算的密钥管理方案不一定是一个好方案。同样,传感器节点的物理特性还决定了其存储容量,一个符合实际应用的密钥管理方案需要使每个传感器节点预先分配的信息尽可能的少。

5. 动态的拓扑变化

网络的动态变化包括两种情况:传感器节点的动态加入和退出。因为传感器节点的能量限制和脆弱性等因素,不断地有传感器节点不能工作,对于不能工作尤其是受到攻击的传感器节点,密钥管理方案要能够保证网络的后向安全性,即保证被攻击的传感器节点离开后不能继续获得网络中的重要数据。由于不断地有传感器节点离开,所以有些长期性任务就要求不断地有新的传感器节点加入。密钥管理方案应该能够保证网络的前向安全性,即新传感器节点不能得到其加入前网络中的秘密信息。密钥管理方案必须考虑其网络拓扑变化的适应性,根

据传感器节点的加入或退出,保证网络的前向安全性和后向安全性。

6. 可扩展性

无线传感器网络的节点规模少则几十个,多则成千上万个。随着网络规模的扩大,密钥协商所需的计算、存储和通信开销都会随之增大,如许多的组密钥机制的相关参数(加密操作的次数、接收的字节数)会随着组成员数目的增加而迅速增加。在传输信息的能耗远大于计算能耗时,应该把网络划分为较小规模的分组,在组内处理信息然后重新加密发送到其他的组中会节省网络的能量消耗。密钥管理方案和协议必须能够适应不同规模的网络。

7. 密钥撤销

当一个传感器节点被攻击者俘获,对网络产生破坏行为时,密钥管理方案能够提供有效的机制从网络中撤销该传感器节点的密钥。撤销机制是一种轻量化的保护机制,该机制不会消耗太多的网络通信资源。

1.3 密钥管理方案的分类

由于缺乏普遍适应性的设计规范,无线传感器网络密钥管理方案具有较高的开放性。当前无线传感器网络正处于不断发展的阶段,因此对密钥管理方案的研究存在必要性。根据不同密钥管理方案的性质及侧重点,将现有的密钥管理方案按照密钥建立的概率、网络的结构以及拓扑方案的动态性、使用的密码学体制、密钥协议是否混合等特性进行分类[36-38]。无线传感器网络密钥管理方案的分类如图 1-1 所示。

1. 静态密钥管理与动态密钥管理

根据网络中的密钥在节点部署之后是否更新,无线传感器网络密钥管理方案可分为静态密钥管理和动态密钥管理两类。在静态密钥管理中,节点预分配一定数量的密钥,部署之后通过相互协商生成通信密钥,通信密钥在整个网络生存期内不考虑密钥更新和撤回;而在动态密钥管理中,密钥的分配、协商和撤回操作周期性进行。前者的特点是通信密钥无须频繁更新,不会产生更多的计算和通信开销。后者的特点是可以使传感器节点通信密钥处于动态更新状态,攻击者很难通过俘获传感器节点来获取实时的密钥信息,但密钥的动态分配、协商、更新和撤回操作将产生较大的通信和计算开销。

2. 私钥密码体制和公钥密码体制下的密钥管理

密码体制分为私钥密码体制(对称密码体制)和公钥密码体制(非对称密码体制)。

所谓私钥密码体制,是指加密密钥与解密密钥相同或者彼此容易相互确定的加密算法。在大多数私钥加密算法中,加密密钥和解密密钥是相同的。使用私钥加密算法的加密体制称为私钥密码体制。私钥密码体制算法的实现速度快,这个特点使它有着广泛的应用,特别适合于海量数据的加密。因为算法不需要保密,所以制造商可以开发出低成本的芯片以实现数据加密。私钥密码体制存在两个主要问题。一是密钥的分配与管理方面的困难。加密与解密使用的是相同的密钥,收发双方必须事先通过某种秘密途径商定一个密钥。另外,当 n 个人通信时,需要的密钥数为 $n(n-1)/2$ 个,若有 100 个人,所需要的密钥数就是 4 950 个。因此,有关密钥的分配、安全传送和保密管理是一件很困难的事情。二是数据的完整性保护方面的困难。

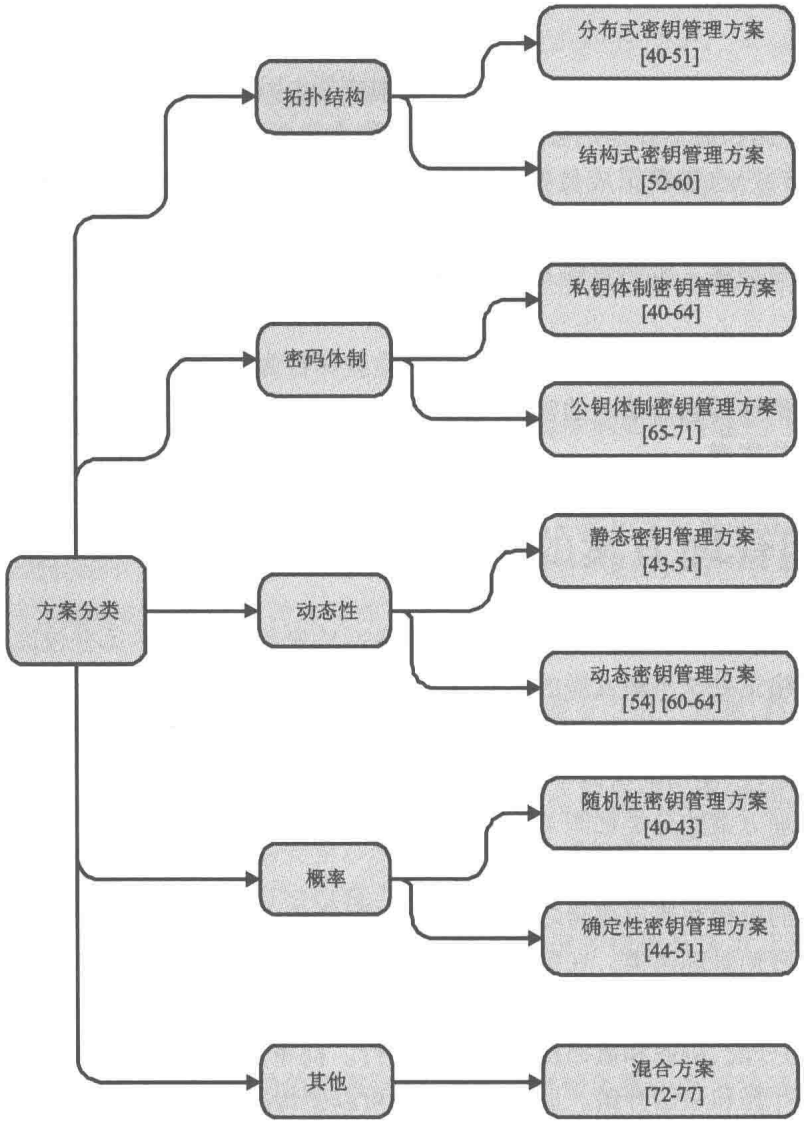

图 1-1 无线传感器网络密钥管理方案的分类

由于保密通信双方都具有共同的加密密钥和解密密钥,信息的接收方可以很容易地篡改原文内容,而信息的发送方也可以否认自己所发的内容。私钥密码体制在数字签名和身份认证方面的应用是相当困难和不现实的。私钥密码体制的安全性依赖于加密算法的强度和密钥的安全性。加密算法必须具有足够的强度,使得仅根据密文去解密信息在计算上不可能实现,因此无须确保算法的安全性,但必须保证密钥的安全性。在私钥密码体制中,最著名的是美国数据加密标准 DES。

公钥密码体制,即加密和解密使用的密钥是不相同的,也称为双密钥加密体制。公钥密码体制的基本思想是不仅公开加密算法,而且加密用的密钥也公开。即可以将每一用户的加密密钥作为公钥文件,像电话簿一样公开,只要解密密钥保密即可,而且各用户的解密密钥由各用户自己保管。若用户 A 要向用户 B 发送信息,A 可以从公钥文件中查到 B 的加密密钥,利

用它向 B 发送密文,B 收到密文后利用只有自己知道的解密密钥解密得到明文。由于这种加密体制的加密密钥是公开的,所以称这种加密体制为公钥密码体制。它在密钥管理与使用方面为用户带来的好处显而易见,在数字签名与身份认证领域也有着广阔的前景。1978 年由 Ronal Rivest、Adi Shamir 和 Len Adleman 共同提出的 RSA 算法就是公钥体制中最著名的加密算法之一[39]。

公钥密码体制中,加密密钥与解密密钥是不同的。任何人都可以使用其他用户的公开密钥对数据进行加密,但是只有拥有保密的私有密钥的用户才能对加密的数据进行解密。在这种体制下,即使知道了加密算法和加密密钥也不会因此泄露加密数据。虽然从理论上讲,解密密钥可由加密密钥计算出来,但是这种密码体制建立的思想基础是使这种逆向计算在实际应用中不可行。也就是说,在实际应用中,解密密钥不可能由加密密钥或加密信息、加密技术以及破译技术简单地产生或推算出来。如果解密密钥需要世界上最快的计算机运行数十年才能算出,那么这种密码事实上就是安全的。

公钥密码体制与私钥密码体制相比有如下特点。

(1)在使用上,首先公钥密码体制的分配与管理优于私钥密码体制,公钥密码体制的加密算法和加密密钥均可以通过任何通道公布于众,仅将解密密钥保密;其次它易于解决密码通信系统发送方和接收方的认证问题,便于实现数字签名,确认双方的身份。

(2)在算法设计上有很大的不同。在私钥密码体制算法中,加密过程中所用的全部步骤的逆过程就是解密过程的全部步骤;而在公钥密码体制算法中,加密和解密遵循着两条不同的途径,因此不可能从加密过程的步骤反过来确定解密过程的步骤。换句话说,即使知道了加密过程也不可能推算出解密过程。在算法设计上,私钥密码体制算法往往设计成相当复杂的数学方程,其保密强度建立在算法运算的复杂性上;而公钥密码体制算法虽然有使用上的优势,但在算法设计上比传统算法的限制多。这是因为公开密钥算法可能提供更多的信息,使得窃密者可以对算法进行攻击。一般来说,公钥算法都是基于一种单向函数,其保密强度是建立在一种特定的已知数学问题求解困难这个假设的基础之上的。

(3)两者产生的密钥方式不同。私钥密码体制中,密钥用简单的随机选取方式;而在公钥密码体制算法中,加密密钥和解密密钥均采用有效的特殊方法计算得来。

由于公钥密码体制的独特之处从根本上克服了私钥密码体制在使用上的主要缺点,加之其在数字签名方面的广阔应用前景,使它为密码技术在商业、金融等电子商务及民用领域的普遍应用创造了条件,展示出了广阔的前景。公开密钥算法可分为三类:①基于大整数分解问题的公钥密码算法;②基于离散对数问题的公钥密码算法;③基于椭圆曲线上的离散对数问题的公钥密码算法。

根据所使用的密码体制的不同,无线传感器网络密钥管理可分为私钥密码体制下的密钥管理和公钥密码体制下的密钥管理两类。公钥密码体制下的密钥管理由于对节点的计算、存储及通信等能力要求比较高,曾被认为不适用于无线传感器网络。但近几年的一些相关研究表明,公钥加密算法经过优化后性能有所改善,可以适用于现有的无线传感器网络。从安全的角度来看,公钥密码体制下的密钥管理的安全强度在计算意义上要高于私钥密码体制下的密钥管理。

3. 分布式密钥管理方案和结构式密钥管理方案

根据无线传感器网络的网络结构以及拓扑情况，可将方案分为分布式密钥管理方案和结构式密钥管理方案。

在分布式密钥管理方案中，所有的节点具有相同的通信能力和计算能力，在节点密钥的协商中，更新通过节点之间相互协作来完成。由于受到无线传感器网络的部署环境以及经济成本等因素的影响，这类方案实际的可用性相对较低，需针对具体情况进行改进。

在结构式密钥管理方案中，有一些普通节点或高性能节点需要完成比其他节点更多以及更重要的工作，如进行数据融合或管理其成员节点。结构式密钥管理方案又可分为逻辑分层密钥管理方案和异构分层密钥管理方案。逻辑分层密钥管理方案中某些网络中节点在逻辑上被分在一组，节点之间逻辑关系呈树状。同一组内的节点共享一个组内密钥，组与组之间存在共享密钥，甚至所有节点都拥有一个全局共享的密钥。值得注意的是，逻辑关系上在一起的节点，其物理拓扑不一定在一起。异构分层密钥管理方案以异构传感器网络为基础，是由一些具有不同通信、计算以及感应能力的传感器节点所构成的无线传感器网络。异构传感器网络已成为当前无线传感器网络的研究热点，其优点在于无线传感器网络引入异构节点可有效地提高整个网络的性能以及寿命。

4. 随机性密钥管理与确定性密钥管理

根据节点的密钥计算方法划分，无线传感器网络密钥管理可分为随机性密钥管理和确定性密钥管理。在随机性密钥管理中，节点的密钥通过随机选取的方式获取，如从一个大密钥池里随机选取一部分密钥，或从多个密钥空间里随机选取若干个密钥。而在确定性密钥管理中，密钥是以确定的概率方式计算出的。随机性密钥管理的优点是密钥分配简单，部署方式灵活；缺点是密钥分配具有盲目性，节点可能存储一些无用的密钥。确定性密钥管理的优点是密钥的分配具有较强的针对性，节点的存储空间利用得较好，任意两个节点之间可以直接建立通信密钥；缺点是部署方式灵活性降低，密钥协商的计算和通信开销较大。

1.4 各章的内容安排

第 2 章，简述了几种经典的密钥管理方案。

第 3 章，针对无线传感器网络能量、计算能力、存储空间以及带宽等局限性问题，提出了一种新的基于部署信息的密钥预分配方案。该方案采用正方形和正六边形分别对网络进行分区，不但在覆盖全网的同时分区之间没有重叠区域，而且每个分区相邻的分区数仅为 8 个和 6 个。节点仅需预分配数量较少的密钥，就能够以较大的概率建立共享密钥，即使存在大量的移动节点仍能保持较大的连通概率。本章还对 SQD-KPS 方案和 HEX-KPS 方案进行了仿真比较。

第 4 章，为了适用节点的频繁移动性，提出了一种基于椭圆曲线密码体制的异构网络密钥管理方案。同一簇内的所有节点可以直接建立共享密钥，而不同簇的节点可以通过基站或簇头构建多路径密钥。节点之间能相互验证密钥的有效性，可以抵抗假冒、重放和伪造等攻击。

第 5 章，为了在无线传感器网络中实现身份认证机制，采用椭圆曲线的双线性加密技术对

节点的身份进行认证;提出了一种无须任何第三方认证服务器的动态信任模型。在该动态信任模型中,邻居节点之间通过相互认证来建立共享密钥和到基站的路径信息,从而构建一个可信任的无线传感器网络。

第6章,提出了一种无线传感器网络的单向路径密钥管理方案,只有在节点之间需要通信时才建立配对密钥。在节点之间建立数据通信密钥时,节点只在密钥请求过程中利用节点间相互签名来验证节点和路径的有效性,而在返回源节点的密钥应答过程中,中间节点不需要进行相互签名验证。

第2章　典型的密钥管理方案

密钥管理方案要综合考虑无线传感器网络的连通性、存储消耗、通信消耗以及安全性，不同的密钥管理方案有不同的侧重点。下面分析几种典型的密钥管理方案。

2.1　全局密钥管理方案

预置全局主密钥方案[78]是最简单的密钥建立过程。该方案是在以下3个假设的基础上实现的。

(1)假设传感器节点的能量资源是有限的，尤其针对大型网络应尽可能地减少传感器节点的能量消耗。

(2)假设传感器节点是静止的或有较低的移动能力，允许所有的传感器节点在同一时间移动会使问题更复杂。

(3)每个传感器节点共享一个主密钥，假设该主密钥是安全的。

在网络部署之前，每个传感器节点预置一个相同的主密钥。当网络初始化时，每个传感器节点广播密钥协商信息与自己的邻居传感器节点协商会话密钥。假设在基站的有效通信范围内有 A 和 B 两个传感器节点，当传感器节点 B 收到传感器节点 A 的密钥协商请求时，同时传感器节点 A 也收到了传感器节点 B 的密钥协商请求，A、B 可以分别计算会话密钥，公式为

$$K_{AB} = \mathrm{MAC}_K[N_A \mid N_B] \tag{2-1}$$

在该方案中，每个普通节点与基站之间共享全局密钥，优点是计算复杂度低，每个节点需要的存储密钥的空间非常小，对普通节点资源和计算能力要求不高；只要节点都能够连接到基站就能进行安全通信。

由于网络中只有一个密钥，所以很容易增加新的节点，支持的网络规模取决于基站的能力，可以支持上千个节点。该方案的缺点是网络的安全性较差，一个被俘节点泄露密钥，整个网络节点的密钥都会被泄露，从而导致网络的安全机制完全失效。另有人提出将主密钥存储在抗俘获的硬件里，以降低节点被俘获泄露密钥的危险，但这增加了节点的成本和开销，并且抗俘获硬件的安全也是相对的。

另外一种预置全局密钥对方案就是保证任意两个传感器节点都能共享一个密钥。这种方案的主要思想是在网络部署之前首先由离线密钥服务器生成 $n(n-1)/2$ 个密钥，每个节点存储的密钥数为 $n-1$ 个，任意两个节点之间都共享一个密钥。该方案的优点是由于网络中的通信不依赖于基站，所以网络的灵活性比较强，预置了网络中的所有密钥，减少了网络的通信负载，计算复杂度低，任意两个节点间的密钥是独享的，所以当一个节点被俘获后不会影响网络中其他节点的安全性。假定节点 A、节点 B 和节点 C 彼此分别通过共享密钥建立了安全的通

信链路，当节点 C 被俘获后只影响与节点 C 有共享密钥的节点 A 和节点 B，节点 A 和节点 B 只需删除与节点 C 共享的密钥即可，而对节点 A 和节点 B 之间的通信却没有影响。该方案的缺点是支持的网络规模小，因为传感器节点的存储量有限，当网络中节点数目足够多时，每个节点的密钥存储量将大大地超过节点的存储量，所以网络的可扩展性很差。

2.2　随机密钥管理方案

2002 年，Eschenauer 和 Gligor 提出了一种随机密钥预分配方案[46]。EG 方案的基本思想是首先建立一个比较大的密钥池，任何节点都拥有密钥池中的一部分密钥，那么任意两个节点间存在一个概率，使得双方可以拥有一对相同的密钥，从而建立安全链路。

随机密钥预分配方案的具体实施过程如下。

1. 密钥预分配

在一个比较大的密钥空间内，为一个无线传感器网络选择一个密钥池，并为选中的密钥池中的密钥附加一个唯一的 ID。在密钥预分配时，从密钥池中任意选择 m 个密钥部署在每个节点中。这 m 个密钥构成一个节点的密钥组，节点密钥组的大小，受节点存储能力的限制。方案应保证每两个节点之间至少拥有一个共享密钥的概率大于预先设定的概率 P。

2. 共享密钥的发现

节点密钥预分配完成之后，它们就被部署到预期的位置。部署之后，每一个节点开始利用与周围节点共享的密钥，寻找自己的邻居节点。寻找邻居节点的方式有很多种，最简单的就是节点通过广播自己的密钥 ID，寻找与自己有共享密钥的邻居节点，如果节点发现其他节点与自己有共同的密钥，则可以利用共享密钥与其建立安全通信链路。但是这种方法极大地增加了网络中的传输负载，在能量受限的传感器网络中不可取。

3. 路径密钥的建立

在随机预分配模型下，只有当两个节点存在共享对密钥时，才可以进行通信。而当两个节点间不存在共享密钥时，可以通过在节点间建立路径密钥，进而建立安全通信链路。在论述之前，首先假定节点 A 希望与节点 B 通信，但是 A 和 B 两个节点间不存在共享密钥。A 首先向它的一个邻居节点 C 发出信息，希望与节点 B 通信。如果节点 C 与节点 B 存在共享密钥，则节点 C 生成一个共享密钥 K_{AB} 分别发送给节点 A 和节点 B。此时，节点 C 的作用可以看作是一个密钥分发中心。经过共享密钥的发现和路径密钥的建立，网络中的所有节点都可以相互进行安全通信。

4. 密钥撤销机制

由于每个节点都包含一定数量的密钥信息，如果某个节点被俘获，网络的安全会受到一定的威胁。为了应对节点俘获，网络中的其他节点必须能够删除与被俘获节点间的共享密钥。为了能够检测被俘获的节点，EG 方案中设定了控制节点，该节点的功能类似于一些方案中的基站，它具有很高的安全性，能够检测出被俘获的节点。同时，EG 方案还认为在节点部署前，控制节点与网络中的所有节点具有共享密钥。当检测到一个节点被俘获时，为了有效地删除