分类号 TP957 学号 12060025

UDC 密级 公开

工学硕士学位论文

国防科大学位论文 LaTeX 模板使用手册

硕士生姓名

学科专业 网络工程

研究方向 网络工程

指导教师

二〇一四 年 十一 月

面向规模化传感网的数据认证关键技术研究

Candidate:

Advisor:

A dissertation

Submitted in partial fulfillment of the requirements

for the degree of Master of Engineering

in Large-scale Wireless Sensor Network Data Authentication

November 3, 2014

独 创 性 声 明

本人声明所呈交的学位论文是我本人在导师指导下进行的研究工作及取得的研究成果。尽我所知，除文中特别加以标注和致谢的地方外，论文中不包含其他人已经发表和撰写过的研究成果，也不包含为获得国防科学技术大学或其他教育机构的学位或证书而使用过的材料。与我一同工作的同志对本研究所做的任何贡献均已在论文中作了明确的说明并表示谢意。

学位论文题目：面向规模化传感网的数据认证关键技术研究

学位论文作者签名：_____ 日期： 年 月 日

学位论文版权使用授权书

本人完全了解国防科学技术大学有关保留、使用学位论文的规定。本人授权国防科学技术大学可以保留并向国家有关部门或机构送交论文的复印件和电子文档，允许论文被查阅和借阅;可以将学位论文的全部或部分内容编入有关数据库进行检索，可以采用影印、缩印或扫描等复制手段保存、汇编学位论文。

(保密学位论文在解密后适用本授权书。)

学位论文题目：面向规模化传感网的数据认证关键技术研究

学位论文作者签名：_____ 日期： 年 月 日

作者指导教师签名：_____ 日期： 年 月 日

目　录

摘　要 i

ABSTRACT ii

第一章　绪论 1

1.1　本文研究背景和意义 1

1.1.1　无线传感网概述 1

1.1.2　规模化无线传感网数据认证 5

1.2　本文研究内容 6

1.3　本文组织结构 6

第二章　相关研究概述 8

2.1　无线传感网安全技术概述 8

2.1.1　无线传感网面临的安全威胁 8

2.1.2　无线传感网现有的安全技术 10

2.2　无线传感网认证机制概述 12

2.2.1　无线传感网数据认证概述 12

2.2.2　无线传感网身份认证概述 14

2.3　无线传感网密钥分配理论概述 15

2.3.1　无线传感网密钥分配方案分类 15

2.3.2　无线传感网典型密钥分配方案概述 16

第三章　多跳长路径上多节点联合数据认证 19

3.1　无线传感网数据认证模型 19

3.1.1　多跳长路径上多节点联合数据认证模型 19

3.1.2　系统模型和设计目标 20

3.2　多跳长路径上多节点联合的数据认证机制设计与实现 21

3.2.1　符号与定义 21

3.2.2　多节点联合数据认证方案 22

3.2.3　安全性能分析 24

3.3　路径上节点关系的维护 25

3.3.1　基站维护 25

3.3.2　节点自动维护 25

3.4　本章小结 26

第四章 数据认证方案优化 27
4.1 多路径抗节点失效机制 27
4.1.1 设计实现 27
4.1.2 安全性能分析 30
4.2 动态步长多节点联合数据认证 30
4.2.1 动态步长多节点联合数据认证机制设计 30
4.2.2 安全性能分析 32
4.3 本章小结 33
第五章 密钥分配与消息认证码的实现 34
5.1 面向数据认证的密钥分配方案 34
5.1.1 单向 hash 链 34
5.1.2 基于单向 hash 链的密钥分配 35
5.2 消息认证码的实现 38
5.2.1 消息认证码 39
5.2.2 MAC 设计实现 40
5.3 本章小结 41
第六章 仿真实验与结果分析 43
6.1 实验平台环境 43
6.1.1 仿真实验环境 43
6.1.2 无线传感网数据认证仿真框架 44
6.2 多跳长路径上多节点联合数据认证仿真实验 46
6.3 数据认证优化方案仿真实验 46
6.4 本章小结 46
第七章 总结与展望 47
7.1 本文总结 47
7.2 未来工作于展望 47
致谢 49
参考文献 50
作者在学期间取得的学术成果 54

表 目 录

表 2.1 无线传感网常见的攻击与防御措施 9
表 2.2 无线传感网主要的密钥分配方案 15
表 3.1 相关符号说明 21
表 5.1 消息认证码相关符号定义 34
表 5.2 预分配密钥池 36

图 目 录

图 1.1 无线传感网系统结构 2
图 1.2 无线传感网节点结构 3
图 1.3 无线传感网协议结构 3
图 2.1 $\mu TESLA$ 认证机制 12
图 2.2 多级 $\mu TESLA$ 认证机制 13
图 2.3 基于网格的密钥预分配方案 18
图 3.1 无线传感网应用场景 19
图 3.2 多节点联合数据认证中上下行相关节点 21
图 3.3 多节点联合数据认证中数据报文发送过程 23
图 3.4 节点自动维护上下行相关关系的过程 26
图 4.1 多路径抗节点失效机制中的不相交路径 28
图 4.2 多路径抗节点失效机制中的编织路径 28
图 4.3 多路径抗节点失效机制的密钥分配 29
图 4.4 动态步长多节点联合数据认证 31
图 4.5 面向动态步长多节点联合数据认证的密钥分配 31
图 5.1 共享密钥建立过程 37
图 5.2 SCBC-MAC 方案 41

摘　要

无线传感网在许多大范围监测领域都有广泛的应用，在环境监测、军事侦察等领域都有规模化的应用。无线传感器节点通常被部署在环境恶劣的无人值守区域，容易节点受损或者节点受攻击，导致传感网的传输受到严重影响。根据无线传感器节点计算能力、存储空间有限的特点，我们设计了多跳长路径上多节点联合的数据认证机制，有效利用了数据认证机制保障了传输路径上的安全。

深入研究了无线传感网中数据认证理论，设计实现了多跳长路径上多节点联合数据认证协议，进行虚假数据过滤，有效限制了攻击者利用妥协节点发动共谋攻击的威胁。并设计了路径上节点关系的维护算法，保证了数据认证机制的稳定性，对协议的安全性能进行了分析评价。

针对多跳长路径上多写点联合数据认证协议的不足，对算法进行了优化，提出了多路径抗节点失效机制和动态步长多节点联合数据认证机制，目标是提升数据传输的可靠性，降低数据认证机制的通信开销，并对优化方案的安全性能进行了分析评价。

围绕多跳长路径多节点联合数据认证机制的需求，对密钥分配方案进行了深入研究，提出了基于单向 hash 链的密钥分配方案，并对认证中的 MAC 进行了研究，提出了适应数据认证机制需求的 MAC 码。

通过仿真实验证明了本文中提出的方案的安全性能以及优化效果达到了预期目标。

关键词: **无线传感网**; **网络安全**; **数据认证**; **密钥分配**;

ABSTRACT

Wireless sensor network has been widely used in many large-scale monitoring field, are used to scale in the field of environmental monitoring, military reconnaissance, etc.. Wireless sensor nodes are usually deployed in unattended areas in bad environment, easily damaged or node by node attack, resulting in transmission of sensor network is seriously affected. Computing ability, limited storage space according to the characteristics of the wireless sensor node, we design the authentication mechanism of data combined with multi node multi hop long path, the effective use of data authentication mechanism to ensure the safety of transmission path.

In-depth study of data in wireless sensor network authentication theory, designed the joint data of multi node authentication protocol for multi hop long path, false data filtering, effectively limiting the attacker by compromised nodes launch collusion attack threat. And the design of the maintenance algorithm between nodes on the path, ensure the stability of data authentication mechanism, the safety performance of protocol analysis.

Aiming at the deficiency of multi hop long path write more joint data authentication protocol, the algorithm is optimized, proposes a multi-path resistance to node failure mechanism and dynamic step joint data multi node authentication mechanism, the goal is to improve the reliability of the data transfer, reduce communication overhead data authentication mechanism, and the safety performance of the optimization scheme the analysis evaluation.

Multi hop path around the long joint data multi node authentication mechanism for key distribution scheme needs, in-depth research, put forward the key distribution scheme based on one-way hash chain, and the authentication of MAC has been studied, put forward to meet the demand of the MAC code data authentication mechanism.

The simulation results proved that the proposed scheme of safety performance and the optimization effect to achieve the expected goal.

Key Words: Wireless sensor network;Network security; Data authentication; Key distribution scheme;

第一章　绪论

本章介绍了无线传感网的结构，及其应用领域。并介绍了无线传感网的特点，针对规模化传感网数据认证的需求和面临的挑战进行了分析。最后对本文研究的课题背景和研究意义进行介绍，然后对本文的研究内容和文章的组织结构予以说明。

1.1　本文研究背景和意义

无线传感器网络 (Wireless Sensor Networks，无线传感网) 是一种特殊组织结构的移动自组网[1]，在环境监测、工业控制、资源监控、智能家居、医疗保健和军事等各种领域都有广泛应用，有非常重要的地位和作用。随着无线传感网技术的不断发展，很多应用进入了日常生活中，物联网技术也将成为未来发展的重要方向。无线传感网的各种技术发展紧跟具体的应用需求，随着各种应用场景需要的安全性越来越高，安全问题也成为了阻碍无线传感网大规模发展的一个制约。

大范围监测在环境监测和军事侦察等诸多关系国家社会重大安全的领域都具有重要的地位和作用。在环境监测领域，往往面临范围野外受限甚至恶劣条件，在海洋等资源监测领域，水声通信等基础技术还不是很完善，在军事侦察对抗领域更是要应对破坏攻击情况，传统的大范围实时监测机制和系统都难以得到有效部署，使用无线传感技术成为了最好的解决方案。规模化无线传感网因此应运而生，而且为满足大范围监测的需要，无线传感网的规模越来越大。

规模化无线传感网面临的安全威胁更多，攻击的影响更大，而且由于传感器节点的特点，传统的安全机制和协议无法直接适用于无线传感网，使得安全问题更加凸显。因此针对规模化无线传感网安全机制的研究成为了热门研究方向。

1.1.1　无线传感网概述

1.1.1.1　无线传感网结构

无线传感器节点被部署在目标监测区域，大量的传感器节点通过无线广播的方式，以一定的算法自组织成为一个多跳的无线网络。如图 1.1所示，是一个典型无线传感网的结构[2]，由三部分组成：监测区域的传感器节点、与外部网络连接的网关或基站、远程数据中心。在监测区域的传感器节点一般通过算法组成若干的簇，每个簇通过簇头节点与其他簇或者基站通信，这样的方案节约了节点的能量。簇内节点收集到监测数据以后通过簇头节点的整合，形成报文通过一定的路径发送给基站，基站进一步通过外部网络设备，如互联网、卫星等将监测数据传输到远程数据中心。

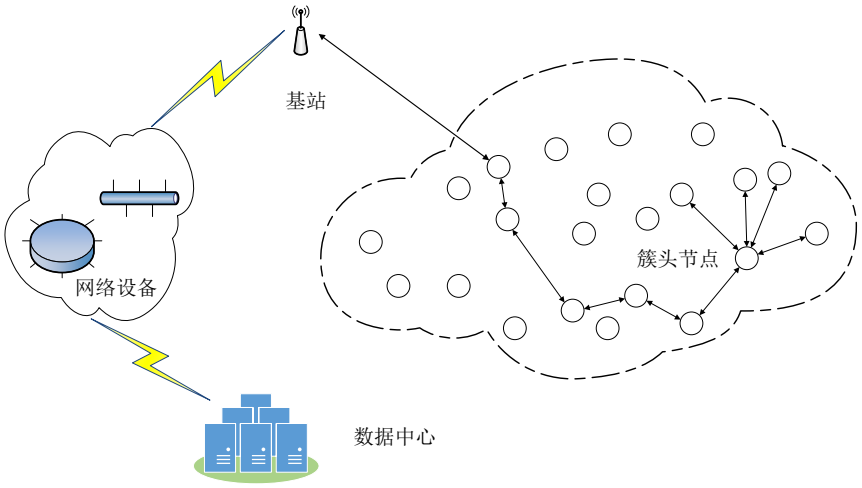

图 1.1　无线传感网系统结构

无线传感网中，基站的计算和存储能力都比较强，基站的功能可以是一个数据处理中心，向网络广播控制信息，从监测区域获取数据。也可以是一个网络网关，负责数据向远程数据中心的传输。

1.1.1.2　无线传感器节点结构

传感器节点是无线传感网的基本组成单元，负责数据采集、发送等基本功能。无线传感器节点一般仅具有很小的存储空间，较弱的计算能力，因此单个节点无法完成复杂的感知任务，需要大量的节点协同工作。

随着电子技术的发展，无线传感器节点的性能也有了很大的提升，如 Crossbow 公司研发的 TelosB，CPU 频率为 8MHz，有 10KB 的 RAM，使用 2.4GHz 无线电，能达到 250Kbps 数据传输，使用两节 AAA 电池 (5 号电池) 供电。国产传感器节点典型的有美新的 MEMSIC 无线模块，工作频率可选 433 MHz、868-915MHz 或 2.4GHz，拥有 5 年电池寿命，支持 10-100 米的发射范围，拥有 19.2kbps-240kbps 的数据传输速率。

这些传感器节点的设计原理基本相同，主要包括 4 个模块：传感模块、数据处理模块、无线通信模块和能量供应模块。如图 1.2所示，是一个典型的无线传感器节点的结构图。传感模块主要负责从感知区域通过传感器获取数据，并将数据转化为适合进行网络传输的数字信号；数据处理模块主要包括处理和存储功能，负责控制传感器节点的运行，对传感模块获取的数据进行处理和存储，数据报文的整合与认证都是由数据处理模块完成，一般该模块需要嵌入式系统的支持，如 UC Berkeley 的开源嵌入式系统 TinyOS[3] 等；无线通信模块负责与其他传感器节

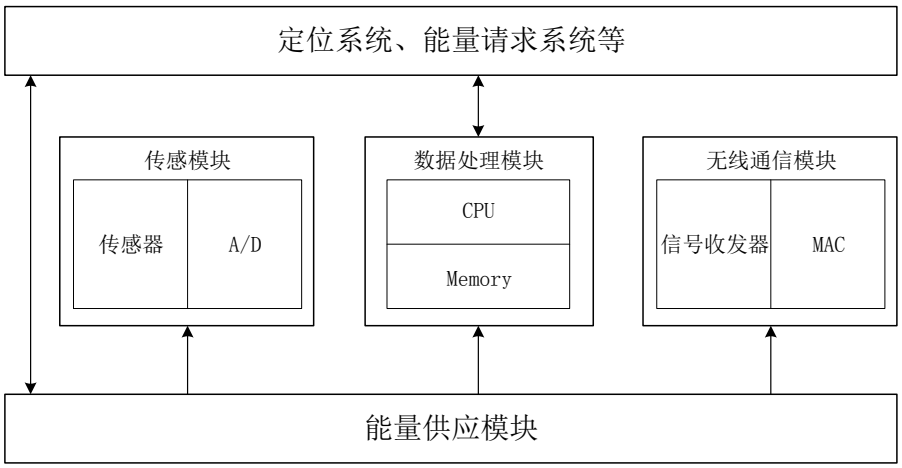

图 1.2　无线传感网节点结构

点或基站之间的通信，传感器节点一般使用内置天线进行数据收发；能量供应模块负责给其他模块供应能量，大部分传感器节点使用微型电池作为电源，因此能量非常有限。传感器节点中还包括一些负责定位、同步等功能的部件。

1.1.1.3　无线传感网协议结构

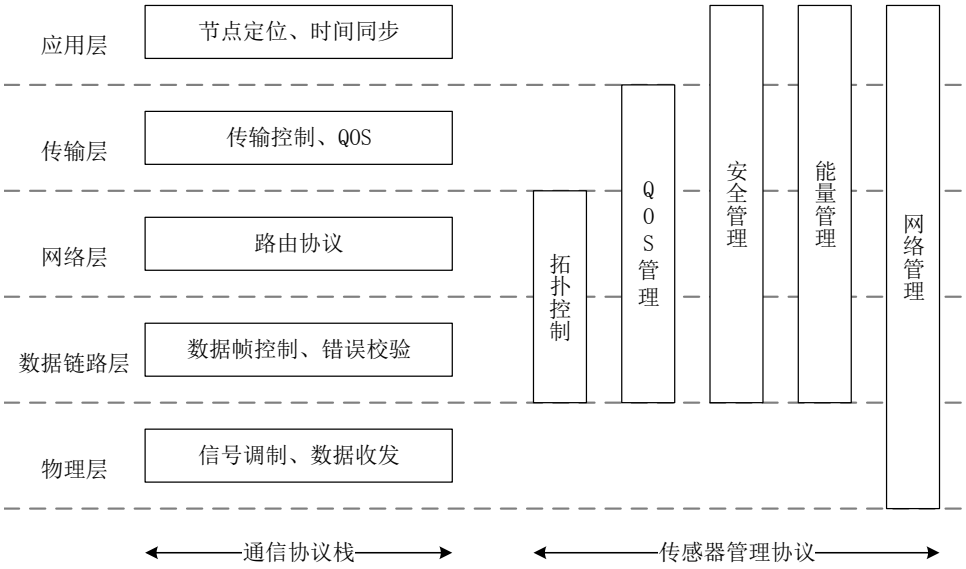

图 1.3　无线传感网协议结构

无线传感网的通信协议栈和相关网络管理技术是当前的主要研究内容，协议结构如图 1.3所示。因为无线传感网是面向特定需求的网络，因此针对不同的部署环境，不同的网络部署结构，要对通信协议栈进行优化，使能量消耗、抗节点损耗、抗攻击能力等适应传感网的应用需求。

类似于 OSI 网络模型，无线传感网的通信协议栈由物理层、数据链路层、网络层、传输层、应用层组成：

物理层：物理层是通信协议栈的最底层，主要功能是将数据调制成适合传输的数字信号，通过无线电、红外灯无线介质完成传感器节点的数据收发。

数据链路层：数据链路层负责装配数据帧，对数据帧进行 MAC 校验，进行差错控制，向网络层提供透明可靠的数据传输服务。

网络层：主要负责无线传感网中的路由功能，将数据通过有效路径传送到目标节点，向传输层提供端对端的数据传输服务。

传输层：传输层负责数据报文的传送和控制，为应用层提供可靠的传输服务，对网络进行流量控制，进行服务质量控制（QOS）。

应用层：直接为应用提供服务，提供相应的应用协议和服务接口。

传感网管理协议提供了拓扑管理、QOS 管理、安全管理、能量管理和网络管理等功能，实现对无线传感网以及各个节点的监控和管理。

1.1.1.4 无线传感网的应用前景

分布式传感网在军事中的应用是无线传感网的雏形，随着电子技术的不断发展，传感器节点的性能不断提升，无线传感网各种协议的完善和发展，使无线传感网在环境监测、军事侦察、智能家居、智能公路等各个领域得到了大量的应用，其应用前景十分广泛。

- 环境监测：无线传感网能完成大范围监测的任务，在自然数据采集中发挥重要作用，尤其是海洋监测传感网和内陆水文传感网等应用领域。如 Li 等人将无线传感网部署在水产养殖水域，对水环境数据进行检测[4]。
- 军事侦察：由于无线传感网具有自组网、部署简单、容许节点失效等特点，适合部署在危险的敌对区域，完成军事侦察、战场环境监测等任务，因而在军事领域有很大应用前景，是现代化电子战的重要战略武器。如美国海军将开发的自主分布式 DADS（Deployable Autonomous Distributed System）用于沿海广大海域的警戒、反潜和反水雷[5]。
- 智能家居：智能家居是通过无线传感器将房间中的各种家电等设备连接起来，实现家居环境的监测以及远程控制，构建出智能的居住环境[6]。
- 智能公路：通过部署在公路上的无线传感器节点以及车载传感器节点，共同组成智能公路传感网络，对交通状况实现自动监测，引导车流等，实现自动化的公路交通管理。

1.1.2 规模化无线传感网数据认证

1.1.2.1 规模化无线传感网的数据认证需求

无线传感网中的认证包括身份认证和数据认证。身份认证是对网络中节点的合法身份的一种断定机制，是数据认证的基础。无线传感网数据认证主要包括两个方面:

- 数据来源合法性，主要以身份认证为基础，通过数据报文中的认证机制判定数据报文的来源的合法性。
- 数据完整性，通过数据认证的机制，确保节点收到的数据报文没有被非法进行篡改。

在环境监测等领域，规模化传感网每天都会产生海量的感知数据。在军事侦察领域，随着侦察区域的扩大，侦察精度的提高，传感网感知的数据量飞速增长。尤其在实时监测场景，数据量大、传输实时性要求高，无线传感器节点的性能限制使得规模化传感网实现可靠传输具有非常的难度，合适的数据认证机制可以为其提供有力支持。在无线传感网中数据泄露、错误数据甚至虚假数据会对网络的安全造成重大影响。尤其在重要战略场景或军事场景，还要考虑破坏攻击的可能，因此数据认证更为安全攸关。

1.1.2.2 规模化无线传感网数据认证面临的挑战

复杂环境下数据高安全性要求对数据认证提出的挑战。实时监测传感网通常部署环境恶劣，而且缺乏基础设施的建设，由于自然环境和主动攻击等对节点的破坏，使节点的失效率很高，网络拓扑结构动态变化，数据传输质量不够稳定，而且存在突发大故障潜因，需要在容灾抗毁前提下进行数据认证，确保传输的安全性。

端对端传输为数据认证提出的挑战。完全依靠广播等数据传输机制，在规模化无线传感网中，传输效率过低，消耗的节点能量和通信资源过大，而且容易受到泛洪攻击的影响。有效利用规模化传感网中端对端数据传输，能够有效的保证传输效率。在端对端传输中，由于多跳传输的原因，当路径中出现妥协节点时，整条路径容易被攻破，从而造成数据传输被攻击，因而在多路径端对端的数据传输中，有效利用数据认证机制加强路径上的安全保障是安全传输的关键。

轻量级认证机制及其实现技术为数据认证提出的挑战。规模化无线传感网传输的数据量大，要求处理快捷。在节点资源能力受限，通信能耗受限的前提下，需要计算、存储、通信都轻量级的水平，保障网络安全、传输可靠性、高效性和数据可信，具有很大难度。传统的的认证机制使用的密码算法复杂度未达到轻量级，不适合规模化传感网网络资源受限的特点，我们需要设计适合实时性较高的规模无线传感网达到轻量级算法。

攻击对抗对数据认证提出的挑战。无线传感网一般部署在恶劣环境中，而且具有自组网络的多跳性、无中心性和自组织性等特征，致使其通信协议栈的各个层级都容易遭受到各种形式的攻击，我们需要设计能够适应有限节点能量，有限计算能力的数据认证算法，对抗各种攻击，保证无线传感网传输数据的来源合法性和完整性。

1.2 本文研究内容

本文根据无线传感网的安全需求以及其特点，针对数据认证问题展开研究，使用多节点联合的思路对数据认证机制进行了深入研究，并设计实现了关键算法。主要工作如下:

1. 提出了多跳长路径上多节点联合数据认证的模型，设计了多跳长路径上多节点联合数据认证协议，并设计了路径上节点关系的维护算法，对协议的安全性能进行了分析评价。
2. 针对多跳长路径上多写点联合数据认证协议的不足，对算法进行了优化，提出了多路径抗节点失效机制和动态步长多节点联合数据认证机制，并对优化方案的安全性能进行了分析评价。
3. 围绕多跳长路径多节点联合数据认证机制的需求，对密钥分配方案进行了深入研究，提出了基于单向 hash 链的密钥分配方案，并对认证中的 MAC 进行了研究，提出了适应数据认证机制需求的 MAC 码。

1.3 本文组织结构

本文一共分为七章。

第一章　绪论，介绍了课题的选题背景，描述了无线传感网的特点，介绍了无线传感网的相关安全技术，列出了本文的主要研究内容和本文组织结构。

第二章　相关研究概述，本章首先对无线传感网的安全技术进行了概述，然后重点对数据认证和密钥分配两种安全技术进行了论述。

第三章　多跳长路径上多节点联合数据认证，本章提出了无线传感网中多跳长路径多节点联合的数据认证模型，及其设计目标。重点介绍了关键算法与协议的设计实现，对多节点联合数据认证机制的安全性能进行了分析评价。

第四章　数据认证方案优化，本章针对多跳长路径上多节点联合数据认证进行了优化，提出了多路径抗节点失效和动态步长多节点联合数据认证两个优化方案，并对它们的安全性能进行了分析评价。

第五章　密钥分配与 MAC 设计，本章对多节点联合数据认证中的密钥分配方案以及使用的 MAC 的设计进行了介绍，提出了基于单向 hash 链的密钥分配方案，以及适应多节点联合数据认证的 MAC 码。

第六章　仿真实验与结果分析，本章在仿真平台上对多跳长路径多节点联合数据认证机制，以及其优化方案进行了仿真实验，对它们的安全性能结果进行了评价。

第七章　总结与展望，本章对全文的工作做了总结，指出了数据认证机制现阶段的不足以及未来研究中需要研究及完善的地方。

第二章　相关研究概述

无线传感网在环境监测、工业控制、资源监测和军事侦察等领域都有重要的应用，具有非常良好的前景。但是区别于传统的网络，无线传感器节点一般都部署在无人值守的环境恶劣地区或敌对区域，可能受到敌人的攻击破坏，所以安全问题十分突出。同时由于无线传感器节点的存储空间和计算能力的限制，安全机制的复杂性受到约束，因此设计适合无线传感网应用需求的安全机制十分重要。

本章首先对无线传感网的安全技术进行概述，然后对无线传感网的认证机制及其密钥分配方案进行概述。

2.1　无线传感网安全技术概述

无线传感网的节点一般部署在无人值守区域，使得无线传感网的安全问题尤为突出，特别是在军事侦察等应用领域。无线传感网不能直接沿用传统无线网络的安全机制，设计无线传感网的安全机制时，必须考虑到无线传感器网的如下限制[7]：

- 节点的存储空间、计算能力和通信能力有限，特别是节点的能量有限，严重制约了安全机制的发展。
- 无线传感网有无线自组网的缺点，缺乏基础设施建设，节点之间使用不安全的无线通信。
- 部署的位置一般是敌对区域或者危险区域，节点很容易受到物理攻击或者破坏。

无线传感网的应用决定了其安全目标与传统网络有所不同，更侧重于保护感知的数据，保证数据的安全。在无线传感网中，安全技术的目标主要包括[8]：

- 数据认证：通过认证确保数据来自经过身份认证的节点，保证数据的安全。
- 数据保密：确保只有通过认证的节点才能获取消息中的内容，不会暴露保密的内容。
- 数据完整性：确保所有受到的消息没有被未经授权的设备所篡改。
- 可用性: 确保传感器节点在受到攻击时仍然能提供指定的基本服务。
- 数据新鲜：保证数据在指定时间内到达目的节点，确保数据的有效性。

2.1.1　无线传感网面临的安全威胁

无线传感网的协议栈包括传输层、网络层、链路层和物理层，各层都会遭到不同的攻击。对于各层的攻击，有各种防御手段来保护无线传感网的安全，传输层主要研究认证机制及面向认证的密钥管理技术，网络层主要研究路由安全协议，

数据链路层主要研究数据帧的安全传输，物理层主要研究节点间通信信道安全。无线传感网中常见的攻击与防御措施[8] 如表 2.1所示：

表 2.1　无线传感网常见的攻击与防御措施

网络层次	常见的攻击	防范措施
传输层	泛洪攻击	用户询问
	同步破坏攻击	认证机制
网络层	泛洪攻击	广播和组播半径限制
	黑洞攻击	节点身份认证，冗余路径
	错误定向攻击	数据帧转发签名
	蠕虫洞攻击	基于信任等级的路由
	创建路由环	篡改校验、认证
	汇聚节点攻击	加密、逐跳认证机制
	虚假路由攻击	冗余机制、数据一致性检测
数据链路层	资源耗尽攻击	限制通信速度，竞争门限控制
	碰撞攻击	纠错校验码
	非公平竞争攻击	使用非优先级策略
物理层	拥塞攻击	使用优先级消息、宽频通信、间歇通信
	无线干扰	变频通信、跳频通信
	物理破坏	节点伪装和隐藏

物理层受到的攻击主要包括拥塞攻击、无线干扰和物理破坏。拥塞攻击是物理层最常见的攻击，Xu 等就提出了 4 种不同的拥塞攻击方法[9]，能够使无线传感网停止工作。无线干扰是干扰传感器节点的通信信道，和拥塞攻击一样都能严重影响节点的数据发送和接收。通过物理攻击，篡改节点信息是物理层的另一种攻击方法，攻击者能获得节点的内存信息，包括密钥和加密数据，从而破坏该节点的工作。

数据链路层容易受到碰撞攻击，攻击者利用协议的漏洞，在无线传感网发送大量的干扰数据包，与正常数据包传输发生碰撞，造成无线传感网正常数据无法传输，并且消耗节点能量。数据链路层还容易受到资源耗尽攻击，即向特定节点发送大量数据，消耗其节点能量，使之失效。非公平竞争是指攻击者通过发送高优先级的数据包，在网络中一直占据通信信道，使得正常节点一直无法使用信道，无法发送数据。

在无线传感网中，大量的传感器节点部署在监测区域内，报文需要经过多跳才能到达基站，无线传感网的特性决定了它没有固定的拓扑结构，所以每个节点都能进行路由，因此攻击者可以利用该特点发动网络层攻击。网络层受到的攻击

包括泛洪攻击、黑洞攻击、错误定向攻击、蠕虫洞攻击、创建路由环攻击、汇聚节点攻击和虚假路由攻击。

传输层受到的攻击包括泛洪攻击和同步破坏攻击。当攻击者发送大量的连接请求，就能严重影响到无线传感网的通信，甚至无法进行正常网络通信，也就是泛洪攻击。同步破坏攻击是指向建立了通信连接的节点不断发送伪造的发送失败消息，使节点一直因为帧丢失而进行重传，而且达到攻击传感器网络的目的。

无线传感网各个协议栈都容易受到攻击，虽然都有相应的防御的措施，但是现阶段的安全机制方案还不够完善，严重制约了无线传感网的应用和发展。

2.1.2 无线传感网现有的安全技术

无线传感网面临着多种攻击的威胁，许多安全技术方案在保护其安全方面已经有了突破。对于无线传感网的安全技术，在保证数据传输安全的前提下，其设计要考虑到如下需求：- 稳定性：整个无线传感网的安全体系不会因为个别节点的失效或者被攻击而瘫痪。- 可扩展性：传感网加入新节点，不会对原有的安全体系造成影响，同时不应产生过大的计算开销。- 灵活性：安全技术不能影响到网络的部署结构的灵活性。- 低开销：安全技术的计算开销、通信开销和存储开销应当适合无线传感器节点的能力，不会影响到节点的正常功能。

无线传感网现有的安全技术主要包括加密算法、安全路由、数据聚合、入侵检测、认证机制和密钥管理，其中认证机制和密钥管理将在 2.2 节与 2.3 节进行详细论述。

2.1.2.1 密码算法

由于无线传感器节点自身的局限性，计算能力和节点存储空间有限，导致目前非对称密码算法在传感器节点不能直接应用。而对称密码算法需要的计算能力更小，存储空间开销也相对较小，因而目前的传感器网络主要使用的是对称密码算法。如 RC5[10]、RC6[11]、Camellia[12]、TEA[13] 和 MISTY1[14] 等对称加密应用在无线传感网中，在文献 [15] 中，Law 等对这些对称加密算法在无线传感器节点中的运行性能进行了比较和分析。

虽然现阶段非对称密码还很少应用在无线传感网的安全协议中，但是随着硬件技术的进步，传感器节点的计算和存储能力不断提高，低开销的非对称密码算法应用在无线传感网的安全协议中成为了可能，也成为了现阶段无线传感网密码算法研究的热点。现阶段非对称密码在传感器节点上的尝试主要是基于椭圆曲线的密码算法（ECC），David 等将 ECC 应用在 TinyOS 中 [16]，Gura 等将 ECC 和 RSA 在 MICA 上成功实现[17]，并对它们进行了分析比较。

2.1.2.2 安全路由

路由技术在传统的网络中有非常成熟的协议，但是由于无线传感网的特性，没有特定的路由节点，每个节点都要完成路由的功能，导致无线传感网的路由技术与传统网络有较大区别。现阶段多数路由协议都注重提高路由效率，以降低节点的能量消耗，但是这样也造成了潜在的安全问题。

许多相关研究都针对无线传感网的路由安全问题进行了探索，如 Deepak 等提出的多路由机制[18]，通过在多条路径上传输同一个数据报文，来防御选择性转发攻击，但是该方案中，数据报文需要传输多次，造成通信开销的浪费。还有其他路由协议通过加密和认证等方法提高路由的安全性能，如 Karlof 等人的方案[19]和 Li 等人的方案 [20]。

2.1.2.3 数据聚合

数据聚合减少了无线传感网中的冗余数据，降低了通信开销，节约了节点能量。通过数据聚合安全机制，提高了无线传感网中数据私密性，提高了网络传输的安全性。

Priyanka 等人在数据聚合中添加了错误数据检测机制，提出了一种高效的数据聚合方案[21]，保证了数据的安全传输。类似的研究还有 Suat 等人的方案[22]，通过将数据聚合和安全传输以及错误报文过滤相结合，提高了无线传感网数据传输的安全。

Sivagami 等人提出的方案[23] 中，通过多节点对之间延迟发送消息认证码来对发送的数据进行认证，实现了安全的数据聚合，并且降低了传输开销。

Zhu 等人提出了一种错误数据报文过滤机制[24]，通过节点间的交叉认证，保证了错误报文在被捕获节点不超过设计参数的情况下会在路径中被过滤。

2.1.2.4 入侵检测

当无线传感器节点的部署在敌对区域时，很容易受到攻击，节点被捕获或者受损不可避免，而攻击者可以通过这些妥协节点发送进一步的攻击，从而影响整个无线传感网的安全。因此在无线传感网中，入侵检测技术可以发现网络中的异常情况，并识别恶意节点，成为了无线传感网的重要安全技术手段。入侵检测主要通过对传感网中的数据发送行为和数据报文进行分析，发现异常事件，并确定恶意行为的来源节点。

无线传感网的入侵检测机制主要由入侵检测、入侵跟踪和入侵相应 3 部分构成。在 Wang 等人提出的方案中[25]，构建了覆盖可疑节点及其相邻节点的支配树，通过同可疑节点的相邻节点进行合作，来判断可疑节点是失效节点或者是恶意节点，并通过使用基于覆盖的启发式技术来提升检测效率。

恶意节点检测方案还有 Mathews 等人的检测方案[26]，Zhang 等人提出的基于位置的妥协节点检测机制[27]，以及 Agah 等提出的基于非合作博弈的入侵检测方案[28]。

2.2 无线传感网认证机制概述

无线传感网的核心功能是在目标区域采集数据，并将数据传输到数据中心。攻击者通常会针对部分节点进行攻击，在捕获节点以后，利用这些节点联合对整个无线传感网进行攻击，因此认证机制在保证无线传感网数据安全传输中发挥重要作用。认证机制按照不同的方法，可以分为对称密钥和非对称密钥认证机制、消息认证和身份认证机制或广播认证和单播认证机制。在本节中，主要讨论无线传感网的数据认证和身份认证。

2.2.1 无线传感网数据认证概述

无线传感网的数据认证有基于对称密钥和基于非对称密钥两种，因为节点的性能限制，现阶段的方案主要是基于对称密钥实现。

现阶段的数据认证方案主要是 Perrig 等人提出的 $\mu TESLA$ 方案[29]，以及基于 $\mu TESLA$ 的改进方案。如图 2.1所示，是 $\mu TESLA$ 方案的认证过程，$\mu TESLA$ 是

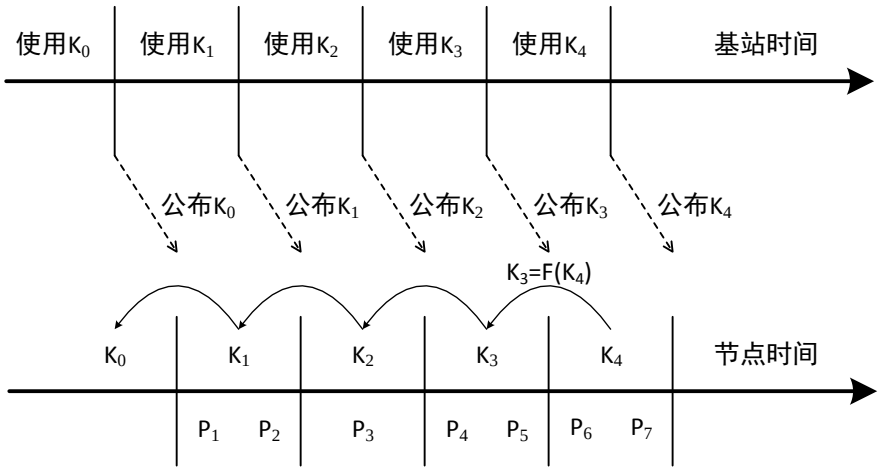

图 2.1 $\mu TESLA$ 认证机制

基于对称密钥的，对报文计算消息认证码的认证密钥和节点对报文进行认证的密钥是相同的。其认证过程包括密钥建立、广播报文、自举接收者和对报文认证等步骤。其中密钥分发是通过单向 hash 函数 F 来实现的，如 $K_3 = F(K_4)$。然后广播一个密钥 K_i 加密后的报文，无线传感网中基站和节点采用不同的时隙，使广播加密报文和接收到相应的密钥不同步。通过延迟发布密钥 K_i，使得认证过程具有非对称性，提高认证的安全性能。通过比较报文的接收时间和认证密钥发布的时隙，

能对报文的安全性进行检查。但该方案仍有其缺点：密钥的发布延后于报文的到达，因此节点接收到的报文必须缓存在节点中，浪费节点宝贵的存储空间，并且有可能被攻击者发动泛洪攻击，大量的伪造报文填满传感器节点的缓存空间，导致无线传感网传输功能失效，攻击者也容易发动虫洞攻击，威胁传感网的安全。

Liu 等人基于 $\mu TESLA$ 方案，提出了多级 $\mu TESLA$ 方案[30]，采用多级密钥链解决 $\mu TESLA$ 方案中密钥链占用存储空间过大，容易导致泛洪攻击的问题。该方案使用预装初始化参数的方案，代替 $\mu TESLA$ 方案中通过单播进行初始化的过程。如图 2.2，是多级 $\mu TESLA$ 方案的认证过程。在该方案中，Liu 使用了 2 级时间，在 1 级时间中，将时间划分为 n_0 个间隔，每个时间间隔对应该级的单向 hash 链中的密钥 $K_i, 1 \le i \le n_0$，其中密钥还是同 $\mu TESLA$ 方案，使用单向 hash 链生成。一个 1 级时间间隔又被划分为 n_1 个 2 级时间间隔，每个 2 级时间间隔的密钥使用 $K_i, 1 \le i \le n_0$ 作为密钥种子生成。每个 2 级时间间隔内发送的报文用对应的密钥进行认证，其中的密钥链头 $K_i, 0$ 在前一个 1 级时间发布。

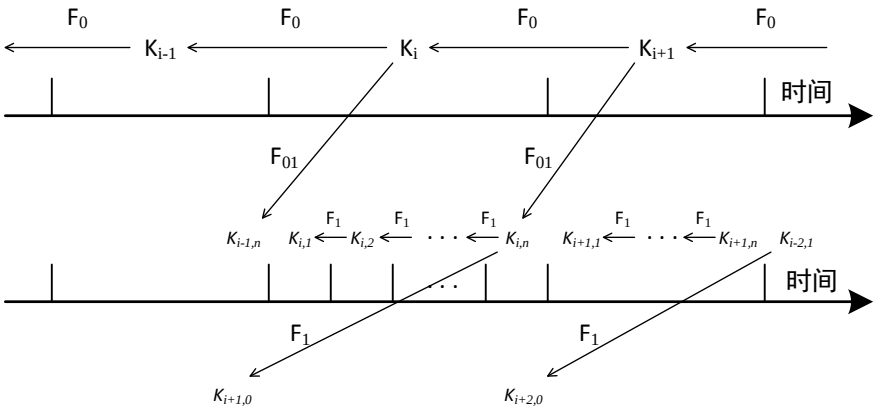

图 2.2　多级 $\mu TESLA$ 认证机制

在裴庆祺等人的 $\mu TESLA$ 改进方案中[31]，引入了 (t, n) 的门限秘密共享，每个认证密钥被分隔为 n 个密钥片，分配到各个基站。在无线传感网中执行原有的 $\mu TESLA$ 方案，将密钥片进行广播，当一个节点接收到超过 t 个密钥片之后，就通过秘密共享的算法，对认证密钥进行恢复，重构出认证密钥。该方案提高了 $\mu TESLA$ 方案的认证率，并且有高可靠性和高容忍性的特点，缺点是通信开销明显增加。

Anas 等人提出了一种基于信任模型的认证方案[32]，使用一个轻量级的基于椭圆曲线的简单认证密钥协议。通过通信实体之间建立信任级别，使非对称密钥认证系统能在资源有限的无线传感器节点上运行。

Dong 等人利用消息预认证提出了一个基于密钥链的过滤方案[33]，能对无线传感网中的广播进行过滤，有效减少虚假广播对传感网数据传输的影响，该方案的缺点是无法有效防御攻击者的联合节点攻击。

2.2.2 无线传感网身份认证概述

攻击者可以通过对网络发送大量的虚假数据报文，大量消耗节点的计算和存储能力，消耗节点的能量，导致传感网的失效。因此对传感网中的节点进行身份认证尤为重要。文献 [34] 中，利用随机配对密钥分配方案，一个密钥仅会分配给一对节点，来实现一种非常简单的身份认证，即两个节点通过使用预分配的密钥对消息的加密和解密判断是否是经过认证的节点。但是该方案无法实现真正的身份认证，因为被捕获的节点可以伪装成正常节点进行欺骗，对无线传感网进行攻击。

现有的身份认证方案主要有非对称密钥认证和秘密共享认证。由于无线传感器节点的限制，现阶段非对称密钥认证的实现一般是消耗能量较多的计算由基站完成，消耗能量较少的计算由节点完成。秘密共享的认证则是基于多个节点共同对一个节点进行认证。

虽然现阶段由于传感器节点的限制，非对称密钥没有被广泛应用于无线传感网的认证，但是许多研究也对此进行了探索。在非对称密钥机制中，椭圆曲线密码（Elliptic Curve Cryptography,ECC) 是一种轻量级的方案，研究结果表明，160 位的 ECC 能获得相当于 1024 位 RSA 密码的安全性能。而且使用非对称密钥不需要 $\mu TESLA$ 方案中的延迟发布密钥，还能提高认证系统的安全性。

Watro 等人提出了一个基于 RSA 算法的认证机制 TinyPK[35]，该方案使用请求 -应答机制。该方案使用了双重校验，来保证认证机制的安全性。当一个节点需要同另一个节点进行认证时，向该节点发送一个请求信息，其中包括两部分。第一部分是使用认证中心的私钥进行签名的请求节点的公钥，第二部分是使用请求节点私钥签名的时间戳和消息认证码。应答节点接收到该请求消息以后，使用认证中心的公钥对第一部分进行解密，获取请求节点的公钥。使用请求节点的公钥解密第二部分，获得时间戳和消息认证码，通过时间戳和消息认证码的校验，来判断请求节点的合法性。如果通过，则建立两个节点之间的安全通信。

在 Bauer 等人的方案[36] 中，使用了秘密共享的思想进行身份认证。当一个节点请求对另一个节点的认证时，应答节点发送消息给认证中心，宣告自己被请求做认证处理，处理中心将请求节点的私钥进行划分，将秘密片广播给应答节点的邻居节点，所有节点发回给认证中心一个判定消息，如果通过认证的消息超过阈值，则请求节点通过认证，应答节点此时与认证中心进行交互，更新自己的私钥。

现有的身份认证方案还有 Benenson 提出的基于 ECC 的方案[37]，Cao 等基于 vBNN-IBS 提出的多用户广播认证方案[38]。

2.3 无线传感网密钥分配理论概述

进行认证的基础是密钥的分配，设计一个面向无线传感网需求的密钥分配方案，才能保证认证机制的性能。无线传感网中的密钥分配与传统无线网络有较大区别，在传统的无线网络中，密钥分配方案的研究已经取得了许多成果，但是由于无法适应无线传感网的特点，这些成果无法应用于无线传感网中。因为 WSN 节点资源的限制，传统无线网络中节点计算开销和通信开销较大的密钥分配方案无法适用。在设计无线传感网的密钥分配方案时，不仅要保证方案的安全性能，也要权衡计算开销和通信开销。

2.3.1 无线传感网密钥分配方案分类

近些年来，WSN 的密钥分配有了许多新的研究成果，根据所适用的密钥是否是对称密钥，可以将方案分为对称密钥方案和非对称密钥方案。随着传感器技术的发展，非对称密钥技术可能成为将来无线传感器密钥分配的主流，但是由于目前无线传感器节点的计算能力和存储空间的限制，现有的无线传感网密钥分配以对称密钥方案为主。基于对称密钥，有很多的密钥分配机制的研究成果，表 2.2列出了目前无线传感网主要的密钥分配方案：

表 2.2　无线传感网主要的密钥分配方案

数学结构	密钥分配方案	密钥分配方法
密钥池	E-G 方案	随机预分发
	q-composite 方案	
	PIKE 方案	基于网格预分发
二元对称多项式	Blundo 方案	确定预分发
	Liu-Ning 方案	基于随机子集预分发
	GBKP 方案	基于网格预分发
	CPKS 方案	基于位置预分发
MDS 码生成矩阵	Blom 方案	确定预分发
	Du-Deng 方案	基于随机子集预分发
区组	Camtepe 方案	组合设计
	Camtepe 混合组合设计方案	组合设计及随机预分发

2.3.2 无线传感网典型密钥分配方案概述

根据密钥分配方法的不同，我们对不同类别的无线传感网密钥分配方案进行概述：

2.3.2.1 基于随机预分发的密钥分配

Eschenauer 和 Gligor 基于随机图理论，提出了无线传感网中随机密钥预分配的方案[39](简称 E-G 方案)，该方案包括 3 个阶段。在密钥预分发阶段，密钥分发中心生成一个足够大的密钥池 P，然后对于每个传感器节点，从中随机选择 m 个不同的密钥，形成一个密钥环，并将密钥保存到传感器节点的存储空间中。在密钥发现阶段，每个节点通过相邻节点发现机制寻找物理上相邻的节点，由于所有节点的密钥是从密钥池中随机取出的，相邻节点可能存在相同的密钥，如果相邻节点存在共享密钥，则作为两者之间的会话密钥。当相邻节点之间不存在共享密钥，则开始路径密钥建立阶段。通过在密钥发现阶段建立的节点连通图 $G(V,E)$(V 为传感器节点的顶点集合，E 为有共享密钥的传感器节点之间构成的边集)，在图中查找一条通往没有共享密钥的相邻节点的路径，建立相邻节点之间的路径密钥。

在 E-G 方案中，两个相邻节点之间有共享密钥的概率 p 同节点存储密钥数 m 之间的关系可以表示为：$p = 1 - \frac{((P-m)!)^2}{(P-2m)!P!}$。E-G 方案使得每个节点只需要存储较小数量的密钥，就可以有较高概率使得无线传感器网络完成密钥建立过程，符合无线传感网的特点要求。但是 E-G 方案作为最早提出的无线传感网密钥预分发方案，也有自身的缺点，当妥协节点增多时，无法保证无线传感网的通信安全，因为节点不具备防篡改的机制。而且当一个节点被捕获时，节点上存储的密钥材料全部都暴露给了攻击者，而且这些密钥可能是其他节点间的会话密钥，也就是使攻击者能攻击其他节点之间的通信。

在 E-G 方案的基础上，有许多方案对随机密钥预分配进行了改进，提升随机密钥预分配机制的性能。Chan 等人在 E-G 方案的基础上提出了 q-composite 随机密钥预分配方案[34]，每个节点从密钥池 P 中获取 m 个不同的密钥。方案的密钥个数阈值为 q，当两个节点之间的共享密钥个数 q' 满足 $q' > q$，则两个节点之间使用 hash 函数 $K = hash(K_1||K_2||\cdots||K_{q'})$ 生成会话密钥，在 q-composite 方案中，hash 函数使用了 SHA-1[40]。q-composite 保证了相邻节点之间的安全链路，密钥个数阈值增大时，链路的安全性能也增大。在无线传感网被捕获节点较少时，该方案节点间链路的安全性能比 E-G 方案更好，但是当被捕获节点增多时，该方案的安全性能明显下降。

在 Blom 的对称密钥生成方案[41] 基础上，Du 等人将其与随机密钥预分发结合，提出了无线传感网多密钥空间密钥预分发方案[42]。先使用 Blom 方案生成 ω 个密钥空间，每个节点从中选择 τ 个密钥空间保证在存储空间中 $(2 \le \tau \le \omega)$，如

果两个节点上存储了一个相同的密钥空间，则他们之间计算生成一个共享密钥。与 E-G 方案和 q-composite 方案相比，Du-Deng 方案通过计算适合的参数 ω 和 τ，能明显提高抵抗链路攻击的性能，但是同时也增加了节点的计算开销。

Blundo 利用二元对称多项式的性质，提出了节点对密钥建立方案[43]。密钥服务器随机生成一个有限域上的 k 阶二元对称多项式 $f(x,y)=\sum_{i,j=0}^{k}a_{i,j}x^iy^j$，对于对称多项式，有 $f(x,y)=f(y,x)$。对于任意节点 i，服务器计算 $f(i,y)$，然后将 $k+1$ 个系数存入节点存储空间。当节点 i 和节点 j 需要建立对密钥时，计算 $f(i,y)$ 在 $y=j$ 时的值，计算 $f(j,y)$ 在 $y=i$ 时的值，因为 $f(i,j)=f(j,i)$，所以 $f(i,j)$ 就可以作为节点 i 和节点 j 之间的对密钥。

在 Blundo 方案的基础上，Liu-Ning 提出了基于对称二元多项式池的随机密钥预分配方案[44]。密钥服务器在有限域 F_q 上随机生成一个二元对称多项式的集合 $\phi=\{f_i(x,y),i=1,\cdots,t\}$，对于节点 i，将子集 $\phi_i\subseteq\phi$ 装入存储空间。当两个节点发现有相同的二元多项式，则直接使用 Blundo 的节点对密钥建立方案建立会话密钥。当被捕获的节点较少时，Liu-Ning 方案有较好的安全性能，但是在攻击者捕获了较多节点，也就是获得较多二元多项式的时候，链路的安全性能相较 E-G 方案和 q-composite 方案更低。

利用节点的位置信息，Liu 提出了最近对密钥方案 (CPKS)[45]，节点实际分布位置在其期望分布位置周围服从均匀分布。每个节点与自己期望分布位置最近的 t 节点之间建立对密钥，例如，对节点 u 的相邻节点 v，密钥服务器生成对密钥 $K_{u,v}$，并将 $u,K_{u,v}$ 和 $v,K_{u,v}$ 分别存入节点 u 和节点 v。通过两个节点之间的 ID 信息可以判断两个节点之间是否存在对密钥。在节点位置信息已知时，该方案相比前述方案有更好的性能，缺点是网络扩展性较差，加入新节点，需要大量节点能量消耗。

Du 提出的基于部署知识的方案[46] 中，将密钥池 S 划分为 $t\times n$ 的子密钥池 $S_{i,j}(1\le i\le t,1\le j\le n)$，子密钥空间 $S_{i,j}$ 对应着部署组 $G_{i,j}$。根据部署位置的信息，不同的子密钥池之间发现共享密钥。该方案提高了无线传感网中节点链路连通的概率，但是子密钥池的划分对安全性能的影响较大。

2.3.2.2 基于网格预分发的密钥分配

为了解决随机密钥预分配方案中链路密钥的不确定性，Liu 提出了基于网格的密钥预分配方案 (GBKP)[47]。对一个 $m\times n$ 的传感网，如图 2.3所示，G_i 为部署分组。对 G_i 中的节点分配 ID 集合 $\{(i-1)m+j|j=1,\cdots,m\}$，对 G_i' 中的节点分配 ID 集合 $\{i+(j-1)m|i=1,\cdots,n\}$。服务器生成 $m+n$ 个对称二元多项式分配给每行每列，使得同一行或同一列的节点能直接生成对密钥，不同行或列的节点，通过中间节点生成链路密钥。类似的基于网格预分发的密钥分配方案还有 Chan 提出的 PIKE 方案[48]。

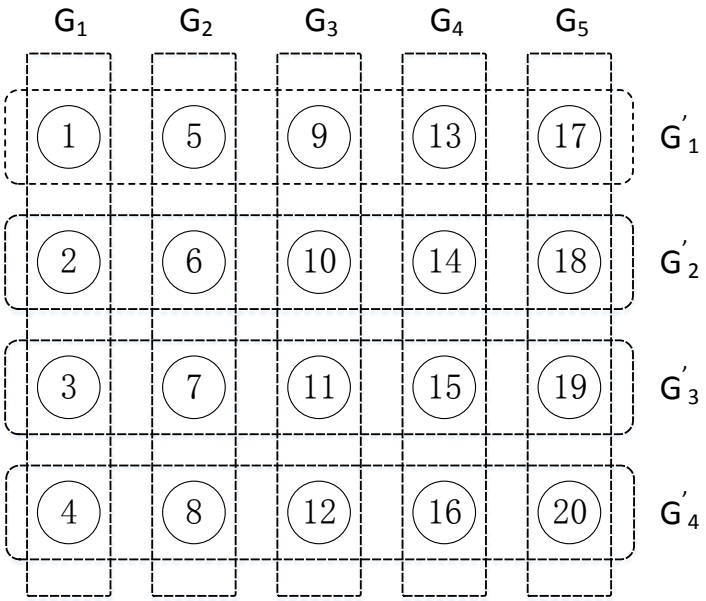

图 2.3　基于网格的密钥预分配方案

2.3.2.3　基于组合设计的密钥分配

Camtepe 把组合设计的理论应用于无线传感网的密钥分配[49]，使用组合设计理论来划分密钥池和密钥环。对一个规模为 N 的无线传感网，生成一个对称 BIBD，$(n^2+n+1, n+1, 1)$，其中 n 为满足 $n^2+n+1 \geq N$ 的最小素数，密钥池的大小为 n^2+n+1，密钥环的长度为 $n+1$。这个方案保证了无线传感网中的任意一对节点有共享密钥，或通过中间节点生成的链路密钥。为了解决该方案在网络规模方面的限制，Camtepe 还提出了组合设计与广义四边形想结合的方案。

第三章　多跳长路径上多节点联合数据认证

本章讨论在无线传感网中应用数据多节点联合认证机制，研究利用多跳长路径上的节点联合，实现错误数据检测。3.1 节介绍无线传感网多节点联合数据认证相关模型，提出了多跳长路径上多节点联合的数据认证及其攻击模型和设计目标。3.2 节设计实现了多跳长路径上多节点联合的数据认证机制。3.3 节提出了无线传感网长路径上节点关系的维护方案。

3.1　无线传感网数据认证模型

3.1.1　多跳长路径上多节点联合数据认证模型

无线传感网被广泛应用在环境监测、数据采集等领域中。如图 3.1所示是一个典型的无线传感网的应用场景，在每个监测区域中，部署的传感器节点采集数据或感知事件后将数据发送给相应的簇头节点。簇头节点将接收到的数据进行聚合之后，通过其与基站之间的若干传感器节点传输给基站。

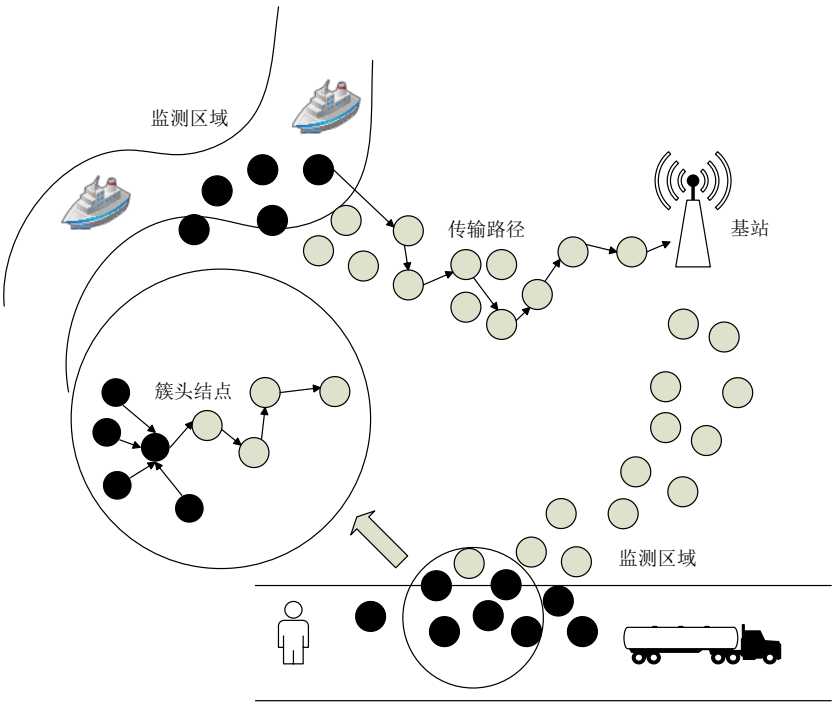

图 3.1　无线传感网应用场景

无线传感网的认证包括传感器节点认证和数据认证，本文主要讨论数据认证。传统的无线传感网认证方式是相邻节点，也即单跳之间利用预分配的密钥进行认

证。由于无线传感器节点发射功率等的限制，通信范围很小，攻击者很容易通过针对性地攻击或捕获节点，获取到密钥信息，从而攻破整个网络的认证系统。利用预共享密钥密钥和节点信息生成节点间的共享对密钥，然后使用共享对密钥认证报文，能提高传感器网络的抗攻击的能力。

完全依靠广播传输机制，在大规模大数据无线传感网中，传输效率过低，消耗的传输能量和资源过大。有效利用大规模传感网中多跳长路径进行端对端数据传输，能够有效的保证传输效率。但是由于无线传感网部署环境恶劣、无人值守等原因，节点很容易被捕获或者被入侵，发送大量错误数据或垃圾数据，消耗传感器节点的能量，传统的认证机制无法对抗这种攻击。本文研究的多节点联合数据认证机制，利用路径上多节点联合进行认证，能够有效地检测出垃圾报文，节约节点的能量。多节点联合数据认证通过维护传输路径上节点对之间的共享密钥，相隔多跳进行认证，有效提高认证系统抗攻击能力。

3.1.2 系统模型和设计目标

3.1.2.1 系统模型

由于无线传感器节点的通信是基于广播的，所以攻击者很容易监听所有通信，注入虚假数据报文。本文假设当攻击者能够获得妥协节点的完全控制，可以获取节点中的所有密钥信息，并利用其发送虚假报文或者丢弃正常报文。攻击者的主要攻击手段是通过发送大量的虚假数据报文，达到消耗传感器节点能量的目的。在本文的认证机制研究中假设攻击者能够有针对性地入侵节点，并利用妥协节点之间的联合来对抗认证机制。

本文中我们假设每个节点同基站之间都有共享密钥，而且每个节点都与它一跳内的相邻节点建立了对密钥，利用 LEAP[50] 中提出的对密钥建立方案可以实现这个目标。通过使用[42, 44] 等密钥建立方案，不相邻的节点之间可以建立对密钥，并在节点发现阶段获得对方的节点 ID 信息。簇与基站之间通过发现簇头之间的对密钥，形成多跳长路径，进行数据报文传输。

3.1.2.2 设计目标

本章所研究的多跳长路径上多节点联合的数据认证机制包括如下设计目标:

1. 基站能够检测出所有虚假数据报文，保证传感网监测功能不受虚假报文的干扰。
2. 当被入侵或捕获的节点数不大于 t（t 为系统设计参数）时，能保证虚假数据报文被丢弃。
3. 传输路径注入的虚假数据报文，被检测并丢弃前经过尽量少的跳数，对于给定的 t，我们的多节点联合认证系统有相应的虚假数据报文传播跳数上限。

4. 认证机制计算高效，消耗能量小，适应无线传感网的要求。
5. 能够有效应对节点失效，能够对传输路径上的节点关系进行维护，保证认证机制的稳定性。

3.2 多跳长路径上多节点联合的数据认证机制设计与实现

3.2.1 符号与定义

本文中相关的符号定义如表 3.1所示：

表 3.1 相关符号说明

符号	描述
CN_i	簇内节点
t	簇内节点个数，不包括簇头节点
CH_i	簇与基站之间长路径上的簇头节点
AK_{si}	ID 为 i 的簇内节点与基站之间的共享密钥
AK_{uv}	节点 u 与节点 v 之间的共享密钥
h_i	簇头节点 CH_i 距离 BS 的跳数
$MAC(k, s)$	消息 s 通过密钥 k 生成的消息认证码

我们定义对于多跳长路径上的节点，当 $|i-j|=t+1$ 时，CH_i 和 CH_j 为相关节点。当 $i-j=t+1$ 时，节点 CH_i 为节点 CH_j 的上行相关节点，节点 CH_j 为节点 CH_i 的下行相关节点。对于簇内节点，节点 CH_i 为节点 CN_i 的上行相关节点，节点 CN_i 为节点 CH_i 的下行相关节点。如图 3.2所示，在 $t=3$ 的簇与基站之间由 8 个簇头节点组成传输路径，其中 CN_3 为 CH_3 的下行相关节点，其中 CH_7 为 CH_3 的上行相关节点。

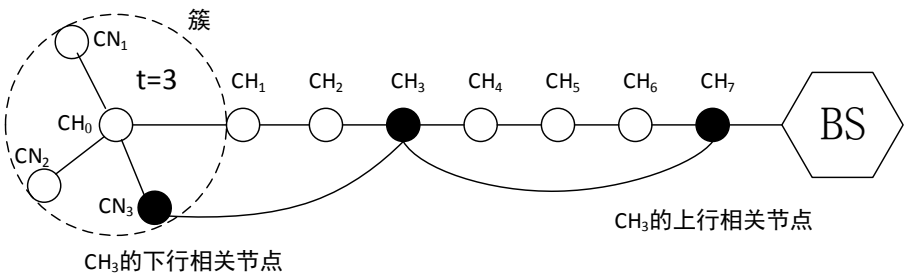

图 3.2 多节点联合数据认证中上下行相关节点

3.2.2 多节点联合数据认证方案

我们的多跳长路径上多节点联合数据认证方案主要包括初始化、数据报文发送、路径中过滤、基站认证四个阶段。

3.2.2.1 初始化

传感器节点被部署到目标区域时会被分配唯一的 ID 和足够的密钥材料，保证每个节点与基站之间都有唯一的共享密钥 AK_{si}。

在初始化阶段节点要获取上下行相关节点信息，在我们的多节点联合数据认证方案中，基站（Base Station,BS）会广播一个 HELLO 报文。簇头节点在收到 HELLO 报文以后，保存 $t+1$ 个 ID 信息作为上行节点，用自己的 ID 替换掉报文中距离自己 $t+1$ 跳的节点的 ID，其中被替换的 ID 信息作为其上行相关节点的 ID，然后将报文继续广播。簇头节点会把该 HELLO 报文中 $t+1$ 个 ID 分别发送给 $t+1$ 个簇节点，包括簇头节点，这样每个节点都获得了上行相关节点的 ID，并有了自己上行节点的 ID 信息。在接收 HELLO 报文以后每个簇头会节点记录下其到 BS 之间的跳数。

簇头节点会向 BS 发送一个 ACK 报文，其中包括 $t+1$ 个簇节点的 ID。当簇节点的上行相关节点受到该 ACK 报文以后，保存下 $t+1$ 个 ID 信息作为其下行相关节点，其中相距离自己 $t+1$ 跳的节点的 ID 作为其下行相关节点 ID，用自身的 ID 替换以后转发。BS 收到 ACK 报文以后就建立了一条从簇到 BS 的多跳长路径，而且各个节点都发现了其上下行相关节点的 ID，并有了自己下行节点的 ID 信息。

3.2.2.2 数据报文发送

簇节点监测到事件 E 以后，必须要 $t+1$ 个节点都发出报文才能确认监测到的事件，如果没有至少 $t+1$ 个节点的报文，则认为是无效事件。

簇节点 $CN_i(1 \le i \le t)$ 对于事件 E 首先使用其与 BS 之间的共享密钥 AK_{si} 计算消息认证码 $MAC(AK_{si}, E)$，称其为簇节点 MAC，并使用其与上行相关节点 CH_i 的共享密钥计算消息认证码 $MAC(AK_{CN_iCH_i}, E)$，称其为相关节点 MAC。簇头节点 CH_0 从 $t+1$ 个簇节点（包括簇头节点）收集到 $t+1$ 份报文后对数据进行整合后发送。如图 3.3所示，是一个事件 E 被感知和发送的过程。

在图 3.3的传输过程中，簇头节点 CH_0 收到簇节点的数据报文以后，对每个节点的簇节点 MAC 使用 XOR 运算进行压缩，缩小传输报文的大小，降低节点能量消耗，记作 $XMAC(E)$:

$$XMAC(E) = MAC(AK_{s1}, E) \oplus MAC(AK_{s2}, E) \oplus MAC(AK_{s3}, E) \oplus MAC(AK_{s0}, E) \tag{3.1}$$

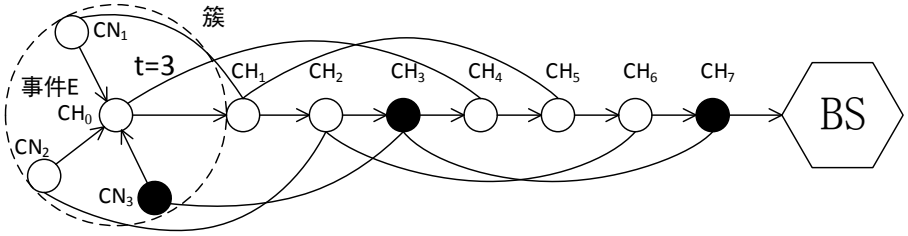

图 3.3　多节点联合数据认证中数据报文发送过程

簇的 ID 记作 C_i，簇头节点 CH_0 距离 BS 的跳数记作 h，则对于事件 E 簇头节点 CH_0 发给 BS 的报文 R 可以记作:

$$R = E, h_0, \{CH_0, CN_1, CN_2, CN_3\}, XMAC(E), \{MAC(AK_{CN_1CH_1}, E), MAC(AK_{CN_2CH_2}, E), MAC(AK_{CN_3CH_3}, E), MAC(AK_{CH_0CH_4}, E)\} \tag{3.2}$$

报文 R 中包含了簇节点的 ID: CH_0, CN_1, CN_2, CN_3，从而 BS 能够认证压缩的 $XMAC(E)$。

3.2.2.3　路径中过滤

当节点 CH_i 从下行节点收到报文 R 以后，首先用相邻节点共享密钥对进行认证。然后使用其上下行相关节点的共享密钥对 E 计算 MAC，并更新报文 R。对于图 3.3中的节点 CH_1，收到来自 CH_0 的报文后，使用与其下行相关节点 CN_1 之间的共享密钥对 E 计算消息认证码 $MAC(AK_{CH_1CN_1}, E)$，与报文 R 中的第 $(h_0 - h_i) - ((h_0 - h_i)/(t+1)) * (t+1) = 1$ 个相关节点 MAC，$MAC(AK_{CN_1CH_1}, E)$ 进行比较，如果不同则丢弃报文 R；如果相同，使用与其上行相关节点 CH_5 之间的共享密钥对 E 计算消息认证码 $MAC(AK_{CH_1CH_5}, E)$，并替代原报文 R 中的 $MAC(AK_{CN_1CH_1}, E)$，并将其转发给下一节点，更新后发送给节点 CH_2 的报文 R 为:

$$R = E, C_i, h_0, \{CH_0, CN_1, CN_2, CN_3\}, XMAC(E), \{MAC(AK_{CN_1CH_5}, E), MAC(AK_{CN_2CH_2}, E), MAC(AK_{CN_3CH_3}, E), MAC(AK_{CH_0CH_4}, E)\} \tag{3.3}$$

3.2.2.4　基站认证

当 BS 收到报文 R 后，使用 BS 与报文 R 节点 ID 列表中 $t+1$ 个簇节点之间的共享密钥计算 MAC，并用 XOR 运算计算这 $t+1$ 个 MAC 的值，与报文 R 中的 XMAC 比较，如果不同，则丢弃报文。如果相同，则对事件 E 作出响应。

3.2.3 安全性能分析

由于我们的方案使用了 XOR 运算压缩的 XMAC 保证了 BS 能检测出所有的错误报文，并且有相邻节点认证，下面我们对多节点联合认证的安全性能进行分析时，仅讨论路径中过滤的情况。

当一个节点被捕获时，攻击者就能获得一个能经过认证的 MAC 来欺骗它的上行相关节点。当传感器传输路径中被捕获的节点达到 t 个时，则攻击者可以用 t 个 MAC 组成的报文欺骗 t 个未被攻击的上行相关节点。但是我们的多节点联合数据认证机制需要 $t+1$ 个有效 MAC 才能通过认证，攻击者的入侵报文会被某个未被攻击的节点丢弃，因为它下行相关节点的 MAC 是无效的。因此我们的方案能保证当攻击者没有捕获超过 t 个节点的时候，入侵报文在被丢弃前仅能欺骗 t 个未被攻击节点。

通过上面的分析，我们的多节点联合数据认证机制的安全性是基于上下行相关节点间的认证的。我们下面对攻击者捕获了最多 t 个节点情况下的安全性进行分析，路径中过滤的攻击主要包括两个部分，簇内节点攻击和路径中节点攻击。

3.2.3.1 簇内节点攻击

当所有被攻击的 t 个节点都是簇内节点，没有路径中的节点被捕获时，不管簇头节点有没有被捕获，数据报文 R 中的 $t+1$ 个 MAC 中总会有一个是无效 MAC，从而被离簇头最近的 $t+1$ 个路径节点（如图 3.3中的节点 CH_1, CH_2, CH_3, CH_4）中的某个检测出来并丢弃。说明簇内节点攻击中，错误数据报文仅能欺骗最多 t 个未被攻击节点。

3.2.3.2 路径中节点攻击

我们讨论被攻击的 t 个节点在初始化阶段的 ACK 过程中能协作进行攻击的情况。我们讨论最坏情况，当被捕获的 t 个节点中包括了簇头节点 CH_0，且从 CH_0 到 BS 之间间隔 t 个未被捕获节点均匀分布，可以表示为：

$$\begin{aligned} &CH_0, \{CH_{1,1}, CH_{1,2}, \cdots, CH_{1,t}\}, N_1, \{CH_{2,1}, CH_{2,2}, \cdots, CH_{2,t}\}, \\ &N_2, \cdots, N_{t-1}, \{CH_{t,1}, CH_{t,2}, \cdots, CH_{t,t}\}, \cdots, BS \end{aligned} \tag{3.4}$$

其中 $CH_0, N_1, N_2, \cdots, N_{t-1}$ 是被捕获的 t 个节点，任意两个被捕获节点被 t 个未被捕获节点分隔。

在初始化阶段，簇头节点 CH_0 在 ACK 阶段通过发送一个伪造的 ID 信息组，$y, CH_0, N_1, N_2, \cdots, N_t$，其中 y 为任意伪造的节点信息，使得上下行相关关系确定过程中，未被捕获节点的下行相关节点都为被捕获节点。由于间隔 t 个未被捕获节点之后，是一个被捕获的节点，伪造的 ACK 不会因为 y 是伪造的节点信息而被

丢弃，而是重新将 $y, CH_0, N_1, N_2, \cdots, N_t$ 转发给上行节点。完成了 ACK 过程以后，所有的未被捕获节点的下行相关节点都是被捕获节点。

簇头节点 CH_0 发送的错误数据报文 R 可以表示为：

$$\begin{aligned} R = & E, C_i, h_0, \{CH_0, CN_1, \cdots, CN_t\}, XMAC(E), \{MAC(AK_{N_tCH_1}, E), \\ & MAC(AK_{N_{t-1}CH_2}, E), \cdots, MAC(AK_{CH_0CH_t}, E), MAC(AK_y, E)\} \end{aligned} \tag{3.5}$$

其中 $MAC(AK_y, E)$ 为伪造的 MAC。这个错误的数据报文能欺骗 t^2 个未被捕获节点，也就是攻击者捕获了最多 t 个节点时最坏的情况。

3.3 路径上节点关系的维护

我们的多节点联合数据认证机制是基于节点的上下行相关关系的，每个节点需要在初始化阶段发现其上行相关节点 ID 和下行相关节点 ID，这样才能通过节点间的共享对密钥计算 MAC，对数据报文进行认证。如果基站和簇头节点之间的多跳长路径是静态的，那只需要在初始化阶段进行一次上下行相关节点发现。但是由于无线传感网的特性，簇头节点在簇内是选举产生的，经常发生变化，还有传感器节点由于环境原因或者遭受攻击都有可能失效，导致路径的变化。因而需要对路径节点的上下行相关关系进行维护，以适应无线传感网的变化。下面从基站维护和节点自动维护两个情况介绍节点关系的维护。

3.3.1 基站维护

在相对稳定的无线传感网传输路径上，BS 会周期性广播信标消息，信标信息中捎带每个节点的 ID 信息。在初始化阶段，每个簇头节点都记录了自己到 BS 之间的跳数 h。当一个节点收到信标消息以后，如果 $h \geq t+1$，则检查该消息中 $t+1$ 个上行节点的 ID，如果 $h < t+1$，则检查该消息中 h 个上行节点的 ID。如果所有上行节点 ID 信息没有变化，路径中该节点的上行节点没有变化。如果有变化则在发送给 BS 的信标消息中附带节点变化消息，BS 重新发送 HELLO 报文，进行上下行相关节点发现的过程。

3.3.2 节点自动维护

在基站维护的过程中，如果信标消息的广播周期较短，会造成大量的数据传输，消耗传感器节点的能量；如果信标消息的广播周期较长，那么部分节点失效或被攻击就会造成大量的数据报文被丢弃，所以我们需要节点自动维护的机制，修复路径中的节点上下行相关关系。

我们的节点自动维护机制是基于 GPSR 协议[51] 中的右手准则的。我们假设每个节点都自动相邻节点的相对位置。如图 3.4所示是一个节点自动维护的过程，当

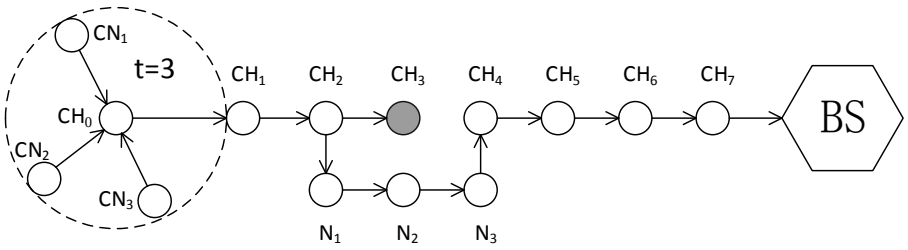

图 3.4　节点自动维护上下行相关关系的过程

节点 CH_2 检测到 CH_3 失效以后，给它的逆时针方向的第一个相邻节点 N_1 发送一个修复消息，消息中包括了 CH_2 的 t 个上行节点的 ID，$\{CH_4, CH_5, CH_6\}$，不包括 CH_3。N_1，N_2 按照初始化阶段的规则进行转发，当 N_3 收到修复消息以后，发现消息中有 CH_4 的 ID，是它的相邻节点，这样就发现了一条替代路径。N_3 将消息发送给 CH_4 以后，CH_4 将上行节点 ID，$\{CH_4, CH_5, CH_6, CH_7\}$ 捎带在消息中转发给 N_3，同初始化阶段的 HELLO 报文。完成这些过程以后，新路径上的节点就建立上下行相关关系，也就是修复了这条长路径。

3.4　本章小结

本章提出了无线传感网中数据认证模型，针对相关攻击模型，提出了多跳长路径上多节点联合的数据认证方案。设计实现了多节点联合数据认证协议，并对其安全性能进行了分析。为了维持多节点联合数据认证机制的稳定性，设计了路径上相关节点关系维护的机制。

第四章　数据认证方案优化

本章讨论对无线传感网多节点联合数据认证机制进行优化，利用多种方案提升数据认证机制的检测效率，降低节点能量消耗。4.1 节介绍无线传感网节点失效问题，提出了多路径抗节点失效的机制。4.2 节设计动态步长的多节点联合数据认证机制。

4.1　多路径抗节点失效机制

由于无线传感网部署的环境恶劣，且容易受到攻击，使得节点的稳定性很难保证，整个网络的拓扑结构很容易发生变化。在 3.3 节中，我们讨论了在拓扑结构变化频率不大的情况下，通过传感器网络自身的维护机制，维护路径节点的上下行相关关系，适应无线传感网拓扑结构的变化。但是在节点失效或者被攻击比较频繁时，无线传感器网络结构变化很快，而原有的维护方案是通过重建路径来完成的，因而通信开销较大，造成大量节点能量损耗。

为了适应节点失效较多，传感网拓扑结构变化较大的情况，我们提出了多路径抗节点失效的方案。通过在初始化阶段预定义若干条不相交路径，对每个节点失效的情况预定义编织路径。但在一个传输阶段，只有一条路径被使用，并进行数据认证。当路径受到攻击，或者节点失效时，使用备用的不相交路径或者编织路径。

在多路径抗节点失效方案中，我们使用了单向 hash 链来分配密钥，提升了网络的安全性能，并节省了节点存储密钥的开销。每个节点使用单向 hash 函数从它的上行相关节点的密钥生成密钥，具体的密钥分配方案将在第五章进行详细描述。

4.1.1　设计实现

在多路径抗节点失效机制中，节点上下行相关关系不是研究重点，不再详细介绍，沿用第三章中多跳长路径多节点联合数据认证的方案。我们在多路径抗节点失效机制中，使用了单向 hash 链来分配密钥，能更好地保证认证机制的安全性，降低节点保存密钥的存储开销。我们的路径抗节点失效机制包括了初始化和密钥分配、数据报文发送、路径中过滤、基站认证、路径选择五个阶段。

4.1.1.1　初始化和密钥分配

传感器节点被部署到目标监测区域之后，基站会给每个节点生成一个共享密钥, 这是每个节点与基站之间的共享密钥 AK_{si}。然后每个簇通过预定的选举机制选举一个簇头节点，BS 通过广播路由请求完成传感器网络的路由发现。

在多节点联合数据认证方案中，我们使用 HELLO 报文和 ACK 报文来完成路径发现和上下行相关关系的建立，在簇与 BS 之间建立一条多跳长路径。在多路径

抗节点失效方案中，我们在初始化建立多条不相交长路径以及多条编织路径。虽然有多条路径，在我们的方案中，一次传输过程只会使用一条主路径，其他路径作为网络被攻击时的备选路径。

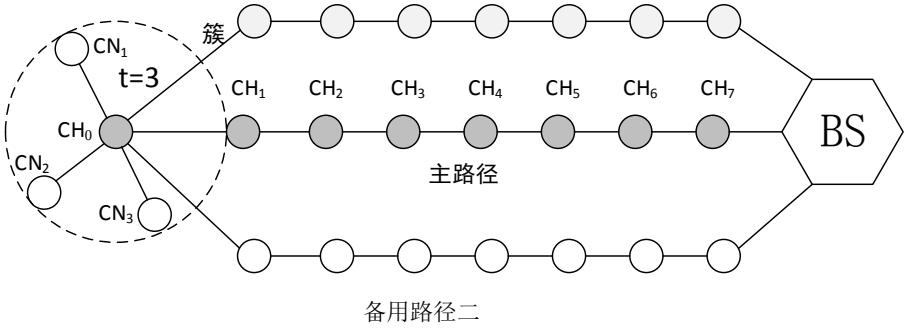

图 4.1　多路径抗节点失效机制中的不相交路径

如图 4.1所示，簇与 BS 之间建立了 3 条不相交路径。不相交路径通过以下步骤建立:

- 建立一条簇头与 BS 之间的主路径。
- 建立一条与主路径不相交的，且跳数最短的路径，作为备用路径一。
- 建立一条与主路径以及备用路径一不相交的，且跳数最短的路径，作为备用路径二。

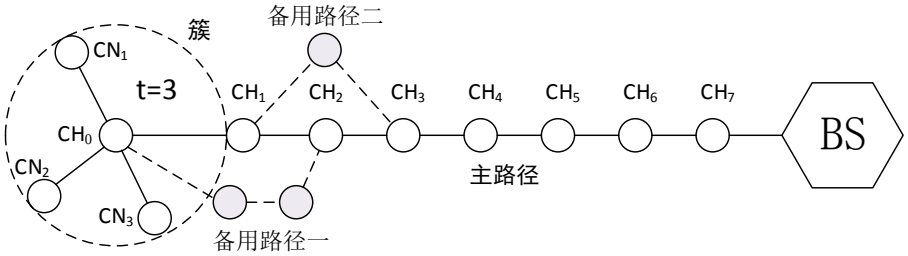

图 4.2　多路径抗节点失效机制中的编织路径

如图 4.2所示，路径上的节点完成备用编织路径的建立。编织路径通过以下步骤建立:

- 建立一条簇头与 BS 之间的主路径。
- 对主路径上的每个节点，寻找不包括该节点的簇与 BS 之间的最短路径。在图 4.2 中，第一条编织路径就是不包括节点 CH_1，从节点 CH_0 到节点 CH_2 之间的编织路径。相似的，第二条编织路径是不包括节点 CH_2 的从节点 CH_1 到节点 CH_3 的编织路径。

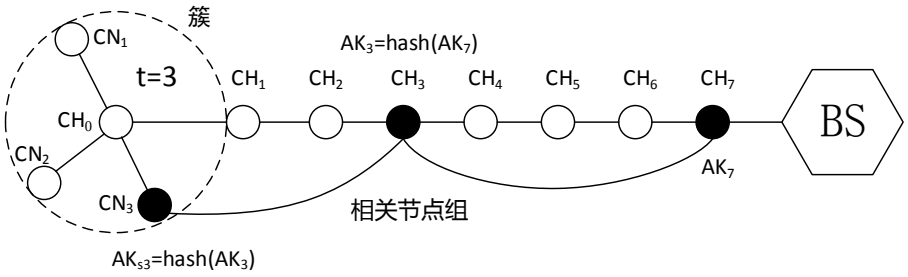

图 4.3　多路径抗节点失效机制的密钥分配

在我们的多路径抗节点失效方案中，我们使用了单向 hash 链来进行密钥分配，如图 4.3所示。BS 给每个上下行相关节点组生成一个 AK，下行节点使用单向 hash 函数 H 从上行节点的密钥得到自己的密钥。图 4.3中所示，节点组 $\{CN_3,CH_3,CH_7\}$，距离 BS 最近的节点 CH_7 从 BS 获取 BS 生成的密钥 AK_7，它的下行节点 CH_3 通过单向 hash 函数获取密钥 $AK_3 = H(AK_7)$。类似的，节点 CN_3 获取密钥 $AK_{s3} = H(AK_3)$。通过这样的密钥分配，每个节点存储密钥的空间开销变小了，同时节点被攻击时丢失的密钥信息变少了。

4.1.1.2　数据报文发送

同多节点联合数据认证一样，簇节点监测到事件 E 以后，必须要 $t+1$ 个节点都发出报文才能确认监测到的事件，如果没有至少 $t+1$ 个节点的报文，则认为是无效事件。簇节点 MAC 压缩后记作 $XMAC(E)$:

$$XMAC(E) = MAC(AK_{s1}, E) \oplus MAC(AK_{s2}, E) \oplus MAC(AK_{s3}, E) \oplus MAC(AK_{s0}, E) \tag{4.1}$$

在多路径抗节点失效方案中，我们使用簇序号 C_i 来标记簇信息，代替原方案中的簇 ID 集，减小了传输开销。在簇头节点 CH_0 生成的报文 R 可以记作:

$$\begin{aligned} R = & E, C_i, h_0, XMAC(E), \{MAC(AK_{s1}, E), \\ & MAC(AK_{s2}, E), MAC(AK_{s3}, E), MAC(AK_0, E)\} \end{aligned} \tag{4.2}$$

4.1.1.3　路径中过滤

当节点 CH_i 从下行节点收到报文 R 以后，首先用相邻节点共享密钥对进行认证。然后使用其上下行相关节点的共享密钥对 E 计算 MAC，并更新报文 R。对于图 4.3中的节点 CH_3，收到来自 CH_2 的报文后，首先使用单向 hash 函数计算得出其下行相关节点的密钥 $AK_{s3} = H(AK_3)$。用 AK_{s3} 对事件 E 计算消息认证码 $MAC(AK_{s3}, E)$, 与报文 R 中的第 $(h_0 - h_i) - ((h_0 - h_i)/(t+1)) * (t+1) = 3$ 个相关节点 MAC，也就是 $MAC(AK_{s3}, E)$ 进行比较，如果不同则丢弃报文 R；如果相同

则使用密钥 AK_3 对事件 E 计算消息认证码 $MAC(AK_3, E)$，并替代原报文 R 中的 $MAC(AK_{s3}, E)$，将其转发给下一节点 CH_4，更新后发送的报文 R 为：

$$R = E, C_i, h_0, XMAC(E), \{MAC(AK_1, E), MAC(AK_2, E), MAC(AK_3, E), MAC(AK_0, E)\} \tag{4.3}$$

4.1.1.4 基站认证

当 BS 收到报文 R 后，首先获取报文中的簇序号 C_i，使用 BS 与簇 C_i 的节点 ID 列表中 $t+1$ 个簇节点之间的共享密钥计算 MAC，并用 XOR 运算计算这 $t+1$ 个 MAC 的值，与报文 R 中的 XMAC 比较，如果不同，则丢弃报文。如果相同，则对事件 E 作出响应。

4.1.1.5 路径选择

当路径中节点受到攻击时，BS 会收集到相应的信息，通过妥协节点检测技术[26]，BS 能确定哪些路径被攻击，妥协节点检测技术不是本文的重点，而是专注于妥协节点检测技术在数据认证中的应用。当 BS 确定了受攻击的路径以后，切换到未被攻击的备用路径。

同多节点联合数据认证机制中的节点关系维护相比，我们的多路径抗节点失效是通过预先定义备用路径，是一个应对节点攻击的前瞻性安全机制。而多节点联合数据认证机制中的节点维护是一种即时修复的方法，在节点失效或被攻击频率较高时，会造成传感器网络的传输路径不稳定，受攻击的影响更严重，还会造成大量的节点能量消耗。

4.1.2 安全性能分析

4.2 动态步长多节点联合数据认证

在无线传感网的多跳长路径传输中应用我们的多节点联合数据认证机制，能有效保证数据的安全传输，但是数据报文中附带了大量的 MAC 信息，加重了传感器节点的能量消耗。因此我们提出了一个动态步长的多节点联合数据认证，在传感器网络节点受攻击影响较小的时候，压缩所传输的报文，降低节点能量消耗。

4.2.1 动态步长多节点联合数据认证机制设计

动态步长多节点联合数据认证是在多节点联合数据认证的基础上，对其进行改进，使得通信开销得到优化。在 4.1 节中，我们讨论了在传感网拓扑结构变化较大时，使用多路径抗节点失效的机制来保证传感网传输稳定性。对于一条簇到 BS 之间的传输路径，如果路径比较稳定，则可以通过压缩数据报文的方式来降低传输开销。在我们提出的动态步长多节点联合数据认证机制中，是通过动态调整多节点联合认证中的节点组间隔步长来实现的。

在多节点联合数据认证中，根据步长的动态调整，对数据报文中的相关节点MAC进行相应程度的压缩处理，在路径传输的安全性与路径传输通信开销之间进行平衡，在保证路径安全性的情况下，降低通信开销。如图4.4所示，是一个簇节点数为4，步长为3的多节点联合数据认证。

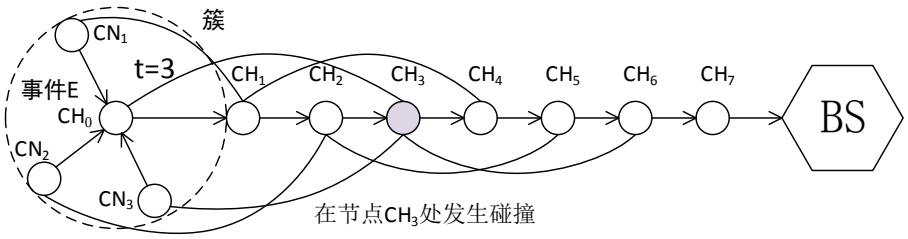

图4.4　动态步长多节点联合数据认证

4.2.1.1　面向动态步长多节点联合数据认证的密钥分配

在动态步长多节点联合数据认证中，我们也使用单向hash链来完成认证密钥的分配。不同于图4.3中所示的密钥分配，在步长动态变化时，上下行相关节点组会发生碰撞，也就是不同的簇节点在同一个上下行相关节点组当中。如图4.4中，节点 CH_0 和节点 CN_3 在同一个上下行相关节点组中，上行相关节点都是节点 CH_3。

对于上下行相关节点的碰撞，我们通过对簇内节点添加虚拟的上下行顺序来解决。在如图4.4的传输路径上，将4个簇节点的虚拟上下行关系设为 $\{CN_3, CN_2, CN_1, CH_0\}$，也即步长为3时，节点 CH_0 是节点 CN_3 的上行相关节点。

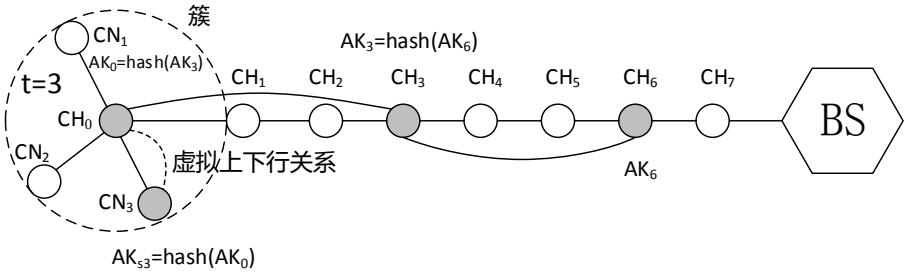

图4.5　面向动态步长多节点联合数据认证的密钥分配

如图4.5所示，即为图4.4所示的动态步长多节点联合数据认证情景的密钥传输示例。节点 CH_0 和节点 CN_3 都是簇节点，但是在同一个上下行相关节点组内，所以在节点 CH_0 和节点 CN_3 之间虚拟上下行相关关系，节点 CN_3 的密钥从节点 CH_0 的密钥计算而来，$AK_{s3} = H(AK_0)$。

4.2.1.2 报文数据压缩传输

使用单向 hash 链的密钥分配方案，给虚拟上下行相关节点分配了密钥以后，如图 4.4的动态步长多节点联合数据认证中，节点 CH_0 对簇节点数据进行整合之后的报文 R 可以表示为:

$$\begin{aligned} R = & E, C_i, h_0, XMAC(E), \{MAC(AK_{s1}, E), MAC(AK_{s2}, E), \\ & MAC(AK_0, E) \oplus MAC(AK_{s3}, E)\} \end{aligned} \tag{4.4}$$

其中 $MAC(AK_0, E) \oplus MAC(AK_{s3}, E)$ 为节点 CH_0 和节点 CN_3 的簇节点 MAC 使用 XOR 运算压缩后的结果。

我们用 p 表示步长，对于 $h - h_0 \leq p$ 的节点，在收到报文后，首先计算其下行相关节点的密钥。在图 4.4的示例中，节点 CH_3 收到报文 R 以后，首先计算下行相关节点的密钥 $AK_0 = H(AK_3)$。对事件 E 计算消息认证码 $MAC(AK_0, E)$，并与报文 R 中第 $(h_0 - h_i) - ((h_0 - h_i)/p) * p = 3$ 个 MAC 进行比较，如果相同则用 $MAC(AK_3, E)$ 替换之。如果不同则计算间隔一跳的下行相关节点的密钥 $AK_{s3} = H(AK_0)$，对事件 E 计算消息认证码 $MAC(AK_{s3}, E)$，并与 $MAC(AK_0, E)$ 进行 XOR 运算，$MAC(AK_0, E) \oplus MAC(AK_{s3}, E)$ 与报文 R 中第 3 个 MAC 进行比较，如果相同则用 $MAC(AK_3, E)$ 替换之。如果都不同，则表示是错误数据报文，但是不同于前面提出的方案，我们不将其直接丢弃，而是将 $XMAC(E)$ 置为全 0。对于 $h - h_0 > p$ 的节点，同前述方案一样，只进行一次 MAC 验证。在经过路径节点的验证后，节点将报文继续转发给上行节点。

4.2.1.3 动态步长调整机制

在 BS 收到报文以后，会对报文中的 $XMAC(E)$ 进行验证。如果 $XMAC(E)$ 为全 0，则说明有错误数据报文在路径中被检测出来，这样说明传输路径的安全水平较低，则 BS 提高路径的传输步长 p，这样能提升检测出错误数据报文的概率。如果 BS 连续收到若干个正常，达到一个阈值以后，我们认为路径是安全的，则 BS 降低路径的传输步长 p，减小报文的大小，节约节点的传输能量。

4.2.2 安全性能分析

在 BS 收到报文以后，会对报文中的 $XMAC(E)$ 进行验证。如果 $XMAC(E)$ 为全 0，则说明有错误数据报文在路径中被检测出来，这样说明传输路径的安全水平较低，则 BS 提高路径的传输步长 p，这样能提升检测出错误数据报文的概率。如果 BS 连续收到若干个正常，达到一个阈值以后，我们认为路径是安全的，则 BS 降低路径的传输步长 p，减小报文的大小，节约节点的传输能量。

4.3 本章小结

本章针对多节点联合数据认证机制中，节点失效或者受攻击对路径中的节点相关关系的影响，我们提出了多路径抗节点失效的机制，设计实现了相关算法。为了优化多节点联合数据认证的通信开销，我们设计实现了动态步长多节点联合数据认证机制。对两个优化方案，都进行了相关安全性能的分析。

第五章　密钥分配与消息认证码的实现

本章首先讨论数据认证机制中的密钥分配方案，以及认证过程中使用的消息认证码的实现。在 6.1 中基于单向 hash 链的思想，设计实现了面向数据认证机制的密钥分配方案。在 6.2 节中设计了适应无线传感网认证需求的 MAC 码。

5.1　面向数据认证的密钥分配方案

在本节中我们讨论研究单向 hash 链的性质，并将其应用到密钥分配中，设计基于单向 hash 链的的密钥分配机制。

我们对本章中出现的符号的定义如表 5.1所示：

表 5.1　相关符号定义

符号	描述
$\|\mathbf{K}\|$	K 的长度
$< i >$	表示将整数 i 用 b 位二进制表示
$\mathbf{A}\|\|\mathbf{B}$	将字符串 A 与 B 进行串联
$E_K(M)$	对消息 M 使用密钥 K 进行分组密码置换
$A \ll i$	将字符串 A 左移 i 位，右边填 0
$\mathbf{A} \oplus \mathbf{B}$	将字符串 A 与字符串 B 按位异或

5.1.1　单向 hash 链

本节中的密钥分配方案是基于单向 hash 函数的特性来保证无线传感网中的密钥安全的。通过使用单向 hash 链生成密钥池，能保证在密钥部署时的安全需求，还可以通过建立节点间的通信密钥有效防止攻击者通过身份冒充对节点间通信攻击。我们对单向 hash 链的定义以及本文方案中选取的单向 hash 函数进行说明。

5.1.1.1　单向 hash 链的定义

hash 函数是通过压缩映射将任意长度的消息压缩为一个固定长度的摘要的函数。对一个任意大小的消息，hash 函数能输出一个给定长度的散列值，一个 hash 函数 H 可以表示为 $H : \{0,1\}^* \rightarrow \{0,1\}^i$，其中 i 为输出的散列值的长度。满足下列条件的 hash 函数称作单向 hash 函数：

1. hash 函数 $H(x)$ 的输入 x 为任意长度
2. hash 函数 $H(x)$ 的输出为给定长度
3. hash 函数 $H(x)$ 的计算方便，也就是对于一个给定的输入 x，hash 值输入 $y = H(x)$ 的计算是方便的

4. 对于给定的 hash 值 $y = H(x)$，找出 x 在计算上是不可行的
5. 对于给定的输入 x，找出另一个消息 $x' \neq x$，满足 $H(x') = H(x)$ 在计算上是不可行的
6. 找出任意两个消息 x 和 y，满足 $H(x) = H(y)$ 在计算上是不可行的，也就是 $H(x)$ 具有抗碰撞性

通过对一个字符串种子 K_0 使用 hash 函数进行迭代，形成一个字符串链，称作 hash 链。如果使用的 hash 函数是单向 hash 函数，则 hash 链称作单向 hash 链，链中的字符串具有不可逆计算的特性。例如对于单向 hash 函数 $H(x)$，通过 $K_{i+1} = H(K_i), 0 \leq i < n$ 迭代生成的单向链 $K_0, K_1, \cdots, K_n$ 就是一个单向 hash 链。

5.1.1.2 单向 hash 函数的选择

典型的单向 hash 函数有 SHA-1 或者 RC5 等，可以通过将算法简化，使之适应无线传感网的需求。在 SHA-1 方案中，输入是最大 2^{64}bit 的消息，输出是固定 160bit 的消息摘要。我们的方案中将 SHA-1 的输出改进为 64bit（也就是我们的数据认证机制中的密钥长度），作为我们的单向 hash 链生成函数。

改进后的基于 SHA-1 的单向 hash 函数算法可以表示为算法 5.1：

5.1.2 基于单向 hash 链的密钥分配

在第四章中已经简要介绍了多路径抗节点失效中的密钥分配，在这节中对我们的基于单向 hash 链的密钥分配方案进行详细论述。主要分为四个部分，分别是密钥预分配、共享密钥发现、路径密钥发现和密钥分配的扩展性。

5.1.2.1 密钥预分配

在传感器节点被部署到目标监测区域之前，每个节点预先装配了足够了密钥材料，包括节点的 ID 信息，以及单向 hash 函数 H（在上节中已经详细论述）。基站基于单向 hash 函数 H 生成预分配密钥池：

$$K_{i,j} = H^1(K_{i-1,j}) = \cdots = H^i(K_{0,j}) \quad (i = 1, 2, \cdots, n) \tag{5.1}$$

其中 j 为单向 hash 链的序号，n 代表单条 hash 链中的密钥个数，$H^i(K_{0,j})$ 代表密钥 $K_{0,j}$ 经过 i 次 hash 函数的迭代。将每条 hash 链上的密钥反序排列，得到的 hash 链序列为 $K_{i,j}, \cdots, K_{1,j}, K_{0,j}$。基站共生成 m 条单向 hash 链作为密钥池，则整个预分配密钥池可以如表 5.2表示：

部署节点时，预分配的密钥从密钥池中取出，分配给节点。最先被分配的密钥是密钥池中靠前的密钥集合，也即密钥集合 $K_{n,1}, K_{n,2}, K_{n,3}, \cdots, K_{n,m}$ 最先被分配，后续部署到无线传感网中的节点依次从预分配密钥池中取出密钥集合进行分配。通过这样的预分配方式，不同阶段部署的节点使用的不同的密钥集合中的密钥，

算法 5.1 单向 hash 函数

已知： 输入消息 $x, |x| = 64$

求： 消息摘要

1: $M \leftarrow x||1||0^r|| < |x| >$，将消息 x 填充为 512 位
2: 将消息 M 分隔为 $w_0, w_1, \cdots, w_{15}$
3: $A \leftarrow h_0 = 0x67452301$
4: $B \leftarrow h_1 = 0xEFCDAB89$
5: $C \leftarrow h_2 = 0x98BADCFE$
6: $D \leftarrow h_3 = 0x10325476$
7: $E \leftarrow h_4 = 0xC3D2E1F0$
8: **for** $i = 16$ to 79 **do**
9: $\quad w_i \leftarrow (w_{i-3} \oplus w_{i-8} \oplus w_{i-14} \oplus w_{i-16}) \lll 1$
10: **end for**
11: **for** $i = 0$ to 79 **do**
12: $\quad temp \leftarrow A \lll 5 + f(B, C, D) + E + w_i + K_i$
13: $\quad E \leftarrow D$
14: $\quad D \leftarrow C$
15: $\quad C \leftarrow B \lll 30$
16: $\quad B \leftarrow A$
17: $\quad A \leftarrow temp$
18: **end for**
19: $A \leftarrow h_0 + A$
20: $C \leftarrow h_2 + C$
21: **return** $A||C$

表 5.2　预分配密钥池

$K_{n,1}$	–	$K_{n-1,1}$	–	$\cdots$	–	$K_{2,1}$	–	$K_{1,1}$	–	$K_{0,1}$
$K_{n,2}$	–	$K_{n-1,2}$	–	$\cdots$	–	$K_{2,2}$	–	$K_{1,2}$	–	$K_{0,2}$
$K_{n,3}$	–	$K_{n-1,3}$	–	$\cdots$	–	$K_{2,3}$	–	$K_{1,3}$	–	$K_{0,3}$
					$\cdots$					
$K_{n,m}$	–	$K_{n-1,m}$	–	$\cdots$	–	$K_{2,m}$	–	$K_{1,m}$	–	$K_{0,m}$

限制了被攻击节点泄露的密钥对整个无线传感网的影响，攻击者不能对已经建立的安全通信链路进行攻击。由于密钥池是一系列的反序单向 hash 链，单向 hash 链的特性决定了泄露的密钥无法推导出密钥池中的密钥，因此攻击者无法进行节点冒充攻击。

5.1.2.2 共享密钥发现

节点被部署到目标区域以后，利用相应的分簇算法，对网络结构进行组织，选举每个簇的簇头。在簇的建立完成以后，节点之间开始共享密钥发现的过程。

在第二章中，我们已经讨论过密钥预分配方案的缺点，当节点被攻击而成为妥协节点时，节点中的预分配密钥都会被攻击者获得，可以对无线传感网的通信进行攻击。因此我们需要在节点之间发现相同的预分配密钥，并生成节点对之间的共享密钥。建立共享密钥的过程如图 5.1所示：

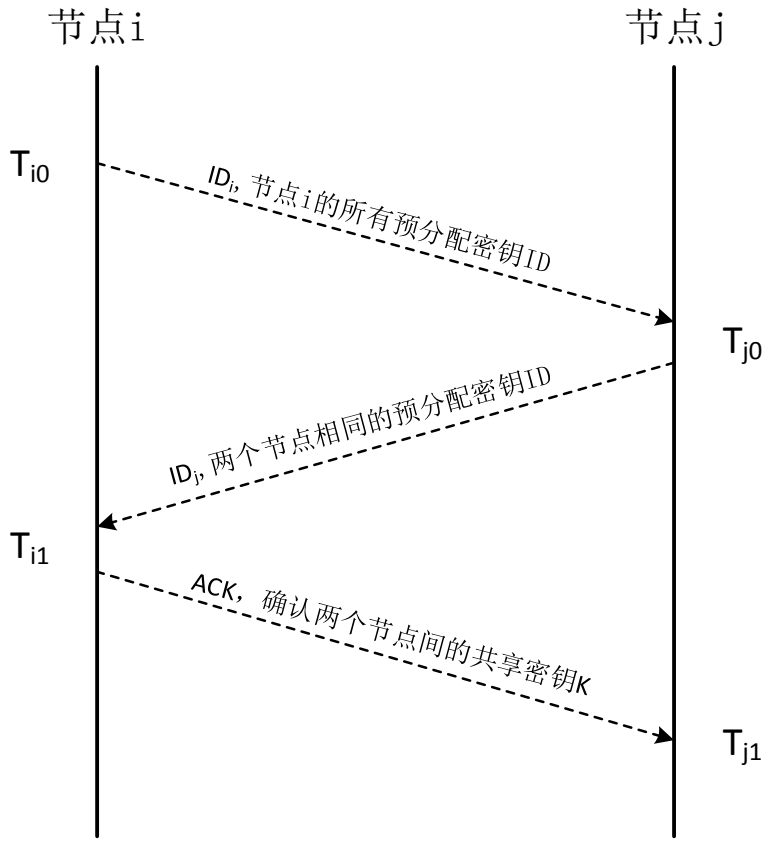

图 5.1 共享密钥建立过程

节点部署到目标区域到网络进行初始化阶段的时间内，假设网络是不受攻击的影响，节点不会被攻击或者被捕获，能安全进行信息的交换。相邻的节点 i 与节点 j 之间发现共享密钥的过程是先由节点 i 将其节点 ID 以及所有预分配密钥的 ID 一起广播。节点 j 收到邻居节点的 ID 以及预分配密钥 ID 以后，在自己的预分配密钥中进行寻找，如果有相同的预分配密钥 K_x，则将自己的 ID 以及相同的预分

配密钥 ID 一起发送给节点 i。节点 i 在受到节点 j 的节点 ID 和预分配密钥 ID 后，利用预装配的单向 hash 函数 H 进行共享密钥的计算：

$$K = H(< ID_i > \| < ID_j > \| K_x) \tag{5.2}$$

通过将两个节点的节点 ID 与相同的预分配密钥 K_x 进行拼接以后的单向 hash 函数计算结果作为两个节点的新共享密钥，这样增强了相邻节点间通信链路的安全性，两个节点的预分配密钥即使因为其他节点被捕获而泄露，攻击者也无法计算出共享密钥 K，对节点间的通信进行攻击。

5.1.2.3 路径密钥发现

在我们的多跳长路径多节点联合数据认证机制中，通过在路径中发现上下行节点相关关系，对路径中传输的数据报文进行认证。对于路径密钥，我们使用单向 hash 函数来进行分配，基站为每个上下行相关节点组生成一个单向 hash 链作为密钥池，并将这个 hash 链的密钥种子发送给该相关节点组中距离基站最近的节点。

然后在上下行相关节点组中，每个节点依次使用上行相关节点的路径密钥使用单向 hash 函数计算自己的路径密钥，$AK_i = H(AK_{i+t})$。通过这样的密钥分配方案，使用了预装配的密钥材料，节约了存储空间的开销，同时单个节点被攻击而被捕获时，丢失的密钥信息较少。

5.1.2.4 密钥更新

无线传感网中，有两种情况需要进行密钥更新：由于无线传感器节点被部署在无人值守区域，容易受到攻击或物理破坏，导致节点失效或者被捕获，攻击者能获取其中的密钥，继而对整个无线传感网进行攻击，所以需要对密钥进行更新；由于无线传感器节点的能量有限，在工作一段时间之后，超过传感器节点的使用期限，需要将失效节点从无线传感网中移除，并对网络中的密钥进行更新。密钥更新包括两类：

事件触发的更新：无线传感网中有节点能量耗尽而失效时，节点被攻击破坏而失效时都会触发传感网进行密钥的更新。当有新的节点加入传感网，需要同原有节点建立通信链路时也会触发密钥更新。

时间触发的更新：对于基站工作的时间轴，认为一个时间间隔后部分节点的能量可能会耗尽，从而触发密钥更新。新的节点部署到位后，通过共享密钥发现，可以对新加入的节点进行身份认证，保证整个传感网密钥的安全。

5.2 消息认证码的实现

本节讨论适应无线传感网认证需求的消息认证码（Message Authentication code，MAC），首先介绍了集中常见的 MAC，然后提出了我们方案中 MAC 的设计。

5.2.1 消息认证码

消息认证码是无线传感网中最常见的防数据篡改的工具，利用两个节点之间的共享密钥，对发送的消息进行认证，可以检查消息有没有在传输的过程被篡改。

利用消息认证码通过如下过程来进行认证：发送消息的节点使用共享密钥 K 对消息 M 计算相应的消息认证码 $MAC(K,M)$，将 $MAC(K,M)$ 附加在消息报文中发送；当节点接受到该消息报文后，也使用共享密钥 K 对消息 M 计算相应的消息认证码，并与报文中附带的 $MAC(K,M)$ 进行比较，如果相同则说明消息在传输过程中没有被篡改，否则就认为消息已经被篡改。

消息认证码的实现主要可以分为两类：基于 hash 函数的 MAC 和基于分组密码的 MAC。

5.2.1.1 基于 hash 函数的 MAC

基于 hash 函数的 MAC 一般将共享密钥作为 hash 函数的一个参数，典型的基于 hash 函数的 MAC 有 HMAC[52]。

HMAC 的计算可以表示为 $HMAC(K,M) = H((K \oplus opad)||H((K \oplus ipad)||M))$，其算法如算法 5.2所示：

算法 5.2 基于带密钥的 hash 函数的消息认证码 HMAC

已知： 输入消息 **M**，认证密钥 **K**，
hash 函数 H，数据块字长 **B**

求： 消息认证码 HMAC

1: **if** $|\mathbf{K}| > \mathbf{B}$ **then**
2: $K \leftarrow H(K)$
3: **end if**
4: $\mathbf{K} \leftarrow \mathbf{K}||(0x00)^{B-|K|}$
5: $ipad \leftarrow (0x36)^{\mathbf{B}}$
6: $\mathbf{S} \leftarrow H(\mathbf{K} \oplus ipad)||\mathbf{M})$
7: $opad \leftarrow (0x5c)^{\mathbf{B}}$
8: $HMAC \leftarrow H(\mathbf{K} \oplus opad)||\mathbf{S})$

5.2.1.2 基于分组密码的 MAC

基于分组密码的 MAC 最早的方案是 CBC-MAC，作者又在 CBC-MAC 方案的基础上增加了计算的并行性，提出了 XOR-MAC 方案 [53]。XOR-MAC 可以分为随机异或 MAC 方案（XMACR）和基于计数器异或方案（XMACC）。

随机异或 MAC 方案（XMACR）的算法和基于计数器异或方案（XMACC）的算法分别如算法 5.3和算法 5.4所示：

算法 5.3 XMACR

已知: 输入消息 **M**，认证密钥 **K**，
分组密码 $E : k \times \{0,1\}^n \rightarrow \{0,1\}^n$

求: 消息认证码

$M \leftarrow M||1||0^t$，将 M 填充为 $n-b-1$ 的整数倍
if $|M| \leq (n-b-1)2^b$ **then**
    将消息 M 分隔为 $M_1, M_2, \cdots, M_m$
end if
$r \leftarrow \{0,1\}^{n-1}$
$y_0 \leftarrow E_K(0||r)$
for $i = 1$ to m **do**
    $y_i \leftarrow y_{i-1} \oplus E_K(1|| < i > ||M_i)$
end for
return r, y_m

算法 5.4 XMACC

已知: 输入消息 **M**，认证密钥 **K**，
分组密码 $E : k \times \{0,1\}^n \rightarrow \{0,1\}^n$

求: 消息认证码

$M \leftarrow M||1||0^t$，将 M 填充为 $n-b-1$ 的整数倍
if $|M| \leq (n-b-1)2^b$ **then**
    将消息 M 分隔为 $M_1, M_2, \cdots, M_m$
end if
$counter \leftarrow counter + 1$
$y_0 \leftarrow E_K(0|| < counter >)$
for $i = 1$ to m **do**
    $y_i \leftarrow y_{i-1} \oplus E_K(1|| < i > ||M_i)$
end for
return $counter, y_m$

5.2.2 MAC 设计实现

使用 XOR-MAC 等方案虽然增加了并行性，对计算长消息的 MAC 有较好的效率，但是这些算法使用了密钥扩展，多次调用伪随机函数，导致计算短消息时开销过大。由于 CBC-MAC 等方案对长度扩展攻击的防御不够好，我们在其基础上进行了改进，提出了 SCBC-MAC 方案。SCBC 方案的计算过程如图 5.2所示：

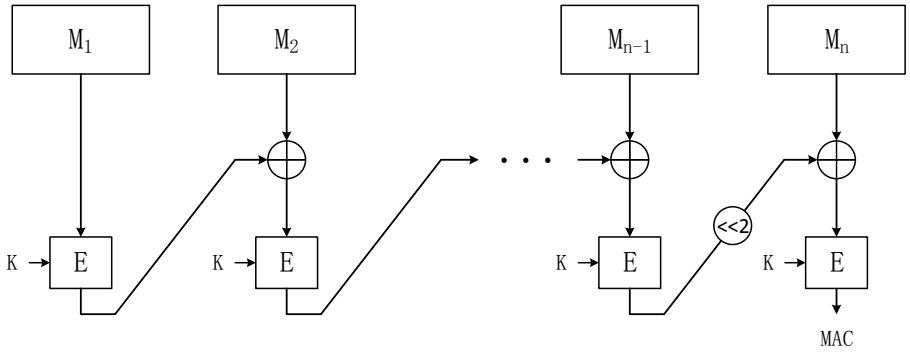

图 5.2　SCBC-MAC 方案

通过对消息 M 进行填充 $M||1||0^t$，使得消息 M 可以表示为 $M = (M_1||M_2||\cdots||M_n) \in (\{0,1\}^l)^n, l \geq 2$。我们的 SCBC-MAC 方案计算 MAC 可以表示如下：

$$SCBC_K(M) = E_K(E_K(\cdots E_K(E_K(M_1) \oplus M_2)\cdots) \ll 2 \oplus M_n) \tag{5.3}$$

我们通过在最后一个消息块进行 XOR 运算之前，增加了一个左移 2 位的操作，这样简单的调整有效阻止了长度扩展攻击。SCBC-MAC 的算法可以表示为算法 5.5：

算法 5.5 SCBC-MAC

已知： 输入消息 **M**，认证密钥 **K**，
分组密码 $E : k \times \{0,1\}^n \rightarrow \{0,1\}^n$

求： 消息认证码

1: $M \leftarrow M||1||0^t$，将 M 填充为 l 的整数倍
2: **if** $l \geq 2$ **then**
3: 　　将消息 M 分隔为 $M_1, M_2, \cdots, M_n$
4: **end if**
5: $y_0 \leftarrow 0^l$
6: **for** $i = 1$ to $n - 1$ **do**
7: 　　$y_i \leftarrow y_{i-1} \oplus E_K(M_i)$
8: **end for**
9: $y_n \leftarrow E_K(y_{n-1} \ll 2 \oplus E_K(M_n))$
10: **return** y_n

5.3　本章小结

本章主要完成了密钥分配方案和消息认证码的设计。针对数据认证中的密钥分配需求，我们设计实现了基于单向 hash 链的密钥分配方案。对于报文传输阶段

中使用的消息认证码，我们介绍了多种 MAC 方案，并针对我们的数据认证机制需求设计了 SCBC-MAC 方案。

第六章　仿真实验与结果分析

在第三章中我们设计实现了多跳长路径上多节点联合数据认证机制，第三章中提出了对多节点联合数据机制的优化方案，并对它们进行了理论分析。在本章中我们将使用仿真实验平台，对数据认证机制进行实验验证，并对它们的性能进行比较分析。6.1 节介绍实验平台的环境，及相关仿真软件的介绍。6.2 节是多跳长路径上多节点联合数据认证仿真实验及结果分析。6.3 节是数据认证优化方案仿真实验及结果分析。

6.1　实验平台环境

6.1.1　仿真实验环境

为了搭建无线传感网的仿真环境，本文采用了仿真平台 OMNeT++（Objective Modular Network testbed in C++）进行仿真，在 Windows 7 的主机中安装的版本为 OMNET++4.6b1。主机的配置为：

- DDR3 内存，容量 8G，频率 1600MHz
- Core 双核处理器，主频 2.6GHz

现在进行网络仿真的工具很多，还有有 NS2、NS3、OPNET、TOSSIM、GloMoSim 和 PowerTOSSIM 等平台。NS2 和 NS3 平台虽然有丰富的协议库支持，但是仿真时数据量过大，对复杂的无线传感网场景的仿真不合适，而且学习曲线比较高。OPNET 平台要实现无线传感网仿真，需要添加能量模型，而且其最大问题是仿真速度慢，效率会随网络规模和流量增大而降低。TOSSIM、GloMoSim 和 PowerTOSSIM 等其他仿真平台也有相应的局限性。

本文的实验中，我们选择了 OMNeT++ 平台，OMNeT++ 是面向对象的离散事件仿真工具。OMNeT++ 基于 Eclipse 平台构建，是一款开源的仿真集成环境，由建模工具、仿真运行工具和输出结果分析工具等组成。OMNeT++ 还有 INET、INETMANET 或 MIXIM 等类库支持网络仿真，利用这些开源的包，很容易对各种网络协议进行仿真实验。

在 OMNeT++ 中，主要使用 C++ 语言创建仿真对象类，并使用 ned 文件配置仿真的参数，一个 OMNeT++ 的仿真模型包括如下部分：

1. 网络拓扑结构描述文件（.ned 文件）：使用 ned 文件对仿真网络中的信道、门、连接和模块等进行配置。
2. 消息或包定义文件（.msg 文件）：对网络中传输的消息或者数据报文进行定义，OMNeT++ 会自动从.msg 生成相应的消息类。

3. 模块描述文件（.h 和.cc 文件）：使用 C++ 语言描述模型中的各个模块。

仿真模型使用 C++ 编译器将.ned 网络拓扑结构描述文件、.msg 消息或包定义文件以及模块描述文件进行编译后，同仿真内核库以及用户接口库进行链接，生成可执行的仿真程序。OMNeT++ 不同于其他仿真平台，生成的仿真程序可以运行于没有安装 OMNeT++ 的机器上。

6.1.2 无线传感网数据认证仿真框架

下面将对搭建的无线传感网数据认证仿真模型进行介绍，在我们的无线传感网数据认证机制研究中，我们的仿真模型主要包括两种对象：传感器节点和基站。在本文中，我们假设所有的传感器节点均为相同的配置，部署时的能量相同。

6.1.2.1 模块配置

在 OMNeT++ 仿真平台中，使用 ned 文件配置相应的模块，传感器节点的配置文件如下所示，节点包括了一个输入输出门向量：

```
simple Node
{
    parameters:
        double txRate @unit(bps);
        double radioDelay @unit(s); // 时间片
        volatile double iaTime @unit(s); // 数据包发送间隔时间
        @display("i=device/wsn");
    gates:
        inout out;
}
```

基站的配置文件如下所示，基站也包括一个输入输出门向量，仿真实验中假设基站的通信不会受信道冲突的影响：

```
simple Bs
{
    parameters:
        @display("i=device/antennatower_l");
    gates:
        inout bsRadio[];
}
```

6.1.2.2 模块类实现

在我们的仿真实验中，传感器节点模块和基站模块都使用 C++ 编写，我们对两个模块的实现做简要的介绍。

传感器节点使用了固定时间间隔内随机生成数据报文的方式仿真数据采集的过程，并采用自消息完成数据传输给簇头的过程，其采集过程函数表示如下：

```
void Node::initialize() {
    char msgname[20];
```

```
    sprintf(msgname, "event sensor # %d", getIndex());
    startEvent = new cMessage(msgname);
    iaTime = &par("iaTime");
    radioDelay = par("radioDelay");
    //事件捕获后的发送时间
    simtime_t t = simTime() + iaTime->doubleValue();
    if (ev.isGUI())
       getDisplayString().setTagArg("t", 2, "#808000");
    scheduleAt(t, startEvent);
}
```

传感器节点仿真发送数据包的过程主要由函数 handleMessage 完成:

```
void Node::handleMessage(cMessage* msg) {
    int src = getIndex();
    char msgname[40];
    sprintf(msgname, "event from cluster node %d", src);
    PacketCn *pkt = new PacketCn(msgname);
    pkt->setBitLength(952);
    pkt->setSource(src);
    pkt->setEvent(event);
    WATCH(pkt);
    //下一个事件发送时间，形成一个包传送给BS
    simtime_t tt = simTime() + iaTime->doubleValue();
    simtime_t nextTime=0;
    if((ceil(simTime()/radioDelay)*radioDelay)<tt)
       nextTime = tt;
    else
       nextTime = tt+radioDelay;
    ev << "send packet:"<<pkt<<" when "<<nextTime<< endl;
    send(pkt, "out$o");
    scheduleAt(nextTime, startEvent);
}
```

基站模块主要是接收数据报文，并对报文中的 XMAC 进行认证，确定报文的身份，其主要函数如下:

```
void Bs::handleMessage(cMessage* msg) {
    PacketCh *pkt = check_and_cast<PacketCh *>(msg);
    int event=pkt->getEvent();
    //计算event的XMAC
    int eventMac=this->Xmac(event);
    if(pkt->getXmac()==eventMac){
       ev<<"event received!"<<endl;
    }
    else{
       ev<<"trash packet!"<<endl;
    }
    delete pkt;
}
```

6.2 多跳长路径上多节点联合数据认证仿真实验

6.3 数据认证优化方案仿真实验

6.4 本章小结

本章首先介绍了仿真实验环境的搭建，对使用 OMNET++ 进行无线传感网的仿真进行了介绍，对相关实验的框架搭建进行了说明。使用 OMNET++ 平台对我们的多跳长路径上多节点联合的数据认证机制进行仿真实验，验证该数据认证方案有较好的安全性能。我们还对两个优化方案进行了仿真，实验结果表明两个方案分别对检测成功率和通信开销有较好的改进。

第七章　总结与展望

本章对本文的研究进行总结，针对课题研究中待完善的地方，提出下一步工作的设想。

7.1　本文总结

无线传感网在许多大范围监测领域都有广泛的应用，在环境监测、军事侦察等领域都有规模化的应用。无线传感器节点通常被部署在环境恶劣的无人值守区域，容易节点受损或者节点受攻击，导致传感网的传输受到严重影响。因此需要对无线传感网中的传输进行认证，保证数据传输的安全性。但是由于无线传感器节点计算能力、存储空间有限，而且节点能量受到限制，因此安全机制的设计必须满足轻量级的要求，以适应传感器节点的限制。我们设计了多跳长路径上多节点联合的数据认证机制，有效利用了数据认证机制保障了传输路径上的安全。

本文主要工作总结如下:

1. 深入研究了无线传感网中数据认证及其密钥分配的理论，分析了它们的发展研究现状，分析了数据认证在无线传感网中的应用，并总结了各种方案的优点和宝贵经验。
2. 提出了多跳长路径上多节点联合数据认证的模型，设计实现了多跳长路径上多节点联合数据认证协议，并设计了路径上节点关系的维护算法，对协议的安全性能进行了分析评价。
3. 针对多跳长路径上多写点联合数据认证协议的不足，对算法进行了优化，提出了多路径抗节点失效机制和动态步长多节点联合数据认证机制，并对优化方案的安全性能进行了分析评价。
4. 围绕多跳长路径多节点联合数据认证机制的需求，对密钥分配方案进行了深入研究，提出了基于单向 hash 链的密钥分配方案，并对认证中的 MAC 进行了研究，提出了适应数据认证机制需求的 MAC 码。
5. 通过仿真实验验证了本文中提出的方案的安全性能以及优化效果。

7.2　未来工作于展望

本文设计实现的多跳长路径上多节点联合的数据认证机制能够很好地提升了无线传感网数据传输的安全性，取得了一定的成果。但是由于无线传感网本身的复杂性以及部署场景的多样性，我们的机制对不同工作场景下的无线传感网的适应性还需进一步研究，在数据认证的具体算法以及密钥分配等方向还有进一步研究的空间。结合现阶段以及完成的工作，我们未来可做的相关工作有:

1. 本文研究的数据认证机制与无线传感网现有的各层次协议结合还不够，在后续的工作中可以将数据认证机制同其他协议结合起来，例如同网络层的路由协议相结合，将数据认证的相关报文使用路由报文发送。
2. 针对本文的数据认证机制提出的两个优化方案，虽然在仿真实验环境中已经进行了验证，但在实际的无线传感网中部署比较复杂，需要通过搭建真实的传感器节点平台，对相关方案进行针对性的优化。
3. 密钥分配方案的设计实现还不够完善，需要对相关的算法进行进一步的改进，形成完整的密钥管理机制，并对密钥分配方案的效率和安全性进行分析评价。使用的单向 hash 函数还有改进的空间，可以进一步压缩其计算开销。

致　谢

参考文献

[1] Su Y S W. A survey on sensor networks [J]. 2002.

[2] Intanagonwiwat C, GOvindan R, Estrin D. Directed Diffusion: A scalable anr robust communication paradigm for sensor networks [J]. MOBICOM. 2000.

[3] TinyOS Home Page [EB/OL]. http://www.tinyos.net/.

[4] Li H, Hua X. Water Enviroment Monitoring System Based on Zigbee Technology [C]. In Intelligent System Design and Engineering Applications (ISDEA), 2013 Third International Conference on. Jan 2013: 1607–1609.

[5] Owen M, Klamer D, Dean B. Evolutionary control of an autonomous field [C]. In Information Fusion, 2000. FUSION 2000. Proceedings of the Third International Conference on. July 2000: MOD1/3–MOD1/9 vol.1.

[6] Meyer S, Rakotonirainy A. A Survey of Research on Context-Aware Homes. [C]. In ACSW Frontiers. 2003: 159–168.

[7] Kulkarni G, Shelk R, Gaikwad K, et al. Wireless sensor network security threats [C]. In Communication and Computing (ARTCom 2013), Fifth International Conference on Advances in Recent Technologies in. Sept 2013: 131–135.

[8] Modares H, Salleh R, Moravejosharieh A. Overview of Security Issues in Wireless Sensor Networks [C]. In Computational Intelligence, Modelling and Simulation (CIMSiM), 2011 Third International Conference on. Sept 2011: 308–311.

[9] Xu W, Trappe W, Zhang Y, et al. The feasibility of launching and detecting jamming attacks in wireless networks. [C]. In MobiHoc. 2005: 46–57.

[10] Rivest R L. The RC5 Encryption Algorithm [R]. 1997.

[11] Handschuh H. RC6. [C]. In Encyclopedia of Cryptography and Security (2nd Ed.). 2011: 1033–1034.

[12] Matsui M, Nakajima J, Moriai S. A Description of the Camellia Encryption Algorithm. RFC 3713 (Informational). April 2004.

[13] Wheeler D J, Needham R M. TEA, a Tiny Encryption Algorithm. [C]. In FSE. 1994: 363–366.

[14] Ohta H, Matsui M. A Description of the MISTY1 Encryption Algorithm. RFC 2994 (Informational). November 2000.

[15] Law Y W, Doumen J, Hartel P H. Survey and benchmark of block ciphers for wireless sensor networks. [J]. TOSN. 2006, 2 (1): 65–93.

[16] Malan D J, Welsh M, Smith M D. A public-key infrastructure for key distribution in TinyOS based on elliptic curve cryptography. [C]. In SECON. 2004: 71–80.

[17] Gura N, Patel A, W A, et al. Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs [C]. In 2004 Workshop on Cryptographic Hardware and Embedded Systems(CHES2004). 2004: 119–132.

[18] Ganesan D, Govindan R, Shenker S, et al. Highly-resilient, energy-efficient multipath routing in wireless sensor networks. [C]. In MobiHoc. 2001: 251–254.

[19] Karlof C, Wagner D. Secure routing in wireless sensor networks: attacks and countermeasures. [J]. Ad Hoc Networks. 2003, 1 (2-3): 293–315.

[20] Li Z, Trappe W, Zhang Y, et al. Robust statistical methods for securing wireless localization in sensor networks. [C]. In IPSN. 2005: 91–98.

[21] Priyanka S F, Nikita C. False Data Detection in Wireless Sensor Network with Secure communication. [C]. In International Journal of Smart Sensors and Ad Hoc Networks (IJSSAN). 2005: 66–71.

[22] Özdemir S, Cam H. Integration of False Data Detection With Data Aggregation and Confidential Transmission in Wireless Sensor Networks. [J]. IEEE/ACM Trans. Netw. 2010, 18 (3): 736–749.

[23] Sivagami V, Kumar C. False Data Detection Using MAC pairs in Wireless Sensor Networks [C]. In International Journal of Smart Sensors and Ad Hoc Networks (IJSSAN). April 2013: 539–545.

[24] Zhu S, Setia S, Jajodia S, et al. An Interleaved Hop-by-Hop Authentication Scheme for Filtering of Injected False Data in Sensor Networks. [C]. In IEEE Symposium on Security and Privacy. 2004: 259–271.

[25] Wang G, Zhang W, Cao G, et al. On supporting distributed collaboration in sensor networks [C]. In Military Communications Conference, 2003. MILCOM '03. 2003 IEEE. Oct 2003: 752–757 Vol.2.

[26] Mathews M, Song M, Shetty S, et al. Detecting compromised nodes in wireless sensor networks [C]. In SNPD 2007. Eighth ACIS International Conference on. 2007: 273–278.

[27] Zhang Y, Liu W, Lou W, et al. Location-based compromise-tolerant security mechanisms for wireless sensor networks. [J]. IEEE Journal on Selected Areas in Communications. 2006, 24 (2): 247–260.

[28] Agah A, Das S K, Basu K, et al. Intrusion Detection in Sensor Networks: A Non-Cooperative Game Approach. [C]. In NCA. 2004: 343–346.

[29] Perrig A, Szewczyk R, Tygar J, et al. SPINS: Security Protocols for Sensor Networks [J]. Wireless Networks. 2002, 8 (5): 521–534.

[30] Liu D, Ning P. Multilevel μTESLA: Broadcast authentication for distributed sensor networks. [J]. ACM Trans. Embedded Comput. Syst. 2004, 3 (4): 800–836.

[31] 裴庆祺，沈玉龙，马建峰．无线传感器网络安全技术综述 [J]．通信学报．2007，28．

[32] Husseini A E, M'hamed A, El-Hassan B, et al. Trust-based authentication scheme with user rating for low-resource devices in smart environments. [J]. Personal and Ubiquitous Computing. 2013, 17 (5): 1013–1023.

[33] Dong Q, Liu D, Ning P. Pre-authentication filters: providing dos resistance for signature-based broadcast authentication in sensor networks. [C]. In WISEC. 2008: 2–12.

[34] Chan H, Perrig A, Song D. Random key predistribution schemes for sensor networks [C]. In IEEE Symposium on Security and Privacy. 2003: 197–213.

[35] Watro R J, Kong D, fen Cuti S, et al. TinyPK: securing sensor networks with public key technology. [C]. In SASN. 2004: 59–64.

[36] Bauer K, Lee H. A Distributed Authentication Scheme for a Wireless Sensing System [C]. In ACM Transactions on Information and System Security. March 2004: 1–35.

[37] Benenson Z. Realizing Robust User Authentication in Sensor Networks [C]. In In Real-World Wireless Sensor Networks (REALWSN. 2005.

[38] Cao X, Kou W, Dang L, et al. IMBAS: Identity-based multi-user broadcast authentication in wireless sensor networks. [J]. Computer Communications. 2008, 31 (4): 659–667.

[39] Eschenauer L, Gligor V D. A Key-Management Scheme for Distributed Sensor Networks [C]. In ACM Conference on Computer and Communications Security (CCS'02). November 2002.

[40] Stinson D R. Combinatorial designs: constructions and analysis. [J]. SIGACT News. 2008, 39 (4): 17–21.

[41] Blom R. An Optimal Class of Symmetric Key Generation Systems [C]. In EUROCRYPT. 1984: 335–338.

[42] Du W, Deng J, Han Y S, et al. A pairwise key predistribution scheme for wireless sensor networks [J]. ACM Transactions on Information and System Security (TISSEC). 2005, 8 (2): 228–258.

[43] Blundo C, Santis A D, Vaccaro U, et al. Perfectly secure key distribution for dynamic conferences [J]. Information and Computation. 1998, 146 (1): 1–23.

[44] Liu D, Ning P, Li R. Establishing pairwise keys in distributed sensor networks [J]. ACM Transactions on Information and System Security (TISSEC). 2005, 8 (1): 41–77.

[45] Liu D, Ning P. Location-based pairwise key establishments for static sensor networks [C]. In SASN. 2003: 72–82.

[46] Du W, Deng J, Han Y S, et al. A Key Predistribution Scheme for Sensor Networks Using Deployment Knowledge [J]. IEEE Trans. Dependable Sec. Comput. 2006, 3 (1): 62–77.

[47] Liu D, Ning P, Du W. Group-based key predistribution for wireless sensor networks [J]. TOSN. 2008, 4 (2).

[48] Chan H, Perrig A. PIKE: peer intermediaries for key establishment in sensor networks [C]. In INFOCOM. 2005: 524–535.

[49] Çamtepe S A, Yener B. Combinatorial design of key distribution mechanisms for wireless sensor networks. [J]. IEEE/ACM Trans. Netw. 2007, 15 (2): 346–358.

[50] Zhu S, Setia S, Jajodia S. LEAP+: Efficient security mechanisms for large-scale distributed sensor networks [J]. ACM Transactions on Sensor Networks (TOSN). 2006, 2 (4): 500–528.

[51] Karp B, Kung H-T. GPSR: Greedy perimeter stateless routing for wireless networks [C]. In Proceedings of the 6th annual international conference on Mobile computing and networking. 2000: 243–254.

[52] Bellare M, Canetti R, Krawczyk H. Message Authentication Using Hash Functions: the HMAC Construction [J]. CryptoBytes. 1996, 2 (1): 12–15.

[53] Bellare M, Guérin R, Rogaway P. XOR MACs: New Methods for Message Authentication Using Finite Pseudorandom Functions. [C]. In CRYPTO. 1995: 15–28.

作者在学期间取得的学术成果

发表的学术论文

[1] Zongxiao Lan , Geming Xia , Aolong Zhou. Communication cost optimized session key transmission scheme for WSN based on non-perfect secret sharing. ICITMI, 2014.