分类号 TP957 学号 0123456

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 蓝宗骁

学科专业 网络工程

研究方向 网络工程

指导教师 夏戈明 教授

国防科学技术大学研究生院

二〇一四年十月

面向规模化大数据传感网的数据认证关键技术研究

Candidate: Lan Zongxiao

Advisor: Associate Professor Xia Geming

A dissertation

Submitted in partial fulfillment of the requirements

for the degree of Master of Engineering

in Large-scale Wireless Sensor Network Data Authentication

Graduate School of National University of Defense Technology

Changsha, Hunan, P. R. China

October 22, 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：国防科学技术大学学位论文 LaTeX 模板

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：国防科学技术大学学位论文 LaTeX 模板

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

表 目 录

图 目 录

摘　要

国防科学技术大学是一所直属中央军委的综合性大学。1984 年, 学校经国务院、中央军委和教育部批准首批成立研究生院，肩负着为全军培养高级科学和工程技术人才与指挥人才，培训高级领导干部，从事先进武器装备和国防关键技术研究的重要任务。国防科技大学是全国重点大学，也是全国首批进入国家“211 工程”建设并获中央专项经费支持的全国重点院校之一。学校前身是 1953 年创建于哈尔滨的中国人民解放军军事工程学院，简称“哈军工”。

关键词: **国防科学技术大学**; 211; **哈军工**

ABSTRACT

National University of Defense Technology is a comprehensive national key university based in Changsha, Hunan Province, China. It is under the dual supervision of the Ministry of National Defense and the Ministry of Education, designated for Project 211 and Project 985, the two national plans for facilitating the development of Chinese higher education.

NUDT was originally founded in 1953 as the Military Academy of Engineering in Harbin of Heilongjiang Province. In 1970 the Academy of Engineering moved southwards to Changsha and was renamed Changsha Institute of Technology.The Institute changed its name to National University of Defense Technology in 1978.

Key Words: NUDT; MND; ME

第一章　绪论

本章首先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

规模化传感网既是前沿研究问题，又在国家社会重大安全领域有着预期的应用前景，预期将得到广泛应用和持续的发展。本研究适应大规模大数据无线传感需求的数据认证机制，设计相关认证算法、协议及有关密钥分配管理的算法，并将在仿真平台和实际传感器节点平台上实现、验证和测试有关功能。将为大规模大数据无线传感网的数据认证提供可行的技术方案，为了解决无线传感网的安全传输提供了工程上的解决范例。

1.1.1　无线传感网概述

正文内容
正文内容

1.1.2　无线传感网对数据认证的需求

无线传感网的安全需求主要有两方面：面向基础设施的通信安全及面向数据的信息安全。前者为无线传感网完成数据采集、数据传输、数据融合等基本功能提供支撑，后者提供实现数据机密性、完整性、不可否认性等信息安全机制。通信安全主要包括以下内容：- 节点安全性：指传感器节点的部署隐蔽性及抗受损能力。要求节点不易被发现，且节点内部通过代码混淆等方法提供一定的机密信息保护措施。- 防御能力：指无线传感网抗外部攻击及内部攻击的能力。要求在敌手攻击下，部分节点受损不会影响网络的整体功能。- 入侵检测能力：指识别入侵行为，确定入侵者身份、位置等信息，主动丢弃入侵者发出的虚假数据的能力。

信息安全主要包括以下内容：- 数据机密性：通过加密技术及访问控制能确保网络中的消息明文不会暴露给非授权实体。- 不可否认性：通过消息签名、身份认证、访问控制等方式有效识别消息源。- 数据完整性：通过消息认证码 (MAC)、消息签名等技术提供数据在传输过程中的防篡改能力。- 数据新鲜性：通过消息新鲜性参数确保消息在其时效范围内被目标实体接收。

除了保证必要的通信安全及数据安全，安全协议的设计还应当考虑如下因素：- 抗毁性：部分节点受损不会导致整个网络安全体系瘫痪。- 可扩展性：安全协议不应当对网络节点的加入与移除造成影响。- 灵活性：安全协议不应当影响网络部

署的灵活性。- 低开销：安全协议带来的计算开销、通信开销、存储开销及对应能耗应当是传感器节点可承受的。

1.2 本文研究内容

正文内容
正文内容
正文内容
正文内容

1.3 本文组织结构

第二章　相关研究

2.1　无线传感网安全技术概述

保密性 (Confidentiality)。数据的保密性是重要的安全需求，要求网络中的敏感信息在存储和传输过程中都要保证数据的保密特性，也就是对非授权用户是保密的。. 完整性 (Integrity)。有了数据保密性的保证，接收端还不能保证收到的数据是正确的，即在传输过程中未被恶意更改，数据完整性鉴别保证了数据在传输过程中没有被恶意的修改。认证性 (Authentication)。认证性实际上就是对于网络中包含的传感器节点必须保证其生成的身份是可信的，也就是节点不能被冒充和伪造。新鲜性 (Freshness)。新鲜性就是数据符合一致的时间轴，也就是保证消息队列的时间一致性和不可重复性，从而杜绝攻击者通过重放旧的消息达到其攻击目的，数据的新鲜性主要用来防止复制节点攻击不可否认性 (Non-repudiation)。节点间进行数据传输和转发时，参与传输的节点不能否认自己在传输过程中的行为。可用性 (Availability)。一旦网络检测发现遭到攻击，(如复制节点攻击) 要求传感器网络能够按照事先设定的工作方式向合法用户提供信息访问的权限。健壮性 (Robustness) 由于无线传感器网络具有较强的动态性和不确定性，因此要求其对各种安全攻击具有较强的适应特性，即使攻击者的攻击行为得逞，通过健壮性也可以使其攻击行为带来的后果最小化。

2.1.1　无线传感网的安全威胁

2.1.2　无线传感网的安全机制

2.1.2.1　密码算法
2.1.2.2　安全路由
2.1.2.3　数据聚合
2.1.2.4　入侵检测
2.1.2.5　认证机制
2.1.2.6　密钥管理

2.2　无线传感网认证机制概述

在本节中，我们首先介绍无线传感网数据认证机制，然后概述现有的面向无线传感网的密钥分配方案。

表 2.1　无线传感网常见的攻击与防范措施

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
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
	物理破坏	节点伪装和隐藏

2.2.1　无线传感网数据认证概述

2.2.2　无线传感网密钥分配方案概述

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。

近些年来，WSN 的密钥分配有了许多新的研究成果，

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

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。

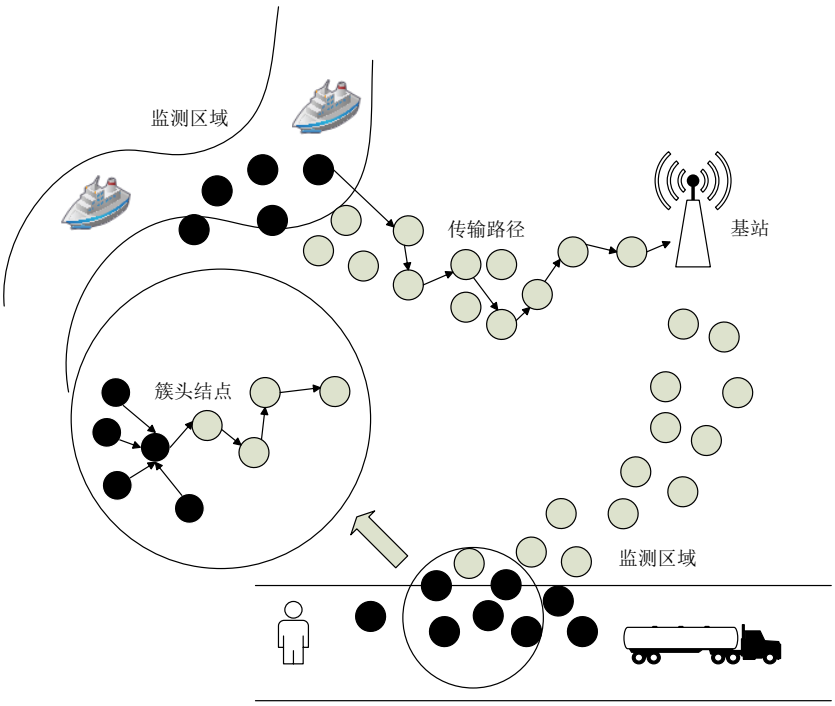

图 3.1　无线传感网应用场景

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[1] 中提出的对密钥建立方案可以实现这个目标。通过使用 [2, 3] 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:

- 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。
- 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。
- 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。
- 认证机制计算高效，消耗能量小，适应无线传感网的要求。

- 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。

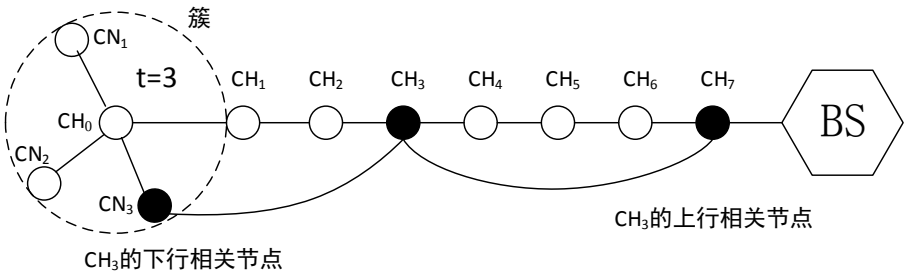

图 3.2 多节点联合数据认证中上下行相关节点

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 $XMAC(E)$:

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

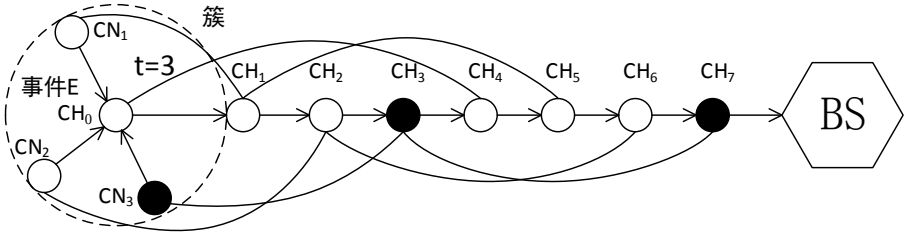

图 3.3　多节点联合数据认证中数据报文发送过程

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:

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

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:

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

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 [4] 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，

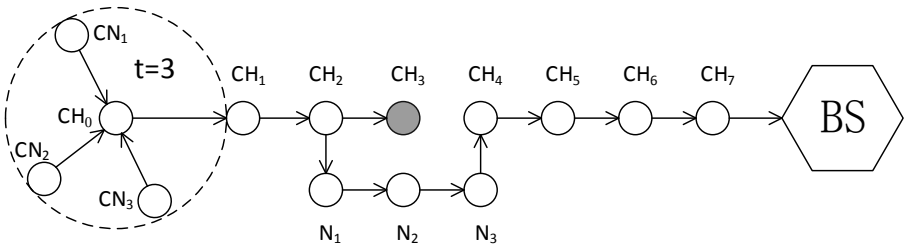

图 3.4　节点自动维护上下行相关关系的过程

当节点 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

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实现

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。

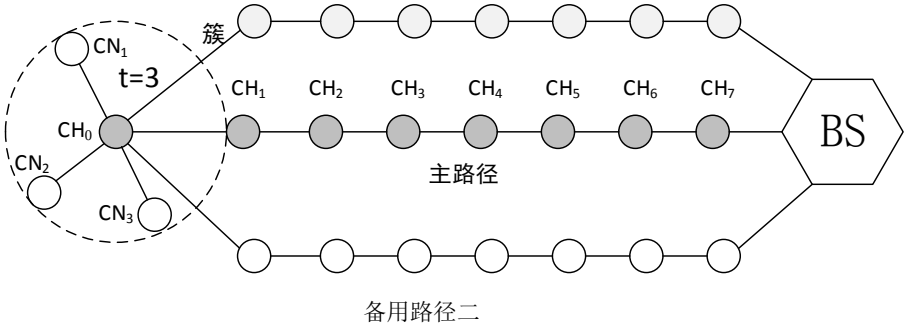

图 4.1　多路径抗节点失效机制中的不相交路径

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。

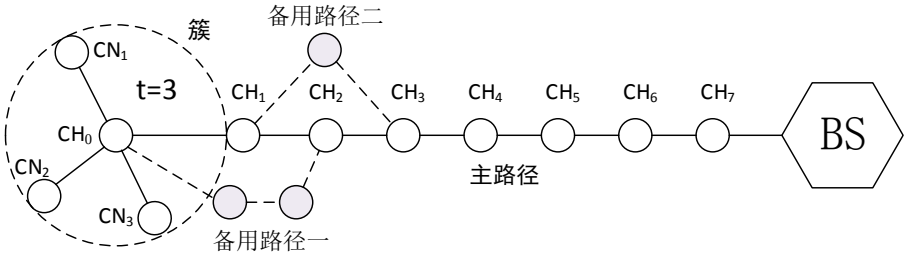

图 4.2　多路径抗节点失效机制中的编织路径

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。

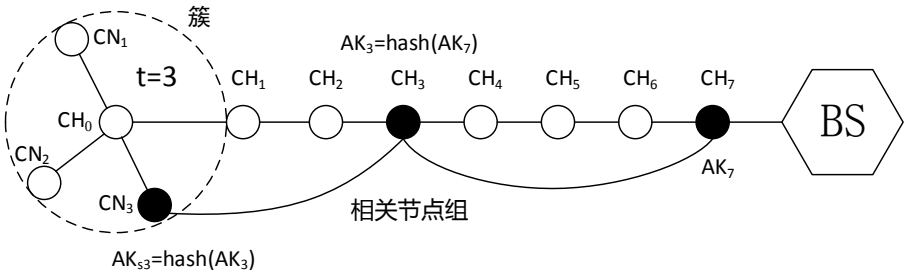

图 4.3　多路径抗节点失效机制的密钥分配

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[5]，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

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。

4.2 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。

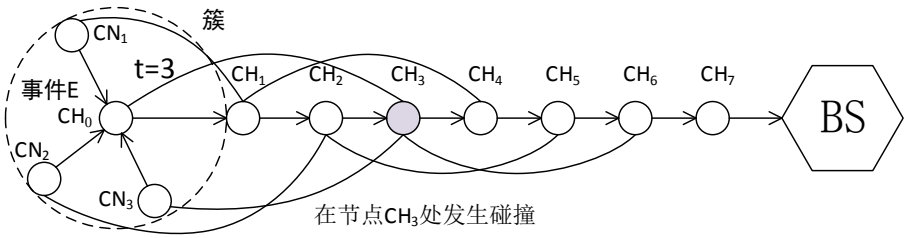

图 4.4　动态步长多节点联合数据认证

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。

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，$AK_{s3} = H(AK_0)$。

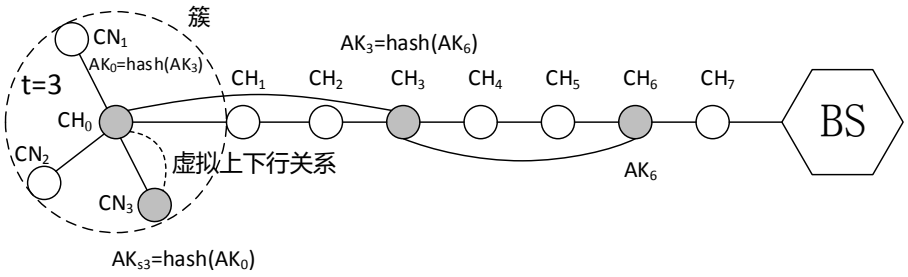

图 4.5　面向动态步长多节点联合数据认证的密钥分配

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 $h - h_0 \le p$ 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

4.3 本章小结

第五章　密钥分配与 MAC 设计

5.1　基于单向 hash 链的密钥分配方案

5.1.1　单向 hash 链

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：

- hash 函数 $H(x)$ 的输入 x 为任意长度
- hash 函数 $H(x)$ 的输出为给定长度
- 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
- 对于给定的 hash 值 $y=H(x)$，找出 x 在计算上是不可行的
- 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

本文利用

5.2　轻量级 MAC 码

5.3　本章小结

第六章　仿真实验与结果分析

```
void Ch::handleMessage(cMessage* msg) {
   //cluster header
   if (getIndex() == 0) {
      if (msg == sendPkt) {
         //generate packet of event
         char msgname[30];
         sprintf(msgname,"event @ %s",SIMTIME_STR(simTime()));
         ev<<"simtime:"<<simTime()<<endl;
         eventPkt->setName(msgname);
         eventPkt->setSource(getIndex());
         eventPkt->setHopCount(hopCount);
         eventPkt->setXmac(eventPkt->getEvent()-123);
         eventPkt->setBitLength(pkLenBits->longValue());
         int n = gateSize("radio");
         send(eventPkt,"radio$o",n-1);
         eventPkt=new PacketCh("");
         scheduleAt(simTime() + radioDelay, sendPkt);
      } else {
         PacketCn *pkt = check_and_cast<PacketCn *>(msg);
         int src = pkt->getSource();
         int event = pkt->getEvent();
         ev << "from #" << src << "with event:" << event <<
            endl;
         eventPkt->setMac(src,1011000+src);
         eventPkt->setEvent(eventPkt->getEvent()+event);
      }
   }
   //en-route节点
   else {
      int n = gateSize("radio");
      double duration=pkLenBits->longValue()/txRate;
      ev<<"duration time:"<<duration<<endl;
      sendDelayed(msg,duration,"radio$o",n-1);
   }
}
```

第七章　总结与展望

7.1　本文总结

正文内容

7.2　未来工作于展望

正文内容

致　谢

本人的学位论文是在我的导师夏老师的亲切关怀和悉心指导下完成的。他严肃的科学态度，严谨的治学精神，精益求精的工作作风，深深地感染和激励着我。从课题的选择到论文的最终完成，夏老师都始终给予我细心的指导和不懈的支持。在此谨向夏老师致以诚挚的谢意和崇高的敬意。

在此，我还要感谢在一起愉快的度过大学生活的每个可爱的同学们和尊敬的老师们，特别是同一个宿舍的卢遥、鲁勇通信，正是由于你们的支持，在学业上互相帮助，共同进步，我才能克服一个一个的困难和疑惑，直至本文的顺利完成。

在论文即将完成之际，我的心情无法平静，从开始进入课题到论文的顺利完成，有多少可敬的师长、同学、朋友给了我无言的帮助，在这里请接受我诚挚的谢意! 谢谢你们!

参考文献

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] Mathews M, Song M, Shetty S, et al. Detecting compromised nodes in wireless sensor networks [C]. In Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2007. SNPD 2007. Eighth ACIS International Conference on. 2007: 273–278.

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.