ICS 35.040
L 80

中华人民共和国国家标准

GB/T 30269.601—2016

信息技术　传感器网络
第601部分:信息安全:通用技术规范

Information technology—Sensor network—
Part 601:Information security:General technical specifications

2016-04-25 发布　　2016-08-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前言 …… Ⅰ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　缩略语 …… 4
5　概述 …… 4
5.1　传感器网络资产 …… 4
5.2　安全模型 …… 4
5.3　安全环境假设 …… 5
5.4　安全威胁 …… 5
5.5　安全策略 …… 6
5.6　传感器网络安全目标 …… 8
6　安全机制 …… 8
6.1　密钥管理机制 …… 8
6.2　访问控制 …… 9
6.3　鉴别机制 …… 9
6.4　路由安全 …… 9
6.5　安全数据融合 …… 9
6.6　加密机制 …… 9
6.7　安全审计机制 …… 9
6.8　帧安全机制 …… 10
6.9　协调器变换的安全机制 …… 10
7　安全等级划分 …… 10
7.1　安全等级划分概述 …… 10
7.2　安全等级划分方法 …… 10
7.3　安全等级划分要求 …… 11
附录A（资料性附录）　密钥管理 …… 18
附录B（资料性附录）　访问控制机制 …… 22
附录C（资料性附录）　路由安全 …… 28
附录D（资料性附录）　安全数据融合机制 …… 33
附录E（资料性附录）　帧安全机制 …… 35
附录F（资料性附录）　协调器变换安全机制 …… 39
参考文献 …… 42

前　言

GB/T 30269《信息技术　传感器网络》拟分为以下几部分：

——第 1 部分：参考体系结构和通用技术要求；

——第 2 部分：术语；

——第 301 部分：通信与信息交换：低速无线传感器网络网络层和应用支持子层规范；

——第 302 部分：通信与信息交换：面向高可靠性应用的无线传感器网络媒体访问控制和物理层规范；

——第 303 部分：通信与信息交换：基于 IP 的网络层规范；

——第 304 部分：通信与信息交换：面向视频的媒体访问控制层和物理层规范；

——第 305 部分：通信与信息交换：超声波通信协议规范；

——第 401 部分：协同信息处理：支撑协同信息处理的服务及接口；

——第 501 部分：标识：传感节点标识符编制规则；

——第 502 部分：标识：传感节点解析和管理规范；

——第 503 部分：标识：传感节点标识符注册规程；

——第 601 部分：信息安全：通用技术规范；

——第 602 部分：信息安全：低速率无线传感器网络网络层和应用支持子层安全规范；

——第 603 部分：信息安全：密钥管理技术规范；

——第 701 部分：传感器接口：信号接口；

——第 702 部分：传感器接口：数据接口；

——第 801 部分：测试：通用要求；

——第 802 部分：测试：低速无线传感器网络媒体访问控制和物理层；

——第 803 部分：测试：低速无线传感器网络网络层和应用支持子层；

——第 804 部分：测试：传感器接口测试规范；

——第 805 部分：测试：传感器网关测试规范；

——第 806 部分：测试：传感节点标识符解析一致性测试技术规范；

——第 807 部分：测试：网络传输安全测评规范；

——第 808 部分：测试：低速率无线传感器网络网络层和应用支持子层安全测评规范；

——第 809 部分：测试：传感网系统安全测评规范；

——第 901 部分：网关：通用技术要求；

——第 902 部分：网关：远程管理技术要求；

——第 903 部分：网关：逻辑功能接口技术规范；

——第 1001 部分：中间件：传感器网络结点数据交互规范。

本部分是 GB/T 30269 的第 601 部分。

本部分按照 GB/T 1.1—2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本部分凡涉及密码相关内容，按国家有关法规实施。

本部分由全国信息技术标准化技术委员会(SAC/TC 28)提出并归口。

本部分起草单位：中国电子技术标准化研究院、重庆邮电大学、深圳市海思半导体有限公司、山东省计算中心、中国科学院软件研究所、西安西电捷通无线网络通信有限公司。

本部分起草人：陈星、王浩、赵华伟、张立武、张向东、徐静、董挺、汪付强、杜志强。

信息技术　传感器网络
第601部分:信息安全:通用技术规范

1　范围

GB/T 30269的本部分针对传感器网络传输的安全威胁和安全目标,提出了传感器网络的安全模型,描述了传感器网络安全策略、机制、等级。

本部分适用于传感器网络的安全设计、开发、运营和维护,可为传感器网络安全评估提供参考。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB/T 18336.1—2008　信息技术　安全技术　信息技术安全性评估准则　第1部分:简介和一般模型

GB/T 30269.2—2013　信息技术　传感器网络　第2部分:术语

3　术语和定义

GB/T 30269.2—2013界定的以及下列术语和定义适用于本文件。

3.1

传感器网络　sensor network

利用传感器网络结点及其他网络基础设施,对物理世界进行信息采集并对采集的信息进行传输和处理,并为用户提供服务的网络化信息系统。

3.2

结点鉴别　node authentication

证实结点是其所声称的结点。

3.3

脆弱性　vulnerability

可能被威胁所利用的资产或若干资产的薄弱环节。

[GB/T 20984—2007,定义3.18]

3.4

可信第三方　trusted third party

在同安全相关的活动方面,被其他实体信任的安全机构或其代理。

[GB/T 25069—2010,定义2.2.4.6]

3.5

密钥材料　keying material

确立和维持密码密钥关系所必需的数据(如密钥,初始化值)。

[GB/T 25069—2010,定义2.2.2.108]

3.6

共享密钥　shared key

两个或多个结点之间在初始密钥材料的基础上建立的长期共享的密钥。

3.7

会话密钥　session key

为保证一对结点之间的保密通信或消息鉴别而随机产生的密钥。通信完成后，会话密钥即被销毁。

3.8

密钥建立　key establishment

为一个或多个实体产生一个可用的、共享的秘密密钥的过程。密钥建立包括密钥协商、密钥传送等。

[GB/T 25069—2010，定义 2.2.2.118]

3.9

敏感标记　sensitivity label

表示主体/客体安全级别和安全范畴的一组信息。

[GB/T 25069—2010，定义 2.2.1.93]

3.10

数据新鲜性　data freshness

保证接收到数据的时效性，确保没有重放过时的数据。

3.11

数据融合结点　data convergence node

进行数据的收集、处理和传送，去除数据中的冗余信息的结点。

3.12

直接密钥　direct key

能够直接通信的两个邻居结点之间建立的共享密钥。

3.13

路径密钥　path key

没有共享直接密钥的两个传感器结点，利用已经与之建立共享密钥的结点构成多跳的安全路径，并在此基础上建立的共享密钥。

3.14

密钥连通性　key connectivity

经密钥协商后传感器结点之间成功建立直接密钥的可能性的特性。

3.15

攻击容忍性　attack resilience

部分传感器结点受损或被俘获后，其他结点的密钥不被暴露的特性。

3.16

前向安全性　forward security

在当前参与密钥协商的部分(或全部)传感器结点的共享密钥和会话密钥泄露的情况下，攻击者不可能重新计算出先前时间段的共享密钥和会话密钥的特性。

3.17

授权　authorization

赋与某一主体可实施某些动作的权力的过程。

[GB/T 25069—2010，定义 2.1.33]

3.18

保密性　confidentiality

使信息不泄露给未授权的个人、实体、进程，或不被其利用的特性。

[GB/T 25069—2010，定义 2.1.1]

3.19

数据完整性　data integrity

数据没有遭受以未授权方式所作的更改或破坏的特性。

[GB/T 25069—2010，定义 2.1.36]

3.20

可用性　availability

已授权实体一旦需要就可访问和使用的数据和资源的特性。

[GB/T 25069—2010，定义 2.1.20]

3.21

鉴别　authentication

提供对于某个实体自称身份的保证。

[GB/T 18794.2—2002，定义 3.3]

3.22

密钥管理　key management

根据安全策略，实施并运用对密钥材料进行产生、登记、认证、注销、分发、安装、存储、归档、撤消、衍生、销毁和恢复的服务。

[GB/T 25069—2010，定义 2.2.2.114]

3.23

资源　resource

传感器网络中需要保护的数据、结点设备、存储容量、计算能力、能量以及通信带宽等。

3.24

外部用户　external user

在传感器网络之外与传感器网络交互的任何实体。

3.25

主体　subject

引起信息在客体之间流动的人、进程或设备等。

[GB 17859—1999，定义 3.4]

3.26

客体　object

信息的载体。

[GB 17859—1999，定义 3.3]

3.27

安全功能策略　security function policy

描述特定安全行为的一组规则，由系统安全功能执行并可表达为对系统的一组安全功能需求。

[GB/T 25069—2010，定义 2.2.1.4]

3.28

安全策略　security policy

指明传感器网络中如何管理、保护和分配资产（包括结点、网络、数据等）的一组安全规则、指导、惯例和实践。

3.29

安全机制　security mechanism

实现安全功能，提供安全服务的一组有机组合的基本方法。

[GB/T 25069—2010，定义 2.2.1.5]

4　缩略语

下列缩略语适用于本文件。

AC：访问控制器(Access Controller)

ACL：访问控制列表(Access Control List)

ACS：访问控制服务器(Access Control Server)

ADT：授权数据类型(Authorized Data Type)

AI：认证信息(Authentication Information)

DN：目的结点(Destination Node)

ID：身份信息(Identification)

MAC：消息鉴别码(Message Authentication Code)

PIB：个域网信息库(PAN Information Base)

VP：有效期限(Valid Period)

5　概述

5.1　传感器网络资产

传感器网络资产的描述，如表 1 所示。

表 1　传感器网络资产

资产	描述	脆弱性
结点资产	结点资产是指构成结点的各种软硬件资产，其中硬件资产包括执行器、传感器、控制器、存储器等，软件资源包括协议栈软件等	结点资产脆弱性是指结点软硬件资产可能遭受损害的环节，包括开放的部署区域，工作环境恶劣以及结点资源受限等方面
网络资产	网络资产是指网络中构建通信链路的通信基础设施，包括通信模块、通信接口等，也包括集成网络组件和各子系统的网络协议	网络资产脆弱性是指各种网络通信基础设施可能遭受损害的环节，包括结点资源受限，网关、路由等专用设备易遭受物理损害，复杂的网络结构，开放的通信环境以及各网络协议和安全机制中可能出现的安全漏洞等
数据资产	数据资产是指由构成传感器网络的组件产生、加工、存储和传输的传感器信息以及控制信息，其中传感器信息包括采集信息以及结点发起的命令消息等	数据资产脆弱性是指在数据资产产生、加工、存储和传输全过程中可能的遭受损害的环节，包括结点资源受限，工作环境恶劣，开放的通信环境以及安全机制中可能出现的安全漏洞等

5.2　安全模型

传感器网络安全模型参考 GB/T 18336.1—2008，面向数据、网络、结点三层的安全威胁，提出相应

的安全策略，给出安全机制和安全目标。如图 1 所示。

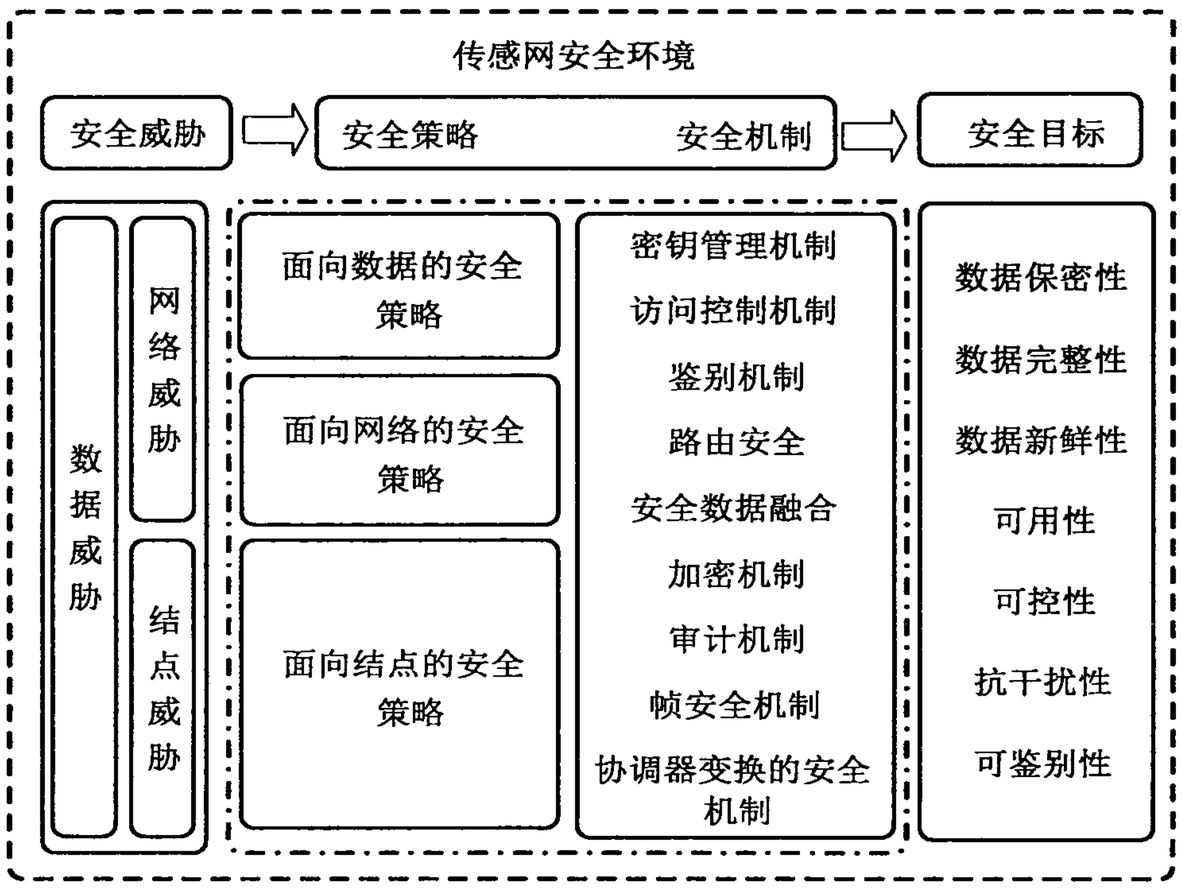

图 1　传感器网络安全模型

本模型为传感器网络安全的实施提出参考性模型架构。当传感器网络遭受到安全威胁时，应按照本模型提出的安全策略选取恰当的安全机制来实现整个网络的安全目标。

在设定传感器网络安全环境的前提下，分析归类传感器网络目前面临的安全威胁，针对归类的威胁进行安全策略的制定，每类策略可由安全机制中的一种或几种来提供支持，以达到所制定的一种或几种安全目标。

5.3　安全环境假设

传感器网络的安全环境假设如下：

a）　能够执行基本的安全协议，例如密钥的建立，是假定执行了基本的协议，没有遗漏主要的步骤。

b）　由于传感器网络中设备成本较低，假设传感器网络中的硬件抵抗攻击的能力有限。

c）　假设任何应用都可以访问底层。

d）　安全协议栈上不同层间彼此信任，同一个设备上运行的全部应用彼此相互信任。

5.4　安全威胁

5.4.1　威胁主体

威胁主体可用经验、资源和动机来描述。表 2 为与传感器网络关联的威胁主体。

表 2　威胁主体描述

威胁主体	经验	资源	动机
可信第三方或经过可信第三方授权的结点	低/高	丰富	无恶意
执行不恰当操作的授权结点	低/高	丰富	恶意
鉴别过期的结点	低/高	适度	恶意
外部未授权者	高	少/适度	恶意
诸如地震、洪水、火灾等不可抗力	无	丰富	无

5.4.2 威胁描述

表 3 是传感器网络所面临的威胁的描述。

表 3 威胁描述

威胁	威胁描述
物理威胁	由自然灾害以及非法人员潜入监测区域进行偷窃或物理破坏的行为所造成的网络硬件设施的损失或损坏。主要针对于部署在开放区域的结点
传输威胁	影响数据传输过程或传输结果的恶意行为，如阻塞、碰撞、延时、中断、拦截、篡改、伪造、欺骗等威胁
自私性威胁	结点为节省自身能量或得到更多网络资源而对网络整体利益造成损害的一种自私、贪心的行为
拒绝服务威胁	是指破坏网络的正常运作，降低网络或使网络丧失执行某一期望功能的能力，如硬件失败、软件bug、资源耗尽、环境条件等

5.4.3 攻击描述

表 4 是传感器网络可能遭受的攻击描述。

表 4 攻击描述

攻击	攻击描述
拥塞攻击	攻击者在获取目标网络通信频率的中心频率后，通过在这个频点附近发射无线电波进行干扰，使得攻击结点通信半径内的所有传感器网络结点不能正常工作
碰撞攻击	攻击者和正常结点同时发送数据包，使得数据在传输过程中发生了冲突，导致整个包被丢弃
耗尽攻击	通过持续通信的方式使结点能量耗尽。如利用协议漏洞不断发送重传报文或确认报文，最终耗尽结点资源
非公平竞争	攻击者不断发送高优先级的数据包从而占据信道，导致其他结点在通信过程中处于劣势
选择转发攻击	攻击者拒绝转发特定的消息并将其丢弃，使这些数据包无法传播，或者修改特定结点发送的数据包，并将其可靠地转发给其他结点
Sinkhole(黑洞)攻击	攻击者通过申明高质量路由来吸引一个区域内的数据流通过攻击者控制的结点，达到攻击网络的目的
Sybil(女巫)攻击	攻击者通过向网络中的其他结点申明有多个身份，达到攻击的目的
泛洪攻击	攻击者通过发送大量攻击报文，导致整个网络性能下降，影响正常通信
同步破坏攻击	攻击者通过采用同步机制不断地伪造消息并发给已经建立通信连接的结点，导致结点无休止的运行同步恢复协议

5.5 安全策略

5.5.1 面向数据的安全策略

数据是传感器网络应用的主要内容，数据安全是传感器网络安全的核心，面向数据的安全策略由一系列安全机制实现，如表 5 所示。

表 5　面向数据的安全策略

安全机制	说　　明
安全数据融合机制	安全数据融合机制应在任何条件下保障融合数据的真实性和准确性以及融合数据传输安全
鉴别机制	鉴别机制包括数据鉴别和身份鉴别两种，用于确保特定数据或特定身份的真实性及有效性
加密机制	对数据进行密码变换以产生密文
审计机制	审计机制对传感器网络中各种与安全有关的事件和行为进行检测、收集、记录和分析，并针对特定事件及行为采取相应行动
访问控制机制	访问控制机制以控制用户对传感器网络的访问为目的，能够防止未授权用户访问传感器网络的结点和数据

5.5.2　面向网络的安全策略

网络通信为上层应用提供服务，面向网络的安全策略由一系列安全机制实现，如表 6 所示。

表 6　面向网络的安全策略

安全机制	说　　明
路由安全	路由安全机制是以保证网络在受到攻击时仍能进行正确的路由发现、构建和维护为目标的安全机制
协调器变换安全机制	用以优化协调器变换过程中的结点和协调器的鉴别和安全材料的分发过程
帧安全机制	通过网络层帧的辅助帧头实现网络层帧结构的完整性以及网络层帧结构载荷的保密性
密钥管理机制	在一种安全策略指导下密钥的产生、存储、分配、删除、归档及应用
访问控制机制	访问控制机制以控制用户对传感器网络的访问为目的，能够防止未授权用户访问传感器网络的结点和数据

5.5.3　面向结点的安全策略

面向结点的安全策略由一系列安全机制实现。采用高效冗余的密码算法、安全有效的密钥管理机制、轻量级的安全协议等策略或机制来实现基于结点的安全，为网络层通信和应用层数据提供安全基础设施，如表 7 所示。

表 7　面向结点的安全策略

安全机制	说　　明
密钥管理机制	在一种安全策略指导下密钥的产生、存储、分配、删除、归档及应用
鉴别机制	鉴别机制包括数据鉴别和身份鉴别两种，用于确保特定数据或特定身份的真实性及有效性
审计机制	审计机制对传感器网络中各种与安全有关的事件和行为进行检测、收集、记录和分析，并针对特定事件及行为采取相应行动
访问控制机制	访问控制机制以控制用户对传感器网络的访问为目的，能够防止未授权用户访问传感器网络的结点和数据

5.6 传感器网络安全目标

5.6.1 概述

传感器网络安全目标由数据安全目标、网络安全目标、结点安全目标构成。按照传感器网络实际应用安全保护需求，确立各安全保护等级数据、网络、结点安全目标。

5.6.2 安全目标属性

5.6.2.1 数据保密性

使信息不泄露给未授权的个人、实体、进程，或不被其利用的特性。传感器网络确保具有保密性要求的数据在传输过程中不被泄露给未授权的个人、实体、进程，或不被其利用。在需要时确保数据在存储过程中不被泄露给未授权的个人、实体、进程，或不被其利用。

5.6.2.2 数据完整性

数据没有遭受以未授权方式所作的更改或破坏的特性。传感器网络采用国家相关标准规定的完整性机制，通过自主完整性策略和强制完整性策略，检测所有数据以及敏感标记在传输和存储过程中是否被有意地改动和破坏，并提供更正被改动数据的能力。

5.6.2.3 数据新鲜性

保证接收到数据的时效性，确保没有重放过时的数据。传感器网络确保各类设备采用安全机制对接收数据的新鲜性进行验证，并丢弃不满足新鲜性要求的数据，以抵抗对特定数据的重放攻击。

5.6.2.4 可用性

已授权实体一旦需要就访问和使用的数据和资源的特性。

5.6.2.5 可控性

在保障传感器网络中数据保密性、完整性、可用性的前提下，提供相应的安全控制部件，形成控制、检测和评估环节，构成完整的安全控制回路实现传感器网络可控性。

5.6.2.6 抗干扰性

传感器网络采用适当的机制来防止对数据发送、接收和转发的无线干扰，避免对网络的信息传输造成严重影响。

5.6.2.7 可鉴别性

可鉴别性分为数据可鉴别和身份可鉴别。数据可鉴别是指产生有效性证据以验证特定传输中的数据内容没有被伪造或者篡改，确保数据内容的真实性。身份可鉴别是指传感器网络维护每个访问主体的安全属性，同时提供多种身份鉴别机制，以满足传感器网络不同安全等级的需求。在进行鉴别时，传感器网络提供有限的主体反馈信息，确保非法主体不能通过反馈数据获得利益。

6 安全机制

6.1 密钥管理机制

传感器网络的密钥管理机制涉及以下三个方面：

a） 密钥材料的产生、分发、更新和注销；

b） 共享密钥的建立、撤销和更新；

c） 会话密钥的建立和更新。

传感器网络密钥管理机制首先必须考虑可用性、机密性、数据完整性、不可否认性等安全需求，对于共享密钥、会话密钥建立过程还应考虑实体鉴别、数据源鉴别、密钥新鲜性、前向安全性等。传感器网络密钥管理机制应具备可扩展性、灵活性、密钥连通性、攻击容忍性。

传感器网络密钥生存周期及密钥管理的一般模型符合附录 A 的规定。

6.2 访问控制

访问控制机制以控制用户对传感器网络的访问为目的，能够防止未授权用户访问传感器网络的结点和数据。访问控制机制可以包括：

a） 自主访问控制

当传感器网络的外部用户需要访问传感器网络的资源时，通过访问控制列表或访问能力列表等策略对用户的访问实施控制的机制。

b） 强制访问控制

为系统中的用户、结点和数据指定敏感标记，以保证每个用户只能访问到那些被标明可以由他访问的资源的一种访问约束机制。

详细描述见附录 B。

6.3 鉴别机制

传感器网络主要针对数据、网络和结点采用相应鉴别技术，可采用传感器网络内部结点之间的鉴别、传感器网络结点对用户的鉴别和传感器网络消息鉴别等机制。

6.4 路由安全

路由安全机制是以保证网络在受到攻击时仍能进行正确的路由发现、构建和维护为目标的安全机制，包括数据保密和鉴别机制、数据完整性和新鲜性校验机制、设备和身份鉴别机制以及路由消息广播鉴别机制等。详细描述见附录 C。

6.5 安全数据融合

安全数据融合机制，以保障数据保密性、数据传输安全、数据融合的准确性为目的，通过加密、安全路由、融合算法的设计、结点间的交互证明、结点采集信息的抽样、采集信息的签名等机制达成。详细描述见附录 D。

6.6 加密机制

见 GB/T 15629.15—2010 中 7.6。

6.7 安全审计机制

安全审计机制对传感器网络中各种与安全有关的事件和行为进行检测、收集、记录和分析，并针对特定事件及行为采取相应行动。其目的是忠实记录传感器网络中发生的一切与安全相关的事件和行为，确保传感器网络按照既定的适当的安全策略进行处理，识别和分析未经授权的动作或攻击，发现网络入侵和违规行为，并将该行为归结到为其负责的实体上。受审计机制制约的安全相关事件包括，但不局限于：敏感数据的访问和非正常改变；安全机制使用记录，如访问权限或能力的授予和删除、主体或目标安全属性的改变；管理操作等。

6.8 帧安全机制

帧安全机制，以实现网络层帧结构的完整性以及网络层帧结构载荷的保密性为目标。网络层帧的安全保护机制应使用国家密码行政主管部门指定的算法。对网络层帧的安全处理方法是通过网络层帧的辅助帧头来指示的。详细描述见附录 E。

6.9 协调器变换的安全机制

协调器变换的安全机制，主要优化协调器变换过程中结点与协调器之间的鉴别和密钥材料的分发过程，为协调器变换提供安全支持。详细描述见附录 F。

7 安全等级划分

7.1 安全等级划分概述

传感器网络的安全等级分为五级，其安全保护能力随着安全等级的提高而逐渐提高。

第一级：本级的传感器网络需要保护的资产价值很低，面临的威胁很小。其安全目标包括：能够确保网络中传输的数据不被无意识地截取、破坏；在网关处可以进行自主访问控制和用户身份鉴别。

第二级：本级的传感器网络需要保护的资产价值较低，面临的威胁较小。本级的安全目标包括：能够进行有效的密钥管理；确保网络中传输的数据不被有意地截取、破坏；确保网络中关键数据的新鲜性；具有一定的抗无线干扰能力；在网关处可以进行自主访问控制和鉴别主体身份；可对传感器网络的安全事件进行审计。

第三级：本级的传感器网络需要保护的资产价值较高，面临的威胁较大。本级的安全目标包括第二级的所有安全目标，此外还提出：实施安全的密钥/密钥材料备份机制以及安全的密钥管理机制；通过维护主体和资源的敏感标记来实施强制访问控制；能够鉴别数据的真实性，并能够保护残留信息的安全性。

第四级：本级的传感器网络需要保护的资产价值很高，面临的威胁很大。本级的安全目标包括第三级的所有安全目标，此外还提出：在密钥管理中提出了密钥的可信产生、共享密钥的前向安全性以及密钥的安全更新；提出将完整性与保密性扩展到所有数据，并能够对完整性遭到破坏的数据进行更正；避免非法主体通过鉴别数据冒充合法主体。

第五级：本级的传感器网络需要保护的资产价值极高，面临的威胁极大。本级别包含第四级的所有安全目标，此外还提出：密钥/密钥材料的备份进行硬件级的保护；被捕获的结点不会对网络造成安全威胁；对每个资源的访问进行控制；采用硬件保护机制保证鉴别数据的安全性。

7.2 安全等级划分方法

传感器网络安全等级划分要考虑的安全功能要素主要包括：数据完整性、数据保密性、数据新鲜性、数据鉴别能力、密钥管理、抗干扰性、访问控制、身份鉴别、客体重用、敏感标记、审计。

传感器网络安全等级划分方法如表 8 所示。

表 8 传感器网络安全等级表

安全等级划分要素	第一级	第二级	第三级	第四级	第五级
数据完整性	+	++	++	+++	+++
数据保密性	+	++	++	+++	+++

表 8（续）

安全等级划分要素	第一级	第二级	第三级	第四级	第五级
数据新鲜性	×	+	+	++	++
数据鉴别	×	×	+	++	++
密钥管理	×	+	++	+++	++++
用户身份鉴别	+	++	+++	++++	+++++
抗干扰性	×	+	++	+++	++++
自主访问控制	+	++	++	++	+++
强制访问控制	×	×	+	+	+
结点鉴别	×	+	++	+++	++++
客体重用	×	×	+	+	++
敏感标记	×	×	+	+	+
审计	×	+	++	++	++
注：“+”表示对安全功能要素的要求，“+”数量的增加表示安全功能要素强度的提高；“×”表示无要求。					

7.3 安全等级划分要求

7.3.1 第一级

7.3.1.1 数据安全要求

7.3.1.1.1 数据完整性

传感器网络采用国家相关标准规定的完整性机制，通过自主完整性策略，能够检测关键数据（如组网数据、关键应用数据）在传输过程中是否被有意地改动和破坏。

7.3.1.1.2 数据保密性

传感器网络应采用一定的安全编码方式，确保关键数据（如组网数据、关键应用数据）在传输的过程中不会意外地泄密。

7.3.1.2 网络安全要求

7.3.1.2.1 用户身份鉴别

当用户需要访问传感器网络的资源时，首先要求用户标识自己的身份，并使用保护机制（例如：口令）来鉴别用户的身份，阻止非授权用户访问用户身份鉴别数据。

7.3.1.2.2 自主访问控制

当传感器网络的用户需要访问传感器网络的资源时，需在网关处实施定义和控制命名用户和传感器网络资源的访问，依据一定的访问控制模型（如访问控制矩阵、取予模型或者动作实体模型）允许命名用户以用户和（或）组的身份规定并控制资源的共享；阻止非授权用户读取敏感信息。

7.3.2 第二级

7.3.2.1 数据安全要求

7.3.2.1.1 数据完整性

同 7.3.1.1.1。

7.3.2.1.2 数据保密性

传感器网络采用国家密码行政主管部门规定的算法，确保关键数据（如组网数据、关键应用数据）在传输过程中不被非法读取。

7.3.2.1.3 数据新鲜性

传感器网络应采用适当的安全机制（如序列号或询问/应答机制）来确保接收方能验证所接收的数据没有被重放。

7.3.2.2 网络安全要求

7.3.2.2.1 密钥管理

传感器网络各类结点的密钥/密钥材料由相应级别的密钥生成中心产生，该产生过程不可预测，相关数据不能被篡改。密钥/密钥材料的预分发应以安全可信的方式进行。

7.3.2.2.2 用户身份鉴别

当用户需要访问传感器网络的资源时，

a) 要求用户标识自己的身份。

b) 使用保护机制（例如：口令或其他鉴别机制）来鉴别用户的身份，阻止非授权用户访问用户身份鉴别数据。

c) 通过为用户提供唯一标识、传感器网络系统能够使用户对自己的行为负责。

d) 传感器网络系统还具备将身份标识与该用户所有可审计行为相关联的能力。

7.3.2.2.3 抗干扰性

传感器网络应采用适当的机制来防止对数据发送、接收和转发的无线干扰，避免对网络的可用性造成严重影响。

7.3.2.2.4 自主访问控制

当传感器网络的外部用户需要访问传感器网络的资源时，

a) 在网关处实施定义和控制命名用户对传感器网络资源的访问，依据一定的访问控制模型（如访问控制矩阵、取予模型或者动作实体模型）允许命名用户以单个用户和（或）组的身份规定并控制资源的共享。

b) 阻止非授权用户读取敏感信息，并控制访问权限扩散。自主访问控制机制根据用户指定方式或默认方式，阻止非授权用户访问资源。访问控制的粒度是单个用户。没有存取权的主体只允许由授权主体指定对传感器网络资源的访问权。

7.3.2.2.5 网络安全审计

当主体需要访问传感器网络的资源时，传感器网络能够创建和维护受保护资源的访问审计跟踪记

录。传感器网络能够创建传感器网络与安全有关的审计跟踪记录。

7.3.2.3 结点安全要求

7.3.2.3.1 结点鉴别

传感器网络应能提供多种安全强度的结点鉴别机制，以确保传感器网络结点间根据不同的安全等级需求采用相应的鉴别机制验证对方身份的真实性和合法性。传感器网络结点鉴别机制是基于密码算法的，具有共享密钥的结点之间能够实现相互鉴别。如，可采用基于简单安全变换的方法实现传感器网络结点间的鉴别。

7.3.2.3.2 结点安全审计

传感器网络结点能够创建和维护受保护资源的访问审计跟踪记录。

7.3.3 第三级

7.3.3.1 数据安全要求

7.3.3.1.1 数据完整性

同 7.3.1.1.1。

7.3.3.1.2 数据保密性

同 7.3.2.1.2。

7.3.3.1.3 数据新鲜性

同 7.3.2.1.3。

7.3.3.1.4 数据鉴别

传感器网络应能提供数据鉴别机制，能产生有效性证据以验证特定传输中的数据内容没有被伪造或者篡改，确保数据内容的真实性。

7.3.3.2 网络安全要求

7.3.3.2.1 密钥管理

密钥管理应满足以下几点：

a) 传感器网络各类结点的密钥/密钥材料由相应级别的密钥生成中心产生，该产生过程不可预测，相关数据不能被篡改。

b) 密钥/密钥材料的预分发应以安全可信的方式进行。应采用加密机制备份密钥/密钥材料。

c) 采用密钥管理机制，确保传感器网络中一定数量的结点被俘获后，泄密的结点密钥不会对当前整个传感器网络的安全性造成严重影响。

d) 确保结点的退出以及新结点的加入不会影响传感器网络的安全性。

e) 应提供适当的密钥销毁方法，保证销毁过程的不可逆。

7.3.3.2.2 用户身份鉴别

同 7.3.2.2.2。

7.3.3.2.3 抗干扰性

同 7.3.2.2.3。

7.3.3.2.4 自主访问控制

同 7.3.2.2.4。

7.3.3.2.5 强制访问控制

传感器网络对所有主体及其所控制的资源实施强制访问控制。为这些主体和资源制定敏感标记。所有主体对资源的访问应满足：

a) 主体的安全级别不高于客体的安全级别时，可执行添加操作。
b) 主体的安全级别不低于客体的安全级别时，可执行修改已有内容操作。
c) 主体的安全级别不低于客体的安全级别时，可执行读操作(表示只读)。
d) 主体的安全级别不低于客体的安全级别时，可执行控制命令操作。
e) 传感器网络使用身份和鉴别数据，鉴别用户的身份，并保证用户创建的传感器网络的主体的安全级和授权受该用户的安全级和授权的控制。

7.3.3.2.6 网络安全审计

当传感器网络的主体需要访问传感器网络的资源时，传感器网络能够创建和维护受保护资源的访问审计跟踪记录，并能阻止非授权的主体对它访问或破坏。传感器网络能够创建传感器网络内部与安全有关的审计跟踪记录。

7.3.3.3 结点安全要求

7.3.3.3.1 结点鉴别

同 7.3.2.3.1。

7.3.3.3.2 客体重用

对于传感器网络中的各类存储体，对其初始指定、分配或再分配一个主体之前，释放该存储体所含的信息以及信息的所有授权。对于一个指定的主体集而言，当其获得对一个已被释放的存储体的访问权时，该存储体中以前的数据内容不再可用。

7.3.3.3.3 敏感标记

传感器网络需要维护与主体及其所访问的资源相关的标记。这些标记是强制访问控制的基础。

7.3.3.3.4 结点安全审计

传感器网络结点能够创建和维护受保护资源的访问审计跟踪记录，并能阻止非授权的主体对它访问或破坏。

7.3.4 第四级

7.3.4.1 数据安全要求

7.3.4.1.1 数据完整性

传感器网络采用国家相关标准规定的完整性机制，通过自主完整性策略和强制完整性策略，能够检

测所有数据以及敏感标记在传输过程中是否被有意地改动和破坏，并提供更正被改动数据的能力。

7.3.4.1.2 数据保密性

传感器网络采用国家密码行政主管部门规定的算法，确保所有数据在传输过程中不被非法读取。

7.3.4.1.3 数据新鲜性

同 7.3.2.1.3。

7.3.4.1.4 数据鉴别

传感器网络应能提供数据鉴别机制，能产生包含数据产生者身份的有效性证据以验证特定传输中的数据内容没有被伪造或者篡改，确保数据内容的真实性。

7.3.4.2 网络安全要求

7.3.4.2.1 密钥管理

密钥管理应满足以下几点：

a) 传感器网络各类结点的密钥/密钥材料由相应级别的密钥生成中心产生，该产生过程不可预测，相关数据不能被篡改。
b) 密钥/密钥材料的预分发应以安全可信的方式进行。应采用加密机制备份密钥/密钥材料。
c) 采用密钥管理机制，确保传感器网络中一定数量的结点被俘获后，泄密的结点密钥不会对当前整个传感器网络的安全性造成严重影响。且不会影响有关结点在前一个阶段建立的共享密钥的安全性。
d) 确保结点的退出以及新结点的加入不会影响传感器网络的安全性。在进行密钥更新时，应确保新密钥在传输过程中的保密性和完整性。
e) 应提供适当的密钥销毁方法，保证销毁过程的不可逆。

7.3.4.2.2 用户身份鉴别

当用户需要访问传感器网络的资源时，

a) 要求用户标识自己的身份。
b) 传感器网络系统维护用户身份识别数据并确定用户访问权及授权数据，并使用保护机制（例如：口令或其他鉴别机制）来鉴别主体的身份，阻止非授权主体访问主体身份鉴别数据。保证鉴别数据的安全性，避免非法主体利用鉴别数据冒充合法主体。
c) 通过为主体提供唯一标识、传感器网络系统能够使主体对自己的行为负责。
d) 传感器网络系统还具备将身份标识与该主体所有可审计行为相关联的能力。

7.3.4.2.3 抗干扰性

传感器网络应采用适当的机制来防止对数据发送、接收和转发的无线干扰，避免对网络的可用性造成一定的影响。

7.3.4.2.4 自主访问控制

同 7.3.2.2.4。

7.3.4.2.5 强制访问控制

同 7.3.3.2.5。

7.3.4.2.6 网络安全审计

同 7.3.3.2.6。

7.3.4.3 结点安全要求

7.3.4.3.1 结点鉴别

传感器网络应能提供多种安全强度的结点鉴别机制，以确保传感器网络结点间根据不同的安全等级需求采用相应的鉴别机制验证对方身份的真实性和合法性。传感器网络结点鉴别机制是基于密码算法的，具有共享密钥的结点之间能够实现相互鉴别。如，可采用基于对称密码算法实现传感器网络结点间的鉴别。

7.3.4.3.2 客体重用

同 7.3.3.3.2。

7.3.4.3.3 敏感标记

同 7.3.3.3.3。

7.3.4.3.4 结点安全审计

同 7.3.3.3.4。

7.3.5 第五级

7.3.5.1 数据安全要求

7.3.5.1.1 数据完整性

同 7.3.4.1.1。

7.3.5.1.2 数据保密性

传感器网络采用国家密码行政主管部门规定的算法，确保所有数据在传输和存储过程中不被非法读取。

7.3.5.1.3 数据新鲜性

同 7.3.4.1.3。

7.3.5.1.4 数据鉴别

同 7.3.4.1.4。

7.3.5.2 网络安全要求

7.3.5.2.1 密钥管理

密钥管理应满足以下几点：

a) 传感器网络各类结点的密钥/密钥材料由相应级别的密钥生成中心使用硬件密码设备产生，该产生过程不可预测，相关数据不能被篡改；

b) 密钥/密钥材料的预分发应以安全可信的方式进行。密钥/密钥材料的备份应采用国家密码行

政主管部门认可的硬件密码设备采用加密的方法实施；

c) 采用密钥管理机制及其他机制(如硬件防窜扰机制)，确保传感器网络中任意数量的结点被捕获后，泄密的结点密钥不会对当前整个传感器网络的安全性造成影响，且不会影响有关结点在前一个阶段建立的共享密钥的安全性；

d) 确保结点的退出以及新结点的加入不会影响传感器网络的安全性；在进行密钥更新时，应确保新密钥在传输过程中的保密性和完整性；

e) 应提供适当的密钥销毁方法，保证旧密钥销毁过程的不可逆。

7.3.5.2.2 用户身份鉴别

同 7.3.4.2.2。

7.3.5.2.3 抗干扰性

传感器网络应采用适当的机制来防止对数据发送、接收和转发的无线干扰，以确保对网络的可用性造成的影响降至最低。

7.3.5.2.4 自主访问控制

同 7.3.2.2.4。

7.3.5.2.5 强制访问控制

同 7.3.3.2.5。

7.3.5.2.6 网络安全审计

同 7.3.3.2.6。

7.3.5.3 结点安全要求

7.3.5.3.1 结点鉴别

传感器网络应能提供多种安全强度的结点鉴别机制，以确保传感器网络结点间根据不同的安全等级需求采用相应的鉴别机制验证对方身份的真实性和合法性。如，可采用基于非对称密码算法，利用数字签名技术实现传感器网络结点间的鉴别。

7.3.5.3.2 客体重用

同 7.3.3.3.2。

7.3.5.3.3 敏感标记

同 7.3.3.3.3。

7.3.5.3.4 结点安全审计

同 7.3.3.3.4。

附 录 A
（资料性附录）
密 钥 管 理

A.1 概述

密钥管理机制依赖于基本的密码机制，分为以下三类：

a） 采用对称密码技术的机制；

b） 采用非对称密码技术的机制；

c） 采用对称、非对称技术结合的机制。

不用的机制适用于不同的应用需求。采用对称密码技术的机制，适用于对安全级别要求较低的传感器网络，例如安全级别在三级以下的传感器网络宜采用基于对称密码技术的机制。而对于安全级别要求较高的传感器网络，则需要采用基于非对称密码技术的机制。

A.2 密钥生存周期

一个密钥从产生到销毁要经历一系列的状态，这些状态确定了其生存周期。三种主要的状态是：

a） 待激活：在待激活状态，密钥已产生好但并未激活供使用；

b） 激活：在激活状态，密钥用于按密码技术处理信息；

c） 次激活：若已知某个密钥已被泄露，应马上变为本状态，此时密钥将只用于解密或验证。

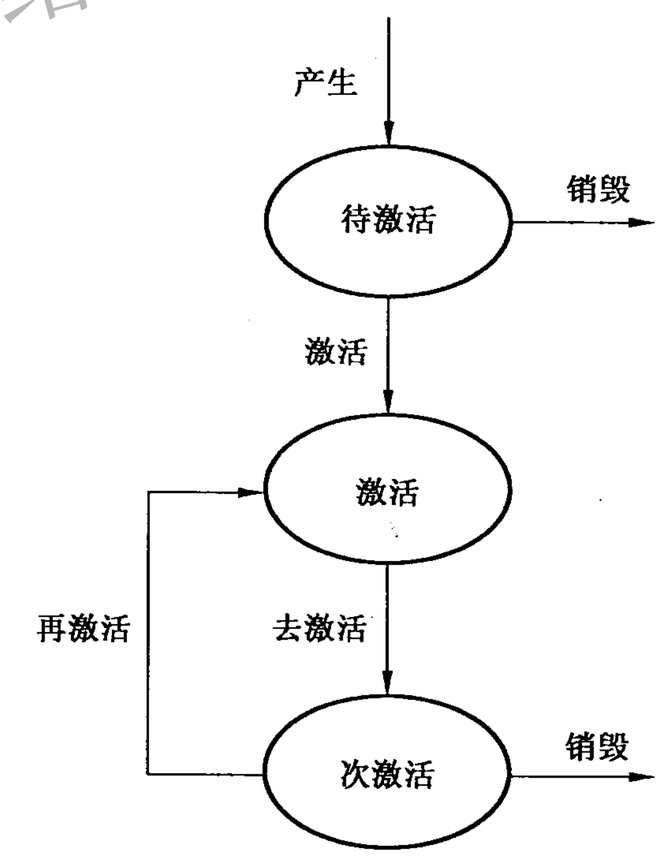

图 A.1 密钥生存周期

图 A.1 表示密钥生存期的一般模型，表明上述状态和相应的转移。密钥由一种状态向另一种状态变化时，经历图 A.1 所示的下述转移：

产生是指产生密钥的过程，应根据指定的密钥产生规则进行；激活是使密钥生效，以便进行密码运算；次激活是限制密钥的使用，在密钥已过期或已被撤消的情况下执行该过程；再激活是使一个次激活密钥可重新用于密码运算；销毁是终止密钥的生存期，应是不可逆的，包括密钥的逻辑销毁，也可能包括物理销毁。

传感器网络密钥管理机制涉及到不同类型的密钥：密钥材料、共享密钥（包括直接密钥和路径密钥）、会话密钥。每种密钥从建立到撤销的整个有效期之内，可能会处在多个不同阶段，需要根据具体应用需求对密钥进行维护和更新。不同的密钥类型生存期的长短不同，在同一个密钥材料的有效期内，共享密钥可能撤销和更新多次；在同一个共享密钥的有效期内，会话密钥可能撤销和更新多次。

会话密钥在通信双方结点通信完成后即被销毁。会话密钥的泄露不能影响到共享密钥的安全。若某个共享密钥泄露，则可信第三方将其撤销，并与相关结点交互，分发更新的密钥。共享密钥的泄露并不意味着密钥材料的泄露。但是若某个密钥材料泄露，则相应的共享密钥也必须撤销，并在密钥材料更新后，重新建立共享密钥。

A.3 采用对称技术的机制

传感器网络可信第三方对网络中的对称密钥进行管理。

a) 密钥产生

由于传感器网络独有的特点，传统的密钥管理机制不能直接应用。例如传感器网络中结点资源严格受限，要求必须采用轻量级的密钥管理机制；无固定基础设施，导致安全通信不能依赖于固定的基础设施或者一个信任中心来实现，而要采用分布式密匙管理技术或者层次式密钥管理技术。

分布式密匙管理中，所有结点具有相同的通信能力和计算能力。推荐采用基于密钥预分配的机制，例如基于密钥池的密钥预分配、基于多项式池的密钥预分配等。结点密钥的协商、更新通过预分配的密钥材料和相互协作来完成。

密钥产生是传感器网络可信第三方以安全的方式为结点产生预分配的密钥材料的过程，该产生过程不会被篡改，产生方式不可预测。

b) 密钥登记

密钥登记将结点密钥材料与结点标识相关联。这由登记机构提供，可以是可信第三方。登记机构以安全的方式存储密钥及其相关信息的记录。该部分是可选的。

c) 密钥分发

无线传感设备在安装于现场之前，应该根据实际需求向设备写入相应的初始密钥材料。可以通过可信第三方直接配置给设备，或者通过手持设备进行分发。

d) 密钥安装

无线传感设备以保护密钥不被泄露的方式写入可信第三方分发的密钥材料。

e) 共享密钥建立

1) 直接密钥建立

这种通信连接的模型如图 A.2 所示（图中数字代表交换的步骤）：

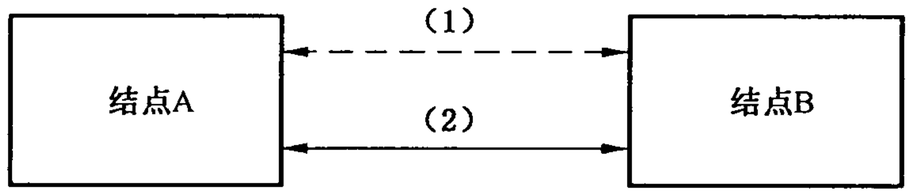

图 A.2 直接密钥建立模型

若结点设备中写入的初始密钥材料即为其与邻居结点间共享的直接密钥，且结点知道密钥是与哪个结点所共享，则直接密钥发现(1)跳过，可直接转入会话密钥建立(2)。

若结点设备中写入的初始密钥材料即为其与邻居结点间共享的直接密钥，但是结点并不确切知道对应的共享结点，则需要直接密钥发现过程(1)。直接密钥发现与接下来的会话

密钥建立可以合并到一个协议中。

2) 路径密钥建立

在没有直接密钥的情况下，若一对结点之间存在多跳安全连接，则可以建立路径密钥。除去安全路径发现过程外，路径密钥建立是一个有可信第三方参与的密钥建立过程，需采用下述图 A.3 和图 A.4 中模型。可信第三方可能是两结点共同的邻居结点，簇头结点或者 BS 等。

图 A.3 中可信第三方可能是通信双方结点共同的邻居结点、簇头结点(通信双方结点均在该簇内)或者 BS。

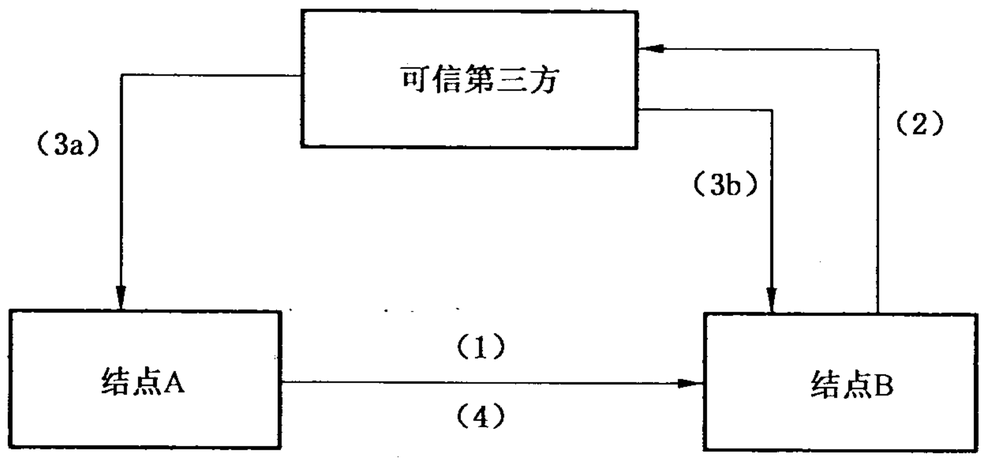

图 A.3 路径密钥建立 1

图 A.4 中模型给出了当通信双方结点之间的安全路径上有两个结点时，或者通信双方位于不同的簇内时，密钥建立的模型。

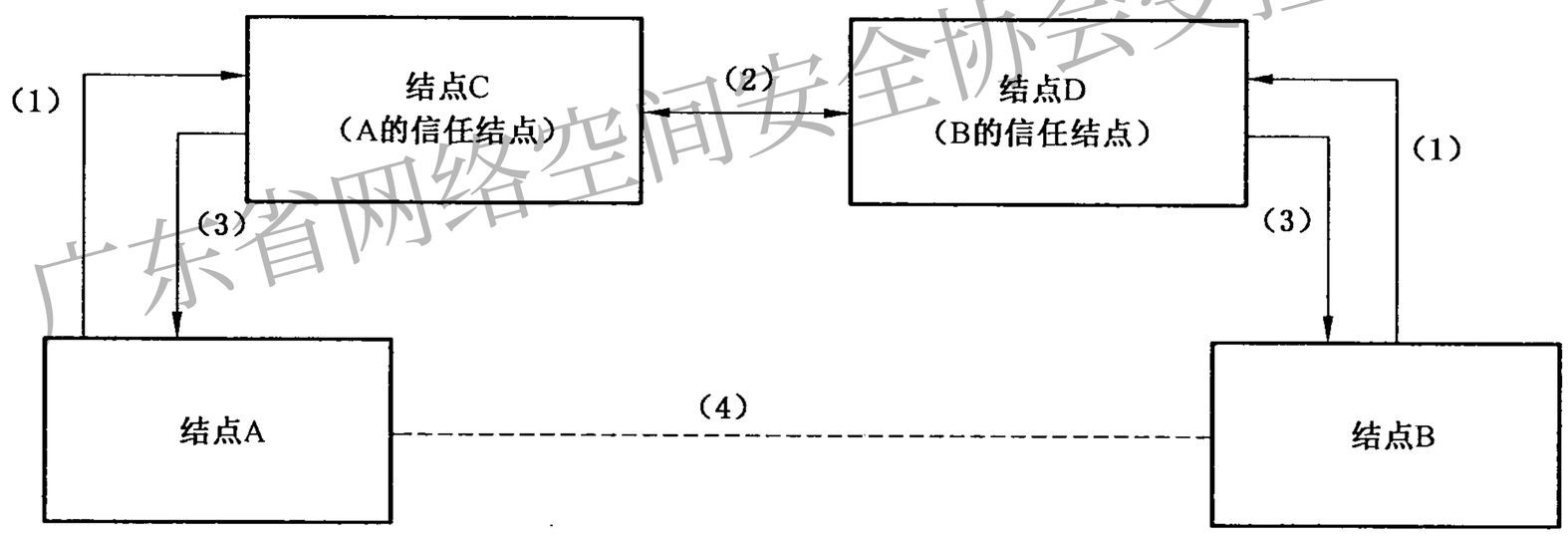

图 A.4 路径密钥建立 2

图 A.4 中结点 C 与结点 D 之间互相信任。二者可以共同协商出一个供结点 A 和结点 B 使用的共享密钥；也可以其中一个做为密钥分发中心，另一个转发消息。

若结点 A 信任的结点集，与结点 B 信任的结点集之间仍然没有安全连接，则查找结点 C 与结点 D 共同的信任结点 X。再由结点 X 产生会话密钥，分发给 C 和 D，再分别分发给 A 和 B。由于传感器网络中距离较远的结点不会需要建立安全链路，所以由此产生的信任链长度是可以接受的。路径密钥建立与会话密钥建立也可以合并到一个协议当中。

f) 密钥更新

密钥材料有一定的生存周期，当需要更新时，可信第三方重新选定密钥材料，然后利用密钥加密密钥对其加密后再分发给整个无线传感器网络中的相应结点。结点接收到密钥信息后，用自己的密钥加密密钥解密，并且更新自身密钥信息。

更新的密钥应确保是可信第三方真实合法的产生，并及时发送到提出更新请求的结点，可能还包括其对等结点。

g) 密钥撤销

在结点正常的密钥更新之后，可信第三方将撤销所有过期的密钥。当发现密钥的安全受到威

胁、密钥已经泄漏等情况时，可信第三方也可以在密钥未过期之前，强制撤销某个密钥。可信第三方应将撤销通知包括密钥标识、撤销的日期时间、撤销的原因等发布给相关结点。

若发现某个结点为恶意结点，可信第三方有权利删除该结点，撤销该结点的密钥材料。其余结点若发现自己正在使用相关密钥材料，则向可信第三方申请更新。

h) 密钥注销

若选择了密钥登记，则密钥注销是必须的，由登记机构解除密钥与结点的关系。

i) 会话密钥建立

通信双方结点在共享密钥的基础上，可采用图 A.2 中的模型进行会话密钥的建立。

A.4 采用非对称技术的机制

传感器网络中可信第三方对网络中的非对称密钥进行管理。

a) 密钥产生

传感器网络可信第三方使用某种密码算法以安全的方式为结点产生公私钥对，该产生过程不会被篡改，产生方式不可预测。

b) 密钥证书生成

认证机构接受密钥的认证请求后签发密钥证书，确保公开密钥与结点的联系。该部分是可选内容，例如，在基于 ID-PKC 的密钥管理机制中无该部分内容。

c) 密钥分发

无线传感设备在安装于现场之前，应该根据实际需求向设备写入自己的私有密钥和公开密钥(证书)。可以通过可信第三方直接配置给设备，或者通过手持设备进行分发。

d) 密钥安装

无线传感设备以保护密钥不被泄露的方式写入可信第三方分发的密钥。

e) 会话密钥建立

基于非对称技术的密钥管理机制中，任意两个结点之间可以进行密钥协商(1)建立会话密钥，其通信连接的模型如图 A.5 所示：

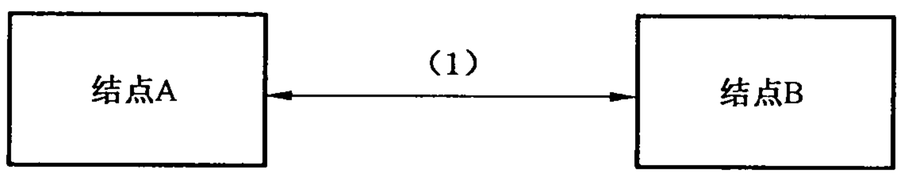

图 A.5 基于非对称技术的会话密钥建立

若采用基于证书的密钥管理机制，则必须提供高效的证书验证方案，例如利用 Merkel tree 等。

f) 密钥更新

公开密钥证书有一定的生命期，是在证书中或是由认证机构定义的一个有效期限。在公开密钥证书即将到期之前，需要进行证书更新。可信第三方撤销结点的到期证书，重新签发。

g) 密钥撤销

当结点私有密钥的损坏、结点请求撤销、结点被损坏等情况发生时，应具有一定的程序和快速的通信方法能安全地撤消结点公开密钥(证书)。当结点私有密钥因为某种原因而被撤销时，所有有关的公开密钥(证书)也必须被撤销。撤销机制要考虑传感器网络结点资源受限和无固定基础设施的特点，不推荐撤销列表的方法。

附 录 B
（资料性附录）
访问控制机制

B.1 概述

访问控制的目的是为了控制用户对传感器网络资源的访问，防止非法用户访问传感器网络的结点资源和数据资源。为了实现传感器网络的访问控制，可能需要其他安全机制的参与，如：敏感标记、鉴别、数据保密性、数据完整性。

B.2 自主访问控制

自主访问控制在网关实施，访问控制策略由网络管理员在网关进行制定，策略可通过访问控制表与访问能力表两种方式实现。为了实现自主访问控制，网关需要满足：能够对访问者的身份进行鉴别；能够标识传感器网络内的各设备；能够制定访问控制策略并实施访问控制三个条件。

在这种访问控制机制中，访问者启动访问过程，由网关对访问进行控制。控制模型如图 B.1 所示。

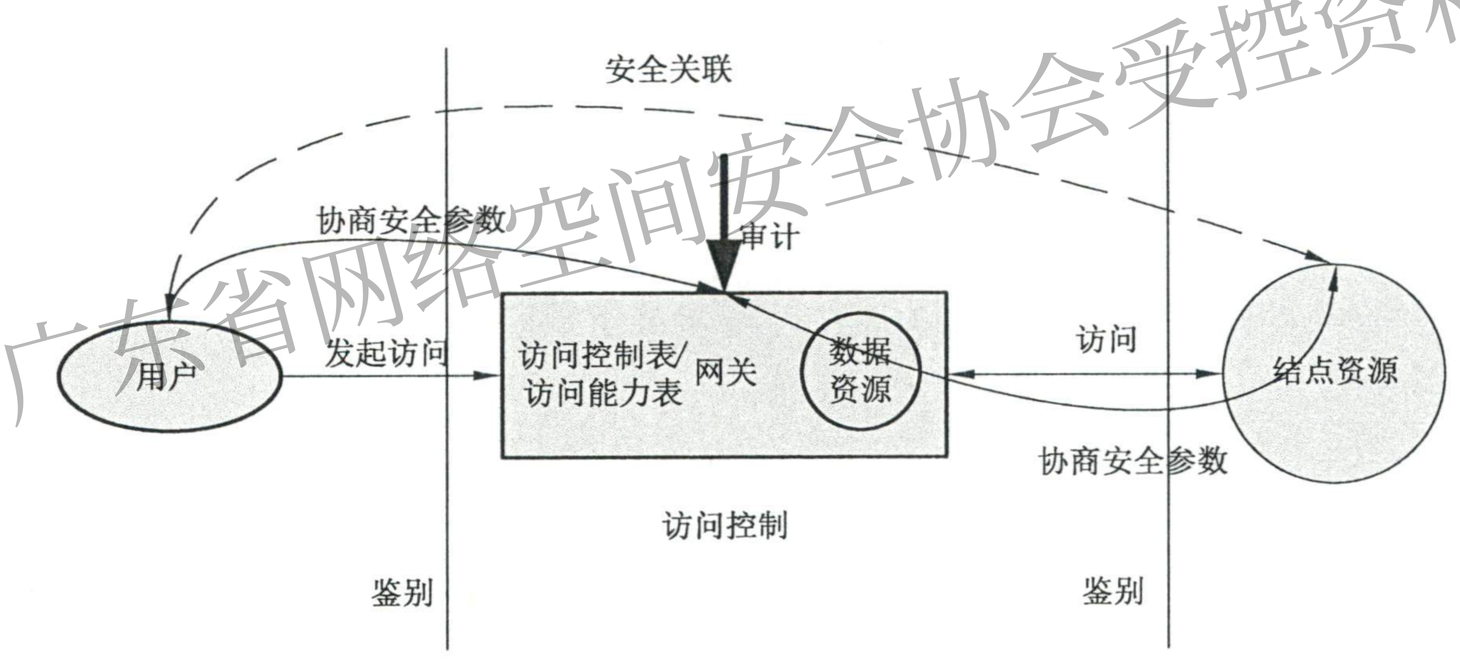

图 B.1 自主访问控制参考模型

B.2.1 访问控制策略

自主访问控制策略可由两种方式实现：访问控制表、访问能力表。

a) 在通过访问控制表进行访问控制时，网关需制定访问控制表，明确指明网内的每种设备可由哪些用户访问，以及进行何种类型的访问（读取、发送控制命令）；

b) 在通过访问能力表进行的访问控制中，网关需制定访问能力表，明确指明每个合法用户能够访问哪些设备资源，以及进行何种类型的访问（读取、发送控制命令）。

B.2.2 访问控制方式

访问控制方式可分为基于用户身份的访问、基于组的访问及基于角色的访问。

a) 在高级别安全中，如果明确指出细粒度的访问控制，那么需要基于每个用户进行访问控制。

b) 否则，为了简化访问控制表，提高访问控制的效率，在各种安全级别的自主访问控制模型中，均可通过用户组和用户身份相结合的形式进行访问控制。

c) 为了实现灵活的访问控制，可以将自主访问控制与角色相结合，实施基于角色的访问控制，这便于实现角色的继承。

为了保证安全性，在基于用户身份和用户组的访问控制中，应避免访问权限的传递性。

B.2.3 访问控制对象

对访问实施控制的对象包括数据和传感器网络的结点设备。

a) 对于数据的访问，假设传感器网络已将数据集中到网关处，这种访问事实上是对网关数据的访问。在这种访问控制中，网关需明确标识出不同类别和不同用途的数据，并制定相应的访问控制表/访问能力表。

b) 对于传感器网络设备的访问，网关需明确标识出每个传感结点，并在网关处设置访问控制表/访问能力表。同时，为了确保这种访问不被非法利用，需通过网关为用户和传感设备之间建立安全关联，提供访问的鉴别、数据的保密性与完整性。

B.3 强制访问控制

为了实施强制访问控制，传感器网络系统需能够按照统一的安全策略对用户和被访问的资源设置安全标记，以表明安全级别。根据应用场景的不同，强制访问控制可以在网关处实施，也可以在被访问的设备上实施。

在这种访问控制机制中，访问者启动访问过程，由网关对访问进行控制。控制模型如图 B.2 所示。

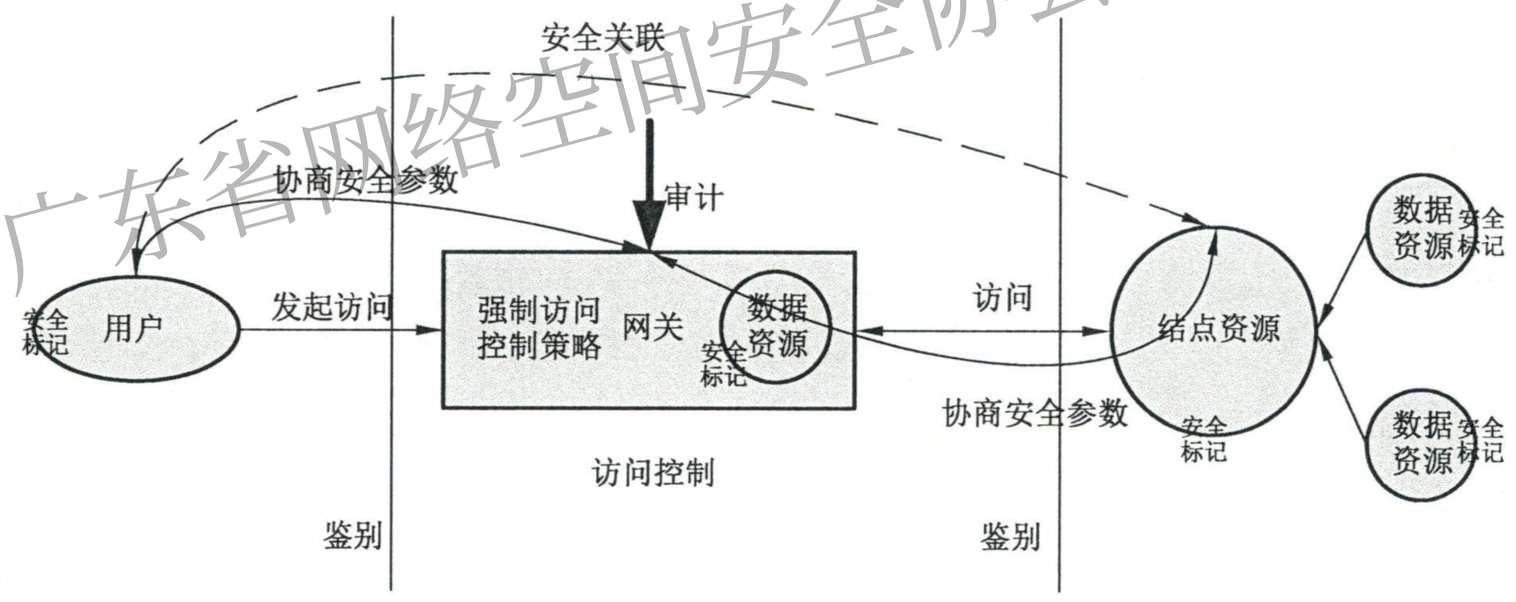

图 B.2 强制访问控制参考模型

B.3.1 访问控制策略

主体在访问传感器网络的资源时，其操作分为：只读、改写或删除已有数据、添加数据和发送控制命令四类。

强制访问控制的策略如下：当主体的安全级别不高于客体的安全级别时，可执行添加操作；当主体的安全级别不高于客体的安全级别时，可执行改写或删除自己数据的操作；主体的安全级别不低于客体的安全级别时，可执行只读操作；当主体的安全级别不低于客体的安全级别时，可执行发送控制命令操作。

B.3.2 访问控制方式

根据不同的应用场景，强制访问控制可基于单个用户、用户组和角色进行实施，即为不同的用户、用户组或角色设置不同安全级别的标记，根据这些标记实施强制访问控制。

B.3.3 访问控制对象

B.3.3.1 在网关处实施访问控制

传感器网络系统需对用户和被访问的资源进行安全分级，并打上安全标记，然后在网关处实施强制访问控制。网关的资源分为两种：数据资源、结点资源。

B.3.3.1.1 数据资源：假设传感器网络数据集中在网关处，且已进行安全分级，则通过强制访问控制策略实施访问控制。

B.3.3.1.2 结点资源：假设传感器网络结点处于网关后面，可由网关实施强制访问控制。首先将结点设备进行安全分级，然后按照强制访问控制策略实施访问控制。为了确保这种访问不被攻击，网关需为结点和用户建立安全关联，确保访问的鉴别性、数据的保密性与完整性。

B.3.3.2 在结点处实施访问控制

传感器网络系统需对用户和被访问的资源进行安全分级，并打上安全标记，然后在结点处实施强制访问控制。结点实施强制访问控制的前提：结点能够识别用户的安全标记，并能通过比较决定是否为用户提供访问，且网关需为结点和用户建立安全关联，确保访问数据的保密性和完整性。结点的资源为结点本身和结点的数据。

B.3.3.2.1 结点本身的访问控制

结点能够通过简单的鉴别机制识别合法用户，并根据自身的安全级别和用户的安全级别决定是否接受用户的访问(数据的读写、发送控制命令)。这种控制中，结点数据的安全级别与结点的安全级别相同。

B.3.3.2.2 结点数据的访问

在这种访问控制中，传感结点可挂接多个传感器，且不同传感器的数据有不同的安全级别。传感器网络系统预设各类型传感数据的安全级别。结点根据比较自身不同类别数据的安全级别以及用户的安全级别，来实施强制访问控制。

注：在实际操作中，可将自主访问控制与强制访问控制相结合，如根据知其所需原则，可实施如下的访问控制：在网关处实施自主访问控制，在结点处实施强制访问控制。

B.4 低开销访问控制机制

该机制是一种不需要传感器网络中的其他结点参与认证过程的、低开销的传感器网络访问控制机制。

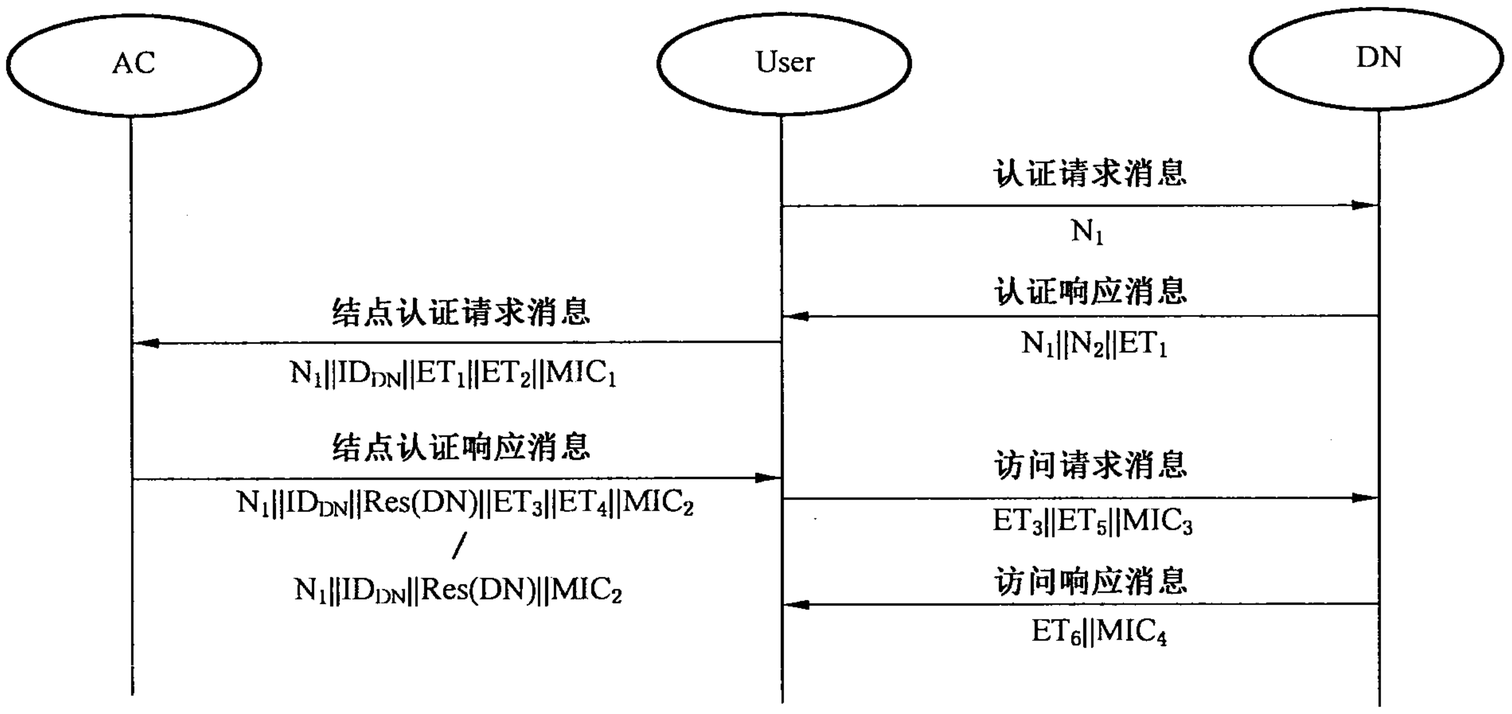

图 B.3　低开销访问控制机制

如图 B.3 所示，图中 AC 是访问控制器；User 是用户；DN 是目的访问结点。以 User 访问 DN 为例，具体的访问控制过程如下：

a) User 在向传感器网络中的 DN 发送访问请求之前，首先向传感器网络中的 DN 发送认证请求消息，该消息中主要包含 User 产生的询问 N_1；

b) DN 收到 User 的认证请求消息后，产生询问 N_2，并利用与 AC 之间的共享密钥 KAC，DN 计算 $ET_1=E(KAC,DN,N_1)$，将 $N_1||N_2||ET_1$ 作为认证响应消息发送给 User，其中，E 为对称加密算法；

c) User 收到 DN 的用户认证响应消息后，首先判断消息中的询问 N_1 是否是 User 选择的询问，若不是，直接丢弃该响应消息；若是，则利用与 AC 之间的共享密钥 KAC，User 计算 $ET_2=E(KAC,User,N_1)$，计算消息鉴别码 $MIC_1=H(KAC,User,N_1||ID_{DN}||ET_1||ET_2)$，构造结点认证请求消息 $N_1||ID_{DN}||ET_1||ET_2||MIC_1$ 发送给 AC，其中，ID_{DN} 是 DN 的身份标识，H 为单向哈希函数，E 为对称加密算法；

d) AC 收到 User 的结点认证请求消息后，首先根据 MIC_1 判断消息的完整性，若不完整，丢弃该消息；若完整，利用与 DN 之间的共享密钥 KAC，DN 解密 ET_1，若解密后得到的 N_1 与 User 在步骤 3)中发送的 N_1 不相等，AC 构造结点认证响应消息 $N_1||ID_{DN}||Res(DN)||MIC_2$ 发送给 User，其中，$Res(DN)=Failure$，表示 AC 对 DN 鉴别失败，其中 $MIC_2=H(KAC,User,N_1||ID_{DN}||Res(DN))$；若解密后得到的 N_1 与 User 在步骤 3)中发送的 N_1 相等，AC 利用与 User 共享的密钥 KAC，User 解密 ET_2，若解密后得到的 N_1 与 User 在步骤 3)中发送的 N_1 不相等，终止鉴别；若解密后得到的 N_1 与 User 在步骤 3)中发送的 N_1 相等，AC 生成 User 和 DN 间的会话密钥 KDN，User，并根据 User 的身份标识查询 ACL，获得 User 的访问控制信息 ACLUser，连同 User 的访问期限 Tv，利用 KAC，DN 计算 $ET_3=E(KAC,DN,IDUser||KDN,User||TV||ACLUser)$，并利用 KAC，User 计算 $ET_4=E(KAC,User,KDN,User)$，计算消息鉴别码 $MIC_2=H(KAC,User,N_1||ID_{DN}||Res(DN)||ET_3||ET_4)$，构造结点认证响应消息 $N_1||ID_{DN}||Res(DN)||ET_3||ET_4||MIC_2$ 发送给 User，其中，$Res(DN)=True$ 表示 AC 对 DN 鉴别成功，ID_{DN} 是 DN 的身份标识，H 为单向哈希函数，E 为对称加密算法；

e) User 收到 AC 的结点认证响应消息后，首先判断询问 N_1 是否是 User 选择的询问，若不是，丢弃该响应消息；若是，根据 MIC_2 判断消息的完整性；若不完整，丢弃该消息；若完整，User 根据 Res(DN)判断 DN 的合法性，若 $Res(DN)=Failure$，表示 DN 非法，User 终止访问；若 $Res(DN)=True$，User 解密消息中的 ET_4，产生询问 N_3，连同 DN 的询问 N_2 以及 User 的访问请求 QUser 利用刚才解密后获得的、与目的访问结点间的会话密钥 KDN，User 计算 $ET_5=$

E(KDN,User,N_2||N_3||QUser)，计算消息鉴别码 MIC_3=H(KDN,User,ET_3||ET_5)，构造访问请求消息 ET_3||ET_5||MIC_3 发送给 DN，其中，H 为单向哈希函数，E 为对称加密算法；

f) DN 收到 User 的访问请求后，首先解密 ET_3，获得会话密钥 KDN,User，根据 MIC_3 判断消息完整性，若不完整，终止访问；若完整，利用 KDN,User 解密 ET_5，判断解密后得到的询问 N_2 是否 DN 选择的询问 N_2，若不是，终止访问；若是，再确认解密 ET_5 后获得的 IDUser 是否请求访问的 User 的身份标识，若不是，终止访问；若是，记录当前时刻 TC，从 TC 到(TC+TV)这段时间即为 User 的访问有效期，用户只能在此有效期内访问网络数据，DN 根据 ACLUser 判断 User 的访问请求 QUser 是否合法，若不合法，终止访问；若合法，生成应答数据 RDN，连同 N_3 利用 KDN,User 计算 ET_6=E(KDN,User,N_3||RDN)，计算消息鉴别码 MIC_4=H(KDN,User,ET_6)，构造访问请求响应消息 ET_6||MIC_4 发送给 User，其中，H 为单向哈希函数，E 为对称加密算法；

g) User 收到请求响应消息后，首先根据 MIC_4 判断消息完整性，若不完整，丢弃该消息；若完整，利用 KDN,User 解密 ET_6，判断解密得到的询问 N_3 是否是 User 选择的询问 N_3，若不是，丢弃该消息；若是，User 保存应答数据 RDN，后续 User 与 DN 之间的访问请求和应答数据均利用 KDN,User 加以保护。

B.5 移动用户访问控制机制

本机制是一种既适用于传感器网络对移动用户的访问控制也适用于对静止用户的访问控制的传感器网络访问控制机制。该机制适用于移动用户的传感器网络访问控制。

下述 ACS 表示访问控制服务器，ACL 表示访问控制列表。

a) ACS 构造 ACL 以及用户身份信息，并在用户访问网络之前进行协议初始化。

1) ACS 构造 ACL，该 ACL 包括 U_ID 字段、ADT 字段、VP 字段、AI 字段，其中：

U_ID 字段：用户的身份标识；

ADT 字段：用户被授权访问的数据类型；

VP 字段：用户被授权访问网络的期限；

AI 字段：用于认证用户身份的认证依据。

在构造 ACL 后，ACS 对用户进行注册，注册过程如下：ACS 根据网络用户的身份标识 U_ID 确定该用户能够访问的网络数据类型 ADT 和访问期限 VP，构造该用户的身份证明以及用于认证该身份证明的认证依据 AI，并将 U_ID、ADT、VP、AI 作为新条目字段插入 ACL 列表中，记做 ACLU_ID；

2) 用户访问传感器网络之前，先向 ACS 发送身份证明请求信息；收到身份证明请求信息后，如果该用户已注册，ACS 将事先为该用户构造的身份证明发送给该用户，并将 ACL 列表中与该用户 U_ID 对应的、包括 ADT、VP、AI 用户访问控制信息的 ACLU_ID 以认证的方式发送给所有网络结点，结点在用户的有效期 VP 之前保存这些信息；如果用户未注册，ACS 直接丢弃用户的身份证明请求信息。

b) 用户访问网络时，由网络中用户的单跳通信区域内的所有结点构成临时访问控制网关对用户进行认证，用户认证成功后，通过预测用户将要到达的位置，将认证成功的消息扩散到用户的下一个临时访问控制网关中的结点。

1) 用户访问网络时，由传感器网络中用户的单跳通信区域内的所有结点构成临时访问控制网关对用户进行访问控制，临时访问控制网关根据用户的移动不断变化；用户向临时访问控制网关发送自己的身份证明，收到用户的身份证明后，临时访问控制网关中的所有结点先判断是否保存有与该用户对应的 ACLU_ID 信息，如果存有该信息，表明该用户处于有

效期内，根据 ACLU_ID 中的用户 AI 信息对用户的身份证明进行认证，如果认证成功，则投 PASS 票，并向临时访问控制网关内的所有结点间进行广播，如果网关中的结点收到的 PASS 票数等于或超过一个阈值 P，则表示用户认证成功，其中该阈值 P 由网络所有者自定义；如果用户不在有效期内、或用户在有效期内但身份认证失败、或用户在有效期内且身份认证成功但 PASS 票数低于阈值 P，均表示认证失败，网络终止该用户的访问；

2) 认证成功后，临时访问控制网关中的结点根据用户的运动方向、运动速度等对 t 时间后用户将要到达的位置进行预算，并在时间 t 后根据位置预算结果将用户认证成功的消息发送给下一个临时访问控制网关，即当前临时访问控制网关内的结点；如果用户仍处于有效期 VP 内，则当前临时访问控制网关仍然承认用户的合法性，并在经过时间 t 后，将认证成功消息发送到下一个目标区域，即临时访问控制网关内；在用户访问网络的整个过程中，临时访问控制网关中的结点不断的根据用户的运动方向、运动速度等对用户将要到达的位置进行预算，并将用户认证成功的消息扩散到用户将要到达的位置；认证成功消息利用结点间预设的安全通道在网络中进行传输。

c) 临时访问控制网关对用户的访问进行授权管理。

1) 用户获得认证后，用户将访问请求 Q 连同用户的 U_ID 以安全的方式发送给临时访问控制网关中的结点；

2) 临时访问控制网关内的结点收到用户的访问请求 Q 后，首先判断用户是否处于有效期，如果处于有效期，根据 ADT 信息判断用户访问请求 Q 的合法性，如果合法，则将访问请求 Q 连同用户的 U_ID 以安全的方式发送给用户的目的访问结点，目的访问结点是传感器网络中的任意结点，该结点将始终认为由临时访问控制网关转发的访问请求 Q 是合法的，并将根据访问请求 Q 做出响应，授权过程结束；如果用户不在有效期内、或用户在有效期内但访问请求 Q 不合法，结点将直接丢弃用户的访问请求 Q，终止该用户的访问。

附 录 C
（资料性附录）
路 由 安 全

C.1 路由发现消息安全

路由发现消息安全，根据安全级别设置，利用数据保密和鉴别机制、数据完整性和新鲜性校验机制，防止路由消息被假冒，识别伪造或被篡改的路由消息。主要包括路由请求消息和路由响应消息的保密性、完整性等。具体见附录 E 中网络层流出帧和流入帧处理。

C.2 路由器和结点鉴别

路由器和结点鉴别实现路由发现过程中路由器和结点之间的相互鉴别。见表 C.1 标识符请求命令帧和标识符响应命令帧，及表 C.2 的路由请求设备和路由器之间是否需要进行鉴别的标识。

表 C.1 网络命令帧

命令帧标识符	命令名称	子章节
0x0f	标识符请求命令帧	D.2.1
0x10	标识符响应命令帧	D.2.2
0x11-0xff	保留	—

表 C.2 网络信息库(NIB,Network Information Base)

属性	ID	类型	只读	范围	描述	默认
nwkRouterAuthen	0xab	布尔	No	TURE 或 FALSE	该值为 TRUE，请求路由的设备需要鉴别所要选择的路由器；接收路由请求的路由器需要鉴别发起路由请求的设备。 该值为 FALSE，则不需要进行鉴别操作。	FALSE

C.2.1 设备标识符请求命令帧

路由器或者设备，使用设备标识符请求命令帧请求指定设备的标识符。设备标识符请求命令帧的负载应按图 C.1 所示的格式编排。

八位位组:1	1	2/8	0/2/8
命令标识	请求类型	请求设备地址	待鉴别设备地址

图 C.1 设备标识符请求命令格式

C.2.1.1 MAC 数据服务请求

为了使用 GB/T 15629.15—2010 定义的 MAC 数据服务发送这个命令，应提供以下信息：

a) 目的 MAC 地址和 PAN 标识符应根据请求类型分别设置为相应的设备的网络地址或者相应组的多播地址，和相应设备或者组所在的 PAN 标识符。

b) 源 MAC 地址和 PAN 标识符应设置为发送设备标识符请求命令帧的设备的网络地址和 PAN 标识符。

c) 帧控制字段应指示该帧是一个 MAC 数据帧，并且，由于网络层发出的任何安全帧都应使用网络层安全，帧控制字段的 MAC 安全子字段设置为禁用。

d) 寻址模式和 intra-PAN 标志应设置为支持这里描述的寻址字段。

C.2.1.2 网络层头字段

设备标识符请求命令通过单播或组播的方式发送，网络层头字段应设置如下：

a) 源地址字段应设置为命令帧发起设备的 16 位网络地址。

b) 帧控制字段的源地址字段应设置为 1，网络层头的源地址字段应存在，包含帧发起设备的 64 位地址。

c) 目的地址字段应根据请求类型设置为相应的命令帧接收设备的 16 位网络地址，或者命令帧接收组的多播地址。

C.2.1.3 网络层负载字段

设备标识符请求命令帧的网络层负载包含一个命令标识符、请求类型、请求设备的地址和待鉴别的设备的地址等字段。其中：

命令标识符：为 0x0f，指示为设备标识符请求命令帧。

请求类型如图 C.2 所示：

Bits:0-2	3	4	5-6	7
保留	请求设备地址指示	待鉴别设备地址指示	请求响应设备类型	请求标识符类型

图 C.2 请求类型字段格式

请求设备地址指示：0，指示“请求设备地址字段”使用 16 位短地址；1，指示“请求设备地址字段”使用 64 位地址。该字段默认值为 1。

待鉴别设备地址指示：0，指示“待鉴别设备地址”字段使用 16 位短地址；1，指示“待鉴别设备地址字段”如果出现，使用 64 位地址。

请求响应设备类型：00，指示发向直接路由器或待鉴别的路由器；01，指示发向直接路由器或待鉴别路由器的父结点；10，指示发向直接路由器或待鉴别路由器父结点的子结点；11，指示发向用户监视端。

请求标识符类型：0，表示请求“请求设备地址”对应设备的路由器的标识符；1，表示请求“待鉴别设备地址”字段对应的路由器的标识符。

请求设备地址：初始发起该标识符请求命令帧的设备地址，可以为 16 位短地址，或者 64 位地址。

待鉴别设备地址：“请求标识符类型”为 0 时，该字段不出现；“请求标识符类型”字段为 1 时，请求该字段指示的设备的标识符。可以为 16 位短地址，或者 64 位地址。

C.2.2 设备标识符响应命令帧

设备标识符响应命令帧使得接收到设备标识符请求命令帧的设备可以反馈指定设备的标识符。设

备标识符响应命令帧的负载应按照图 C.3 所示的格式编排。

八位位组:1	1	2/8	8
命令标识	响应类型	设备地址	设备标识符

图 C.3　设备标识符响应命令格式

C.2.2.1　MAC 数据服务请求

为了使用 GB/T 15629.15—2010 定义的 MAC 数据服务发送该命令,应提供以下信息:

a)　目的 MAC 地址和 PAN 标识应设置为发送设备标识符请求命令帧的设备的网络地址和 PAN 标识符。

b)　源 MAC 地址和 PAN 标识符应设置为发送设备响应标识符命令帧的设备的网络地址和 PAN 标识符。

c)　帧控制字段应设置为指示该帧是一个 MAC 数据帧,并且,由于任何网络层发出的安全帧都使用网络层安全,所以,帧控制字段的 MAC 安全子字段设置为禁用。

d)　寻址模式和 intra-PAN 标志应设置以支持这里描述的寻址字段。

C.2.2.2　网络层头字段

为了使设备标识符响应命令能够正确到达目的设备,并完成设备标识符反馈,要求提供以下信息:

a)　网络层头中的源地址应设置为发送帧设备的 16 位网络地址。

b)　网络层头的目的地址字段应设置为接收到的设备标识符请求命令帧中“请求设备地址”字段对应的设备的地址。

c)　因为这是一个网络层命令帧,帧控制字段的源地址子字段应设置为 1,网络层头的源地址字段应该出现并包含帧的发送设备的 64 位地址。帧控制字段中的目的地址子字段应设置为 1,网络层头的目的地址应该出现并设置为接收到的设备标识符请求命令帧中“请求设备地址”相应的设备的 64 位地址。

C.2.2.3　网络层负载字段

响应类型如图 C.4 所示:

Bits:0-5	6	7
保留	设备地址指示	响应标识符类型

图 C.4　网络层负载字段

命令标识符:为 0x10,指示为设备标识符响应命令帧。

设备地址指示:0,指示“设备地址”字段使用 16 位短地址;1,指示“设备地址”字段使用 64 位地址。

响应标识符类型:根据响应的标识符请求命令帧中的“请求标识符类型”设置。

设备地址:指示反馈的为该地址所对应的设备的标识符。可以为 16 位短地址,或者 64 位地址。

设备标识符:指示“设备地址”字段对应设备的标识符。

C.2.3　路由器和结点鉴别过程

参与路由发现的设备,接收到路由响应命令之后,可以对响应的路由器进行鉴别,以提高路由安全性。

设备在接收到路由响应命令之后,判断 nwkRouterAuthen 属性如果为 FALSE,则不需要对发送路

由响应命令帧的路由器进行鉴别。

如果该属性为 TRUE,那么设备首先查找自身是否存储有发送路由响应命令帧的路由器的标识符,如果有,则对响应路由器的鉴别通过;如果没有,设备判断其路由表中,是否有状态为 ACTIVE 的路由条目,如果有,设备则向任一状态为 ACTIVE 的路由条目中的路由器发送标识符请求命令帧,并设置“请求响应设备类型”字段为 00,指示发向直接路由器;设置“请求标识符类型”字段为 0,指示请求“待鉴别设备地址”字段指定的路由器的标识符;设置“请求设备地址”字段为设备自身地址,可以设置为 16 位短地址或者 64 位长地址;设置“待鉴别设备地址”字段为发送路由响应命令帧的路由器的地址,可以为 16 位短地址或 64 位地址;并启动定时器,等待反馈的标识符响应命令帧;如果没有,设备则向发送路由响应命令帧的路由器发送标识符请求命令帧,并设置“请求响应设备类型”字段为 00,指示发向待鉴别路由器;设置“请求标识符类型”字段为 1,指示请求“请求设备地址”字段对应设备的路由器的标识符;设置“请求设备地址”字段为设备自身地址,可以设置为 16 位短地址或者 64 位长地址;“待鉴别设备地址”字段不出现;并启动定时器,等待反馈的标识符响应命令帧。

接收到“请求响应设备类型”字段为 00 的标识符请求命令帧的路由器,首先查找自身是否存储有“请求设备地址”对应设备的路由器的标识符(“请求标识符类型”字段为 1),或者是否存储有“待鉴别设备地址”字段对应设备的标识符(“请求标识符类型”字段为 0),如果有,路由器则向“请求设备地址”字段指示的设备发送标识符响应命令帧,并设置“设备地址”字段为“请求设备地址”对应设备的路由器的地址,设置“设备标识符”字段为上述路由器的标识符(标识符请求命令帧中的“请求标识符类型”字段为 1);或者,设置“设备地址”字段为“待鉴别设备地址”字段对应的设备地址,设置“设备标识符”字段为上述设备的标识符(标识符请求命令帧中的“请求标识符类型”字段为 0)。根据标识符请求命令帧中的“请求标识符类型”字段设置标识符响应命令帧中的“响应标识符类型”;如果没有,路由器则向其父结点转发接收到的标识符请求命令帧,并修改命令帧中的“请求响应设备类型”字段为 01。

接收到“请求响应设备类型”字段为 01 的标识符请求命令帧的设备,首先查找自身是否存储有“请求设备地址”对应设备的路由器的标识符(“请求标识符类型”字段为 1),或者是否存储有“待鉴别设备地址”字段对应设备的标识符(“请求标识符类型”字段为 0),如果有,设备则向“请求设备地址”字段指示的设备发送标识符响应命令帧,并设置“设备地址”字段为“请求设备地址”对应设备的路由器的地址,设置“设备标识符”字段为上述路由器的标识符(标识符请求命令帧中的“请求标识符类型”字段为 1);或者,设置“设备地址”字段为“待鉴别设备地址”字段对应的设备地址,设置“设备标识符”字段为上述设备的标识符(标识符请求命令帧中的“请求标识符类型”字段为 0)。根据标识符请求命令帧中的“请求标识符类型”字段设置标识符响应命令帧中的“响应标识符类型”;如果没有,设备则向其子结点转发接收到的标识符请求命令帧,并修改命令帧中的“请求响应设备类型”字段为 10;并启动定时器,等待其子结点反馈的标识符响应命令帧,在定时器定时到之前,如果接收到任一子结点反馈的标识符响应命令帧,设备则转发该响应命令帧;如果没有接收到任何子结点反馈的标识符响应命令帧,设备则向用户监视端转发接收到的标识符请求命令帧,并修改请求命令帧中的“请求响应设备类型”字段为 11。

接收到“请求响应设备类型”字段为 10 的标识符请求命令帧的设备,首先查找自身是否存储有“请求设备地址”对应设备的路由器的标识符(“请求标识符类型”字段为 1),或者是否存储有“待鉴别设备地址”字段对应设备的标识符(“请求标识符类型”字段为 0),如果有,设备则向“请求设备地址”字段指示的设备发送标识符响应命令帧,并设置“设备地址”字段为“请求设备地址”对应设备的路由器的地址,设置“设备标识符”字段为上述路由器的标识符(标识符请求命令帧中的“请求标识符类型”字段为 1);或者,设置“设备地址”字段为“待鉴别设备地址”字段对应的设备地址,设置“设备标识符”字段为上述设备的标识符(标识符请求命令帧中的“请求标识符类型”字段为 0)。根据标识符请求命令帧中的“请求标识符类型”字段设置标识符响应命令帧中的“响应标识符类型”;上述标识符响应命令帧通过设备的父结点转发。如果没有,则丢弃接收到的标识符请求命令帧,终止操作。

用户监视端接收到“请求响应设备类型”字段为 11 的标识符请求命令帧后,首先查找自身是否存储

有“请求设备地址”对应设备的路由器的标识符(“请求标识符类型”字段为 1),或者是否存储有“待鉴别设备地址”字段对应设备的标识符(“请求标识符类型”字段为 0),如果有,设备则向“请求设备地址”字段指示的设备发送标识符响应命令帧,并设置“设备地址”字段为“请求设备地址”对应设备的路由器的地址,设置“设备标识符”字段为上述路由器的标识符(标识符请求命令帧中的“请求标识符类型”字段为 1);或者,设置“设备地址”字段为“待鉴别设备地址”字段对应的设备地址,设置“设备标识符”字段为上述设备的标识符(标识符请求命令帧中的“请求标识符类型”字段为 0)。根据标识符请求命令帧中的“请求标识符类型”字段设置标识符响应命令帧中的“响应标识符类型”;如果没有,则丢弃接收到的标识符请求命令帧,终止操作。

如果发送请求响应指示字段为 00 的设备,在定时器定时到之前没有接收到标识符响应命令帧,则判定发送路由响应命令帧的路由器没有通过鉴别;如果接收到标识符响应命令帧,则反馈的“设备标识符”是否与发送路由响应命令帧的路由器的标识符一致(“响应标识符”字段为 0),或者“设备地址”指示设备是否为曾经为其提供路由,并且判定“设备标识符”字段是否与相应设备的标识符一致。如果判定结果为否,则判定发送路由响应命令帧的路由器没有通过鉴别。否则,判定发送路由响应命令帧的路由器通过鉴别。

参与路由发现的路由器,也可以对发送路由请求的设备进行鉴别。接收到路由请求的路由器,判断 nwkRouterAuthen 属性如果为 FALSE,则不需要对发送路由请求命令帧的设备进行鉴别;如果该属性为 TRUE,那么路由器首先查找自身是否存储有发送路由请求命令帧的设备的标识符,如果有,则对路由请求设备的鉴别通过;如果没有,路由器则向其父结点发送标识符请求命令帧,并设置“请求响应设备类型”字段为 01,指示发向父结点;设置“请求标识符类型”字段为 0,指示请求“待鉴别设备地址”字段指定的设备的标识符;设置“请求设备地址”字段为路由器自身地址,可以设置为 16 位短地址或者 64 位长地址;设置“待鉴别设备地址”字段为发送路由请求命令帧的设备的地址,可以为 16 位短地址或 64 位地址;并启动定时器,等待反馈的标识符响应命令帧。后续过程与上述参与路由发现的设备对于响应路由器的鉴别过程类似,参考适用。且,当参与路由发现的路由器通过对发送路由请求的设备的鉴别时,参与路由发现的路由器应保存发送路由请求的设备的标识符。

附 录 D
（资料性附录）
安全数据融合机制

D.1 监督者

监督者是一种角色，由特殊结点或者普通结点担任，在一定周期内起到对融合信息的监督作用。监督结点在获得监督权限后，在周期内不间断的发送监督信息。

D.2 机制实施

图 D.1 所示为安全数据融合机制的执行过程。

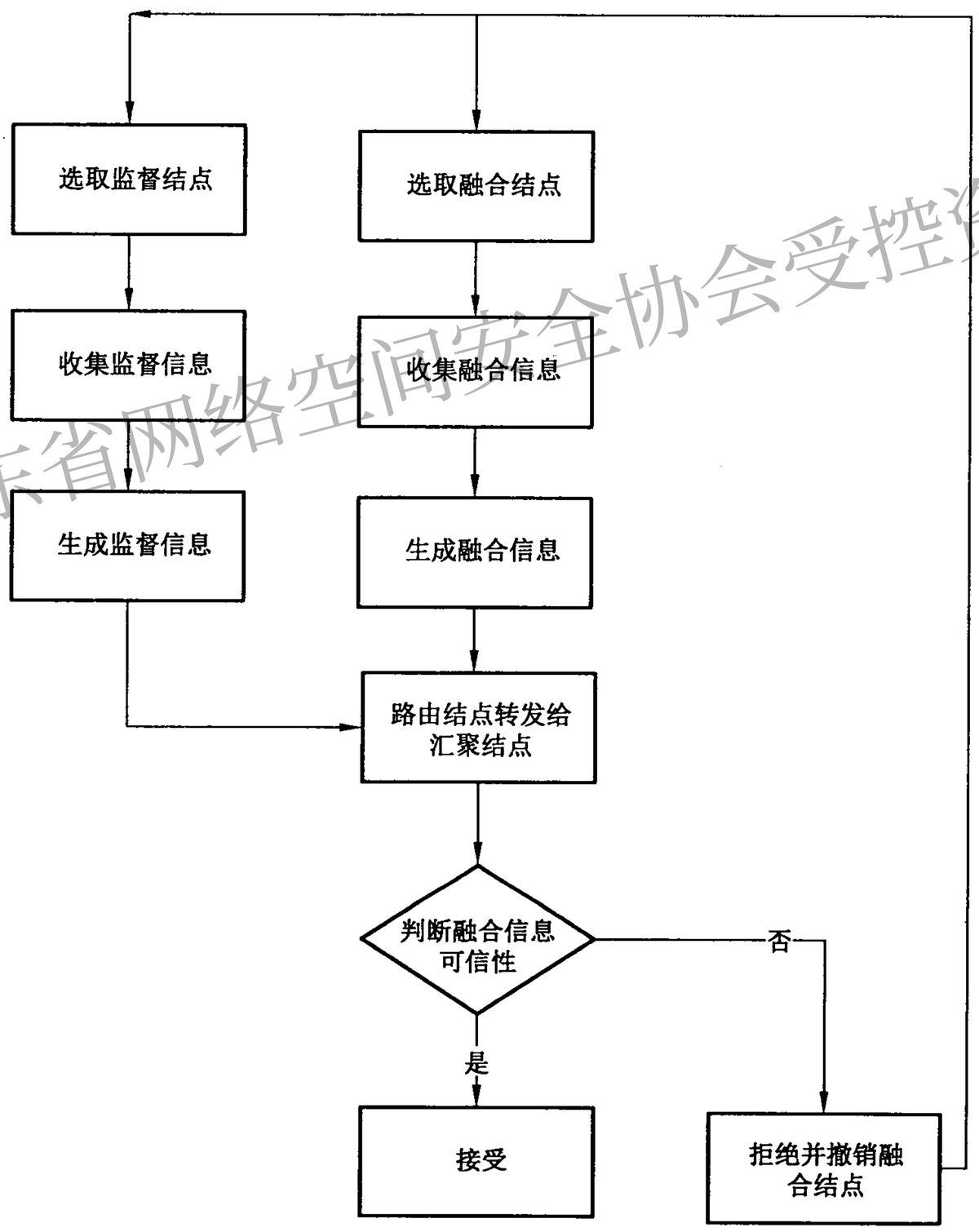

图 D.1 监督机制执行步骤示意图

D.2.1 选取融合结点

融合结点的选取方法不做限定。

D.2.2 监督结点的选取和监督功能的执行

D.2.2.1 监督结点的选取机制

由信任中心或汇聚结点指定，也可随机选取。选取方式不做限定，监督者备选结点不包括融合结点。

D.2.2.2 监督信息的范围

监督范围为以监督结点为圆心一跳通信距离为半径的圆型区域。

D.2.2.3 监督结点的周期

监督周期 Ts 的计算由公式 $Ts=M\times Tmax\leqslant Tc$ 得出，监督结点周期为监督范围内普通结点通信周期最大值的 M 倍($M\geqslant 1$)，Tmax 为监督结点监督范围内结点通信周期的最大值，Tc 为数据融合周期，是相关采集结点通讯周期最大值的 N 倍($N\geqslant 1$)。

D.2.2.4 监督功能的执行

监督功能的执行与数据融合同时进行。监督者利用网络通信的特点，收集监督范围内普通结点采集的、发送给所监督融合结点的报文，并进行数据融合。

D.2.2.5 监督信息的上传方式

监督信息发送给路由结点，监督信息采用自身与基站的对偶密钥加密。如汇聚结点在一段时间内未收到监督报文，则判定聚合结点为恶意结点。

D.2.3 汇聚结点对聚合信息可信性的判断

汇聚结点根据监督结点上传的信息，对融合信息的可信性进行判断。当汇聚结点判定聚合结点融合信息不可信时，下发报文撤销融合结点。

附 录 E
（资料性附录）
帧安全机制

E.1 引言

本附录描述网络层帧结构的完整性保护以及网络层帧结构载荷的保密性保护。对于网络层帧头部的保密性保护由 MAC 层帧的载荷保密性机制提供，参见 GB/T 15629.15—2010。相关术语和原语定义参见 GB/T 30269.301—2014。

E.2 网络层安全概述

当 NLDE-DATA.request 原语中的 SecurityEnable 参数为 FALSE 时，应明确禁止网络层的安全机制。否则，当网络层产生的帧需要加密，或者高层 NIB（见表 E.1）中的 *nwkSecureAllFrames* 属性为 TRUE 时，应启用网络层帧的安全保护机制。网络层帧保护机制应使用国家密码行政主管部门指定的算法和密码运算模式。网络层帧所用的安全等级，由 NIB 的 *nwkSecurityLevel* 属性给出。上层通过设置活动网络密钥、备用网络密钥、帧计数器以及所用安全等级等方式，来控制网络层的安全处理操作。网络层帧的安全结构如图 E.1 所示：

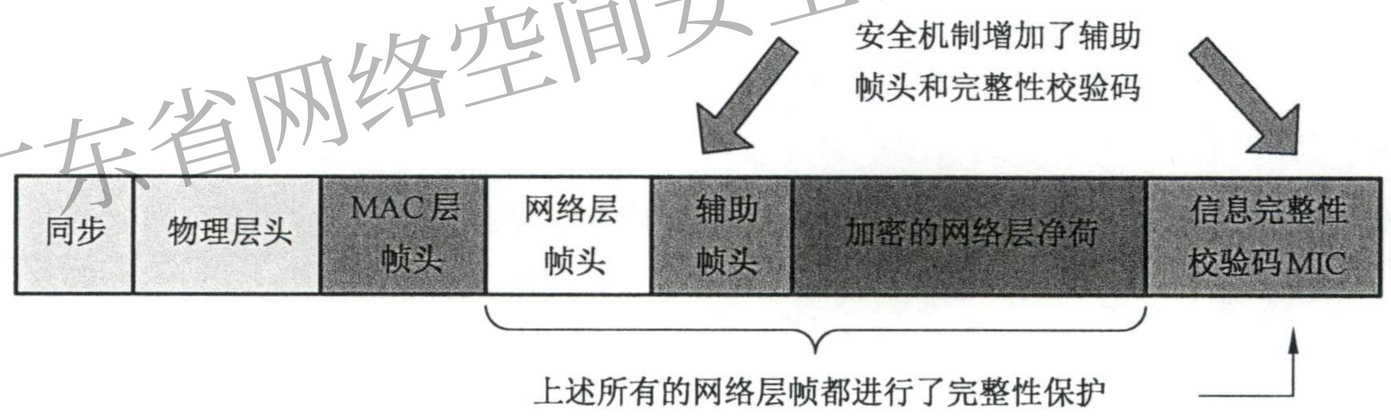

图 E.1 网络层帧的安全结构

E.3 安全的网络层帧

网络层的帧格式包括一个网络层帧头和一个网络层净荷域。网络层帧头包括帧控制域和路由域。当 NPDU 帧启用安全保护时，帧控制域中的安全位应置为 1，以表示辅助帧头的存在。加密的网络层帧的格式如图 E.2 所示。辅助帧头位于网络层帧头和净荷域之间。

字节数：可变	14	可变	
初始的网络层帧头	辅助帧头	加密的净荷	加密的信息完整性校验码 MIC
		网络层帧的安全载荷	
完整的网络层帧头	完全的网络层净荷		

图 E.2 安全的网络层帧格式

网络层的个域网信息库 PIB（personal area network information base）包含管理网络层安全所需的

各种属性。各属性可分别用 NLME-GET.Request 和 NLMESET.request 原语进行读写。与安全相关的网络层 PIB 属性如表 E.1～表 E.3 所示。

表 E.1　NIB 安全属性

属性	标识符	类型	范围	描述	默认值
nwkSecurity Level	0xa0	Octet	0x00～0x07	网络层输入帧和输出帧的安全等级;所允许的安全等级标识符如表 E.6 所示	0x05
nwkSecurity MaterialSet	0xa1		可变	一组网络安全材料描述符的集合,可用于维护活动网络密钥和备用网络密钥	—
nwkActiveKeySeqNumber	0xa2	Octet	0x00～0xFF	*nwkSecurityMaterialSet* 中活动网络密钥的序列号	0x00
nwkAllFresh	0xa3	Boolean	TRUE FALSE	当输入帧计数器的内存溢出时,用于指示网络层输入帧是否需进行新鲜性检查	TRUE
nwkSecureAll Frames	0xa5	Boolean	TRUE FALSE	指示是否需对网络层输入和输出数据帧启用安全保护。如果设置为 0x01,那么需对所有的输入和输出帧进行安全处理(发往当前设备、安全子域为 0 的数据帧除外);如果该属性值为 0x01,那么网络层不能转发安全子域为 0 的帧。 NLDE-DATA.request 原语中的 SecurityEnable 参数将覆盖该属性的设置	TRUE

表 E.2　网络安全材料描述符的元素

名称	类型	范围	描述	默认值
KeySeqNumber	Octet	0x00～0xFF	由信任中心分配给网络密钥的序列号,可在密钥更新时对网络进行区分,并对输入帧进行安全操作	00
OutgoingFrameCounter	4 字节的有序集合	0x00000000～0xFFFFFFFF	输出帧计数器	0x00000000
IncomingFrameCounterSet	输入帧计数器描述符的取值集合,见表 E.3	可变	输入帧计数器的值、以及相应的设备地址的集合	空集
Key	16 字节的有序集合	—	密钥的实际取值	—
KeyType	Octet	0x00～0xFF	密钥类型: 0x01＝标准 0x05＝高安全性 其他值保留	0x01

表 E.3　输入帧计数器描述符的元素

名称	类型	范围	描述	默认值
SenderAddress	设备地址	任意的 64 位有效地址	扩展的设备地址	取决于特定设备
IncomingFrameCounter	4 字节的有序集合	0x00000000～0xFFFFFFFF	输入帧计数器	0x00000000

E.4 辅助帧头格式

辅助帧头中应包括一个安全控制域和一个帧计数器域，也可能包含一个源地址域和密钥序列号域，如表 E.4 所示。

表 E.4 辅助帧头的格式

字节数：1	4	0/8	0/1
安全控制	帧计数器	源地址	密钥序列号

E.4.1 安全控制域

安全控制域中包含安全级别，密钥标识符和扩展的临时子域，其格式如表 E.5 所示。

表 E.5 安全控制域的格式

比特：0-2	3-4	5	6-7
安全级别	密钥标识符	扩展临时子域	保留

E.4.1.1 安全级别子域

安全级别标识符指示了如何对输出帧和输入帧进行保护，是否对荷载进行了加密，以及帧内数据真实性的程度(可由信息完整性代码 MIC 的长度所反映)。MIC 的位长度可以是 0，32，64 或 128，这决定了对 MIC 进行随机猜测时的猜中概率。安全级别的安全特性如表 E.6 所示。注意：安全级别标识符并不表示各安全级的相对强度。

表 E.6 网络层和应用层可用的安全级别

安全级别标识符	安全级别子域	安全属性	数据加密	帧完整性(MIC 长度)
0x01	‘001’	MIC-32	OFF	YES(M=4)
0x02	‘010’	ENC-MIC-32	ON	YES(M=4)
0x03	‘011’	ENC-MIC-64	ON	YES(M=8)
0x04	‘100’	ENC-MIC-128	ON	YES(M=16)
0x05	‘101’	ENC-MIC-128	ON	YES(M=16)

E.4.1.2 密钥标识符子域

密钥标识符子域包含 2 位，用来标识保护帧所用的密钥。密钥标识符子域的编码如表 E.7 所示。

表 E.7 密钥标识符子域的编码表

密钥标识符	密钥标识符子域	描述
0x00	‘00’	一个数据密钥
0x01	‘01’	一个网络密钥
0x02	‘10’	一个“密钥传输”密钥
0x03	‘11’	一个“密钥载入”密钥

E.4.1.3 扩展临时子域

如果辅助帧头中存在源地址域，那么扩展临时子域应设置为 1；否则设置为 0。

E.4.2 计数器域

计数器域提供了网络层帧的新鲜性，可防止对重复帧的处理。

E.4.3 源地址域

仅当扩展临时子域的值为 1 时，辅助帧头中才包含源地址域。如果存在源地址域，那么该域表示负责对网络层帧提供安全保护的设备的 64 位扩展地址。

E.4.4 密钥序列号域

仅当密钥标识符子域的值为 1(对应网络密钥)时，辅助帧头中才包含密钥序列号域。如果存在密钥序列号域，那么该域表示对网络层帧提供安全保护的网络密钥的序列号。

附 录 F
（资料性附录）
协调器变换安全机制

F.1 协调器变换安全

协调器变换的安全机制，用以优化协调器变换过程中的结点和协调器的鉴别和安全材料（如，安全密钥，帧计数，密钥计数，安全级别信息等）的分发过程，为协调器变换提供安全支持。

支持本附录定义的协调器变换安全机制的设备的附加邻居表见表 F.1，网络命令帧表见 F.2。

表 F.1 附加邻居字段表

字段名称	字段类型	有效范围	描述
Extend OldCor Address	整型	原协调器 64 位地址	邻居的原协调器的唯一的 64 位地址
IsOldCorSec	布尔	TRUE or FALSE	指示邻居是否与原协调器存在安全关系： TRUE＝存在 FALSE＝不存在

表 F.2 网络命令帧

命令帧标识符	命令名称	子章节
0x11	安全材料请求命令帧	G.2
0x12	安全材料响应命令帧	G.3
0x13-0xff	保留	—

F.2 安全材料请求命令帧

安全材料请求命令帧使得参与协调器变换的新协调器能够向原协调器请求指定设备的安全材料。安全材料请求命令帧的负载格式应该按照图 F.1 的格式编排：

八位位组：1	1	8	…	8
命令标识	请求安全材料 结点的数量	结点 1 的地址	…	结点 n 的地址

图 F.1 安全材料请求命令帧负载

F.2.1 MAC 数据服务请求

为了使用 GB/T 15629.15—2010 定义的 MAC 数据服务发送该命令，应提供以下信息：

a) 目的 MAC 地址和 PAN 标识符应分别设置为帧要送到的相邻设备的网络地址和 PAN 标识符；

b) 源 MAC 地址和 PAN 标识符应设置为发送安全材料请求命令帧的设备的地址和 PAN 标识符；

c) 帧控制字段应设置为指示该帧是一个 MAC 数据帧，并且，由于网络层发出的任何安全帧都使用网络层安全，所以，帧控制字段的 MAC 安全子字段设置为禁用；

d) 寻址模式和 intra-PAN 标志应设置为支持这里描述的寻址字段。

F.2.2 网络层帧头字段

安全请求命令帧是以单播的形式发送给进行协调器变换的原协调器。网络层头字段应设置如下：源地址字段始终设置为该命令发起设备，即参与协调器变换的新协调器的 16 位网络地址；帧控制字段的源地址字段应设置为 1，网络层头字段的源地址字段应存在，包含帧的发起设备的 64 位地址；目的地址字段始终设置为参与协调器变换的原协调器的 16 位网络地址；帧控制字段的目的地址字段应设置为 1，网络层头的目的地址字段应存在，且应包含参与协调器变换的原协调器的 64 位地址。

F.2.3 网络层负载字段

安全请求命令帧负载包含命令标识符字段、请求安全材料结点的数目字段，以及所要请求安全材料的各个结点的 64 位地址列表字段。即：命令标识字段：设置为 0x11；请求安全材料结点的数目：设置为所要请求的安全材料的结点数目；结点 i 的地址：设置为所要请求安全材料的结点 i 的地址，$i=1\cdots n$。

F.3 安全材料响应命令帧

安全材料响应命令帧用于参与协调器变换的原协调器向新协调器反馈所请求的设备的安全材料。安全材料响应命令帧负载的格式应按照图 F.2 的格式进行编排：

八位位组:1	1	1	可变	…	可变
命令标识	结点数量	安全材料单位	结点 1 的安全材料	…	结点 n 的安全材料

图 F.2 安全材料响应命令帧负载

F.3.1 MAC 数据服务请求

为了使用 GB/T 15629.15—2010 定义的 MAC 数据服务发送该命令，应提供以下信息：

a) 目的 MAC 地址和 PAN 标识符应分别设置为帧要送到的相邻设备的网络地址和 PAN 标识符；

b) 源 MAC 地址和 PAN 标识符应设置为发送安全材料响应命令帧的设备的地址和 PAN 标识符；

c) 帧控制字段应设置为指示该帧是一个 MAC 数据帧，并且，由于网络层发出的任何安全帧都使用网络层安全，所以，帧控制字段的 MAC 安全子字段设置为禁用；

d) 寻址模式和 intra-PAN 标志应设置为支持这里描述的寻址字段。

F.3.2 网络层帧头字段

安全材料响应命令帧是以单播的形式发送给请求安全材料的新协调器。网络层头字段应设置如下：

a) 源地址字段始终设置为该命令发起设备，即参与协调器变换的原协调器的 16 位网络地址；

b) 帧控制字段的源地址字段应设置为 1，网络层头字段的源地址字段应存在，包含帧的发起设备的 64 位地址；

c) 目的地址字段始终设置为参与协调器变换的新协调器的 16 位网络地址；

d) 帧控制字段的目的地址字段应设置为 1，网络层头的目的地址字段应存在，且应包含参与协调器变换的新协调器的 64 位地址。

F.3.3 网络层负载字段

八位位组:1	1	1	可变	…	可变
命令标识	结点数目	安全材料单位	结点 1 的安全材料	…	结点 n 的安全材料

图 F.3 网络层负载字段

安全材料响应命令帧负载包含命令标识字段、结点数目字段、安全材料单位字段，以及所要反馈的各个结点的安全材料列表(见图 F.3)。即：

命令标识符：设置为 0x12；

结点数目字段：设置为反馈的安全材料的结点的数目；

安全材料单位：设置为后续安全材料的单位：0x00-64 位；0x01-128 位；0x02-256 位；0x03-0xff 保留；

结点 i 的安全材料：设置为反馈的结点 i 的安全材料。这里安全材料具体指代的内容，需要根据安全材料协商机制确定。

F.4 协调器和结点鉴别

参与协调器变换的新协调器，根据表 F.1 中的 Extend OldCorAddress 和 IsOldCorSec 参数，确定如果有两个或两个以上的来自同一个原协调器、并且与原协调器存在安全关系的结点，选择自身作为协调器，新协调器即利用本规范定义的鉴别和密钥分发机制建立与原协调器的安全关系。如果建立成功，协调器则向原协调器发送安全材料请求命令帧，请求指定结点的安全材料。原协调器接收到安全材料请求命令帧后，构造安全材料响应命令帧，反馈所请求结点的安全材料。新协调器接收到原协调器反馈的指定结点的安全材料之后，与指定结点建立安全关系。如果没有两个以上的来自同一个原协调器并且与原协调器存在安全关系的结点选择新协调器作为协调器，或者，新协调器原协调器建立安全关系不成功，或者新协调器没有接收到反馈的指定结点的安全材料，新协调器就利用本规范定义的鉴别和密钥分发机制建立与相应结点的安全关系。

参 考 文 献

[1] GB 17859—1999 计算机信息系统安全保护等级划分准则

[2] GB/T 15629.15—2010 信息技术 系统间远程通信和信息交换 局域网和城域网 特定要求 第15部分:低速无线个域网(WPAN) 媒体访问控制和物理层规范

[3] GB/T 18794.2—2002 信息技术 开放系统互连 开放系统安全框架 第2部分:鉴别框架

[4] GB/T 20984—2007 信息安全技术 信息安全风险评估规范

[5] GB/T 25069—2010 信息安全技术 术语

[6] GB/T 30269.301—2014 信息技术 传感器网络 第301部分:通信与信息交换:低速无线传感器网络网络层和应用支持子层规范

[7] ISO/IEC 29180:2012 信息技术 系统间远程通信和信息交换 泛在传感器网络用安全框架(ISO/IEC 29180:2012 Information technology—Telecommunications and information exchange between systems—Security framework for ubiquitous sensor networks)

中 华 人 民 共 和 国
国 家 标 准
信息技术 传感器网络
第 601 部分:信息安全:通用技术规范
GB/T 30269.601—2016
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲 2 号(100029)
北京市西城区三里河北街 16 号(100045)
网址 www.spc.net.cn
总编室:(010)68533533 发行中心:(010)51780238
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 3 字数 84 千字
2016 年 9 月第一版 2016 年 9 月第一次印刷
*
书号:155066·1-53933 定价 42.00 元

GB/T 30269.601-2016