广东工业大学

硕士学位论文

ZigBee安全接入认证机制研究与应用

姓名：邹小武

申请学位级别：硕士

专业：通信与信息系统

指导教师：徐杜

20100601

摘 要

无线通信技术、嵌入式技术和数据处理技术的发展，正推动着无线网络及其应用的高速发展。今天，无线网络已经成为人们生活中不可缺少的一部分。然而安全问题却一直制约着网络的有效应用和发展。不论是移动通信网络、宽带无线接入网还是无线个域网传输都要经过无线传输环境，其信息的传输容易受到攻击和窃听。如何保证网络的安全性是应首先考虑的关键问题。首先，用户端和网络端之间的无线接口是开放的，使得在无线信道上传送的信令和业务信息很容易被他人窃听，而且很难被发现。其次，用户端和网络端之间缺乏固定的物理连接，用户必须通过无线信道来传送其身份信息，以便网络对其进行身份认证。由于无线接口的开放性，必须采用适当的认证方案保护通信内容以防非法使用网络服务。当电子商务、电子政务、军事通信等重要信息通过无线环境传输时，如果存在信息泄漏或非法用户，接入网络可能会造成巨大的损失。因此研究无线接入的安全机制显得非常必要。

无线网络安全技术的研究就是要通过对无线网络的信息安全关键和共性技术开展研究，包括安全体系结构、密码算法、认证技术、密钥交换协议、及其它安全相关协议的研究，重点解决移动通信网络、无线局域网以及宽带无线接入网等典型的无线网络的严重信息安全问题，包括非法信息截取、未授权信息服务以及插入攻击等，逐步形成我国无线网络信息安全技术保障体系。

ZigBee 是一种具有独特优越特性的短距离、低速率、低能耗无线通信技术，无线测控网是它的最主要的应用领域。它正在成为无线互联网的一个重要组成部分和补充。ZigBee 的接入网安全问题将会是整个无线互联网安全体系的重要问题之一，具有很深刻的研究意义。为了保证信息传输的安全性，ZigBee 技术中采用了对称加密的安全机制。密钥由网络层和应用层根据实际应用需要生成，并对其进行更新、传送、管理和存储等。

本文就是对这一安全机制进行分析和研究，并借鉴第三代移动通信网、无线局域网等各种无线网络的安全体系结构的研究模式，以期清楚了解 ZigBee 网络的认证、加密和路由安全体系，解决 ZigBee 网络信息传输过程中的安全问题。

文章最后对 NS2 网络仿真软件进行了详细介绍，并使用该软件对 ZigBee 无线网络路由协议进行了仿真研究，获得仿真结果。最后，使用协议形式化验证工具 AVISPA 来验证改进 ZigBee 无线网络路由协议的安全性，结果表明改进路由协议算法是可行的。

关键词：认证协议；密钥交换；AES；NS2；AVISPA

Abstract

Wireless communication technology, embedded technology and data processing technology are driving the high-speed development of wireless networks and applications. Today, wireless networks have become an indispensable part of life, but the development and application of it has been restricted by security. Whatever the the mobile communication network, broadband wireless access network or wireless personal area network, the transmission has to go through the wireless environment, where information transmission vulnerable to attacks and eavesdropping, how to ensure the security of the network is the key issue. First, the client and the wireless interface between the network is so open that the wireless channel on the transmission of signaling and other business information can easily be tapped. Secondly, the lack of a fixed physical connection between the client and the network, the user has to send identity information to the network though a radio channel for the authentication of their identity. Since the opening of the wireless interface, an appropriate certification program takes to protect the content against illegal use of communications network services. When the e-commerce, e-government, military, communications and other important information transmitted through the wireless environment, if the information leakage or illegal user, the network may result in huge losses, so the research wireless access security mechanism is necessary.

The Research of Wireless Network Security Technology is a study of the key and common of information security technologies, including security architecture, cryptographic algorithms, authentication, key exchange protocol, and other security-related research protocols. The technologies focus on solution mobile communications networks, wireless local area networks and broadband wireless access network, and typical of wireless networks such as serious information security problems, including illegal information interception, unauthorized information services and into attacks. Thus, gradually form wireless network information security technology system.

ZigBee is an excellent feature unique short-range, low speed, low power wireless

communication technology, it is becoming an important part of the wireless Internet. ZigBee Access Network security will be one of the most important issues of the wireless Internet security system, with heavy research significance. In order to ensure the security of information transfer, ZigBee technology uses symmetric encryption for security. The network layer and application layer generate key from the actual application need, and update, send, manage, storage it.

This paper is analysis and research for this security mechanism, and drawing the third generation mobile communication network, wireless LAN and other wireless network security architecture research model to understand the ZigBee network authentication, encryption, and routing security system, in order to address ZigBee network information security problems during transmission.

Finally, the NS2 network simulation software is described in detail, by means of this software, the advanced ZigBee wireless network routing protocols was simulated with simulation results. Finally, the security of ZigBee wireless network routing protocols was proved by the formal verification tools of AVISPA, the results showed the improved routing algorithm is feasible.

Keywords: Authentication Protocol; Key exchange; AES; NS2; AVISPA

第一章 绪论

ZigBee传感器网络是当前国际上备受关注的、新兴前沿研究的热门技术，它能够通过各类集成化的微型传感器协作地实时监测、感知和采集分散在一定范围的各种环境或监测对象的信息，通过嵌入式系统对信息进行处理，并通过随机自组织无线通信网络以多跳中继方式将所感知信息传送到用户终端。ZigBee技术具有十分广阔的应用前景，在自然灾害监测、动植物生存环境监测、农业、远程医疗、危险区域远程测控等许多领域都有重要的科研价值和巨大实用价值，已经引起了世界许多国家军界、学术界和工业界的高度重视，并成为传感器网络领域进入2000年以来公认的新兴前沿热点技术，被认为是将对二十一世纪通信技术产生巨大影响力的技术之一。

1.1 概述

无线传感器网络是一种无基础设施的无线网络，它综合了传感器技术、嵌入式计算技术、分布式信息处理技术和无线通信技术，能够实时监测、感知和采集网络分布区域内的各种环境或监测对象的信息，并对这些数据进行处理，获得详尽而准确的信息，最后将信息通过自组织网络传送给用户。

无线传感器网络作为一种独立出现的网络，它的基本组成单位是无线传感器节点，这些节点集成了传感器、微处理器、无线接口和电源管理四个主要模块。传感器、微机电系统(MEMS)、集成电路、以及低功耗无线通信等技术的飞速发展，使得低成本、低功耗、多功能的微型无线传感器网络的大规模应用成为可能，这些微型无线传感器是集成的光机电一体化系统，具有无线通信、数据收集和处理、协同工作等功能。它们共同组成了无线传感器网络，导致了一种全新的信息获取和处理模式，微型传感器节点可以随机或者特定地布置在工作环境中，通过无线通信实现自组织，获取周围环境的信息，形成分布自治系统，相互协同完成特定的任务。长期以来，低价、低传输率、短距离、低功率的无线通讯市场一直存在着。蓝牙技术出现，一度让工业控制、家用自动控制、玩具制造商等业者雀跃不已，但是 Bluetooth 的售价一直居高不下，严重影响了这些厂商的使用积极性。当

初的那些为蓝牙技术兴奋的业者大部分参加了 IEEE802.15.4 小组，负责制定 ZigBee 的物理层和媒体介入控制层。IEEE802.15.4 规范是一种经济、高效、低数据速率(<250kbps)、工作在 2.4GHz 和 868 / 928Hz 的无线技术，用于个人区域网和对等网状网络，是 ZigBee 应用层和网络层协议的基础。ZigBee 是一种新兴的近距离、低复杂度、低功耗、低数据速率、低成本的无线网络技术，它是一种介于无线标记技术和蓝牙之间的技术提案。主要用于近距离无线连接。它依据 802.15.4 标准，在多个小型的节点之间实现相互协调通信。这些节点通常只需要很少的能量，以接力的方式通过无线电波将数据从一个节点传到另一个节点，所以它们的通信效率非常高。

1.1.1 传感器网络体系结构与特点

无线传感器网络系统通常包括传感器节点、网关和服务器。

传感器节点可以完成环境监测、目标发现、位置识别或控制其他设备的功能；此外还具有路由、转发、融合、存储其他节点信息等功能。

网关负责连接无线传感器网络和外部网络的通信，实现两种网络通信协议之间的转换，发送控制命令到传感器网络内部节点，以及传送节点的信息到服务器。

服务器用于接收监测区域的数据，用户可远程访问服务器，从而获得监测区域内监测目标的状态以及节点和设备的工作情况等。

无线传感器网络通常具有如下主要特点：

(1)自组织。传感器网络系统的节点具有自动组网的功能，节点间能够相互通信协调工作。

(2)多跳路由。节点受通信距离、功率控制或节能的限制，当节点无法与网关直接通信时，需要由其他节点转发数据，完成数据的传输，因此网络数据传输路由是多跳的。

(3)动态网络拓扑。在某些特殊的应用中，无线传感器网络是移动的，传感器节点可能会因能量消耗完或其他故障而终止工作，这些因素都会使网络拓扑发生变化。

(4)节点资源有限。传感器网络在能量、计算量和存储量方面比一般移动网络所受限制要大得多，很多节点的电源不能更换或充电，于是电源寿命就决定节点寿命。

(5)易出故障。传感器网络易出故障，需要安排冗余节点提高可靠性，或者随时加入新节点代替故障节点，保证传感器网络持续精确地工作。

1.1.2 传感器网络基本构架

传感器节点通常分散布置于一个区域中。节点收集数据，并路由数据到汇聚点（sink），再到最终用户。汇聚点经过因特网或卫星与任务管理节点通信。

协议层次包括：物理层、数据链接层、网络层、传输层、应用层。

物理层的功能是频率选择、载频生成、信号检测、调制、数据加密，并且比较延迟、散布、遮挡、反射、绕射、多路径和衰减等信道参数，为路由及重构提供依据，减小能耗是物理层设计中最重要的部分。

数据链层的功能：数据流选通、数据帧检测、介质访问、错误控制以确保可靠的点到点，或点到多点连接。 在传感器网络中链路层非常重要的部分就是MAC，通过它要实现两个目标：产生网络基础结构和节点间有效地均匀共享通信资源。传感器网络不能直接采用现有 MAC 协议，如蓝牙和 MANET，因为现有MAC 协议是 QoS 和带宽效率导向，而传感器网络有其特殊性和独特要求：节点数目众多、发射功率和发射范围小、网络拓扑多变。

网络层的功能：保证能量效率、实现节点间协同时数据融合、采用基于属性的编址和基于位置信息的控制。网络层最主要的任务是实现节点间协同时数据融合。数据融合是在数据中心路由过程中，克服数据爆炸和重叠的技术。数据爆炸就是反复把复制的消息送到同一节点，使得数据过载；数据重叠就是如果两个以上节点在共同观察区，会同时传感同一激励，造成相同信息的冗余传输。这二者都会造成网络能源的大量无谓消耗。

当系统需要访问因特网或其他外部网时传输层特别重要。传输控制协议（TCP）及其现有的传输窗机制十分适合于传感器网络极为严酷的环境。像 TCP 分隔这样的方法在传感网与其他网络（例如互联网）交互时可能会十分有用。在这种方法里，TCP 链接终止于汇聚点，汇聚点和其他节点的通信则用一个专门的传输层协议处理。

应用层是根据任务构建的应用软件。目前应用效果比较好、比较广泛的应用层协议主要有：传感器管理协议（SMP21）；任务分配和数据公告协议（TADAP22）；传感器查询和数据传播协议（SQDDP23）。

传感器查询和数据传播协议（SQDDP）为用户应用程序提供界面，以支持查询、对查询的响应、收集回答。

传感器网络的通信系统可以按照功能划分为三个平面：能量管理平面、移动管理平面、任务管理平面。能量管理平面管理节点如何利用能源，例如节点收到消息后可能断开接受器。当节点能量较低时，节点对邻点广播，报告不能路由信息。剩余能量保留作传感用。移动管理平面监测和注册节点的移动，维持到用户的路由。节点可能跟踪它的邻节点。任务管理平面平衡和调度在给定区域的传感任务，根据能量水平决定哪些节点执行传感任务。

1.1.3 传感器网络路由协议概述

相对于传统无线通讯网络而言，传统无线通讯网络研究的重点放在无线通讯的服务质量(QoS)上，而无线传感器节点是随机分布，电池供电，因此目前无线传感器网络路由协议的研究重点是放在如何提高能量效率上，当前流行的几个无线传感器网络的路由协议主要有：泛洪协议、Gossiping 协议、SPIN 协议、定向扩散(Directed Diffusion)协议、LEACH 协议。

泛洪(Flooding)协议[1]是一种传统的无线通讯路由协议。该协议规定，每个节点接受来自其他节点的信息，并以广播的形式发送给其他邻居节点。如此继续下去，最后将信息数据发送给目的节点。但这个协议容易引起信息的“内爆”(Implosion)和“重叠”(Overlap)，造成资源的浪费。因此在泛洪协议的基础上，提出了闲聊(Gossiping)协议。

Gossiping 协议是在泛洪协议的基础上进行改进而提出的。它传播信息的途径是通过随机的选择一个邻居节点，获得信息的邻居节点以同样的方式随机的选择下一个节点进行信息的传递。这种方式避免了以广播形式进行信息传播的能量消耗，但其代价是延长了信息的传递时间。虽然 Gossiping 协议在一定程度上解决了信息的内爆，但是仍然存在信息的重叠现象。

SPIN(Sensor Protocol for Information via Negotiation)协议[2]是一种以数据为中心的自适应路由协议。SPIN 协议的目的是：通过节点之间的协商，解决 Flooding 协议和 Gossiping 协议的内爆和重叠现象。SPIN 协议有 3 种类型的消息，即 ADC、REQ 和 DATA。 ADC 用于数据的广播，当某一个节点有数据可以共享时，可以用其进行数据信息广播。 REQ 用于请求发送数据，当某一个节点希望接受 DATA

数据包时，发送 REQ 数据包。 DATA 为传感器采集的数据包。在发送一个 DATA 数据包之前，一个传感器节点首先对外广播 ADV 数据包，如果某一个节点希望接受要传来的数据信息，则向发送 ADV 数据包的节点回复 REQ 数据包，因此，便建立起发送节点和接受节点的联系，发送节点便向接受节点发送 DATA 数据包。

定向扩散协议[3]是一种基于查询的路由机制。整个过程可以分为兴趣扩散、梯度建立以及路径加强三个阶段。在兴趣扩散阶段，汇聚节点向传感器节点发送其想要获取的信息种类或内容。兴趣消息中含有任务类型、目标区域、数据发送速率、时间戳等参数。每个传感器节点在收到该信息后，将其保存在 CACHE 中。当整个信息要求传遍整个传感器网络后，便在传感器节点和汇聚节点之间建立起一个梯度场，梯度场的建立是根据成本最小化和能量自适应原则。一旦传感器节点收集到汇聚节点感兴趣的数据，就会根据建立的梯度场寻求最快路径进行数据传递。

LEACH(LOW-Energy Adaptive Clustering Hierarchy)是一种以最小化传感器网络能量损耗为目标的分层式协议[4]。该协议的主要思想是通过随机选择类头节点，平均分担无线传感器网络的中继通讯业务来达到平均消耗传感器网络中节点能量的目的，进而可以延长网络的生命周期。LEACH 协议可以将网络生命周期延长 15%。LEACH 协议分为两个阶段：类准备阶段和数据传输阶段。

近几年，针对无线传感器网络路由协议的研究相对于传统的无线通讯路由协议吸引了更多人的研究视线。从上面分析可以看出，每种协议之间是相互联系的。因此，从某种意义上来讲，很难说清楚到低是那种协议更有优势。基于对这些协议的比较分析表明，一个好的无线传感器网络路由协议应具备如下特征：具有动态的选择汇聚节点的能力、快速的数据融合技术及随机路径的选择能力。

1.1.4 传感器网络安全技术

安全是系统可用的前提，需要在保证通信安全的前提下，降低系统开销，研究可行的安全算法。由于无线传感器网络受到的安全威胁和移动 ad hoc 网络不同，所以现有的网络安全机制无法应用于本领域，需要开发专门协议。目前主要存在两种思路简介如下：

一种思想是基于路由安全的角度出发，寻找尽可能安全的路由以保证网络的安全。如果路由协议被破坏导致传送的消息被篡改，那么对于应用层上的数据包

来说没有任何的安全性可言。一种方法是“有安全意识的路由”(SAR)[5]，其思想是找出真实值和节点之间的关系，然后利用这些真实值去生成安全的路由。该方法解决了两个问题，即如何保证数据在安全路径中传送和路由协议中的信息安全性。这种模型中，当节点的安全等级达不到要求时，就会自动的从路由选择中退出以保证整个网络的路由安全。可以通过多径路由算法改善系统的稳健性，数据包通过路由选择算法在多径路径中向前传送，在接收端内通过前向纠错技术得到重建。

另一种思想是增强安全协议，在此领域也已经产生了大量的研究成果。传感器网络的任务是为某种特定需要提供安全保护的，提供一个安全解决方案将为解决这类安全问题带来一个合适的模型。在具体的技术实现上，先假定基站总是正常工作的，并且总是安全的，满足必要的计算速度、存储器容量，基站功率满足加密和路由的要求；通信模式是点到点，通过端到端的加密保证数据传输的安全性；射频层总是正常工作。基于以上前提，典型的安全问题主要有：信息被非法用户截获；一个节点遭破坏；识别伪节点；如何向已有传感器网络添加合法的节点。

就目前而言，无线传感器网络中有两种专用安全协议：基于时间的高效的容忍丢包的流认证协议 μTESLA[6] 和安全网络加密协议 SNEP (Sensor Network Encryption Protocol)。SNEP 的功能是提供节点到接收机之间数据的鉴权、加密、刷新，μTESLA 的功能是对广播数据的鉴权。因为无线传感器网络可能是布置在敌对环境中，为了防止供给者向网络注入伪造的信息，需要在无线网络中实现基于源端认证的安全组播。但由于在无线传感器网络中，不能使用公钥密码体制，因此源端认证的组播并不容易实现。传感器网络安全协议 SPINK 中提出了基于源端认证的组播机制 uTESLA，该方案是对 TESLA 协议的改进，使之适用于传感器网络环境。其基本思想是采用 Hash 链的方法在基站生成密钥链，每个节点预先保存密钥链最后一个密钥作为认证信息，整个网络需要保持松散同步，基站按时段依次使用密钥链上的密钥加密消息认证码，并在下一时段公布该密钥。

1.2 ZigBee 技术概述

由IEEE802.15.4标准的PHY和MAC层再加上ZigBee的网终层和应用层组成的ZigBee协议，由于网络节点具有成本低、体积小、能量和通信能力有限等特点，

所以这种网络的突出特点是网络系统支持低成本、易实现、低功耗等。

1.2.1 ZigBee 的技术特点

ZigBee 依据 IEEE 无线个域网[7]（Wireless Personal Area Network，WPAN）工作组的一项标准，即 IEEE802.15.4 标准，在许多微小的传感器节点间互相协调通信。这些传感器节点只需要很少的能量，以接力的方式通过无线电波将数据从一个传感器传到另一个传感器，具有其它无线传输技术无法比拟的优势：

(1)低功耗：由于传输数据量较小，信号的收发短，ZigBee 节点实行休眠模式。设备搜索时延一般为 30ms，休眠激活时延为 15ms，活动设备信道接入时延为 15 ms。因此 ZigBee 节点非常省电，节点电池工作时间可以长达 6 个月至 2 年左右。

(2)网络容量大：一个 ZigBee 网络最多包括 255 个网络节点，若是通过网络协调器，网络可以容纳 65000 多个节点设备，再加上各个网络协调器可以互连，整个网络的节点数目将十分可观。

(3)具有较高的可靠性和安全性：为了提高传输数据的可靠性，ZigBee 采用了时隙化的载波侦听和冲突避免的信道接入 CSMA-CA（Carrier Sense Multiple Access With Collision Avoidance）算法。同时 ZigBee 在网络层和媒体接入控制层都加入了安全保密机制，采用了 IEEE802.15.4 媒体接入层的安全保障策略：a）访问控制，设备保存那些网络中被信任的设备名单。b）资料加密，使用高级 128 位的对称加密（AES-128）算法。

(4)低成本：ZigBee 模块初始成本约为 6 美元，随着市场的成熟会很快降到 1.5~2.5 美元，而且 ZigBee 协议免专利费用。

ZigBee 技术的出现弥补了以往无线通信市场上低成本低功耗设备领域的空缺，它特别适用于那些设备成本较低，传输数据量较小，低功耗的应用场合，主要应用于工业控制、消费电子设备、汽车自动化、家庭和楼宇自动化、医用设备控制等。在工业控制领域，可以对关键部件的技术参数进行监控，以掌握设备运行情况；在医疗设备控制方面，可以在病人身上安置传感器，可让医生随时远程了解病情。

1.2.2 ZigBee 协议栈

ZigBee协议架构建立在IEEE 802.15.4标准基础之上。其物理层(PHY)和媒体访

问控制层(MAC)采用IEEE 802.15.4标准。ZigBee联盟则定义了ZigBee协议的网络层(NWK)、应用层(APL)和安全服务规范。其协议构架如图1-1所示。ZigBee协议以OSI七层参考模型为基础，定义了其中与LR.WPAN应用相关的协议层[8]。协议栈的每层为其上层提供一套服务功能：数据实体提供数据传输服务，管理实体提供其他的服务。每个服务实体和上层之间的接口称作"服务访问点(SAP)"，通过SAP交换一组服务原语为上层提供相关的服务功能。

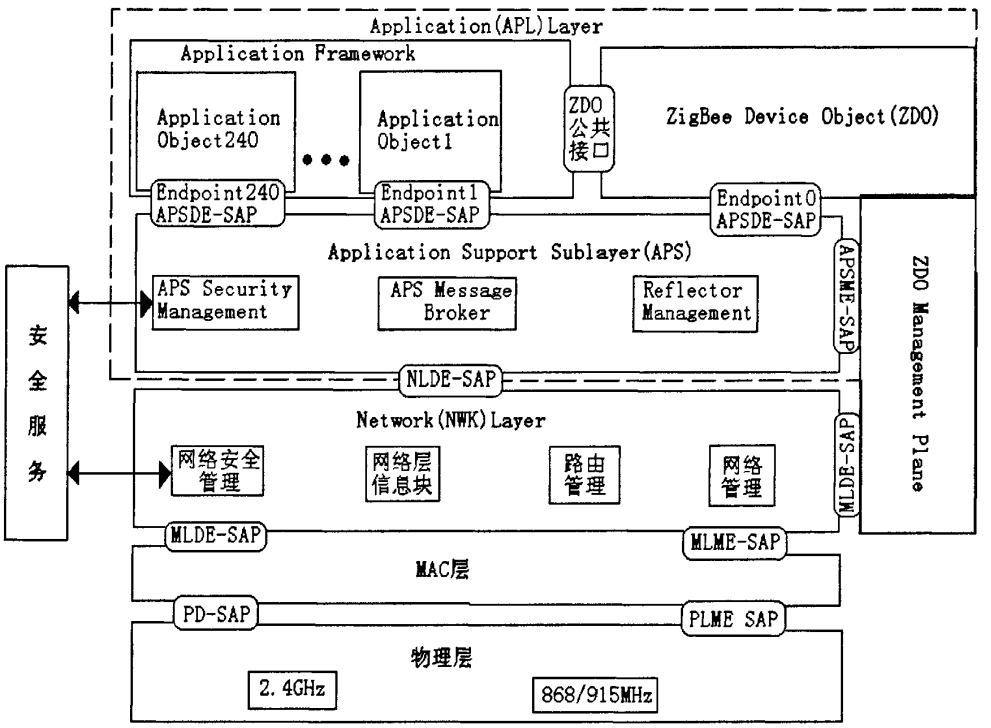

图1-1 ZigBee协议体系结构

Fig 1-1 ZigBee protocol architecture

物理层定义了无线信道、与MAC子层之间的接口，提供物理层数据服务和物理层管理服务。物理层的功能主要包括激活 / 休眠无线收发设备、对当前信道进行能量检测、链路质量指示、为载波检测多址与碰撞避免(CSMA/CA)进行空闲信道评估、信道选择，数据的发送和接收。ZigBee的通信频率在物理层来规范。根据不同的国家和地区，为ZigBee提供的工作频率范围不同，ZigBee所使用的频率范围分别为2.4GHz和868/915MHz。因此，IEEE 802.15.4定义了两个物理层标准，分别是2.4GHz物理层和868/915 MHz物理层。两个物理层都基于直接序列扩频(DSSS，Direct Sequence Spared Spectrum)技术，使用相同的物理层数据包格式，区别在于工作频率、调制技术、扩频码片长度和传输速率的不同[9]。

ZigBee技术的MAC层所采用的是IEEE 802.15.4标准的MAC层协议规范。MAC层处理所有物理层无线信道的接入，其主要功能为：网络协调器产生网络信标，与信标同步，支持个域网(PAN)链路的建立和断开，为设备的安全性提供支持，信道接入方式采用免冲突载波检测多址接入(CSMA/CA)机制，处理和维护保护时隙(GTS)机制，在两个对等的MAC实体之间提供一个可靠的通信链路。MAC层在服务协议汇聚层(SSCS)和物理层之间提供了一个接口。从概念上说，MAC层包括一个管理实体，通常称为MAC层管理实体(MLME)，该实体提供一个服务接口，通过此接口可调用MAC层管理功能。同时，该管理实体还负责维护MAC层固有的管理对象的数据库。该数据库包含了MAC层的PAN信息数据库(PIB)信息。图1-2描述了MAC层的结构和接口。

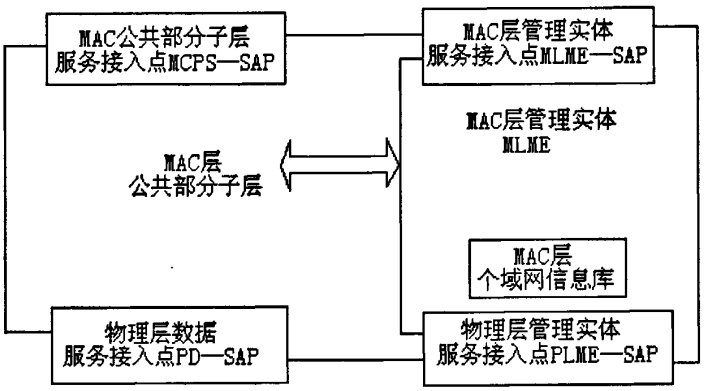

图1-2 MAC层参考模型

Fig 1-2 MAC layer reference model

ZigBee网络层的主要功能就是提供一些必要的函数，确保ZigBee的MAC层正常工作，并且为应用层提供合适的服务接口。为了向应用层提供其接口，网络层提供了两个必需的功能服务实体，它们分别是数据服务实体和管理服务实体，如图1-3所示。网络层数据实体通过网络层数据实体服务接入点(NLDE-SAP)提供数据传输服务，网络管理层实体通过网络层管理实体服务接入点(NLME-SAP)提供网络管理服务。网络层管理实体利用网络层数据实体完成一些网络的管理工作，并且网络层管理实体完成对网络信息库(NIB)的维护和管理。网络层通过MCPS-SAP和MLME-SAP接口为MAC层提供接口，通过NLDE-SAP与NLME-SAP接口为应用层提供接口服务。网络层管理实体提供网络管理服务，允许应用与协议栈相互作用。网络层管理实体提供如下服务：配置一个新设备，为操作按照要求充分布局协议栈的能力。布局选择包括作为ZigBee协调器开始操作或加入一个现有的网络；开

始一个网络；加入和离开网络；寻址；邻居友备发现；

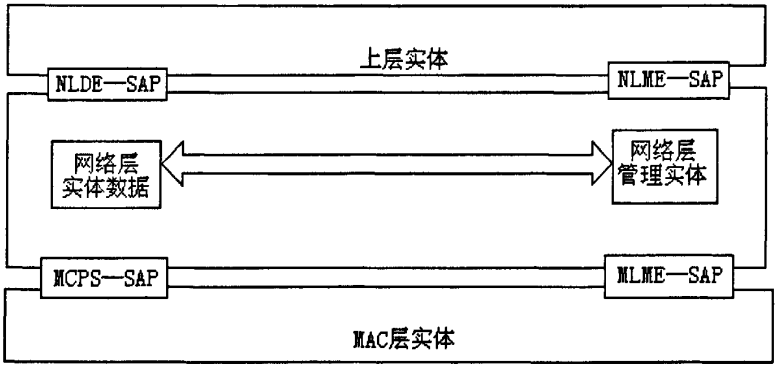

图1-3 网络层参考模型

Fig 1-3 Network Layer Reference Model

路由发现；接收控制；网络层数据实体为数据提供服务。在两个或多个设备之间传送数据时，将按照应用协议数据单元(APDU)的格式进行传送，并且这些设备必须在同一个网络中，即在同一个内部个域网中。网络层数据实体主要提供生成网络层协议数据单元(NPDU)和指定拓扑传输路由的服务。

ZigBee应用层框架包括应用支持层(APS)、ZigBee设备对象(ZDO)和制造商所定义的应用对象。ZigBee协议结构包括大量的层状元件，包含IEEE 802.15.4 MAC层和PHY层及ZigBee网络(NWK)层。每层提供它们相应的服务和能力。APS sublayer的责任包括维护绑定表，这一功能使两个设备匹配在一起(基于他们的服务和需要)及在两个一定的设备之间发送消息。ZDO的任务包括在网络层定义设备的功能。比如ZigBee协调器或末端设备，在网络层发现设备和确定他们应提供哪种应用服务。发起和／或响应绑定请求并在网络设备之间建立一个安全关系。

ZigBee设备对象(ZDO)，描述了功能的基本分类，这些功能在应用对象设备范围和APS间提供一个接口。ZDO放置在应用帧框架和应用支持子层之间，它能够满足执行在ZigBee协议栈之间的普通请求。ZDO主要负责：初始化应用支持子层、网络层和安全服务规范；从终端应用组装(集合)构架信息以确定和执行发现、安全管理、网络管理和绑定管理。

1.2.3 ZigBee网络安全需求

由于ZigBee网络通过无线电波在空中传输数据，在数据发射机覆盖区域内的几乎所有的无线网络用户都能接触到这些数据。只要具有相同接收频率就可能获

取所传递的信息。要将无线网络环境中传递的数据仅仅传送给一个目标接收者是不可能的。另一方面，由于无线设备在存储能力、计算能力和电源供电时间方面的局限性，使得原来在有线环境下的许多安全方案和安全技术不能直接应用于ZigBee 网络环境，例如防火墙对通过无线电波进行的网络通讯起不了作用，任何人在区域范围之内都可以截获和插入数据；计算量大的加密/解密算法不适宜用于移动设备等。因此，需要研究 ZigBee 网络环境的安全理论、安全方法和安全技术。与有线网络相比无线网络所面临的安全威胁更加严重，所有常规有线网络中存在的安全威胁和隐患都依然存在于无线网络中：外部人员可以通过无线网络绕过防火墙，对专用网络进行非授权访问；无线网络传输的信息容易被窃取、篡改和插入，无线网络容易受到拒绝服务攻击(DoS)和干扰；内部员工可以设置无线网卡以端对端模式与外部员工直接连接。此外，无线网络的安全技术相对比较新，安全产品还比较少。由于 ZigBee 网络在移动设备和传输媒介方面的特殊性，使得一些攻击更容易实施，其安全威胁的具体表现主要有：

a) 攻击者伪装成合法用户，通过无线接入非法访问网络资源；

b) 无线链路上传输的未被加密的数据被攻击者截获；

c) 针对无线连接或设备实施拒绝服务攻击；

d) 不适当的数据同步可能破坏数据的完整性；

e) 恶意实体可能得到合法用户的隐私；

f) 某些节点设备容易丢失，从而泄露敏感信息；

g) 设备的不适当配置可能造成数据的泄露；

h) 恶意用户可能通过无线网络连接到他想攻击的网络上去实施攻击；

i) 恶意用户可能通过无线网络，获得对网络的管理控制权限。

要实现信息的机密性、完整性、可用性以及资源的合法使用这四个基本安全目标，必须采取相应的安全措施对付四种基本安全威胁，即信息泄露、完整性破坏、拒绝服务和非法使用[10]。

总之，无线网络的脆弱性是由于其媒体的开放性、终端的移动性、动态变化的网络拓扑结构、协作算法、缺乏集中监视和管理点以及没有明确的防线造成的口因此，在无线网络环境中，在设计实现一个完善的无线网络系统时，除了考虑在无线传输信道上提供完善的移动环境下的多业务服务平台外，还必须考虑其安全方案的设计，这包括用户接入控制设计、用户身份认证方案设计、用户证书管理

系统的设计、密钥协商及密钥管理方案的设计等等。其中，认证技术和保密性是关键。

1.3 本文主要工作

本文主要针对 ZigBee 无线网络安全接入与应用的核心问题——接入认证、密钥交换与路由协议进行了研究，并取得了相关的研究成果。

1．在介绍现有的无线传感器网络结构体系、安全技术及特点的基础上，对 ZigBee 网络协议体系及特点进行分析，并对其安全需求进行重点讨论。

2．研究无线网络的认证协议与认证技术，对 ZigBee 安全体系与认证技术进行研究，以信任中心为起点对设备接入认证过程进行分析。

3．在研究 ZigBee 网络密钥的应用基础上，主要分析 ZigBee 网络应用层中的密钥建立、密钥传输、密钥请求和密钥交换服务，并对 ZigBee 网络密钥更新和恢复进行研究。

4．在研究 ZigBee 网络应用的各种安全操作后，对 ZigBee 网络中应用的各种安全方案进行分析。

5．ZigBee 网络中，由于网络内节点资源有限，数据包的传送通常需要通过多跳通信方式到达目的端。因此，对路由协议的研究是十分必要的。在分析常用的两种路由算法后，给出改进策略，并提出一种改进的 AODVjr+Cluster 路由协议，同时用 NS2 仿真软件对其进行对比仿真分析。

6．通过对网络层的需求分析，参照国际标准化组织 Internet RFC2501 规定的网络仿真性能评估定量指标。分析对比几种仿真平台，选取 NS2 做为本文研究的仿真平台，并对其安装搭建、工作原理、功能模块、程序设计过程、仿真流程及数据处理等进行了介绍。最后，采用形式化验证工具 AVISPA 对改进的 AODVjr+Cluster 路由协议的安全性进行验证。

第二章 ZigBee 网络认证技术

认证协议的主要作用是确保只有获得授权的用户才能接入系统，访问系统资源。它是通过密码技术使得一个实体向另一个实体证明了某种声称的属性的一个过程[11]。在开放的 ZigBee 无线网络环境中，认证协议的重要性主要体现在两个方面：确认主体的身份以及为通信主体分发会话密钥。对于计算资源、存储资源和能源受陷的 ZigBee 无线网络环境来说，认证协议的性能尤其重要。本章旨在研究 ZigBee 无线网络认证方法。

2.1 认证协议概述

认证协议是允许访问系统资源的基本条件，是安全分布式系统和客户/服务器系统必需的一个基本组成部分，是验证一个用户、处理或设备的过程。国际标准 ISO/IEC9798-1[13]将认证定义为一个实体对另一个实体所称身份的验证。认证的基本要求是正确性和安全性。正确的认证保证一个实体不可能假冒成另一个实体，然而，一个实体在经过正确认证后也有可能出现安全问题。因为如果认证过程中的秘密被暴露，那么通过认证建立起来的会话就是不安全的，因此认证也必须是安全的。还有另外一种称为消息认证的认证形式，消息认证可以保证接收者收到的消息与发送者发送的消息是相同的。

2.2 认证协议与认证技术

当前主流的认证协议有：无可信第三方的对称密钥协议、应用密码校验函数(CCF)的认证协议、具有可信第三方的对称密钥协议、对称密钥重复认证协议、无可信第三方的公开密钥协议和具有可信第三的公开密钥协议等。

认证技术主要有[14]：证明消息的新鲜性和主体真实性的标准机制；双方认证和单方认证；包含可信第三方的认证。

判断某条消息是否新鲜是数据源认证必不可少的一部分，同样在实体认证中，主体也要考虑与意定通信方通信的真实性。因此，证明消息新鲜性或主体真实性的机制就成为认证协议中最基本的一个组成部分。通常主要采用的机制有:挑战一

应答机制(Challenge-response Mechanisms)、时戳机制(Timestamp Mechanism)、序列号或随机数机制等。

双方认证 (Mutual Authentication)是指两个通信实体间的互相认证。需要指出的是双方认证并非是简单的两次单方认证。为此，ISO 和 IEC 已经标准化了许多双方认证机制，如 ISO 公钥三次传输双方认证协议。

在某些情况下，可以使用基于可信第三方(TTP-Trusted Third Party)的集中化认证服务。这种 TTP 服务方式可以是在线的也可以是离线的。认证服务由在线 TTP 提供时，该 TTP 会与系统中或子系统中的大量用户有长期的联系。在 TTP 的帮助下，任意两个用户之间，即使完全不相识，也能够建立安全通信。ISO/IEC 标准化认证协议(9798 系列)有两个标准的结构需要在线的可信第三方的参与其中一个称为“ISO 四次传输认证协议”，另一个称为“ISO 五次传输认证协议”。这两个协议都实现了双方实体认证和认证的密钥协商。

此外，认证协议是建立在密码体制上的，密码体制分为公钥密码体制和对称密码体制。通常公钥密码体制的计算成本约为对称密码体制的 1000 倍，但是公钥密码体制比对称密码体制具有优势：提供不可否认性、可以进行离线认证、提供匿名性等。由于节点资源受陷，在 ZigBee 无线网络的认证协议中，通常基于对称密码体制。但有时也会根据特殊安全需求，同时基于公钥密码体制和对称密码体制，利用二者各自的优势，提高认证协议的效率和性能。

认证协议的设计与特定的应用环境有关，当一个认证主体接收到一个信息时，需要判断信息的完整性、新鲜性和信息是否被重放。通常利用消息的适当的冗余度来识别所接收信息在传送过程中是否被修改过，而且接收者通过信息的冗余度能够意识到自己是否完成了正确的操作。因此，在认证协议中如何把握信息的冗余度也是一个关键问题。

依据认证协议设计所针对的侧重点不同，可以将认证协议细分为实体认证（身份认证）协议、数据源认证、认证及密钥交换协议等，用来防止假冒、篡改、否认等攻击。

实体认证协议，其目的是证明一个用户、系统或应用所声称的身份，更多地涉及验证消息发送者所声称的属性，其目的是防止非法用户接入和访问系统。

数据源认证协议，亦称之为消息认证，是验证通信数据的来源，主要涉及验证消息的某个声称属性。只采用消息认证技术是不能阻止重放攻击的，通常采用

与消息一起提供用户身份的方法来实现数据源认证，例如数字签名。实体认证和数据源认证有单向认证和双向认证。单向认证出验证者认证通信方的身份，而双向认证中通信双方都要进行认证。

认证及密钥交换协议，为身份已经被确认的参与方建立一个共享秘密，致力于为通信双方产生一条安全信道。目的主要有：(1)认证网络用户的身份，防止非法用户假冒合法用户身份占用网络资源、删除或篡改用户存储的数据；(2)认证的分配会话密钥，以便于通过加密技术保护合法用户在网络上通信的内容，防止非法用户窃听。这类协议将认证和密钥交换协议结合在一起，是网络通信中最普遍应用的安全协议。

2.3 认证协议的分析

协议分析是揭示密码协议中存在安全漏洞的重要途径[15]。协议分析的方法有非形式化方法和形式化分析方法。作为密码协议中最基本、最常用的协议—认证协议，在用非形式化的方法进行分析时容易发生错误[16]。一直以来，认证协议的形式化分析受到重视和广泛关注，出现出了很多的研究方法。

所谓形式化方法是指用数学方法描述和推理，基于计算机的系统。直观的说，就是规范语言+形式推理，在技术上通过精确的数学手段和强大的分析工具得到支持[17]。其表现形式通常有逻辑、离散数学、状态机等等。规范语言包括语法、语义以及满足关系等几部分。认证协议的形式化分析方法可以归纳成四类，即基于推理的结构性方法，基于攻击的结构性方法，基于证明的结构性方法和基于计算复杂性的可证明安全方法。可证明安全的方法是由 Bellare，Canetti 和 Krawczyk 于 1998 年提出的，这种方法不仅能够证明密码协议的安全性，还提出了模块化构造安全协议的方法，经过几年的发展，尽管仍旧存在各种各样的缺点，但可证明安全在协议安全性论证上的价值仍然是其他方法无法比拟的，并且也是我们得到正确的、安全的协议过程中一个非常重要的工具[18]。文中对 ZigBee 认证协议的形式化分析采用的就是可证安全的方法。

可证明安全方法采用了归纳推理过程(从一个已知的前提得出结论的逻辑过程)，其主要思想是把攻破协议的问题规约到求解某个困难问题上。1984 年，Goldwasser 和 Micali 为“可证明安全性”做出了奠基性的工作，将概率引入了密码

学[19]。1987 年，Fiat 和 Shamir 提出了“随机预言机模型”(Random Oracle Model，RO 模型)[20]。在随机预言机模型中，Hash 函数(散列函数)被假设为理想函数。Hash 函数被形式化为一个预言机，生成真随机值。可证明安全性的核心理论是提供模型和定义，安全性也最终简化为原子原语的安全性。Bellare 和 Rogaway(BR93)将这种思想应用于密钥交换协议，建立了攻击者能力模型及相关的安全定义，并且对两方的实体认证和密钥交换协议进行了安全性证明。此后，出现了很多 BR93 模型的扩展，如 Bellare 和 Rogaway 于 1995 年提出的密钥建立模型 BR95[21]、Bellare，Pointcheval 和 Rogaway(BPR)于 2000 年提出的基于口令的相互认证和密钥建立模型[22]、Bresson，Chevassut 和 Pointcheval(BCP)于 2001 年提出的群组认证的密钥交换安全模型[23-25]以及最近 Abdalla，Fouque 和 Pointcheval(AFP)提出的基于口令的认证的密钥交换模型[26]。Bellare，Canetti 和 Krawczyk(BCK)[27]在 1998 年引入了模块化的思想，通过提供可重用的模块来构造新的可证安全的协议。在此基础上，Shoup 提出了 Shoup 密钥交换模型[28]，Canetti 和 Krawczyk 提出了 Canetti-Krawczyk(CK)模块化的协议分析与设计模型畔[29]，Canetti 在 CK 模型的基础上又进一步提出了通用可组合(Universally Compassable，UC)模型[30-31]。其中应用比较广泛的是 CK 模型、BCP 模型以及 UC 模型。

2.4 ZigBee 安全体系与协议认证研究

完整的安全体系是任何通信技术大范围应用的前提，ZigBee技术的发展同样离不开其安全体系的完善。接入认证是任何一个网络保障安全的第一道防线，用户需要通过接入认证来确认它的合法性，然后再确定这个用户的特定权限。用户在进入一个安全系统之前，首先要经过一个接入认证过程，用户向系统出示自己的身份，身份认证机制对用户的身份进行判定，判断是否为合法用户，确定用户的身份，从而使用户获得相应的访问权限；对于不合法的用户则拒绝访问。用户在进入系统之后，系统内部的安全机制也会根据身份认证机制所确定的用户身份来对用户进行检测，判断是否为合法用户。可见接入认证机制是安全系统中的进入安全系统的第一道屏障，其它的安全服务都依赖于它。如果身份认证出了问题，其它的安全服务也将功亏于溃[32]。

2.4.1 ZigBee 网络安全体系结构

ZigBee 网络安全体系结构包括协议栈的 3 层安全机制。MAC 层、NWK 层、APS 层的安全机制任务为负责安全地传输它们各自的帧。此外，APS 子层提供服务来建立和维护安全关系。ZigBee 设备对象（ZDO）管理设备的安全政策和安全配置。

ZigBee网络采用了对称密钥的安全机制。密钥由网络层和应用层根据实际应用需要生成，并对其进行管理、存储、传送和更新等。安全机制由安全服务提供层提供，系统的整体安全性是在模板级定义的，这就是说模板定义某一特定网络中应该实现何种类型的安全。这个安全级别由ZigBee安全体系结构提供，它依赖于对称密钥安全保护、保护机制的使用和密码机制的适当的执行，以及与之相关的安全政策。安全体系结构中的信任从根本上减少了安全初始化中的信任、密钥资料的安装、安装进程中的信任和密钥资料的存储。

安全协议的执行（如密钥建立），都假设完全地执行全部协议，且不遗漏任何步骤。还应该假定如期望中地操作随机数目生成器。此外，它假定如果用一种不安全的方法获取密钥，就不能在设备外获取密钥。这就是说，一个设备不能有目的或无意的传送它的密钥资料到另外一个设备，除非在密钥运输之中密钥资料受到保护。

2.4.2 ZigBee 信任中心应用概述

信任中心在一个 ZigBee 网络内所有设备信任的设备上运行，为了网络和点对点应用配置管理的目的进行密钥分配。信任中心的配置是在商业模式或住宅模式中进行操作，并且可能通过直接发送链路密钥或直接发送主密钥用于帮助建立端到端应用密钥。

商业模式下，信任中心被设计为用于高安全级别的商业应用。在这种模式下，信任中心将维护设备列表、主密钥、链路密钥和网络密钥，它需要控制和执行网络密钥的更新政策以及网络准入。此时，存储器要求信任中心随网络中设备数量增大而增加，要 NIB 中的 nwkAllFresh 属性设置为 TRUE。

信任中心的住宅模式被设计为低安全级别的居住应用。在该模式下，信任中心将维护设备列表、主密钥和带有网络中所有设备的链路密钥，但是，它将维护

网络密钥并控制网络准入政策。此时，存储器要求信任中心不随网络中设备数量增大而增加，要 NIB 中的 nwkAllFresh 属性设置为 FALSE。

2.4.3 ZigBee 认证过程

设备请求连接到一个安全网络时，需要经过一系列的安全认证，只有在确定了设备的身份、属性及其安全性之后，设备才能被允许加入网络。一个设备通常通过以下两种方式加入网络：设备用 MAC 层连接程序来加入网络和设备直接同一个预先所指定的设备连接加入网络。ZigBee 主要通过信任中心来实现设备的接入控制与认证。信任中心作为网络中的所有设备所信任的设备，它负责对每个要加入网络的设备进行身份认证及安全验证。设备一旦通过安全认证，信任中心将为其分配密钥。严格意义上来说，网络中的所有成员将公认一个信任中心，而且在每个安全的网络中都有一个确切的信任中心。其首要目的是确保只有获得权限的终端或节点才能接入网络系统，访问系统资源。而对于一个已经存在网络中且被确认的设备，如它提供了接入控制服务，则在它的接入控制列表中（ACL）将含有一个设备的列表，该列表所包含的是其希望接收帧的发出设备。如图 2-1 所示，信任中心对设备的认证主要在设备连接网络过程中实现。

当设备要连接网络时，其应用层会向网络层发送NLME-NETWORK-DISCOVERY.request原语，网络层接收到该原语后，将发送MLME-SCAN.request原语请求MAC层执行一个主动扫描。新设备的MAC层在扫描过程中一旦接收到有效长度不为零的信标时，将向其网络层发送一个包含信标设备地址、是否允许连接和信标载荷信息的MLME-BEACON-NOTIFY.indication原语。该设备的网络层将检查信标载荷中的协议标识符域的值，并验证它是否与ZigBee协议识别符匹配。若不匹配，则将忽视该信标。反之，设备从所接收的信标中，将相关的信息复制到它的邻居表中。

在MAC层完成对信道的扫描，向网络层管理实体发送MLME-SCAN.confirm原语之后，网络层将发送NLME-NETWORK-DISCOVERY.request原语，其参数包括扫描得到的网络属性参数。这些属性参数主要有ZigBee版本号、堆栈结构、个域网标识符参数（PANID）设置为所希望连接的网络标识符，RejoinNetwork参数设置为FALSE，JoinAsRouter参数设置为设备是否以路由器同网络连接。

只有那些还没有同网络连接的设备才能执行该连接流程。如果任何其他设备

执行这个连接流程，则网络管理实体将终止这个流程，并且向其上层发送状态参数INVALID-REQUEST的NLME-JOIN.request原语。

对于一个还没有同网络连接的设备，NLME-JOIN.request原语将使得网络层在邻居表中搜索一个合适的父设备。合适的父设备必须满足3个条件：一个所希望的PAN标识符；允许连接；路由成本不超过3。如果在邻居列表中存在潜在的父设备子域，则该子域设置为1。

如果邻居列表不包括合适的父设备，网络层管理实体将发送参数状态为NOT-PERMITTED的NLME-JOIN.confirm原语。若邻居列表中存在多个合适的父设备，则选择具有到协调器节点最小跳数的设备。如果同时有多个到协调器节点最小跳数的设备，可以在其中任意选择一个。一旦选择一个父设备，网络层管理实体将向MAC层发送NLME-ASSOCIATE.request原语，其原语的地址参数为在邻居列表中所选择的设备的地址，并通过MLME-ASSOCIATE.confirm原语将连接的状态返回到网络层管理实体。

如果试图连接网络没有成功，网络层将会接收到从MAC层发送来的MLME-ASSOCIATE.confirm，并同时反馈状态参数为错误代码。如果状态参数表明拒绝与邻居设备连接（PAN容量PAN接入拒绝），则尝试连接的设备将把邻居列表中潜在的父设备子域设置为0，以表明尝试连接失败。潜在父设备为0使的网络层将不会发送另一个连接请求原语去尝试连接该邻居设备。每次发送MLME-SCAN.request原语，将邻居表中的潜在父设备子域设置为1。如果潜在的父设备不允许连接新的路由器，并且要连接的设备将JoinAsRouter参数设置为TRUE，则连接请求也可能不成功。此时，NLME-JOIN.confirm原语将给出NOT-PERMITTED的状态，子设备的应用层将再次尝试连接，但此时只能作为一个终端设备，并将发送另一个NLME-JOIN.request原语，且将原语的JoinAsRouter参数设置为FALSE。如果尝试连接失败，网络层管理实体将试图从邻居列表中寻找另一个合适的父设备。若不存在这样的设备，网络层管理实体将发出NLME-JOIN.confirm原语，其状态参数值为MLME-ASSOCIATE.confirm原语所返回的值。又若尝试连接网络失败，并且存在第2个邻居的设备，该设备可以作为适合的父设备，则网络层将启动连接第2个设备的MAC层连接程序。网络层将不断重复这个过程，直到成功地与网络连接或者已经尝试了所有可能连接的网络。如果设备不能成功地连接由上层所指定的网络，网络层管理实体将通过

NLME-JOIN.confirm原语来终止进程，其原语的状态参数为最后收到的MLME-ASSOCIATE.confirm原语所返回的值。在这种情况下，设备将不接收有效的逻辑地址，也不允许在网络中通信。

若连接网络成功，网络层将收到MLME-ASSOCIATE.confirm原语，该原语中必将包括一个在网络中唯一的16位逻辑地址，并且设备在未来的通信中将使用这个逻辑地址。然后，网络层将设置相对应的邻居表的关系域，有来表示邻居设备作为它的父设备。此时，父设备将把新连接的设备增加到它的邻居表中。

如果设备试图同一个安全网络连接，如果它作为一个路由器，则在发送信标前，必须等待父设备对它进行验证，验证通过之后才可以进行连接。这个过程相当于对设备进行接入认证。

父设备在接收子设备加入请求之前，其网络层管理实体先要确定设备是否愿意接收其他子设备的连接请求。同意请求之后，父设备通过与协调器交互信息，根据网络自身安全属性对自设备进行验证，验证通过后父设备将为该子设备分配一个网络地址，并可以依据信任中心发出的安全等级将子设备的访问权限进行设置。

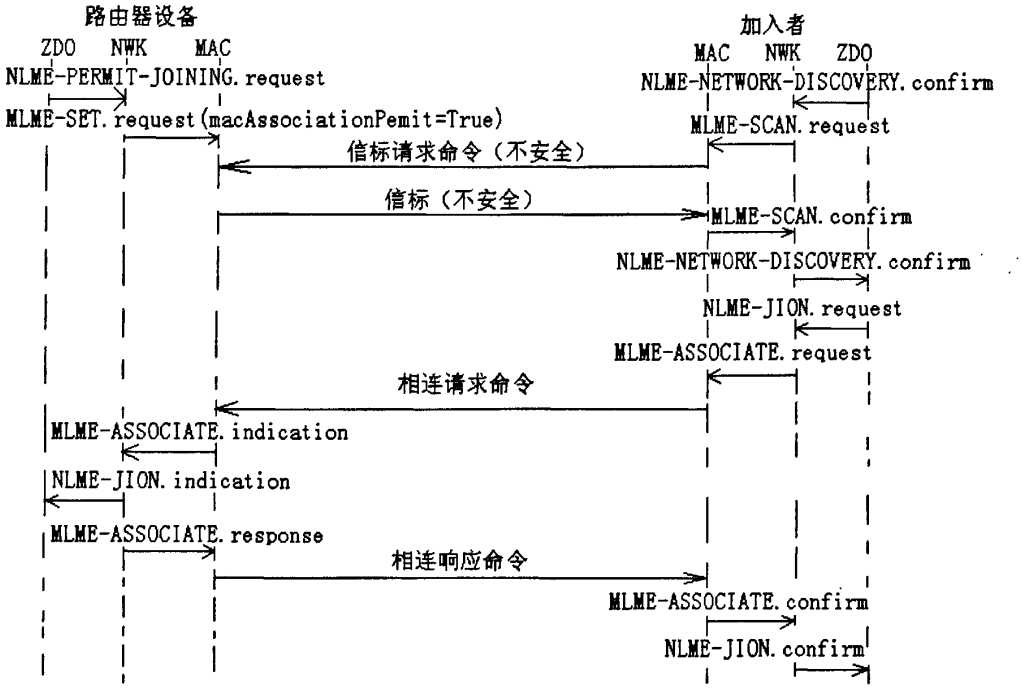

图2-1 设备连接网络过程

Fig 2-1 Devices connect to the network process

在整个验证过程中，协调器充当信任中心，网络层采用分布式地址分配方案

来分配网络地址，即该方案为每一个父设备分配一个有限的网络地址段。这些地址在一个特殊的网络中是唯一的，并由父设备分配给它的子设备。信任中心决定父设备权限、网络安全级别，并通过父设备负责对请求连接设备进行间接验证、控制访问权限。

总而言之，ZigBee 网络主要通过配置信任中心来实现网络的认证功能。无论是在居住模式还是在商业模式，信任中心将控制和执行设备的网络准入。认证的主要思路是：信任中心首先验证在运行密钥建立协议之前安装在每个设备里初始信任信息（如主密钥），若设备的初始信息验证通过，它将对设备能否连接网络给予验证，并为已经通过验证的设备分配密钥，从而确保设备之间端到端的通信安全及整个网络的安全运转。

2.5 本章小结

本章主要对 ZigBee 网络认证过程及其安全体系进行了详细分析，包括认证协议的概述、主流认证技术的介绍、认证协议的分析方法、及协议安全的形式化验证方法。

第三章 ZigBee 网络密钥研究

3.1 密钥交换协议概述

密钥交换协议是安全通信的基础，安全性和正确性是最基本的要求。通常，通信方运行认证协议的目的在于能够在高层或者应用层上进行安全通信。因此，为了进行高层或应用层安全通信而运行的实体认证协议通常都包含认证的密钥建立，或者密钥交换(Key Exchange)等过程。在认证的密钥建立协议中，密钥建立素材也是重要的协议消息，它也是数据认证的内容。

密钥交换协议是 n 方消息驱动协议的一种特殊情况，需要增加一些语法来描述。一个 n 方消息驱动协议是 n 个程序的集合，其中每个程序由不同的参与者运行。在密钥交换 KE (Key-Exchange)协议 π 中，Pi 收到的激活请求的形式是 establish-session (Pi，Pj，s，role)，Pj 是另一个参与者，s 是会话标识(session-id)，roles {l, R}表示 Pi 是发起者还是 π 响应者。

密钥交换协议中 Pi 的本地输出形式是(Pi，Pj，s，K)，Pj、s 同上，K 是会话密钥。密钥交换协议的一次执行称为一个密钥交换会话(KE-session)。空的 K 表示会话出现错误，相应的密钥交换会话的状态是被中止的(aborted)。非空的 K 被标识为‘秘密’，相应的密钥交换会话的状态是完成的(completed)。

在密钥交换协议的一次执行中，Pi 有一个输入为{Pi，Pj，s，role}的会话，Pj 有一个输入为{Pi，Pj，s’，role’ }的会话。如果 S=S’，则称这两个会话是匹配的（注意，这里并不要求 role 不等于 role’)。

3.2 密钥的建立、传输、请求与交换服务

APS 层负责那些需要安全地传输输出帧、安全接收输入帧以及安全建立和密钥的处理步骤。网络层发送原语到 APS 层对密钥进行管理，下表 3-1 列出了用于密钥管理和维护的服务原语。上层也决定使用哪一个安全级别保护输出帧。在这个规范中，对所有帧和域的格式根据它们在 NWK 层传输的次序进行了描述，从左到右，最左边的位先传送。每个域中的位数字从 0（最左边且最不重要）到 k-1（最右边且最重要），该域的位长度为 k。比单个字节长的域将有次序的发送到下一层，

该域包含最低数字位的字节到包含最高数字位的字节。

表 3-1 APS 层安全原语

Table 3-1 APS Layer Security Primitives

APSME 安全原语	描述
APSME-ESTABLISH-KEY	使用 SKKE 方法与另一个 ZigBee 设备建立链路密钥
APSME-TRANSPORT-KEY	从一个设备到另一个设备传输安全资料
APSME-UPDATE-DEVICE	当一个新的设备加入网络或一个已存在的设备离开网络时，通知信任中心
APSME-REMOVE-DEVICE	信任中心用来通知路由器：路由子设备将从网络中移除
APSME-REQUEST-KEY	设备用来请求信任中心发送应用主密钥或发送当前的网络密钥
APSME-SWITCH-KEY	信任中心用来告知设备交换一个新的网络密钥

3.2.1 密钥的建立

APSME 提供允许两个设备相互建立链路密钥的服务。初始信任信息（如主密钥）必须在运行密钥建立协议之前安装在每个设备里。

APSME-ESTABLISH-KEY.request 原语用来初始化一个密钥建立协议。当需要和另一个设备安全通信时使用该原语。其中，一个设备作为发起设备，另一个设备作为响应者。发起设备发出 APSME-ESTABLISH-KEY.request，其参数显示出响应设备的地址信息，以及用来启动密钥建立的密钥建立协议（既 SKKE 间接或直接）。只有当一个设备要求与一个响应设备建立链路密钥时，发起设备的高层产生这种原语。如若发起设备希望使用响应者的父设备作为联络（为了 NWK 安全的目的），它将设置 UseParent 参数为 TURE，ResponderParentAddress 参数为响应者父设备的 64bit 延长地址。接收 APSME-ESTABLISH-KEY.request 原语，其 KeyEstablishmentMethod 参数等于 SKKE，将令 APSME 执行 SKKE 协议。本地 APSME 将作为这个协议的发起者，由 ResponderAddress 参数指示的 APSME 将作为这个协议的响应者，并且 UseParent 将控制是否通过 ResponderParentAddress 参数给定的响应者的父设备间发送信息。

在一个建立密钥协议执行完成或失败后，发起者和响应者的 APSME 将发送 APSME-ESTABLISH-KEY.confirm 原语到 ZDO。如果密钥建立成功，发起者和响

应者的 AIB 将根据新的链路密钥进行更新，发起者将能安全地与响应者通信。如果没能成功建立密钥，AIB 将不会发生改变。

响应者收到一个来自发起者的初始密钥建立请求消息时，它的 APSME 将发出 APSME-ESTABLISH-KEY.indication 原语到 ZDO，并将与发起者相联系的主密钥存在其 AIB 中。ZDO 接收到 APSME-ESTABLISH-KEY. indication 原语后，可能使用 KeyEstablishmentMethod 和 InitiatorAddress 参数来决定是否建立一个发起者密钥，同时 ZDO 通过 APSME-ESTABLISH-KEY.indication 原语来响应。

响应者的 ZDO 将使用 APSME-ESTABLISH-KEY.response 原语来响应一个 APSME-ESTABLISH-KEY.indication 原语。ZDO 将决定是否继续建立密钥或中断建立。该决定显示在 APSME-ESTABLISH-KEY.indication 原语的 Accept 参数里面。APSME-ESTABLISH-KEY.Response 原语由 ZDO 产生，并提供给 APSME，跟随一个来自发起设备的请求来启动一个密钥建立协议。这一原语给响应者 ZDO 提供了一个决定是否拒绝建立一个带有指定发起密钥的机会。如果 Accept 参数为 TRUE，响应者的 APSME 将尝试执行由 KeyEstablishmentMethod 参数指示密钥建立协议。如果 KeyEstablishmentMethod 等于 SKKE，APSME 将执行 SKKE 协议。本地的 APSME 将作为这个协议的响应者，由 InitiatorAddress 参数指示的 APSME 将作为这个协议的发起者。若 Accept 参数为 FALSE，本地 APSME 将中断并删除所有与不确定的密钥建立协议有关的媒体数据。图 3-1 中显示了两个设备之间成功建立密钥的必要的原语的传输次序。

发起者和响应者上的 APSME 执行“对称—密钥”、“密钥—协定”方案。分享密钥应为在发起者之间分享的主密钥，是从适当的主密钥要素 AIB 中的 DeviceKeyPairSet 属性中获得的。

3.2.2 密钥的传输服务

APSME 提供传输密钥服务，允许一个发起者向一个响应者传输密钥资料。它能传输不同类型的密钥资料，如表 3-2 所示。

当一个发起设备上的 ZDO 请求传输一个密钥到一个响应设备时，将产生 APSME-TRANSPORT-KEY.request 原语，该原语的接收将引起 APSME 产生一个“传输—密钥”命令包。如果 KeyType 参数为 0x00（即信任中心主密钥），密钥子域将被设置为 DestinationAddress 参数的值，源地址子域将被设置为本地设备地址。

该命令帧将被安全保护。如果安全进程成功，它将发出 NLDE-DATA.request 原语到 TransportKeyData 参数的 ParentAddress 子参数所述的设备。如果 KeyType 参数为 0x01，则密钥子域将被设置为 TransportKeyData 参数的 Key 子参数的值，序列数子域将被设置为该参数的 KeySeqNumber 子参数的值，目的地址子域将被设置为 DestinationAddress 参数的值，源地址子域将被设置为本地设备地址。这个命令帧将被安全保护。如果安全进程成功，它通过发出 NLDE-DATA.request 原语到 TransportKeyData 参数的 ParentAddress 子参数或 DestinationAddress 参数所指定的设备。

表 3-2 APSME-TRANSPORT-KEY.request 参数

Table 3-2 APSME-TRANSPORT-KEY.request parameters

参数名	类型	有效范围	描述
Dest-Address	设备地址	任何有效的 64bit 地址	目的设备的延长 64bit 地址
Key-Type	整型	0x00	0x00 表示这是一个主密钥，使用它在信任中心和另一个设备之间建立链路密钥；
		0x01	0x01 表示这是一个网络密钥；
		0x02	0x02 表示这是一个主密钥，使用它在两个设备之间建立链路密钥；
		0x03	0x03 表示这是一个链路密钥，使用它在两个设备之间作为安全基础。
Transport-KeyData	可变的	可变的	密钥与证明和使用参数一起传输

当 APSME 接收一个已成功地加密和鉴权的传输密钥命令时，它将产生 APSME-TRANSPORT-KEY.indication 原语用来告知 ZDO 接收密钥信息。并且它的密钥类型域设置为 2 或 3（即应用链路或主密钥）。APSME 接收到一个已成功地加密和鉴权的“传输—密钥”命令时，它同样产生 APSME-TRANSPORT-KEY.indication 原语，但它的密钥类型域设置为 0 或 1（即信任中心或网络密钥），并且密钥描述符域的目的地址子域等于本地地址。

在接收一个传输密钥命令后，APSME 将执行输入、输出帧安全进程，然后检查密钥类型子域。如果密钥类型域设置为 2 或 3，APSME 将发出

APSME-TRANSPORT-KEY. indication 原语，它的 SrcAddress 参数设置为密钥传输命令的源地址，KeyType 类型参数设置为密钥类型域。TransportKeyData 参数将被设置如下：Key 子参数将被设置为密钥域，PartnerAddress 子参数将被设置为对方地址域，如果发起者域的值为 1，Initiator 参数将被设置为 TRUE，反之则设置为 0。如果密钥类型子域设置为 0 或 1，并且目的地址等于本地地址，APSME 将发出 APSME-TRANSPORT-KEY. indication 原语，它的 SrcAddress 参数设置为密钥传输命令的源地址，KeyType 类型参数设置为密钥类型域。TransportKeyData 参数将被设置如下：Key 子参数将被设置为密钥域，在它为一个网络密钥的情况下，KeySeqNumber 子参数将被设置为序列数域。如果密钥类型子域设置为 0 或 1，并且目的地址不等于本地地址，APSME 将发送命令到目的地址域显示的地址，并发出带有安全失效的 NLDE-DATA.request 原语。

当接收一个不安全的传输密钥命令时，APSME 将检查密钥类型子域。如果密钥类型子域设置为 0，并且目的地址域等于本地地址，设备不具备信任中心主密钥和地址（即 AIB 中的 apsTrustCenterAddress），此时，APSME 应该发出一个 APSME-TRANSPORT-KEY. indication 原语。同样，如果密钥类型子域设置为 1，并且目的地址域等于本地地址，设备不存在网络密钥，则 APSME 将发出一个 APSME-TRANSPORT-KEY. indication 原语，并且目的地址域等于本地地址，设备不存在网络密钥，则此时 APSME 将发出 APSME-TRANSPORT-KEY. indication 原语。如果 APSME 发出一个 APSME-TRANSPORT-KEY. indication 原语，它的 SrcAddress 参数设置为密钥传输命令的源地址，KeyType 类型参数设置为密钥类型域。TransportKeyData 参数将被设置如下：Key 子参数将被设置为密钥域，并且当它为一个网络密钥的情况下，KeySeqNumber 子参数将被设置为序列数域。

3.2.3 密钥的请求服务

APSME 提供请求密钥服务，该服务允许一个设备请求来自另一个设备（如它的信任中心）的当前网络密钥或主密钥。

当设备的 ZDO 请求一个当前网络密钥和一个新的端到端应用主密钥时，它将产生 APSME-REQUEST-KEY.request 原语，该原语允许 ZDO 请求一个当前网络密钥和一个新的端到端应用主密钥。接收到 APSME-REQUEST-KEY.request 原语后，设备将产生一个请求密钥命令帧，这个命令帧的密钥类型域将设置为与 KeyType

参数相同的值相同。如果 KeyType 参数为 0x02（即应用密钥），这个命令帧的对方地址域将为 PartnerAddress 参数。反之，这个命令帧的对方地址域将不存在。将安全保护应用于这个命令帧，如果安全进程成功，它将发出一个 NLDE-DATA.request 原语到 DestAddress 参数所述的设备。

当 APSME 接收一个请求命令帧，且该帧成功地被加密和鉴权后，它将产生 APSME-REQUEST-KEY. indication 原语。在接收该原语后，ZDO 将被告知 SrcAddress 参数涉及的设备正在请求一个密钥。这个命令帧的密钥类型域将设置为与 KeyType 参数的值相同。如果 KeyType 参数为 0x02，PartnerAddress 参数显示设备将接收的密钥，该密钥与请求密钥设备的密钥是相同的。

3.2.4 密钥交换服务

APSME 提供密钥交换服务，该服务允许一个设备（如它的信任中心）告知另一个设备它将交换一个新的主动网络密钥。

当设备的 ZDO（如信任中心）想告知一个设备交换一个新的主动网络密钥时，它将产生 APSME-SWITCH-KEY.request 原语，该原语允许一个设备请求另一个设备它将交换一个新的主动网络密钥。在接收到该原语后，设备首先产生一个交换密钥命令帧，该命令帧的序列数域将被设置为与 KeySeqNumber 参数的值相同。将安全保护应用于这个命令帧，如果安全进程成功，它将发出一个 NLDE-DATA.request 原语到 DestAddress 参数所指定的设备。

当 APSME 接收一个请求命令帧，且该帧成功地被加密和鉴权后，它将产生 APSME-SWITCH-KEY. indication 原语。在接收该原语后，ZDO 将得知 SrcAddress 参数涉及的设备正在请求 KeySeqNumber 参数涉及的网络密钥，使其成为新的活动网络密钥。

3.3 ZigBee 网络密钥的更新

当网络密钥需要更新时，信任中心和网络设备将分别执行各自的以下进程实现更新。

操作在住宅模式时，出于限制执行复杂度的折中考虑和减少安全成本，信任中心将不会执行网络更新。网络设备处于居住模式的正常操作状态（即信任中心

主密钥不存在)将不接收更新的网络密钥。此时，将忽略传输密钥或者一个 KeyType 参数设置为 0x01（即网络密钥）的交换密钥命令。

操作在商业模式时，信任中心将保持和维护网络中所有设备的列表。为实现网络密钥的更新，信任中心首先发出新网络密钥到该设备列表中的每个设备，并且让每个设备交换这个新的密钥。通过发出 APSME-TRANSPORT-KEY.request 原语，新的网络密钥将被发送到网络列表中的设备，且该原语的 DestAddress 参数设置为列表设备的地址，KeyType 参数设置为 0x01（即网络密钥）。TransportKeyData 子参数将设置如下：KeySeqNumber 子参数设置为这个网络密钥的序列计数值，NetworkKey 子参数设置为网络密钥，UseParent 子参数设置为 FALSE。如果对于之前分配的网络密钥序列计数描述为 N，则对于这个新网络密钥的序列计数将为（N+1）mod256。通过发出 APSME-SWITCH-KEY.request 原语，信任中心让每个设备交换这个新的密钥，该原语的 DestAddress 参数设置为列表中设备的地址，KeySeqNumber 参数设置为更新网络密钥的序列计数值。

网络设备处于商业模式的正常操作状态（即信任中心主密钥存在）下，在接收 KeyType 参数设置为 0x01 的 APSME-TRANSPORT-KEY.indication 原语后，只有 DestAddress 参数与信任中心地址相同（如 AIB 的 apsTrustCenterAddress 属性中所维护的）时，设备将接受 TransportKeyData 参数作为一个网络密钥。如果设备接受，并且如果设备有能力存储一个预备的网络密钥，TransportKeyData 参数包含的密钥和序列数数据将代替预备的网络密钥。否则，TransportKeyData 参数包含的密钥和序列数数据将代替主动网络密钥。

网络设备处于商业模式的正常操作状态（即信任中心主密钥存在）下并且在接收 APSME-SWITCH-KEY. indication 原语后，仅仅当 SrcAddress 参数与信任中心地址相同时，一个设备将交换它的主动网络密钥为 KeySeqNumber 参数涉及的密钥（如 AIB 的 apsTrustCenterAddress 属性中所维护的）。

对于两个设备的成功的网络密钥更新进程，如图 3-1 所示，信任中心首先将发出带有序列数 N 的网络密钥到设备 1 或设备 2。其中，设备 1 为一个 FFD，有存储两个网络密钥的能力，一个主动密钥和一个预备密钥。此时，设备 2 应为 RFD，只能存储单一的网络密钥。接收传输密钥命令之后，设备 1 用新的网络密钥来代替它的预备密钥；但是设备 2 必须用新的密钥来代替它的网络密钥。在接收交换密钥后，设备 1 让新的网络密钥成为主动网络密钥；而设备 2 仅有一个主动网络

密钥，所以它忽视了这一命令。

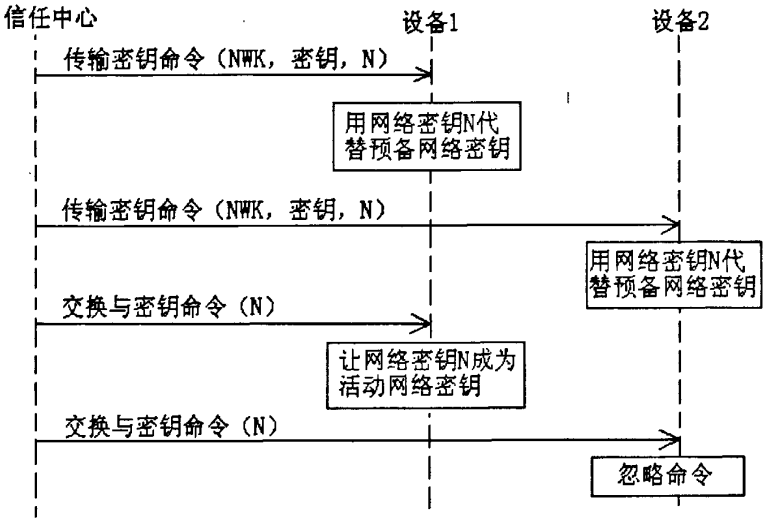

图 3-1 两个设备的网络密钥更新进程

Fig 3-1 Update process of two equipment network key

3.4 ZigBee 网络密钥的恢复

需要恢复网络密钥的时候，一个网络设备和信任中心将按已经设置模式执行恢复进程操作。具体流程如图 3-2 所示，网络设备从信任中心请求当前网络密钥。信任中心用当前密钥响应，并告知设备交换这个密钥。

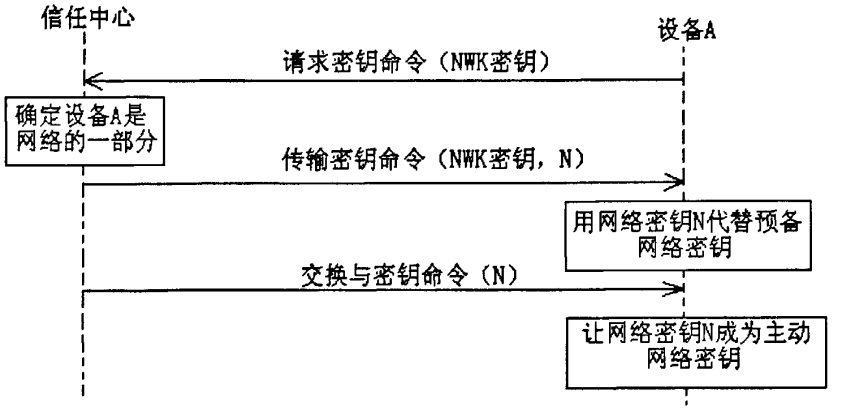

图 3-2 网络密钥恢复进程

Fig 3-2 Recovery process of network key

网络设备处于居住模式的正常操作状态下，并在接收到 KeyType 参数设置为 0x01 的 APSME-REQUEST-KEY.indication 原语后，信任中心将判断 SrcAddress 参

数所指示的设备是否存在于网络上所有设备的列表中。如果设备出现在该列表上，信任中心将发出 APSME-TRANSPORT-KEY.request 原语，其 DestAddress 参数设置为正在请求密钥设备的地址，并且 KeyType 参数设置为 0x01。TransportKeyData 子参数设置如下，KeySeqNumber 子参数设置为这个网络密钥的序列计数值，NetworkKey 子参数设置为网络密钥，UseParent 子参数设置为 FALSE。接下来，通过发出 APSME-SWITCH-KEY.request 原语，信任中心将要求一个设备交换这个新的密钥，该原语的 DestAddress 参数设置为已请求密钥设备的地址，KeySeqNumber 参数将设置为更新网络的序列计数值。

3.5 本章小结

密钥交换协议(Key-exchange protocol)是通信双方在不安全的网络环境中产生共享密钥的机制。本章主要分析 ZigBee 网络应用层中的密钥建立、密钥传输、密钥请求和密钥交换服务，并对 ZigBee 网络密钥更新和恢复进行了较为详细分析。

第四章 ZigBee 网络的安全方案研究

ZigBee 技术规定的安全方案使用以下几种安全操作：位顺序、串接、整数编码和计时器增加、计数模式（CTR）加密、密码链块-信息鉴权码（CBC-MAC）验证、计数模式和密码链块-信息鉴权码（CCM）的加密和验证、高级加密标准（AES）加密、个域网信息库（PIB）的安全要素。

其中的密码算法能提供以下几种不同的密码属性（密码服务）：

机密性(Confidentiality)：确保数据仅能为那些被授权的主体获得。通常是通过这种方式来实现，即对数据进行加密以使得只有掌握正确解密密钥的主体能够恢复它的。在密码协议中，机密性是确保密钥和其它数据安全的重要手段。具体通过对称或非对称密码算法实现。

数据完整性(Integrity)：确保数据没有被未授权的主体修改。通常是通过以下方式来实现：Hash 函数和加密相结合的方式（例如数字签名）或消息鉴别码（Message Authentication Code，简称 MAC）。数据完整性在密码协议中起到保护身份域、临时值（Nonce）等消息元素的作用。

数据源鉴别(Data Origin Authentication)：确保所接收的到数据确实是来自所声明的源头。由于修改了数据必然修改了它的起源，所以数据源鉴别包含了数据完整性。可以通过 MAC 或数字签名算法来实现。

非否认性(Non-repudiation)：防止消息的发送方或接收方对他所发送过的消息进行抵赖。通常是通过数字签名算法来实现。鉴别和密钥建立协议中很少使用这一密码属性，但在电子商务协议中应用的较为普遍。

4.1 ZigBee 安全方案概述

当设备在安全模式下运行时，就使用安全方案。安全方案由提供了安全服务的、在 MAC 帧上执行的一系列安全操作组成。安全方案的名称会显示对称加密算法、模式和完整性码比特长度。完整性码的比特长度小于或等于对称算法的块长度，并决定了概率——完整性码的随机假设是正确的。比特长度和以下算法强度并不对应。对于所有在 ZigBee 标准中的安全方案，所用算法是高级加密算法。通常情况下，执行安全操作的设备应支持 AES-CCM-64 安全方案，以及 0 个或者附

加多个另外的安全方案。每个安全方案由一个字节值指定（如表 4-1 所示），标识符 0x00 表示没有使用安全模式。

表 4-1 安全方案列表

Table 4-1 List of security program

标识符	安全组件名称	安 全 服 务			
		接入控制	数据加密	帧完整性	序列更新(可选)
0x00	None				
0x01	AES-CTR	X	X		X
0x02	AES-CCM-128	X	X	X	X
0x03	AES-CCM-64	X	X	X	X
0x04	AES-CCM-32	X	X	X	X
0x05	AES-CBC-MAC-128	X		X	
0x06	AES- CBC-MAC-64	X		X	
0x07	AES- CBC-MAC-32	X		X	

4.2 安全操作

安全方案的组成通常采用了位顺序、串联、整数编码和计数器增加、CTR 加密、密码链块-信息鉴权码(CBC-MAC)验证、计数模式和密码链块-信息鉴权码(CCM)的加密和验证、高级加密标准(AES)加密及个域网信息库(PIB)的安全要素。

1．位顺序

在 ZigBee 协议标准中的安全操作，位被定义为集合{0，1}中的一个元素。一个 8 位字节（即一个字节）定义为一个 8 的位串，该串按照所发送的顺序排列，其中 bit7 为字节中的第一位、bit0 为最后一位。一个字节串按照最高的字节排在最前面的顺序进行排列。

2．串联

两个长度分别为 m 和 n 的字节串 a 和 b 的串联表示为 a ‖ b，它是一个长度为 m+n 的字节串，最左边的 m 个字节等于 a，最右边的 n 个字节等于 b。

3．整数编码和计时器增加

除非特别的声明，否则在本文所介绍的安全操作中，当整数表示为字节串时，

第一个字节（即字节 0）对应最高位的字节，并且第一个字节中的第一位(bit7)对应于 MSB。长度为 n 的字节串 A，写为位串 $A=a_{0,7}a_{0,6}a_{0,5}\ldots a_{n-1,1}a_{n-1,0}$。字节串或者位串被转换成整数 I，把每一位的值 $a_{i,j}$ 设置为 $a_{i,j}*2^{8i+j}$ 的值，并将 I 设置为所有值的和。

计数器增加操作以编码成长度为 n 的字节串的整数为输入。当请求计数器增加操作时，整数加 1。若所增加的整数小于 2^{8n}，操作将返回新的整数编码字节串。否则，操作将把计数器设置为 2^{8n}-1，并返回一个错误（即计数器操作导致整数溢出）。

4．密码分组链接(CBC)模式

CBC 算法过程如下[36,37]：

for $i=1$ *to* n $Y_i=E_k(P_i\oplus Y_{i-1})$（加密）；（初值 Y_0 为计数器或不重复的伪随机数）

for $i=1$ *to* n *do* $P_i=D_k(Y_i)\oplus Y_{i-1}$；（解密）

$Y_n=E_{k_1}(Y_n)$（可选进程）；MAC=$MSB_m(Y_n)$；（认证）

当最后一组明文长度 r 小于分组长度 T 时，可采用补位或密文挪用等措施。当 m=T 时，一般要采用可选进程，以减轻穷举攻击的威胁。CBC 模式既可作为加密模式，又可作为认证模式，还可以作为认证加密模式。当 CBC 模式作为认证加密模式时，需要采用可选进程。CBC 模式作为认证模式时称为 CBC-MAC 模式[38]，已经成为国际标准(IS0/IEC9797-1：1999)，且被我国采纳(GB5852-1995)。

5．计数器(CTR)加密模式

CTR 加密模式是由 Diffie 和 Hellman 于 1979 年提出的，也相当于一个序列密码算法，其优点是可并行处理。加州大学的 P.Rogaway 等强烈推荐此模式作为标准，目前已经发展成标准加密模式之一，其算法过程如下[39,40]：

for $i=1$ *to* n *do* $\{IV_i=IV+i;S_i=E_k(IV_i);\}$（可预处理）

（初值 IV 一般为计数器，或为不重复的伪随机数，IV_i 可扩展至所需长度）

for $i=1$ *to* $n-1$ *do* $C_i=P_i\oplus S_i$；（加密）

$C_n=P_n\oplus MSB_r(S_n)$；（加密）

$P_i=C_i\oplus S_i$； $P_n=C_n\oplus MSB_r(S_n)$；（解密）

CTR 模式与 CBC-MAC 模式组合构成 CCM 模式。

在 ZigBee 协议标准中，使用的计数器模式(CTR)对称加密算法由在 CTR 中使

用一个块密码生成的密钥流组成，其包含一个给定的密钥和随机数(Nonce)，并对密钥流与明文和完整性码做一次异或运算。随机数是一个时戳，一个计数器或者一个希望避免非鉴权消息重新执行的特殊标记。解密操作由生成的密钥流组成，并对密钥流和密码异或运算而获得明文。

密码块链-消息鉴权码(CBC-MAC)对称算法由完整性码的生成组成，它在 CBC 模式里使用块密码计算消息，该消息包含它本身数据开始端的已鉴权数据的长度。认证操作包含计算完整性码，并比较接收到的完整性码。

CTR 加密加上 CBC-MAC(CCM)联合对称加密和鉴权机制由完整性码的生成组成，其完整的编码跟随加密的明文数据和完整性之后。输出是由加密数据和加密完整性码组成。用于此安全组件中的对称鉴权操作由一个完整性码的产生组成，这个完整性码在 CBC 模式下使用一个密码块计算一个时戳。时戳后跟随填补的一个已鉴权的数据，接着是一个已填补的明文数据（如果存在）。认证操作包含该完整性码的计算和对已接收的完整性码的比较。用于该安全组件中的对称加密操作由一个密钥流产生组成的，这一密钥流用 CTR 中的一串密码使用 CTR 中带有给定密钥和时戳的块密码，并对密钥流和完整性码、明文（若存在）执行异或操作（XOR）。解密操作包含由密钥流的产生和带着为了获得密钥流与密码进行 XOR 操作，并从而获得明文和完整性码。

对称密钥是 ACL 项的 AES 密钥，将被正确地用于执行 CTR 加密、CCM 加密和鉴权、CBC-MAC 鉴权三者之一的操作。不同的安全组件将不会用同一个 AES 密钥。帧计数器是一个不停运行的计数器，它应该包括 MAC 帧的 MAC 净载荷。每传输一个安全帧，该计数器加 1。该计数器不会溢出，这个值有助于确保 CCM 时戳是唯一的，并且允许接收方使用计数器来确保刷新。

密钥序列计数器是一个由高层确定的计数器，且应该被包含在MAC帧的MAC净载荷域。该值有助于确保 CCM 时戳的唯一性，并允许接收方用计数器来确保时效性。若在刷新时接收方的刷新操作失败，则高层不执行该计数器减 1 操作。

可选的外部帧计数器和可选的外部密钥序列计数器是一个可能存储在 ACL 项中的域，其分别表示最后收到的帧计数器和密钥序列计数器的值，并位于与这个 ACL 项中相应的安全帧中。如果 ACL 项中包括可选的外部帧计数器和可选的外部密钥序列计数器域，MAC 将用这个域的值去校验接收到的安全帧的有序刷新值。

4.3 AES-CTR 安全方案

当设备运行在安全模式时，可选择使用 AES-CTR 安全方案。安全方案中的加密操作包括在 MAC 帧净载荷域中使用数据分享的 AES-CTR 加密或解密执行，帧计数器和密钥序列计数器。

对于 AES-CTR 安全方案来说，存储在 macDefaultSecurityMaterial 或在 ACL 中的 ACLSecurityMaterial 域中的安全资料由一个对称密钥、一个帧计数器和一个密钥序列计数器组成，及用于输入帧的可选的帧计数器和序列计数器。当执行这些可选的操作时，安全方案在接收到的帧上提供有序的更新安全服务。在一个被保护的帧的 MAC 净载荷中的净载荷域由帧计数器、密钥序列计数器和加密净载荷组成。加密净载荷域的长度与它加密前的长度是相等的。对于产生密钥流的 CTR 加密函数的输入块由一个标记字节、传送帧的设备的源地址、帧计数器、密钥序列计数器的值和块计算器的值组成。在该方案中的 CTR 加密操作将进行如下的参数化：块密码将用 AES 加密算法；计数器输入块除了第一个块的模块计数器设置为 0 以外，每一个计数器都是一样的。

当调用 AES-CTR 安全方案保护一个输出帧时，MAC 层将执行下列操作：

(1)获得它自身的 64 位扩展地址，aExtendedAddress，连同来自 MAC PIB 的帧计数器和序列计数器一起构建时戳。

(2)用来自(1)步骤中的计数器输入块，对使用 CTR 加密的帧的 MAC 净载荷中的净载荷域进行加密。

(3)组合帧计数器、序列计数器和(2)步骤的输出，获得新的净载荷域。

(4)帧计数器值的增加，若成功，把新的计数器的值插入到 MAC PIB 中。若因计数器值溢出而使增加操作失败，设备将中止此操作，同时发出状态参数为 FAILED-SECURITY-CHECK 的 MLME-COMM-STATUS.indication 原语到上层。

当调用 AES-CTR 安全方案保护一个输入帧时，MAC 层将执行下列操作：

(1)如果可选的外部帧计数器和外部密钥序列计数器包含在相应的 macDefaultSecurityMaterial 或者 ACLSecurityMaterial 域中，通过校验收到的密钥序列计数器大于或等于来自该设备的外部密钥序列计数器，以确保有序的更新。若密钥序列计数器大于或等于外部密钥序列计数器，则校验接收到的帧是否大于或等于该设备中的外部帧计数器。若这些校验都失败了，该设备将拒绝接收此帧，

并发出状态为 FAILED-SECURITY-CHECK 的 MLME-COMM-STATUS.indication 原语到上层。

(2)从帧中或者从 ACL 中获取 64 位扩展的源地址，从 MAC 净载荷中的净载荷域中提取出帧计数器的值和序列计数器的值，并构建计数器输入块。若因为难以获得时戳而不能重建数据，设备将发出 MLME-COMM-STATUS.indication 原语上层，其状态为 FAILED-SECURITY-CHECK。

(3)CTR 解密操作由生成的密钥流组成，并对密钥流和密码异或运算而获得明文，步骤(2)中计数器输入块对加密的净载荷域进行解码。

(4)利用存在的 MAC 中的净载荷中的净载荷域代替来自步骤(3)中的已解码的数据。若已执行了步骤(1)中可选择的操作，并检测成功，最后得到的序列计数器和最后得到的帧计数器的值将被设置为接收到的值。

通过以上分析可以知道，AES-CTR 安全方案主要提供了设备访问控制、数据加密以及有序更新三项安全服务。

其中访问控制的功能主要有：防止非法的主体进入受保护的网络资源；允许合法用户访问受保护的网络资源；防止合法的用户对受保护的网络资源进行非授权的访问。数据加密可以帮助保护数据不被查看和修改，并且可以帮助在本不安全的信道上提供安全的通信方式。例如，可以使用加密算法对数据进行加密，在加密状态下传输数据，然后由预定的接收方对数据进行解密。如果第三方截获了加密的数据，解密数据是很困难的。有序更新，作为一种安全服务，采用一种规定的接收顺序对帧进行处理。当接收到一个帧信息后，得到一个新的刷新值，将该值与前一个刷新值进行比较，如果新的刷新更新，则检验正确，并将前一个刷新值刷新成该值。若新的刷新值比前一个刷新值更旧，则检验失败。这种服务能过保证设备接收的数据信息是新的数据信息。

在该方案中缺少了对数据帧完整性的检验与保护，而完整性是保证信息在发送过程中不会被改变，如拦截、插入、删除、篡改和伪造等。因此，在使用该方案网络中的恶意攻击或无线信道干扰都可能使信息发送受到破坏。因此，该方案不适合在安全性要求很高的实际应用中（比如：军事行动）。

4.4 AES-CCM 安全方案

当设备运行在安全模式下时，也可以选用 AES-CCM 安全方案。方案中的加密操作包含执行与 MAC 净载荷连接的 MHR 上的 AES-CCM 鉴权（或校验）、使用共享数据以及在帧计数器和密钥序列计数器的 MHR 中加密(或解密)净载荷域。AES-CCM 安全方案将选用 32 位、64 位或 128 位完整性码来实现。

对 AES-CCM 安全方案来说，存储在 ACL 中的 macDefaultSecurityMaterial 或者 ACLSecurityMaterial 域中的安全资料包含一个对称密钥，一个帧计数器和一个密钥序列计数器，以及可能用于输入帧的可选的帧计数器和序列计数器。当执行这些可选的操作时，安全方案在接收帧上提供有序的更新安全服务。在保护帧的 MAC 净载荷中的净载荷域是由帧计数器、密钥序列计数器、加密净载荷和加密完整性码组成。已加密的净载荷域的长度与它加密之前的长度是相等的。已加密的完整性码子域的长度与完整性码所要求的长度是一致的。用作 CCM 鉴权和加密功能的时戳是由包含在帧中的确定数据和两种设备都能独立获得的数据组成。

其中，CCM 操作将如下参数化：块密码应该是 AES 加密算法；长度域的字节长度应该是 2 字节；鉴权域 M 的长度应该为所要求的 4 字节，8 字节或者 16 字节。

当调用 AES-CCM 安全方案来保护输出帧时，MAC 子层将执行的操作主要有：获得本身的 64 位扩展地址，aExtendedAddress，连同来自 MAC PIB 的帧计数器和序列计数器一起构建时戳；使用 CCM 鉴权和加密算法来加密和鉴权在帧中的 MHR 和 MAC 净载荷，使用 MHR 和 MAC 净载荷中的无净载荷子域作为鉴权数据，MAC 负载的净载荷子域作为消息；组合帧计数器、序列计数器和上一步的输出来获得新的净载荷域；增加帧计数器，把新的计数器的值插入到 MAC PIB 中。如果因为计数器值溢出是增加操作失败，则设备将中止这一操作，并发送状态为 FAILED-SECURITY-CHECK 的 MLME-COMM-STATUS.indication 原语到上层。

当调用该方案来保护输入帧时，MAC 子层的操作主要有：

若相应的 macDefaultSecurityMaterial 和 ACLSecurityMaterial 域中包含可选的外部帧计数器和外部密钥序列计数器，则能通过校验接收到的密钥序列计数器的值是否大于或等于设备中的密钥序列计数器的值，来确保有序更新。若密钥序列计数器的值等于外部密钥序列计数器的值，则校验接收到的帧计数器的值是否大于设备中的外部帧计数器的值。若以上的检测都失败，设备将拒绝接收该帧，并

发出状态为 FAILED-SECURITY-CHECK 的 MLME-COMMSTATUS.indication 原语到上层。

移除来自 MAC 净载荷中的净载荷子域的帧计数器和序列计数器的值，构建时戳。如果因为数据不能获得而使得不能构建时戳，设备将拒绝接收帧并发出状态为 FAILED-SECURITY-CHECK 的 MLME-COMM-STATUS.indication 原语到上层。

用 CCM 解密和校验来解密完整性码，检验已加密的净载荷子域。使用 MHR 和 MAC 净载荷中的无净载荷子域作为鉴权数据，用加密净载荷子域作为消息，用上一步的时戳来计算。如果完整性码失败，设备将丢弃该帧，并发出状态为 FAILED-SECURITY-CHECK 的 MLME-COMMSTATUS.indication 原语到上层。

用上一步中的解密数据来代替 MAC 净载荷中现有的净载荷子域。如果执行了可选的外部帧计数器和外部密钥序列计数器的操作，并检测成功，最后得到的序列计数器的值和帧计数器的值将设置为收到的值。

通过以上分析可以知道，AES-CCM 安全方案可以提供接入控制、数据加密、确保帧的完整性、有序更新（可选）四项安全服务。相比之于 AES-CTR 安全方案而言，该方案中增加了对数据帧完整性的检验与保护，完整性是保证信息在发送过程中不会被改变，如拦截、插入、删除、篡改和伪造等。因此，在使用该方案网络中的恶意攻击或无线信道干扰都不会使信息发送受到破坏。因此，该方案适合在安全性要求很高的实际应用中（比如：机密商业活动等）。

4.5 AES-CBC-MAC 安全方案

当设备运行在安全模式时，也可选择使用 AES-CBC-MAC 安全方案。该方案中的加密操作是由执行 MHR 和 MAC 净载荷上的 AES-CBC-MAC 鉴权组成。该方案将使用 32 位，64 位或 128 位完整性码执行，并提供接入控制和帧整数的安全服务。

对 AES-CBC-MAC 安全方案来说，存储在 macDefaultSecurityMaterial 中的或 ACL 中的 ACLSecurityMaterial 域中的安全资料由一个对称密钥组成，在两个帧之间没有要求的声明信息。保护帧的 MAC 净载荷中的净载荷域中的净载荷域由带有完整性码的现有净载荷组成。其完整性码子域的长度与要求的完整性码一致，即 4 个字节对应 32 位，8 字节对应 64 位，16 字节对应 128 位。

在该方案中，产生完整性码的 CBC-MAC 鉴权函数的输入是由鉴权数据的长度组成（不含长度域本身），其后是 MHR 和 MAC 净载荷。其输入分成 16 字节块，从左到右执行，直至最后一个块为止。总输入长度也有可能小于 16 字节。

AES-CBC-MAC 安全方案中，定义的 CBC-MAC 操作将进行如下参数化：块密码使用 AES 加密算法；CBC-MAC 鉴权函数的输入的格式如前所述；完整性码 M 的长度应是所要求的 32bit、64bit 或 128bit。

当调用 AES-CBC-MAC 安全方案保护输出帧时，MAC 层将执行以下操作：第一步，先确定连接 MAC 净载荷的 MHR 的字节长度（在安全操作执行前），并且编码的长度定为一个字节的整数；然后，用 CBC-MAC 鉴权来计算帧中 MHR 上和 MAC 净载荷上的完整性码；最后，组合第二步的输出和 MAC 净载荷中现有的净载荷，获得新的净载荷域。

调用该方案来保护输入帧时，MAC 子层将执行以下操作：在安全操作应用之前，确定与 MAC 净载荷连接的 MHR 的字节长度，并把长度编码成 1 字节的整数长度；然后，再把 MAC 净载荷的净载荷域分解成净载荷和完整性码子域，并使用 CBC-MAC 鉴权校验完整性码，同时向上层发出状态为 FAILED-SECURITY-CHECK 的 MLME-COMMSTATUS.indication 原语；最后，移除 MAC 净载荷中的净载荷域的完整性码。

通过上述的分析可以知道，该方案只能提供接入控制和帧完整性安全服务。所以该方案通常只应用于安全等级较低的场合或用于接入认证过程中。

4.6 本章小结

在 ZigBee 技术中，可以根据实际情况的应用需求，即根据设备的工作模式以及是否选择安全措施等情况，由 MAC 层为设备提供不同的安全服务。本章简要分析了 ZigBee 安全方案中采用的安全操作，并对安全方案进行了详细分析，同时给出了各种安全方案所能提供的安全级别。

第五章 ZigBee 路由协议改进及网络节点设计

ZigBee 传感器网络中，由于网络内节点资源有限，数据包的传送通常需要通过多跳通信方式到达目的端。因此，数据包的传送延迟和节点的剩余能量成为了路由设计的重点，如何根据不同的应用需求设计高效率的路由选择算法是实际应用中网络层设计的一个主要任务。

5.1 ZigBee 常见路由算法分析

IEEE802.15.4/ZigBee 网络层支持如图 5-1 所示的三种拓扑结构：星型、簇树型和网状型拓扑结构[41]。星型网络中，整个网络由一个称为 ZigBee 协调器的设备来控制。ZigBee 协调器负责发起和维护网络正常工作，保持同网络的终端设备来通信。网状型和簇树型拓扑结构中，ZigBee 协调器负责启动网络以及选择关键的网络参数，也可以使用 ZigBee 路由其来扩展网络结构。簇树型网络中，采用分级路由策略来传送控制信息和数据。树型网络可以采用基于信标的方式进行通信。Mesh 网络中，设备之间使用完全对等的通信方式。Mesh 网一般是由若干个 FFD 连接在一起组成骨干网，每个节点都可以与它的无线通信范围内的其它节点通信，但它们中也有一个会被推荐为 ZigBee 协调点。

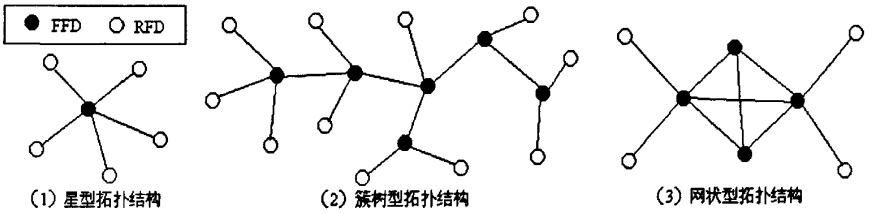

图 5-1 ZigBee 网络拓扑

Fig 5-1 ZigBee network topology

5.1.1 Cluster-Tree 算法简介

Cluster-Tree（簇树）算法[42]中，节点根据分组目的节点的网络地址计算分组的下一跳。对于地址为A深度为d的ZigBee路由节点，如果下述表达式（1）成立，则具有地址为D的目的设备为子设备，其中C_{skip}由网络地址分配机制确定。

$$A<D<A+C_{skip}(d-1) \qquad (1)$$

如果确定分组的目的节点是接收节点的一个后代，节点就将分组发送给它的一个子节点，此时如果满足:

$$D>A+R_m * C_{skip}(d) \quad (2)$$

则说明目的节点是它的一个终端子节点，这时下一跳节点地址N为:

$$N=D \quad (3)$$

否则，

$$N=A+1+\{[D-(A-1)]/ C_{skip}(d)\} * C_{skip}(d) \quad (4)$$

如果目的节点不是接收节点的一个后代，则将分组发送给它的父节点。

5.1.2 AODVjr 算法

AODVjr是一种简化版本的AODV(Ad hoc按需距离矢量路由协议)，主要是考虑到ZigBee无线传感器网络的电池能量有限性、应用方便性等因素，而简化了AODV的一些特点。在MESH结构的ZigBee网络中一般使用AODVjr算法来进行路由发现和数据传输。AODVjr舍弃了AODV中的目标序列号和跳数，只能是目标节点来对最先到达的RREQ信号做出响应，而不是像AODV中已知到目的节点路径的中间节点也可以做出响应。这种策略也被称作点到点策略。同时AODVjr取消了HELLO信息的发送，由Destination定期向Source发送KEEP_ALIVE连接信息来维持路由。当Source在一段时间内没有收到Destination发来的KEEP_ALIVE信号时，它认为此条路径失效，必要时重新进行路由发现。此外，AODV中的RERR信号以及前驱列表在AODVjr算法中也无需考虑。这使得ZigBee的路由发现简单且实用、且更加节能高效。图5-2是使用AODVjr算法时寻找路由的方式，可看到RREQ广播和RREP回复的过程。R5是中心协调器，当终端设备D6要发送数据给R2，D6先把数据发送给具有路由功能的父节点R7，R7查找自身路由表，没有发现到一条到R2的有效路径，于是发起一个路由发现过程，构建并同时洪泛RREQ包。R2选择最先到达的RREQ包的传送路径R7—R6—R2，并返回RREP信息，R7收到R2发来的RREP信号，路由路径建立，R7就会按这条路径来发送缓存的数据。在此期间，R2定期发送KEEP—ALIVE包，用以维护路由信息。

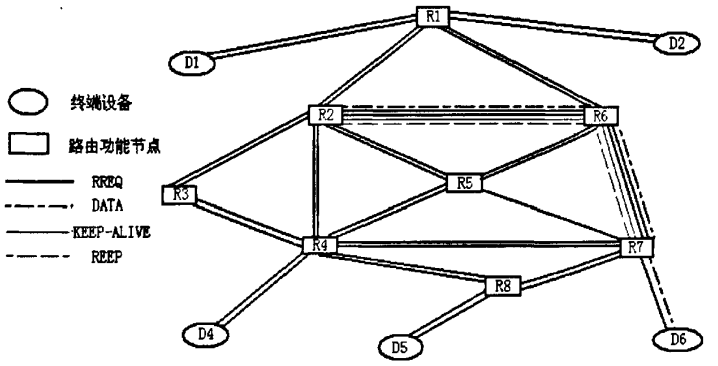

图5-2 使用AODVjr协议的包的传送

Fig 5-2 Packet transmission by AODVjr protocol

由以上分析可知，AODVjr 路由协议在通常情况下能工作得很好，但当节点数较多时，协议的性能就会急剧下降，这是因为 AODV 的路由发现本质上还是使用泛洪方式的扩散法，当网络规模较大、节点数较多时，RREQ 等路由控制报文激增，导致网络超负荷运行和拥塞，大大降低了网络的性能。因此，减少网络中路由报文的数量，是提高性能的关键。

5.2 两种算法的改进策略

5.2.1 Cluster-Tree 算法的改进策略

为使簇树路由算法在缩短平均时延方面有更好的效果，应该考虑邻居节点列表和选择下一跳节点是到目的节点的最短路径的节点。这是基于Greedy算法的思路，因此没有必要去证实最后采用了一条最短的路径。改进的算法主要包括以下3步：

1）如果目的节点在它的邻居列表中，直接传输到对应的节点；

2）如果目的节点是它的子节点，选择自身的子节点作为下一跳；

3）如果不属于以上两种情况之一，那么选择除其子节点外邻居列表中到达目的节点最少跳数的节点作为下一跳。

用 NS-2 仿真软件[43]进行模拟实验，将 Cluster-Tree 和改进的 Cluster-Tree 进行比较，重点是对比两者在数据传送过程中报文分组的端到端的平均延时。仿真结果证明了改进后算法的在缩短时延方面更为有效。图 5-3 是在相同的节点数量下，簇树路由协议改进前后数据包端到端的平均延时。从图中可以看出，随着源节点

数目的增多时延变长。在相同源节点数目的情况下，延时的总体趋势是随着节点数变多而变大，这是由于随着源节点数目的增加会使网络过于拥塞，包成功接收的时间变长，因此会加长时延。而在源节点数目相同的情况下，改进的 Cluster-Tree 算法的时延是相对较小的。

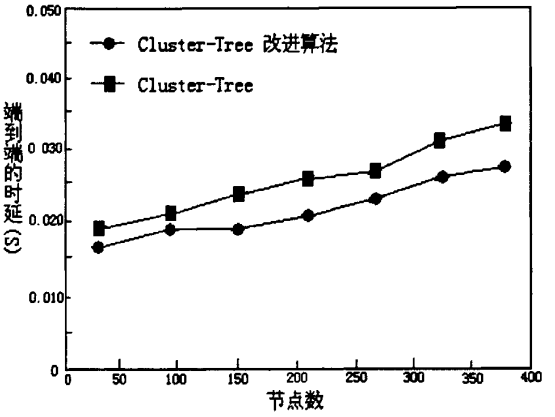

图5-3 端到端平均延迟的对比

Fig 5-3 Comparison of end to end average delay

5.2.2 改进 AODVjr 算法的基本策略

对AODVjr算法[44]进行改进时，一般从能量角度考虑，根据节点的剩余能量状态分为充足、不充足及即将耗尽3种等级。路由发现过程中，中间节点在收到路由RREQ报文后，根据节点自身能量等级决定下一步动作。算法如下：1)收到RREQ报文后，判断自身能量状态：能量在第1等级时，直接转2)；能量在第2等级时，等待一段时间后转2)；能量在第3等级时，转3)。2)判断自身是否为目的节点，若不是，转发RREQ报文；若是，回复RREP报文。3)不对RREQ进行响应。

当出现源节点在一段时间后仍没发现有效路由，则重新进行路由尝试，此时路由节点不再进行能量区分以保证路由正常建立。通过上述改进，每个节点根据自身的状况有选择地转发RREQ报文，能阻止在能量不足的节点上建立路由，有效地减少了RREQ报文的广播风暴，可以在总体上提高网络性能。

实际应用中，为降低算法实现的复杂度，减少通信量，节约电池能量，有效提高ZigBee网络的总体性能，在原AODVjr算法中引进了因特网中的“捎带确认”技术。文献[45]中对此有详细介绍并通过实验证明了改进算法的可行性。

5.3 一种基于AODVjr的Cluster网络路由策略

通过对上述改进后的算法和改进的策略分析可知：改进的Cluster-Tree结构的优点在于可以增加网络的覆盖范围，在缩短时延和数据聚合方面有较为明显的优势[46]。但其缺点也很明显，这种非自适应算法决定了不可能最大限度延长网络的生存时间。而AODVjr算法具有灵活的路由查找功能，其按需路由提高了协议效率，具有快速适应动态链路环境、较低的处理和内存开销以及支持多播的特点且具有自主学习和发现拓扑的能力，但是因需要维护路由表而有初始延迟且容易产生RREQ广播风暴而耗费能量。为此，提出了融合了上述两种改进算法优点的一种基于AODVjr的Cluster网络路由策略，即优化的AODVjr+Cluster路由算法。

5.3.1 簇的建立过程

协议在设计的之初将整个ZigBee网络分成多个簇[47]，簇的建立过程可分为四个阶段：簇首节点的选择、簇首节点的广播、簇的建立和调度机制的生成。每个簇又由多个节点组成，这些节点按功能又分成3种类型的节点：簇首，簇成员和网关节点。簇首作为簇的中心，负责路由过程建立后向簇内成员广播和簇结构的建立，收集簇成员的数据并在融合处理后发送给网关节点。簇的划分是依据下面的规则的基础建立的：

(1)中心节点是一个簇首；

(2)簇首必须是有路由能力的节点，且网络深度为偶数的节点；

(3)深度为奇数的节点则属于它的父节点的簇；

(4)终端节点的簇属于它的父节点的簇。

簇首建立过程如图5-4所示。

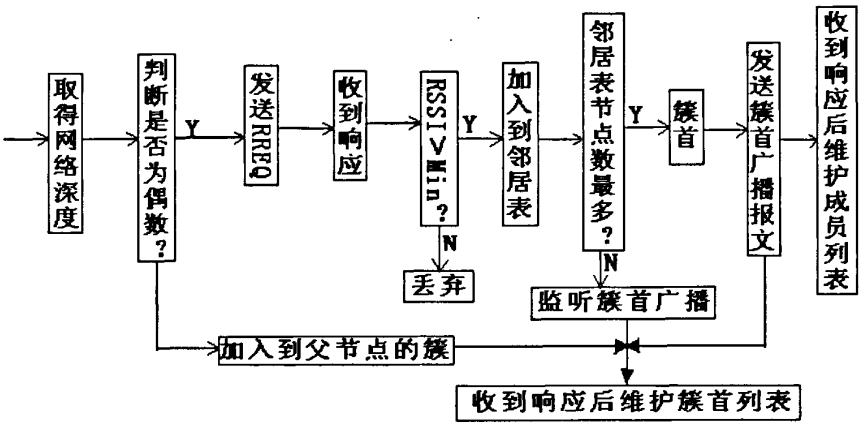

图5-4 簇首的建立过程

Fig 5-4 Process of establishing the first cluster

簇的建立过程是根据节点分布的密集度来划分。簇首的短地址作为该簇的标签。簇的划分是按隔一个深度做一次划分，因为中心节点的深度为0且是一个簇首，所以在深度为偶数的路由节点里面选择一个簇首，簇首的短地址就是这个簇的所有成员的标识。除以中心节点为簇首形成一个簇外，其它的簇首则是根据节点的分布情况来选择的，基于AODVjr的分簇路由根据判断信号强度来确定网络中节点的密集程度。在簇形成的开始阶段，判断网络深度，网络深度为偶数的节点向外广播RREQ，收到RREQ的节点向源节点发送一个确认信息，则发送RREQ的源节点把收到的确认信息按照所规定的最小信号强度来取舍，若大于这个值，则这个节点加入邻居表里，最后根据比较邻居表里周围节点的数目选定节点数最多的节点作为簇首，这个节点的短地址作为这个簇的标签，节点一旦被选定为簇首节点，则向它的周围节点发送簇首广播报文，收到广播报文的节点在自己不是簇首的情况下发送簇加入报文，簇首发送加入响应后，即加入到该簇。簇成员节点维护一个簇首节点列表，簇首节点维护一个网络的所有簇成员列表。

5.3.2 路由过程的建立与维护

AODVjr+Cluster的路由请求过程类似于Z_AODV的方式。源节点有数据要发送给目标节点时，首先在自己的路由表中查寻到目标节点的路径，若路由存在且有效，则直接发送数据；反之，若路由不存在或路由存在但已标明为无效时，源节点则开启一个泛洪路由发现过程。新路由建立伊始，源节点创建一个路由请求包RREQ，并向其周围节点广播。如果邻居节点收到RREQ，则根据计算簇标签的方

法计算出目的节点的簇标签，并在它的邻居表中增加这个簇标签的一个路由接入点，路由查找表中也增加一个目的节点的网络地址的路由接入点；在中间节点收到RREQ时，则与它的路由搜索表中的比较路由成本，如果这个路由成本比较低的话，则更新路由搜索表。之后继续广播，直至到达目的节点为止。

目标节点收到路由请求后，不再广播路由请求，先建立反向路径，并生成一个RREP，RREP中含有最新的各类信息，沿反向路径送至源节点。源节点和中间节点在收到RREP后建立到目标节点的路由，更新系列号等相关信息，源节点建立路由并开始传送数据。这个路由过程一旦建立完毕，源节点向它的簇首发送一个携带有路由信息的路由确认包RNOT(Rote Notify)，簇首在收到这个确认包后再广播一个路由更新包RUPT(Route Update)，簇成员收到这个信息后，则共享节点新建立的路由信息。

数据传送阶段，簇成员通常只与其簇首通信，数据的转发由簇首负责。基于AODVjr的Cluster算法既保证了原有覆盖范围内的数据通信，又在很大程度上节省了能量和缩短了时延。分簇思想具有很明显优点，簇头可以负担数据融合的任务，减少了数据通信量；其拓扑结构有利于分布式算法的应用，适合大规模部署的网络。由于大部分簇内节点在相当长的时间内关闭通信模块，不参加数据转发过程，因此可以延长整个网络的生存时间。

5.3.3 仿真与结果分析

用 NS2 仿真软件（使用方法与流程详见第六章）进行模拟实验，将改进的 AODVjr+Cluster 算法和改进的 AODVjr 进行八种不同节点数量的比较。重点是对比两者在数据传送过程中报文的发送成功率及分组端到端的平均延时。

对节点的配置如下：

（1）节点媒体接入层（MAC 层）设置为 IEEE 802.15.4；

（2）节点路由层设置分别为 AODVjr+Cluster 路由协议和 AODVjr 路由协议；

（3）数据发送时间间隔为 0.1 秒，数据包长度为 80 个字节，模拟稳定的小数据量的数据传输。

（4）无线信号传播模式为 TwoRayGround，这种信号传播模式不单考虑直线传播的信号强度，同时也考虑地面反射的信号强度，比较接近实际环境。

（5）节点设置为固定不动的节点。

仿真结果证明了前者的高效性。在相同的仿真环境下分别运行AODVjr和优化的AODVjr+Cluster的仿真程序并比较仿真结果，图5-5是报文发送成功率比较图，从图中可以看出优化的AODVjr+Cluster协议的数据报文发送成功率要明显高于原来的AODVjr协议。图5-6是网络中两种协议在相同的节点数量下数据包端到端的平均延时，从图中可以看出，随着源节点数目的增多时延变长。在相同源节点数目的情况下，延时的总体趋势是随着节点数变多而变大，这是由于随着源节点数目的增加会使网络过于拥塞，包成功接收的时间变长，因此会加长时延。而在源节点数目相同的情况下，优化的AODVjr+Cluster算法的时延还是相对较小的。在一定的波动范围内，仿真结果符合预期效果。

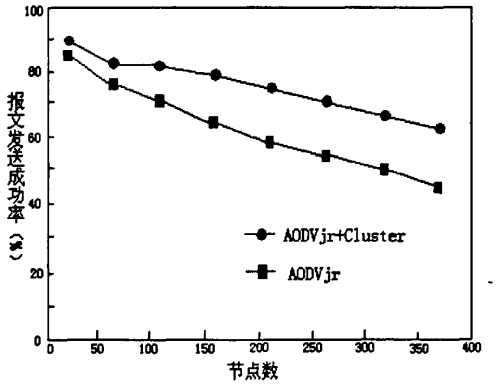

图5-5 报文发送成功率

Fig 5-5 Success rate of sending packets

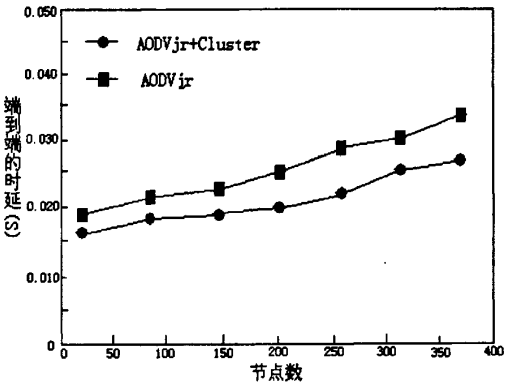

图5-6 端到端的平均延迟

Fig 5-6 End to end average delay

5.4 基于 MC13213 的 ZigBee 硬件设计

5.4.1 终端节点的硬件设计

无线传感器终端节点主要包括：ZigBee 芯片 MC13213、板载 F 型天线、稳压输出芯片、电源电路部分，具体模块结构如框图 5-7 所示。传感器节点的主要功能是采集数据信息及特征指标，并通过射频通信的方式将采集到的数据反馈到控制中心。本设计节点电路中考虑到传感器功能的多样性，在图 5-8 所示节点电路的部分原理图设计中只是预留了传感器接口，并没有将传感器芯片连接进去。根据实际应用需要外接相应传感器，并通过修改应用程序，可以实现节点所需功能。

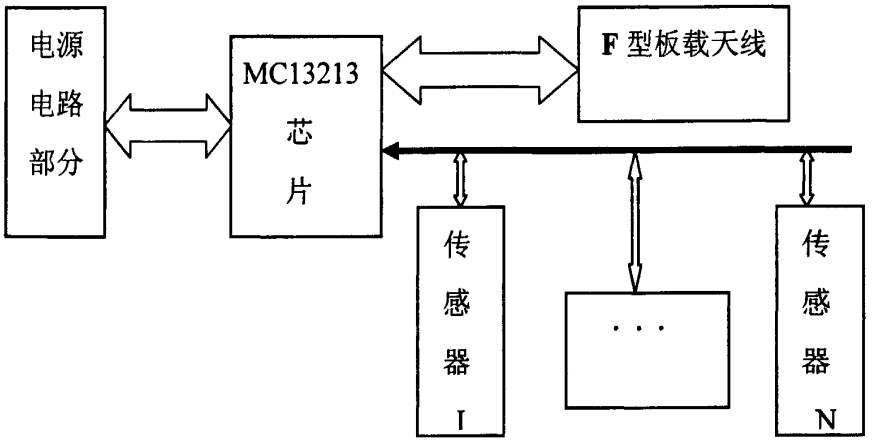

图 5-7 终端子节点模块结构

Fig 5-7 Terminal sub-node module structure

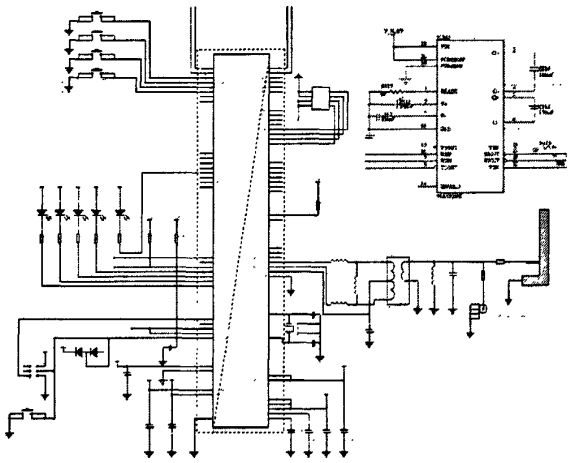

图 5-8 节点电路的主要部分原理图

Fig 5-8 Main part of the node circuit schematic

5.4.2 路由节点的设计

路由节点的模块结构如图 5-9 所示，其中 ZigBee 模块与终端子节点是相同的，主要完成无线收发功能。因为需要一定的数据处理功能，采用 ATMEGA128 八位的高性能低功耗微处理器，根据中心节点（控制中心）传来的指令对子节点进行控制，同时接受子节点发送来的数据，并对数据进行处理，通过 LCD 显示，并且把数据转发给中心节点。

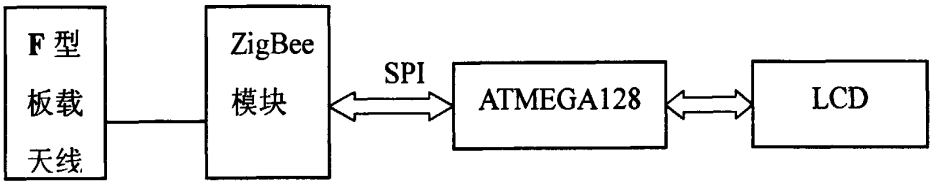

图 5-9 路由节点模块结构

Fig 5-9 Routing node module structure

5.4.3 中心节点的设计

中心节点做为网络协调器，无线通信模块可以采用终端子节点的设计，为了增加网络协调器与以太网的连接和增强控制能力，在本设计中采用了基于ARM9系列的嵌入式微处理器S3C2410作为硬件平台的嵌入式系统，ARM9通过SPI与ZigBee通信模块连接。

如图5-10所示，ZigBee模块只负责无线收发，ARM实现数据处理功能。在该ARM平台上，建立Linux上的Web服务器，通过Web服务器与Internet连接。

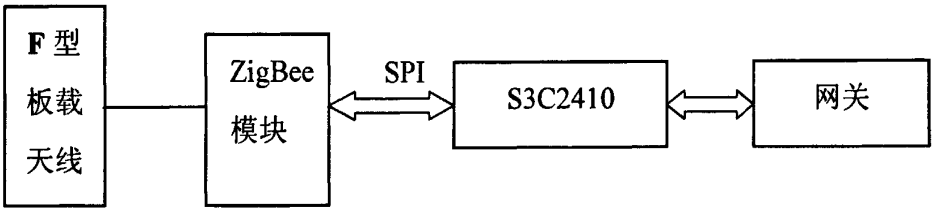

图 5-10 中心节点模块结构

Fig 5-10 Center node module structure

5.5 本章小结

本章详细介绍两种适用于ZigBee网络的路由协议，分析这两种路由算法同时提出相应改进策略。并在结合两种路由的基础上提出一种基于AODVjr的簇树网络路由，仿真结果表明此方案具有可行性。最后，依据Fiscale公司提供的芯片MC13213，提出基于MC13213的ZigBee硬件节点设计流程及方法。

第六章 仿真平台研究及形式化验证

6.1 网络仿真性能评估参数概述

通过对网络层的需求分析，可以知道路由协议包括网络的大规模性、动态性、负载平衡性、数据融合和容错机制等众多指标。参照国际标准化组织 Internet RFC2501[48]规定的网络仿真性能评估定量指标，在本章中选用了三个具有代表意义的性能评价指标。

1．时延指标

数据传输的时延特性，决定了网络通信的实时性能。平均时延时间是指发送一个事件到接收这个事件的平均等待时间。该指标对路由算法执行效率的测度和统计具有非常重要的意义，它影响到传感器网络源节点与目的节点间的总通信时间，反映了网络的通信性能。

$$Average\ Delay(s)=\frac{\sum_{i=1}^{n}(receive_{t_i}-send_{t_i})}{n}(s) \qquad (1)$$

其中 $Average\ Delay(s)$ 表示平均时延，$receive_{t_i}$ 接收到第 i 个数据包的时刻，$send_{t_i}$ 表示发出第 i 个数据包的时刻。

2．分组收发率

分组收发率在本文中的定义为：应用层实际接收到的分组数和总发送分组数的比值。分组传递率（*Packet Delivery*）是指成功接收到的分组总数与防真过程中产生的分组总数的比值，在很大程度上反映了路由协议的可靠性和完整性。

$$Packet\ Delivery=\frac{\sum_{i=1}^{n}receive_i}{\sum_{i=1}^{n}send_i} \qquad (2)$$

其中 *Packet Delivery* 表示分组传递成功率，$receive_i$ 表示接收到的第 i 个数据包，$send_i$ 表示发出的 i 个数据包。

3．路由开销（Routing Overhead）

路由开销是指传感器网络节点在仿真期间传输的路由控制分组总数。路由的

控制信息少，则开销低，从而协议的运行效率提高，带宽和能源消耗相应降低。另外，路由开销也是代表协议扩展性的指标，可用来比较适应网络拥塞的能力。

6.2 网络仿真平台的选取

目前，模拟仿真领域内的主流软件有NS2、OPENT、OMNET++等，其中NS2的使用程度最高，许多科研机构都采用NS2进行网络仿真。NS2对网络协议具有良好的接口支持，使用者可以对它进行功能性扩展。而且在NS2中添加了NS早期版本不具备的CMU无线模块，因此选取NS2作为本问的网络仿真平台。下表6-1是目前市场上三种主流网络仿真软件的比较。

表6-1 网络仿真软件比较

Table 6-1 Comparison of network simulation software

指 标	OPNET	OMNET++	NS2
仿真特点	事件驱动	事件驱动	事件驱动
建模方法	面向对象	面向对象	面向对象
建模环境	图形化编辑器	命令符编辑器	命令符编辑器
模型扩展	继承或开发新模块	继承或开发新模块	继承或开发新模块
模拟过程演示	支持动态演示	支持动态演示	支持动态演示
仿真结果分析	用结果分析器输出	用图形显示输出	用图形显示输出
运行平台	Windows、Unix、Solaris	Solaris、Unix	Unix、Linux、Windows
价 格	昂 贵	需要一定的费用	免 费

6.3 NS2网络协议仿真平台

1、软件简介

NS2是一个由UC Berkeley开发的、用于仿真各种IP网络的为主的、优秀的、公开源代码的网络仿真软件。它是从1989年的实时网络仿真器改进而成的。1995年，美国国防部远景规划署所资助的VINT项目对NS2的开发提供了极大的支持。VINT项目吸引了诸如UCB，LBL和Xerox PRC等著名科研机构的积极参与。

2、工作原理与功能模块

NS的仿真原理—网络组件。NSobject是所有基本网络组件的父类，它本身的

父类是 TclObject 类。这个类的对象有一个基本功能，就是处理数据包（PACKET）。所有的基本网络组件可以划分为两类，分类器（Classifier）和连接器(Connector)。它们都是 NSobject 的直接子类，也是所有基本网络组件的父类。分类器的派生类组件对象包括地址分类器和多播分类器等。连接器的派生类组件对象包括队列，延迟，各种代理和追踪对象类。应用程序是建立在传输代理上的应用程序的模拟。NS2 中有两种类型的“应用程序”，数据源发生器和模拟的应用程序。NS 是离散事件驱动的网络仿真器，它使用 Event Scheduler 对所有组件希望完成的工作和计划该工作发生的时间进行列表和维护。

NS2 仿真器封装了许多功能模块，最基本的是节点、链路、代理、数据包格式等等，以下分别是各个模块的简单介绍。

（1）事件调度器：目前 NS2 提供了四种具有不同数据结构的调度器，分别是链表、堆、日历表和实时调度器。

（2）节点（node）：是由 TclObject 对象组成的复合组件，在 NS2 中可以表示端节点和路由器。

（3）链路（link）：由多个组件复合而成，用来连接网络节点。所有的链路都是以队列的形式来管理分组的到达、离开和丢弃。

（4）代理（agent）：负责网络层分组的产生和接收，也可以用在各个层次的协议实现中。每个 agent 连接到一个网络节点上，由该节点给它分配一个端口号。

（5）包（packet）：由头部和数据两部分组成。一般情况下，packet 只有头部、没有数据部分。

3、层次结构

NS2 在模型化构建方面做了大量的工作，具备十分丰富的网络元件构件库，而且元件对象之间很容易组合和扩展。因此，可以利用已有的网络元件对象，也可以在特定需要情况下进行一些功能性扩展，从而组合出研究需要的网络模型，然后进行网络模拟仿真。NS2 软件定义了结构类和解释结构类两种结构对象类，其层次结构如图 6-1 所示。

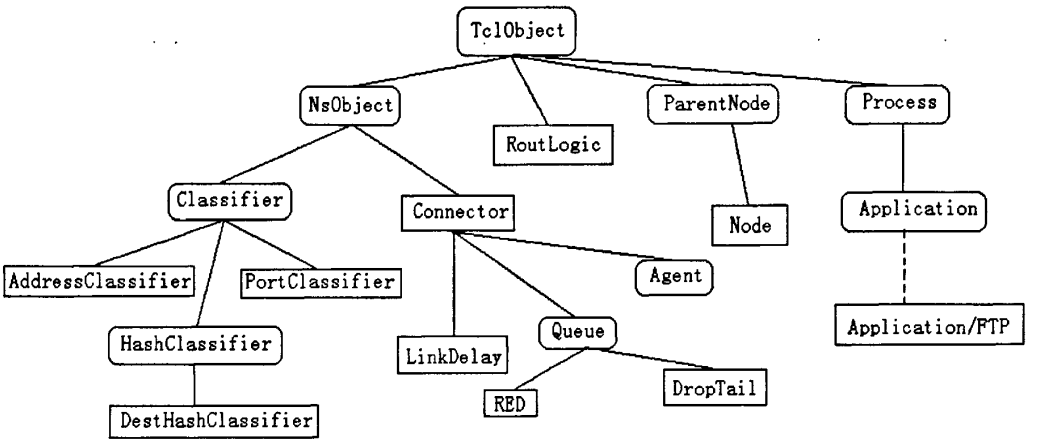

图 6-1 NS2 的层次结构

Fig 6-1 NS2 hierarchy

6.4 协议仿真程序设计过程

6.4.1 仿真平台的搭建

将网络仿真平台 NS2 安装在带有 Cygwin 模拟 Unix 系统软件的 Windows 平台上。

1、Cygwin 软件的安装

具体安全过程可参考 Cygwin 官方网站。安装完成执行时，系统会自动在 Cygwin 软件的 home 的目录下生成一个以当前电脑使用者命名的文件夹。为使后面的叙述方便，假设本文 Cygwin 的安装路径为 c:\ cygwin\home\user ID。具体安装过程如下。

使用 cd 目录命令指向 ns-allinone-2.29 目录，输入安装命令./install;

编辑 home 目录下的文件.bashrc，把 NS2 相关的路径加入到 PATH 字段中。

至此，NS2 网络仿真平台成功地安装在 Windows 系统上。

2、用 C++语言建立新协议

将新的协议扩展到 NS2 时，有以下几个问题需要考虑：

(1)定义新的数据结构以及决定代理的继承类;

(2)设置 Otcl 连接接口函数，修改命令触发函数 command()和接收函数 recv();

(3)新协议建立结束后，需要对新协议有关的 NS2 源程序作一些必要的修改;

(4)重新编译 NS2 代码，生成可执行文件。

6.4.2 移动节点模型

NS2 移动节点模型如下图 6-2 所示，移动节点的无线信道与网络元件介绍如下：

(1)链路层：节点的链路层与一个用来把 IP 解析成物理地址的 ARP 模块相连。

(2)地址解析：节点将从链路层接收请求的 ARP 物理地址写入到数据分组的头部。

(3)队列类：接口队列类 PriQueue 负责对所有缓冲队列中的数据分组进行过滤，并删除具有明确目标地址的数据分组，同时，它将路由的数据分组优先处理。

(4)Mac 层：实现了 IEEE802.11 DFC MAC 协议。

(5)网络接口：它是移动节点通信信道的访问接口。

(6)无线广播模型：移动节点的无线信号传输模型。

(7)天线：安装在移动节点上的单一增益全向天线。

(8)无线信道：将数据分组拷贝传递给与通信信道连接的节点。

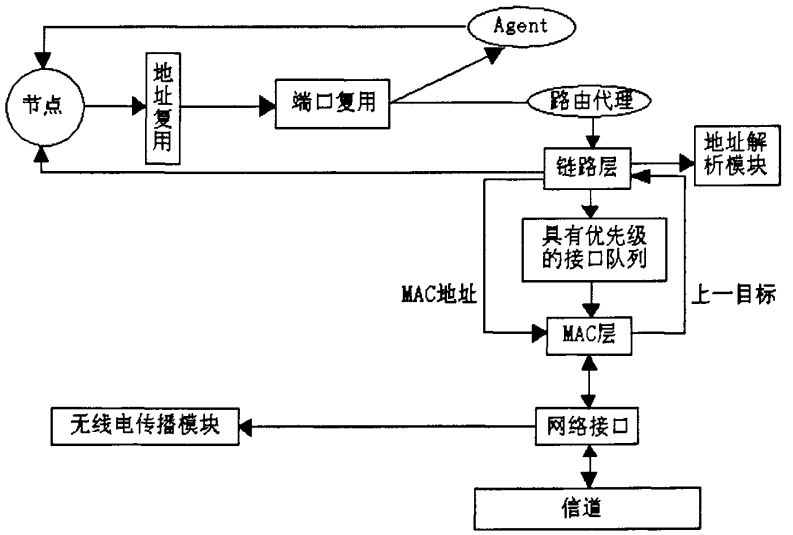

图 6-2 移动节点模型

Fig 6-2 Mobile Node Model

6.4.3 网络仿真的一般流程

利用 NS2 对网络进行仿真时，必须清楚仿真所涉及的层次结构。如果只是对已有的网络元素进行仿真实现，那么只需要编写 Otcl 代码而不需要对 NS2 作任何

修改；如果要对 NS2 进行功能上的扩展，则需要按照添加新协议的方法重新编译 NS2 软件。通常的流程如图 6-3 所示。

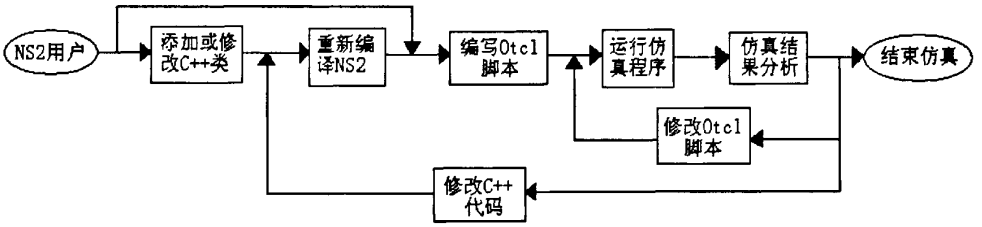

图 6-3 NS2 的网络仿真流程

Fig 6-3 NS2 network simulation process

利用 NS2 进行协议仿真的实现流程如下：

(1)创建网络仿真器并配置仿真的网络拓扑结构；

(2)创建新协议的代理结构，包括通信模型的建立和通信协议绑定；

(3)依据协议仿真的要求对节点进行配置、路由、代理等的初始化过程；

(4)构造 Otcl 类并且编写必要的 Otcl 类代码；

(5)调用可视化工具 Xgraph 或 Nam 进行仿真结果的追踪。

6.5 仿真结果数据处理与分析

路由协议仿真结束之后，可以在相应的目录下得到 trace 跟踪文件*.tr 和动态演示文件*.nam，其中 trace 跟踪文件记录了路由协议仿真过程中响应的所有事件，而动态演示文件*.nam 用来动态显示路由协议仿真的全部过程。

6.5.1 数据流与运动场景

在 NS2 中，可以在定义网络元素时加入加载运动场景和数据流文件的代码。

```
set val(cp) "./cp-n40-a40-t40-c4-m0"
set val(sc) "./sc-x2000-y2000-n40-s25-t40"
set val(cp) "cbrfile"     // 数据流场景文件
set val(sc) "scenefile"     // 节点运动场景文件
```

文中所需要的仿真场景分别由 cbrgen 和 setdest 命令生成的。

文中生成数据流场景文件使用的命令如下：

```
ns cbrgen.tcl -type cbr -nn 40-seed 1 -mc 18 -rate 2.0 > cbr-40n-18m-2r
```

文中节点运动场景文件使用的命令如下：

setdest -v 1 -n 40 –p0-M 10 -t 200 -x 2000 -y 2000 > scene-40n-0p-10M-200t-2000x-2000y

6.5.2 仿真元素与网络参数

使用 NS2 进行仿真，要定义节点的仿真元素与网络参数，代码如下述所示。

```
#定义元素和网络参数
set val(chan)           Channel/WirelessChannel
set val(prop)           Propagation/TwRayGround
set val(netif)          Phy/WirelessPhy
set val(mac)            Mac/802_11
set val(ifq)            Queue/DropTail/PriQueue
set val(11)             LL
set val(ant)            Antenna/OmniAntenna
set val(x)      2000    ; # X dimension of the topgraphy
set val(y)      2000    ; # Y dimension of the topgraphy
set val(ifqlen)   512   ; # max packet in ifq
set val(Routing)  ac-ZigBee  ; # Routing Protocol
set val(nn)       40         ; # how mang nodes are simulated
set val(stop)     40.0       ; # simulation time
```

6.5.3 仿真对象与跟踪文件

生成网络仿真器对象 ns_。命令如下所示：

```
set ns_[new Simulator]
```

Trace 文件的功能是详细记录模拟的过程，trace 可以根据用户的需要记录模拟过程中的所有细节。当一次模拟结束之后，所留下的唯一记录就是 trace 文件，所有的对模拟的分析都是基于 trace 文件的。为了支持 trace 记录，每个分组都包含一个特殊的 common 分组头，在这个分组头中包含了分组的序列号、分组的类型值（由产生该分组的 Agent 来设定）、分组的大小（以字节为单位，用来决定分组的传输时间）和端口标识等。无线 trace 文件的格式可以分为以下几个字段。

(1)事件类型。包括发送、接收、丢弃、转发四种类型；

(2)常规标记。代表时间或全局设置；

(3)下一跳信息。包括本节点的 ID 和下一跳节点的 ID；

(4)节点特性标记。包括节点 ID、节点坐标、节点能量水平、trace 层次、事件发生原因；

(5)IP 层信息。包括源节点地址和端口号、目的节点地址和端口号、分组类型、分组大小、流标识、分组唯一标识、分组 TTL 值；

(6)MAC 层扩展信息。包括持续时间、目的节点以太网地址、源节点以太网地址、以太网类型；

(7)应用层信息。包括各种类型应用的信息。

跟踪文件对象用于记录仿真过程的 trace 跟踪文件和 nam 跟踪文件。以下代码分别生成了 trace 跟踪文件对象和 nam 跟踪文件对象。

```
set val(out)            "ac-ZigBee.tr"        #生成 trace 跟踪文件
set val(simulation)     "ac-ZigBee.nam"       #生成 nam 跟踪文件
```

接下来，本文使用以下代码创建全局控制器（God）对象。

```
set god[create-god $val(nn)];                 # Create God Object
```

通过以下代码来配置传感器节点对象的参数。

```
$ns_node-config-adhocRouting $val(adhocRouting) \
        -11Type   $val(11) \
        -macType   $val(mac) \
        -ifqType   $val(ifq) \
        -ifqLen   $val(ifqLen) \
        -antType   $val(ant) \
        -propType   $val(prop) \
        -phyType   $val(netif) \
        -topoInstance   $topo \
        -agentTrace   $val(agttrc) \
        -routerTrace   $val(rtrtrc) \
```

当网络协议仿真结束后，NS2 会产生两个包含详细跟踪信息的跟踪文件。这些跟踪数据可以用于后期的分析处理，也可以利用 NAM 工具演示整个协议的仿真

过程。

在协议程序仿真结束之前，需要作一些必要的中止处理，包括停止网络节点的事件响应、终止仿真器运行、关闭跟踪文件对象等工作。以下是退出仿真程序的代码：

```
$ns_at      $val(stop).0002 "finish" ;  #在 val(stop)时刻调用 finish 子程序
proc finish {}  {      ;#建立一个名为 finish 的完成过程
        global ns_tracefd namtrace
        $ns_flush-trace ;        #刷新仿真过程中所有 trace 对象的缓冲区
        close $tracefd ;         #关闭跟踪对象
        close $namtrace ;        #关闭跟踪文件
        exec nam hls_test.nam &   }
$ns_at   $val(stop).0005 "puts\"NS EXITING... $val(out) $val(simulation)\" ;
$ns_halt"
```

此外，需要在仿真程序结束函数的后面给出开始进行网络仿真的命令代码。

```
puts "Starting Simulation... "
$ns_run
```

以上是 ac-ZigBee 网络协议仿真的全部过程和方法，将编写的协议仿真在以 ac-ZigBee.tcl 命名的文件中，运行 Cygwin 软件并输入命令：ns ac-ZigBee.tcl，即可以开始进行网络协议的模拟仿真。

6.5.4 仿真结果可视化处理

跟踪对象文件*.nam 用来动态显示数据包的路由信息和协议仿真的全部过程等内容，在 Cygwin 窗口中运行命令：nam *.nam，系统将会自动打开 NAM 演示界面。图 6-4 展示的是对 30 个节点进行网络仿真时的 NAM 演示界面。其中带数字的圆圈包含了节点的 ID 号，而大圆环则表示节点的无线通信半径，该通行半径受到节点的发射功率限制。

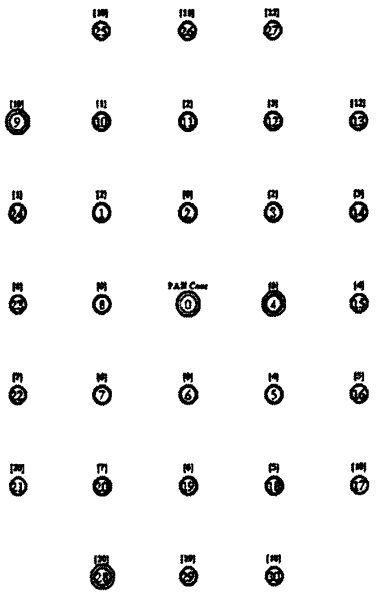

图 6-4 网络节点分布图

Fig 6-4 Distribution network nodes

此外，NS2 带有 Gnuplot 和 Xgraph 等绘图软件，可以绘制静态曲线来展示网络协议仿真结果。这对于分析跟踪数据之间的关系，变化趋势等内容非常有帮助。

6.6 协议安全的形式化验证

本文采用协议形式化验证工具 AVISPA 来验证改进的 AODVjr+Cluster 路由协议的安全性，安全形式化验证结果表明本文改进的路由协议在节点间相互通信时，具有较好的安全性能，可以有效地保证路由数据包的完整性，验证主体的真实性和抵御重放路由攻击行为。

6.6.1 AVISPA 简介

AVISPA 采用的是 HLPSL 语言，并融合了四种不同的分析终端。用户可以通过设定网络协议的运行环境、入侵者的攻击能力、参与者标识、实现目标等变量，并指定协议预期需要达到的安全特性，建立安全协议的分析模型。AVISPA 工具集中的分析终端可以分析出安全效果能否达到要求，进而采取相应的安全策略。其体系结构如下图 6-5 所示。

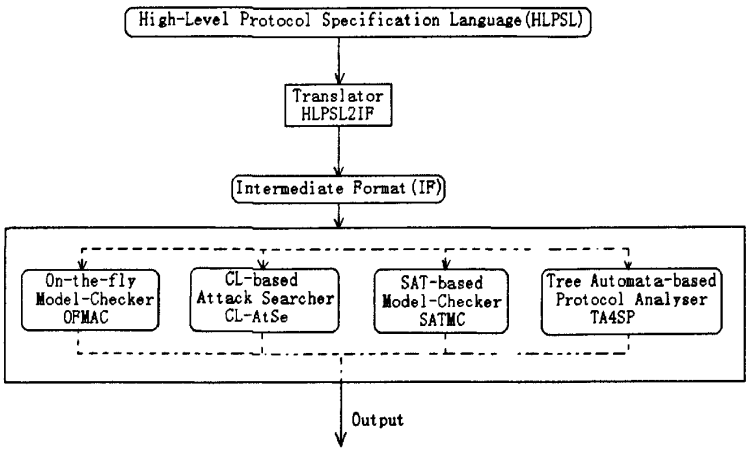

图 6-5 AVISPA 体系结构

Fig 6-5 AVISPA architecture

6.6.2 协议形式化验证的实现过程与分析

在改进的 AODVjr+Cluster 路由协议中，节点间通信时具体实现了保证数据源真实性、数据包完整性、抵御重放攻击行为等服务。

其中，节点 A 希望节点 B 建立一个共享密钥 K，但 A 和 B 只是分别同 S 拥有共享密钥。由此，A 向 S 发出一个密钥请求，并希望此密钥包含 A 和 B 的身份信息。图 6-6 是此协议的一个图示。

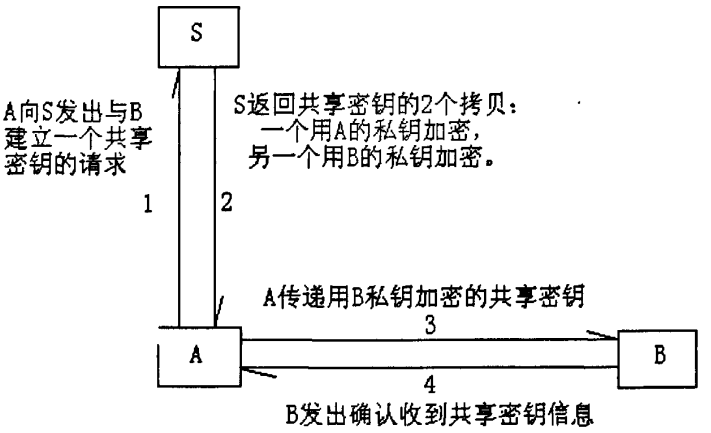

图 6-6 协议流程示意图

Fig 6-6 Flow chart of the agreement

利用 HLPSL 语言编写出验证协议安全性所需要的代码，并将其保存在 ac-ZigBee.hlpsl 文件中，其中的主要代码如下所示：

role alice (A, S, B: agent,

```
        Ka : symmetric_key,
    SND_SA, RCV_SA, SND_BA, RCV_BA: channel(dy))
.....
transition
1. State = 0 ∧ RCV_BA(start) =|>
   State':= 2 ∧ Na' := new()
          ∧ SND_SA(A.B.{Na'}_Ka)

2. State = 2 ∧ RCV_SA(A.B.{K'.Na.Ns'}_Ka.X') =|>
   State':= 4 ∧ SND_BA(A.B.X'.{Na.Ns'}_K')

3. State = 4 ∧ RCV_BA(A.B.{Ns.Na}_K) =|>
   State':= 6 ∧ request(A,B,alice_bob_na,Na)
end role
```

上述程序代码中，利用A作为发起端。其中变量state表示验证时的初始状态，变量transition代表节点通信会话过程中的状态变化。根据改进路由协议安全原理，在发起端A和接收端B的通信会话过程均进行了一定的状态变化。

```
role server (A, S, B : agent,
          Ka, Kb : symmetric_key,
          SND_AS, RCV_AS: channel(dy))
played_by S
.....
1. State = 1 ∧ RCV_AS(A.B.{Na'}_Ka) =|>
   State':= 3 ∧ Ns' := new() ∧ K' := new()
          ∧ SND_AS(A.B.{K'.Na'.Ns'}_Ka.{K'.Na'.Ns'}_Kb)
          ∧ secret(K',k,{A,B,S})
end role
.....
role session(A, S, B : agent,
          Ka, Kb : symmetric_key)
```

```
  def=
        local
        SSA, RSA,
        SBA, RBA,
        SAS, RAS,
        SAB, RAB : channel (dy)
     composition
          alice (A, S, B, Ka, SSA, RSA, SBA, RBA)
       /\ server(A, S, B, Ka, Kb, SAS, RAS)
       /\ bob (A, S, B, Kb, SAB, RAB)
end role
```

由于相互通信的双方在会话过程中可能出现节点的重放攻击行为，因此要考虑不同的环境角色，其中变量goal就是路由协议要实现的安全目标。据此，设置如下：

```
role environment()
   def=
        const a, b, s : agent,
        ka, kb, ki : symmetric_key,
        alice_bob_na, k: protocol_id
        intruder_knowledge = {a, b, s, ki}
        composition
      session(a,s,b,ka,kb)
   /\ session(a,s,i,ka,ki)
   /\ session(i,s,b,ki,kb)
end role


goal
      secrecy_of k
      authentication_on alice_bob_na
end goal
environment()
```

打开形式化验证工具 AVISPA 软件的在线仿真网页界面，进入 Expert 的窗口，如图 6-7 所示。

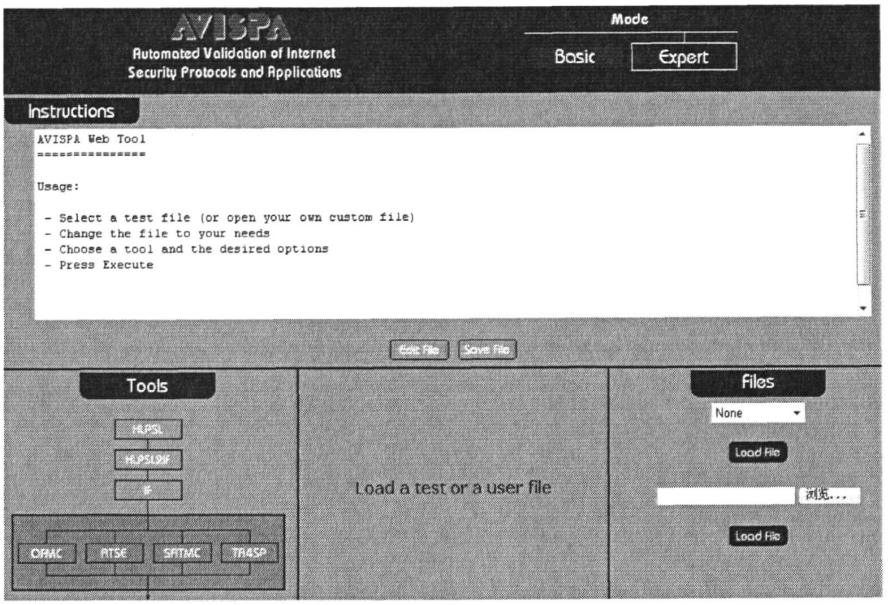

图 6-7 AVISPA 验证操作窗口

Fig 6-7 AVISPA verify operation window

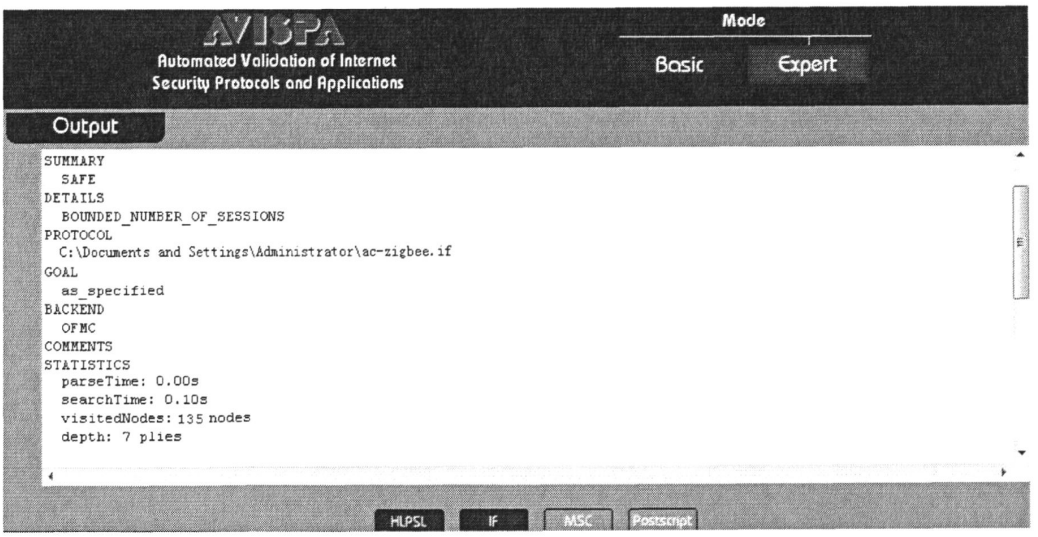

图 6-8 协议安全性形式化验证结果

Fig 6-8 Protocol Security Formal Verification Results

输入命令 avispa ac-ZigBee.hlpsl—ofmc，并设定相关参数。对 ac-ZigBee.hlps 安全形式化程序进行验证，最终结果如下图 6-8 所示，SUMMARY 显示结果为 SAFE；GOAL 显示为 as_specified；访问节点数为 135 个；遍历时间为 0.10s。此结果表明该协议的安全性是符合预期目标的。

6.7 本章小结

本章在分析网络层需求的基础上，参照国际标准化组织 Internet RFC2501 规定的网络仿真性能评估定量指标。在分析对比了几种仿真平台之后，选取 NS2 做为本文研究的仿真平台，并对其安装搭建、工作原理、功能模块、程序设计过程、仿真流程及数据处理等进行了介绍。最后，采用形式化验证工具 AVISPA 对改进的 AODVjr+Cluster 路由协议的安全性进行验证。结果表明改进的路由算法是符合预期效果的。

总结与展望

随着 ZigBee 网络技术、无线通信技术和计算机网络技术的发展，ZigBee 无线网络因其可移动性、安装简便、高灵活性、低能耗性以及扩展性而得到迅猛发展。在 ZigBee 无线网络带给人们极大的方便的同时，也带来了一系列有限网络不存在的安全问题，安全问题已经成为限制 ZigBee 无线网络技术应用普及的一个主要障碍。基于对 ZigBee 无线网络安全接入与应用的核心问题——接入认证、密钥交换与路由协议的研究，本文对 ZigBee 安全体系与认证技术、网络密钥、安全方案及路由协议进行了研究，提出了一种改进的路由策略，由此实现了可靠的数据包传送及较好的平均延时特性。详细介绍了 NS2，并用 NS2 网络模拟软件对 ZigBee 网络进行了仿真。最后，采用协议形式化验证工具 AVISPA 来验证改进的 AODVjr+Cluster 路由协议的安全性，安全形式化验证结果表明本文改进的路由协议具有较好的安全性能，可以有效地保证路由数据包的完整性，验证主体的真实性和抵御重放路由攻击行为。

针对目前所做的关于 ZigBee 无线网络安全接入认证应用方面的研究，有待进一步研究与分析的地方有：

(1)继续研究 ZigBee 无线网络的安全方案，改进相关安全操作，提出更加丰富的解决方案以供更多的个性化选择，满足各种不同网络环境的安全需求。

(2)深入研究当前的无线网络的路由机制，针对 ZigBee 无线网络典型的应用需求，提出更加丰富的、高效的路由解决方案。

参考文献

[1] Hedetnieme S, Liestman A. A Survey of Gossiping and Broading in Communication Networks [J]. 1998, 18(4): 319~349

[2] Heinzelman W, Kulik J, Balakrishman H. Adaptive Protocols for Information Dissemination for Wireless Sensor Networks[A]. Proceedings of the ACM MobiCom' 99 [C], 1999: 174~185

[3] Intanagonwiwat C, Govindan R, Estrin D. Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks [A]. Proceedings of the 6th Annual ACM/IEEE International Conference on MobiCom' 00 [C], 2000: 56~57

[4] Heinzelman W, Chandrakasan A, Balakriskhnan H. Energy-efficient Communication Protocols for Wireless Sensor Networks [A]. IEEE Proceedings of the Hawaii International Conference System Sciences' 00 [C], 2001: 23~27

[5] Sohrabi K, Gao J, Ailawadhi V et al. Protocols for Self-organization of a Wireless Sensor Network [J]. IEEE Personal Communications, 2000, 7(5): 16~27

[6] Pering A, Szewczyk R, Wen V, Culler D, Tygar J D. SPINS: Security Protocols for Sensor Networks. In Proceedings of the 11th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterpries (WETICE' 02) [C], 2002

[7] 无线个域网（WPAN）协议, http://www.ieee802.org/15/

[8] 彭天笑，缪小红．基于ZigBee的WPAN构建方案[J]．电信工程技术与标准化, 2006：40~44

[9] 任秀丽，于海斌．ZigBee无线通信协议实现技术的研究[J]．计算机工程与应用．2007(6)：143~145

[10] 王育民，刘建伟. 通信网的安全一理论与技术，西安电子科技大学出版社，1999 年

[11] 毛文波著(王继林, 伍前红等译)．现代密码学理论与实践．北京：电子工业

出版社,2006

[12] 王贵林，卿斯汉，周展飞．认证协议的一些新攻击方法．软件学报,2001,12(6)：907~913

[13] ISO/IEC9798-1，http://www.iso.org

[14] Wenbo Mao. Modem Cryptography：Theory&Practice. Published by Perntice Hall PTR, Jul 25

[15] 王亚弟, 束妮娜, 韩继红, et al．密码协议形式化分析．北京：机械工业出版社,2006

[16] 王育民，刘建伟．通信网的安全—理论与技术．西安：西安电子科技大学出版社，2000

[17] 卿斯汉.认证协议两种形式化分析方法的比较[J].计算机学报,2003,14(12)：2028~2036.

[18] 薛锐，冯登国．安全协议的形式化分析技术与方法[J]．计算机学报，2006，29(1)：1~20

[19] K.K.R.Choo, C.Boyd, Y.Hitchcock．Errors in computational complexity proofs for protocols．Advances in Cryptology Asiacrypt 2005, 2005, 624~643

[20] S.Goldwasser, S.Micali.Probabilisitic Encryptiom Journal of Computer and System Sciences．1984,28(3)：270~299.

[21] A.Fiat, A.Shamir. How to prove yourself: Practical solutions to identification and signature problems．In Advances in Cryptology-Crypto'86, 1987, l86~194

[22] M.Bellare, P.Rogaway. Entity Authentication and Key Distribution: Advances in Cryptography—CRYPT0'93, 1994, 232~249

[23] M.Bellare, P.Rogaway. Provably secure session key distribution：the three party case．In Proceedings of the 27th ACM Symposium on the Theory of Computing．New York：ACM Press，1995，57~66

[24] M.Bellare，D.Pointcheval，P.Rogaway．Authenticated key exchange secure against dictionary attacks．Advances in Cryptology-Eurocrypt 2000, 2000, 139~155

[25] E.Bresson, O.Chevassut, D.Pointcheval．Provably Authenticated Group DH Key Exchange The Dynamic case．In Proceedings ofAsiacrypt'02, 2001, 290~309

[26] E.Brcsson, O.Chevassut, D.Pointcheval. Dynamic group Diffe-Hellman key exchange under standard assumptions. Advances in Cryptology-Eurocrypt 2002, Proceedings, 2002, 321~336

[27] E.Bressort, O.Chevassut, D.Pointcheval, et al. Provably Authenticated Group DH Key Exchange In Proceedings of ACM CCS'01. New York: ACM Press,2001,255~264

[28] M.Abdalla, P.A.Fouque, D.Pointcheval. Password-based authenticated key exchange in the three-party setting. Public Key Cryptography-Pkc 2005, 2005, 65~84

[29] M.Bellare, R.Canetti, H.Krawczyk. A Modular Approach to the Design and Analysis of Authentication and Key-Exchange Protocols. In Proceedings of the Proc. of the 30th Annual Symp. on the Theory of Computing. New York: ACM Press, 1998, 419~428

[30] V.Shoup. On Formal Models for Secure Key Exchange(Version 4)(Technical Report No. RZ 3120(#93166)). IBM Research, Zurich, 1999

[31] R.Canetti, H.Krawczyk. Analysis of key-exchange protocols and their use for building secure channels. Advances in Cryptology-Eurocrypt 2001, 2001, 453~474

[32] Harold F.Tipton, Micki Krause, 王顺满,陶然,杨鼎才,郭守则等译. 信息安全管理手册(卷 I I)(第四版)[M]. 北京：电子工业出版,2004

[33] Wedel.G, Kessler.V, Formal Semantics for Authentication Logics. Computer Security ESOROCS 96, Springer LNCS 1146, 219~241

[34] CCITT.CCITT draft recommendation X.509. The directory-authentication framework, Version7, 1987

[35] V Kessler, G .Wedel. A UTLOG-An advanced logic of authentication, Computer Security Foundations Workshop VII, 1994. CSFW 7. Proceedings, 14-16 June 1994, PP: 90~99

[36] 王育民, 刘建伟. 通信网的安全—理论与技术[M]. 西安：西安电子科技大学出版社, 1999. 69~456

[37] Schneier B. 应用密码学—协议、算法与 C 源程序 [M]. 吴世忠等译. 北京：机械工业出版社, 2000. 1~376

[38] StinsonDR..密码学原理与实践(第二版)[M]. 冯登国译. 北京：电子工业出版社，2003

[39] Lipmaa H, Rogaway P, Wagner D. Comments to NIST concerning AES Modes of operations: CTR-Mode Encryption [EB/OL]

[40] 吴文玲. 简评 AES 工作模式[J]. 中国科学院研究生院学报，2002，19(3)：324~333

[41] 李文仲,段朝玉. ZigBee 无线网络技术入门与实战[M]. 北京：北京航空航天大学出版社,2007

[42] 蒋挺,赵成林. 紫蜂技术及其应用[M]. 北京:北京邮电大学出版社,2006

[43] 鲍凤卿. 基于 Ns2 的 ZigBee 网络节点接入的研究[J]. 信息技术, 2008, 11(5)：95~98

[44] 杜焕军,张维勇,刘国田. ZigBee 网络的路由协议研究[J]. 合肥工业大学学报: 自然科学版, 2008,31(10)：1617~1621

[45] 朱向庆,王建明. 利用捎带技术提高 ZigBee 网络性能的方法[J].微计算机信息(嵌入式与 SOC),2008,24(3-2)：56~58

[46] 刘湘雯,侯惠峰,张霞等. 基于群树结构的 IPv6 无线传感器网络的组网及路由协议[J].计算机科学,2007,34(5)：28~31

[47] Hou Ting-Chao，Tsai T J．An Access—based Clustering Protocol for Multihop Wireless Ad Hoc Networks[J]．IEEE Joumal on Selected Areas in Communications．2001，19(7)：1201~1210

[48] S.Corson, J.Macker, “Mobile Ad hoc Networking (MANET)：Routing Protocol Performance Issues and Evaluation Considerations”, RFC2501

攻读学位期间发表论文

发表论文：

[1] 邹小武, 徐杜, 蒋永平, 周燕灿. ZigBee网络基础路由分析与改进. 电脑知识与技术[J]，2009, 11(5)：9242~9245. 与学位论文的第5章第2、3节内容相关。

[2] 周燕灿, 徐杜, 蒋永平, 邹小武. 基于 ZigBee 的楼宇监控系统的应用设计. 仪器仪表用户[J], 2010，17(2)：14~15。

[3] 邹小武, 徐杜, 蒋永平, 周燕灿. ZigBee 网络路由分析与节点设计. 广东工业大学学报[J]. 2010, 6(2) .与学位论文的第 5 章第 4 节内容相关。

致 谢

在完成硕士学位论文之际，衷心感谢我的导师徐杜教授和师母蒋永平高级工程师，能够有幸成为徐老师的学生将是我终生的荣幸！感谢两位老师三年以来一直孜孜不倦地教诲，耐心地指导、毫无怨言和毫无保留地传授。谢谢两位老师在学业上给予我悉心的指导，不仅为我创造了良好自由的学习氛围，并且为我提供先进齐全的实验设备与环境，使我顺利完成从课程学习到科学研究的转变。我所取得的每一点成绩都与两位老师的谆谆教诲和耐心点拨息息相关。两位老师渊博的学术知识，敏锐的科学洞察力，民主的科研作风以及崇高的哲人风范让我受益匪浅，将是鞭策我不断进步的源源动力。希望两位老师身体健康，生活开心。

感谢同门师兄奉泽浩、柯居鑫、凌远焕、刘长红和师姐蒋姣丽、黄凤爱耐心地教导；感谢实验室同门周燕灿、戴中兴、郭伟华、叶伯洪、廖一鸣和文艳华三年来对我学习上和生活上的帮助和支持；感谢同门师弟曾衍仁、冼土明、黄品松、等给我慷慨的帮助；感谢徐彬，林尤惠等许多同届好友给我无私的帮助和慷慨的支持；谢谢所有信息工程学院07级的硕士研究生同学，与你们一起学习和生活，我很开心，愿你们前途无量。

感谢我的家人，特别是我的父亲和母亲，谢谢你们这么多年一直默默的付出；谢谢你们将我抚养成人；谢谢你们给我一个健康成长的环境；谢谢你们给我提供获得高等教育的机会；谢谢你们给我提供的一切。希望你们身体健康、天天开心。

衷心感谢所有关心、支持和帮助过我的老师，同学和亲朋好友们！

邹小武

2010年5月于广州大学城