·网络与计算机应用·

近场通信技术分析

吴思楠，周世杰，秦志光

(电子科技大学计算机科学与工程学院 成都 610054)

【摘要】对近场通信技术的相关标准作了分析；对其发展过程、目前的状况和未来的发展趋势作了详细的介绍。分析了该技术在商业环境中的运用模式和应用开发中的关键问题。安全问题成为决定应用是否成功的重要因素，文中分别从链路层和应用层对近场通信技术中的安全问题作了全面的分析，说明了目前近场通信技术发展的情况和存在的困难，并指出未来的技术发展方向和趋势。

关 键 词 近场通信； 协议； 安全； 标准
中图分类号 TN92 文献标识码 A

Analysis of Near Field Communication Technology

WU Si-nan，ZHOU Shi-jie，QIN Zhi-guang

(School of Computer Science and Engineering, University of Electronic Science and Technology of China Chengdu 610054)

Abstract This paper analyzes the international standard of Near Field Communication (NFC). Authors survey the developing history of the technology; describe the current status, as well as point out the tendency of them. The model in commercial environment and the problems of application development are analyzed. Security has become an important factor in application. So authors also discuss the security problems from link level and application level. This paper analyses the existing problems and the goal of further developments.

Key words near field communication; protocol; security; standard

近场通信(Near Field Communication，NFC)是由Philips公司和Sony公司在2002年共同联合开发的新一代无线通信技术，并被欧洲电脑厂商协会(ECMA)和国际标准化组织与国际电工委员会(ISO/IEC)接收为标准。2004年，Nokia、Philips和Sony公司成立NFC论坛，共同制定了行业应用的相关标准，推广近场通信技术。与蓝牙、UWB和802.11等无线通信协议相比，NFC的通信距离更短，软硬件实现更简单。各种电子设备间能够以非常简便、快速的方式建立安全的连接进行信息交换，实现移动电子商务的功能，如智能海报的应用等[1]。

1 NFC应用模式

NFC由非接触式识别和互连技术发展而来，是一种在十几厘米的范围内实现无线数据传输的技术。在单一芯片上，它集成工作在13.56 MHz主频段的无线通信模块，实现了非接触式读卡器、非接触式智能卡和设备间点对点通信的功能。在一对一的通信中，根据设备在建立连接中的角色，把主动发起连接的一方称为发起设备，另一方称为目标设备。发起和目标设备都支持主动和被动两种通信模式。主动通信模式中，发起和目标设备都通过自身产生的射频场进行通信。被动通信模式中，发起设备首先产生射频场激活目标设备，发起通信连接；然后目标设备对发起方的指令产生应答，利用负载调制技术进行数据的传输。在被动通信模式中，设备工作的耗电量很小，可以充分地节省电能。

在实际应用中存在三种主要的NFC应用模式：

(1) 读写模式，如图1a所示。NFC设备充当阅读器，对符合ISO/IEC 14443、15693和18092规范的智能卡进行读写。

(2) 智能卡模式，如图1b所示。NFC设备模拟智能卡的功能与读写器进行交互。目前只支持ISO/IEC 18092规范，暂不支持对ISO/IEC 14443和15693智能卡的模拟。

收稿时间：2007 – 09 – 09
作者简介：吴思楠(1982 –)，男，硕士生，主要从事网络安全与射频识别方面的研究.

(3) 点对点模式，如图1c所示。支持NFC设备间的通信。

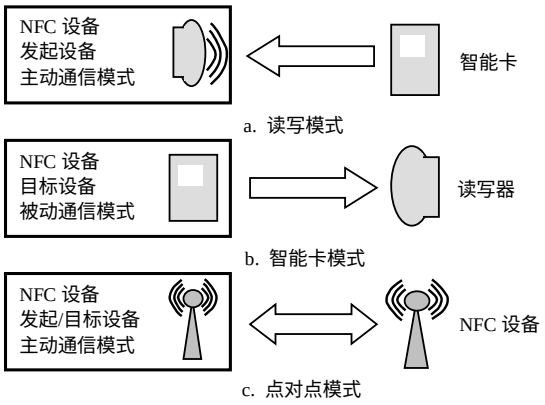

图1　NFC的应用模式

2　NFC中的连接与传输技术

NFCIP-1[2]标准中规定了调制机制、编码、传输速率、帧结构、射频接口，同时还有初始化过程、冲突检测和传输协议等规则，支持106 kb/s、212 kb/s和424 kb/s三种传输速率；更高的传输速度在ISO/IEC21481标准中得到支持。

2.1　帧结构

不同的传输速率具有不同的帧结构。在106 kb/s的速率下存在以下三种帧结构：

(1) 短帧，用于通信的初始化过程，由起始位、7位指令码和结束位三部分顺序组成。

(2) 标准帧，用于数据的交换，由起始位、*n*字节指令或数据和结束位顺序组成。

(3) 检测帧，用于多个设备同时进行通信的冲突检测。

速率212 kb/s和424 kb/s的帧结构相同，由前同步码、同步码、载荷长度、载荷和校验码顺序组成。前同步码由至少48 b的“0”信号组成；同步码有两个字节，第一个字节为“B2”(十六进制)，第二个字节为“4D”；载荷长度由一个字节组成，载荷由*n*个字节的数据组成；校验码为载荷长度和载荷两个域的CRC校验值。

2.2　冲突检测

冲突检测是NFC设备初始化过程中的重要过程，分为以下情况：

(1) 冲突避免，即防止干扰其他正在通信的NFC设备和同样也工作在此频段的电子设备。标准规定所有NFC设备必须在初始化过程开始后，首先检测周围的射频场，只有不存在外部射频场时，才进行下一步操作。判定外部射频场是否存在的阈值为0.187 5 A/m。

(2) 单设备检测。NFCIP-1中定义了SDD(Single Device Detection)算法，用于区分和选择发起设备射频场内存在的多个目标设备。SDD主要是通过检测NFC设备识别码或信号时隙来实现。

2.3　初始化过程

NFC设备的默认状态均为目标状态。目标设备不产生射频场，保持静默以等待来自于发起者的指令。应用程序能够控制设备主动从目标状态转换为发起状态。设备进入发起状态后开始冲突检测，只有在没有检测到外部射频场时，才激活自身的磁场。应用程序确定通信模式和传输速率后，开始建立连接传输数据，如图2所示。

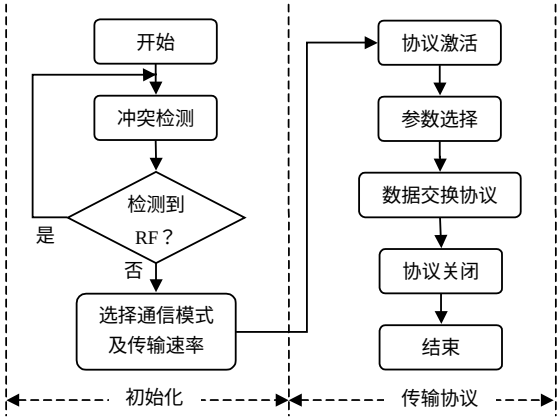

图2　初始化流程

2.4　传输过程

由NFCIP-1标准中制定的传输协议负责数据的传输。在图2中，传输协议包含协议激活、数据交换和协议关闭三个主要过程：

(1) 协议激活负责发起设备和目标设备间属性请求和参数选择的协商。

(2) 数据交换协议为半双工工作方式，以数据块为单位进行传输，包含错误处理机制。数据交换协议中的多点激活(Multi-Activation)特性允许发起设备在同一时刻激活存在于射频场内的多个目标设备，使发起设备能够同时和多个目标设备进行通信，在多个目标设备间进行快速的切换，而不必花费时间释放一个目标，再去激活下一个。

(3) 在数据交换完成后，发起设备执行协议关闭过程，包括撤消选中和释放连接。撤消选中过程停止目标设备，释放分配的设备标识符，并恢复到初始化状态。释放连接使发起设备和目标设备均恢复到初始化状态。

2.5 对PCD和VCD的支持

NFCIP-2标准增加了对接近耦合设备(PCD，ISO/IEC14443)和邻近耦合设备(VCD，ISO/IEC 15693)的支持[3]，故NFCIP-2中制定了一种灵活的网关系统，用来进行NFC、PCD和VCD三种模式的检测和选择。

3 NFC中的数据交换标准技术

NFC论坛在NFCIP-1标准的基础上制定了数据交换格式的标准，以支持应用层数据的转换。NDEF(NFC Data Exchange Format)[4]中定义了用于信息交换的消息封装格式。该格式是一个轻量级的二进制消息格式，可用于把任意大小和类型的应用层数据封装到一个简单的消息结构中。

NDEF消息由一个或多个NDEF记录[5]顺序组成，组成消息的第一个和最后一个记录分别被标记为消息开始和消息结束。记录自身不包含任何索引信息。记录间的序列关系暗含在组成消息的串行化结构中。

NDEF记录是承载有效载荷的数据单元。用户产生的应用层数据被NDEF生成器封装成多个记录，然后组成NDEF消息，最后由设备接口完成消息的发送。接收方在收到完整的NDEF消息后，由NDEF解析器解开消息，从记录中获得应用层数据。NDEF解析器只能判断一个消息的结构是否规范，或该消息是否过长超出了处理能力。因此，更复杂的错误处理和附加服务(如QoS)则需要由应用程序来完成。

4 NFC中的程序开发技术

NFC的应用主要集中于移动设备，而Sun公司的J2ME是移动设备上使用最广泛的应用开发平台。NOKIA和BenQ等公司联合开发了基于J2ME平台的非接触通信接口规范JSR 257(Contactless Communication API)[6]，提供了以非接触方式访问智能卡和条形码的接口，完成了NFC技术链上的最后一环，为应用开发做好了准备。

5 NFC中的安全问题

目前，安全问题日趋显得突出，成为决定一个应用是否成功的重要因素。NFC应用中的安全问题主要分为链路层安全和应用层安全。

5.1 链路层安全

链路层的安全即为NFC设备硬件接口间通信的安全[7]。因NFC采用的是无线通信，所以很容易被窃听。实现窃听并不需要特殊的设备，并且标准是开放的，攻击者能够轻松地解码监听到的信号。NFC设备工作范围在10 cm以内，因此窃听设备与正在通信的设备之间的距离必须很近。具体的距离多大很难确定，因为它同时受到发起、目标和窃听设备的性能、功率等多方面影响。

与其他无线通信一样，攻击者能很容易实施对无线信号的干扰，影响正常通信的进行，达到类似DoS攻击的效果。

消息篡改的难度很大，攻击者需要功能较强的设备，把自己的信号附加到正常的信号中。为了改变正常通信中的0、1信号，应针对不同程度的振幅偏移键控(Amplitude Shift Keying，ASK)、不同的编码方式进行复杂的操作。

除了使用10% ASK的曼彻斯特编码的情况下，存在修改任意比特位的可能性，其他只有在特定的条件下才能被篡改。

消息插入的可能性虽然存在，但要实现是几乎不可能的。因为攻击者要在发起设备和目标设备间“繁忙”的通信过程中，插入自己的消息，很容易与正常通信发生冲突，并被检测到。

对于中间人攻击，由于在NFC通信环境下，无线信号能被参与通信的各方检测到，故试图对消息进行截取和发送的动作都将暴露无遗。因此，中间人攻击在具体的实施方案中是不可能实现的。

攻击解决方案通过建立加密的安全信道，可以很好地抵抗窃听、篡改、插入等威胁。由于不存在中间人攻击，Diffie-Hellmann协议可以很好地工作在NFC的通信环境中。

安全信道可使用该密钥交换协议，在通信双方间交换一个共享秘密值，由共享秘密值生成对称密码算法(3DES或AES)的密钥，然后使用该密钥加密通信数据。在具体使用中，NFC设备需要建立一套完善的检测机制作为各项安全措施的基础。对于通信干扰，只能做到检测发现这一步。

5.2 应用层安全

应用层安全包括除链路层外、所有NFC中开发使用的安全问题。

(1) 数据的保密性。信用卡、票据、个人身份等敏感数据都可能因为NFC的应用而存储在移动设备中，应保证关键数据只能被合法的程序、合法的用户访问。

(2) 认证服务。在应用过程中，移动设备往往还需要与其他设备或在线的服务进行交互，如电信运

营商、银行交易支付系统等，应在设备和服务提供者之间进行认证。

在MIDP版本2.0中，J2ME对MIDlet访问敏感的API建立了一个安全模型，以控制移动设备中应用程序的行为[8]。安全模型中使用了信任和非信任MIDlet的概念。非信任MIDlet对受限API的访问时将受到限制，需要由用户来控制访问的许可。JSR177[9]和JSR219[10]同时为通用安全机制提供了API，例如对加解密算法、HTTPS和SSL等的支持，使应用程序能够建立一套完整的安全机制。

采用专用的安全芯片来保证NFC使用过程中的安全。安全芯片能够支持复杂的加解密算法，并负责存储密钥，主要有两种实现模式：

(1) NFC+SIM模式。SIM卡的芯片上存储移动电话客户的信息、加密密钥等内容，可供电信运营商对客户身份进行鉴别[11]。在这种情况下，SIM将托管NFC相关的移动商务应用程序和安全密钥。

(2) NFC+安全IC模式。将特定的安全芯片等器件集成在手机等移动设备中；支付、票证等应用程序的安全密钥则存储在安全IC中。将NFC和安全IC组合在单一封装的芯片中，单位成本最具吸引力，也更加灵活。飞利浦目前制造的NFC和智能卡IC都支持双线数字接口。NFC芯片和安全芯片之间的接口(S2C)与现有的非接触式标准完全兼容，并已提交给ECMA进行标准化[12]。

在具体应用中可以改进已有的认证协议，运用到发起和目标设备的单向或双向认证上[13]。

6　结 束 语

目前，NFC技术还只停留在小范围的使用中。一方面，支持NFC的硬件产品非常匮乏，且价格还没有进入一个合理的范围。各项规范仍需完善，尤其应用程序的开发，还需要有力的支持。另一方面，NFC若要实现最大范围内的推广普及，涉及到硬件厂商、电信、金融、零售等多个行业的整合，其中的利益分配和业务重组是一个复杂且困难的问题。同样，用户的接受程度也至关重要。只有在用户对使用NFC的便捷性、安全性和隐私保护等方面感到满意时，才会乐于使用。

参 考 文 献

[1] NFC Forum. Smart poster record type definition technical specification[J/OL]. http://www. nfc-forum.org/specs/, 2006-07-24.

[2] ISO/IEC 18092. Information technology-telecommunications and information exchange between systems—Near field communication inter-face and protocol (NFCIP-1) [J/OL]. http://www. iso. org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=38578, 2004-05-21.

[3] ISO/IEC 21481. Information technology-telecommunications and information exchange between systems—Near field communication inter-face and protocol (NFCI P-2) [J/OL]. http://www.iso.org/iso/iso_catalogue/ catalogue _tc/catalogue_detail.htm?csnumber=40261, 2007-07-10.

[4] NFC Forum. NFC data exchange format (NDEF)[J/OL]. http://www.nfc-forum.org/specs/, 2006-07-24.

[5] NFC Forum. NFC record type definition (RTD)[J/OL]. http://www.nfc-forum.org/specs/, 2006-07-24.

[6] Nokia Corporation. JSR 257: Contactless communication API[J/OL]. http://www.jcp.org, 2006-10-02.

[7] HASELSTEINER E, KLEMENS B. Security in near field communication (NFC) strengths and weaknesses[J/OL]. http://events.iaik.tugraz.at/RFIDSec06/Program/index. htm, 2007-07-10.

[8] JONATHAN K. Understanding MIDP 2.0's security architecture[J/OL]. http://developers.sun.com/mobility/midp/articles/permissions/, 2003-09-15.

[9] Sun Microsystems. JSR177: Security and trust services APIs [J/OL]. http://java.sun.com/javame/reference/apis/jsr177/, 2007-07-10.

[10] Sun Microsystems. JSR: 219: Security [J/OL]. http://java.sun.com/javame/reference/apis/jsr219/, 2007-07-10.

[11] JEREMY Q. Security in the GSM system[J/OL]. http://www.gsm-security.net/gsm-security-papers.shtml, 2004-05-01.

[12] Philips Electronics. S2C interface for NFC—Adding a general purpose interface between NFC and secure IC to decure NFC[J/OL]. http://www.nxp.com/products/identification/nfc/, 2005-01-21.

[13] CHEN Yung-chin, WANG Wei-lin, HWANG Min-shiang. RFID authentication protocol for anti-counterfeiting and privacy protection[C]//Advanced Communication Technology, The 9th International Conference. IEEE Conference Proceeding. [S.l.]: IEEE, 2007: 255-259.

编　辑　黄　莘