智能家居设备电力线链路加密方法①

林粤伟

(青岛科技大学 信息科学技术学院, 青岛 266061)
(海信集团有限公司 博士后科研工作站, 青岛 266000)

摘 要: 介绍当前智能家居设备互联架构及方式, 论述现有智能家居设备中电力线通信加密方法存在的问题. 提出一种基于NFC的电力线通信加密方法, 该方法使用NFC卡的UID生成网络密钥并对电力线网络链路进行加密. 实测表明, 该方法较好的解决了现有电力线通信加密存在的问题, 增加了NFC读卡的便捷性、准确性、稳定性, 具有较高的安全性, 对外界干扰具有较强的抑制能力.

关键词: 电子技术; 干扰抑制; 近场通信; 智能家居; 电力线通信

Encryption Method of Power Line Links of Intelligent Home Furnishing Devices

LIN Yue-Wei

(College of Information Science and Technology, Qingdao University of Science and Technology, Qingdao 266061, China)
(Post-Doctoral Research Center, Hisense Group Co. Ltd., Qingdao 266000, China)

Abstract: The interconnect architecture and method of modern intelligent home furnishing devices are introduced. The problems of power line communication's encryption method in current intelligent home furnishing devices are discussed. A NFC-based encryption method of power line communication is proposed. The NFC card's UID is used by this method to produce network member key and to complete the encryption process of PLC link. Through actual measurement, the current problems of power line communication's encryption method is resolved well by the NFC-based method, the convenience, accuracy, and stability levels of NFC card reading process are increased. The method's safety level is high, and has strong interference restraining ability towards outside interference.

Key words: electronic technology; interference restraining; near field communication; intelligent home furnishing; power line communication

引言

随着电子通信、物联网技术的发展, 智能家居中的各类智能终端(包括 3G/4G 智能手机、平板电脑、个人电脑、智能家电等)需要连接到网络彼此互联互通才能实现各自的智能功能[1]. 传统的智能家居互联技术多用 WiFi 等无线技术, 在家庭内部等密闭空间内, 具有多道墙体时, 无线信号穿墙损耗较大, 导致通信速率性能下降明显. 该现象在房屋规模较大(如别墅等)场景下影响尤甚. 因此, 需要研发新颖的智能家居组网关键技术, 以解决现有智能家居组网存在的上述问题. PLC(Power Line Communication, 电力线通信)技术可以利用电力线进行数据传输[2-7], 既能传输高带宽数据[8], 又能克服 WiFi 的无线信号穿墙能力差而导致性能较大幅度降低的缺点. 该技术已应用于电力网络, 远程传输窄带的控制数据(比特率一般为 kbps 量级). 而家庭内部智能家居设备之间则一般是在相对近距离的局域网范围内传输宽带的多媒体业务数据(比特率可达 10Mbps 或 100Mbps 量级), 不能直接使用以往电力网络中的 PLC 技术.

目前国内外科研机构、企业在家庭网络的 PLC 技术应用技术方面有一定研究, 形成了 G.hn、HomePlug AV (IEEE 1901)等主要协议标准[9]. 用户在进行基于这

① 基金项目:国家科技重大专项研究项目(2012ZX03002028);青岛科技大学博士科研基金(210-010022614)

收稿时间:2015-11-30;收到修改稿时间:2015-12-28 [doi: 10.15888/j.cnki.csa.005254]

些协议的 PLC 模块组网时, 需要设置模块之间 PLC 链路的加密连接, 而现有技术在建立加密连接时存在问题:加密时间长、加密过程繁琐、存在误加密的可能性, 影响了用户体验[10]. 本文引入 NFC(Near Field Communication, 近场通信)技术进行 PLC 设备的加密, 能够快速、方便、准确地建立智能家居设备之间的底层加密通信链路, 且具备较好的抗干扰能力.

1 关键技术

1.1 PLC 家庭互联架构

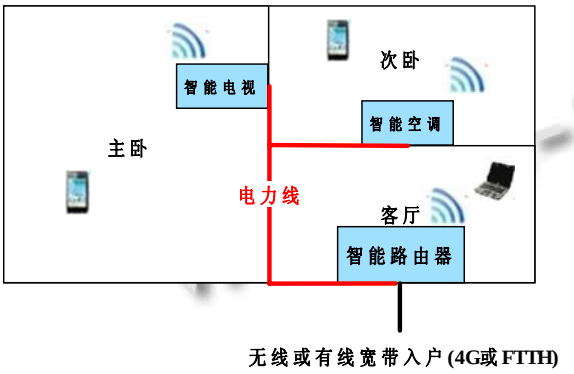


图 1 智能家居设备互联

如图 1, 考虑两室一厅的家庭住房. 客厅中的智能路由器连接 Internet, 负责宽带入户接入. 使用 PLC 电力线技术增强网络覆盖:两间卧室也分别放有支持 PLC 的智能家居设备(可以是智能电视、空调等), 从而拓展了家庭 WiFi 网络覆盖, 各设备之间通过 PLC 电力线传递数据.

1.2 现有 PLC 链路加密方法、问题与解决方案

多个支持 HomePlug AV 协议的电力线设备可以组成一个音视频逻辑网络(AV Logical Network, AVLN), 该网络中的电力线设备必须具有相同的 128 位的网络成员密钥(Network Member Key, NMK)[10], 同一 AVLN 中的电力线设备在 MAC 层对数据进行 128 位的 AES 加密[11]. NMK 机制确保了 AVLN 中的设备彼此进行私密、安全的通信, 避免其他非本 VLAN 的电力线成员设备的非法接入和访问.

用户在进行 PLC 模块组网时, 需要设置模块之间 NMK 值, 而现有方法在此过程中存在问题. 比如两个欲组成 PLC 通信网络的智能电视 A 和智能电视 B, 现有加密方式: 在智能电视 A 上电后, 首先需要人工按下智能电视 A 上的物理加密按键 1~3 秒, 待人工观察 PLC 加密灯闪后, 再按下智能电视 B 上的加密按键 1~3 秒钟直至智能电视 B 的 PLC 加密灯闪烁. 此时智能电视 A 和智能电视 B 之间会彼此发包, 以协商确定 PLC 通信网络的 NMK 值[10]. 除了智能电视, 其他智能家居设备, 如空调、冰箱等通过上述方式建立 PLC 网络的过程均存在以下缺点:加密时间长: 每个设备需要按键 1~3 秒, 当设备较多时, 需要消耗大量时间; 加密过程繁琐: 需人工按键并用肉眼观察加密灯的状态, 且需要发送数据包进行 NMK 协商; 存在误加密的可能性: 如果用户甲准备在智能电视 A 和智能电视 B 之间建立 PLC 通信连接, 当按下智能电视 A 的加密键后, 在准备按下智能电视 B 的加密按键时, 用户乙按下了智能电视 C 的加密按键, 则智能电视 A 和智能电视 C 会彼此发包协商 NMK, 这显然破坏了加密的可靠性、安全性, 既没有完成预期设备间的 PLC 通信连接, 又与不需要通信的设备建立了电力线通信连接. 因此, 需要一种新技术, 能够快速、方便且准确地完成智能家居电子设备之间的电力线通信连接. 本文提出并实现了基于 NFC[12,13]的 PLC 链路加密, 具体技术方案如下.

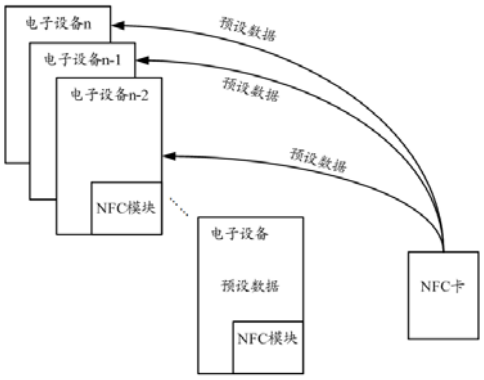


图 2 基于 NFC 的加密方法

如图 2 所示, 在将某张 NFC 卡靠近智能家居电子设备之后, 电子设备中的 NFC 读卡模块读取到 NFC 卡中的预设数据, 本文预设的是 NFC 卡的唯一标示符(即 Unique ID, UID)[14,15], 并基于 UID 生成 NMK, 然后将该 NFC 卡依次靠近其他电子设备, 比如共 n 个电子设备, 则分别靠近 n 个电子设备中的每个电子设备, 使得这 n 个电子设备分别读取到 NFC 卡中的预设数据, 然后 n 个电子设备之间就可以基于该预设数据生成 NMK 并建立电力线通信连接, 无需用户对每个电子设备分别进行人工操作来协商 NMK, 只需在每个 PLC

设备附近进行“刷卡”操作, 即可为每个电子设备设置 NMK, 操作过程简单方便, 极大降低了误加密和非法电力线通信连接的概率. 本方法具有较高的安全性: 一方面, 类似网卡 MAC 地址, 理论上每张 NFC 卡的 UID 具有全球唯一性, 从而提高了 PLC 加密接入的安全性和可靠性. 另一方面, NFC 属短距离无线通信, 有效通信距离很短, 无线射频信号被非法截取的可能性相对较低, 因此被广泛应用于金融领域. 需要补充说明的是, 类似家中房门的钥匙不能丢失或借用给外人, 一旦加密用的 NFC 卡被丢失或外借, 存在被他人获取乃至非法复制并恶意攻击的可能性. 这时需要更换加密用的 NFC 卡(即更换 UID)并重新加密, 相当于更换了房门的钥匙和门锁, 以防止 PLC 设备被非法访问或攻击.

1.3 硬件组成与软件流程

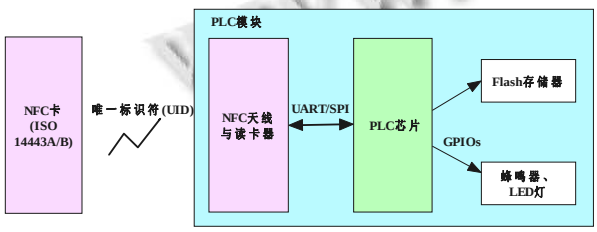


图 3 基于 NFC 的 PLC 加密模块硬件结构图

如图 3, NFC 卡(支持市面最为多见的 ISO 14443A/B 类卡[14,15])靠近 PLC 设备时, NFC 读取芯片会将事先固化在NFC卡中的唯一标示符(即Unique ID, UID)字段值读取出来, 并通过 UART 串口或 SPI 等接口将其传递给 PLC 芯片. PLC 芯片获取 UID 后, 对其进行加密运算(如哈希运算), 将运算结果作为 PLC 传输链路的 128 位 AES 加密算法的密钥(即 Network Member Key, NMK), 并将其存储在 Flash 的专门存储区域中. 最后, 根据 NFC 读卡加密的成功或失败结果设置蜂鸣器和 LED 灯的状态, 给操作人直观提示. 其中, NFC 读卡器可以选取 TI 公司的 TRF7970(RF 收发器, 完成NFC射频功能)和MSP430(16位单片机, 完成 NFC 基带功能)组合, 也可选取其他公司的 NFC 芯片. PLC 芯片可以选取高通公司的 AR6410 或其他芯片, 只要具有 UART 或 SPI 等接口, 且可运行多任务嵌入式操作系统即可. PLC 芯片中 NFC 软件流程如下图所示, 关于 NFC 读取芯片的软件逻辑, 将在后文结合干扰抑制技术进行论述.

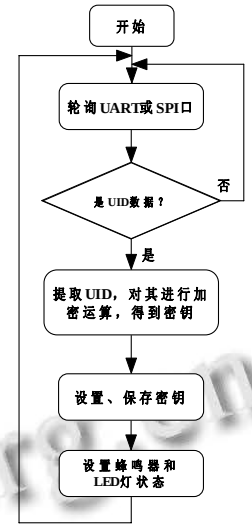


图 4 基于 NFC 的 PLC 加密模块软件流程图

1.4 抑制外界对 NFC 读卡器的干扰

1.4.1 抑制强电模块的空间电磁辐射干扰

现有 NFC 读卡器抗干扰机制并不完善, 无法处理由于强电对弱电干扰导致的误读卡问题. 本文的 NFC 读卡器从 NFC 卡获取 UID 数据来对 PLC 电力线通信链路进行加密. 在数字电路板与电源板位于狭小空间内的应用场景中(比如以智能插座的形式封装于家庭住房墙体内的暗盒中), 属强电部分的 220V 市电电源供电模块和属弱电部分的 NFC 读卡器距离很近. 由于 220V 强电电源噪声的辐射干扰, 会导致 NFC 读卡器被误触发, 错误的返回信号: 即在无卡时读卡器误认为有卡, 而在有卡时读卡器误认为无卡. 因此, 需要设计专门的 NFC 抗干扰读卡方法, 以解决该问题.

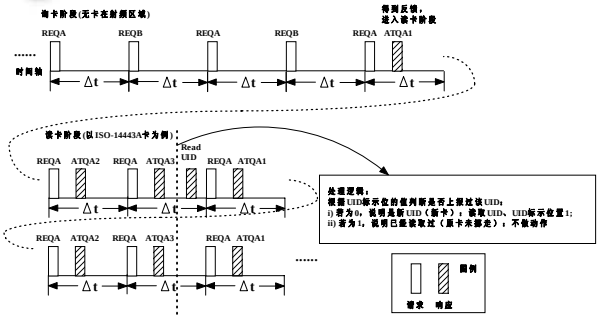


图 5 抑制强电模块对 NFC 读卡的干扰

为了尽可能的降低强电干扰带来的影响, 引入“连续一致表决算法”. 如图5, 设Δt为每次的查询时间间隔(该数值可调), 即每隔Δt 时长, 就发射一次

REQA(REQB)命令. 寻卡阶段:这个阶段读卡器不知道用户会使用 A 类卡还是 B 类卡, 于是以Δt 为时间间隔轮循发送 REQA 和 REQB 命令, 当卡片响应 REQA(REQB)命令, 则说明该卡可能为 A(B)卡, 接着即可进入到第二阶段——识卡阶段. 寻卡阶段的这个方式保证了读卡器对不同类型的卡片都达到最快的响应速度. 识卡阶段:进入识卡阶段, 实际就是利用连续的一致表决, 以最终确认 A(B)卡, 并上传其 UID 号. 该算法要求连续三次 REQA 命令之后均能得到连续三次有效的、一致的 ATQA 返回. 不然, 表决算法就需重新计数.

这个方法带来两个好处:1)在连续三次的 ATQA 值均一致的结果下, 该结果由电源辐射随机干扰导致的可能性已经微乎其微, 所以它极大概率滤除了电源辐射噪声带来的负面影响. 2)防抖动: 一方面, 实际应用时, 卡片在读卡器 RF 辐射区域内, 由于环境因素未必每次都能成功读卡. 因为要求卡片在进入读卡器 RF 辐射区内时, 只上报一次 UID, 如果此卡片已经上报过一次UID, 中间由于环境因素引起ATQA未能正常反馈, 读卡器会认为卡片已经离开读卡器 RF 辐射区(实际卡片还在区域内), 会导致 UID 再上报一次. 该方法不仅要求无卡到有卡的验证需要连续的三次有效认证. 其实, 从有卡到无卡的验证也需要连续三次有效认证. 所以它排除了这种随机的环境干扰因素; 另一方面, 当卡片在读卡器 RF 辐射区边界时, 由于人手的抖动, 也会让读卡器误认为卡片脱离读卡区域后又再次进入, 进而造成 UID 再次上报等后续读卡行为.

1.4.2 抑制人手抖动干扰

可以依靠增加查询间隔时间Δt 的方法来解决上述人手无意识抖动带来的问题, 该方法与单片机、嵌入式系统中较常遇到的键盘按键防抖设计类似. Δt 这个时间影响两个因素: 刷卡响应速度与人手握住卡片在读卡器 RF 辐射区边界的防抖性能, 因此需要合理设置Δt, 这关系到用户完成刷卡行为所需的时长: 时长过短, 虽能达到高度的刷卡敏捷性(很快的刷卡响应速度), 但会导致人手抖动引起的误读卡概率显著增大; 时长过长, 虽能降低人手抖动误读卡概率, 但牺牲了刷卡敏捷性(需等待相对漫长的时间才能完成刷卡行为), 用户刷卡体验受到负面影响. 正常的人为有意识“刷卡”行为, 从卡接近读卡器到离开, 至少需要 500ms 的完成时间(蓄意的快速刷卡行为除外). Δt 的取值根据大量的实验数据, 在边界防抖性能和用户体验之间综合考量得出, 实际可取 200ms, 则读卡器判定人手是否有刷卡行为和持卡的人手是否已离开 RF 辐射区域所需的时长为 t=3*Δt=600ms, 在 NFC“防抖动性能”和“刷卡敏捷性”之间获得了较好的性能折中.

2 测试情况

如图 6, 实测时将所设计的支持电力线通信的家用智能路由器以智能插座的形式嵌入到家庭住房的墙体暗盒中, 其电路板包括数字板和电源板两部分. 数字板上放置 NFC、PLC 等弱电器件; 电源板与 220V 强电相接, 具有较大的空间辐射电源噪声, 如前文所述, 会对数字板上离其较近的 NFC 读卡器的读卡行为产生干扰. 采用本文设计的抗干扰措施后, 经实测, 发现该干扰得到了很好的抑制, NFC 读卡器可以正常读卡并获取卡中的数据. 经上万次读卡实测, 采用本文提出的干扰抑制技术后, 没有出现误读卡的现象. 而未采用该干扰技术时, 误读率在 10%左右. 所设计电路板实物照片及主要器件介绍如图 7 所示.

安全性方面, 我们尝试先用某张 NFC 卡加密两个智能插座的 PLC 链路并建立通信连接, 之后用另一张 NFC 卡(两者的 UID 不同)“刷”第三个智能插座, 且这三个智能插座底层用电力线连接. 结果发现第三个插座无法与其他两个插座建立 PLC 通信连接, 这表明采取该加密方法的安全性较高. 需要注意的是, 第一张 NFC 卡不能被其他用户非法获取并对第三个插座进行非法 PLC 链路加密.

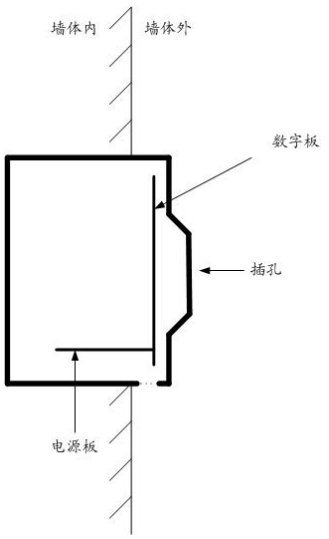
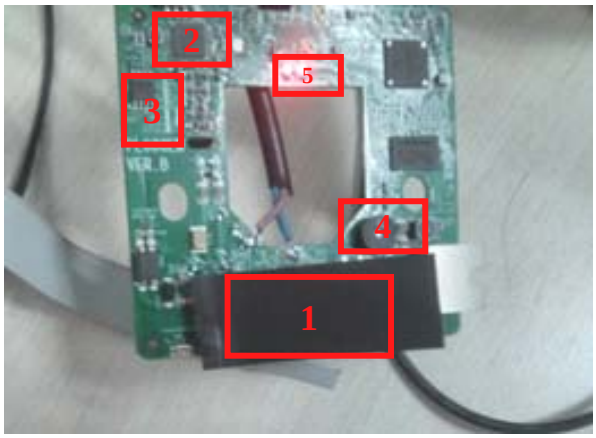


图 6　实测示意图



1）NFC读卡模块　　4）蜂鸣器
2）PLC芯片　　5）LED灯
3）Flash存储器

图 7　电路板实物照片

3　结论

基于电力线的智能家居设备底层组网方式是对现有组网方式(如无线 WiFi)的有效补充, 可以弥补现有组网方式的缺陷. 为了确保通信安全性, 电力线通信需要进行加密, 而现有加密方式在便捷性、安全性、可靠性方面存在问题. 本文提出的基于 NFC 的电力线通信加密方法较好解决了该问题. 经实测, 读卡便捷、准确、稳定, 且具有较好的抗强电与人手抖动干扰的能力.

参考文献

1 张川.智能家庭网络:技术、标准与应用实践.北京:人民邮电出版社,2014.2:1−14.

2 殷树刚,张成文,田海亭,等.载波侦听/冲突检测机制应用于低压电力线载波通信的适应性分析.电网技术,2012,36(8):233−238.

3 Ali KM, Lai SW, Messier GG. An evaluation of frequency domain PLC interference cancellation, for DSL systems, IEEE International Conference on Communications (ICC), 2013. 4315−4320.

4 Mudriievskyi S. Power line communications: State of the art in research, development and application. AEU-International Journal of Electronics and Communications, 2014, 68(7): 575−577.

5 戚佳金,陈雪萍,刘晓胜.低压电力线载波通信技术研究进展.电网技术,2010,34(5):161−172.

6 刘晓胜,戚佳金,宋其涛,等.基于蚁群算法的低压配电网电力线通信组网方法.中国电机工程学报,2008,28(1):71−76.

7 Ahmed M, Lampe L. Power line communications for low-voltage power grid tomography. IEEE Trans. on Communications, 2013, 61(12): 5163−5175.

8 梁栋,张保会,牛东文,等.用于多用户宽带电力线通信的同步信号的设计与实现.中国电机工程学报,2014,34(1):197−205.

9 Carcelle X. Power Line Communications in Practice, London UK: Artech House, 2009.2: 217−245.

10 HomePlug AV2 White Paper. www.homeplug.org. 2013. 3−12.

11 Daemen J, Rijmen V. The Design of Rijndael: AES-the Advanced Encryption Standard. Germany: Springer, 2002: 1−8.

12 王淼.NFC 技术原理与应用.北京:化学工业出版社,2014.6:1−10.

13 贾凡,佟鑫.NFC 手机支付系统的安全威胁建模.清华大学学报(自然科学版),2012,52(10):1460−1464.

14 Type 2 Tag Operation Technical Specification. http://www.nfc-forum.org. [2007-07-09].

15 ISO/IEC 14443-3, Identification cards - Contactless integrated circuit(s) cards - Proximity cards - Part 3: Initialization and anticollision. 2000.7: 1−37.