基于国密技术的 Zigbee 安全通信模型设计*

石皓铭 朱雪平 陈积常** 李建

南宁学院信息工程学院，南宁 530200

摘 要 针对 ZigBee 通信技术在智能家居应用中面临的数据窃取、信息篡改、信息重放、业务否认等网络安全威胁，提出应用国家商用密码技术保护 ZigBee 通信安全的需求，构建基于国密技术的 ZigBee 安全通信系统模型，运用 SM2～SM4 等国家商用密码算法、数字签名等技术，设计了相关认证协议。协议的安全性分析表明，所设计的模型能够抵御黑客发动的主动攻击和被动攻击，在密码应用的合规性、正确性和有效性方面具有一定优势。

关键字 ZigBee 技术，智能家居，CA 认证，国家商用密码算法，数字签名

Design of Zigbee Security Communication Model Based on National Cryptography Technology

Shi Haoming Zhu Xueping Chen Jichang Li Jian

School of Information Engineering Nanning University
Nanning 530200,China;
943667593@qq.com

Abstract—In response to the network security threats faced by ZigBee communication technology in smart home applications such as data theft, information tampering, information replay, and business denial, this paper proposes the need to apply national commercial cryptography technology to protect ZigBee communication security. A ZigBee secure communication system model based on national cryptography technology is constructed, and relevant authentication protocols are designed using national commercial cryptography algorithms such as SM2 to SM4, digital signatures, and other technologies. Security analysis shows that the model designed in this paper can resist both active and passive attacks launched by hackers, and Has certain advantages in terms of compliance, correctness, and effectiveness of password applications.

Keywords—Zigbee technology, smart homes, CA authentication, national commercial cryptographic algorithm, digital signature

1 引 言

随着物联网、智能家居、智慧城市等领域的快速发展，对 ZigBee 这种低功耗、低速率、短距离无线通信技术的需求越来越大。作为国外引进的一种移动通信技术，如何应用国家商用密码技术保障其通信安全是产业界和学术界共同关注的研究课题[1]。

目前，国内外对于 ZigBee 的研究已经取得了一定的进展。国外有关 ZigBee 的研究主要集中在协议设计、网络拓扑结构、安全性等方面。其中，协议设计是 ZigBee 研究的核心内容之一。美国国家标准技术研究所（NIST）提出了一种基于 ZigBee 的无线传感器网络协议，该协议可以实现低功耗、低成本、高可靠性的无线传感器网络[3]。瑞典皇家理工学院的研究人员提出了一种基于 ZigBee 的无线传感器网络拓扑结构，该结构可以实现高效的数据传输和节点管理[4]。在安全性方面，英国伦敦大学学院的研究人员提出了一种基于 ZigBee 的安全协议，该协议可以保护无线传感器网络的数据安全和隐私[5]。

国内方面，ZigBee 的研究主要集中在应用领域和技术创新方面。在应用领域方面，有关基于 ZigBee 的智能家居系统可以实现家庭设备的远程控制和智能化管理[6-8]。在技术创新方面，基于 ZigBee 的无线传感器网络技术研究可以实现低功耗、低成本、高可靠性的无线传感器网络[9-11]。在安全性方面，人们多关注安全监控、安全接入、安全通信与传输、安全管理等方面的研究与技术应用[12-15] 。

虽然国内外对于 ZigBee 的研究已经取得了一定的进展，但是仍要面临一些问题和挑战。例如，ZigBee 的安全性问题需要进一步加强，ZigBee 的应用领域需要进一步拓展，ZigBee 的技术创新需要进一步深入。为此，本文深入分析应用国家商用密码技术保护 ZigBee 通信安全的需求，提出一种基于国密技术的

*基金资助：本文得到南宁学院一流专业培育项目(2020YLZYPY01) 的资助。

**通讯作者：陈积常，教授，943667593@qq.com.

ZigBee 安全通信系统模型，设计了相关认证协议。最后通过分析协议的安全性，说明所设计的模型能够抵御黑客发动的主动攻击和被动攻击，在密码应用上具有合规性、正确性和有效性。

2 国密 ZigBee 智能家居安全通信系统需求分析

2．1 系统需求分析

首先，智能家居系统需要具备安全通信的功能。采用基于 Z 国密的 ZigBee 安全通信模型技术，可以确保通信过程中的数据安全性和隐私保护。这种技术可以对数据进行加密和解密，防止数据被黑客窃取或篡改，保障用户的隐私和安全。

其次，智能家居系统需要支持多设备互联。智能家居系统中有多种智能设备，如智能灯具、智能门锁、智能窗帘等，这些设备需要互相控制和信息共享。因此，智能家居系统需要支持多种智能设备的互联，实现设备之间的互相控制和信息共享。

第三，智能家居系统需要支持远程控制。用户可以通过手机、平板等移动设备远程控制智能家居设备，实现随时随地的控制和管理。这种功能可以提高用户的生活便利性和舒适度。

第四，智能家居系统需要实现智能化管理。通过智能算法和数据分析，实现智能化管理，如自动化控制、场景联动等，提高用户的生活便利性和舒适度。例如，智能家居系统可以根据用户的生活习惯和喜好，自动调节室内温度、光线等，提高用户的生活质量。

第五，智能家居系统需要提供友好的人机交互界面。智能家居系统需要支持语音、手势、触控等多种交互方式，方便用户的操作和使用。这种功能可以提高用户的使用体验，使用户更愿意使用智能家居系统。

最后，智能家居系统需要保证数据安全和系统稳定性。采用数据加密、备份等技术，确保用户数据的安全性和可靠性。同时，保证系统的稳定性和可靠性，避免系统崩溃、数据丢失等问题，提高用户使用体验。

2．2 模型功能性需求分析

国密ZigBee智能家居安全通信系统的模型功能性需求主要包括以下几个方面：

① 安全性：系统需要提供高度的安全性，确保通信过程中的数据不被窃取、篡改或伪造。为此，系统需要支持国密算法，包括SM2、SM3、SM4等，以保证数据的加密、签名和认证。此外，系统还需要支持安全密钥管理，包括密钥生成、分发、更新和撤销等功能，以确保密钥的安全性和可靠性。

② 可靠性：系统需要保证通信的可靠性，确保数据的正确传输和接收。为此，系统需要支持可靠传输协议，包括ARQ（自动重传请求）和FEC（前向纠错）等，以确保数据的完整性和可靠性。此外，系统还需要支持网络拓扑管理，包括路由选择、拓扑优化和网络维护等功能，以确保网络的稳定性和可靠性。

③ 兼容性：系统需要兼容不同厂商的智能家居设备，确保设备之间的互通性。为此，系统需要支持标准化协议，包括ZigBee、Z-Wave、BLE等，以确保设备的互通性和兼容性。此外，系统还需要支持设备管理，包括设备发现、配置和控制等功能，以确保设备的可用性和兼容性。

④ 易用性：系统需要具备良好的用户界面和操作体验，方便用户进行操作和管理。为此，系统需要支持友好的界面设计，包括图形化界面、语音提示和操作指南等，以提高用户的使用体验和满意度。此外，系统还需支持智能化管理，包括自动化配置、智能推荐和智能诊断等功能，以提高用户使用效率和便捷性。

⑤ 扩展性：系统需要具备一定的扩展性，能够支持新的智能家居设备和功能的添加。为此，系统需要支持模块化设计，包括插件式架构、可扩展接口和开放API等，以方便第三方开发者进行扩展和定制。此外，系统还需要支持互联互通，包括与其他智能家居平台的对接和互联互通等功能，以提高系统的整体性和互操作性。

3 国密 ZigBee 智能家居安全通信系统模型设计

本文设计的国密 ZigBee 智能家居安全通信系统架构如图 1 所示。该系统结构包括内部网络和外部互联网，内部网络用于在家控制家居设备，外部网络用于实现远程控制。内部网络采用 ZigBee 协议通信方式，数据量小、传输距离短、节点多。外部网络采用安全的内网穿透方案 ZeroTier，并基于 MQTT 协议进行远程控制。MQTT 服务器作为中心控制器，路由器作为 MQTT 服务器，手机客户端和 Z-Wave 控制器作为 MQTT 客户端。内部网络的 ZigBee 终端节点通过传感器采集室内的温度、光照等信息，并通过 ZigBee 协议发送给 Z-Wave 控制器。Z-Wave 控制器再通过 WiFi 发送给 MQTT 服务器。手机客户端和作为控制设备，可以发送控制信息给 MQTT 服务器。MQTT 服务器再发送给 Z-Wave 控制器，Z-Wave 控制器依据接收的控制信息，控制家居设备进行相应动作，如开启或关闭。窗帘、开/关电灯等。

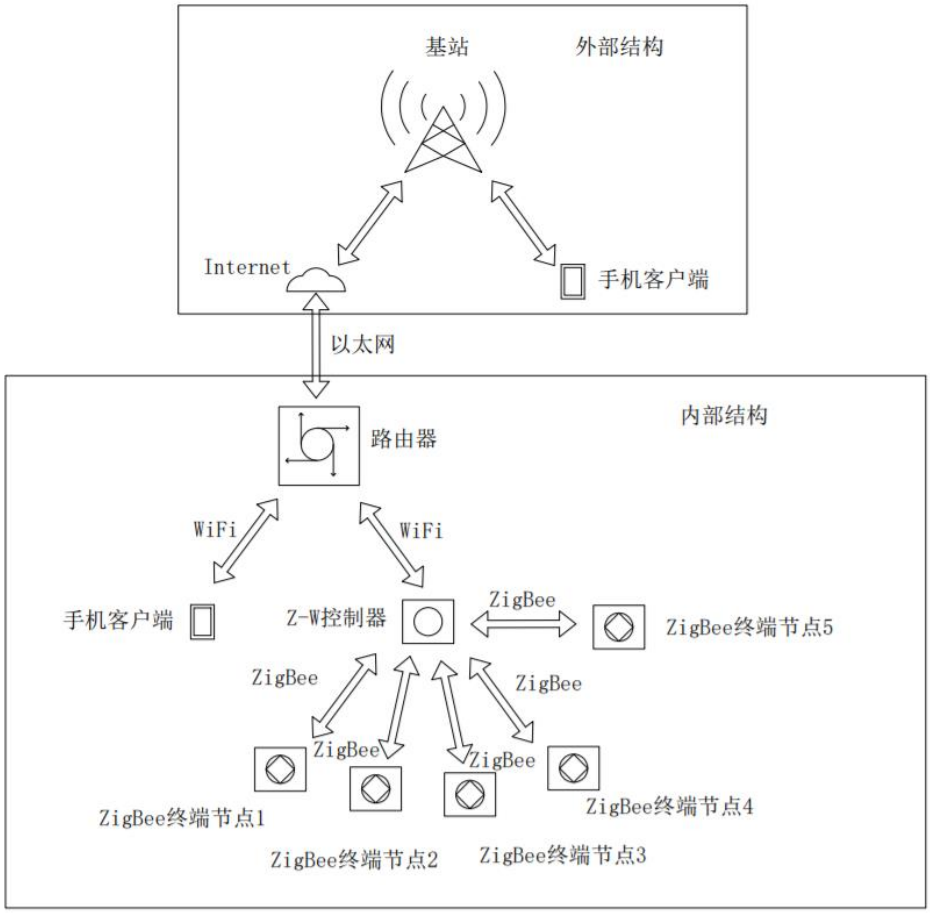

图 1 国密 ZigBee 智能家居安全通信系统架构图

MQTT 服务器采用的是一种基于发布/订阅模式的消息传输协议[16]，它是一种轻量级的、开放的、简单的、易于实现的、可扩展的协议。MQTT 服务器可以用于连接物联网设备和应用程序，实现设备之间的通信和数据传输。MQTT 服务器通常由三个部分组成：客户端、代理服务器和消息代理。客户端是指连接到 MQTT 服务器的设备或应用程序，代理服务器是指负责转发消息的服务器，消息代理是指负责存储和转发消息的组件。MQTT 服务器支持多种消息传输模式，包括点对点通信、广播和多播等。它还支持多种安全机制，如 TLS/SSL 加密、用户名和密码认证等，以保证数据的安全性和可靠性。MQTT 服务器已经成为物联网领域中最流行的消息传输协议之一，被广泛应用于智能家居、智能城市、工业自动化等领域。

ZeroTier 则是一种虚拟网络技术[17]，它可以将多个设备连接到一个虚拟网络中，实现设备之间的通信和数据传输。ZeroTier 的特点是易于使用、安全可靠、跨平台、高效稳定。它可以在任何操作系统上运行，包括 Windows、Mac、Linux、iOS、Android 等。ZeroTier 的工作原理是通过创建一个虚拟网络，将多个设备连接到这个虚拟网络中，然后通过 ZeroTier 的服务器进行数据传输。ZeroTier 的服务器是分布式的，可以在全球范围内部署，以保证数据传输的速度和可靠性。ZeroTier 还支持多种安全机制，如加密、身份验证等，以保证数据的安全性和可靠性。ZeroTier 已经被广泛应用于物联网、云计算、远程办公等领域，成为了一种重要的虚拟网络技术。

4 身份认证及授权密码应用工作流程

4.1 国密 ZigBee 智能家居安全通信系统协议设计

本文设计的国密 ZigBee 智能家居安全通信系统协议的设计思路是：使用数字签名技术、SM2 等算法实现了手机客户端 A、Z－W控制器 Z 和 MQTT 服务器 M 三方之间的双向身份认证；在认证通过后，双方就可以利用互相传送的数据其中包含了自身的私钥和对方公钥，从而完成加密解密相关的数据的操作。在本次协议中，使用了一些符号，而这些符号的含义如表 1 所示。协议的流程如图 1 所示。

4.2 协议流程图说明

（1）$ID_A||T_1||E_{SK_A}[H(ID_A||T_1)]||E_{SKCA}(T_2||ID_A||PK_A)$

手机客户端 A 发送自己的身份信息、时间戳和数字签名，以及自己的证书给 Z-W 控制器 Z。证书包含了由 CA 签发的信息，由此来证明客户端 A 的真实身份。

表 1 协议通信符号说明

符 号	说 明
IDA	手机客户端 A
IDZ	Z－W控制器 Z
IDM	MQTT服务器M
T	时间戳
H	杂凑值
‖	拼接操作
Ex[Y]	用x对Y进行加密
Dx[Y]	用x对Y进行解密
DpkA	手机客户端 A 用 SM2 算法的公钥
DskA	手机客户端 A 用 SM2 算法的私钥
DpkZ	Z－W控制器 Z 用 SM2 算法的公钥
DskZ	Z－W控制器 Z 用 SM2 算法的私钥
DpkM	MQTT服务器M用SM2算法的公钥
DskM	MQTT服务器M用SM2算法的私钥
PASSWORD	口令
DS_Auth	SM2公钥密码算法和SM3杂凑算法的数字签名认证算法

（2）Z－W控制器 Z 对进行手机客户端 A 的身份验证：

① Z－W控制器 Z 利用 CA 的公钥确认手机客户端 A 证书的真实性。

$CertA=D_{PKCA}[E_{SKCA}(T_2||ID_A||PK_A)]=T_2||ID_A||PK_A$

② 使用 Z-W 控制器 Z 的公钥验证 A 的签名是否真实。

$H_1=Z_{PKA}[E_{SKA}(H(ID_A||T_1))]=H(ID_A||T_1)$

③ Z-W 控制器 Z 对相关数据进行哈希运算，得到哈希值 $H_2=H(ID_A||T_1)$。

④ 如 H_1 和 H_2 相等，Z-W 控制器 Z 就可以确认发送方是手机客户端 A，否则 Z-W 控制器 Z 无法确认发送方的身份。

（3）$ID_A||ID_Z||T_3||E_{SKZ}[H(ID_A||ID_Z||T_3)]||E_{SKCA}(T_4||ID_Z||PK_Z)$

Z-W 控制器 Z 向手机客户端 A 发送包含时间戳、身份、Z 的签名数据以及由 CA 签发的证书的信息。

（4）手机客户端 A 对 Z-W 控制器 Z 的身份验证：

① 使用 CA 的公钥对 Z-W 控制器 Z 的证书进行验证确认，从而确保 Z 证书的真实性。

$Cert\ Z=D_{PKCA}[E_{SKCA}(T_4||ID_Z||PK_Z)]=T_4||ID_Z||PK_Z$

② 使用 Z-W 控制器 Z 的公钥验证 Z 的签名是否真实。

$H_3=Z_{PKZ}[E_{SKZ}(H(ID_A||ID_Z||T_3))]=H(ID_A||ID_Z||T_3)$

③ Z-W 控制器 Z 对相关数据进行哈希运算，从而获得哈希值[7] H_4

$H_4=H(ID_A||ID_Z||T_3)$ ④如若 H_3、H_4 是否相等，则手机客户端 A 就可以发送方确认对方就是 Z-W 控制器 Z，不然手机客户端 A 就不能确认信息发送方是否为 Z-W 控制器 Z。

（5）$ID_A||T_5||E_{SKA}[H(ID_A||T_5)]||E_{SKCA}(T_2||ID_A||PK_A)$

手机客户端 A 向 MQTT 服务器发送相关身份数据。

（6） MQTT 服务器 M 对手机客户端 A 身份验证：

① 使用 CA 的公钥验证 A 发送过来的信息，从而确认手机客户端 A 证书的真实性。

② 手机客户端 A 的利用公钥解析 M 的签名从而获得哈希值。

③ MQTT 服务器 M 运算得出哈希值[6] 。

④ 判断哈希值是否相等，如果相等则 MQTT 服务器 M 就能确认信息发送方就是手机客户端 A，不然就不能确认对方身份信息的真实性。

（7）$ID_A||ID_M||T_6||E_{SKM}[H(ID_A||ID_M||T_6)]||E_{SKCA}(T_7||ID_M||PK_M)$

MQTT 服务器 M 向手机客户端 A 发送相关身份数据。

（8）同（2）、（4）、（6）步骤：手机客户端 A 对对方进行身份鉴别；验证通过就能确定信息发送方是 MQTT 服务器 M。

（9） $ID_A||T_8||DS\_Auth||E_{SKA}[H(ID_A||T_8||DS\_Auth)]$

手机客户端 A 向 Z-W 控制器 Z 发送相关身份数据。

（10） Z-W 控制器 Z 会验证并确认手机客户端 A 发送的信号：

① 通过使用手机客户端 A 的公钥验证 C 的签名是否真实。

$H_5=D_{PKA}[E_{SKA}[H(ID_A||T_8||DS\_Auth))]=H(ID_A||T_1||DS\_Auth)$

② Z-W 控制器 Z 运算得出哈希值 H_6。

$H_6=H(ID_A||T_1||DS\_Auth)$

③ 判断 H_5、H_6 是否相等，如果相等就能确认该

信号是由手机客户端 A 所传送的，不然就无法确认信息的来源处。

（11） $ID_Z||T_9||E_{SK_Z}[H(ID_Z||T_9)]||E_{SKCA}(T_4||ID_Z|PK_Z)$

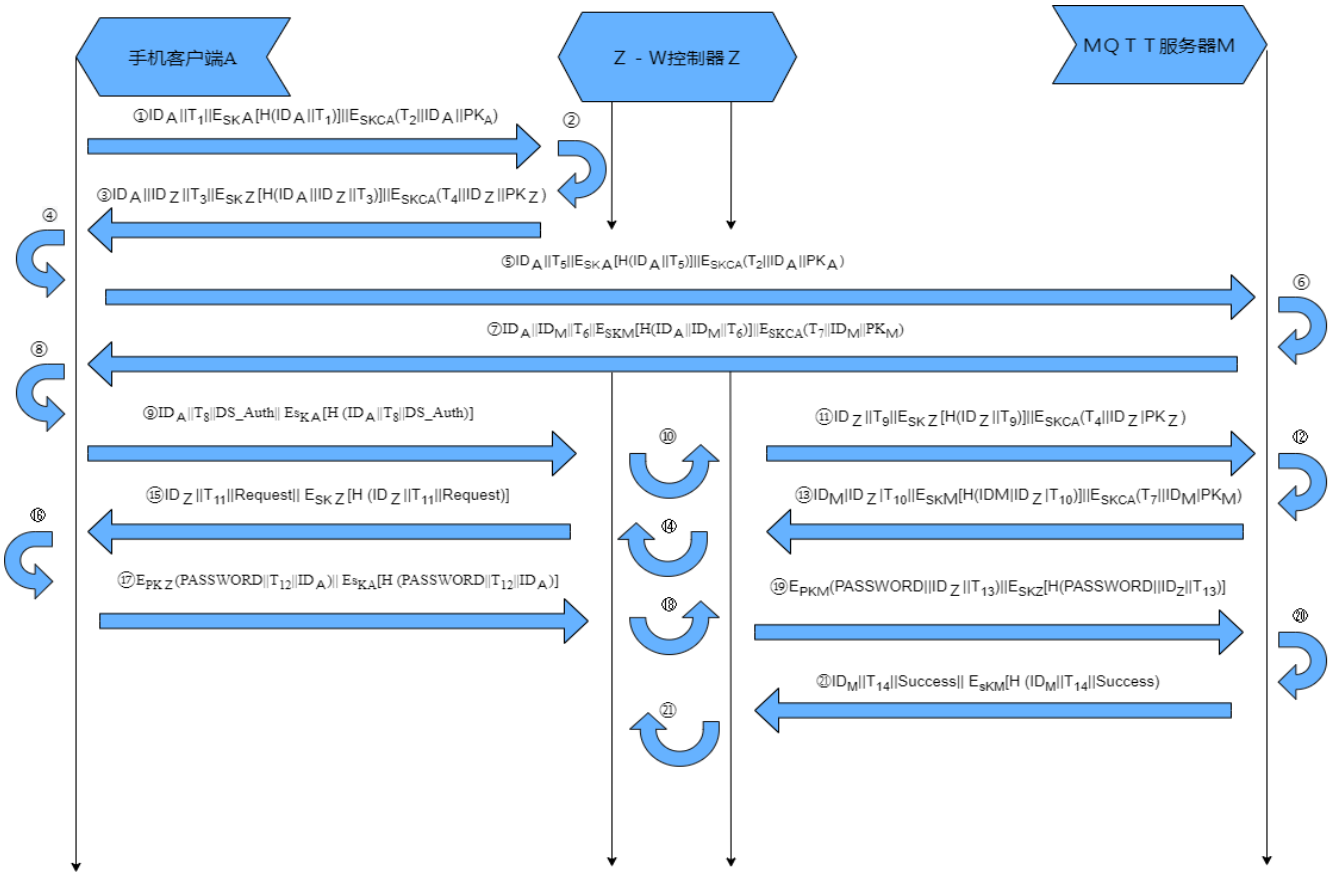

图 2 协议流程图

（12） MQTT 服务器 M 对对信息发送方进行身份验证，只有验证通过，才能确认发送方是 Z-W 控制器 Z。

（13） $ID_M|ID_Z|T_{10}||E_{SK_M}[H(ID_M|ID_Z|T_{10})]||E_{SKCA}(T_7||ID_M|PK_M)$

MQTT 服务器 M 向 Z-W 控制器 Z 发送相关身份数据。

（14）Z-W 控制器对信息发送方进行身份验证，只有验证通过，才能确认发送方是 MQTT 服务器 M。

（15） $ID_Z||T_{11}||Request||E_{SK_Z}[H(ID_Z||T_{11}||Request)]$

Z-W 控制器 Z 向手机客户端 A 发送相关数据，手机客户端 A 对对方发送的信息进行鉴定；鉴定信息是由 Z-W 控制器 Z 发送过来的。

（16） 同（10）步骤，手机客户端 A 对对方发送 Z-W 控制器 Z 向 MQTT 服务器 M 发送相关身份数据。

的信息进行鉴别；鉴别发送的信息是 Z-W 控制器 Z 发送过来的。

（17） $E_{PK_Z}(PASSWORD||T_{12}||ID_A)||E_{SKA}[H(PASSWORD||T_{12}||ID_A)]$

手机客户端 A 对 PASSWORD 等数据进行加密，采用的是 SM3 算法。以及运用 A 的私钥运算起 SM2 算法接收数据的哈希值进行数字签名。

（18）Z-W 控制器 Z 执行以下操作：

① 使用 Z-W 控制器 Z 的私钥解密签名信息获取哈希值 H_{13}，运输出哈希值

$H_7=H(PASSWORD||T_{12}||ID_A)$

② 用手机客户端 A 的公钥解密签名信息获取哈希值 H_{14}，运算出哈希值

$H_8=H(PASSWORD||T_{12}||ID_A)$

③ 如果 H_{13} 和 H_{14} 相等，那么 Z-W 控制器 Z 可确认该消息是由手机客户端 A 发送的且没有遭受篡改。

（19） $E_{PK\ M}$ (PASSWORD||ID $_{Z}$ ||T_{13})|| $E_{SK\ Z}$ [H(PASSWORD||ID_Z||T_{13})]

Z-W 控制器运行 SM3 算法对 PASSWORD 等数据进行加密，从而能保证机密且确保数据的完整性。Z-W 控制器 Z 运行 SM3 算法加密数据 PASSWORD 等，从而能保证机密且确保数据的完整性；随后 Z-W 控制器 Z 使用私钥运行 SM2 算法对 PASSWORD 等数据进行签名。

（20）MQTT 服务器 M 执行以下操作：

① Z 根据给定的私钥，解密签名信息并获取哈希值 H_9，从而计算新的哈希值

H9=H(PASSWORD||ID Z ||T13)

② 通过使用 A 的公钥对签名信息进行解密，可以得到哈希值 H21。然后，计算该哈希值

H_{10}=H(PASSWORD||ID_Z||T_{13})

③ 如果 H_9 和 H_{10} 相等，那么 MQTT 服务器 M 可以确定该消息是由 Z-W 控制器 Z 发送过来并且没有遭受篡改。当 Z－W 控制器向 M Q T T 服务器发送已加密的用户身份信息和经过加密的口令信息时，服务器会对这些信息进行解密并将它们与数据库中储存的信息进行比对确认。

（21）D_M||T_{14}||Success|| Es_{KM}[H (ID_M||T_{14}||Success)

互相验证成功后，MQTT 服务器 M 向 Z-W 控制器 Z 发送相关数据，并且 MQTT 服务器 M 将用私钥完成签名。

（22） Z-W 控制器 Z 对发送过来的数据进行鉴别，如确认该信息来自 MQTT 服务器 M，则 M Q T T 服务器与手机客户端 A 取得联系，并成功登陆服务器。

4．3 安全性分析

（1） 抗身份假冒攻击

该系统采用国密 SM2 算法对设备进行身份认证，防止非法设备接入系统。每个设备都有唯一的身份标识符，只有经过身份认证的设备才能接入系统，从而有效防止身份假冒攻击。具体来说，系统在设备接入时，会要求设备提供其身份标识符和相应的密钥，然后使用 SM2 算法对其进行身份认证，只有认证通过的设备才能接入系统。

并且该系统的三方都进行了双向身份认证,并且由上面的流程图说明可得使得 Z 的随机生成数被保存在安全芯片中。而被受信任的 CA 则利用 PKI 发布其余的签名证书，因此只有满足条件的才能签名公钥对于的签名私钥。如 A 给 Z 发送相关信息，Z 通过验证相关信息绝密其哈希值等来判断 A 的身份的真实性，并且 Z 的验证运算又包含 A 所发送的相关信息。同理，A 也可以由此来验证 Z 来实现双向验证。因此，只要能守护自身的私钥，其余都不能伪造相关信息，盗领其身份。

（2） 抗重放攻击

A 对 Z 发送的相关信息包含大量内容，如自身的时间戳，而时间戳则是数字签名所带来的数据，并且对象也包含量了签名参数、时间等。所以，如若，非法入侵者重放了一条 A 的信息给了 Z，Z 能够通过相关信息计算时间戳，从而判断信息的新鲜值，来判断信息发送放是否在恶意攻击，从而达到抗重放攻击的功能。

（3） 抗篡改攻击

国密 zigbee 安全通信模型采用了 SM2 和 SM3，同时还引入了数字签名技术，以保证通信的机密性、完整性和认证性。这些安全机制的综合应用，使得该模型具有较强的抗篡改攻击能力。

具体来说，国密 zigbee 安全通信模型的抗篡改攻击能力主要体现在以下方面：

SM3 算法用于数据完整性保护，通过对接收到的数据进行摘要计算，并与预先计算好的摘要进行比对，验证数据是否被篡改。SM3 的散列长度较长，相对于其他散列函数而言，碰撞概率更低，让数据验证更加安全可靠。

SM2 算法用于数字签名在通信过程中，发送方会对每个数据包进行数字签名，并将签名值附加在数据包中。接收方在接收到数据包后，也会进行数字签名验证，并将验证结果与数据包中的签名值进行比较。如果两者一致，则说明数据包未被篡改。否则，接收方会拒绝该数据包。这种机制可以有效防止数据包被篡改或伪造攻击。

4．4 性能对比分析

根据 GB/T39786-2021《信息安全技术 信息系统应用基本要求》,我们将论文方案与参考文献[18]、[19]进行了对比分析，对比的内容主要涉及抗密钥攻击、身份验证、抵抗篡改攻击、密码应用正确、密码应用合规、密码应用有效等方面。国密 ZigBee 智能家居安全通信协议的实验对比平台实在 Linux 操作系统平台上，利用 Xshell 终端模拟软件和 GmSSL 密码工具箱来实现的。

实验对比结果见表 2。从方案对比结果可以看出，文献[18]使用的 ECC 实现技术较为复杂，需要更复杂的数字签名和认证机制，这可能会增加系统的复杂性

和成本。而文献[19]则没有提供用户与电子身份认证系统交互消息的安全防护。相比之下，本文方案提供了双向认证，并采用国密算法 SM2/SM3/SM4，能够有效地防止篡改、假冒和重放攻击，具有较高的安全性。

表 2 设计方案比较

安全性能	文献[19]方案	文献[18]方案	本文方案
身份验证	数字证书	多因素身份验证	数字签名、数字证书
密码算法	AES	ECC	SM2、SM3、SM4
安全协议	无	有	有
抵抗篡改攻击	是	是	是
抵抗假冒攻击	是	是	是
抵抗重放攻击	否	否	是
提供双向认证	否	否	是
抵抗密钥攻击	是	否	是
密码应用正确	否	是	是
密码应用合规	否	是	是
密码应用有效	否	否	是

5 结束语

在分析 ZigBee 通信面临的信息窃密、信息篡改、信息重放、身份假冒、业务否认等网络威胁的基础上，本文提出了一种应用国密技术保护 ZigBee 通信的方案，构建基于 ZigBee 技术的安全通信系统模型，运用 SM2～SM4 等国家商用密码算法、数字签名等技术，设计了相关认证协议。安全性分析表明，与现有的方案相比，本文方案提供了双向认证，并采用国密算法 SM2/SM3/SM4，能够有效地防止篡改、假冒和重放攻击，具有较高的安全性、正确性和有效性。

参 考 文 献

[1] 李东林,古丽米拉·克孜尔别克.基于 ZigBee 的智能家居系统研究 综述[J].计算机时代.2019,(6):23-25, 30

[2] 蒲泓全, 贾军营, 张小娇,等. ZigBee 网络技术研究综述[J].计算机系统应用,2013,22(09):6-11

[3] 黄太波, 赵华伟, 潘金秋,等.ZigBee 协议栈的安全体系综述[J],山东科学,2012,25(2):59-66

[4] 张东阳.基于 ZigBee 的无线传感器网络定位技术研究[D].长春：吉林大学，2020.

[5] 刘叶,秦丽明,汪莎莎,等.ZigBee 网络物理层安全传输方法设计[J].山西电子技术,2017,(4):69-71.

[6] 林婷婷, 樊森, 张新英.基于 ZigBee 的智能家居公共安全系统控制平台研究[J].机械工程与自动化,2023, (04):36-38

[7] 于国福.基于 ZigBee3.0 技术的智能家居系统设计[J]. 电视技术. 2022,46(10):222-225

[8] 邓楷煊, 张金尧, 许彩望.ZigBee 技术下的智能家居系统设计[J].物联网技术,12(9):91-93+97

[9] 杨静.Zigbee 技术在无线传感器网络中的应用分析[J].无线互联科技,2020,17(19):17-18

[10] 王思华, 郑树强, 丁轶华.ZigBee 无线传感器网络技术及其应用探讨[J].无线电工程,2020,50(5):415- 417

[11] 韩薇薇.基于 ZigBee 技术的无线网络应用研究[J].信息记录材料. 2022,23(10):233-236

[12] 林婷婷,樊森,张新英.基于 ZigBee 的智能家居公共安全系统控制平台研究[J].机械工程与自动化. 2023, (04):36-38

[13] 张彩娇.基于 ZigBee 无线通信技术的基站安全监控系统设计[J].数字通信世界,2023,(3):5-7

[14] 王海珍, 廉佐政, 谷文成.基于 ZigBee 的智能家居系统安全通信研究[J].电子测量技术,2021,44(18):78- 84

[15] 张军,严丽娜, 兰宇浩.基于签密技术的 ZigBee 网络信息安全传输问题研究[J].通信技术,2021,54(10): 2418-2421

[16] 陈文艺，高婧，杨辉．基于 MQTT 协议的物联网通信系统设计与实现[J]．西安邮电大学学报，2020,25(3):30-36.

[17] 钱立．一种内网穿透控制智能家居设备的方案[J]．现代信息科技，2020,4(18):177-179..

[18] 张晓华. 基于 ZigBee 的自动抄表系统研究与设计[D].青岛：青岛科技大学,2009

[19] 侯坤,闵新力.基于 Zigbee 的粮情监控系统加密算法[J].计算机工程,2011,37(S1):146-148,155