智能家居系统中的物联网数据安全与隐私保护

闫保峰
（山西应用科技学院，山西省太原市，030000）

摘要　智能家居系统是指通过互联网技术将各种家用设备联网，实现智能化控制和管理的系统。随着物联网技术的不断发展和普及，智能家居系统逐渐成为现代家庭的重要组成部分，为人们提供了便利、舒适和安全的居住环境。然而，随着智能家居设备数量和功能的增加，物联网数据的安全性和隐私保护问题日益突出，成为智能家居系统发展面临的重要挑战。本文分析了智能家居系统中的物联网数据安全与隐私保护的实施策略，并分析了基于TSL/SSL加密协议的高速率数据加密方法。

关键词　智能家居系统；物联网；数据安全；隐私保护；加密

中图分类号：TP309　文献标识码：B
文章编号：1008-0899(2025)02-0028-03

随着智能家居系统的普及，其涉及的数据范围也越来越广泛，包括家庭成员的健康数据、安防监控数据、家庭环境数据等，这些设备通过互联网进行数据交换和控制指令传输，隐私数据如果被不法分子获取，不仅可能导致个人隐私泄露，还可能造成财产损失或者安全风险，导致家庭隐私泄露、设备被篡改或者系统被入侵，确保智能家居系统中的物联网数据安全性成为亟需解决的问题。

1　节点自组网

采用TLS/SSL协议进行设备间的安全通信，确保数据传输过程中的加密与完整性验证，设备之间采用基于数字证书的身份认证方式，确保通信双方的合法性，并建立严格的访问控制策略，只允许经过授权的设备进行通信与数据交换。

首先，使用AES或RSA等高强度加密算法对数据进行加密，确保数据传输的机密性，设计可靠的密钥管理机制，确保密钥安全的生成、分发和更新。其次，定期进行安全漏洞扫描与风险评估，及时发现并修复系统中存在的安全漏洞，在此基础上制定应急响应计划，对可能的安全风险进行预案设计与应对措施，并对个人隐私数据进行匿名化处理，在数据传输和存储中采用脱敏技术，降低敏感数据泄露的风险，从而制定隐私协议和政策，明确规定数据收集、使用和共享的范围和目的，保护用户的隐私权益。最后，需要配置安全监控系统，实时监测设备间通信和数据传输的安全状态，发现异常行为立即报警并采取应对措施，在此基础上记录安全事件和日志，有助于事后分析安全事件的原因和影响，并对安全策略进行调整和改进。与此同时，还需要为系统管理员和用户提供定期的安全培训，增强其对安全问题的认识和应对能力，并强化用户安全意识，提醒用户采取良好的密码管理、设备更新等安全实践措施。

在自组网的过程中，频谱管理是避免信道冲突的重要手段，通过对频谱资源的合理规划和管理，可以避免不同设备或网络之间的频道干扰，使用频谱扫描技术，可以检测到当前频谱使用情况，选择空闲频道或者低干扰频道进行通信，从而降低信道冲突的可能性。

在节点自组网中，采用碰撞检测技术可以及时发现数据包碰撞，避免同时发送多个数据包导致的信道冲突，实施退避机制，即在发生碰撞后随机选择一个时间延迟再次尝试发送，以减少碰撞的发生频率，提高数据传输成功率。此外，分时复用是将时间划分为若干时隙，在每个时隙内只允许一个设备进行数据传输，从而避免多个设备同时占用信道导致的冲突，通过轮询或者时间分配的方式，使得各个设备在各自的时隙内进行数据传输，减少了信道冲突的可能性。

2　网关TLS/SSL协议安全加密

作者简介：闫保峰（2003~），男，汉族，山西运城人，本科在读，研究方向：软件工程。

2.1　证书生成与配置

在智能家居系统中，物联网数据的安全传输是至关重要的，特别是网关与云服务器之间的通信，使用TLS/SSL协议进行安全加密可以有效保护数据的机密性和完整性，需要为网关和云服务器分别生成数字证书。证书一般包含公钥、私钥和数字签名等信息，证书的生成可以通过自签名、证书颁发机构（CA）签发等方式进行。自签名证书适用于私有网络或内部通信，而CA签发的证书通常具有更高的可信度和广泛性。

在网关和云服务器上配置证书时，需要将生成的证书和私钥导入到相应的证书存储中，如Keystore（Java平台）或Certificate Store（Windows平台）等，配置时需要注意证书的有效期、密钥长度、加密算法等安全参数，确保证书的安全性和合规性。具体而言，选择CA签发的证书，需要向CA机构申请证书并验证身份。CA机构会颁发包含公钥和数字签名的数字证书，证书中还包含CA的根证书信息，网关和云服务器会使用CA的根证书验证对方的数字证书有效性，确保通信双方的身份合法和通信安全。

此外，还需要定期更新证书是保证通信安全的重要步骤。证书的有效期通常为1年或更长，到期后需要重新申请或续期证书，避免证书过期导致通信故障或安全风险，证书更新时需要注意更新证书内容、更新密钥等步骤，确保更新后的证书与原证书兼容并且安全可靠。

2.2　密钥交换与协商

在智能家居系统中，物联网数据的安全传输对于网关与云服务器之间的通信至关重要。密钥交换与协商是TLS/SSL协议安全加密过程中的关键步骤，在TLS/SSL协议中，密钥交换的目的是确保网关与云服务器之间能够建立安全的通信密钥，用于对数据进行加密和解密。

在RSA密钥交换中，网关和云服务器分别生成公钥和私钥对。网关使用云服务器的公钥加密一个随机生成的对称密钥，并发送给云服务器，云服务器使用自己的私钥解密得到该对称密钥，从而完成密钥交换过程。Diffie-Hellman密钥交换是一种基于离散对数问题的密钥交换算法。它允许通信双方在不直接传递密钥的情况下协商出共享的对称密钥，保证了密钥交换的安全性，密钥协商是指通信双方根据密钥交换过程协商出的临时密钥生成最终的通信密钥。在TLS/SSL协议中，密钥协商主要有以下几种方式：①使用对称加密算法（如AES）来保护通信数据，那么密钥交换后直接得到的就是对称密钥，通信双方可以直接使用该密钥进行加密和解密操作；②对于长时间的通信会话，可以使用临时的会话密钥来保护通信数据，会话密钥是通过密钥协商阶段生成的，用于一段时间内的通信保护；③在密钥协商过程中，确保即使长期密钥被泄露，之前和未来的通信数据也仍然是安全的，这称为前向安全性。

2.3　握手过程

握手过程开始于客户端向服务器发送ClientHello消息，其中包含了客户端支持的TLS/SSL版本、加密套件列表（包括加密算法、密钥长度等）、随机数以及压缩方法等信息。服务器收到客户端的ClientHello消息后，会回复一个ServerHello消息。在ServerHello中，服务器选择与客户端相匹配的TLS/SSL版本、加密套件，并生成一个随机数。此时，双方确定了通信使用的TLS/SSL版本和加密参数。服务器在ServerHello消息之后，会将自己的数字证书发送给客户端。证书包含服务器的公钥、证书有效期、CA签名等信息。客户端会验证服务器证书的有效性，包括证书是否过期、是否由受信任的CA签发等。

客户端收到服务器的证书后，会生成一个随机数（Pre-master Secret），并使用服务器的公钥加密该随机数，然后发送给服务器。这一步骤是为了确保后续通信中的对称密钥交换安全性服务器收到客户端发送的加密的Pre-master Secret后，使用自己的私钥进行解密，得到Pre-master Secret。服务器和客户端根据约定的协商方式（如Diffie-Hellman）使用该Pre-master Secret生成共享的对称密钥（Master Secret）。经过客户端和服务器的密钥协商过程后，双方都已经获得了相同的Master Secret。

2.4　数据传输与加密解密

一旦TLS/SSL握手过程完成并建立了安全的通信通道，网关与云服务器之间的数据传输就可以开始了。所有的数据传输都会通过这个安全通道进

行，确保数据在传输过程中不被窃取或篡改。在数据传输过程中，通常会采用对称加密算法来保护数据的机密性。常见的对称加密算法包括AES（高级加密标准）、3DES（Triple Data Encryption Standard）等。这些算法具有高效性和安全性，能够保护数据的隐私和完整性。对称加密算法需要使用密钥来进行加密和解密操作。在TLS/SSL握手过程中，客户端和服务器已经协商生成了一个共享的对称密钥（Master Secret）。这个密钥会被用于后续数据传输的加密和解密。为了适应不同大小的数据传输需求，加密的数据通常会被分段处理。对称加密算法将每个数据块使用密钥进行加密，并在传输前添加一些控制信息，确保接收方能够正确解密和还原数据。

在加解密的过程中，网关将要传输的数据按照数据块大小划分，然后使用协商好的对称密钥进行加密。加密后的数据在传输过程中不易被窃取和篡改。云服务器接收到加密数据后，使用相同的对称密钥进行解密操作。解密后的数据可以被服务器正常处理和分析，保证了数据的完整性和可读性，除了加密保护数据的机密性外，TLS/SSL协议还通过消息认证码（MAC）等机制保护数据的完整性。MAC会对数据进行哈希计算，生成一个摘要，用于验证数据在传输过程中是否被篡改。

3 消息认证码的哈希计算

消息认证码（MAC）是一种用于保证数据完整性和真实性的技术手段，它通过对数据进行哈希计算生成一段固定长度的认证码，用于验证数据在传输过程中是否被篡改或者伪造，在消息认证码的计算过程中，通常会使用哈希函数来生成认证码。哈希函数是将任意长度的输入数据转换为固定长度的输出。

选择合适的哈希算法，如SHA-256（安全哈希算法256位版本）、MD5（消息摘要算法5）、SHA-1等。这些算法有不同的输出长度和安全性等特点，将要传输的数据作为输入，经过哈希函数处理后得到哈希值，即消息认证码。这个哈希值就是用来验证数据完整性的关键。其次，接收方在接收到数据后，同样使用相同的哈希算法对接收到的数据进行哈希计算，得到接收到的数据的哈希值。然后将接收到的哈希值与传输过来的认证码进行比对。如果不一致，则说明数据可能被篡改或伪造，需要进一步的处理，比如丢弃该数据或者重新请求数据。

4 结语

本文深入探讨了智能家居系统中物联网数据的安全传输问题，特别是针对网关TLS/SSL协议安全加密的关键技术进行了详细阐述。在证书生成与配置阶段，必须确保网关和云服务器的数字证书有效且安全，同时密钥交换与协商环节保障了安全通信的密钥安全性。握手过程则建立了安全的通信通道，数据传输与加密解密阶段使用对称加密算法保护数据机密性，消息认证码的哈希计算则确保了数据的完整性和真实性。综合以上技术措施，智能家居系统的安全加密机制在保障物联网数据传输安全性和隐私保护方面发挥了关键作用，为用户提供了安全可靠的智能家居体验，对智能家居系统的发展具有重要意义。

参考文献

[1] 崔聚丰，郁舒兰，李晶.用户视角智能家居物联网监控系统现状与发展[J].家具，2023，44(4):31-35.

[2] 吴晴.基于物联网的智能家居系统[J].移动信息，2023，45(4):4-6.

[3] 孙宇舸，叶柠，匡涌.基于物联网的智能家居控制系统设计与实现[J].科技创新与应用，2022，12(34):110-113.