蓝牙传输安全调研与可靠传输系统设计

学号： 姓名：

摘要：随着蓝牙技术的不断发展，其应用范围从传统的点对点文件传输、语音通信等拓展至医疗监护、室内定位、智能家居等物联网领域，并展现出了较高的应用价值。然而无线信道的开放性使蓝牙与生俱来地面临着安全攻击的威胁，虽然蓝牙规范提供了一定的安全机制，但其仍存在缺陷，不能满足军事领域的安全需求，这也限制了蓝牙在军事应用领域的进一步发展。本文通过深入研究现有蓝牙安全机制，总结归纳其安全缺陷，并结合军事领域的应用需求，提出蓝牙安全增强模型和消息安全传输架构作为解决当前蓝牙通信安全隐患的选项。

关键词：蓝牙；安全传输；传输机制；安全漏洞

## Bluetooth Transmission Security Research and Reliable System Design

## Student number: 21009200659 Name: HAN Zhifeng

**Abstract:** With the continuous development of Bluetooth technology, its scope of application has expanded from traditional point-to-point file transfer, voice communication, etc. to the Internet of Things (IoT) fields such as medical monitoring, indoor positioning, smart home, etc., and has shown a high value for military applications. However, the openness of the wireless channel makes Bluetooth inherently face the threat of security attacks. Although the Bluetooth specification provides a certain security mechanism, it still has defects and cannot meet the security requirements of the military field, which also limits the further development of Bluetooth in the field of military applications. In this paper, we propose a Bluetooth security enhancement model and a secure message transmission architecture by deeply studying the existing Bluetooth security mechanisms, summarizing and generalizing its security defects, and combining with the application requirements in the military field.

**Key Words:**  Bluetooth; Secure Transmission; Transmission Mechanisms; Security Breaches

1. **引言**

在无线技术迅猛发展的今天，蓝牙以其低成本、低复杂度、高可靠性的特点，在物联网领域得到了广泛应用，并展现出了较高的军事应用价值。然而无线信道的开放性和蓝牙规范自身安全机制的缺陷使蓝牙面临众多安全威胁，这也限制了蓝牙在军事领域的进一步应用和发展。因此，研究并解决蓝牙技术存在的安全问题具有重要的现实意义。

1. **背景**

作为一种短距离的无线通信技术，蓝牙以跳频方式工作于全球通用的 2.4GHz ISM（Industrial Scientific Medical, 工业、科学、医学）频段，具有抗干扰能力强、应用成本低、实现复杂度小等优点[1]。蓝牙可以有效实现近距离内各种设备间的数据交互和资源共享，目前已作为标准的通信接口配置于智能手机、笔记本电脑等移动设备。

蓝牙 v4.0 规范[2]中首次提出的低功耗工作模式，主要面向数据传输量小且突发性强的应用场景，能够满足传感器设备的通信需求，推动了蓝牙技术在物联网领域的应用和发展。由于其良好的性质，蓝牙已被用于智能家居、医疗监护、室内定位等众多领域[3-6]，并展现出了较高的军事应用价值。例如，蓝牙网络可用于涉密装/设备的精确定位管控、官兵训练时生命体征的监测、军用车载网络及军事领域的智能医疗系统等。

随着蓝牙应用范围的扩展，其安全问题也越来越受到人们的关注。无线信道的开放性使蓝牙与生俱来地面临着窃听、篡改、重放等安全威胁，但资源有限、计算能力差的特点和低功耗的要求又限制了高复杂度密码算法的使用。虽然蓝牙规范设计了一定的安全机制，但相关研究[7-9]表明，这些安全机制仍然存在缺陷，不能满足军事、金融等高安全领域的应用需求。

针对蓝牙规范存在的安全问题，众多研究学者提出了安全增强机制[10-14]。为实现设备间的身份认证和密钥协商，现有的蓝牙安全传输方案需要将敏感的秘密参数保存于设备存储器，然而，这种存储方式不能抵抗复制攻击[15]。攻击者可以捕获开放环境中自我保护能力差的蓝牙设备，并从其存储器中提出密钥、算法参数等敏感信息。利用上述参数，攻击者既可以恢复出该设备参与的通信过程中的所有消息明文，也能够伪造合法设备的身份，传递虚假消息。因此，要将现有的蓝牙安全方案应用于高安全领域，必须在设备中增加芯片安全防护机制，以抵抗复制攻击的威胁，但该方式实现代价较高[16]，减弱了蓝牙低成本的优势。

综上所述，虽然蓝牙技术有着良好的军事应用价值，但是现有的蓝牙安全机制不能满足军事领域的安全需求。

1. **蓝牙传输安全机制现状**

蓝牙传输信息基于蓝牙协议栈，现行低功耗蓝牙BLE协议栈的具体内容如图 1 所示。

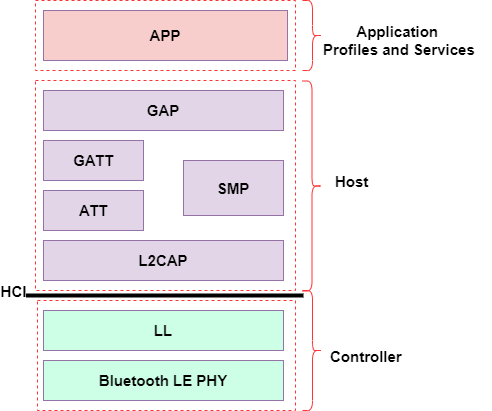


图1 现行蓝牙协议栈

1、物理层（Physical Layer，简写 PHY）：PHY层用来指定BLE所用的无线频段，调制解调方式和方法等。是1Mbps自适应跳频的GFSK射频，工作于免许可证的2.4GHz ISM（工业、科学与医疗）频段。PHY层做得好不好，直接决定整个BLE芯片的功耗，灵敏度以及selectivity等射频指标。

2、链路层（Link Layer，简写 LL）：LL层是整个BLE协议栈的核心，也是BLE协议栈的难点和重点。LL层要做的事情非常多，比如具体选择哪程度 个射频通道进行通信，怎么识别空中数据包，具体在哪个时间点把数据包发送出去，怎么保证数据的完整性，ACK如何接收，如何进行重传，以及如何对链路进行管理和控制等等。LL层只负责把数据发出去或者收回来，对数据进行怎样的解析则交给上面的GAP或者ATT。

3.主机控制接口层（Host Controller Interface，简写 HCI）：HCI是可选的，HCI主要用于2颗芯片实现BLE协议栈的场合，用来规范两者之间的通信协议和通信命令等。

4、通用访问配置文件层（Generic access profile，简写GAP）：GAP是对LL层payload（有效数据包）如何进行解析的两种方式中的一种，而且是最简单的那一种。GAP简单的对LL payload进行一些规范和定义，因此GAP能实现的功能极其有限。GAP目前主要用来进行广播，扫描和发起连接等。

5逻辑链路控制及自适应协议层（Logical Link Control and Adaptation Protocol，简写 L2CAP）：L2CAP对LL进行了一次简单封装，LL只关心传输的数据本身，L2CAP就要区分是加密通道还是普通通道，同时还要对连接间隔进行管理。

6、安全管理层（Security Manager，简写 SM）：SMP用来管理BLE连接的加密和安全的，如何保证连接的安全性，同时不影响用户的体验，这些都是SMP要考虑的工作。

7、属性协议层（Attribute protocol，简写 ATT）：简单来说，ATT层用来定义用户命令及命令操作的数据，比如读取某个数据或者写某个数据。BLE协议栈中，开发者接触最多的就是ATT。BLE引入了attribute概念，用来描述一条一条的数据。Attribute除了定义数据，同时定义该数据可以使用的ATT命令，因此这一层被称为ATT层。

8、通用属性配置文件层（Generic Attribute profile，简写 GATT）：GATT用来规范attribute中的数据内容，并运用group（分组）的概念对attribute进行分类管理。没有GATT，BLE协议栈也能跑，但互联互通就会出问题，也正是因为有了GATT和各种各样的应用profile，BLE摆脱了ZigBee等无线协议的兼容性困境，成了出货量最大的2.4G无线通信产品。

蓝牙协议栈分为主机和控制器两个部分，其中保证信息安全的主要层级为SMP层。为保证消息的安全传输，蓝牙规范分别在主机和控制器两个层面提供了安全机制，包括设备认证、链路密钥协商、数据传输加密、完整性保护等。具体而言，蓝牙规范定义了配对过程来实现设备间的认证和链路密钥建立，通过 128 位 AES 算法对信道中的数据进行加密，并利用 CRC 循环冗余校验来提供数据完整性保护。此外，新版本的蓝牙规范还引入随机地址来实现对设备隐私的保护。

1. **蓝牙传输安全漏洞现状**

由上述蓝牙机制可知，相较于早期采用 E0 加密算法的蓝牙规范，现有蓝牙规范的安全性已有较大改进，但仍存在一些漏洞，其在信息传输方面的漏洞主要包括以下三个方面：

**（1）链路密钥建立过程安全性不高**

蓝牙设备间的链路密钥由长期密钥（LTK）派生得到，对于初次建立连接的两个蓝牙设备，LTK 由一端设备产生，经短期密钥（STK）加密后传输至另一端设备。STK 的计算过程为 ,其中， 和 分别为两个蓝牙设备产生的随机数，在信道中以明文形式传输，TK 为临时密钥。因此，链路密钥的安全性由临时密钥 TK 的机密性决定。

针对不同的应用需求，蓝牙简单配对协议（Secure Simple Pair, SSP）提供了 JW、PE和 OOB 三个安全等级的关联模型，用于产生临时密钥 TK。其中，JW 模型主要用于无输入/输出（Input/Output, I/O）能力的蓝牙设备，该模型不提供任何安全保护，把 TK 值设置为 0；PE 模型在设备支持数值输入或显示时使用，将 TK 值设置为两个设备上输入或显示的数值；OOB 模型则利用带外信道传递 TK 值。虽然 PE 模型和 OOB 模型具有较高的安全性，但攻击者可通过篡改用于 I/O 能力交换的报文，从而迫使蓝牙设备选择 JW 模型进行配对。此时，攻击者可以利用从信道中获取的明文信息计算出长期密钥 LTK，进而得到链路密钥。

由此可见，蓝牙规范提供的链路密钥建立过程容易遭受中间人攻击，不能保证链路密钥的安全性。

**（2）未提供对多播消息的保护机制**

一对多的匹克网是蓝牙通信的基本拓扑，因此，在大多数应用领域，蓝牙网络由一个中心设备和多个外围设备组成。当中心设备需要向多个外围设备发送同样的消息时，利用多播通信方式可以有效减小设备的资源开销。虽然蓝牙提供了一对多的数据传输方法，但并未提供对多播数据的加密保护机制，也未提供组密钥的协商方案。蓝牙信道中一对多数据以明文形式传输，不能抵抗窃听、篡改、重放等各类安全威胁。因此，要利用多播方式传输蓝牙数据，必须设计相应的消息安全传输机制。

**（3）不能抵抗复制攻击的威胁**

完成初次连接配对的两个蓝牙设备，可通过绑定过程传递共享的密钥参数，以在下次连接中实现快速的设备认证和链路密钥建立。这些共享的密钥参数保存于蓝牙设备的非易失性存储器。然而，在蓝牙网络中外围设备通常资源受限、自我保护能力差，攻击者可以通过捕获某个外围设备，并利用如图 2 所示的复制攻击方法从其存储器中提出密钥、算法参数等敏感信息。

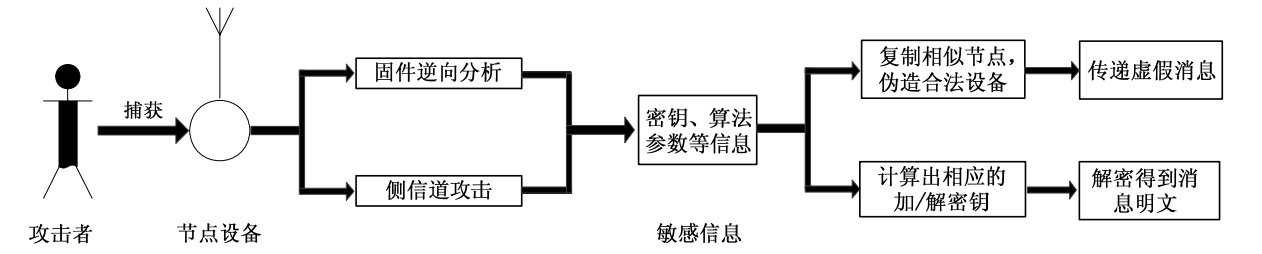


图2 复制攻击流程

利用上述参数，攻击者既可以恢复出该设备参与的通信过程的消息明文，也能够伪造合法设备的身份，传递虚假信息。因此，蓝牙规范提供的安全传输机制未考虑特定设备自我保护能力差的特点，不能有效抵抗复制攻击的威胁。

1. **蓝牙传输安全问题解决思路——可靠传输系统设计**

**5.1 安全增强模型设计**

由于蓝牙规范提供的安全机制存在缺陷，要实现蓝牙数据的安全传输，必须设计相应的安全增强方案。结合军事领域的应用需求，在现有蓝牙安全机制的基础上，设计安全增强模型，如图 3 所示。

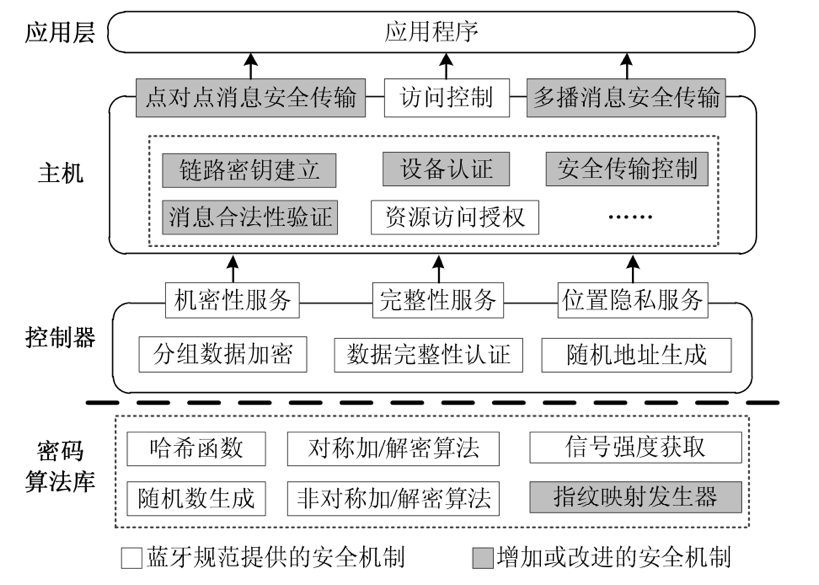


图3 蓝牙安全增强模型

蓝牙安全增强模型中各层安全实体的功能如下：

（1）密码算法库。密码算法库用于向控制器安全实体和主机安全实体提供基本的密码运算调用接口，如哈希函数、加/解密算法、随机数生成函数等。相较于原有密码算法库，安全增强模型中新增了指纹映射发生器，并为控制器和主机提供相应的内部调用接口。该指纹映射发生器以硬件形式实现，其核心模块为 PUF，用以提取蓝牙设备的“硬件指纹”，建立输入参数与输出参数之间不可克隆的映射关系，是安全传输功能实现的基础。

（2）控制器安全实体。控制器中的安全实体以硬件形式实现，具有运算速度快、安全强度高等优点，但存在实现难度大、灵活性差等缺点。因此，控制器中的安全实体主要是运算量大、安全要求高的算法，包括分组数据加密、数据完整性认证、随机地址生成等。

（3）主机安全实体。主机中的安全实体以固件代码形式实现，虽然执行效率不如硬件形式实现的安全实体，但其灵活性较高、易于设计实现且开发成本较低。因而，密钥协商、身份认证等安全方案多以固件形式实现。本文给出的安全增强模块在原有主机安全实体的基础上，改进链路密钥建立和设备认证机制，增加消息合法性验证，并改进相应的安全传输控制功能，用于向应用层提供安全性更高的点对点消息和多播消息传输服务。

**5.2 安全传输架构建立**

依据安全增强模型，对蓝牙 4.0 BLE 协议栈进行改进。本文主要在主机层的安全管理器协议（SMP）的基础上进行修改，并以固件形式实现所需安全增强方案。改进后的蓝牙协议栈如图 4 所示。

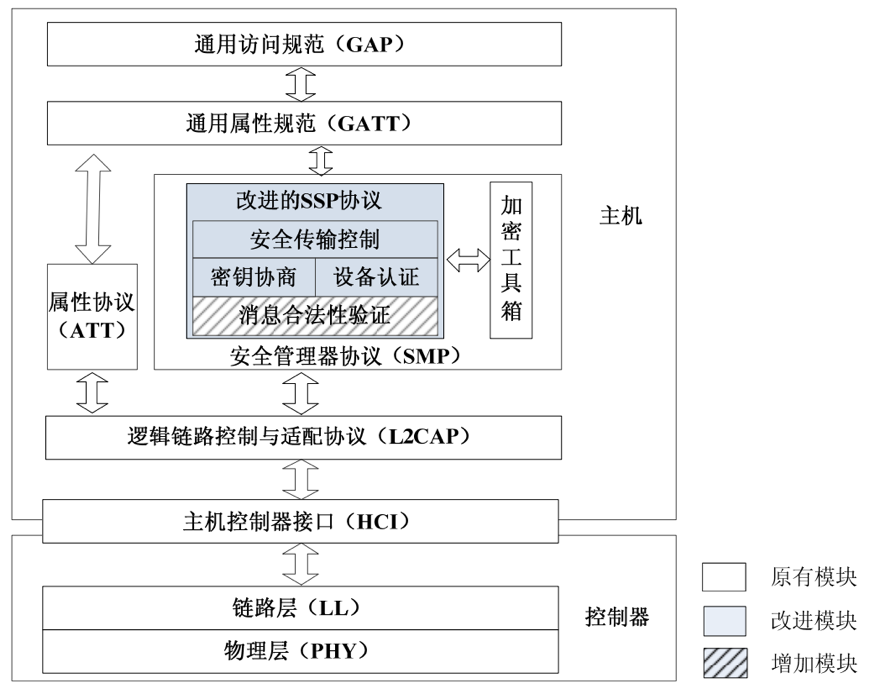


图4 改进的蓝牙协议栈

改进的蓝牙协议栈中各层的组成及功能如下：

（1）控制器。蓝牙控制器通过天线与外界连接，可以分为物理层（PHY）和链路层（LL）。其中，物理层利用调制和解调技术，实现蓝牙数据包的发送和接收；链路层定义了蓝牙设备间建立连接和传输信息的规则，以及计算校验值和加密序列的方法。

（2）主机控制器接口。主机控制器接口（HCI）用于连接主机和控制器，主要负责主机和控制器间控制信号和数据信号的传输。

（3）主机。蓝牙主机位于 HCI 之上，包括逻辑链路控制与适配协议（L2CAP）、安全管理器协议（SMP）、属性协议（ATT）、通用属性规范（GATT）和通用访问规范（GAP）。其中，L2CAP 是一个复用层，可使蓝牙复用不同的信道，并支持数据的分片和重装；SMP用于处理蓝牙连接及通信过程中与安全相关的事宜；ATT 定义了蓝牙设备访问对端设备数据的一组规则；GATT 位于 ATT 之上，定义了属性的类型及使用方法；GAP 描述了实现设备发现、连接建立、服务发现、绑定建立等过程的方法。

本文主要针对蓝牙在传输方面的安全漏洞，因而，对蓝牙协议栈的改进主要集中于主机的SMP 部分，具体包括改进其密钥协商、设备认证和安全传输控制模块，并增加对消息的合法性验证机制。

在蓝牙网络中，中心设备通常为智能手机、电脑等设备，具有较高的安全性和较强的自我保护力，而外围设备常为资源受限的信息采集节点，如传感器设备、输入/输出设备等，此类设备自我保护能力较差，易遭受复制攻击。因此，中心设备可以拥有能够保存敏感信息的安全数据库，而外围设备难以实现安全数据库，不能长期保存敏感信息。基于上述前提，依据安全增强模型，在改进的蓝牙协议栈的基础上建立消息安全传输架构，如图 5 所示。

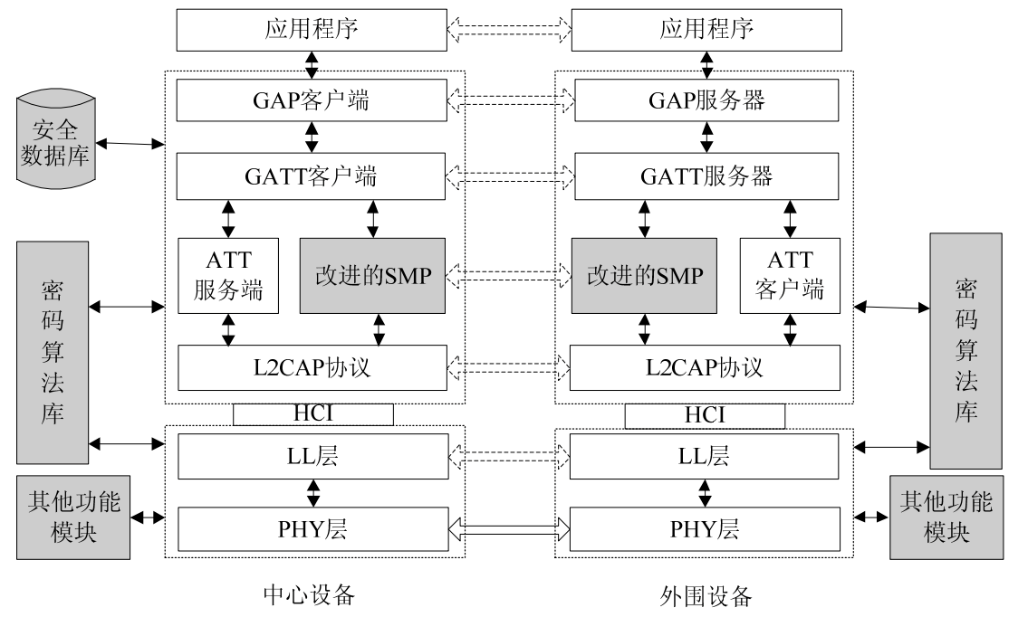


图5 安全传输架构

1. **结 论**

近年来，随着蓝牙技术的日益成熟，其实现成本逐渐变低、设备功耗逐渐减小、通信距离不断增大，蓝牙的应用领域也迅速拓展。当前，蓝牙的应用已不再局限于传统的近距离文件传输和语音通信，而是向室内定位、智能交通、医疗监护等物联网领域延伸。然而蓝牙规范提供的安全机制存在缺陷，不能满足高安全领域的需求，这也限制了蓝牙技术在其他领域的进一步发展。

本文在研究蓝牙安全机制的基础上，归纳出其存在的漏洞。针对上述安全漏洞，建立蓝牙安全增强模型，并结合蓝牙协议栈设计出消息安全传输架构，为蓝牙安全传输的实现奠定基础。

**参考文献：**

1. Bluetooth SIG, Bluetooth SIG Specification of the Bluetooth system: core package version 1.1[EB/OL]. (2000-12-01) [2018-3-20]. http://www.bluetooth.org.
2. Bluetooth SIG, Bluetooth SIG Specification of the Bluetooth System: Core Package version 4.0[EB/OL]. (2009-12-17) [2018-3-20]. http://www.bluetooth.org.
3. Mokhtari G, Zhang Q, Nourbakhsh G, et al. BLUESOUND: A New Resident Identification Sensor—Using Ultrasound Array and BLE Technology for Smart Home Platform[J]. IEEE Sensors Journal, 2017, 17(5):1503-1512.
4. Singh M, Jain N. Performance and Evaluation of Smartphone Based Wireless Blood Pressure Monitoring System Using Bluetooth[J]. IEEE Sensors Journal, 2016, 16(23):8322-8328.
5. Díaz J J V, González A B R, Wilby M R. Bluetooth Traffic Monitoring Systems for Travel Time Estimation on Freeways[J]. IEEE Transactions on Intelligent Transportation Systems, 2016, 17(1):123-132.
6. Yuan Z, Yang J, You L, et al. Smartphone-Based Indoor Localization with Bluetooth Low Energy Beacons[J]. Sensors, 2016, 16(5):596.
7. Phan C W, Mingard P. Analyzing the Secure Simple Pairing in Bluetooth v4.0[J]. Wireless Personal Communications, 2012, 64(4):1-19.
8. Barnickel J, Wang J, Meyer U. Implementing an Attack on Bluetooth 2.1+ Secure Simple Pairing in Passkey Entry Mode [J].IEEE. 2012:17-24.
9. Haataja K, Toivanen P. Two practical man-in-the-middle attacks on Bluetooth secure simple pairing and countermeasures [J]. IEEE Transactions on Wireless Communications, 2010, 9(1):384-392.
10. 黄艺波, 黄一才, 郁滨. 基于哈希链的 BLE 密钥协商方案设计[J]. 系统仿真学报, 2016, 28(6):1412-1418.
11. Perrey H, Ugus O, Westhoff D. WiSec' 2011 Poster: Security Enhancement for Bluetooth Low Energy with Merkle's Puzzle[J]. Acm Sigmobile Mobile Computing & Communications Review, 2011, 15(3):45-46.
12. Premnath S N, Gowda P L, Kasera S K, et al. Secret key extraction using Bluetooth wireless signal strength measurements[J]. 2014:293-301.
13. Diallo A S, Al-Khateeb W F M, Olanrewaju R F, et al. A Secure Authentication Scheme for Bluetooth Connection[C]. International Conference on Computer and Communication Engineering. IEEE, 2015:60-63.
14. Xu G L, Yu B. Security enhanced design of the Bluetooth simple pairing protocol. [C] Computer Science and Network Technology (ICCSNT), 2011 International Conference on. IEEE, 2011: 292-296.
15. Parno B, Perrig A, Gligor V D. Distributed detection of node replication attacks in sensor networks[A]. In: Proceedings of IEEE Symposium on Secudty and Privacy[C]. Oakland, California, USA, 2005: 49-63.
16. Marchand C, Bossuet L, Mureddu U, et al. Implementation and characterization of a physical unclonable function for IoT: a case study with the TERO-PUF[J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2017.