物联网无线协议安全综述

张伟康 [1,2], 曾凡平 [1,2], 陶禹帆 [1,2], 李向阳 [1,2]

[1] 中国科学技术大学 计算机科学与技术学院 合肥 中国 230027

[2] 中国科学院 无线光电通信重点实验室 合肥 中国 230027

摘要 近些年来, 随着物联网的快速发展, 其应用场景涵盖智慧家庭、智慧城市、智慧医疗、智慧工业以及智慧农业。相比于传统的以太网, 物联网能够将各种传感设备与网络结合起来, 实现人、电脑和物体的互联互通。形式多样的物联网协议是实现物联网设备互联互通的关键, 物联网协议拥有不同的协议栈, 这使得物联网协议往往能表现出不同的特性。目前应用较广的物联网协议有 ZigBee、BLE、Wi-Fi、LoRa、RFID 等, 这些协议能根据自身特性的不同应用在不同领域, 比如说 LoRa 被广泛应用于低功耗广域网、RFID 被用于设备识别。然而, 由于物联网端设备只拥有受限的计算和存储资源, 无法在其上实施完备的安全算法, 许多物联网协议会在功耗和安全性之间进行取舍, 使得物联网协议的安全性得不到保障。物联网协议的安全性直接关系到物联网系统的安全性, 所以有必要对物联网协议的安全性进行分析。

本文阐述常见的几种物联网协议所具备的安全能力, 包括物联网协议在保护机密性、完整性以及身份认证上所制定的规则。然后从常见的无线协议攻击出发, 包括窃听攻击、重放攻击、电池耗尽以及射频干扰, 分析了这几种协议在面对这些攻击时的表现。除此之外, 我们比较了常见的几种物联网协议, 总结他们的面对攻击时的不同, 并且总结物联网协议安全的相关研究工作。最后, 我们展望并总结了物联网协议安全的发展方向, 认为结合形式化验证、轻量级加密以及区块链技术是提高物联网协议安全性的有效方法。

关键词 物联网; 无线协议; ZigBee; BLE; 攻击

中图法分类号 TP309.2 DOI 号 10.19363/J.cnki.cn10-1380/tn.2022.03.04

A Survey for Security of IoT Wireless Protocols

ZHANG Weikang[1,2], ZENG Fanping[1,2], TAO Yufan[1,2], LI Xiangyang[1,2]

[1]School of Computer Science and Technology, University of Science and Technology of China, Hefei 230027, China

[2]Key Laboratory of Wireless-Optical Communications, Chinese Academy of Sciences, Hefei 230027, China

Abstract In recent years, with the rapid development of the Internet of Things, its application scenarios have covered smart home, smart city, smart medical treatment, smart industry and smart agriculture. Compared with traditional Ethernet, the Internet of Things can combine various sensing devices with the network to realize the interconnection of people, computers and objects. Various IoT protocols are the keys to realize the interconnection of Internet of Things devices. IoT protocols occupy different protocol stacks, which make the IoT protocols show different characteristics. At present, ZigBee, BLE, Wi-Fi, LoRa, RFID and so on are widely used. These IoT protocols can be applied to different application scenarios according to their own characteristics. For example, LoRa is widely used in LPWAN and RFID is used for device recognition. However, as IoT end devices only occupy limited computing and storage resources, it is impossible to implement a complete security algorithm for them. Many IoT protocols balance their power consumption and security, so it is necessary to evaluate the security of IoT protocols.

This paper describes the security capabilities of these Internet of Things protocols, including the rules of IoT protocols implemented in protecting confidentiality, integrity and identity authentication. Then we analyze the security problems of each protocol from the common wireless protocol attacks, including eavesdropping attack, replay attack, battery depletion and RF interference. We analyze the IoT protocols' behaviors while facing these wireless attacks. Besides, we compare some common IoT protocols on security properties and reactions while facing attacks and we conclude relevant research works about IoT protocols' security. At the end of this paper, we prospect and summarize the development direction of Internet of Things protocol security, and believe that it is an effective method to improve the security of IoT protocols by combining formal verification, lightweight encryption technology and blockchain technology.

Key words the Internet of Things; wireless protocol; ZigBee; BLE; attack

通讯作者: 曾凡平, 博士, 副教授, Email: billzeng@ustc.edu.cn。

本课题得到科技部网络空间安全项目物联网与智慧城市安全保障关键技术研究 (No.2018YFB080340) 资助。

收稿日期: 2021-10-20; 修改日期: 2021-12-24; 定稿日期: 2022-06-24

1 引言

物联网是指由相互关联的计算设备、数字机器、物体、动物或者人组成的网络, 在物联网环境下, 围绕我们身边的许多事物可以被连接到互联网上。在近些年的发展下, 物联网与特定需求相结合, 诞生出了智能制造、智能电网、智能家居、智能工业等应用场景, 物联网的自动化为个人、企业带来了生产生活上的便利。根据《物联网白皮书》(2018 年)[1], 全球的物联网产业规模从 2008 年的 500 亿美元已经增长到了 2018 年近 1510 亿美元。在 2019 年, 大规模物联网连接的数量增加了 3 倍, 达到近 1 亿[2], 物联网在快速发展的同时, 也暴露出了许多安全隐患。

由于物联网端设备可使用的能量少, 同时还要维持设备长期运转, 这就使得物联网设备不能实施完整的安全算法, 让攻击者有机可乘。针对物联网的攻击可以泄露个人数据的隐私, 影响工业控制的正常运行。在 2019 年的黑客大会上, 研究人员公布了在波音 787 关键组件[3]上的众多漏洞, 攻击者能够利用这些漏洞对飞机系统造成损害, 威胁人员的生命安全。

无线协议是物联网的关键, 它能够将不同类型的设备连接到互联网。针对物联网使用场景的不同, 诞生了众多物联网无线协议。有针对近距离通信的 RFID、低功耗蓝牙, 也有中距离通信的 ZigBee、Z-Wave、Wi-Fi 技术, 远距离的 LoRa、NB-IoT 技术。正是这些协议的存在才使得物联网设备能够应用于多种环境。它们使用的协议栈大不相同, 在应对攻击的能力上也表现出了不同的安全等级。例如, 攻击者可以在近场环境下仅通过阅读器就能够得到一个无源标签的内容, 但是攻击者却很难有手段能够直接破译出最新的 WiFi 密码。

目前已经有了一些关于物联网无线协议方面的研究。Jayasree 等人[4]对物联网与工业物联网环境分析其存在的安全隐患, 分别阐述了针对物联网环境的物理、网络、软件以及数据的攻击手段, 然而不足的是, 研究内容中并未包含对物联网具体协议的分析。本文弥补了这一不足, 从物联网常见的协议入手讲述协议面临的攻击。Katharina 等人[5]从形式化验证的角度入手, 总结了近些年针对物联网协议的形式化验证手段和验证结果, 其中分析的协议包括了 ZigBee、Z-Wave、Bluetooth 等绝大多数物联网协议。与之相比, 本文的协议分析基于成功执行的攻击手段, 可以说, Katharina 等人利用形式化验证技术, 提供了在设计上对物联网协议的安全分析, 而本篇综述的工作是在真实的物联网环境中阐述各个协议的安全表现。

本文的结构如下: 第二节分析协议具备的安全策略, 以及保证了哪些安全属性。虽然物联网协议在安全策略上作了相关的保护, 但是仍然面临着一些可能遭受的攻击。第三节列举物联网协议最容易遭受的攻击形式, 并阐述各个物联网协议抵抗特定攻击的能力。第四节针对物联网协议仍然存在的安全问题, 提出一些行之有效的优化建议。第五节对本文作出总结, 阐述本文的研究意义。

2 协议安全策略

物联网设备具有受限的计算资源, 物联网协议需要在更低的功耗上运行。然而物联网设备关乎企业和家庭的安全, 并且设备本身易被攻击者所接触, 所以物联网协议的设计需要在低功耗的基础上确保数据的安全性, 保证实体间的安全通信。

本节将物联网无线协议所需要具备的安全要素分为了安全的配对过程、数据机密性和完整性保护、协议的反重放攻击能力以及抗信号干扰能力。安全的配对过程确保了密钥的安全传输, 需要能够保证密钥的隐私性; 数据机密性大多采用密钥加密进行保证, 而有些物联网协议的密钥算法是过时的, 容易被攻击者所破解; 数据完整性除了能够保证数据传输不失真之外, 还需要能够保证数据不被攻击者所篡改。本节从这些方面分析了几种典型物联网协议的安全性表现, 这些物联网协议中包括了中短距离的 ZigBee、BLE、Wi-Fi, 他们在智能家居等场景中广泛使用, 也包含了长距离的 LoRa 协议, 主要用于智慧城市、智慧农业等场景, 他们的无线属性比对如表 1 所示。

表 1 物联网无线协议对比

Table 1 Comparison of IoT communication protocols

协议	信号范围	传输速率	频带	标准	发布时间
ZigBee	<100m	250kps	2.4GHz	ZigBee	2003
BLE	<100m	1Mbps	2.4GHz	IEEE 802.15.4	2011
Wi-Fi	100m~200m	600Mbps	2.4GHz/5GHz	IEEE 802.15.1	1998
LoRa	>10km	<50kps	900MHz	IEEE 802.11	2015

2.1 ZigBee

ZigBee 通常用于需要较长电池寿命的低数据速率应用, 在智能家居中应用广泛。ZigBee 标准是建立在 IEEE 802.15.4 标准之上的。IEEE 802.15.4 标准已经定义好了物理层和 MAC 层, ZigBee 在此基础上添加了更多的层次, ZigBee 标准的结构层次如图 1 所示。

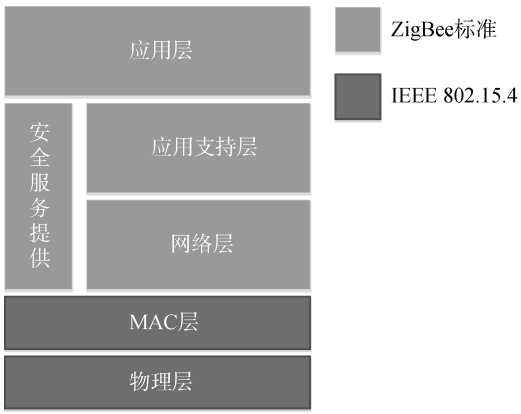

图 1 ZigBee 协议栈
Figure 1 Protocol stack of ZigBee

ZigBee 协议栈的安全服务主要由应用支持层以及网络层提供, 提供了访问控制、数据完整性、数据机密性、反重放攻击的安全服务, 下面依次进行阐述。

(1) 访问控制: IEEE 802.15.4 MAC 层通过维护一个访问控制列表(Access Control list, ACL), 对于每个接收到的消息, 接收节点会检查源地址是否存在于 ACL 表中, 如果不满足, 则消息将被丢弃。

(2) 数据完整性与数据机密性: ZigBee 标准使用了 AES-CCM*作安全保护, 这是高级加密标准的一个小变种, 伴随着被修改过的 CCM 模式(Counter with CBC-MAC)[6], 这种保护方式不仅能够以提供加密的方式保护数据的机密性, 也能够使用消息校验码保护数据的完整性。消息发送者在发送前对消息进行加密, 保证只有目标实体能够读懂它, 发送者在消息发出之前在末尾加上消息校验码, 一方面防止了数据在传送过程中失真, 另一方面给攻击者篡改数据增加了难度。一旦数据与校验码不匹配, 接受者便会丢弃此数据包。ZigBee 提供了八种加密安全等级, 如表 2 所示。比如说在安全等级 5, 通信使用的是 AES 的加密算法以及利用 4 个字节的校验码进行完整性验证[7]。

(3) 反重放攻击: 对于抗重放攻击来说, 每个处于 ZigBee 网络下的节点在发送的数据包中都包含了一个 32 位的帧计数值[8]。随着每次传送而增加, 每个节点都会记录之前已经使用过的计数值。如果节点收到了一个数据包, 而这个数据包中的计数值比之前记录的所有计数值还要小或者相等, 这个包将会被该节点丢弃, 这种机制给予了节点抵抗重放攻击的能力。帧计数值的最大值会达到 0xFFFFFFFF, 但是当计数值达到最大值后, 网络规定此节点不能再作消息传送, 只有在网络密钥更新时重置。

表 2 ZigBee 安全等级
Table 2 Security levels of ZigBee

安全等级	安全属性	加密	校验码
0x00	None	无	无
0x01	MIC-32	无	有(4 字节)
0x02	MIC-64	无	有(8 字节)
0x03	MIC-128	无	有(16 字节)
0x04	AES	有	无
0x05	AES-MIC-32	有	有(4 字节)
0x06	AES-MIC-64	有	有(8 字节)
0x07	AES-MIC-128	有	有(16 字节)

此外, ZigBee 允许生产商通过无线通讯的方式增加系统的特点、修补产品的安全缺陷并应用安全补丁。然而, 空中更新虽然在一定程度上给厂家对于固件安全性的升级作了贡献, 但是如果保护不足的话也会暴露大量的安全威胁。ZigBee 对此的举措包括: 提供了一个唯一密钥用于加密传输的镜像, 提供了为镜像签名的方法, 镜像在生产时就被加密只有指定产品包含解密密钥[7]; 在空中升级中, 当设备接收到加密镜像之后, 他的引导程序会解密该镜像, 认证签名之后升级设备。

2.2 BLE 低功耗蓝牙

低功耗蓝牙是一种超低功耗的无线协议, 普遍应用在手表、游戏机、医疗传感器等场景。低功耗蓝牙的协议栈如图 2 所示。

图 2 蓝牙低功耗协议栈
Figure 2 Protocol stack of bluetooth low energy

蓝牙低功耗的协议栈中, 物理层用来指定 BLE 所使用的无线频段和调制解调方法; 链路层是蓝牙低能耗协议栈的核心, 负责选择使用哪个射频信道进行通信, 如何识别数据包, 保证数据的完整性以及对链路的管理和控制等; L2CAP 层负责数据的分割和重组以及信道的复用; ATT 层用来定义用户命令及命令操作的数据; 安全管理层用来管理 BLE 连接的加密和验证安全; GATT 层用来规范数据内容, 并对属性进行分类管理; GAP 层主要负责广播、扫描和发起连接。

蓝牙低功耗的安全属性可以归结为数据机密性、数据完整性、自适应跳频。

(1) 数据机密性和完整性: 蓝牙的配对一共有 4 种模式, 分别是直接工作、数字比对、键入密码以及带外配对。“直接工作”模式是发生在配对的至少一方既没有输入密码的能力, 也没有展示密码的能力。“数字比对”是通信双方都键入 6 位密码, 如果比对成功则配对。“键入密码”模式要求通信一方键入 6 位密码。“带外配对”是在频带不同时进行的配对模式。除了配对模式之外, BLE 也定义了 4 种配对安全等级。低功耗安全配对(LE Secure Connections Pairing)是最安全的一种, 它在蓝牙标准 4.2 被提出, 使用 P-256 密钥以及笛福赫尔曼密钥交换(Diffie–Hellman key exchange), 生成一个 128 位的长期密钥。第二种安全等级是基于认证的防中间人攻击保护, 使用了键入密钥模式或者带外配对模式来实现, 提供了对于通信方的认证。无认证无中间人保护的安全, 是“不工作”模式下的安全等级, 密钥由设备自动生成。在“无安全”等级, 这种模式下消息是非加密的, 一般用于传送非敏感信息, 比如厂家名称。

(2) 自适应跳频技术: BLE 还使用了自适应跳频技术[9]。在每次数据传输完成之后 BLE 会对信道质量进行评估。如果认为当前信道质量较差, 就将它从信道列表中剔除。这不仅使得 BLE 在 2.4GHz 频段拥挤的无线通信协议中拥有了更多抗干扰的能力, 而且信道的变换使得攻击者需要随时确定信道的跳变, 给监听加大了难度。

2.3 Wi-Fi

Wi-Fi 自创立以来更换过多次安全算法, 从最开始的 WEP 到现在的 WPA3, 安全性已经得到了很大程度的保障。WEP(Wired Equivalent Privacy)发布于 IEEE 802.11a 标准, 跟他的名字描述的动机一样, WEP 的初旨在于提供与有线网络一样的安全性, 结果却是出现了许多安全漏洞, 并在 2004 年被 WiFi 联盟官方放弃。WEP 的安全性不足主要表现在以下几点:

(1) WEP 中只对客户机进行认证而不针对接入点(Access Point, AP), 这可能会导致用户接入恶意 AP 而丢失隐私数据。

(2) WEP 通信中使用的密钥存储在设备中。如果设备被偷窃的话, 攻击者提取网络密钥则能对网络流量进行解密。

(3) 同一个密钥被用在认证和加密, 这在现在看是很不安全的。

(4) WEP 密钥只有 40 比特长[10], 可能会使攻击者的暴力破解获得成功。

相比于 WEP, WPA(Wi-Fi Protected Access)技术主要在 3 个方面作了安全性的增强, 分别是对数据机密性、用户认证以及数据完整性的增强。

(1) 在数据的机密性方面: WPA 使用 TKIP (Temporal Key Integrity Protocol)保证更强的加密, 为了了对已有硬件保持兼容, TKIP 也使用 RC4 流密钥。TKIP 是一种密钥管理协议, 相比于 WEP 的 40 位密钥, 它使用了 128 位的临时密钥, 取代了 WEP 的单一静态密钥, 并且变化每个数据包使用的密钥; TKIP 也使用了一个 48 位的初始化变量(Initialization Vector, IV), 明确了将 IV 用做计数器进行递增。所以说, 临时密钥一直在改变并且 IV 也一直是变化的, 所以通信端生成的是不同的 RC4 流密钥。

(2) 在认证方面: WPA 使用 802.1X EAP(Extensible Authentication Protocol)实现双向认证, 而 WEP 的认证措施是基于使用硬件的 MAC 地址, 这个信息很容易被攻击者偷取。EAP 建立在一个更安全的公钥加密系统上, 以确保只有授权的网络用户才能访问网络。

(3) 在数据完整性方面: WPA 使用 MIC 取代 CRC 校验码; WPA 改进了对于消息完整性的校验, 使用了更安全的信息完整性编码(Message Integrity Check, MIC) [11]。该算法对于对抗攻击者恶意篡改数据有着不错的抵抗性, 而不仅仅是 CRC 校验码只保证了数据的传输不出错。

WPA2 使用了 AES-CCMP(AES-Counter Mode CBC-MAC Protocol)进行加密。AES 是目前很流行的对称加密算法, 相比于 RC4 算法, AES 的安全性更能够得到保证。AES-CCMP 结合了两种复杂的加密技术(counter mode 和 CBC-MAC), AES 自身已经是一种很健壮的算法, counter 模式下使用了一个计数器, 对于每一块要加密的信息, 这个随机数都会发生变化, 这就使得加密密钥不断发生变化, 给攻击增加了难度。CBC-MAC 是一种信息完整度算法, 可以确保消

息在传输过程中没有被修改。

相比于 WPA2, WPA3 主要在以下几点作了改进。对于个人和家庭网络, WPA3 通过使用对等实体同时验证(Simultaneous Authentication of Equals, SAE)取代了 WPA2 的预共享密钥模式。在 WPA2 中, 许多用户往往会设置一个安全性不高的弱密码, 这使得暴力破解对于攻击 WPA2 十分有效。通过 SAE 握手阶段协商一个新的配对主密钥(Pairing Master Key, PMK), 这个 PMK 用于 4 次握手阶段生成新的临时密钥组。即使用户的密码达不到复杂程度, 即便攻击者知晓了用户的弱密码, 他也不能使用这个密码去提取加密通信的密钥。除此之外, WPA3 通过使用随机无线加密(Opportunistic Wireless Encryption, OWE), 当客户机与 AP 相连时, OWE 执行无需身份认证的 Diffie Hellman 密钥交换, 生成只有客户机和 AP 才知道的密钥, 用于加密客户机和 AP 交换的所有数据。另外, WPA3 通过使用受保护的管理帧(Protected Management Frames, PMF)机制, 可以有效地防止攻击者的窃听和伪造消息, 为信息的机密性提供了更可靠的保护[12]。

2.4 LoRa

LoRa 是一种低功耗的长距离网络协议, LoRa 的协议栈包括了 LoRa 物理层、LoRaWAN 链路层协议以及应用层。物理层使用了 CSS 扩频调制技术, 使通信距离更远, 消耗能耗更低; LoRaWAN 主要负责网络的拓扑以及安全的通信等。其中 LoRaWAN 提供的安全策略需要分为两种模式下的安全, 此外 LoRaWAN 提供了对于数据机密性和完整性的保护, 以及反重放攻击的策略。

(1) LoRaWAN 的两种入网模式: LoRaWAN 提供了空中入网和个性化激活两种模式让设备加入 LoRa 网络(这个步骤也被称为设备的激活过程)。加入网络的最终结果是让设备产生三组密钥, 这三组密钥分别是上行/下行数据网络完整性密钥(*FNwkSIntKey*、*NwkSIntKey*)、网络加密秘钥(*NwkSEncKey*)、应用加密秘钥(*AppSKey*)。其中上行/下行数据完整性密钥用于上行链路和下行链路的 MIC 校验码, 网络加密密钥以及应用加密密钥分别用于网络层和应用层的数据加密。在个性化激活模式中, 这三组密钥都在生产时已经被烧录进设备; 而在空中入网模式中, 设备的初始化密钥只有网络初始密钥(*NwkKey*)和应用初始密钥(*AppKey*), 并在与网络服务器的通信中获得参数从而提取这三组密钥。相比之下空中入网的配对模式安全性更高[13]。

(2) 数据的机密性和完整性: LoRa 对数据的传送保证了机密性和完整性, 并且在网络服务器和终端设备之间进行双向认证。LoRaWAN 使用了 128 位的 AES 对称加密算法, 并采用了 CCM* CMAC ECB 加密模式。Counter with CBC-MAC(CCM)模式遵循先认证后加密的策略, 同时提供了对于数据机密性的保护和身份认证, CCM*在 CCM 基础上作了一点小变化, 允许了仅加密以及仅确保完整性的用途。而 LoRaWAN 使用的是 CCM*模式下的仅加密策略对 MAC 帧命令以及应用数据进行加密。LoRaWAN 使用 CMAC(Cipher-based Message Authentication Code)作认证, 形成了先加密后认证的策略。此外, LoRaWAN 应用了 ECB 模式, 将整段明文分为了若干个相同长度的小段, 并对每个小段进行加密, 这更增加了攻击者读懂消息内容的难度。

(3) 反重放攻击: LoRaWAN 在交换信息的数据包中使用了计数器和随机数, 这么做的好处在于有效地防止了重放攻击, 配对过程中的随机数在使用后被主机所记住, 保证不会再被使用。正常消息中的计数器自配对之后依次增长, 如果服务器收到了比当前计数器小的数据包, 则丢弃此数据包[14]。

在介绍了上述的物联网协议之后, 我们对所述的几种物联网协议作横向对比, 整理如表 3 所示。在设备认证方面, 各协议所采用的策略有较大差别。ZigBee 所使用的是基于网络信任中心的认证; 也有许多协议如 BLE 会根据用户的需求改变认证方式, 这其中有安全性较低的直接工作模式, 不通过双方的认证直接配对; Wi-Fi 的几个版本的安全策略也表

表 3 物联网协议安全属性对比

Table 3 Comparison of security properties in IoT communication protocol

安全属性	ZigBee	BLE	Wi-Fi			LoRa
			WEP	WPA	WPA2	
认证	信任中心认证	四种认证方式	基于 IEEE 802.11	EAP 认证	两种认证方式	空中入网/个性化激活
机密性	AES*	根据认证方式, 密钥长度也不同	RC4	TKIP	AES-CCMP	AES
完整性	MIC*	CRC	CRC-32	Micheal[15]	CBC-MAC	CMAC

现出不一样的认证模式, WPA2 支持根据模式决定安全性; LoRa 也同样根据入网的不同采取不同的认证算法。在机密性方面, 许多物联网协议采用了基于 AES 的加密, 这部分的协议有 ZigBee、WPA2、LoRa 等, 而 WEP 所使用的的 RC4 密钥已逐渐被主流协议所抛弃。在保护完整性上, 相对较早的协议如 WEP 采用的是 CRC 消息校验码。与此类似的协议还有 BLE, 但是 CRC 校验码是基于消息的线性验证码, 攻击者有恢复校验码的可能。WPA 使用 64 位的 Micheal 校验码既能够保证消息内容不出错, 也能防止恶意的修改。

3 物联网通信协议遭受的攻击

物联网协议与其他无线协议一样, 同样遭受着无线环境中的潜在威胁, 面临着诸如窃听、中间人攻击、重放攻击等风险。除此之外, 由于物联网协议自身的特性, 攻击者也会对协议的密钥试图破解, 对协议发起 DoS 攻击达到减短设备寿命的目的等。本节以窃听、重放攻击、密钥破解、电池耗尽、射频干扰为例, 分别阐述各协议面对这些攻击的表现。

3.1 窃听

网络窃听是指攻击者通过自己的设备抓取网络中传输的数据包, 进而读出数据包的内容。无线通信的广播特性使其数据极易受到窃听攻击, 任何处于通信环境内的同种协议设备都能够捕捉到数据包, 但如果数据已经作了加密处理, 攻击者也很难对数据包进行解密, 更别说读懂它。下面阐述几种典型物联网协议应对窃听的能力, 以及攻击者针对已经具备加密特性的协议, 是如何实施窃听攻击的[5]。

如 2.1 中表 1 所示 ZigBee 网络定义了 8 种安全方案, 这其中包括了许多只校验数据包而不对数据包进行加密处理的方案, 因此许多 ZigBee 网络是不对数据包采用加密的。攻击者可以使用硬件工具对网络进行嗅探。相关人员开发了一款针对 ZigBee 侦测的渗透测试软件 KillerBee[16], 它能够针对 ZigBee 网络进行窃听、监听密钥、重放等攻击, 其中的 zbdump 工具可以捕获 ZigBee 数据包并存入文件。

BLE 低功耗蓝牙采用了自适应跳频算法有效地降低了被持续窃听的风险。自适应跳频的初始目的是为了使实体通信能够避开通信质量较差的信道。在每次数据传输之后, 都对信道质量进行评估, 如果 BLE 认为当前信道质量较差, 就将它从列表中删除。由于攻击者在窃听流量时需要具体到有流量传输的信道, BLE 的不停切换信道给攻击者的窃听增加了难度。但自动跳频的算法并不是无迹可寻, 有攻击者指出通过持续监听所有信道的流量, 两个相继出现的数据包就确定了跳频的时间间隔、每一跳会经过多少信道, 在确定了这两个值之后, 攻击者就可以有规律的更改窃听程序, 指向性的窃听 BLE 流量包[14]。之后攻击者再结合 3.4 所述的破解 BLE 临时密钥的方法, 就拥有了读懂数据包的能力。

RFID 标签的无源标签对抗窃听的能力较弱。许多无源标签是不进行加密的, 在合法阅读器向标签发送读请求之后, 标签以 RFID 数据包返回消息, 这个消息能够被所有在标签通信范围内的阅读器捕捉[17]。除此之外, 攻击者可以按照窃听到的信号进行伪造。Jonathan 实现了一个具有对 RFID 信号的录制功能的设备, 它能够读取 RFID 标签的内容, 并模拟窃听到的信号进入内部系统[18]。

Wi-Fi 的 WEP 与 LoRaWAN 都对信道传输的数据包进行了加密, 普通的窃听并不能读懂加密数据包的内容, 攻击者将视线转移到密钥生成过程。WEP 以初始化向量 $\boldsymbol{v}$ 以及共享密钥 k 作为材料对数据进行加密, 其中密文 C 与明文 P 的转换公式形如:

$$C=P\oplus \mathrm{RC4}(c,k)$$

其中 RC4 是一种流密钥算法。WEP 存在着初始化向量 $\boldsymbol{v}$ 以及共享密钥 k 重复使用的情况。这样一来, 如果攻击者获得了两个密文 C_1 与 C_2, 将 C_1 再与 C_2 异或, 得到:

$$\begin{aligned} &C_1\oplus C_2\\ =&(P_1\oplus \mathrm{RC4}(\boldsymbol{v},k))\\ &\oplus (P_2\oplus \mathrm{RC4}(\boldsymbol{v},k))\\ =&P_1\oplus P_2 \end{aligned}$$

这样一来就能够消除密钥组的加密作用[19]。LoRaWAN 使用了与 WEP 同样的流密钥, 同样面临着被攻击者越过加密, 解密数据包的风险[20]。

3.2 重放攻击

由于大多数协议都有保证数据机密性的设计, 通信过程使用了加密算法。这使得普通的窃听攻击对系统无效, 但是如果攻击者在捕获到数据包后, 目的不是为了读懂数据, 而是向端设备重复发送此数据包, 由于该数据包的校验码是正确的, 设备对数据包进行解密处理。这样一来, 一旦接收的数据包多了, 就会耗尽设备的处理能力, 对设备造成 DoS 攻击或者欺骗攻击[21]。

ZigBee 的协议栈基于 IEEE 802.15.4 体系。在 IEEE 802.15.4 结构下, 发送者通过在数据包中加入帧计数值为系统提供抵御重放攻击的能力, 其中帧计数值通过通信双方交换的随机数而生成, 而这些

随机数在网络中是以明文形式传输的。试想如果攻击者在窃听阶段知晓了当前的帧计数值, 并使用一个比当前计数值大的值构造数据包, 并不断将此包发送给端设备, 依据标准, 接收节点会比较当前数据包的帧计数值以及记录表中的最大计数值, 如果当前数据包的帧计数值比最大值还要大, 那他会接受该数据包以作处理。虽然攻击者构造的数据包可能不会通过完整性校验, 但事实上接收节点已经花费了大量的时间用于接收和处理了该数据包, 因此使用了这种方法伪造数据包消耗接收节点的电源能量, 影响正常节点的运行[22]。KillerBee 同样提供了针对 ZigBee 网络进行重放攻击的工具, zbreplay 可以在 ZigBee 网络不使用帧计数的情况下对设备进行有效的重放攻击[16]。

在 LoRaWAN v1.0.2, LoRa 消息中使用了帧计数值以防止重放攻击。在设备正常运行时, 攻击者窃听到设备与网关之间通信的数据包并以此进行重放, 网关比对自己所记录的最大的计数值。如果该数据包的帧计数值小于这个最大值, 则会被直接丢弃, 不会对网关造成重放的影响。然而, 攻击者发现在设备进行重置或者帧计数值溢出之后, 终端设备会将计数值重置为 0。在这种情况下, 如果攻击者在重置之前窃听到数据包, 并在重置之后进行重放, 这时的系统帧计数值很小, 则会接受此重放数据包, 这样就可以对系统造成 DoS 攻击[23]。

Wi-Fi 的 WPA2 安全协议自从 2004 发布以来, 由于其采用了 128 位 AES 加密算法以及使用 EAP-based 进行密钥管理。然而在 2017 年 Mathy 等人针对 WPA2 的握手阶段进行重放攻击, 使 WPA2 重置用来生成密钥的相关材料, 通过这种方式将会使 WPA2 重复使用密钥组, 此时的安全等级与 WEP 协议无异[24]。在研究人员发现了 WPA2 的致命漏洞后, Wi-Fi 联盟在 2018 年便重新发布了 WPA3 安全协议[25]。

同样地, RFID 系统也面临着重放攻击的威胁。假设 A 是个合法阅读器, B 是个合法标签, A'与 B'都是非法设备, 将 A'与 B'移动到 A 与 B 周围, 在窃听到 A 与 B 的正常通信后将数据包重放, 这样一来非法设备 B'可以将 B 设备关闭, 而自己作为合法设备而参与通信[26]。

3.3 暴力破解

绝大多数物联网协议都会采用加密保护数据的机密性, 防止攻击者能够轻松地窃听和读懂消息, 而设备会在固件中存储密钥的相关信息, 攻击者在获得与生成密钥的相关信息后有重新生成密钥的可能。

ZigBee 具有标准和高安全两种安全等级, 在使用标准化安全等级时, 当网络密钥并不是以预安装的方式获得, 信任中心会以非加密的形式向设备发送当前 ZigBee 网络正在使用的网络密钥, 攻击者反复让设备重新入网, 并在这个过程中实行窃听, 在窃听到网络密钥之后, 攻击者就具有了解密数据包的能力[27]。

在 BLE 交换密钥的过程中也存在着威胁。在 BLE legacy 模式下, 主从设备在配对的第二阶段会生成并共享临时密钥 *TK*, 并使用该 *TK* 生成以后加密通信的短期密钥 *STK*。然而 *TK* 依赖于通信模式: 如果是继续工作模式, 则 *TK* 就是 0; 如果是键入密钥模式, *TK* 将是一个 6 位数字, 也就是一个 0~999999 之间的值。这两种模式密钥的位数都不够多, 攻击者可以使用暴力破解尝试 *TK*, 在得到了 *TK* 之后, 其他用于计算 *STK* 的值都在网络上以明文传输, 结合 *TK* 和这些值, 攻击者可以计算出 *STK*, 以后就可以用 *STK* 解密通信数据包, 获取敏感信息[28-29]。

在 LoRaWAN v1.0.2 版本中, 设备在使用 OTAA(空中激活)模式入网时, 使用了随机数以参与到密钥组的生成, 但是终端设备并不记录所使用过的随机数, 这就给了随机数有了重复使用的可能, 再加上攻击者可以从 LoRa 设备中直接获取到配对所要使用的预密钥(*AppKey*、*NwkKey*), 重复使用随机数会被攻击者利用来重新生成密钥组[30-31]。除此之外, Emekcan 等人提出了当攻击者能够在物理层面上接触到设备时, 由于 LoRa 终端设备包含了无线电模块和主机微控制器单元, 无线电通过 UART 或 SPI 接口与主机微控制器通信, 主机和无线电模块之间的命令和数据交换可以使用外部硬件拦截。例如如果两个设备都使用的 UART 接口, 则可以使用基本的 FTDI 接口来窃听所有的密钥交换, 攻击者通过这种方式获取加密通信的密钥[25]。

在 Wi-Fi 使用 WEP 作为安全策略时, WEP 会使用 CRC 校验码并将此校验码加入到包末尾提供消息完整性检查。攻击者对此提出了 ChopChop 攻击: 首先通过窃听捕捉到一个 WEP 数据帧, 并去掉密文的后 8 位, 再对这 8 位数据进行暴力枚举, 将修改后的包发送给接入点。如果接入点选择保留, 则证明了攻击者对这 8 位的猜测是正确的, 如此最终能够得到明文[32]。WEP 的改版 WPA 针对这类攻击设置了两重保护, 即接收到的包如果 CRC 校验码通过而 MIC 校验失败, 接入点会收到一个提醒消息校验码出错的包, 如果 60 s 内两个包的校验码都不通过, 通信将

会被暂停 60 s 时间; 第二个办法是使用计数值, 如果收到了比现有计数值小的数据包, 则该包会被丢弃。攻击者开发出进阶版的 ChopChop 攻击, 攻击者会扮演成接入点对客户机发送数据, 他将合法的数据包的部分内容进行修改, 当猜对了这部分内容时, 攻击者会收到一个提醒 MIC 校验失败的包, 这个时候攻击者等待一分钟并继续进行对数据包的猜测[33]。

虽然 WPA2 在 Wi-Fi 历史上持续了 13 年时间, 但它也遭受着暴力破解的攻击。Aircrack-ng 工具可以根据字典库高效地重复尝试 Wi-Fi 密码, Alberto 等人使用 Aircrack-ng[33]工具对 WPA2-PSK 模式进行暴力破解达到了获取 WPA2 预共享密钥的目的[34]。除此之外, Aircrack-ng 还可以对 Wi-Fi 设备进行数据包注入、重放攻击、取消身份认证、伪装成接入点等攻击。

3.4 损耗电池的攻击

能源耗尽攻击是一种能够将设备的能源消耗在设备所不希望的或者非法的活动上, 攻击者的目的在于将终端设备的计算时间用于处理垃圾数据, 因此能够在设备拥有者不期望的情况下更快地耗尽节点的电池资源[35]。

出于节约能耗的考虑, ZigBee 设备的大部分时间都处于休眠状态, 少数时间里设备需要时不时醒来工作、接收数据包。设备在唤醒间隔内醒来, 询问路由器是否有新的数据请求, 如果没有的话, 设备会继续回到休眠状态。在这种场景下, 攻击者可以通过伪装成路由器, 每当设备询问是否有数据请求时, 攻击者都回复有请求, 这就会让设备保持唤醒状态, 通过这种方式设备的电量很快会被消耗殆尽[36]。

LoRaWAN 权衡考虑通信延迟和电池损耗, 将电池损耗由低到高分为了 *A*、*B*、*C* 三类设备。其中 *B* 类设备周期性的唤醒以接收消息, 这个唤醒周期是由来自网关的信标广播所定义的, 而网关发往设备的信标帧是不进行加密的。因此攻击者可以自己组装信标帧, 向设备发送恶意的信标帧, 将唤醒周期定义得很短, 使设备频繁地进行唤醒, 这样一来就能加快 *B* 类设备的电池损耗[17]。

Eugene 等人[37]提出的 Vampire 攻击是一种基于路由的能量耗尽攻击, 常见的采用方法有循环路由和转发[37]。信标路由协议以及基于逻辑 ID 的传感网络都易感 Vampire 攻击, Vampire 能够使网络多消耗 10%的通信能量, 其中, BLE 以及 Z-Wave 都很容易受到这种攻击[37]。

Wi-Fi 设备也同样遭受着资源耗尽攻击, Benjamin 等人通过向 Wi-Fi 设备不断发送 ping 消息、ACK 消息、SYN 同步消息, 以此对设备造成 DoS 攻击。他们发现这样可以将设备的能量耗尽速度加快 18.5%[38]。

3.5 射频干扰

射频干扰攻击的目的是故意干扰无线介质的正常工作。在物理和接入层面, 通过向物理信道不断地注入数据从而使信道被占满, 导致数据传输和接收的异常和错误。无论在哪种情况下, 物理层或 MAC 层, 都可以应用几种不同效率的策略来实现这种攻击。最简单的实现方式就是连续发射信号干扰无线信道, 使合法流量完全被阻塞[40], 对设备造成 DoS 攻击[39]。

由于射频干扰通常发生在物理层, 如果协议在物理层没有采取抵抗干扰的调制技术就会容易受到射频干扰的攻击。LoRa 在物理层上采用了 CSS 扩频调制技术, 这样做的好处使得单个 LoRa 符号比一般的跳频通信的段突发时段要长, 因此对于 AM 脉冲的抗干扰性更强, 并且 CSS 调制技术还有抗多普勒效应的优势[41]。Albert 等人[42]分别对 Wi-Fi 和 LoRa 网络进行射频干扰攻击, 得到的结果是 Wi-Fi 连接在应对干扰时完全地崩溃而 LoRa 连接表现出了超强的抵抗力。但是 LoRa 物理层存在同种信号的干扰问题, 使用特定频率和参数同时发送数据的 LoRa 设备可能会影响彼此的信号。通过滥用这种漏洞, 就有可能恶意地干扰 LoRa 消息[41]。

ZigBee 通信也很容易受到射频干扰, Bastian Bloessl 仅使用了价值 40 美元的 ZigBee 硬件即对网络进行了选择性射频攻击[44]。Dimiyrios 等人发现通过监听 ZigBee 网络能够得到一些有用的网络层命令, 并使用这些命令发起选择性射频和欺骗攻击。

攻击者可以采取所述的五种攻击方法对物联网协议造成有效的攻击, 每种攻击所造成的危害也不同, 我们将无线协议的攻击归纳为表 4。攻击者使用上述的手段, 在协议层面对物联网设备进行攻击, 上述针对物联网协议的攻击研究汇总为表 5。在针对

表 4 无线协议攻击

Table 4 Attacks on wireless protocols

无线攻击	危害的安全属性
窃听	消息机密性
重放攻击	反重放能力、消息完整性
破解密钥	安全的认证过程、机密性
电池耗尽攻击	安全认证
射频干扰	抗干扰能力

表 5 物联网协议面对的攻击汇总表

Table 5 Summary of attacks on IoT communication protocols

	ZigBee	BLE	Wi-Fi	LoRa	RFID
窃听	[16,46-47]	[45,48]	[19,49]	[17,50]	[51-53]
重放攻击	[22]		[24]	[20]	[51]
破解密钥	[27,47]	[28-29]	[19,32-33]	[30-31]	[54]
耗尽电池	[36]	[37,55-56]	[38]	[23]	
射频干扰	[43]	[55]	[57]	[41-42]	

物联网协议的攻击上, 攻击者首先会以窃听到网络通信为基础, 这方面已经有了特定的窃听软件比如说 KillerBee、Ubertooth[45], 但是由于某些协议的物理特性, 比如说 BLE 的自适应跳频给窃听加大了难度。对于针对物联网协议的重放攻击, 主要难点在于定位协议的计数值, 在确认计数值之后就能够进行有效的重放攻击。破解密钥通常从设备的配对过程入手, 比如说可以通过在 ZigBee 配对过程中窃听密钥材料进行破解。耗尽电池的攻击在某些物联网场景下是影响巨大的, 比如说工业物联网, 往往通过修改物联网设备的唤醒周期实行攻击。射频干扰一直是无线协议的一大攻击因素, 有些协议比如说 LoRa 的物理层能够有效抵御其他信号的干扰, 而近距离的 ZigBee、BLE 则更容易被射频干扰所攻击。

4 物联网协议安全的未来展望

虽然物联网协议已经采取了保护数据安全性的措施, 但在面临攻击时依然无法具备完全的抵御能力。原因之一是物联网设备受限的计算资源, 其二在于物联网设备面临的攻击面多, 易被攻击者物理占有。为了应对目前物联网协议暴露的安全问题, 我们提出了 3 点改善物联网协议安全的建议。

4.1 协议形式化验证

由于物联网协议在设计安全算法时必须考虑低功耗的要求, 使得攻击者能够有机可乘实现攻击, 因此很有必要从设计阶段就发现可能存在的漏洞, 以便从一开始就确保系统的安全性。

形式化验证是能够在设计层面上发现可能存在漏洞的技术, 其运行过程如图 3 所示。形式化验证通过一系列基于数学或逻辑的方法验证设计的正确性。进行形式化验证大体需要经过以下步骤: 首先需要详细地学习协议的标准, 再人为地根据标准定义好模型; 接着将这个人为定义好的模型转换为模型检查器的输入; 最后一步就是检查形式化验证的结果, 并根据结果确定标准需要进行更改的建议[5]。

形式化验证技术能够帮助协议开发者们评价协议的安全性, 并在此基础上对协议作出调整和完善。

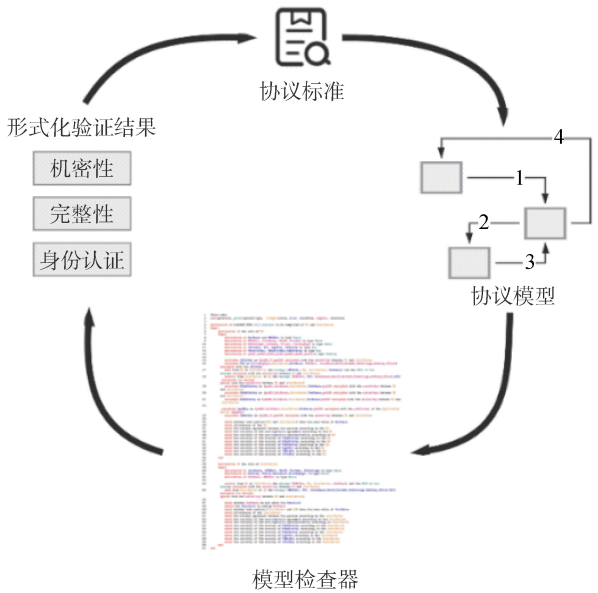

图 3 形式化验证过程

Figure 3 Process of formal verification

目前研究者们已经开发出多种形式化验证工具, 能够给安全性作出定量的分析, 这些形式化校验工具包括但不限于 AVISPA[58]、Event-B[59]、PRISM[60]、Scyther[61]、Tamarin[62]、UPPAAL[63]。Mohamed 等人将 LoRa v1.1 协议标准形式化为模型, 使用 Scyther 对该模型进行了安全检查, 并证明了在 LoRa v1.0 上存在的漏洞已被 LoRa v1.1 所解决[64]。Noomene 等人[65]使用了 Scyther、Tamarin、ProVerif 三个工具对蓝牙低能耗的密钥建立过程进行建模, 对模型评价其隐私保护、可用性、性能以及表现进行评估。此外, 对于物联网设备的测评由于协议众多的关系而影响了覆盖率, 渗透测试人员需要使用对应协议的硬件工具才能对设备进行测评。Mikulkis 等人[66]基于 SDR(软件无线电)研发可以测评物联网协议的工具。目前, 研究者对物联网协议安全性的研究多是出于自己对协议标准的分析, 并在此之上搭建环境模拟攻击场景。物联网的协议众多, 并且协议之间异构程度高, 并且存在着协议更新换代的问题, 对此我们认为, 安全研究者应当在前人的基础上完善协议模型, 使模型能够覆盖更多的安全情况, 并对协议模

型作出完整的安全评价, 最后在形式化验证结果的基础上开展自己的工作。

4.2 轻量级加密及验证

由于物联网设备的计算以及通信性能较低, 传统的密码学方案虽然被证明有很强的安全性, 但很难满足于物联网环境的低功耗要求。对于物联网环境的安全需求, 需要有轻量级的密码和认证算法作为支持[67]。

轻量级密码算法的应用规模比较小, 对轻量级密码吞吐量的要求比普通密码算法要低得多。轻量级密码算法大都基于硬件而实现, 在维持效率的情况下保证安全性。Leander 等人在 DES 的基础上提出了轻量化的 DESL, 使用可减少门电路复杂度的硬件体系结构, 将原来 DES 的 8 个原始 *S* 盒合并为可以重复设计的单一 *S* 盒。相比于 DES 算法, DESL 的吞吐量变低了, 实现面积变小, 更好地适应了低功耗场景[68]。Hong D 等人[69]提出了轻量级分组密钥 HIGHT, HIGHT 是一个 32 轮的迭代密码, 密钥长度为 128 比特, 他在满足轻量级需求的同时保证了足够的安全性。

轻量级认证算法需要做到使用受限的资源做到双向认证, 防止物联网设备遭受的伪装攻击。RFID 系统遭受了攻击者伪装阅读器或者标签的攻击, Kai Fan 针对 RFID 的应用场景提出了一种基于云的轻量化双向认证协议, 经实验证明该协议能够使 RFID 拥有抵抗追踪、重放和伪装的攻击[70]。Mahdi 等人[71]针对智能医疗的应用场景, 为 WBAN(wireless body area network)环境提供轻量化和双元素的认证算法, 能够安全地建立 WBAN 的共享密钥, 使密钥建立免于攻击者威胁。

物联网厂商总是把安全作为设备的最后一环考虑, 如果将轻量化的加密和认证算法与产品相结合, 则在不影响设备性能的前提下保证了安全性。近些年来, 轻量级密码与认证算法一直是物联网安全领域的热点。对此我们认为, 协议本身应当结合轻量级加密和轻量级认证算法作出调整。

4.3 区块链技术的应用

区块链[72]是一个去中心化的、分布式的、共享的、不可篡改的数据库, 它被用于 P2P 网络中存储资产和事务。区块链使用椭圆曲线加密以及 SHA-256 哈希算法提供强大的数据加密和完整性验证。相比于可信第三方, 可信第三方的服务会有被恶意干扰、黑客攻击的风险, 而区块链事务的安全性由大多数网络的参与者所验证。

一方面, 区块链可以给予每个设备唯一的身份识别, 关于设备的基本属性可以安全地存放在区块链中。另一方面, 区块链的设备保证了传输数据的完整性和机密性, 并且由于设备的所有事务都会被记录在区块链上, 这使得追溯更加安全方便。

在物联网与区块链技术结合领域已经有了一些研究。Seyoung Huh 等人[73]提出可以使用区块链平台管理物联网设备, 他们使用 Ethereum 区块链平台管理物联网设备, 将设备的 RSA 公钥存储于区块链上, 得到了一个更易管理, 抵抗攻击能力更好的物联网系统。Oscar Novo[7]将区块链应用于物联网环境下的访问控制, 解决了集中式访问控制系统缺乏可扩展性的能力。

鉴于多数物联网终端设备的存储与计算能力较弱, 如何将区块链技术轻量化以适配物联网终端设备, 这是一个迫切需要解决的关键技术问题。

5 总结与展望

物联网技术应用于众多产业, 并且保持着强劲的发展速度。通信协议由短距离的 RFID, 到中距离的 ZigBee、BLE、Wi-Fi 协议, 再到远距离的 LoRa 协议。这些协议受限于物联网设备的低功耗特点, 暴露出了设计上的安全漏洞。本文对这些协议的安全策略作了阐述, 并介绍了攻击者对协议的攻击手段, 指出了协议在安全方面的不足。

面对物联网的安全需求, 我们认为使用形式化验证技术可以帮助协议规范者们验证自身协议的安全性, 除此之外, 使用轻量化加密和轻量级认证技术可以提供给协议更强的竞争力。面向物联网终端设备, 轻量化的区块链技术是一项迫切需要突破的关键技术。

参考文献

[1] White paper on Internet of things (2018) issued by China Academy of information technolog[J]. *Automation Panorama*, 2018, 35(12): 35.
(中国信通院发布《物联网白皮书(2018 年)》[J]. *自动化博览*, 2018, 35(12): 35.)

[2] Erricson Report. Erricson. https://www.ericsson.com/en/mobility-report/reports. 2020.

[3] *Black Hat 2019*: Arm IDA and Cross Check: Reversing the Boeing 787's Core Network https://www.blackhat.com/us-19/briefings/schedule/#arm-ida-and-cross-check-reversing-the-boeing-78739s-core-network-15716. 2020

[4] Sengupta J, Ruj S, Das Bit S. A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT[J]. *Journal of Network and Computer Applications*, 2020, 149: 102481.

[5] Hofer-Schmitz K, Stojanović B. Towards Formal Verification of IoT Protocols: A Review[J]. *Computer Networks*, 2020, 174: 107233.

[6] Whiting D, Housley R, Ferguson N. Counter with CBC-MAC (CCM)[R]. RFC Editor, 2003.

[7] Whitehurst L N, Andel T R, McDonald J T. Exploring Security in ZigBee Networks[C]. *The 9th Annual Cyber and Information Security Research Conference*, 2014: 25-28.

[8] Meyer R. Security issues and vulnerability assessment of Zigbee enabled home area network implementations[J]2012SecurityIA. 2012.1-81.

[9] Heydon R, Hunn N. Bluetooth low energy[J]. *CSR Presentation, Bluetooth SIG* https://www. bluetooth. org/DocMan/handlers/ DownloadDoc. ashx, 2012.1-63.

[10] Walker J. A History of 802.11 Security[J]. *Rutgers WINLAB. Intel Corporation.* Archived from the original on, 2016, 9:1-26.

[11] Khasawneh M, Kajman I, Alkhudaidy R, et al. A Survey on Wi-Fi Protocols: WPA and WPA2[C]. *Recent Trends in Computer Networks and Distributed Systems Security*, 2014: 496-511.

[12] Wi-Fi-Alliance. WPA3 Specification Version 1.0, https://www. wi-fi.org/, 2018.

[13] Sanchez-Iborra R, Sánchez-Gómez J, Pérez S, et al. Enhancing LoRaWAN Security through a Lightweight and Authenticated Key Management Approach[J]. *Sensors*, 2018, 18(6): 1833.

[14] Mike Ryan.Bluetooth: With low energy comes low security[C].*7th USENIX Workshop on Offensive Technologies*. 2013:4.

[15] Housley R, Whiting D, Ferguson N. Alternate temporal key hash[J]. IEEE doc, 2002, 802.

[16] IEEE 802.15.4/ZigBee Security Research Toolkit. KillerBee. https://github.com/riverloopsec/killerbee. 2011.

[17] Fahmida S, Modekurthy V P, Rahman M, et al. Long-Lived LoRa: Prolonging the Lifetime of a LoRa Network[C]. *2020 IEEE 28th International Conference on Network Protocols*, 2020: 1-12.

[18] Hancke, Gerhard. Eavesdropping attacks on high-frequency RFID tokens[C]. *The 4th Workshop on RFID Security,* 2008: 9440.

[19] Beck, Martin & Tews, Erik. Practical attacks against WEP and WPA[J]. *IACR Cryptology ePrint Archive.* 2008. 472.

[20] Aras E, Ramachandran G S, Lawrence P, et al. Exploring the Security Vulnerabilities of LoRa[C]. *2017 3rd IEEE International Conference on Cybernetics*, 2017: 1-6.

[21] Keung S, Siu K Y. Efficient Protocols Secure Against Guessing and Replay Attacks[C]. *Proceedings of Fourth International Conference on Computer Communications and Networks - IC3N'95*, 1995: 105-112.

[22] Stelte B, Rodosek G D. Thwarting Attacks on ZigBee - Removal of the KillerBee Stinger[C]. *The 9th International Conference on Network and Service Management*, 2013: 219-226.

[23] Yang X Y, Karampatzakis E, Doerr C, et al. Security Vulnerabilities in LoRaWAN[C]. *2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation*, 2018: 129-140.

[24] Vanhoef M, Piessens F. Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2[C]. *The 2017 ACM SIGSAC Conference on Computer and Communications Security*, 2017: 1313-1328.

[25] Kohlios C, Hayajneh T. A Comprehensive Attack Flow Model and Security Analysis for Wi-Fi and WPA3[J]. *Electronics*, 2018, 7(11): 284.

[26] Khattab A, Jeddi Z, Amini E, et al. RFID Security: A Lightweight Paradigm[M]. Cham: Springer, 2017.

[27] Vidgren N, Haataja K, Patiño-Andres J L, et al. Security Threats in ZigBee-Enabled Systems: Vulnerability Evaluation, Practical Experiments, Countermeasures, and Lessons Learned[C]. *2013 46th Hawaii International Conference on System Sciences*, 2013: 5132-5138.

[28] Sevier S, Tekeoglu A. Analyzing the Security of Bluetooth Low Energy[C]. *2019 International Conference on Electronics*, *Information*, *and Communication*, 2019: 1-5.

[29] Kwon G, Kim J, Noh J, et al. Bluetooth Low Energy Security Vulnerability and Improvement Method[C]. *2016 IEEE International Conference on Consumer Electronics-Asia*, 2016: 1-4.

[30] Butun I, Pereira N, Gidlund M. Analysis of LoRaWAN V1.1 Security: Research Paper[C]. *The 4th ACM MobiHoc Workshop on Experiences with the Design and Implementation of Smart Objects*, 2018: 1-6.

[31] Chacko S, Job M D. Security Mechanisms and Vulnerabilities in LPWAN[J]. *IOP Conference Series*: *Materials Science and Engineering*, 2018, 396: 012027.

[32] Tews E, Beck M. Practical Attacks Against WEP and WPA[C]. *The second ACM conference on Wireless network security*, 2009: 79-86.

[33] Li Q. Application and research of airtrack ng in Wi Fi security experiment [J]. *Information & Communications*, 2015, 28(10): 45-46. (李强. Aircrack-ng 在 Wi-Fi 安全实验中的应用与研究[J]. *信息通信*, 2015, 28(10): 45-46.)

[34] Acosta-López A, Melo-Monroy E Y, Linares-Murcia P A. Evaluation of the WPA2-PSK Wireless Network Security Protocol Using the Linset and Aircrack-ng Tools[J]. *Revista Facultad De Ingeniería*, 2018, 27(47): 73-80.

[35] Nguyen V L, Lin P C, Hwang R H. Energy Depletion Attacks in Low Power Wireless Networks[J]. *IEEE Access*, 2019, 7: 51915-51932.

[36] Cao X H, Shila D M, Cheng Y, et al. Ghost-in-ZigBee: Energy Depletion Attack on ZigBee-Based Wireless Networks[J]. *IEEE Internet of Things Journal*, 2016, 3(5): 816-829.

[37] Vasserman E Y, Hopper N. Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks[J]. *IEEE Transactions on Mobile Computing*, 2013, 12(2): 318-332.

[38] Moyers B R, Dunning J P, Marchany R C, et al. Effects of Wi-Fi and Bluetooth Battery Exhaustion Attacks on Mobile Devices[C]. *2010 43rd Hawaii International Conference on System Sciences*, 2010: 1-9.

[39] Vadlamani S, Eksioglu B, Medal H, et al. Jamming Attacks on Wireless Networks: A Taxonomic Survey[J]. *International Journal of Production Economics*, 2016, 172: 76-94.

[40] López M, Peinado A, Ortiz A. An Extensive Validation of a SIR Epidemic Model to Study the Propagation of Jamming Attacks Against IoT Wireless Networks[J]. *Computer Networks*, 2019, 165: 106945.

[41] Aras E, Small N, Ramachandran G, et al. Selective Jamming of LoRaWAN Using Commodity Hardware[C]. *The 14th EAI International Conference on Mobile and Ubiquitous Systems*: *Computing*, *Networking and Services*, 2018: 363-372.

[42] Öst A. Evaluating LoRa and WiFi Jamming. Mid Sweden University, Department of Information Systems and Technology. 2018.

[43] ZigBee Jamming. https://www.bastibl.net/reactive-zigbee-jamming/ Mar. 2019.

[44] Akestoridis D G, Harishankar M, Weber M, et al. Zigator: Analyzing the Security of Zigbee-Enabled Smart Homes[C]. *The 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 2020: 77-88.

[45] Ubertooth. https://github.com/greatscottgadgets/ubertooth. 2014.

[46] Olawumi O, Haataja K, Asikainen M, et al. Three Practical Attacks Against ZigBee Security: Attack Scenario Definitions, Practical Experiments, Countermeasures, and Lessons Learned[C]. *2014 14th International Conference on Hybrid Intelligent Systems*, 2014: 199-206.

[47] Radmand P, Domingo M, Singh J, et al. ZigBee/ZigBee PRO Security Assessment Based on Compromised Cryptographic Keys[C]. *2010 International Conference on P2P*, *Parallel*, *Grid*, *Cloud and Internet Computing*, 2010: 465-470.

[48] Gupta N. Inside Bluetooth Low Energy [M]. Artech House, 2016.

[49] Borisov N, Goldberg I, Wagner D. Intercepting Mobile Communications: The Insecurity of 802.11[C]. *The 7th annual international conference on Mobile computing and networking*, 2001: 180-189.

[50] Dönmez T C M, Nigussie E. Security of LoRaWAN V1.1 in Backward Compatibility Scenarios[J]. *Procedia Computer Science*, 2018, 134: 51-58.

[51] Yang L. RFID system security evaluation and protection technology [M]. Beijing: Publishing House of Electronics industry, 2015. (杨林. RFID 系统安全测评及防护技术[M]. 北京: 电子工业出版社, 2015.)

[52] Juels A. RFID Security and Privacy: A Research Survey[J]. *IEEE Journal on Selected Areas in Communications*, 2006, 24(2): 381-394.

[53] Garfinkel S, Rosenberg B. RFID: Applications, security, and privacy[M]. Pearson Education India, 2006.

[54] Bono S, Green M, Stubblefield A, et al. Security Analysis of a Cryptographically-Enabled RFID Device[C].*USENIX Security Symposium*. 2005, 31: 1-16.

[55] O'Sullivan H. Security vulnerabilities of bluetooth low energy technology (ble)[J]. *Tufts University*, 2015.

[56] Tay H J, Tan J, Narasimhan P. A survey of security vulnerabilities in bluetooth low energy beacons[J]. *Carnegie Mellon University Parallel Data Lab Technical Report* CMU-PDL-16-109, 2016.

[57] Arana P. Benefits and Vulnerabilities of Wi-Fi Protected Access 2 (WPA2) [J]. INFS, 2006, 612: 1-6.

[58] AVISPA. http://www.avispa-project.org/. 2001.

[59] EVENT-B. http://www.event-b.org/.2004.

[60] PRISM. https://www.prismmodelchecker.org/. 2011.

[61] SCYTHER. https://people.cispa.io/cas.cremers/scyther/. Mar. 2011.

[62] TAMARIN. https://tamarin-prover.github.io/manual/tex/tamarin-manual.pdf. 2016.

[63] UPPAAL. http://www.uppaal.org/. Feb. 2008.

[64] Eldefrawy M, Butun I, Pereira N, et al. Formal Security Analysis of LoRaWAN[J]. *Computer Networks*, 2019, 148: 328-339.

[65] Henda N B, Norrman K, Pfeffer K. Formal Verification of the Security for Dual Connectivity in LTE[C]. *2015 IEEE/ACM 3rd FME Workshop on Formal Methods in Software Engineering*, 2015: 13-19.

[66] Mikulskis J, Becker J K, Gvozdenovic S, et al. Snout: An Extensible IoT Pen-Testing Tool[C]. *The 2019 ACM SIGSAC Conference on Computer and Communications Security*, 2019: 2529-2531.

[67] Chen Z, Zeng F P, Chen G Z, et al. A Survey for IoT Security Assessment Technologies[J]. *Journal of Cyber Security*, 2019, 4(3): 2-16.
(陈钊, 曾凡平, 陈国柱, 等. 物联网安全测评技术综述[J]. *信息安全学报*, 2019, 4(3): 2-16.)

[68] Leander G, Paar C, Poschmann A, et al. New Lightweight DES Variants[M]. Fast Software Encryption. Berlin, Heidelberg: Springer Berlin Heidelberg, : 196-210.

[69] Hong D, Sung J, Hong S, et al. HIGHT: A new block cipher suitable for low-resource device[C].*International Workshop on Cryptographic Hardware and Embedded Systems. Springer, Berlin, Heidelberg*, 2006: 46-59.

[70] Fan K, Luo Q, Zhang K, et al. Cloud-Based Lightweight Secure RFID Mutual Authentication Protocol in IoT[J]. *Information Sciences*, 2020, 527: 329-340.

[71] Fotouhi M, Bayat M, Das A K, et al. A Lightweight and Secure Two-Factor Authentication Scheme for Wireless Body Area Networks in Health-Care IoT[J]. *Computer Networks*, 2020, 177: 107333.

[72] Khan M A, Salah K. IoT security: Review, blockchain solutions, and open challenges[J]. *Future Generation Computer Systems*, 2018, 82: 395-411.

[73] Huh S, Cho S, Kim S. Managing IoT Devices Using Blockchain Platform[C]. *2017 19th International Conference on Advanced Communication Technology*, 2017: 464-467.

[74] Novo O. Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT[J]. *IEEE Internet of Things Journal*, 2018, 5(2): 1184-1195.

张伟康 于 2019 年在东北大学计算机科学与技术专业获得学士学位。现在中国科学技术大学计算机技术专业攻读硕士学位。研究领域为物联网安全测评、固件安全。研究兴趣包括：通信协议、模糊测试。Email：buttman@mail.ustc.edu.cn

曾凡平 于 2009 年在中国科学技术大学信息安全专业获得博士学位。现任中国科学技术大学副教授。研究领域为网络信息安全、软件分析与测试。研究兴趣包括：网络与系统安全、软件分析与测试、物联网的云边端资源协同优化。Email：billzeng@ustc.edu.cn

陶禹帆 于 2020 年在中国科学技术大学信息安全专业获得学士学位。现在中国科学技术大学计算机技术专业攻读硕士学位。研究领域为系统安全、物联网安全。研究兴趣包括：物联网协议、安全测评。Email：tyf1999@mail.ustc.edu.cn

李向阳 2001 年在美国伊利罗伊大学厄巴纳-香槟分校(UIUC)计算机科学专业博士。IEEE Fellow，ACM 杰出科学家, 现任 ACM 中国联合主席, 中国科学技术大学教授、博导。研究兴趣主要为物联网、物联网安全、大数据共享与交易、机制设计和算法分析等。六次获国际会议最佳论文奖。Email:xiangyangli@ustc.edu.cn