物联网设备和智能可穿戴设备中的蓝牙低功耗协议：安全和隐私威胁

Tushar Nagrare*、ParulSindhwad、FarukKazi电子与电信工程系，
VJTI，孟买，印度电子邮箱：*tpnagrare m20@et.vjti.ac.in

摘要——**由于功耗极低、网络覆盖范围广且数据传输速度快，低功耗蓝牙（蓝牙低功耗）已成为物联网和智能可穿戴设备的主要传输媒介。随着物联网和低功耗蓝牙连接协议的迅猛发展，有必要探索防御技术，通过实际的安全分析来保护该协议。不幸的是，物联网低功耗蓝牙面临欺骗攻击风险，攻击者可以冒充设备，并向用户提供有害信息。此外，由于该协议采用了简化的策略，因此存在许多安全和隐私漏洞。本文通过STRIDE方法论开展定量安全分析，以构建应对物联网低功耗蓝牙传感器保护问题的框架。因此，本文针对分析中发现的各种暴露面提供可能的攻击场景，并提出缓解策略。鉴于此，作者开展了STRIDE威胁建模，以了解支持蓝牙低功耗的智能可穿戴设备的攻击面。本研究评估了小米手环、OnePlus 手环、Boat Storm 智能手表和Fire Bolt Invincible面临的不同利用场景，包括拒绝服务攻击、权限提升、信息泄露、欺骗、篡改和抵赖。**

索引词——**蓝牙低功耗、STRIDE模型、定量实验分析、可穿戴设备。**

I. 引言

所有物联网设备都至少配备一个传感器单元，使自然环境与计算机系统能够通过蓝牙低功耗、Wi-Fi 和 ZigBee 等通信协议实现更直接的集成 [1], [2]。蓝牙低功耗是一种物联网通信协议，专注于低功耗需求、减少信道跳频，并较早期版本提升了安全性。蓝牙低功耗通常也被称为蓝牙智能（BS），是使用最广泛的物联网通信技术 [3]。蓝牙低功耗属于无线个域网（WPAN）时代，最初于2010年6月被纳入蓝牙核心规范（BCS），并且相较于普通蓝牙具备多项优越特性。物联网已越来越多地应用于企业系统、医疗保健系统、军事应用、信标、新型家居用品及各种应用中。到 2022 [4]时，联网的物联网设备将达到150亿台。几乎所有现代操作系统都支持蓝牙和蓝牙低功耗，包括 Windows 10、Linux、Android 和 Mac OS [5]。

如图 2 所示，BLE配对过程分为三个步骤。首先，两个设备会相互告知将采用哪种配对方式，以及 BLE 设备在初始阶段可以执行什么操作并应预期什么。第二阶段会生成并处理短期密钥（STK）。为了生成

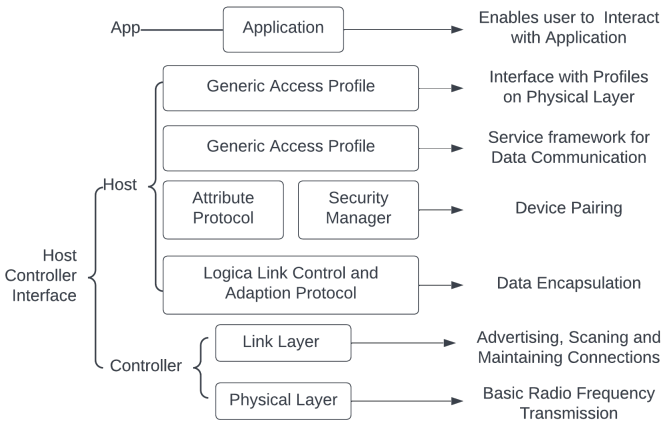

图 1. BLE 协议栈 [25]

STK，两个设备必须就临时密钥（TK）达成一致，并将其与随机整数结合。STK 不会在设备之间传输。如今，蓝牙低功耗已应用于数十亿台设备，因此审视其安全缺陷至关重要。

小米手环 4、Boat Storm 智能手表、OnePlus 手环和 Fire-Boltt Invincible 智能手表等可穿戴设备，以及这些个人和工业设备，让我们的生活更加便利，但也带来了很高的威胁。蓝牙低功耗的广泛应用使其漏洞可能造成致命后果，尤其是在医疗保健应用中。我们发现，小米手环 4、Boat Storm 智能手表、OnePlus 手环和 Fire-Boltt Invincible 智能手表等可穿戴设备存在不安全的配对、不当身份验证和协议实现不完善等问题，使其容易遭受窃听、PIN 码破解及其他攻击 [6]。安全隐患包括泄露个人信息 [7]。他们写道，物联网技术的发展令人担忧，个人安全风险、可识别信息泄露和关键基础设施攻击便是其中的例子，例如会计和金融数据存储 [8]。他写道，关于物联网信任和传感器集成的担忧包括：安全的物联网节点仍可能因传感器面临的威胁而易受攻击[5]。已有多项研究分别探讨了蓝牙低功耗的安全和隐私风险；一些研究人员关注该协议的安全设计，并实施特定攻击，利用协议实现不足之处 [9], [10], [11]。此外，学术界和产业界的安全研究人员在多个场合介绍了针对物联网低功耗蓝牙设备的多种攻击场景

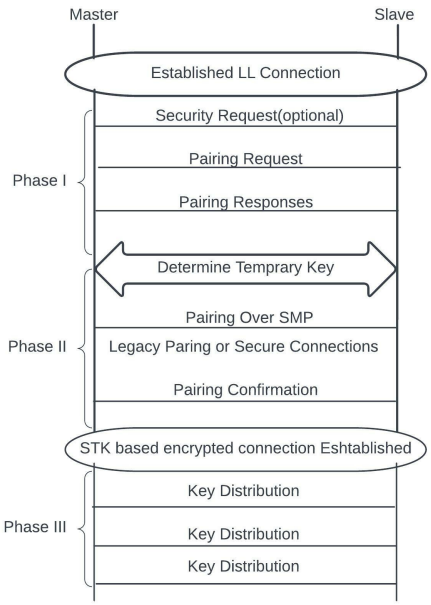

图2. 蓝牙低功耗连接阶段 [3]

通过使用 Btlejack、Adafruit、Ubertooth One 等攻击工具，对物联网蓝牙低功耗设备实施攻击，并在多个安全会议上展示 [12], [13]。本研究旨在评估可穿戴设备的威胁面。

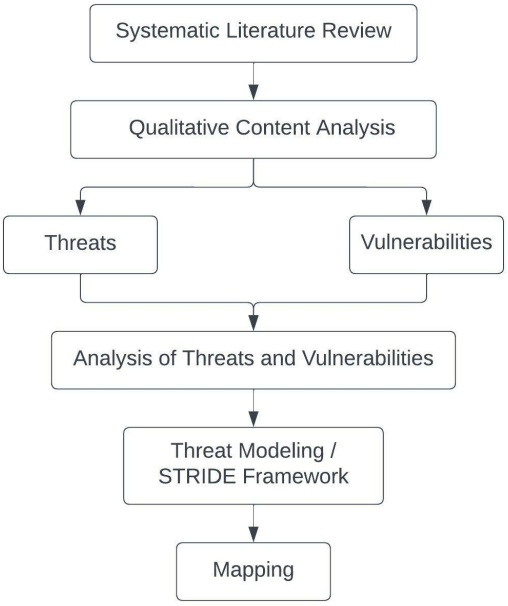

图3. 蓝牙低功耗分析的提出模型

本文的贡献可总结如下：

- 借助对可穿戴设备进行 STRIDE威胁分析，我们识别出多个广为人知（且为最新版本）的蓝牙低功耗协议中存在的漏洞，并据此对 BLE风险进行分类。
- 列举针对蓝牙低功耗可穿戴设备的各种攻击实例，以及用于实施这些攻击的工具，并讨论由此获得的经验教训。
- 针对已观察到的攻击威胁面提出缓解技术。

II. 用于攻击和分析蓝牙低功耗的工具

本节详细介绍了创建硬件和软件工具、用于分析各种蓝牙低功耗漏洞的开源安全研究人员。安全研究人员使用了中间人攻击、被动窃听和蓝牙加密。这些工具展示了标准物联网设备中的安全漏洞，如基于思维导图所示分析结果。本节列出的开源免费工具可帮助安全研究人员、BLE开发人员和测试人员构建低成本应用组件，识别并评估漏洞，并保护支持BLE的物联网设备。本节列出了用于攻击蓝牙低功耗可穿戴设备的各种工具。

A. 硬件工具

1) Ubertooth： Ubertooth是一款用于探索蓝牙的免费工具。Ubertooth提供的设备支持被动检查蓝牙和蓝牙低功耗设备通信。2011年1月发布的Ubertooth One能够检测并解调2.4 GHz频段中带宽为1 MHz的传输信号 [15]。Ubertooth会嗅探数据，并按频率和以dBm为单位的传输强度，对本地流量进行可视化显示。这项研究估算了该区域内的整体蓝牙流量，包括距离诊断，以查找项目范围之外的项目 [4],[14]。信道频率上的信号强度用于构建Ubertooth频谱分析仪，如图12所示：绿色线条表示所识别频率中最强的信号，而白色线条表示当前活动。无线技术通过空中传输数据，因此很容易拦截或篡改这些数据包。

*2) ADA-FRUIT BLE*嗅探器：Adafruit 是一种类似于 Ubertooth 的蓝牙低功耗（蓝牙低功耗）数据包捕获设备。Adafruit 由 Adafruit Industry[16] 创建。它能够拦截发送的数据包。使用此工具分析两台蓝牙低功耗设备。通过 Wireshark 收集数据。

B. 软件工具

1）*Btlejack*：Btlejack 可用于监视、干扰并劫持蓝牙低功耗设备。它现在支持一个或多个此类设备，且这些设备均运行专用固件。该工具基于 BBC Micro: Bit。其最新版本（2.0）支持 BLE 4.0 和 5.0。然而，BLE 5.0 [14] 仅支持 1 Mbps 未编码物理层。BtleJack 通过主动断开主设备并在连接中移动主设备来控制连接，同时进行捕获和嗅探。

2）Wireshark：Wireshark 是一款免费提供的数据包分析器。它是一款开源网络协议分析器，常用于数据包分析。为帮助收集数据，它可以通过以太网、蓝牙、USB 端口和其他通信介质收集信息。使用特定筛选器，Wireshark 图形用户界面（GUI）的用户可以查看图 4 中某些可穿戴设备捕获的数据包；如果供应商未使用加密技术，数据就会以明文直接传输，如图所示。

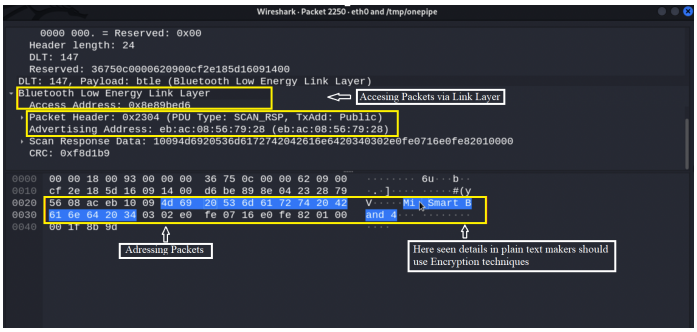

图 4. Wireshark 中嗅探到的数据包

3) Btlejuice：Cauquil 创建了 BtleJuice，并在 2016年 DefCon24 大会上展示了这一针对蓝牙低功耗设备的中间人攻击工具。Btlejuice 由四个部分组成：拦截得分、拦截代理、专用 Web 界面、Python 和 Node.js 绑定。其核心组件是拦截核心和代理。这两个组件彼此独立运行，并通过 WebSocket 协议进行通信。btlejuice 充当蓝牙低功耗配件与移动应用程序之间的代理。

III. STRIDE威胁分析中的安全前提

通过查看可穿戴设备的数据流图，我们可以推导出安全需求，并评估从小米手环 4、Boat Storm 智能手表、OnePlus 手环和 Fire-Boltt Invincible 智能手表等可穿戴设备分析中得到的攻击场景。在确定安全需求时，我们会考虑从数据流图中推导出的攻击场景，因为安全需求旨在阻止攻击者实现其目标。以下是一些安全需求。

1) 添加时间戳：在所有数据交换和连接过程中纳入时间戳，并将时间戳包含在数据包中，以避免重放攻击。

2) 身份验证：即使攻击者编辑了消息，消息认证机制也能识别出更改并阻止其被插入。此外，为避免连接到攻击者的设备、盗取账户以及绕过登录流程，应采用用户身份验证过程。

3) 加密：加密会妨碍攻击者读取和更改原始通信内容。因此，应通过数据包加密过程来防止消息篡改和网络数据包嗅探。此外，在将任何敏感数据保存到数据库之前，必须先对其加密。即使攻击者能够直接接触存储设备，也无法访问这些数据。

4) 流量分析和入侵检测：攻击检测和流量分析：要彻底阻止过量数据传输很困难。因此，我们必须在服务器端通过流量分析和渗透测试来减轻其影响。

5) 安全账户管理：为避免账户盗窃，所有用户都必须安全地管理自己的账户。服务提供商应告知用户账户被盗的可能性，并保护数据存储。

Microsoft 威胁建模工具基于我们的模型生成威胁建模报告，模型以图 5 所示的数据流图呈现。该工具自动生成了 111 项威胁。基于此前关于智能手环安全的研究，我们识别出 44 项可能实现攻击者目标的重要威胁。此外，下文攻击分析部分 A 和 B 将对物联网蓝牙低功耗可穿戴设备上的所有攻击场景进行实际分析。

IV. 可穿戴设备攻击分析

蓝牙低功耗的安全架构与经典蓝牙的安全架构有所不同。蓝牙低功耗支持低功耗、计算能力受限的传感器以及与物联网设备的连接。使用蓝牙低功耗时，我们必须在性能、安全、隐私问题和低功耗之间做出权衡。蓝牙低功耗标准包含多种建立安全连接的方式，包括设备绑定、链路层加密和设备安全列表。遗憾的是，许多物联网低功耗蓝牙设备未能正确实施这些安全方法。因此，由于许多风险源于常见的底层架构或协议中的漏洞，众多安全威胁随之产生；针对这些风险，采用相同的缓解措施即可。有些攻击彼此具有协同效应。本节重点介绍如何利用威胁模型序列组织并实施攻击。

如图5所示的数据流图（DFD）展示了用户信息在智能手机与智能手环之间的传输。表中还列出了针对特定BLE可穿戴设备（小米手环 4、Boat Storm 智能手表、一加手环和 Fire Bolt Invincible）的各种威胁；这些针对所分析可穿戴设备的已识别威胁源自 STRIDE威胁分析。要解决蓝牙低功耗设备中的安全问题，应着重检查系统中的用户数据和智能手环服务。

A. 被动攻击

任何攻击场景的第一步都是被动监听。攻击者会秘密监控已连接设备之间的每一次通信，从而引发各种破坏性攻击。只要以某种方式干扰数据传输，我们就能窃听并截获所有传输的数据。由于数据通过无线方式传输，被动窃听攻击尤其容易得逞；攻击者只需使用 Micro bit V2 之类的拦截器，就能截获设备的无线通信。

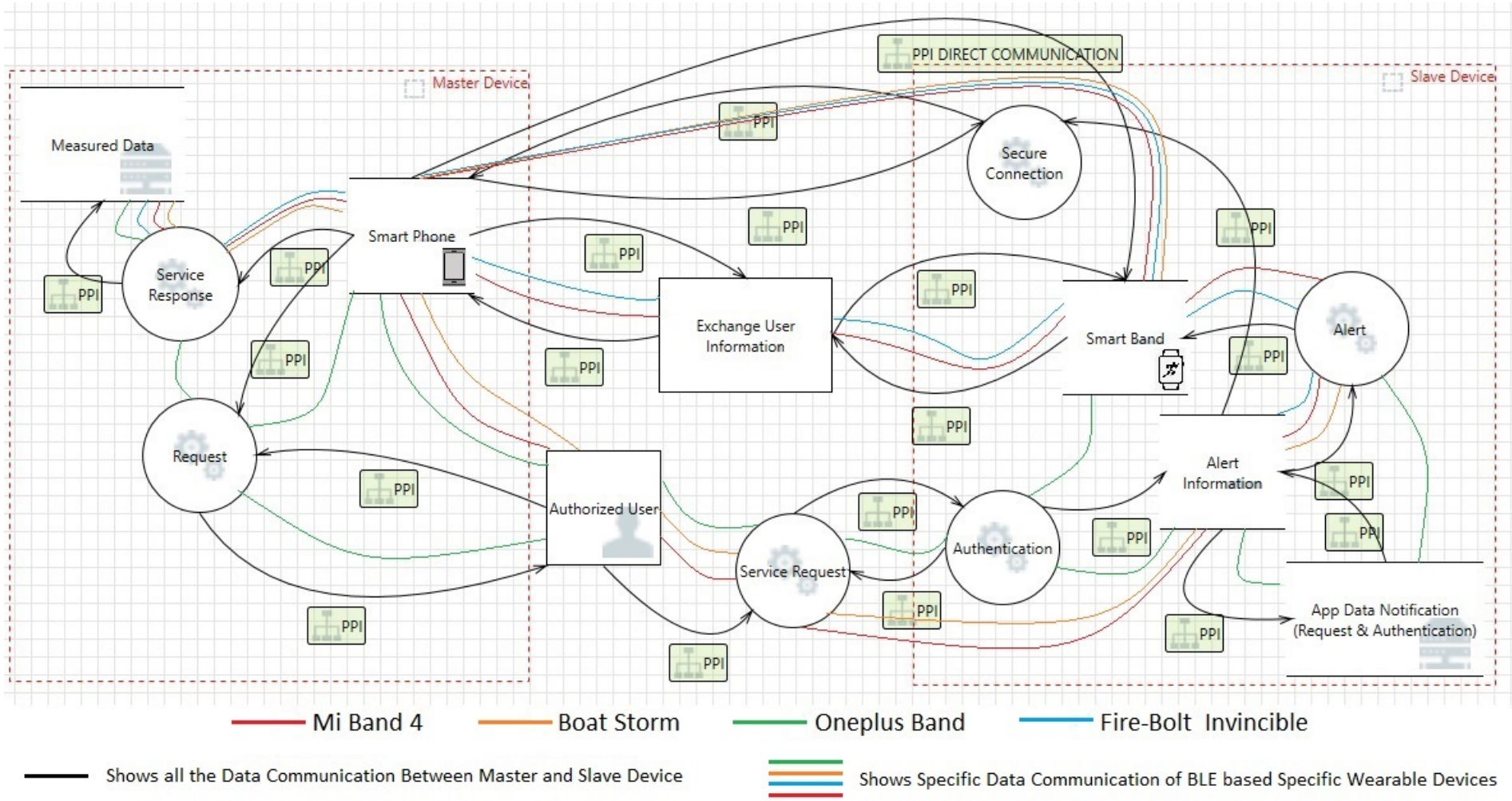

Fig. 5. Data Flow Diagram

表 I 所分析的可穿戴设备面临的威胁

	拒绝服务	权限提升	信息泄露	抵赖	欺骗	篡改
小米手环 4	Yes	No	Yes	No	Yes	No
Boat Storm 智能手表	No	No	Yes	No	No	No
OnePlus 手环	Yes	No	No	No	Yes	No
Fire-Bolt Invincible	Yes	Yes	Yes	No	Yes	Yes

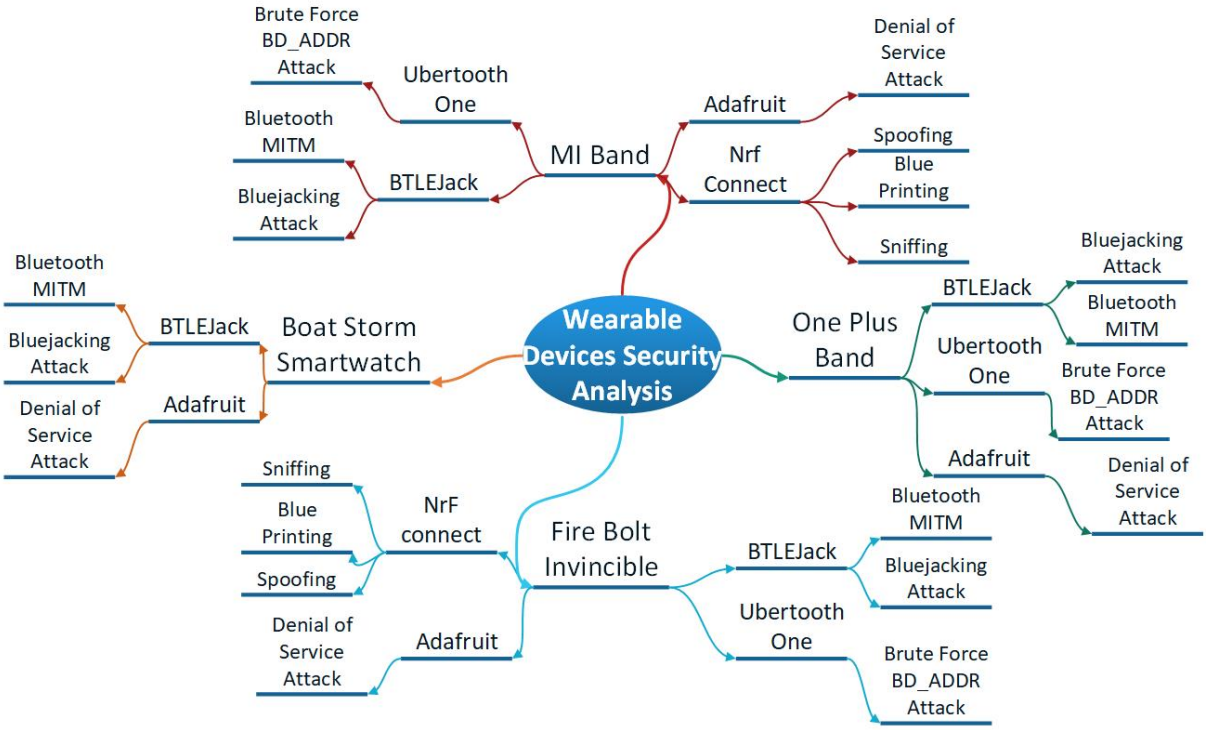

图 6. 安全分析思维导图

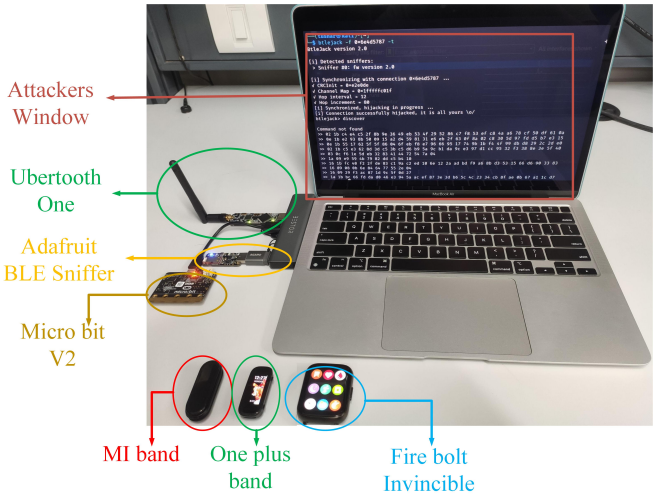

图 7. 攻击者测试平台

（小米手环 4、OnePlus 手环和 Firebolt invincible）这些物联网蓝牙低功耗可穿戴设备由于其可预测且明显的信道切换而特别容易受到这种攻击。

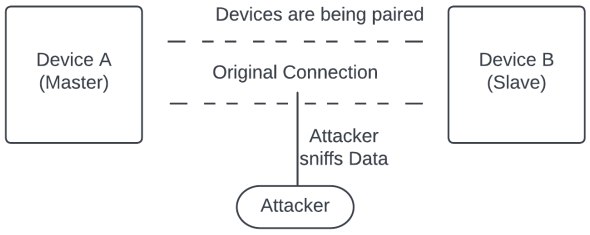

图 8. 被动攻击

由于蓝牙低功耗标准保护不足、加密算法薄弱，以及若干关键交换机制存在缺陷，许多蓝牙低功耗系统（如小米手环 4、Fire-Boltt Invincible 智能手表和 Boat Storm）容易受到此类攻击，攻击者可以轻易解码数据。

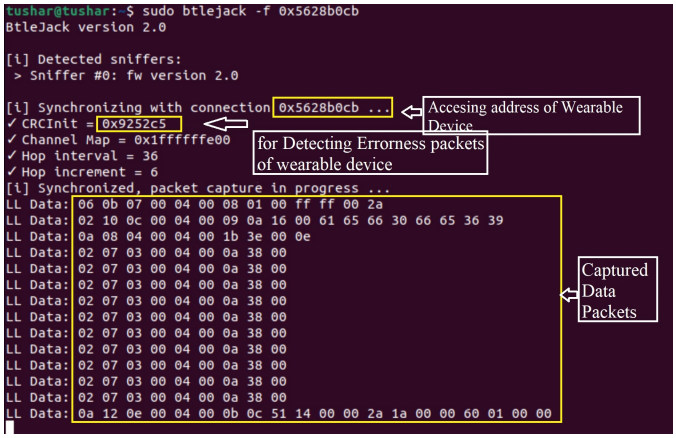

图 9. 使用 Micro bit V2 嗅探数据包

B. 主动攻击

在主动窃听攻击中，攻击者会干扰通信并获取信息。中间人攻击和重放攻击是两种会损害数据完整性的主动窃听攻击形式；在中间人攻击中，攻击者会主动参与通信过程 [11]。与中间人攻击不同，重放攻击不会入侵发送方或接收方，而是由攻击者捕获数据包并重新发送。

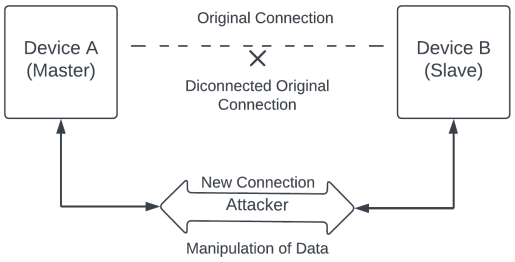

图 10. 主动攻击

1) 暴力破解 *BD-ADDR* 攻击：如前所述，蓝牙协议采用跳频扩频（FHSS），通过在 2.4 GHz ISM 无线电频段的不同信道间跳频来避免干扰 [5]。用于控制这种跳频行为的伪随机序列取自“主设备”。要嗅探设备的数据，必须考虑跳频，这就需要了解 BD-ADDR 的格式。蓝牙帧不包含完整的 BD-ADDR，但包含低位地址部分（LAP），即缩减后的 24 位（三个字节）。实际上，BD-ADDR 由 LAP 和构成高位地址部分的 1 个字节（UAP）组合而成。由于每个帧都会广播 LAP，Ubertooth One 可以被动捕获这些信息，以计算 UAP 和 LAP 部分。使用 Ubertooth-Rx 的扫描模式嗅探设备的 UAP 和 LAP 数分钟后，便可发现获取到的 MAC 标识符，（使用 -z 标志），并让这些设备彼此近距离通信。

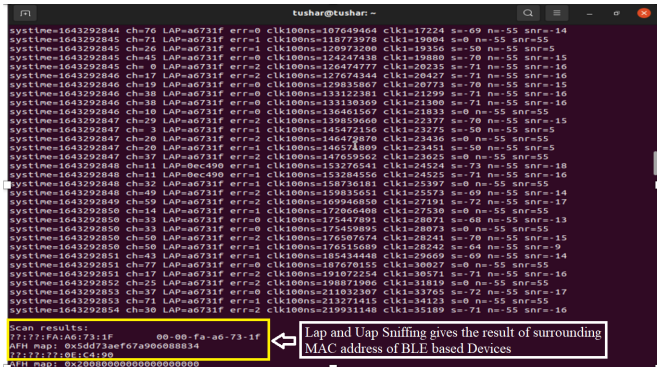

图 11. 使用 Ubertooth 嗅探 LAP 和 UAP 以捕获 MAC 标识符

Ubertooth 可以在隐蔽和不可发现模式下查找设备。Ubertooth 在这里并不是功能齐全的蓝牙低功耗设备；它只是一个嗅探器，用于收集 LAP 和 UAP 以组成地址，并向相应的蓝牙低功耗设备发送查询。

2）蓝牙中间人攻击：已有研究探讨了物联网系统中针对传统蓝牙和蓝牙低功耗的中间人攻击策略，而中间人攻击是一种常见的无线通信威胁 [6]。攻击者通过置身于蓝牙低功耗外围设备之间，可以对这些设备实施中间人攻击。攻击者会拦截并篡改多个设备发出的数据包，然后将其发送给另一台设备。两台设备都不知道自己的数据已被可疑设备拦截或修改。

蓝牙低功耗设备制造商必须严格遵守蓝牙低功耗协议的绑定和加密要求，以防止中间人攻击。最好也避免在不更新设备的情况下使用配对方式。开发者也应采用安全连接，因为与旧版连接相比，它能提供强得多的密码保护。如果中心设备（手机）知道配对设备（小米手环 4）具备输入/输出能力，则应在配对期间提供中间人攻击标志。

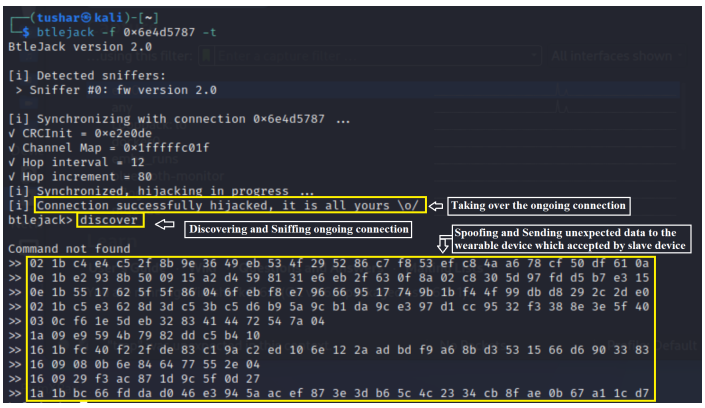

图 12. 中间人攻击

3）蓝牙信息收集：蓝牙信息收集可精确获取设备型号、制造商、唯一标识符（国际移动设备识别码）和软件版本等信息，同时着重关注用户隐私问题。这种利用方式会影响传统蓝牙和蓝牙低功耗。虽然此类攻击可能不会造成重大损害，但攻击者会借此策划针对受害者设备的后续攻击。蓝牙信息收集并非严重攻击，但确实会暴露个人信息。根据蓝牙低功耗标准，物联网低功耗蓝牙设备必须公开广播其 GATT 服务，以便攻击者获取这些数据 [17]。此外，攻击者还可以获知特定制造商部署的设备数量。如果某个设备存在广为人知的安全漏洞，这种攻击可能造成严重损害。如今有多种开源工具可用于实施此类攻击。这些工具可能会收集有关蓝牙协议栈的信息。另一款可快速执行此类攻击的强大应用是适用于智能手机的 nRF Connect，它可以直接向物联网低功耗蓝牙设备写入服务。

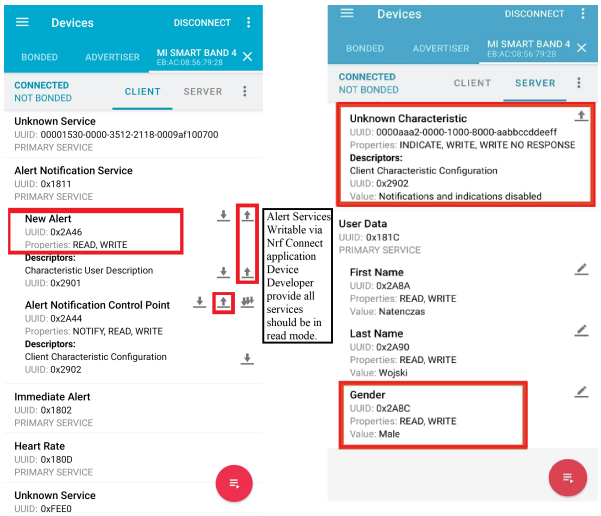

图 13. nRF Connect 应用程序

4) 设备指纹识别：设备指纹识别通过利用设备独有的数据来识别特定设备，例如 MAC 地址、通用唯一识别码、广播数据包和 GATT 服务。如上图 12 所示，设备指纹识别会侵犯用户隐私。许多蓝牙低功耗设备的固定 MAC 地址可用于识别这些设备。通过分析物联网移动应用并从广告中识别静态UUID，若干基于蓝牙低功耗的物联网设备和可穿戴设备容易受到指纹识别攻击 [17]。

- 通用唯一识别码具有层级结构，需要分析其取值集合，以确定用于指纹识别的通用唯一识别码层级。同时，它还能找出应用层缺陷，例如不当使用加密。
- 嗅探到的广播通用唯一识别码会导致物联网设备遭到指纹识别 [13]。因此，多个应用可能会使用同一个通用唯一识别码。实际上，必须连接到该设备。
- 这些值设定了可预测的结果，体现了实现层面的弱点，从而导致设备被识别出来

这些设备似乎容易受到嗅探或未经授权的访问。

我们需要修复应用层漏洞以阻止这种攻击。开发者必须提供具备密码学安全性的功能，并加密凭据。由于广播信号必须进行信道级测量，因此应采用加密技术来隐藏通用唯一识别码 [13]。这样一来，攻击者只能接收到令人烦扰的信号。

5) 蓝牙探测： 查找存在已知安全问题的设备，这种做法称为蓝牙探测。这是为后续更严重的攻击做准备，而非主动攻击。攻击者会使用 Microbit V2 等小型嗅探器，在人群密集的区域探测易受攻击的设备，以避免被发现。攻击者的目标是存在安全漏洞的设备。

不需要蓝牙低功耗连接时，必须使设备保持不可见或处于不可发现模式，以防攻击者发现它。未经身份验证的设备只能提供最基本的信息。

6) 拒绝服务攻击： 在拒绝服务攻击中，支持蓝牙的对等设备可以通过逻辑链路控制与适配协议请求并接收回显。使用 L2CAPping 可以发动拒绝服务攻击。L2CAPping 可用于查看与其他支持蓝牙的设备之间已建立的连接及往返时间。针对智能手机的攻击距离可达到约 10 米。针对笔记本电脑的强力传输距离可达 100 米。可使用 Linux Bluex 工具包附带的 l2ping 等标准工具。l2ping 程序中的若干指令允许黑客指定数据包长度。黑客用恶意程序感染支持蓝牙的设备，使其无法正常供用户使用。这种攻击可能会扰乱受害设备的正常运行，甚至损害其功能。标准 BlueZ 工具发行版中的 l2ping 提供 -s number 选项，允许用户选择 l2ping 的数据包长度。许多设备使用 600 字节的数据包大小。该选项会创建指定大小的数据包，并将其发送到给定的 MAC 地址。因此，终端设备的响应时间会越来越长，被攻击设备的蓝牙功能最终会停止工作。

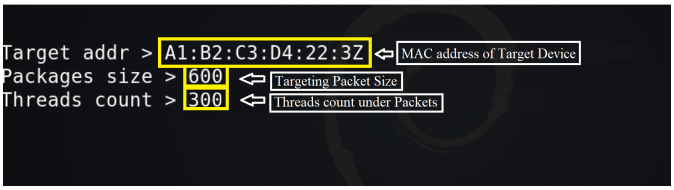

图 14. 使用 Adafruit 发起的拒绝服务攻击

V. 蓝牙低功耗攻击总结

使用蓝牙低功耗协议的物联网设备和可穿戴设备存在多种漏洞。不过，许多问题都归咎于糟糕的协议设计。一些蓝牙低功耗安全策略设备容易受到密码攻击配对技术和蓝牙低功耗隐私漏洞的影响。美国国家标准与技术研究院（NIST）及其他安全系统研究人员已针对某些特定设备提供了相当

旧版本（BLE 4.0版和 4.1版）。根据作者的分析，如图15所示，思维导图展示了物联网低功耗蓝牙在三个 OSI层级（例如物理层、数据链路层和应用层）面临的威胁。物理层攻击伴随着对无线电频谱的攻击。大多数攻击发生在蓝牙数据连接层。数据通过数据传输层传输。攻击者会捕获链路层数据包，并通过链路层发送恶意数据包，因此链路层安全是 BLE开发人员面临的一项重大问题。一些漏洞被设备制造商或开发人员归类为应用层漏洞，原因是应用层的实现不正确。

VI. 未来展望

支持蓝牙低功耗的智能可穿戴设备和物联网设备已成为我们日常生活的一部分。物联网设备数据管理和访问控制需要具备高度安全性。此外，应通过服务器而非用户连接物联网设备。这种设备显著增强了设备管理能力并提升了用户隐私保护水平。该服务器旨在防止物联网设备访问个人数据。然而，如果网络或服务器遭到入侵，所有与之相连的设备都将面临危险。因此，研究人员可能很快会开始探索采用分布式区块链技术来保护相连的物联网设备。各行业都能从BLE网状网络中受益。

VII. 结论

本文研究了物联网低功耗蓝牙设备的有效性。通过分析和实验研究物联网蓝牙低功耗可穿戴设备的攻击面，并利用STRIDE威胁建模工具构建威胁模型，可以轻松评估所发现的威胁。在配对和可写服务阶段，有时仅存在严重漏洞，以及拒绝服务攻击（DoS）、权限提升、信息泄露、欺骗、篡改和抵赖等不同的利用场景；采用适当的配对方法，可以永久保护这一阶段。此外，身份验证技术可使服务UUID无法被应用程序以外的来源访问。本文还通过定量分析，为解决物联网蓝牙低功耗可穿戴设备的安全问题提供了框架。蓝牙低功耗是一种安全的无线通信协议，但前提是正确实施。本文通过调查分析和实践验证，审慎且务实地分析了物联网低功耗蓝牙安全流程，识别了设备配对相关问题中的安全漏洞，并考虑了针对威胁和攻击所采取的安全措施；这些威胁和攻击是在制定具体安全措施时，依据威胁建模及本文所提供的分析确定的。对系统应用安全控制措施可能会引入其他问题，包括密钥管理。因此，重建系统后，必须重复本文所述的方法，以评估安全系统的安全性。

致谢

作者谨此感谢复杂与非线性动力系统卓越中心（CoE）（CNDS）、VJTI及其成员为我们的项目提供了大力支持和平台。

参考文献

[1] W. Albazrqaoe、J. Huang 和 G. Xing，“实用蓝牙流量嗅探系统：设计、实现与对策”，载于《IEEE/ACM网络学报》，第27卷第1期，第71–84页，2018年2月。 2019, 10 1109 2018 2880970 DOI：。/TNET。。S. R. Hussain、S. Mehnaz、S. Nirjon 和 E. Bertino，“面向未经修改的物联网设备的安全无缝低功耗蓝牙连接迁移”，载于《IEEE移动计算汇刊》，第17卷第4期，第927–944页，2018年4月1日，DOI：10.1109/TMC.2017.2739742。[3] Zhang、Yue、Jian Weng、Rajib Dey 和 Xinwen Fu。“蓝牙低功耗（BLE）安全与隐私。”（2019）。[4] Peppet, Scott R.，《物联网监管：管理歧视、隐私、安全与同意的第一步》（2014年3月1日）。《得克萨斯法律评论》，即将刊载，SSRN可获取：https://ssrn.com/abstract=2409074[5] Padgette, J.、Scarfone, K. 和 Chen, L.（2017）。《蓝牙安全指南》。NIST特别出版物，800，121。[6] Melamed, Tal。“针对蓝牙智能设备的主动中间人攻击。”《安全与安保工程国际期刊》8（ 2018 200 211 ）：-

V. Hassija、V. Chamola、V. Saxena、D. Jain、P. Goyal 和 B. Sikdar，“物联网安全综述：应用领域、安全威胁与解决方案架构”，《IEEE Access》，第7卷，第82721–82743页，2019年。[8]《物联网监管：管理歧视、隐私、安全与同意的第一步》，Scott R. Peppet 著，即将刊载于《得克萨斯法律评论》（2014年）。[9] Y. Prakash、V. Biradar、S. Vincent、M. Martin 和 A. Jadhav，“智能低功耗蓝牙安全系统”，载于《无线通信、信号处理与网络国际会议论文集》，印度钦奈，2017年3月，第2141–2146页。[10] S. Sarkar、J. Liu 和 E. Jovanov，“实时嗅探BLE长期连接的鲁棒算法”，载于《IEEE全球通信大会》（GLOBECOM）论文集，美国夏威夷州威可洛亚，2019年12月，第1–6页。[11] M. A. Albahar、K. Haataja 和 P. Toivanen，“蓝牙中间人攻击漏洞：文献综述、新型攻击场景、新型对策与经验教训”，《信息技术安全国际期刊》，第8卷第4期，第25–49页，2016年。[12] A. A. Pammi，“基于BLE的物联网设备的威胁、对策与研究趋势”，硕士论文，计算机科学系，美国亚利桑那州立大学，美国坦佩，2017年。[13] C. Zuo、H. Wen、Z. Lin 和 Y. Zhang，“利用移动应用中的静态UUID自动识别易受攻击的BLE物联网设备指纹”，载于《ACM SIGSAC计算机与通信安全会议》论文集，英国伦敦，2019年11月，第1469–1483页。[14] A. Barua、M. A. Al Alamin、M. S. Hossain 和 E. Hossain，“物联网与可穿戴设备中的低功耗蓝牙安全与隐私威胁：综合综述”，载于《IEEE通信学会开放期刊》，第3卷，第251–281页，2022年，doi：10.1109/OJ-COMS.2022.3149732。[15] “Ubertooth One。”Great Scott Gadgets。2020年。 [在线]。可访问：https://greatscottgadgets.com/ubertoothone/（访问日期：2020年7月17日）。[16] “Bluefruit LE Sniffer。”Adafruit。（在线）。：https://www.adafruit.com/product/2269。[17] G. Celosia 和 M. Cunche，“基于通用属性配置文件的蓝牙低功耗设备指纹识别”，载于《第二届互联网事物安全与隐私国际ACM研讨会》论文集，英国伦敦，2019年11月，第24–31页。[18] S. Soderi，“Polar低功耗蓝牙心率传感器的网络安全评估”，载于《EAI身体区域网络国际会议》论文集，意大利佛罗伦萨，2019年11月，第252–265页。[19] S.-C. Cha、M.-S. Chuang、K.-H. Yeh、Z.-J. Huang 和 C. Su，“帮助用户与附近BLE设备达成同意的用户友好型隐私框架”，《IEEE Access》，第6卷，第20779–20787页，2018年。[20] BLESA：针对低功耗蓝牙重连的欺骗攻击 Jianliang Wu、Yuhong Nan、Vireshwar Kumar、Dave Tian、Antonio Bianchi、Mathias Payer、Dongyan Xu 2018年8月[21] 2019 2020 Sevier, Seth 和 Tekeoglu, Ali（）。《低功耗蓝牙安全性分析》。第1–5页。10.23919/ELINFOCOM.2019.8706457。[22] M. E. Garbelini、S. Chattopadhyay 和 C. Wang，“Sweyn-Tooth：在低功耗蓝牙上释放混乱”，载于《LL加密过程、信道》，第37卷，USENIX协会，2020年，第39–40页。