无线网络窃听威胁及检测技术进展*

王振东,任晨辉,安 洁,张骞允,刘建伟
(北京航空航天大学 网络空间安全学院,北京 100191)

摘 要:随着无线通信技术的迅速发展,无线网络规模急剧增大,当前无线网络的安全威胁形势日益严峻。面向最为常见的无线网络窃听攻击,深入探讨了这类安全威胁的现状和相关检测技术的研究进展,具体分析了主动窃听攻击与被动窃听攻击的两大类窃听检测方法的技术原理及优缺点。同时针对基于本振泄露的被动无线窃听装置检测方法提出了一种软件无线电实现方案,测试了该系统在不同条件下对无线窃听装置的检测性能,验证了 WiFi 无线网络中隐藏式被动窃听装置的检测能力。

关键词:无线网络安全;无线窃听;本振泄露;软件无线电
中图分类号:TP393 文献标识码:A DOI:10.19358/j.issn.2097-1788.2023.01.003
引用格式:王振东,任晨辉,安洁,等. 无线网络窃听威胁及检测技术进展[J].网络安全与数据治理,2023,42(1):23-30.

A survey on wireless eavesdropping threats and countermeasures

Wang Zhendong, Ren Chenhui, An Jie, Zhang Qianyun, Liu Jianwei
(School of Cyber Science and Technology, Beihang University, Beijing 100191, China)

Abstract: With the rapid development of wireless communication technology, the scale of wireless networks is increasing dramatically, while the security attacks against wireless networks become more frequent and difficult to counter. This paper investigates the development status of wireless eavesdropping technology faced by wireless networks. The paper analyzes the operation principles, pros, and cons of the eavesdropping detection methods against active and passive eavesdropping attacks. Meanwhile, a software-defined radio(SDR) implementation of wireless passive eavesdroppers detection approach based on local oscillator leakage is proposed. The detection performance under different conditions is presented, and it demonstrates the validity of detecting hidden passive eavesdropping devices in WiFi networks.

Key words: wireless network security; wireless eavesdropping; local oscillator leakage; software-defined radio

0 引言

近年来随着 5G 通信和物联网等技术的发展,无线设备和无线网络的规模急剧增加。在为大众的日常生活提供极大便利的同时,无线通信也面临着严峻的安全问题[1]。由于无线信号的开放性和无界性,针对无线网络的攻击越来越频繁,防御难度也越来越大。在众多无线网络攻击中,窃听攻击较为隐蔽,其危害不容小觑。窃听攻击不仅对国家秘密和国家安全造成极大威胁,而且关系到商业机密和个人隐私。防范窃听威胁、开展针对窃听攻击的防御和检测技术研究具有十分重要的现实意义与迫切的工程应用需求。

现阶段对窃听攻击的防御手段大部分依赖密码学方案,通过加密等密码学技术保护消息的机密性[2]。然而密码学方案增加了消息的大小和通信链路的负担,造成了较大的传输延时。为了保证较低的传输延时和计算开销,实际的无线设备往往采用安全强度较低的密码学方案,无法有效防御窃听攻击。另外,一些算力受限的无线终端设备由于无法进行复杂运算而没有部署密码学方案,容易受到窃听攻击的威胁。与基于密码学方案的被动防御手段相比,窃听检测方法研究针对无线窃听器的主动防御技术,近年来受到更为广泛的关注。

本文介绍了无线网络的窃听威胁分类,依据具

* 基金项目:国家自然科学基金青年科学基金项目(61901020);青年人才托举工程(2021QNRC001)

体的基于原理,分类讨论了主动窃听攻击和被动窃听攻击两类威胁模型,其中被动窃听攻击方式仅从无线网络中接收无线信号,而不发射任何电磁信号,因此具有更强的隐蔽性。针对这两类窃听攻击手段,本文详细讨论了具体窃听检测方法及其优缺点,并重点综述目前研究相对较少、检测难度更大的被动窃听攻击的检测技术。在此基础上,深入讨论了一种基于本振泄露检测原理的隐藏式无线窃听检测系统设计与软件无线电设计,以实现正常无线网络环境中的隐藏式窃听装置检测。

1 无线网络的主要窃听威胁

无线窃听攻击主要利用了电磁波在自由空间中的传输的无界性与无线网络的开放性,只要窃听攻击方将窃听设备调至合适的频率,窃听设备就可以接收无线网络中合法用户传输的信号[3]。根据窃听设备在窃听过程中是否会发射无线信号,可以将窃听攻击分为主动窃听和被动窃听。表 1 列出了多种窃听攻击方法的无线攻击信号及攻击特点。

1.1 主动窃听攻击

如图 1 所示,主动窃听者除了接收合法通信信号,还会向外传输攻击信号。主动窃听攻击方式一般可依据窃听者传输的攻击信号种类及其攻击目的进行分类:一是噪声干扰,窃听者将人为的干扰信号注入通信网络,干扰信号可降低合法通信信道质量,使得合法发送方降低通信传输速率,从而缩减其与接收方之间的信道容量,此种方式没有牺牲合法发送方与窃听者之间的信道容量,有利于实现窃听攻击[4];二是建设性欺骗中继,当窃听信道状态较合法通信信道好时,窃听者将建设性信号发送给合法接收方[5],以增大通信速率,利于窃听者窃取更多信息;三是导频欺骗,窃听者截获合法接收方的导频序列并重放给合法发送方,这种方式让合法发送方不仅在估计合法信道状态时产生失误,还在根据估计出的合法信道而设计预编码矩阵时偏向窃听者,使窃听者更易窃取信息[6]。

图 1 主动窃听威胁模型示意图

1.2 被动窃听攻击

如图 2 所示,在无线网络中,被动窃听者仅接收信号,而不发射任何攻击无线信号。由于无线传播介质的开放性和共享性,被动窃听者可以监测正常合法通信过程,截获合法传输信号,从中获取信息,以达到其恶意攻击的目的。由于被动窃听者不会主动向外发送信号,以致环境中不会存在区别于合法信号的异常信号,增加了检测窃听器的难度。相应地,这也会使窃听攻击处于被动状态。一些主动窃听可通过注入合适的信号来达到改善信道状态、提高成功实施窃听攻击机率的目的,而被动窃听只能依赖于初始的信道质量,一旦窃听信道状态劣于合法信道,被动窃听者就难以成功实施攻击[4]。因此,被动窃听攻击设计通常会隐蔽地部署在距离合法节点较近的位置来提高信道质量,从而提高窃听攻击的成功率。

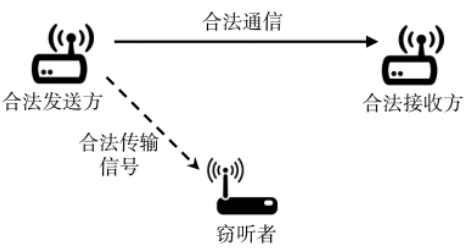

图 2 被动窃听威胁模型示意图

表 1 窃听攻击方法对比

窃听攻击方法	发射的无线攻击信号	技术特点
基于噪声干扰的主动窃听攻击	噪声信号	当窃听信道状态较差时,可降低合法方之间的通信速率
基于建设性欺骗中继的主动窃听攻击	建设性信号	当窃听信道状态较合法信道好时,可增大窃听者与发送方之间的通信速率
基于导频欺骗的主动窃听攻击	导频信号	令合法发送方在合法信道估计时产生失误,并且在设计预编码矩阵时偏向窃听者
被动攻击	不发射攻击信号	只进行信号接收,不主动发射信号,隐蔽性强

2 窃听检测技术研究现状

2.1 针对主动窃听的检测方法

由于主动窃听者主动发射无线电磁信号，除了窃听网络中传播的信息外还可能恶意地干扰正常通信。对于主动窃听器的检测，其目的主要是识别并防范窃听攻击，因此这类无线窃听攻击的检测可以通过检测无线信道中的异常信号来判决。

目前，主动窃听的方式主要有导频欺骗式窃听和噪声干扰式窃听，对于主动窃听器的检测技术研究也大多集中在这两个方向。针对导频欺骗式窃听，有学者提出利用已知的相移键控符号来代替导频符号并进一步通过相位检测来防范主动攻击[7]；另外，Xiong 等人设计了一种接收信号能量比(Energy Ratio Detection，ERD)探测器，通过探测发射器和合法接收器之间信号功率水平不对称性来识别导频欺骗攻击[8]；Tugnait 等人在合法接收器的导频序列上又叠加了一个随机序列，结合一种最小描述长度(Minimum Description Length，MDL)算法来检测主动窃听器的存在[9]。伴随着无线通信系统的进步，大规模多输入多输出(Massive Multiple-Input Multiple-Output，massive MIMO)技术的普及，在此基础上苑坤鹏等人提出了一种通过添加随机导频并运用高维信源计数算法的主动窃听器检测技术[10]；类似地，徐丽采用基于大维随机矩阵理论的方法实现了在大规模 MIMO 系统中检测主动窃听器的存在[11]。针对噪声干扰式窃听，由于干扰器的存在会影响信号强度的分布，Xu 等人提出可以通过检测信号强度并进一步识别主动窃听器[12]；另外，通过频域-时域转换，Lv 等人设计了一种基于时频分布的时变干扰检测方法[13]。整体来说，随着无线信道估计与信号检测技术的长足进步，主动窃听攻击检测手段日益丰富，检测能力已经获得了长足进步。

2.2 针对被动窃听的检测方法

相比于主动窃听器，被动窃听器只是被动接收无线环境中的信号而不会主动发射信号，这就导致难以运用检测主动窃听攻击的手段来检测被动窃听攻击。目前检测被动窃听装置的研究发表较少，从已发表文献来看，被动窃听装置的检测原理主要有近场感应耦合、特征电磁辐射检测以及本振泄露检测三大类。

2.2.1 基于近场感应耦合效应的检测方法

当接收天线和发射天线之间的距离小于所发射的电磁波波长时就会产生感应耦合现象，此时窃听装置天线的存在会使合法用户之间的传递函数失谐，基于该特性，Varshney 等人[14]提出了一种在近场感应耦合通信的环境下(例如射频识别)检测窃听器的方法。他们认为，感应耦合信道及传递函数可以利用相关几何构造和发射器、接收器的特性来计算，而除了合法通信方外，环境中的窃听设备也会参与耦合从而改变原本的传递函数，导致系统失谐。利用这一原理，就可以通过对比有无窃听器时解码的错误率来判断是否存在窃听设备。

但是这种方案是建立在合法通信方之间可获得不存在窃听器时的信道参数的基础上，在现实环境中，这是很难做到的。并且，在实际的无线通信应用中，通信往往是在远场条件下进行。常见的短距离无线通信传输距离如表 2 所示，表中的 Bluetooth、ZigBee 和 WiFi 为远场通信技术。由于窃听器的存在并不会明显地改变发射器和接收器之间的无线信道以及传递函数，远场通信场景下无法使用基于近场感应耦合效应的检测方法。

表 2 常见的短距离无线通信传输距离

无线技术	NFC	RFID	Bluetooth	ZigBee	WiFi
传输距离	<10 cm	5~10 m	10~20 m	10~100 m	300 m

2.2.2 基于特征电磁辐射的检测方法

通信设备中普遍存在的集成电路或芯片都会随着其传输或者处理的信号内容变化，产生微弱的电磁辐射。若无线环境中存在着窃听设备，当其接收特定的信息并对其进行处理时就会产生具有独特时频特征的电磁辐射，因此可以通过检测具备已知特征的电磁辐射来判断被动窃听装置的存在。

目前已有学者基于这一原理进行被动窃听装置的检测技术研究，包括对刺激信号触发电磁辐射的讨论并验证通过电磁辐射特性检测被动窃听器存在的可能[15]；对不同的检测方法进行对比、结合滤波器运用数字信号处理的方法将电磁辐射的检测数据转换为声信号来暴露窃听器的存在等尝试[16]。

除了上述工作之外，被动窃听器必须将接收到的数据进行写入操作，此时内存芯片会产生相应的电磁辐射，Shen 等人基于此设计了 EarFisher 检测系统[17]。他们通过广播特定的数据包来刺激隐藏的窃听装置并检测窃听设备将接收到的数据写入时所

产生的电磁辐射来探测窃听器的存在。测试结果表明,EarFisher 可以在复杂的信号条件下排除一定的干扰并准确地检测出窃听设备,同时还具有良好的自适应性。

然而电子设备在受到刺激时所产生的电磁辐射信号通常十分微弱,且局限于特定的芯片或者电路结构,导致对窃听设备的检测难以获得广泛应用,并且在大部分的研究中难以高效区分出合法接收设备和隐藏的窃听设备,在检测成本和系统复杂度上仍存在诸多提升空间。

2.2.3 基于本振泄露的检测方法

隐藏式窃听器作为一个无线接收机,在技术原理与硬件实现上通常具有与合法接收机相同的电路组成。如图 3 所示,以超外差接收机为例,每个发射器和接收机都有本地振荡器,本地振荡器将直流电转换成具有一定频率、振幅等的交流信号,这些信号在发射器内可作为载波信号将基带信号调制成适合射频无线传输的信号,而在接收机中则通常与接收信号经过混频器解调出基带信号。依据电磁辐射特性,本地振荡器工作时生成的本振信号除了会通过预期传导路径,比如混频器中本振信号的输入口,还会经其他路径到达天线向空间辐射。本振信号通过非预期传导路径的产生辐射效应的行为称作本振泄露。本振泄露是难以避免的,具有本地振荡器的设备在工作时一般都会产生本振泄露,因此可以通过检测环境中的本振泄露信号来检测附近的发射机或接收机。另外,由于硬件层面的制造工艺存在一定的误差,不同设备间的本地振荡器频率一般不同,因此它们的本振泄露信号也存在微小的频率差异,可以通过频域分析方法同时对多个接收机进行检测和识别。

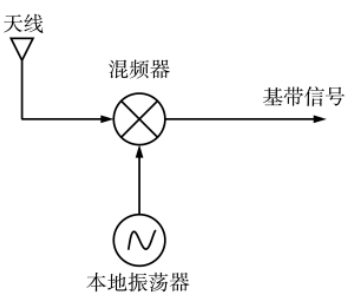

图 3 含本地振荡器的超外差接收机原理示意图

Wild 和 Ramchandran 首先探究了如何利用本振泄露来检测无线接收机,他们利用已有的组件设计了一个检测器,然后将一个电视接收机作为被检测设备并最终验证了通过本振泄露来判断无线接收机存在的可能[18]。此外,Park 等人提出了一种通过检测接收机本振泄露来识别超宽带(Ultra Wide Band,UWB)全球微波接入互操作性移动终端(WiMAX MT)设备的技术[19]。他们指出,当 UWB 设备在传输之前扫描 UWB 通信范围内占用的 WiMAX 频段时,该项技术是十分有效的。随后,他们还利用傅里叶变换对该项技术进行了后续的探索与优化,进一步提高了对接收机本振泄露检测的精度。Mukherjee 等人讨论了如何在 MIMO 系统中利用本振泄露来检测被动窃听器[20]。并且,他们还分析了非相干能量检测以及最佳相干检测的性能,展示了如何利用所提出的方案来提高信道的保密效果。但是作者只对这项技术进行了理论上的演示,他们假设在对窃听器进行检测的过程中需要环境中的其他合法通信方暂停通信,这在现实中是难以实现的。Chaman 等人进一步研究了合法通信信号存在的情况下本振泄露的检测问题,通过消除子载波旁瓣伪影、空域消除合法通信信号等手段实现对窃听器的检测[21]。

虽然本振泄露普遍存在且可以将其作为检测窃听器的一个手段,但在实际环境中,本振泄露的信号强度一般都比较低,从而限制了窃听器的可检测距离。如果本振泄露的功率过小,环境噪声会将本振泄露信号淹没,使得基于本振泄露的检测方法失效。另外,在正常的通信环境中,传输信号和其他合法通信设备的本振泄露也会对窃听器的本振检测带来困难。

3 基于软件无线电的本振泄露窃听检测系统

如前文所述,在被动窃听器的检测方法中,基于近场感应耦合效应检测和基于电磁辐射检测的方法都存在比较大的限制条件。基于近场感应耦合效应的检测距离受限于窃听器的工作频率和天线结构。以 2.4 GHz 频段为例,工作频率为 2.4 GHz 的小型化天线的近场区距离往往小于 1 cm,因此这类方法检测难度较大。而现有基于电磁辐射的检测方法要求窃听器中具有特定的芯片和电路,因此这类方法适用范围存在限制。另一方面,天线和本地振荡器作为现阶段无线接收装置的必备组成部分,通过检测本振泄露来判断窃听装置的存在性是一种通用的方案。本文从本振泄露出发,以 WiFi 频段无线窃听装置检测为例,介绍了一种基于软件无线电

装置的无线窃听器检测系统，能够在成本可控的同时以比较高的准确率检测出微弱的本振信号，从而实现了对隐藏式无线窃听装置的无损检测。

3.1 系统架构与处理流程

该系统的架构如图 4 所示，硬件层使用 USRP 软件无线电设备接收环境信号；数据采集层采集数据并对数据进行预处理；信号处理层对数据采集层的信号进行频域伪影消除、空间对消和环境噪声消除；应用服务层为前端 GUI，与用户进行交互，根据用户需要显示窃听者数量、信号源数量和处理后的时域频域波形图。

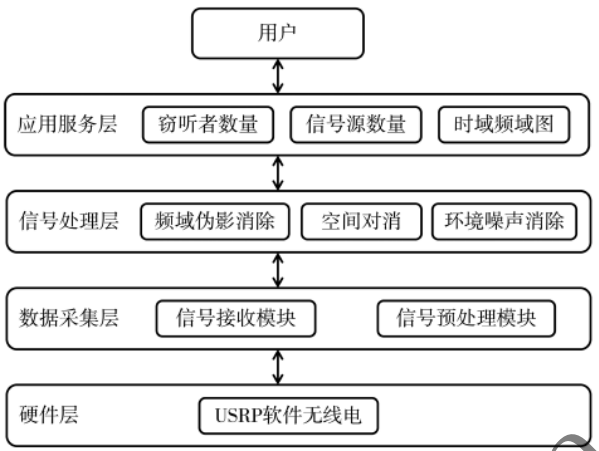

图 4 窃听检测系统架构

其中，信号处理层为该系统的主要模块，该模块的功能是消除接收信号中的合法通信信号。首先，该模块通过加权最小二乘法最小化误差函数计算信号子载波的频率与复振幅，并进一步重构出通信信号，再利用重构信号与接收信号在频域维度消除由信号不连续性引起的伪影和杂散频率。除此之外，在空域维度，该模块使用基于先验信道的载频对消技术消除直流窗口中剩余合法发射机的信号。最后再将所有消除后的样本组合进行大时间窗快速傅里叶变换，通过长时相参积累削弱环境噪声的影响。经过上述处理，该模块暴露了窃听器的本振信号并将分析结果传递给应用服务层。

该系统的工作流程如下：首先使用 USRP 软件无线电接收环境中的 WiFi 信号，然后用 GNU Radio 3.9 对信号进行预处理，处理后的数据传入 MATLAB 中进行频域伪影消除、空间对消、环境噪声消除，经过上述处理，发射机的合法信号被消除，噪声影响也被降低，窃听者的本振泄漏信号被暴露出来，系统就可以在应用服务层输出结果，用户就可以获得目标环境的无线窃听器检测报告。

3.2 系统实现

使用 USRP X310 软件无线电实现了该系统并配置 A、B 两根天线接收环境中的信号，然后用电脑对接收到的信号进行处理，系统配置如表 3 所示。

表 3 系统配置表

项目	配置
系统硬件	USRP X310
操作系统	Ubuntu20.04
系统软件	GNU Radio 3.9、MATLAB
处理器	英特尔酷睿 8250U

首先为了验证检测网卡本振泄露的可行性，对实验使用的电脑网卡进行了测试。表 4 显示了将网卡中心频率设置为 5.7 GHz 时，网卡的本振泄露的泄露频率和信噪比。

表 4 网卡本振泄露频率及信噪比

网卡型号	本振泄露频率/GHz	监听信道/信道频段/GHz	信噪比/dB
AX201	3.648	140/5.7	37.820 3
QCA6174	3.647、3.649	149/5.745	60.646 4
QCA9377	3.648	140/5.7	63.453 1

除了使用网卡外，攻击者也可以使用 USRP 软件无线电进行窃听。使用 USRP 作为窃听器的优势在于攻击者可以自主调节监听频段，并在软件中解码接收到的信号。为了在不同的频率下工作，USRP 软件无线电需要使用支持工作频率范围的 RF 子板，其本振泄漏位于中心频率处。

基于此，使用一台 USRP B210作为发射机，传输标准的 WiFi 数据包，同时使用两台 USRP B210 分别作为接收机和窃听器进行实验。为了减小干扰，在 5.08 GHz 下进行实验，并在这个条件下收集到了该系统性能的基准结果，然后进一步在不同信噪比下进行了性能测试来继续探究该系统工作的信噪比范围。

3.3 功能测试及分析

功能测试的目的为确定该系统能否正确检测出通信环境中窃听器的本振信号。

在进行正式无线通信环境下对窃听器检测的实验前，首先进行了有线通信环境下的预检测，其实

验测试环境如图 5 所示,通过同轴线连接信号发射机以及窃听装置,并布置该窃听器检测系统进行检测。有线通信相较于正常的无线通信环境噪声更小,可以有效验证该系统功能的正确性。经过测试,成功实现了在有线环境下对于窃听器泄露的本振信号的检测从而证明窃听器存在,系统处理过后的图像如图 6 所示,能够明显看到窃听器的本振泄露信号所形成的尖峰,初步验证了该系统能够检测本振信号。

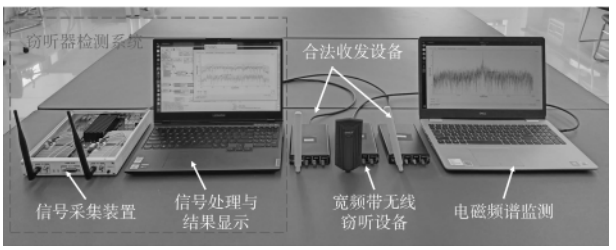

图 5 有线环境测试实验图

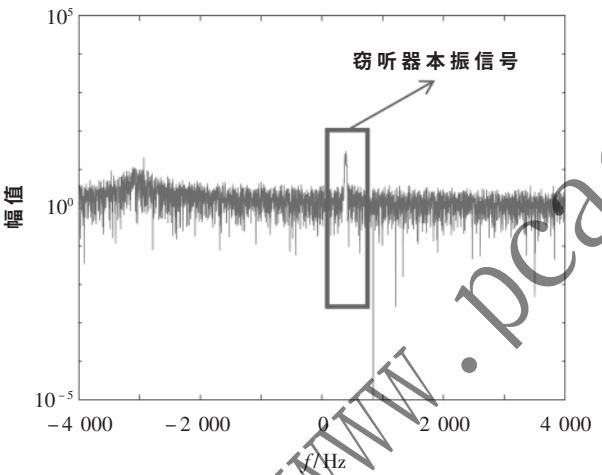

图 6 有线环境下窃听器本振信号

无线通信环境下的测试实验如图 7 所示,其中发射机正常发射信号,窃听器进行窃听,合法接收机正常接收信号,该检测系统接收环境中的信号并进行频域消除、空间对消等处理,处理后的结果如图 8 所示,可以明显看到两个峰值,这代表着成功消除了通信信号,暴露出了环境中的窃听器本振信号和合法接收机本振信号,证明了窃听者的存在。

通过在无线环境中进行实验,证明该系统可以在合法发射机和合法接收机进行正常通信的条件下实现对窃听器的检测,验证了本方案在实际应用中功能的正确性。

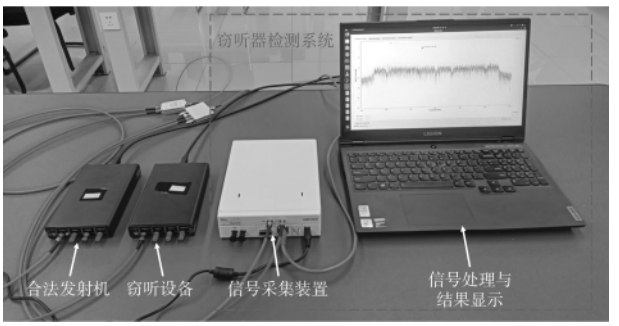

图 7 无线环境测试实验图

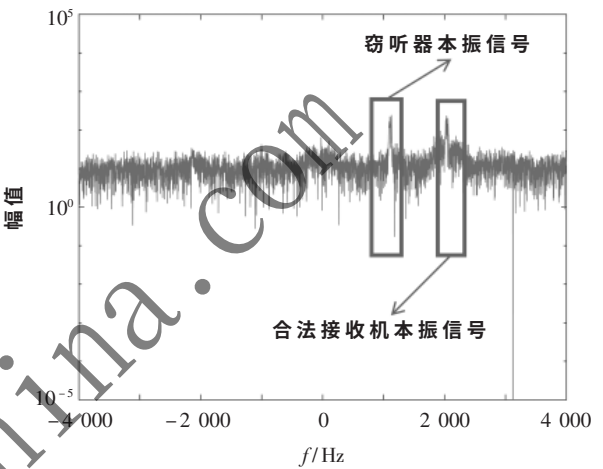

图 8 无线环境下窃听器和合法接收机本振信号

3.4 性能测试及分析

考虑到窃听器工作的复杂通信环境,需要对该系统在不同信噪比下的性能进行检测,并确定本方案的工作环境的信噪比。测试了有线通信环境中 48 dB、43 dB、38 dB、26 dB、25 dB、20 dB 信噪比下本方案的工作效果,以及无线环境下 48 dB 和 45 dB 信噪比下本方案的工作效果,结果如表 5 所示。

经过测试,在有线信道中信噪比大于 25 dB 时该

表 5 不同信噪比下检测性能表

有/无线环境	窃听器接收信噪比/dB	是否成功检测
有线环境	48	是
有线环境	43	是
有线环境	38	是
有线环境	26	是
有线环境	25	是
有线环境	20	否
无线环境	48	是
无线环境	45	是
无线环境	43	否

系统有很好的检测成功率，当信噪比小于 25 dB 时，空间对消处理后的结果难以判断窃听器的本振信号，对于窃听器的检测难度较大，因此可以认为有线通信环境中25 dB 信噪比为本方案的边界环境。

无线通信环境下该系统的性能表现更加值得关注。为了简化实验，在进行无线环境下的性能测试时并不部署合法接收机，实验结果表明，在环境中存在窃听器和该检测系统，且合法发射机正常发射信号(信噪比为 48 dB)的条件下，对收集到的数据进行处理后的图像可以非常清晰地分辨出窃听器的本振信号。在信噪比为 45 dB、窃听器距离 1 m 的条件下，对数据进行处理后的图像如图 9 所示，可以清晰地看到此时窃听器的本振信号。

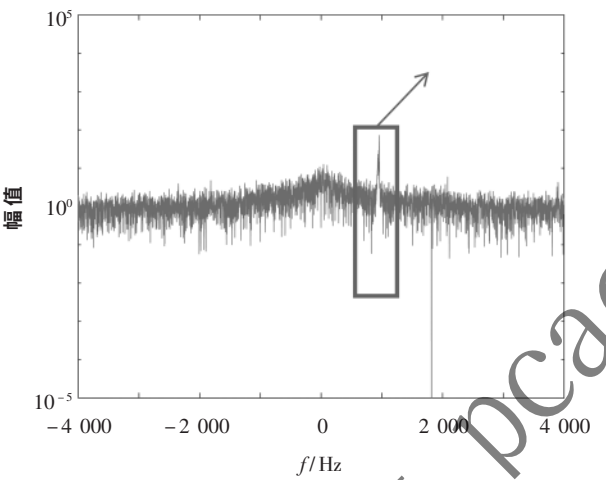

图 9　信噪比 45 dB 下窃听器本振信号

但在低于 45 dB 的信噪比下，空间对消处理后的结果难以判断窃听器的本振信号，对于窃听器本振泄露的检测难度大。通过上述实验结果，该系统可以在实际的无线通信环境中在高于 45 dB 的条件下较好地提取无线窃听器的本振泄露，并以 95% 的正确率检测到 1 m 范围的窃听器，且允许环境中有其他合法通信者可以进行正常通信。

需要指出的是，由于本振泄露功率微弱，可以预见随着检测距离的不断增加，基于检测本振泄露原理的这类窃听装置检测手段在检测距离上仍存在本质上的困难。面向真正意义上的远距离无损检测，仍需在原理上提出更为新颖的方案。

4 结论

随着无线通信规模的快速发展，无线网络的安全问题越来越突出。针对无线网络的窃听威胁严重危害到国家安全、商业机密和个人隐私，研究针对无线窃听器的检测技术具有重大的意义。无线窃听威胁主要包括主动窃听攻击和被动窃听攻击。针对被动窃听攻击的检测方法主要有三类，分别是基于电磁泄露的检测方法、基于近场感应耦合效应的检测方法和基于本振泄露的检测方法。目前，基于本振泄露的检测方法相比而言具有更好的通用性和较高的检测性能。本文以 WiFi 频段的隐藏式窃听装置为例，介绍了一种基于本振泄露原理的窃听检测软件无线电实现方案，验证了隐藏式被动窃听装置检测方法的可行性。通过对硬件系统设计和信号处理算法的进一步优化，有望进一步提高该方法的检测性能，实现更具工程实用性的隐藏式被动无线窃听装置的无损检测。面向未来更远距离条件下的被动窃听装置无损检测，仍需在检测原理上有所突破，利用无线接收机的独有特点，提出新型检测方案，实现这类隐蔽程度高、危害程度大的被动窃听攻击的有效应对。

参考文献

[1] BURG A, CHATTOPADHYAY A, LAM K Y. Wireless communication and security issues for cyber-physical systems and the Internet-of-Things[J]. Proceedings of the IEEE, 2017, 106(1): 38-60.

[2] ZOU Y, ZHU J, WANG X, et al. A survey on wireless security: technical challenges, recent advances, and future trends[J]. Proceedings of the IEEE, 2016, 104(9): 1727-1765.

[3] SALAHDINE F, KAABOUCH N. Security threats, detection, and countermeasures for physical layer in cognitive radio networks: a survey[J]. Physical Communication, 2020, 39: 101001.

[4] 闫莲. 基于物理层安全技术的主动窃听策略研究[D]. 重庆: 重庆大学, 2021.

[5] ZENG Y, ZHANG R. Active eavesdropping via spoofing relay attack[C]//2016 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). IEEE, 2016: 2159-2163.

[6] 刘尊宁. 针对主动窃听的物理层安全研究[D]. 北京: 北京邮电大学, 2018.

[7] KAPETANOVIĆ D, ZHENG G, WONG K K, et al. Detection of pilot contamination attack using random training and massive MIMO[C]//2013 IEEE 24th Annual International Symposium on Personal, Indoor, and Mobile

Radio Communications(PIMRC).IEEE,2013:13-18.

[8] XIONG Q,LIANG Y C,LI K H,et al.An energy-ratio-based approach for detecting pilot spoofing attack in multiple-antenna systems[J].IEEE Transactions on Information Forensics and Security,2015,10(5):932-940.

[9] TUGNAIT J K.Self-contamination for detection of pilot contamination attack in multiple antenna systems[J].IEEE Wireless Communications Letters,2015,4(5):525-528.

[10] 苑坤鹏.大规模MIMO中主动窃听安全问题研究[D].北京:北京邮电大学,2018.

[11] 徐丽.基于随机矩阵理论的大规模MIMO系统窃听用户检测研究[D].北京:北京交通大学,2019.

[12] XU W,TRAPPE W,ZHANG Y,et al.The feasibility of launching and detecting jamming attacks in wireless networks[C]//Proceedings of the 6th ACM International Symposium on Mobile ad Hoc Networking and Computing,2005:46-57.

[13] LV Q,QIN H.An improved method based on time-frequency distribution to detect time-varying interference for GNSS receivers with single antenna[J].IEEE Access,2019,7:38608-38617.

[14] VARSHNEY L R,GROVER P,SAHAI A.Securing inductively-coupled communication[C]//2012 Information Theory and Applications Workshop.IEEE,2012:47-53.

[15] SEGUIN S A.Detection of low cost radio frequency receivers based on their unintended electromagnetic emissions and an active stimulation[M].Missouri University of Science and Technology,2009.

[16] SHAIK A,WENG H,DONG X,et al.Matched filter detection and identification of electronic circuits based on their unintentional radiated emissions[C]//2006 IEEE International Symposium on Electromagnetic Compatibility,EMC 2006,2006.

[17] SHEN C,HUANG J.EarFisher:detecting wireless eavesdroppers by stimulating and sensing memory EMR[C]//18th USENIX Symposium on Networked Systems Design and Implementation(NSDI 21),2021:873-886.

[18] WILD B,RAMCHANDRAN K.Detecting primary receivers for cognitive radio applications[C]//First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks,2005.DySPAN 2005.IEEE,2005:124-130.

[19] PARK S,LARSON L E,MILSTEIN L B.Hidden mobile terminal device discovery in a UWB environment[C]//2006 IEEE International Conference on Ultra-Wideband.IEEE,2006:417-421.

[20] MUKHERJEE A,SWINDLEHURST A L.Detecting passive eavesdroppers in the MIMO wiretap channel[C]//2012 IEEE International Conference on Acoustics,Speech and Signal Processing(ICASSP).IEEE,2012:2809-2812.

[21] CHAMAN A,WANG J,SUN J,et al.Ghostbuster:detecting the presence of hidden eavesdroppers[C]//Proceedings of the 24th Annual International Conference on Mobile Computing and Networking,2018:337-351.

(收稿日期:2023-01-01)

作者简介:

王振东(1999-),男,博士研究生,主要研究方向:无线网络安全理论、软件无线电。

任晨辉(2002-),女,本科,主要研究方向:网络空间安全、信息对抗技术。

张骞允(1992-),通信作者,女,博士,副教授,主要研究方向:无线网络安全、智能感知与识别、电磁频谱安全。E-mail:zhangqianyun@buaa.edu.cn。

(上接第22页)

Attribute and simile classifiers for face verification[C]//2009 IEEE 12th International Conference on Computer Vision.IEEE,2009.

[11] HORÉ A,ZIOU D.Image quality metrics:PSNR vs.SSIM[C]//20th International Conference on Pattern Recognition,ICPR 2010,Istanbul,Turkey,23-26 August 2010.IEEE Computer Society,2010.

(收稿日期:2022-12-31)

作者简介:

钱泽凯(2001-),男,本科,主要研究方向:数据质量管理。

童彦澎(2001-),男,本科,主要研究方向:自然语言处理、情感计算。

刘绍辉(1977-),通信作者,男,博士,副教授,主要研究方向:特征表示、机器学习。E-mail:shliu@hit.edu.cn。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部