今天我们小组要汇报的论文题目为窄带系统的射频指纹识别、建模和分类。主要从研究背景、研究方法、实验结果、结论总结四个方面进行汇报。

首先呢物联网 IoT，应该都比较熟悉，IoT 想实现的事情简单来说就是把很多现实生活中的设备连接到互联网中，这需要 IoT 设备具备最主要的三种能力，传感能力，通信能力，以及简单的处理能力。像这个图上很多设备，比如常见的智能手表，到摄像头甚至暖气片都能联网，IoT 的应用也推动了互联医疗、智慧城市、智慧兵装的发展。

IoT 刚才提到比较重要的概念是得有通信的能力，没有通信就无法组成网络。从通信的角度来说，目前为止，有很多种无线通信协议，比较熟悉的就是与手机相关 Cellular 相关的通信，从 2G 到现在的 5G，或者 WIFI 和蓝牙。其他的像智能家居中的 Zigbee，智能抄表中 NB-IoT，而这篇论文他们主要基于 Lora 设备进行实验。

对于上面提到所有 IoT 技术，都有一个最大的问题没有解决，就是安全问题。这里列了一些 1617 年比较久远的案例。第一个是在医用设备上，比如心脏起搏器，它其实是有无线通信功能的，有研究人员发现，他的加密算法做得比较差，容易被破解；第二个是大众汽车，现在很多车都能无线解锁，靠近车辆就会打开，研究人员破解了解锁车辆的无线信号；第三个是 wifi 的协议漏洞。

那么从物理层安全的角度，主要有两个方面，一个是验证一个是加密，他们这次研究主要针对验证。

传统的验证方法通常是基于密码学的，一个是挑战应答认证，分为对称密钥和公私钥，另一个是设备身份认证。对于对称加密系统，他的问题在于它没有办法很方便的分享一个密码，在物理层很难实现。对于公私钥系统，从计算的角度

非常复杂，简单 IoT 设备不一定有充足的计算资源。对于设备身份信息一般是基于设备的软件地址如 MAC、IP 地址，而这些地址很容易被篡改。

那么有没有一种安全的、不是基于密码学的验证技术？首先先简单介绍一下生物指纹，比如手机的指纹解锁分为两步，录入指纹信息和识别指纹，而这项技术依赖的原理是每个人的生物指纹是独一无二的。那么无线设备，IoT 设备是不是也存在一个独一无二的特征。

事实上，每一个无线射频设备都有独一无二的指纹，叫做 RFF 射频指纹。RFF 独一无二是由于制造工艺的原因，使硬件特性与标准值存在偏差，会对无线传输信号产生轻微影响。由于这些影响唯一、稳定且难以篡改、模仿和克隆的特性，在民用和军用领域有着广阔的应用前景。

可以增强无线网络安全、保护数据隐私、提高全球定位系统、广播自动相关监视系统等关键民用领域的抗欺骗能力。也可以提升电子情报侦察和电磁频谱态势感知等能力，是未来认知电子战、电子侦察、综合频管等领域的关键支撑技术。

在此次研究中，他们主要采用深度学习的方法对设备信息进行训练和推理。就像生物指纹识别的原理一样，射频指纹的识别也主要分为两步，首先接收不同设备发出的信号，传入深度神经网络进行学习，之后对于一个未知设备发出信号，只需要传入推理机就能对设备进行认证。这篇文章中，他们使用了一个比较经典的 CNN 模型，主要根据 AlexNET 进行微调。

从无线的角度来说，接收信号 yt 可以写成上面的公式，DUT 是待检测设备，发出 xt 的信号，发送机的硬件特性为 Fk，经过 Fk 的影响后，会和信道进行卷积操作。接收机接收到后，同样受到接收机硬件特性 G 的影响，再加上热噪声 nt，这就是最基本的接收信号的模型。但在这篇论文中，由于实验会固定发送机和接

收机的位置，所以 ht 的影响可以忽略。

对于发送机的硬件失真建模，其实就是上图的 Tx，他们研究主要考虑了三部分的影响，晶振偏差造成的 CFO（载波频率偏移）和相位噪声；混频器造成的增益不平衡和相位不平衡；以及 PA（功率放大器）的非线性。

不同的硬件特性会给星座图带来不同的变化，这里他们使用的是 4 进制的正交振幅调制。可以看到对于 bcd 来说增益不平衡，相位不平衡和功放非线性带来的变化都是稳定的，可以提取出来，相位噪声造成的影响虽然是不稳定的，但是可以看出影响较小，所以他们就忽略了。

而对于 CFO（载波频率偏移），他们研究发现，在不同时间有不同的影响，从图上可以看出对于不同的设备，在不同时间可能表现出相同的特征，这种时变性不适合作为 RFFI 协议的特征，所以他们对该偏移进行了补偿，在后续的实验也证明了补偿之后的信号能提高模型分类的准确度。

对于接收机的硬件失真建模，其实就是之前图上的 Rx，和发送机类似，也有晶振偏差造成的 CFO（载波频率偏移）和相位噪声以及混频器造成的增益和相位不平衡。而对于接收机内部的 LNA 也就是低噪放，在结构上比较稳定，没有像功放那样的非线性特征。

为了研究发送机和接收机硬件失真对模型性能的影响，具体表现为模型预测的准确度，他们做了两组仿真实验。

首先为了研究发送机硬件失真的影响，他们假设使用同一台完美的接收机，并考虑了不同场合进行对照实验。第一次只考虑增益不平衡，第二次只考虑相位不平衡，然后第三次同时考虑增益和相位不平衡，第四次只考虑功放非线性，第五次考虑所有因素。最后得出这个仿真图。

这个图可能看不太清楚，第一幅图的横坐标是发送信号长度，可以看到随着发送信号长度的增加，准确度有明显提升，这能很好解释，信号越长，从中能够提取的硬件信息就越多，就能更好分类。第二幅图的横坐标是信噪比，随着信噪比的提升，信号受影响幅度越小，也很好理解。从纵向看，两幅图的趋势大致一致。仅考虑单个影响因素的分组分类性能都不太理想，而随着多个考虑因素的叠加，模型性能也逐步提高。

对于发送机的实验是固定了相同的接收机，而实际中，不可能只用一台接收机接收信息，所以他们也做了接收机影响的仿真实验。分别考虑没有硬件失真，只考虑增益不平衡、只考虑相位不平衡和都考虑。

结果表明，接收机的不同会影响模型性能。当接收机没有失真，横坐标为 0 时，有较好的性能，但随着相位不平衡和增益不平衡分别增加，模型性能逐渐降低。当两者同时变化时，性能变化就像这样，也很好理解。这里研究了相同的发送信号和随机的发送信号，从模型的最高点也可以看出，采用相同的信号会更好识别一点。

最后，模型性能也会受到待分类设备数量的影响。当射频失真在同一范围内时，模型对更多的设备进行分类会更加困难，因为他们的特征将彼此更接近。

总的来说，他们此次的研究对窄带发送机和接收机的硬件损伤进行了系统建模，并对其对射频指纹识别的影响进行了广泛的实验和仿真验证。具体来说，硬件损伤涉及晶振缺陷、混频器不平衡和功放的非线性。经过他们三个多月的实验发现晶振缺陷并不稳定，并对其进行了补偿。最后，他们根据其他特性设计了 RFFI 协议，达到了较好的分类性能。