实现安全的5G ORAN部署

TECHnalysis Research公司总裁Bob O'Donnell

摘要

在5G网络的演进过程中，向开放式无线接入网络（ORAN）架构的迁移无疑是最吸引人，最激动人心的一个方面。与蜂窝网络中占据主导地位的专有架构不同，基于ORAN的网络采用了来自多个供应商的组件来创建最佳的解决方案，拥有很高的灵活性。这有助于电信公司和其他服务提供商快速应变、降低成本并且更快、更轻松地实现新特性和新技术。但是，放弃单一供应商解决方案也增加了潜在的攻击面，同时可能给关键基础设施带来安全风险。为了避免这些问题，网络设备供应商和服务提供商需要考虑采用哪些必要组件来保护网络和通过网络的数据。一个很容易被忽视的关键器件就是低功耗FPGA，它可以用于实现各种功能，包括硬件可信根、网络功能加速和ORAN环境中的安全通信等。

> 在灵活的ORAN网络架构中采用安全、基于零信任的硬件器件需要注重最微小的细节，而低功耗FPGA可以在各个环节发挥关键作用。
>
> —首席分析师Bob O'Donnell

引言

当今十分复杂的技术需要考虑的最重要的一个方面就是灵活性。无论是把人送入太空、应对自动驾驶的挑战，还是构建5G蜂窝网络的基础设施，硬件设计工程师总是希望组件不仅能够提供所需的功能，还能以多种方式来实现他们的设计目标。这就是FPGA（现场可编程门阵列）在众多此类极其复杂的设计中显得如此重要的原因。这些芯片本身可以进行编程和重新编程，从而可以提供某些关键功能，满足许多先进技术特定和苛刻的需求。

电信网络数十年来一直依赖各种类型的FPGA来完成加速网络、无线传输数据等功能。如今，随着行业开始向ORAN架构过渡，FPGA，尤其是低功耗FPGA，再次证明了其在硬件可信根、多组件同步、实时网络数据包加密和解密等应用中的价值。

然而，在深入了解更多细节之前，我们有必要先回顾一下蜂窝网络是如何发展的，以及虚拟化、软件定义、开放标准驱动的网络等趋势如何创造新的机遇和挑战。

网络的发展

近年来爱立信、诺基亚和三星网络等主要网络设备供应商都构建了非常复杂的专有解决方案，让蜂窝通信和无线数据的影响力遍及全球。除了少数例外，这些设备与其他供应商的设备不具备互操作性，电信供应商的每个区域子网都要依赖单一的解决方案。鉴于RF（射频）信号本身比较复杂以及每一代蜂窝技术提供的功能相对固定，这种模式尽管有很多局限性，但大多数人依然认为这是相对合理的解决方案。事实上，由于这些系统是闭环、专有的，一些人甚至认为它们具有安全优势——因为不必担心私有领域的安全问题。

然而，多种趋势的汇合产生了这样一种概念，即需要一种新的更加灵活、更具适应性的方法来构建蜂窝网络。首先是向5G的过渡，这种网络增加了一系列新频率，增加更多连接到网络的设备的数量和类型，还有潜力显著降低网络数据传输的延迟。此外，在传统的电信环境中，向软件定义架构的转变已经十分明显，某些关键网络硬件组件的解聚合也是如此。例如，上一代网络中手机信号发射塔的标准基带单元被拆分为DU（分布式单元）、CU（控制单元）和RU（无线单元）。随着网络数据流和应用需求的增加，这种新结构可以提供更专业的功能和灵活的架构。

下一代网络对网络切片等功能也提出了新的要求（将单个组织甚至用户的数据包与其他网络通信数字隔离，以减少延迟、提高性能并提供更好的整体服务）。最后，随着更快的通用计算硬件和专用加速器的出现，网络性能需求得到满足，为网络架构的重大转变奠定了基础。

虽然这种转变尚处于早期阶段，但世界各地的电信公司都开始采使用戴尔、HPE和联想等公司的COTS（商用现货）服务器硬件以及微软、IBM和英伟达等主要厂商以及

Mavenir、Altiostar和Accelleran等一众较小企业的软件为来为他们的部分网络提供解决方案。

最初，大多数软件方面的工作都集中在虚拟化网络资源上，正如过去几十年里虚拟化推动了数据中心的发展和架构重组。然而，随着专用软件的开发以及蜂窝网络设备组件之间建立了互连的开放标准，现在可以以全新的方式将蜂窝网络组合在一起。此外还可以利用CI/CD（持续创新/持续交付）和云原生、容器化的软件架构等新的软件开发方法来加快创新步伐。由于电信公司要求极高的可靠性，整个网络转型可能需要十年或更长时间才能完成。第一步已经完成，但是这反过来又引发了新的担忧，即组合使用来自不同供应商组件引发的问题。

保障连接安全

最主要的担心是安全方面的问题。虽然ORAN架构带来了更高的灵活性，但它也大大增加了网络的潜在攻击面。新架构下不仅可以混合使用来自不同供应商的硬件和软件，而且硬件中单独的组件（例如服务器中基于PCI的加速卡）可以有多个选择。因此，网络架构师和硬件设计人员必须考虑每一种可能的连接，确保所有连接安全可靠。此外，设计人员必须确保每个硬件中的基础固件没有遭到篡改。

为实现这一目标，需要针对不同的要求采取多种不同的安全解决方案。第一步就是让每台设备在启动时通过硬件可信根验证其有效性，并确认器件上的固件没有被修改。莱迪思半导体基于Nexus™平台的低功耗、安全FPGA以及Lattice Sentry™解决方案集合可提供平台固件保护恢复（PFR）机制。多年来，硬件公司一直在服务器和其他关键设备中使用这些功能，并且它们也逐步用于ORAN相关的硬件。此外，可以使用硬件可信根确保器件从制造到交付和安装期间没有遭到任何篡改，从而在整个供应链环节避免克隆、伪造、木马植入或任何其他问题。最后，由于这些低功耗FPGA自带加密功能，可以加密和解密进出固件的数据，再次确保了安全执行固件更新。

安全链路的下一步是与硬件中可能连接到主机CPU的任何组件进行安全的通信，或者更简洁地说，是“保护线路（wire）”。在零信任安全模型下，每个组件都需要通过加密消息向主机系统确认其真实性。这就是全新的莱迪思ORAN™解决方案集合发挥作用的地方，它可以通过PCI和其他总线提供安全通信，来连接主机和这些组件。与莱迪思其他的解决方案集合产品一样，莱迪思ORAN是一个全面的解决方案，包括了定制设计服务、参考设计和演示、软件工具、IP核和硬件平台，还针对小型低功耗FPGA进行了优化。该产品旨在便捷地集成到多种硬件设计中，它包括一个可编程的RISC CPU核心，可以实现各种加密和安全通信协议。此外，它在设计上与Lattice Sentry解决方案集合兼容，扩展了所使用的器件的安全特性。

同步数据

除了保护ORAN解决方案中的硬件外，还须确保各个组件发送数据的时间保持同步。正如之前所讨论过的，核心网络组件的解聚合决定了数据同步会是一个担忧。尤其是无线单元（RU）和分布式单元（DU）的拆分带来了新的挑战。对于传统的封闭网络，模拟无线信号在无线组件的天线处接收，然后转换为数字形式。之后对数据执行几个实时数字信号处理步骤，从而实现现代蜂窝网络必不可或缺的一些功能，例如载波聚合——将接受到的不同频率的信号绑定到单个“聚合”的数字数据模块中。在ORAN环境中，也需要执行类似的步骤。

之前的专有系统有一个共享时钟信号来协调这些工作，在ORAN环境中则需要使用IEE1588标准对数据包进行时间戳记，以便它们跨组件同步。

由于FPGA以并行一致的方式运行，它们已在许多不同的应用中充当可靠的时序资源。因此，它们非常适合ORAN网络架构的同步需求，特别是在RU和DU功能拆分的方案中。莱迪思计划在今年扩展ORAN解决方案，纳入此类基于时序的功能。此外莱迪思还将添加定时和同步服务功能，通过标准的eCPRI（增强型通用公共无线接口）链路在RU和DU之间建立前传连接。

此外，由于该连接未受保护，莱迪思还打算加速实现MACsec功能，便于在该连接上加密和解密以太网数据包。然而，与多年来在传统网络设备中使用的大型FPGA不同，实现ORAN解决方案的莱迪思FPGA是小型、低功耗器件，非常适合多种类型的应用，包括对功耗敏感的小型蜂窝应用 ，这是现代5G网络中越来越重要的一部分应用。

结论和建议

过去几十年中正如我们在数据中心和云计算架构所见证的那样，蜂窝网络正在从专有硬件驱动转变为由软件驱动、虚拟化、容器化和标准化的API定义，它们将释放新的潜力。企业也在寻求这些新型架构所带来的灵活性、速度和多样化的选择，努力让蜂窝网络更具功能性和适应性。随着5G的兴起，电信公司的愿景是从简单的管道供应商转变为更加全面且盈利更强的服务供应商，根据不同行业和不同类型消费者的独特需求提供定制服务。

这样的转变并不容易，也很难快速进行；还需要解决许多关键问题，才能确保他们在实现这些新目标的同时仍然保持当前可靠的运行状态。其中的关键是需要保护器件、跨组件的互连和数据。尤其是必须保护传输中、使用中和静态的数据，让这些更灵活的架构可以像它们所取代的专有架构一样安全。

想要获得进行这种转变所需要的信任度，就需要关注最微小的细节并确保解决方案的所有方面都满足要求。建立在小型、低功耗FPGA上的完善的安全解决方案在实现该目标时可以发挥关键作用，尽管这一点不太为人所知。重点就是确保网络设计人员充分考虑构建解决方案所需的所有组件，在为电信公司提供其所需的灵活性的同时，为他们带来

安全性、同步和低功耗加速。