基于 SDN 和 NFV 的物联网环境架构概述：挑战与解决方案

摘要

物联网（IoT）是一种新兴范式，它确保了现实世界与虚拟世界之间的连接。一般来说，连接的事物构成了现实世界，在这个世界中，组件配备了无线接口。因此，大量智能设备可以直接或通过网络基础设施进行互动和通信。因此，将会生成大量数据。然而，基于物联网的网络并不适合支持数据管理。因此，一种新的架构设计似乎是应对物联网环境中数据快速增长的有效解决方案。在这方面，软件定义网络（SDN）和网络功能虚拟化（NFV）是两种可以帮助克服这些物联网挑战的技术。第一个实现了网络的集中控制。第二个将网络功能的软件和硬件分开。本文概述了基于 SDN 和 NFV 的物联网环境架构，重点讨论了挑战和解决方案。

关键词：物联网（IoT）、软件定义网络（SDN）、网络虚拟化（NV）、网络功能虚拟化（NFV）

1. 引言

近年来，物联网已成为尽可能减少人工干预的重要范式。大量物体能够感知、通信和共享信息，以创建一个万物互联的智能世界。然而，连接设备的快速增长带来了与大量生成数据相关的几个特殊问题。特别是，它包括数据可用性、准确性、安全性和冲突等。软件定义网络（SDN）和网络功能虚拟化（NFV）是两种新架构，旨在管理物联网网络，因为传统系统由于其有限的功能，已无法再支持数据的新动态行为。SDN 的主要思想是使网络可直接编程，并将控制平面与数据平面分离，以提供网络的集中视图。SDN 提供了可管理性和适应性的特性，使其非常适合动态环境，而 NFV 概念通过虚拟化这些任务为网络功能带来了灵活性。此外，NFV 提供了一种潜在的解决方案，可以实现自主管理，并将物理层资源转换为虚拟资源。本文的其余部分组织如下。在第二部分，我们概述了 SDN 和 NFV。第三部分提供了相关工作。第四部分介绍了主要的物联网挑战和解决方案。最后，第五部分总结了论文。

2. 对 SDN 和 NFV 的综述

SDN 和 NFV 是两种应用技术，已显示出在应对物联网挑战方面的效率。让

我们来看看这两个概念。

2.1. 软件定义网络 (SDN)

软件定义网络（SDN）是一种有前景的网络，旨在解耦控制平面和数据平面，以提高网络的可编程性。通过这种方式，基于 SDN 的应用程序可以动态且细粒度地访问网络资源，并在底层基础设施上指定流量设置[1]。

SDN 包含一个集中式控制器，可以在数据平面上单独管理网络。因此，它相比于传统网络减少了复杂性。

SDN 架构通常有三个层面，即数据层、控制层和应用层，如图 1 所示。数据平面通过南向接口连接到控制平面。SDN 控制器的功能是对数据进行控制。同样，SDN 控制器通过北向接口与应用层进行通信[1]。

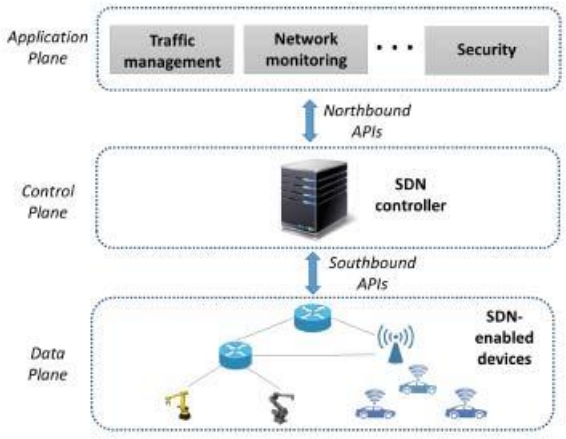

图 1　SDN 中的三层架构

2.2. 网络功能虚拟化 (NFV)

网络功能虚拟化（NFV）是一种技术解决方案，旨在用虚拟资源替代物理资源，以创建一个虚拟环境，从而减少成本和努力。

欧洲电信标准协会（ETSI）已经定义了一个通用的 NFV 架构[2]，该架构包括如图 2 所示的三个主要组件。

更具体地说，这些主要元素是：

- 网络功能虚拟化接口（NFVI）包含一个硬件接口（存储、网络、计算）、一个虚拟接 口（存储、网络、计算），以及一个位于硬件和软件之间的虚拟化层。
- VNF（虚拟化网络功能）是一组可以在 NFV 设备上执行的虚拟化网络功能。
- 网络功能虚拟化管理和编排（NFV MANO）负责网络服务管理，其中包含负责 硬 件和软件网络服务生命周期的 NFV 编排器。经理（VNFM）负责 VNF

的生命 周期，而经理（VIM）负责管理域内的 NFVI 资源。

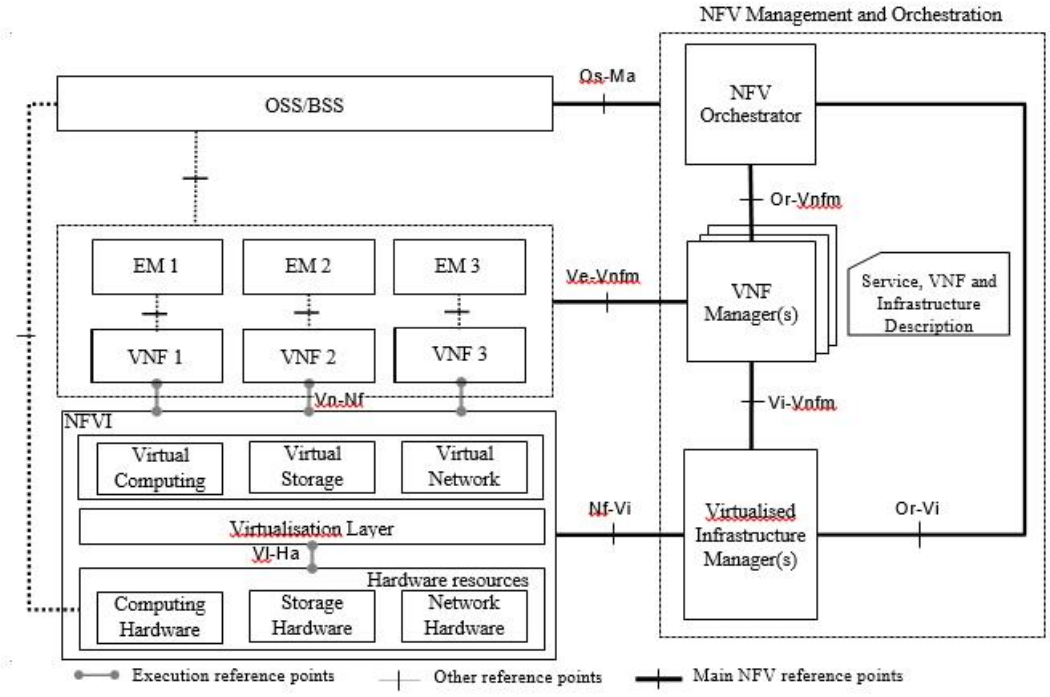

图 2　Severa 高级 NFV 框架

为了解决上述问题，提出了几项工作。在这方面，[1]中的作者提到，由于物联网的演变，网络犯罪分子的攻击数量正在增加。网络犯罪分子旨在利用物联网系统的漏洞进行恶意攻击。传统的安全机制在应对物联网设备的异质性、普遍性和移动性方面已被证明效率低下。SDN 和 NFV 的实施正在迅速改变电信行业，推动物联网安全的突破。本文深入分析了通过基于 SDN 和 NFV 的两种机制提供的主要安全特性，以确保可扩展性、按需网络可编程性、能源效率和移动性支持。

在[3]中，作者提出了一项研究物联网演变的工作。论文重点研究了 SDN 和 NFV 之间的融合，通过将网络的可编程性与虚拟化相结合，以应对数据量的急剧增加。它提到了 SDN 和虚拟化在应对物联网系统中的安全挑战方面的贡献，但没有在这一部分深入探讨，因为这些安全协议、接口和应用的创建和标准化仍然是一个开放的研究领域。然后，它提出了将 SDN、虚拟化和机器学习技术相结合作为研究人员值得探讨的有前景的任务。

在[4]中，作者提出了 SDN 和 NFV 作为关键推动力，通过提供高效的数据处理、分析和存储范式来支持未来物联网应用的需求。此外，它旨在减少需要传输到云端的数据总量。文章提出用虚拟图像替代物理物联网设备，并引入了“智能设备即服务”（SDaaS）的概念，远超经典的服务模型，包括基础设施即服务（IaaS）、

平台即服务（PaaS）和软件即服务（SaaS）。SDaaS 被提议通过提高灵活性、可扩展性、可重用性、减少网络流量以及安全性方面来改进物理设备的虚拟化技术。对该提案的性能分析显示，服务延迟和网络跳数显著减少。传输的数据量减少了多达 66%，电池寿命也有所延长，但这项工作缺乏通过具体结果来证明 SDN 架构如何改进他们的提议。

如前所述，物联网设备正在增大，因此显然网络基础设施必须通过提供足够的连接来支持这一发展，以应对这些情况。在这个意义上，文献[5]中提出了一种基于基础设施共享的新概念。它旨在连接服务，以减少与部署额外基础设施相关的过度投资和成本。更具体地说，作者介绍了一种基于网络虚拟化的架构。该提案的主要关注点是提供网络共享，处理大量数据，简化任务管理。为了实现这些目标，该工作提出了一个模型来研究 SDN/NFV 和 4G 网络之间的相对成本和能耗。获得的结果表明，与 4G 网络相比，基于 SDN/NFV 的网络在节能方面降低了成本。尽管如此，论文在进行测试时并未考虑到机会性资源访问和复用增益。

在[6]中的工作提出了 ANASTACIA 架构，该架构专注于使用 NFV/SDN 在物联网场景中管理安全性和机密性。架构的评估考虑了包括移动边缘计算和管理系统在内的两种不同场景。性能分析表明，所提出的架构能够通过在合理时间内加强政治安全来监控、检测、反应和缓解物联网网络攻击。然而，所进行的测试只考虑了两种攻击，这不足以深入评估该架构的有效性。

在 H2020 欧盟项目背景下，文献[15]中的作者提出了一种新颖的安全机制，旨在利用 SDN 和 NFV 模拟现实世界，以创建一个通常被称为蜜罐网络的虚拟物联网网络环境。性能分析表明，所提出的蜜罐架构似乎非常有效地吸引了来自现实世界的攻击者。

3. 物联网的主要挑战及解决方案

尽管物联网为生活带来了重要的变化，使其更加便捷，但一些挑战正在阻碍这一进程。本概述讨论了该领域中的主要问题，如数据量的增长、异构性、安全性和动态性。

3.1. 安全性

安全在物联网领域中占据了重要部分；因为一切都连接到互联网。因此，数据和人员信息必须得到保障。

物联网攻击可以分为两大类：主动攻击，其中恶意攻击者修改或注入消息以利用漏洞；被动攻击，其中攻击者在网络中主动互动[6]。

主动攻击是一种网络利用方式，黑客在其中更改数据并修改消息的内容。而在被动攻击中，其特征是拦截消息而不进行修改。因此，攻击者观察这些消息，复制它们，并可能将其用于恶意目的[6]。

3.2. 数据增加

预计在未来几年内，将有数十亿台设备连接到网络。因此，很明显需要处理、存储等大量数据。这种数据以更快速度的增加需要一种新的架构来处理这种新的流量行为。

当前的架构无法以低延迟管理和处理大量数据。不幸的是，这在效率和准确性方面极大地影响了物联网系统的质量。

3.3. 异质性

连接的服务和物品应该通过各种无线技术与分布式对象进行交互。因此，这么多异构设备需要新的架构来考虑这种异构性。

数据源的多样性、结构、应用和设备的异质性带来了许多困难，尤其是在存储和处理方面[7][8]。

3.4. 动态性

物联网动态地将许多设备连接到互联网；因此，物联网环境具有非常动态的拓扑结构。因此，新的物联网组件可以每次都连接和断开网络。因此，物联网需要一个灵活的网络架构，以应对这些物联网需求，如动态性和移动性[9]。

3.5. 物联网挑战的提案

对于之前每种类型的物联网挑战，我们将介绍一些提出解决方案的工作。

• 针对安全挑战的提案

在本概述中，表 1 中列出了最突出的安全挑战建筑解决方案的代表性总结。

表 1　安全解决方案

安全解决方案		
物联网挑战	技术	提案

攻击安全挑战	SDN	SDN-IoT 集成架构。它确认可以系统地检测和缓解 DoS 攻击[10]。
攻击漏洞	SDN/NFV	SDN 和 NFV 是补充物联网安全解决方案的最佳候选者[1]。
安全挑战	SDN/NFV	ANASTACIA 安全管理架构旨在处理 NFV/SDN 支持的物联网场景中的安全性和隐私问题[6]。
安全挑战	SDN/NFV	一个应用感知框架，通过使用 SDN 和 NFV 技术在网络切片中实现安全即服务（SECaaS）[11]。
安全挑战	SDN/NFV	该论文提出了一种分布式安全黑色 SDN-IoT 架构，结合 NFV 实现，旨在为智能城市提供网络每一层的安全保障[12]。

- 关于异构性、数据增加和动态性挑战的提案

表 2 中总结了众所周知的、旨在解决数据管理、异构性和动态性挑战的已提出解决方案的代表性概述。

表 2　解决异质性、数据增加和动态性的问题

安全解决方案		
物联网挑战	技术	提案
数据增加	SDN/NFV	SDN 和 NFV 的结合可以处理数据的巨大增长，物联网系统将通过虚拟化扩展网络功能的自动化，

		而 SDN 将优化网络[3]。
异质性	SDN/NFV	SDN 和 NFV 的部署展示了管理异构性的效率[1]。
多个网络跳数 数据量	NFV	解决方案是通过用虚拟图像替换物理物联网设备来实现 SDaaS[4]。
大数据爆炸 能源消耗	SDN/NFV	基于 SDN 和 NFV 的网络部署已经显示出在能源和成本方面的收益[5]。
动态性 流动性	SDN/NFV	SDN-IoT 架构结合 NFV 以应对物联网环境中的动态性挑战[13]。
异质性	SDN/NFV	该论文提出了一个愿景，通过在物联网中使用定义网络（SDIoT）并结合 NFV，提出了一个敏捷、动态的框架，以扩展对 SDN 和 NFV 融合需求的认识[14]。

如前两张表所示，已经通过使用这两种技术 SDN 和 NFV 完成了多项工作，我们可以推断到目前为止，这两种技术是管理物联网不同挑战的最佳候选者。

4. 总结

在本文中，我们提到物联网由于全球数百万设备的连接而不断增长。这种演变带来了一些挑战，例如数据量的增加、漏洞、异质性、动态性等。所有这些挑战表明，传统网络不适应物联网环境来解决这些问题。在本文中，我们讨论了 SDN 和 NFV 的潜力及其管理物联网系统动态特性的能力。本文概述了物联网中的挑战，强调了 SDN 和 NFV 在应对这些挑战中的关键作用。我们的未来工作将通过专注于基于 SDN/NFV 挑战的架构来扩展这项初步研究，以改进这些架构之一。

5. 引用

[1] Ivan Farris, Tarik Taleb, Yacine Khettab, and JaeSeung Song, "A survey on emerging SDN and NFV security mechanisms for IoT systems," IEEE Communications Surveys & Tutorials, vol. 21, no. 1 , pp. 812 - 837, 2019 .

[2] NFV, "GS NFV 002 - V1.2.1 - Network Functions Virtualisation (NFV);Architectural Framework," 2014.

[3] Kuipers, Nikos Bizanis and Fernando, "SDN and virtualization solutions for the Internet of Things: A survey," IEEE Access, vol. 4, pp. 5591 - 5606, 2016.

[4] L. Atzori b , e , J.L. Bellido f , R. Bolla b , a , G. Genovese , A. Iera , A. Jara , C. Lombardo, G. Morabito, "SDN&NFV contribution to IoT objects virtualization," Computer Networks, vol. 149, pp. 200- 212, 2019.

[5] Mamdouh Alenezi, Khaled Almustafa, Khalim Amjad Meerja, "Cloud based SDN and NFV architectures for IoT infrastructure," Egyptian Informatics Journal, vol. 20, no. 1, pp. 1-10, 2019.

[6] Alejandro Molina Zarca, Jorge Bernal Bernabe, Ruben Traperoy, Diego Riveraz, et al. , "Security Management Architecture for NFV/SDN-aware IoT Systems," IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8005 - 8020, 2019 .

[7] Deepak Choudhary, "Security Challenges and Countermeasures for the Heterogeneity of IoT Applications," Journal of Autonomous Intelligence, vol. 1, 2018.

[8] Shanshan Wu ,Liang Bao, Zisheng Zhu, Fan Yi, Weizhao Chen, "Storage and retrieval of massive heterogeneous IoT data based on hybrid storage," 2017 13th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD), 2017.

[9] Intidhar Bedhief, Meriem Kassar, Taoufik Aguili,Luca Foschini, Paolo Bellavista, "Self-Adaptive Management of SDN Distributed Controllers for Highly Dynamic IoT Networks," 2019 15th International Wireless Communications & Mobile Computing Conference(IWCMC), 2019.

[10] Prabhakar Krishnan, Jisha S Najeem and Krishnashree Achuthan, "SDN Framework for Securing IoT Networks," International Conference on Ubiquitous Communications and Network Computing, pp. 116- 129, 2017.

[11] Yacine Khettab, Miloud Bagaa, Diego Leonel Cadette Dutra, Tarik Taleb and Nassima Toumi, "Virtual Security as a Service for 5G Verticals," 2018 IEEE Wireless Communications and Networking Conference (WCNC), 2018.

[12] Md. Jahidul Islam ; Md. Mahin ; Shanto Roy ; Biplab Chandra Debnath ; Ayesha Khatu, "DistBlackNet: A Distributed Secure Black SDN-IoT Architecture with NFV Implementation for Smart Cities," 2019 International Conference on Electrical, Computer and Communication Engineering (ECCE), 2019.

[13] Mike Ojo, Davide Adami and Stefano Giordano, "A SDN-IoT Architecture with NFV Implementation," 2016 IEEE Globecom Workshops (GC Wkshps), 2017.

[14] Rowayda A. Sadek, "An Agile Internet of Things (IoT) based Software Defined Network (SDN) Architecture," Egyptian Computer Science Journal, vol. 42, 2018.

[15] Alejandro Molina Zarca, Jorge Bernal Bernabe, Antonio Skarmeta, Jose M. Alcaraz Calero, " Virtual IoT HoneyNets to mitigate cyberattacks in SDN/NFVenabled IoT networks," IEEE Journal on Selected Areas, vol. 38, no. 6, 2020.