Comprehensive Investigation of Network Function Virtualization (NFV) Deployment in Computer Networks: Benefits, Challenges, and Solutions

Alan Palayil, B.S. Computer and Cybersecurity Engineering, M.S. Cybersecurity Engineering, Illinois Institute of Technology

Modern Internet Technologies (ECE-545) Academic Paper

Abstract

This technical report presents a comprehensive investigation of Network Function Virtualization (NFV) deployment in computer networks. NFV is a promising technology that virtualizes network functions and aims to address the challenges of growing demand for network services and the increasing complexity of network infrastructures. The report provides an overview of NFV technology and its benefits and discusses the key problems associated with NFV deployment, such as security, performance, and management. It also summarizes the existing solutions to these problems, including the use of software-defined networking (SDN), hardware accelerators, and orchestration frameworks. Additionally, the report identifies open issues in NFV deployment and investigates possible solutions. Overall, this report provides valuable insights for network operators and researchers to better understand the benefits and challenges of NFV and pave the way for the wider adoption of this technology in the network domain.

I. INTRODUCTION

The rapid growth of Internet services and the increasing complexity of network infrastructures have driven the need for more flexible, scalable, and cost-effective solutions in computer networks.

Network Function Virtualization (NFV) has emerged as a promising technology to address these challenges by virtualizing network functions and decoupling them from dedicated hardware devices. NFV enables the deployment of network services on general-purpose hardware, reducing the cost and complexity of managing network infrastructures, and improving the agility and flexibility of network operators (Mijumbi et al., 2016; Sun et al., 2021).

Despite the potential benefits of NFV, its deployment in computer networks faces several challenges, such as ensuring security, maintaining performance, and managing the virtualized network functions (Yang & Fung, 2016; Jang et al., 2015; Rehman et al., 2019). For instance, the consolidation of network functions on shared hardware platforms may lead to potential security risks and performance bottlenecks (Linguaglossa et al., 2019). Moreover, the dynamic nature of virtualized environments necessitates efficient management and orchestration mechanisms to cope with the increasing complexity of network services and the need for real-time adaptation (Mijumbi et al., 2016).

This technical report aims to provide a comprehensive investigation of NFV deployment in computer networks, focusing on the benefits, challenges, and existing solutions. The report will review the literature on NFV technology, discuss the main problems associated with its deployment, and summarize the state-of-the-art solutions to address these challenges. These solutions include the use of software-defined networking (SDN) for centralized control and orchestration (Gao et al., 2022), hardware accelerators to improve performance (Linguaglossa et al., 2019), and frameworks for secure and efficient management of virtualized network functions (Kalliola et al., 2017; Santhanamahalingam et al., 2022). Furthermore, the report will identify open issues in NFV deployment and explore potential avenues for future research.

By providing a comprehensive understanding of the benefits and challenges of NFV deployment, this report will offer valuable insights for network operators, researchers, and policymakers to promote the wider adoption of NFV technology in the network domain and facilitate the development of more efficient, scalable, and secure computer networks.

II. LITERATURE SURVEY

This technical report presents a comprehensive investigation of Network Function Virtualization (NFV) deployment in computer networks by analyzing 10 journal/conference papers

downloaded from the IEEE or ACM databases. NFV is a promising technology that virtualizes network functions and aims to address the challenges of growing demand for network services and the increasing complexity of network infrastructures.

1. Mijumbi et al. (2016) provide an overview of NFV management and orchestration challenges. The authors highlight the potential benefits of NFV, such as reduced Capital Expenditure (CapEx) and Operational Expenditure (OpEx), increased service agility, and improved scalability. However, they also identify several challenges related to NFV deployment, such as network security, performance, and management. Mijumbi et al. emphasize the need for efficient and secure management and orchestration solutions to enable network operators to cope with the increasing complexity of network services and the need for real-time adaptation.
2. Yang and Fung (2016) present a survey on security in network functions virtualization, where they identify several security threats, such as hypervisor attacks, side-channel attacks, and malicious virtual network function deployment. The authors also propose several security mechanisms, including intrusion detection and prevention systems, software-defined security, and secure network function chaining. They discuss the challenges associated with securing virtualized environments and emphasize the need for novel security mechanisms and policies to address these challenges.
3. Linguaglossa et al. (2019) provide a survey of performance acceleration techniques for network function virtualization. They review the existing hardware accelerators and software techniques used to improve the performance of virtualized network functions. The authors analyze various solutions, such as Field-Programmable Gate Arrays (FPGAs), Graphics Processing Units (GPUs), and Smart Network Interface Cards (SmartNICs). They also discuss the trade-offs between different acceleration techniques in terms of performance, energy efficiency, and programmability, and identify potential avenues for future research in this area.
4. Sun et al. (2021) propose a novel network function placement algorithm under randomly arrived networking traffic. The authors aim to optimize network function placement to reduce network latency and increase resource utilization. They formulate the problem as a mixed-integer linear programming (MILP) model and propose a heuristic algorithm to efficiently solve the problem. The proposed algorithm is evaluated using simulation

experiments, which demonstrate its effectiveness in achieving low-latency and high-resource utilization.

5. Gao et al. (2022) propose a potential game approach for virtual network function placement in satellite edge computing. They investigate the optimal placement of virtual network functions to maximize network throughput and energy efficiency. The authors model the problem as a potential game and develop a distributed algorithm based on best-response dynamics. They demonstrate the convergence and effectiveness of the proposed algorithm through simulation experiments and compare it with existing solutions in terms of throughput and energy efficiency.
6. Rehman et al. (2019) provide an overview of commercial deployments of NFV. They analyze the factors that have hindered the widespread adoption of NFV and identify the potential solutions to these challenges. The authors discuss issues related to performance, management, and standardization, and emphasize the need for better coordination among industry stakeholders, the development of standardized frameworks and interfaces, and the establishment of best practices for NFV deployment.
7. Santhanamahalingam et al. (2022) present a study of cloud-based VPN establishment using NFV techniques. They investigate the performance and security of VPNs deployed using NFV techniques. The authors propose a cloud-based VPN architecture that leverages NFV and Software-Defined Networking (SDN) technologies to enable flexible and secure VPN service provisioning. They evaluate the proposed architecture using a testbed implementation and demonstrate its effectiveness in terms of performance and security. The results indicate that the proposed architecture provides a promising solution for deploying VPN services using NFV techniques.
8. Kalliola et al. (2017) propose a testbed for security orchestration in a network function virtualization environment. They investigate the feasibility and effectiveness of deploying security functions using NFV techniques. The authors describe the design and implementation of a testbed that combines NFV and security orchestration technologies to enable the deployment and management of security functions in a virtualized environment. They present experimental results that demonstrate the potential of the proposed testbed in terms of security function deployment, performance, and management.

9. Jang et al. (2015) present a survey on interfaces to network security functions in network virtualization. They examine the challenges and requirements of interfacing security functions in a virtualized environment and discuss various approaches for integrating security functions within an NFV infrastructure. The authors propose a taxonomy of security function interfaces based on their location, functionality, and communication patterns, providing a comprehensive overview of the different strategies for interfacing security functions in NFV. Furthermore, they highlight open research challenges and suggest future directions for improving the integration of security functions in virtualized networks.
10. Jie Sun et al. (2019) propose an efficient virtual network function placement algorithm for Poisson-arrived traffic. The authors formulate the virtual network function placement problem as a two-stage stochastic program and develop a sample average approximation (SAA) method to solve it. They also propose an effective heuristic algorithm based on the SAA method to address the computational complexity issues associated with large-scale problem instances. The performance of the proposed algorithm is evaluated through extensive simulations, which demonstrate its effectiveness in handling dynamic traffic patterns and improving resource utilization.

The literature survey demonstrates the growing interest in NFV technology and its potential to revolutionize network service provisioning and management. While significant progress has been made in recent years, several open issues and challenges remain to be addressed to fully realize the potential of NFV. Some key challenges include the need for better performance optimization techniques, more efficient virtual network function placement algorithms, improved security mechanisms, and robust management and orchestration solutions. Addressing these challenges will require ongoing research efforts from both academia and industry, as well as collaboration among various stakeholders, such as network operators, equipment vendors, and standardization bodies.

As NFV technology continues to evolve and mature, new challenges and opportunities are likely to emerge, particularly with the advent of 5G and 6G networks, edge computing, and the Internet of Things (IoT). These developments will create new use cases and requirements for NFV, necessitating further research and innovation in this area. The surveyed papers provide valuable insights into the benefits and challenges of NFV deployment, as well as existing solutions proposed

to address these challenges. They underscore the need for efficient and secure virtualized network functions and management, while identifying challenges related to service assurance, fault management, scalability, and security. The studies also propose future research directions related to the optimization of virtual network function placement, energy efficiency, network security, and orchestration frameworks.

In summary, the literature survey emphasizes the transformative potential of NFV in enabling more flexible, scalable, and efficient network service provisioning. However, it also highlights the need for continued research and development efforts to tackle the challenges associated with NFV deployment. By addressing these challenges and leveraging advances in NFV technology, network operators and researchers can unlock the full potential of NFV and pave the way for the future of computer networks.

III. PROBLEM FORMULATION

The literature survey on Network Function Virtualization (NFV) deployment in computer networks reveals numerous benefits associated with its implementation. However, several challenges and open issues remain to be addressed for NFV technology to achieve its full potential. In this technical paper, we aim to formulate the key problems related to NFV deployment and investigate potential solutions. The main problems identified from the literature survey can be summarized as follows:

1. Performance Optimization: Ensuring that virtualized network functions deliver optimal performance is a critical aspect of NFV deployment. This requires the development of techniques for efficient resource allocation, load balancing, and traffic management.
2. Virtual Network Function Placement: The strategic placement of virtual network functions within the network infrastructure is essential for minimizing network latency and maximizing resource utilization. Novel placement algorithms and strategies need to be devised to optimize the deployment of virtual network functions.
3. Security: The virtualization of network functions introduces new security challenges, such as hypervisor attacks, side-channel attacks, and malicious virtual network function deployment. Robust security mechanisms need to be developed to safeguard NFV-based networks and ensure the confidentiality, integrity, and availability of network services.

4. Management and Orchestration: Efficient management and orchestration of virtualized network functions are crucial for maintaining service quality and network resilience. This involves the design of frameworks and solutions that can automate the deployment, scaling, and monitoring of virtual network functions.
5. Integration with Emerging Technologies: As the networking landscape evolves with the advent of 5G and 6G networks, edge computing, and the Internet of Things (IoT), NFV technology must adapt to cater to new use cases and requirements. This necessitates further research and innovation to ensure seamless integration of NFV with emerging technologies.

By formulating these key problems, this technical paper seeks to provide a comprehensive understanding of the challenges related to NFV deployment and to explore potential solutions that can address these issues. The goal is to facilitate the wider adoption of NFV technology in computer networks, leading to significant improvements in network service provisioning, management, and performance.

IV. CLASSIFICATION OF EXISTING SOLUTIONS

Based on the literature survey and the key problems identified in NFV deployment, we classify the existing solutions into the following categories:

i. Performance Optimization Techniques:

a. Hardware Accelerators: Use of specialized hardware components, such as GPUs, FPGAs, or SmartNICs, to offload and accelerate specific virtualized network functions (Linguaglossa et al., 2019).
b. Software Techniques: Development of advanced software solutions, such as kernel bypass mechanisms and efficient packet processing libraries, to optimize the performance of virtualized network functions.

ii. Virtual Network Function Placement Algorithms:

a. Optimization-based Algorithms: Techniques that employ optimization methods, such as linear programming, integer programming, or genetic algorithms, to find optimal placements for virtual network functions (Sun et al., 2021).

b. Game-theoretic Approaches: Use of game theory and potential game models to analyze and optimize the placement of virtual network functions in various network scenarios (Gao et al., 2022).

iii. Security Mechanisms:

a. Intrusion Detection and Prevention Systems: Deployment of advanced intrusion detection and prevention systems to monitor and protect NFV-based networks from security threats (Yang & Fung, 2016).
b. Software-Defined Security: Utilization of software-defined networking (SDN) principles to enforce security policies and dynamically adapt to changing security requirements.
c. Secure Network Function Chaining: Implementation of secure network function chaining techniques to ensure the integrity and confidentiality of data flows in NFV-based networks.

iv. Management and Orchestration Solutions:

a. NFV Management and Orchestration (MANO) Frameworks: Development of comprehensive frameworks and tools for automating the deployment, scaling, and monitoring of virtual network functions (Mijumbi et al., 2016).
b. Service Assurance and Fault Management: Design of techniques and mechanisms for ensuring service quality, reliability, and resilience in NFV-based networks.
c. Scalability Solutions: Development of strategies for efficient and seamless scaling of virtual network functions to accommodate changing network demands.

v. Integration with Emerging Technologies:

a. NFV in 5G/6G Networks: Research on the incorporation of NFV principles in the design and deployment of 5G and 6G network architectures.
b. NFV in Edge Computing: Exploration of NFV techniques for the deployment of virtual network functions at the network edge, enabling low-latency and context-aware services.
c. NFV in IoT: Investigation of NFV solutions to support the diverse requirements of IoT applications, such as scalability, energy efficiency, and security.

The classification of these existing solutions provides a structured overview of the current state of research in addressing the challenges of NFV deployment. This categorization facilitates a deeper understanding of the various approaches and helps identify potential areas for future research and innovation.

V. OPEN ISSUES IN THE FIELD OF NFV

Despite the significant progress in the development and deployment of NFV technology, several open issues remain to be addressed to fully exploit its potential in transforming computer networks. The literature survey and the classification of existing solutions have allowed us to identify the following open issues that warrant further investigation and research:

i. Performance Optimization:

a. Exploration of novel hardware and software techniques to further improve the performance of virtualized network functions.

b. Development of strategies for balancing performance optimization with other objectives, such as energy efficiency, security, and reliability.

ii. Virtual Network Function Placement:

a. Design of more efficient and scalable algorithms for virtual network function placement, taking into consideration various network constraints, such as latency, bandwidth, and resource utilization.

b. Investigation of dynamic placement algorithms that can adapt to changing network conditions and service demands in real-time.

iii. Security:

a. Identification and mitigation of emerging security threats in NFV-based networks, such as attacks on orchestration and management frameworks.

b. Development of context-aware and adaptive security mechanisms to protect against evolving attack vectors and vulnerabilities.

iv. Management and Orchestration:

a. Enhancement of existing NFV management and orchestration frameworks to accommodate the increasing complexity of network services and infrastructures.

b. Integration of AI and machine learning techniques to improve network management, fault detection, and service assurance in NFV-based networks.

v. Scalability and Resilience:

a. Design of mechanisms for ensuring the scalability and resilience of NFV-based networks in the face of growing service demands and changing network conditions.

b. Investigation of approaches for efficient and seamless scaling of virtual network functions, both horizontally and vertically.

vi. Integration with Emerging Technologies:

a. Analysis of the synergies between NFV and emerging technologies, such as 5G/6G networks, edge computing, and IoT, and the development of solutions to support their specific requirements.

b. Exploration of novel use cases and applications for NFV in the context of these emerging technologies.

vii. Quality of Service (QoS) and Quality of Experience (QoE):

a. Development of QoS-aware virtual network function placement and resource allocation mechanisms to ensure that the performance requirements of various network services are met in NFV-based networks.

b. Evaluation of the impact of NFV on user experience (QoE) and the design of strategies to maintain or improve QoE in the presence of virtualized network functions and associated challenges, such as network latency, jitter, and packet loss.

viii. Real-Time Network Function Virtualization:

a. Investigation of the feasibility and challenges of implementing real-time network functions in NFV-based networks, particularly focusing on latency-sensitive applications, such as industrial automation, autonomous vehicles, and augmented reality.

b. Development of real-time NFV frameworks and mechanisms capable of supporting stringent timing requirements and delivering consistent performance in the presence of variable network conditions and resource constraints.

ix. Energy Efficiency:

a. Development of strategies and techniques to improve the energy efficiency of virtualized network functions, considering both computation and communication aspects, as well as the impact of virtual network function placement on overall energy consumption.

b. Investigation of energy-efficient resource allocation and management mechanisms in NFV-based networks, with a focus on minimizing energy consumption without compromising performance, reliability, and security.

Addressing these open issues will require concerted research efforts from both academia and industry, as well as close collaboration among various stakeholders, such as network operators,

equipment vendors, and standardization bodies. By tackling these challenges and leveraging the advances in NFV technology, researchers and practitioners can unlock the full potential of NFV and pave the way for the future of computer networks.

VI. POSSIBLE SOLUTIONS FOR THE ISSUES

In response to the open issues identified in the literature survey, possible solutions to address these challenges can be proposed as follows:

i. Performance Optimization:

a. Development of novel hardware acceleration techniques and software optimization methods specifically tailored for virtualized network functions, leveraging emerging technologies such as AI, machine learning, and parallel processing.

b. Integration of advanced traffic engineering and load balancing mechanisms to ensure optimal resource utilization and efficient handling of network traffic in NFV-based environments.

ii. Efficient Virtual Network Function Placement:

a. Design and implementation of intelligent and adaptive virtual network function placement algorithms that consider various factors such as network topology, resource availability, and service requirements to optimize network performance and resource utilization.

b. Application of machine learning and optimization techniques to enhance the effectiveness of virtual network function placement strategies and enable self-optimizing NFV-based networks.

iii. Improved Security Mechanisms:

a. Development of comprehensive security frameworks and mechanisms specifically designed for NFV environments, encompassing aspects such as secure virtualization, isolation, authentication, and encryption.

b. Integration of advanced intrusion detection and prevention systems, as well as security monitoring and analytics tools, to enhance the overall security posture of NFV-based networks.

iv. Robust Management and Orchestration Solutions:

a. Design and implementation of scalable, modular, and flexible management and orchestration frameworks capable of handling the dynamic and complex nature of NFV-based networks.

b. Incorporation of advanced automation, AI, and machine learning techniques to enable self-managing and self-healing NFV environments that can automatically adapt to changing network conditions and requirements.

v. Integration with Emerging Technologies and Networking Paradigms:

a. Exploration of synergies between NFV and other emerging technologies, such as 5G/6G networks, edge computing, and the Internet of Things, to create innovative solutions that address new use cases and requirements.

b. Design of novel NFV-based architectures and solutions that are specifically tailored for these emerging paradigms, ensuring their seamless integration and coexistence with existing network infrastructures.

vi. Energy Efficiency:

a. Development of energy-aware virtual network function placement and resource allocation mechanisms that optimize energy consumption while maintaining the required level of performance, reliability, and security.

b. Investigation of energy-efficient hardware and software solutions for virtualized network functions, including energy-aware virtualization techniques, power management strategies, and green networking technologies.

vii. Quality of Service (QoS) and Quality of Experience (QoE):

a. Design and implementation of QoS-aware NFV management and orchestration solutions that ensure the performance requirements of various network services are met.

b. Integration of QoE monitoring and analytics tools to continuously assess user experience and guide the optimization of NFV-based networks accordingly.

viii. Real-Time Network Function Virtualization:

a. Exploration of novel virtualization techniques and architectures that support real-time network functions, specifically tailored for latency-sensitive applications.

b. Design and implementation of real-time NFV frameworks and mechanisms capable of meeting stringent performance, reliability, and timing requirements of mission-critical and

time-sensitive applications, such as industrial automation, healthcare, and emergency services.

ix. Scalability and Elasticity:

a. Development of NFV architectures, management, and orchestration solutions that can efficiently scale to accommodate the growing number of network functions, devices, and services, without compromising performance and reliability.
b. Design and implementation of elastic virtual network function provisioning and resource allocation mechanisms that can dynamically adjust to fluctuations in demand, ensuring optimal resource utilization and cost-efficiency.

By exploring and implementing these possible solutions, researchers and industry practitioners can address the challenges associated with NFV deployment, ultimately unlocking the full potential of NFV technology, and paving the way for the future of computer networks.

VII. CONCLUSION

In conclusion, Network Function Virtualization (NFV) is a transformative technology with the potential to revolutionize the networking landscape by enabling more flexible, scalable, and efficient network service provisioning. The comprehensive investigation presented in this technical report, based on an extensive literature survey, highlights the benefits and challenges of NFV deployment, as well as the existing solutions and open issues in the field. The analysis of the literature reveals significant advancements in NFV technology, including the development of efficient management and orchestration solutions, performance optimization techniques, and security mechanisms. Nevertheless, several challenges and open issues remain, such as service assurance, fault management, scalability, security, and the optimization of virtual network function placement.

The possible solutions outlined in this report address these challenges and pave the way for future research directions, including the exploration of novel NFV architectures, the development of resilient and fault-tolerant solutions, and the enhancement of performance, energy efficiency, and network security. As NFV technology continues to evolve and mature, new opportunities and challenges are likely to emerge, driven by the advent of 5G and 6G networks, edge computing, and the Internet of Things (IoT). By addressing the existing challenges and leveraging the advances

in NFV technology, network operators and researchers can unlock the full potential of NFV and shape the future of computer networks, ultimately leading to significant improvements in network service provisioning, management, and performance.

References

1. Mijumbi, R., Serrat, J., Gorricho, J. L., Latré, S., Charalambides, M., & Lopez, D. (2016). Management and orchestration challenges in network functions virtualization. IEEE Communications Magazine, 54(1), 98-105. DOI: 10.1109/MCOM.2016.7378433
2. Sun, J., Liu, F., Wang, H., Ahmed, M., Li, Y., Zhang, L., & Zeng, H. (2021). Network Function Placement Under Randomly Arrived Networking Traffic. IEEE Transactions on Network and Service Management, 18(1), 624-637. DOI: 10.1109/TNSM.2020.3043006.
3. Yang, W., & Fung, C. (2016). A survey on security in network functions virtualization. In 2016 IEEE International Conference on Communications (ICC) (pp. 1-6). IEEE.
4. Jie Sun, Feng Liu, Manzoor Ahmed, and Yong Li. "Efficient Virtual Network Function Placement for Poisson Arrived Traffic." 2019 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). IEEE, 2019.
5. Jang, H., Jeong, J. (Paul), Kim, H., & Park, J.-S. (2015). A Survey on Interfaces to Network Security Functions in Network Virtualization. In 2015 29th International Conference on Advanced Information Networking and Applications Workshops (pp. 559-564). IEEE. DOI: 10.1109/WAINA.2015.103
6. Gao, X., Liu, R., & Kaushik, A. (2022). Virtual Network Function Placement in Satellite Edge Computing With a Potential Game Approach. IEEE Transactions on Network and Service Management, 19(1), 584-599. DOI: 10.1109/TNSM.2021.3116137
7. Rehman, A. U., Aguiar, R. L., & Barraca, J. P. (2019). Network Functions Virtualization: The Long Road to Commercial Deployments. IEEE Communications Magazine, 57(12), 130-136. DOI: 10.1109/MCOM.2019.1900731
8. Linguaglossa, L., Lange, S., Pontarelli, S., Rétvári, G., Rossi, D., Zinner, T., Bifulco, R., Jarschel, M., & Bianchi, G. (2019). Survey of Performance Acceleration Techniques for Network Function Virtualization. IEEE Transactions on Computers, 68(4), 557-573. DOI: 10.1109/TC.2018.2866438
9. Santhanamahalingam, S., Alagarsamy, S., & Subramanian, K. (2022). A study of cloud-based VPN establishment using network function virtualization technique. In 2022 IEEE

International Conference on Electrical, Computer and Communication Technologies (ICECCT) (pp. 1-6). IEEE. DOI: 10.1109/ICECCT51863.2022.9777615

10. Kalliola, A., Lal, S., Ahola, K., Oliver, I., Miche, Y., & Holtmanns, S. (2017). Testbed for Security orchestration in a network Function Virtualization Environment. 2017 14th IEEE Annual Consumer Communications & Networking Conference (CCNC), 1-6. DOI: 10.1109/ccnc.2017.7983234