SD-NFV Based Network Optimization: An Architectural Framework for Industrial IoT

[1]S.Chandramohan, [2] Dr.M.Senthilkumaran,
[1]*Research Scholar / ECE (IEEE Member), SCSVMV University, Kanchipuram,Tamilnadu, India*
[2]*Associate Professor / CSE, SCSVMV University, Kanchipuram,Tamilnadu, India.*

Abstract

Currently, the manufacturing Industries are moving towards customized production than mass production. Due to rapid advancements in industrial technologies the productivity has been increased when compare to conventional process. Wireless technology and Cyber physical systemswere poised to support technical innovations in the industry with the help of sensor networksto improve manufacturing production efficiently. But the challenges towards the smart manufacturingindustries continue to be fact that occurs in sensor networks and its wide variety of applications. The scope of this paper is to address the leveragesof Network Function Virtualization (NFV) over software defined network (SDN)and Industrial Wireless Network (IWN) towards"Industry4.0"

Keywords: Cyber physical systems, Software defined networks, Industrial Wireless Network, Network Function Virtualization.

1. INTRODUCTION

Traditionally, manufacturing industrial systems are realized through wired communications and it is the first generation method. Later due to advancements in technology and innovations we are moving towards better manufacturing process. Currently, an intelligent system is the need for today's smart manufacturing Industry. The vision of the Industry 4.0 is to make manufacturing industry smarter throughthe advancements of wireless sensor technology, Industrial Internet of Things (IIoT), productions based on cloud platform with cyber security [1].

2. ISSUES AND CHALLENGES.

2.1Data Analytics

Inintelligent manufacturing systems, a hugevolume of data is produced which is unpredictable. Also the data storage plays a vital role.The process of converting large amounts of unstructured raw data retrieved from different sources in an industry forms the core of data Analytics [2].

2.2 Industrial Internet of Things

The future of smart industries are targeting through the advancements of recent technological achievements, such as cloud computing, wireless networks and Internet. It is forcing us to develop and introduce a new modern era of industrial production based on communicational informational linking of manufacturers and customers.Cyber physical systems (CPS) are a new generation of smart manufacturing systems that integrate computer and physical devices. [3].This system allows feedback loops, improving efficient production processes.By using the corresponding wireless sensor technology, cyber - physical systems are able to receive direct physical data and convert them into digital signals. They can share this information and access the available data via Internet of things (IOT) devices. The outlook of Industrial IoT is shown in Fig.1.

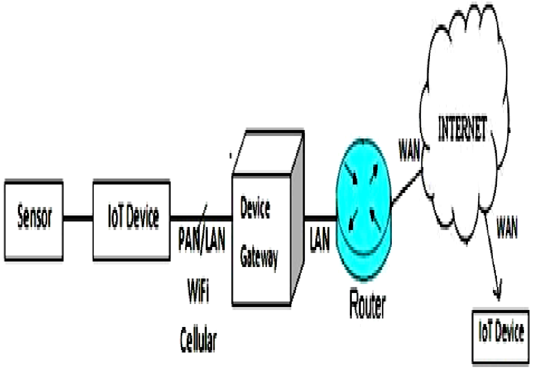

Fig.1.Overview of IIoT

2.3 Industrial Wireless Networks (IWNs)

The IWNs is the new frontier in the intelligent manufacturing Industry by increasing productivity cheaper and deploying new business models. It involves bridging the gap between the existing systems.However, there are still many challenges and barriers for the IWNs under different technical standards/vendor.The collaborative nature of IWNs brings several advantages as well as security issues [10], [11]. In the next few years, as the edge part of smart Industry, the IWNs plays a vital role in transforming traditional manufacturing in to fourth industrial revolution, Industry 4.0

2.4 Cyber Security

The world has ever been connected than it is today. The Internet has become essential to our everyday lives, for industry and individuals, and so too has its security. With our growing advancements on wireless networked systems comes an increase in the variety and scale of threats and cyber attacks. Due to inadequate resource limitations in wireless networks, the overhead associated with security protocols[7]. Therefore, improving our standards has a major role to cyber security as well as fortifies the Internet and its communications that rely on it.Heterogeneity in the protective methods can make it difficult to assess risk systematically and to shelter consistent, adequate cyber security attacks[3],[12].

2.5 Industrial Internet of Things (IIoT)

Cyber physical systems (CPS) are a new generation of smart manufacturing systems that integrate computer and physical devices. This system allows feedback loops, improving efficient production processes. By using the corresponding wireless sensor technology, cyber - physical systems are able to receive direct physical data and convert them into digital signals[13].They can share this information and access the available data via Internet of things (IOT) devices. The Industrial Internet of Things is creating new competitive landscape of industries, as companies are investing in innovative technologies for industrial automation. Further, companies have been able to establish themselves as smart manufacturers using this IIoT advancement [14], [15].

3.Software Defined Network (SDN)

The demands of current industry have risen exponentially over the decades. Due to limitations in maintaining the number of issues inherent in a conventional legacy IWNs.

Cloud computing, industrial data, network and mobile devices are propelling conventional networks to their limits. Computing and huge datastorage has added advantages from innovations in virtualization and automation, but those benefits are constrained by limitation in networks.[4], [5].

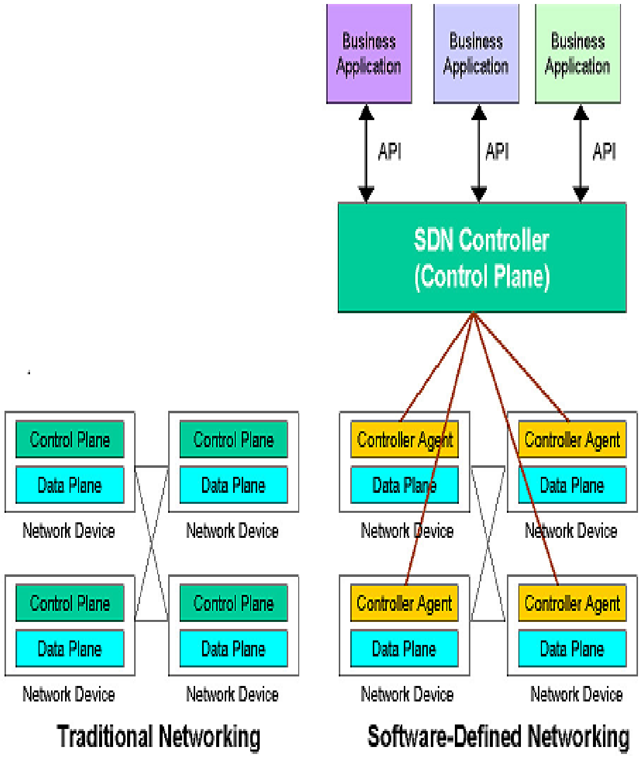

Fig 2: Traditional vs SDN Architecture

The network administrators and Value added resellers knows that SDN is built on switches it can be programmed through SDN controller also it network functions from firewalls, routers, hardware devices and confess network services to be hosted on virtual machines (VM) [8], [9]. It has a hypervisor, also called a virtual machine manager, which concede various operating systems to share a single hardware processor.

In order to make networks programmable for optimum configuration, users are provided with an option to manage networking by means of software.

Today Software-defined networking (SDN) has the capacity to provide data centers by an adjustable way of controllingthe network by which it can take the role of virtualized versions of compute and storage [6].

ISSN: 2233-7857 IJFGCN

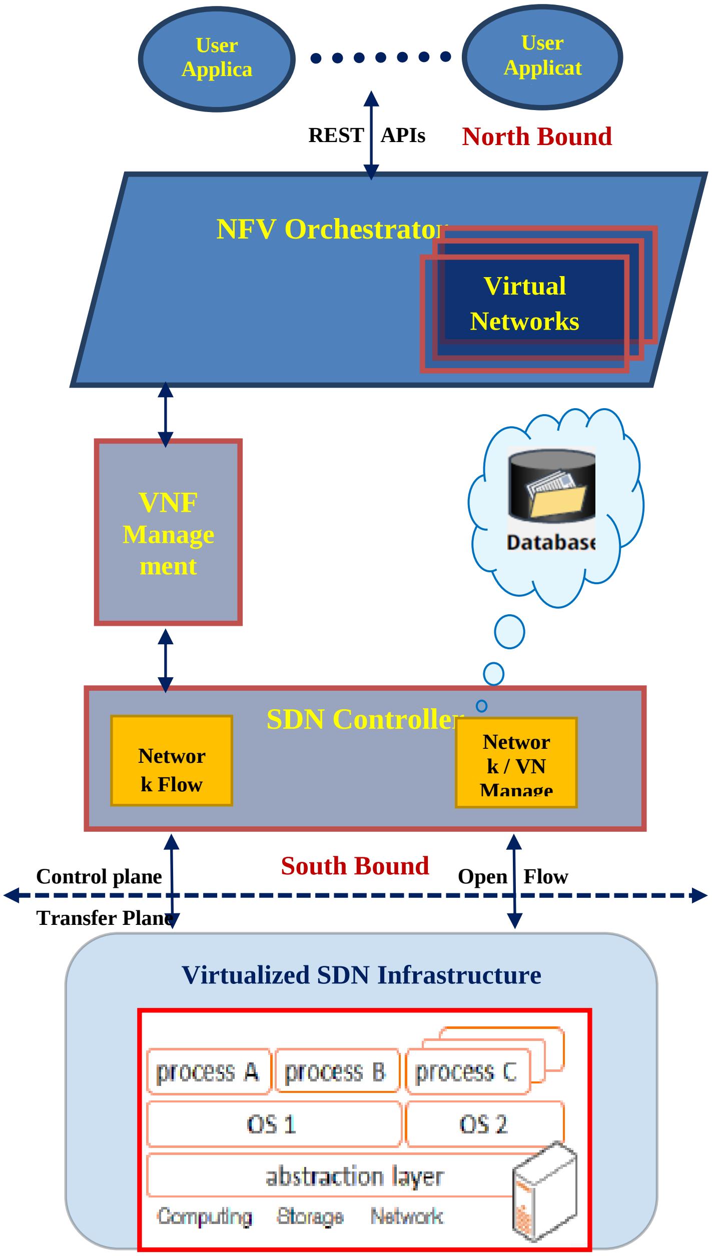

Fig 3 : SD-NFV based Architecture for Industrial IoT.

4. Integration of SDN and NFV Architecture

In wireless sensor network, both SDN and NFV are emerging innovation technologies. These two paradigms have very strong synergies among them, as shown in Fig. 4. By combining these technologies will exploit enormous advantages as well as few challenges too. Integrating SDN with NFV may create lot of advantages to smart industries and also to academicians.

In [18], an SDN-based architecture is proposed to enhance collaborative network-server resource management over cloud data centers.The resource management in SDN control plane with virtualized networks has a significant task, especially to infrastructure service provider. The virtual network function (VNF) provides a new method to deploy and manage networking designs [16], [17].

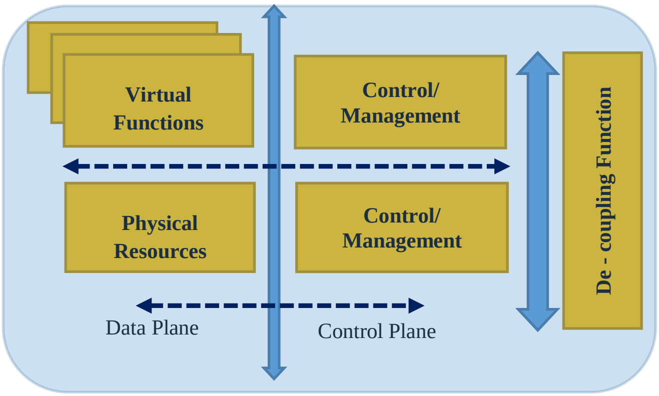

Fig: 4 Integrating Key principles of SD-NFV.

In aProposed SD-NFV framework creating a platform to virtualization environment can be done by mapping based on network status. For example, a substrate network (SN) has to map in dynamic virtual environment. To address this dynamic resource management scenario, we presented an algorithm as shown in Fig. 5. To perform successful substrate mapping with virtual network, the following condition has to satisfy. When a request received from VN to the substrate network and a mapping is executed as per the condition. If the mapping is met as per condition, the resource manager module is successfully triggered. If NOT met the criteria, consider another virtual network request. This algorithm establishes that after the departure of virtual networks, the awaiting virtual networks could be relocated to minimize the usage of resource effectively. It's designed to address the networking components needed to support a virtualized infrastructure that includes virtual servers, storage, and even other networks. The advantage of NFV over other wireless network as follows:

(i) To reduce the demand of in-built purpose hardware and supporting pay-as-you-grow models to remove lavish over-provisioning

(ii) To reduce space, power and management of network services.

(iii) To scale up or down services to allow changing demands via software on any industry-standard server hardware.

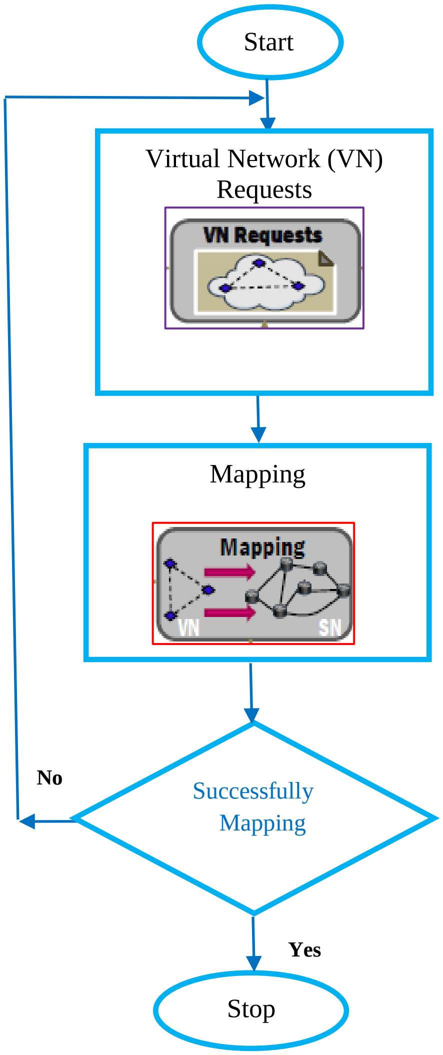

Fig 5 : Algorithm for VN Resource Management.

SD-NFV based Architecture:

The proposed architecture has divided into north-bound interface (NBI) and south-bound interface (SBI). This system may allow dynamically deploying better infrastructure to present industries. The NFVO is responsible for allowing new links, based on that the VNF manager manages to satisfy the network infrastructure service provider. Then the SDN controller plays a vital role for communication between devices and networks at both ends. The SDN controller depicts the dynamic architecture to reconfigure all the networks. Finally, the proposed framework integrates the network virtualization upon SDN principle of splitting the management (control) plane and data plane and the flow migration algorithm can dynamically govern the switching and link resources in this architecture virtually, thus our work facilitate the significance of both technologies

5. Conclusion

The paper mainly focused on the concept of Software Defined Network versus Network Function Virtualization towards Industry 4.0, which allows efficient and customized production. The key elements are addressed with the concepts of latest networking technology for industry 4.0 applications. As the implementation of the industry 4.0 using the advanced wireless sensor technologies like Industrial Wireless Networks, Software Defined Network& Network Function Virtualization increases organized supply chain and industrial management, data collection from the production lines and optimization of that data for the use of Energy Saving and optimized maintenance scheduling.In this work, we present a comprehensive framework in which virtualized SDN concepts has addressed. We attempt a framework by integrating SDN principle (decoupling technique) with NFV orchestration.

References

[1]. Raucea.A, Bello.LL, and O. Mirabella, “Design and implementation of an educational testbed forexperiencing with industrial communication networks,” IEEE transactions on industrial electronics, vol. 54, no. 6, december 2007

[2]. J. Lloret, Wan J D. Zhang S. Zhao L. T. Yang "Context-aware vehicular cyber-physical systems withcloud support: Architecture challenges and solutions" IEEE Commun. Mag. vol. 52 no. 8 pp. 106-113Aug. 2014.

[3]. Imran.M ,Z. Shu J. Wan D. Li J. Lin A. Vasilakos "Security in software-defined networking: Threatsand countermeasures" Mobile Netw. Appl. pp. 1-13 Jan. 2016.

[4]. Giannelli P, Qin Z. G. Denker C.Bellavista N. Venkatasubramanian "A software defined networkingarchitecture for the Internet-of-things" Proc. IEEE Netw. Oper. Manage. Symp. (NOMS) pp. 1-9 May 2014.

[5]. Feamster and H. Kim N. "Improving network management with software defined networking" IEEE Commun. Mag. vol. 51 no. 2 pp. 114-119 Feb. 2013.

[6]. Sezer et al. S "Are we ready for SDN? Implementation challenges for software-defined networks"IEEE Commun. Mag. vol. 51 no. 7 pp. 36-43 Jul. 2013.

[7]. Wan C. Bi, W. Yuan P. Deng T. Taleb J. "An unlicensed taxi identification model based on big data analysis" IEEE Trans. Intell. Transp. Syst. pp. 1-11 Nov. 2015.

[8]. Paul. S, D R. Jain, "Network virtualization and software defined networking for cloud computing: A survey" IEEE Commun. Mag. vol. 51 no. 11 pp. 24-31 Nov. 2013.

[9]. Kolasani B. Ramamurthy "Network innovation using OpenFlow: A survey" IEEE Commun. Surv. Tuts. vol. 16 no. 1 pp. 493-512 Feb. 2014.

[10]. Gerhard P. Hancke *IEEE, Senior Member,* Vehbi C. and Gungor, *Member IEEE,* "Industrial Wireless Sensor Networks: Challenges, Design Principles, and Technical Approaches," IEEE transactions on industrial electronics, vol. 56, no. 10, october 2009

[11]. Wiberg, Bilstrup., "Wireless Technology in industry applications and user scenarios". Procof ETFC, 2001,pp. 123-131.

[12]. Stankovic.J., D.Wager, Security in wireless sensor networks. Communication. ACM 47(6), 53-57 (2004).

[13]. Grosvenor.R, J. Qin, Y. Liu, A Categorical Framework of Manufacturing for Industry 4.0 andBeyond, Changeable, Agile, Reconfigurable & Virtual Production, Procedia CIRP 52 (2016) 173 – 178

[14]. Waldner.M, M. Lorenz, P. Gerbert, Rüßmann, Industry 4.0: The Future of Productivity and Growth in Manufacturing Industries, (April 09, 2015) 1-14.

[15]. Landherr. M, Neuge, M. Leis, Hippmann, "Industrie 4.0- Form the perspective of apllied research", 49th CIRP conference on Manufacturing systems (CIRP-CMS 2016).

[16]. S.Palanivel Rajan, M.Paranthaman, "Characterization of Compact and Efficient Patch Antenna with single inset feeding technique for Wireless Applications", Journal of Applied Research and Technology, ISSN: 1665–6423, Vol. 17, Issue 4, pp. 297-301, 2019

[17]. www.rfwirelessworld.com/Terminology/difference-between-SDN-and-NFV.html

[18]. D. P. Pezaros, Tso.F, K. Oikonomou and Kavvadia.E, "Scalable traffic-aware virtual machine management for cloud data centers," *IEEE Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Jun. 2014, pp. 238–247.

[19]. S.Palanivel Rajan, C.Vivek, "Analysis and Design of Microstrip Patch Antenna for Radar Communication", Journal of Electrical Engineering & Technology, E-ISSN No.: 2093-7423, P-ISSN No.: 1975-0102, Vol. No.: 14, Issue : 2, DOI: 10.1007/s42835-018-00072-y, pp. 923–929, 2019