What is role of SDN (Software Defined Network) in Wireless 5G Network?

1Drishti Dubey, 2Dr.Neeraj Shrivastava
Dept.of Electronics and Communication, R.J.I.T, Tekanpur, Gwalior

***Abstract*: In this paper study in SDN, network control data transmission and separate layers used in this network services. at this each technology infrastructure & how to used installation in network for each devices control, this architecture decouples the network controlling and forwarding functions enabling the network control to become directly programmable and under line infrastructure to be abstract for application and Network (nodes) services, at this technology continuous researchers have to work, implements then after path computation element 2004, at this most recently Ethane.**

I. INTRODUCTION

The term software define networking (SDN) has been coined in recent years, however the concept behind SDN has been evolving since trolled management of forwarding in network nodes implementations by research and industry groups include epsilon. A key challenge in SDN relates to separation of the control and data planes, and maintaining carrier grade service within this framework. The architecture requirements to meet operational expectations in carrier grade network are scalability, reliability, quality of service management [1]. For clarity SDN is described in this article with open networking foundation (ONF) [1] definition: in this SDN architecture, the control planes are decoupled, network intelligence and state are logically centralized, and state are logically centralized, and the underlying network infrastructure abstracted from the application.

SDN focuses on four key features:

- Separation of the control plan from the data plane.
- A centralized controller and view of the network.
- Open interfaces between the devices in the control plan(controllers)and those the data plane Programmability of the network by external applications

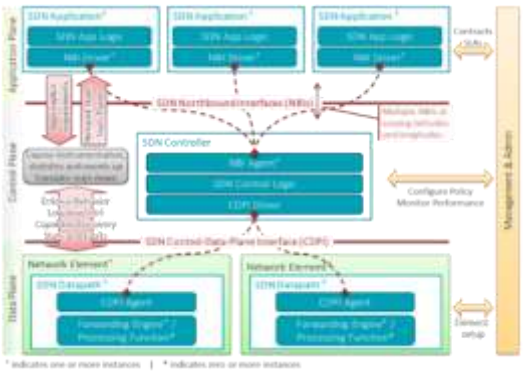

Fig.1. SDN-architecture overview transparent

2 .BACK GROUND : WHY SDN ?

Software defined networking and open flow emerged as a new paradigm of networking software defined software defined (SDN) is changing how we design ,build ,and operate network to achieve business agility, the fundamental purpose of the communication network is to transfer information from one point to another point.

3. DIFFICULT TO POTIMIZE-

Network operators are finding it difficult to introduce to revenue generating service and optimize services and optimize their expensive infrastructure data centers wide-area networks, and enterprise network.

4. KNOWN PROBLEMS-

- Network continues to have services known problems with security, robustness, manageability, mobility and resolvability that have not been successfully addressed so far.

5. CAPITATAL COST-

- Network capitals cost have not been reducing fast enough and operational costs have not been growing putting excessive pressures on network operators.

6. DIFFICULT TO CUSTOMIZE-

Even vendors and third parties are not able to provide customize cost effective solution to address their customers problems.

The control plane is responsible for configuration of the node and programming the paths to be used for data flows, once these paths have been determined, they are pushed down to the data plane, data forwarding at the hardware level is based on this control information, in this traditional approach, once the flow management (forwarding policy) has been defined, the only way to make an adjustment to the policy is via changes to the configuration of the devices. This has proven restrictive for network operators who are keen to scale their networks in response to changing traffic demands, increasing use of mobile devices, and the impact of big data. From these services –focused requirements, SDN has emerged. Control is moved out of the individual network nodes and into the separate, centralized controller. SDN switches are controlled by a network operating system (NOS) That collects information using the API and manipulate their forwarding plane, providing an

abstract model of the network topology to the SDN controller hosting the applications, the controller can therefore exploit complete knowledge of the network to optimize flow management and support service-user requirements of scalability and flexibility .for example bandwidth cab be dynamically allocated into the data plane from the applications.

7. WHERE SDN DOES TAKES US?

SDN implementation open up a means for new innovation and new application dynamic topology control (i.e. adjusting switch usage depending on load and traffic mapping) becomes possible with global network view, this introduce scope for network-wide access control, power management ,and home networking ,foe which the network view is not beneficial but absolutely necessary. The field of software defined networking is quite recent, yet growing at a very fast pace .still, there are important research challenges to be addressed .in this paper, we survey the state –of-the-art in programmable network by providing a historic perspective of the field and also describing in detail the SDN paradigm and architecture. The paper is organized as follows: in section 111 provide an overview of SDN and its architecture .it also describing the open flow protocol.

8. PERFORMANCE VS.FLEXIBILITY: HOW CAN THE PROGRAMMABLE SWITCH BE ACHIEVED?

On fundamental challenge of SDN is how to handle high-touch high security high-performance packet processing flows in an efficient manner. there are two elements to consider: performance. and programmability /flexibility. There the number of initiative [3,4]under way to allow programmability of existing network technologies in a manner conformant with the goals of SDN.beyond these ,the SDN programmability and performance problem remains a challenge to achieve node bandwidth beyond 100GB/s.General purpose processor (CPUs/GPPs)provide the highest flexibility. High-level programming language and design abstraction and the rapid development of complex packet processing functions. The limitation of CPU implementation, however, is its performance and power dissipation, constrained by the general purpose architecture. Nevertheless, multicore processor such as those of the Intel xenon family [5] can be achieve several tens to gigabits of throughout put by load balancing traffic onto multiple cores. Network flow processor (NPUs/NFPs) is optimized processor architectures for network processing. However, the flexibility of implementation is reduced as more detailed knowledge of the device is required in order to define the packet/flow processing function and take full advantage of devices parallel processing capabilities. State-of-the-art NPU (e.g., Metronomes [6]) Promise flow processing performance of over 200GB/s line rate per device and well over 100 Packet/s. programmable logic devices (PLDs)or field programmable gate arrays (FPGAs)have evolved into a technology for telecommunication and network processing. In comparison to microprocessor.PLD are configured using hardware design tools. This technology is ideal for implementing highly parallel and pipelined data paths that are tailored for individual network ***processing*** functions.PLD technologies (e.g., Tabula [7]) can achieve custom data path processing of over 200GB/s per device(e.g.,200M packet/s switching).application –specific standard products (ASSPs)are the cornerstone of high-performance network. they are designed and optimized for widely used function or products aiming for high volume .the drawback of ASSPs is their limited flexibility. as an application –specific solution ,ASICs offer the lowest flexibility while providing the highest performance, power and cost benefits.SDN products are expected to comprise proprietary ASICs to implement the SDN data plane. taking into account the programmability /performance trade-off of data processing technology, it is evident that only a hybrid approach will provide an effective technology solution for SDN.Main SDN node function can be decomposed into clusters of sub function such that features-specific technologies (within or across nodes)are used to satisfy the best performance trade-off in term of power dissipation, cost and scalability. On goals of SDN is to develop network built on general –purpose hardware. The combination of technologies as described in the hybrid architecture supports this goal. With a programmable interface built on standard hardware, a multivendor equipped network becomes a possibility.

9. SCABILITY: HOW CAN THE CONTROLLER BE ENABLED TP PROVIDE A GLOBAL NETWORK VIEW?

Assuming that the performance requirements can be achieved with in the hybrid programmable architecture, a further issue that has seen some discussion but limited solution is scalability in SDN. The issue can loosely be split into controller scalability and network node scalability. The focus here is on controller scalability. The focus here is on controller scalability in which three specific challenges are identified. The first is the latency introduced by exchanging network information between multiple nodes and a single controller. The second how SDN controllers communicate with other controllers using the east and westbound APIs .the third challenges is the size and operation of the controller back-end database. Within a pure SDN environment, a single controller or group of controllers would provide control plane services for a wider number of data forwarding nodes, thus allowing a system-wide view of network resources. An extension to the application layer traffic

optimization (ALTO) data model has been proposed by various organizations in which the ALTO server hosts capable of providing the desired resources. A vertical architecture with bidirectional information flow between each SDN controller and the ALTO server is proposed [8] to support to global network view in term of in proving application performance, ALTO with SDN would be a powerful tool. A specific solution to controller scalability is hyper flow [9].hyper flow is a controller application that sits on the NOX controller and works with an event propagation system. The hyper flow application selectively publishes events that change the state of the system, and the controllers reply all the published events to reconstruct the state. by this means all the controllers share the same consistent network-wide-view. Indeed, this concept of providing the network view by distributing the state over multiple controllers is highlighted in [10], in which a series of solutions to controller salability are described. Onix [11] is a distributed control platform providing abstraction for partitioning and distributing network state onto multiple distributed controllers. Notably, in [10] the authors conclude that the flexibility of SDN provides an opportunity in term of network manageability and functional scalability

10. ECURITY: HOW CAN THE SOFTWARE - DEFINE NETWORK BE PROTECTED FORM MALCIOUS ATTACK?

There has been limited industry and research community discussion to date on the security issue s associated with SDN. A greater focus on security is therefore required if SDN is going to be acceptable in broader deployment. Indeed, a security working group has been set up within open networking foundation (ONF) with this in mind. A number of issue are highlighted are highlighted here that underscore that need for further study and development of security solution. Potential security vulnerabilities exist across the SDN platform. At the controller –application level, question have been raised around authorization mechanism to enable multiple organizations to access network resources while providing the appropriate protection of these resources [12].not all application require the same network privileges, and a security model must be put in place to isolate application and support network protection. One potential solution is role based authorization. FortNox [13] is proposed to resolve the situation when a controller receives conflicting flow rules from two different applications. Role based authorization alone, however does not present a solution for the complexity of SDN requiring isolation of application or resources. The controllers are a particularly attractive target for attack in the SDN architecture open to unauthorized access and exploitation. Furthermore therefore, in the absence of a robust, secure controller platform, it is possible and carryout malicious activities. in the past, such attacks have targeted DNS servers(e.g., the kaminsky DNS attack [14]). Considerably greater damage could be done by such an attack on an SDN controller. a security technology such as transport layer security. (TLS)with mutual authorization between the controllers and their switches can mitigate these threats. Current specification of open flow [1] Describe the use of TLS. however, the security feature is optional ,and the standard of TLS is not specified. a full security specification for the controller-switch interface must be defined to secure the connection and protect data transmitted across it. with a single controller controlling a set of network nodes, implementation of authentication with TLS may provide the necessary security. However, with multiple controllers communicating with a single node or multiple centralized controllers, authrirization and access control becomes more complex. the potential for unauthorized access increase ,and could lead to manipulation of the node configuration and/or traffic through the node for malicious intent. One potential malicious attack is the denial of service (DOS) attack. Within the operation of SDN, as illustrated in there are two options for the handling of a new flow when no flow match exists in the flow table .either the complete packet or a portion of the packet head query. With a large volume of network traffic, sending the complete packet to the controller would absorb high bandwidth. On the plus side, the SDN architecture supports a highly reactive security monitoring analysis, and response system. Form the security perspective SDN can support.

Network forensics: facilitate quick and straightforward, adaptive treat identification and management through a cycle of harvesting intelligence from network, analyzing it, updating policy, and then reprogramming to optimize from network experience.

Security policy alteration: allow you to define a security policy and have it pushed out to all the infrastructure elements, reducing the frequency of miss configuration and conflicting policies across the infrastructure.

Security service insertion: facilitate security service insertion where application like firewalls and intrusion detection systems (IDSs) can be applied to specified traffic according to the organizations policies. However, the security of SDN will only be as good as the defined security policy .implementation of exiting authentication and authorization mechanisms can resolve some aspects of the security challenge. Meanwhile, threat detection and protection techniques will continue to evolve. the key, though, is for individual organization to effectively and comprehensively define their security policies in order to exploit the full extent of available network protection

11. INTEROPERABILITY: HOW CAN SDN SOLUTIONS BE INTEGRATED INTO EXISTING NETWORK?

TO the answer this question requires consideration of interoperability and standardization to support the transition from the traditional network model to SDN. It would be straightforward to deploy a completely new infrastructure based on SDN technology. For this, all element and devices in the network would be SDN-enabled. However there vital systems and businesses today. To simply "swap out" this network for new infrastructure is not going to be possible, and is only well suited for closed environments such as data centers and campus networks. To transition to SDN therefore requires simultaneous support of SDN and legacy equipment. The IETF path computation element (PCF)[15] could help in gradual or partial migration to SDN.

With PCF, the path computation component of the network is moved from the networking node to a centralized role, while raditional network nodes not using PCF continue to use their existing path computation for the flow across multiple network nodes. Further development is required to achieve a hybrid network nodes can operate in harmony. Such interoperability requires the support of an appropriate protocol that both introduces the requirements for SDN communication interfaces and provides backward compatibility with existing IP routing and multiprotocol label switching.

12. CHALLENGES IN SDN

The advent of the first generation (1G) wireless telephony changed the world by connecting people to people, as its predecessor technology could only connect anything to anything .more over unlike its predecessor,5G needs to be conceived as a set of technologies that are efficient and economical in terms of an array of key performance indicators (KPIs)that are efficient and economical in terms of an array of key performance indicators (KPIs)that are of interest to all stakeholders in an omnium-gatherum of application. These KPIs form an operator's perspective; include capacity, quality of service (Quos), and capital expenditure (OPEX).from a user's perspective, the KPIs include seamless connectivity, spatio –temporal uniformity of service, perception of almost infinite capacity or zero latency, and, last but not least ,the cost of service .obviously, no technology can offer infinite capacity or zero latency, but by maintaining a latency shorter than the human sensory and physiological delay in the type of application under use, a false perception of infinite capacity or zero latency cam be provided. for, example if the network can provide a latency below 100ms,10 ms, and 1ms for audio, video sensory organs and associated neural circuitry, the user will have a perception of infinite capacity and zero latency [16].however, designing the complete 5G to be fully self-organizing with end-to–end network behavior intelligence, from the perspective of a self-organizing network(SON)engine, so that it can exploit the cognition of the context of application as well as that of the state of the network to divert and focus the right amount of the network resources when and where needed such that users will perceive seamless and limitless connectivity.5G also has to take into account the recent marriage between Moore's law background computing power and the wireless technology that has triggered a new area the use of wireless communication for novel applications is only bound by imagination. There is hardly an aspect of human life that will not benefit from high -speed wireless communication including health care, mobility, education, governance, and manufacturing, smart grids, entertainment, sports, much more .in the next section we highlight the challenges in SON that have to be addressed before it can become capable of enabling 5G.in the subsequent section, we then present our proposed framework for big data empowered SON (BSON),which can not only address these challenges, but play a pivotal role in meeting the envisioned requirements of 5G.The core idea of BSON is to develop end-to-end visibility of the network by extracting intelligence from big data through application of appropriate machine learning tools.the three main features that make BSON distinct from state-of-the-art SON are:

Full intelligence of the current network status Capability of predicting user behavior Capability of dynamically associating the network response to the network parameters(NPs)

These three capabilities can go a long way to design SON that can meet 5G requirements. In the following, we explain the operation and functional blocks of the BSON framework.

The framework involves the following steps

.

- **Gather data:** from all sources of information into an aggregate data set, big data.
- **Transform:** big data into the right data by developing its. Blueprint. The knowledge building steps in this transformation are explained below. The underlying machine learning and data analytics are explained subsequently
- **MODEL:** Develop a network behavior model, to determine NP and expected new KPIs
- **RUN SON ENGINE:** use the SON engine on the model, to determine a new NP and expected new KPIs.
- **VALIDATE:** If a new NP can be vetted by the expert knowledge or prior experience of the operators, proceed with charges. Otherwise, determine the simulated behavior of the network for new NPs. if simulate behavior tallies the expected behavior (KPIs), proceed with new

NPs.(note this stage adds the much the needed transparency).

13. CONCLUSIONS

This paper describes a proposal programmability with in Network to support the dynamically nature used in future network functions. at this comprehensive proposal for an IEEE wide initiative on Software Defined Network (SDN), which is a new paradigm in designing networks and its components .at this number of outstanding challenges may be resolved .in this paper describe was presented no. of challenges in area of performance, security, scalability and interoperability.

SDN network contribute to the vision in communications of future time

.

REFERENCES

[1]. ITU.T.Rec.Y.1731,"OAM function and mechanisms for Ethernet based network, "https: //www.itu.int/ itudoc/itu-t.

[2]. ONF," software-defined networking: the new norm foe networks,"whitepaper,https://www.opennetworking.org.

[3]. "interface of routing system,"IRTF working group, available: https://datatracker.ietf.org/wg/irs/charter/

[4]. ETSI industry spec. group," Networking function virtualization,"
http://portal.etsi.org/portal/server.pt/community/nfv/367

[5]. R. ozdag," intel Ethernet switch FM6oooseries-soft-ware networking."http://www.intel.co.uk/content/dam/www/public/us/en/documents/white-paper/ethernet-switch-fm6000-sdn-paper.pdf

[6] netronome NPF6XXX flow processor, "http://netronome.com/pages/flow-processors/.

[7]. Tabula, www.taubla.com

[8]. IETF ALTO WG," use cases for ALTO with software defined networks,"http://tools.ietf.org/pdf/draft-xie-alto-sdn-use-cases-01.pdf.

[9]. A. Tootoonchian and y.ganjali," hyper flow: A distributed control plane for open –flow,"proc.2010 internet network management conf. research on Enterprise networking, 2010.

[10]. S.yeganesh, A.Tootoonchian, and y. ganjali," on scalability of software-defined networking model," internet

[11]. T. Koponen et al.," onix: A distributed control platform for large-scale production network," OSDI, 2010.

[12]. IETF Network WG," security requirements in the software defined networking model, "internet draft, https://datatracker.ietf.org/doc/draft-hartman-sdnsec requirement/

[13]. P. Porras et al.,"A security enforcement kernel for open-flow networks ,"proc.1st WKsp.hot topics in software defined networks,2012,pp.121-26

[14]. " kaminsky DNS attack, "http: //dankaminsky.com

[15]. IETF WG," Path computation element, "http://data-tracker.ietf.org/wg/pce/charter/.

[16]. G.P. fettweis,"a 5G Wireless communication vision, "microwave j., dec.2012, pp.24-36

