SECURITY TECHNQUIES IN SOFTWARE DEFINED NETWORKS WITH 5G NETWORKS

Santosh A. Darade[1], Yogita S. Hande[2], M. Akkalakshmi[3]

[1]*Computer Science & Engineering, GITAM School of Engineering, Hyderabad, India*
[2]*Computer Science & Engineering, GITAM School of Engineering, Hyderabad, India*
[3]*Department of Information Technology, GITAM School of Engineering, Hyderabad, India*

Abstract

Today user wants to access many applications, database of different servers which are located at different remote locations, creating high level machine to machine traffic before it returns to the intended user. Users want to access these applications from any devices (smart phones, tablets & notebooks), anywhere, anytime & from any networks whether it is wired or wireless, which results additional data traffic across wide area network. These increasing traffic required additional number of network capacity servers in the data center with large & increased bandwidth, which demands huge parallel processing on thousands of interconnected servers. The emerging network evolved called as Software Define Networking (SDN) to provide open interfaces that enable network administrator/user to develop a software that can control the connectivity provided by a set of network resources and the flow of network traffic through all these resources (router, switch), along with possible monitoring and modification of traffic that may be performed in the network. Our aim is to keep track or protect these traffic which is transfer from one machine to another, protection from unauthorized users and information must be available to authorized users when it is indeed. As the speed increases the network traffic also increases, with the basic architecture of wired technology it is not possible to provide a good speed. We can take challenge to implement new technologies called 5G Fifth Generation Mobile Technology that enable us to meet these challenges into software defined networks.

Keywords—*Software Define Networking; Fifth generation mobile Technology;5G;*

----------***----------

1. INTRODUCTION TO SOFTWARE DEFINE NETWORKING

The emerging technology within network environment evolved called as Software Defined Networking (SDN) that promises to solve many of the existing networking limitations [1]. It is an approach to computer networking, work done at Berkeley and Stanford Universities later on released for public use.

SDN is defined as the physical separation of the network control (network intelligence) & data plane (responsible for forwarding the traffic), where a control plane controls different devices & data plane is responsible to forward, drop the network traffic controlled by network controller. In SDN architecture, the control and data planes are detached, with logically centralized intelligence controller (SDN Control software) & the underlying network infrastructure is abstracted from the applications. Which enable network administrator/user to build high scalable, flexible networks that can easily adapt changing business needs via software rather than the traditional approach via hardware, the SDN basic layer wise architecture is shown in fig. 1 [1][2].

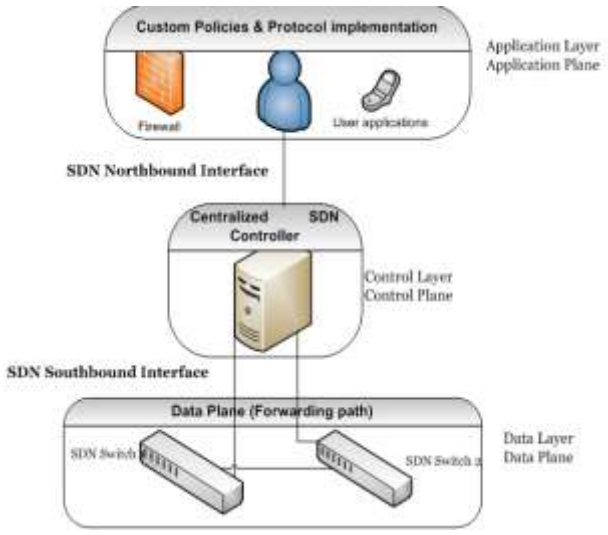

Fig. 1 Layer wise SDN architecture

The three layers of logical SDN architecture namely Application layer (Application plane), Control Layer (Control Plane), & Infrastructure layer (Data Plane). The applications (load balance, firewall, traffic security management & others) exist in the application layer and communicate their network requirements toward the controller plane via northbound interfaces, often called application - control plan interface. The control plane called Network intelligence is (logically) centralized in software-based SDN controllers, which maintain an overall view of

the network & having exclusive control over a set of resources exposed by network elements in the data plane. Control plane interact data plane via southbound interface, often called control-data plane interface (i.e. open flow).

Data plane also called as forwarding plane which consist of set of network elements (device, switches) responsible to moves the data packets on the infrastructure layer to their next destination which is controlled by the remote controller. SDN architectures support a set of Application Programming Interfaces (APIs) which helps to implements common network services, such as routing, multicast, security, access control, bandwidth management, traffic engineering, quality of service, and all forms of policy management.

2. TODAY'S TRADITIONAL NETWORK & 5G CHALLENGES

Internet is ever growing and we are truly pebbles in a vast ocean of information. When it comes to the Internet there are millions and millions of users logging on and off on a daily basis. Following are the present challenges of traditional networks.

1. *Changing traffic patterns***:** If user wants to access their applications from any device, anywhere, anytime & from any networks whether it is wired or wireless which results additional data traffic across wide area network. This shows we need a computational model or underlying networks architecture to carry large amounts of traffic, and to deploy a number of distinct, dynamic applications & service which will handle all these traffic through programmable software.
2. *Need for more bandwidth***:** As mentioned earlier because of increased traffic requires parallel processing on thousands of inter-connected servers. Data center also need to be scaling to very large size, while maintaining end-end-end connectivity. With the higher media/content traffic increases, requirement of more bandwidth increases.
3. *Need of flexible access to IT resources:* Users want to access the applications from any devices, anywhere, anytime & from any networks whether it is wired or wireless, which results additional data traffic across wide area network. It is mandatory to protect these devices also while protecting corporate data [2].
4. *Insecure Connectivity:* The success of the Internet is openness and connectivity (end to end). However, few investors are limiting these fantastic features for more reliable revenue.
5. *Static nature of network:* Network reconfigurations are performed relatively in static way to avoid the risk of service interruption. In case of addition & deletion of network devices like routers & switches it very difficult to network administrator to recognize the networks & manage it to earlier constraints. It is also very difficult to apply a consistent set of access, security, quality of service (QoS), and other policies.
6. *Scalability issue:* We need a new network which is scalable, high-performance; low-cost connectivity among many physical servers, flexible, supportive & programmable, it must give better differentiated service to users with different applications and needs.
7. *Security, Authentication, Trust:* 12% of IT business technologist stated that SDN has security challenges, and 31% were undecided whether SDN is a less secure or a more secure network paradigm than others [3]. A great concern to businesses, public administration and citizens are security and authentication. They are not addressed efficiently in the current Internet. So it is very important to increase trust without compromising openness.
8. *Volume:* The biggest task in internet in coming time is to handle 4 billion mobile users worldwide.
9. *Privacy and Confidentiality*: A machine to machine communication is also growing these days. The new application must obey user's right to privacy and confidentiality.

3. STATE-OF- ART/ LITERATURE SURVEY

- As mentioned earlier Internet is ever growing and we are truly pebbles in a vast ocean of information. If Software Define Networking popularity is increasing, then the security in SDN must be an important agenda. Different authors expressed their views about security challenge in SDN.
- In [4] Nick McKeown et.al encourages networking researcher to add OpenFlow to their switch products for deployment in college campus backbones and wiring closets. But experimental results showed that specific security features are not provided during implementation of OpenFlow table.
- The proposed architecture of scalable intrusion detection Scheme implemented on virtual software defined networking [5], environment using a virtualization infrastructure focuses on distributed traffic sampling at network switches for malicious traffic inspection. If the capacity of traffic increases the present IDS is not scalable for future SDN based technology.
- Antonio Gonzalez et.al [6] programmability offered by Software Defined Networks (SDN) to provide architecture for an Intrusion Prevention Scheme not specifies position of IDS in SDN networks.
- The Learning-IDS (L-IDS) is an intrusion detection Scheme for networks used to communicate with embedded mobile devices. Richard Skowyra, et.al [7] proposed L-IDS can transparently adapt to changing network state in the presence of end-host mobility but IDS will not suitable for real world traffic. The technique proposed is anomaly based detection, so chances of generating false alarms are more. There is no provision made for false positive alarm generation.
- SDN framework and the security challenges introduced by the framework discussed by categorizing the existing work, a set of conclusions and proposals for future research directions are presented Sandra Scott-Hayward et.al [8]. SDN framework has been recognized, but solutions to tackle the challenges are not addressed.

- 5G Mobile Phone Concept discussed by Toni Janevski [9] not addressing the conversions techniques of 5G with any other networks technologies.
- New control plane for 5G network architecture with a case study on unified approach to mobility, handoff, and routing management and offer connectivity management as a service (CMaaS) proposed by Volkan Yazıcı et.al [10] as number of nodes in the wireless network increase complexity of mobile networks also increases.
- The cross-layer architecture combining SDR and SDN characteristics proposed by HSIN-HUNG CHO et.al [11] can effectively use the frequency spectrum and considerably enhance network performance. SDR & SDN security issues not addressed.
- Software defined wireless networks proposed by CARLOS J, S. et.al [12] mentioned the ongoing standardization efforts, and elaborated the possible advantages and disadvantages of SDN in wireless networks. Use cases addressed shows that the operation and management of wireless networks is more complex & along with possible solutions on security and privacy.

4. RESEARCH QUESTIONS/ CHALANGE

Popularity of Software Define Networking is increasing then security in SDN must be an important agenda. The principles of a secure communications are confidentiality, integrity, availability of resource to authorized users, authentication and non-repudiation. The success ration of Internet is reduced because of network security threats, denial of service attacks, internal as well outside attacks, malicious software. Security professionals must take an initiative to secure the data, the network assets (e.g. devices). To design a programmable software design networks & checking it scalability as well as complexity is at high priority. To develop certain mechanisms, tools & techniques which will helps to overcome security issues of SDN network

4.1 Objective of Research

Objective of this research is to address security issues in Software Define Networking for 5G networks & to detect the malicious traffic by proposing general methods of security in SDN for 5G networks. To find conversions methods of SDN with 5G networks (vice versa) along with methods of verification of conversions.

4.2 Proposed Work

In proposed architecture, the network traffic is receiving at switch level & from switch it communicates to SDN controller for their route. SDN controller is configured to install the rule to send the packet to its destination and to the Intrusion Detection Scheme & also responsible for authentication of hosts and policy enforcement. The Intrusion Detection Scheme (IDS) contains set of rules (database) patterns, based on these rules IDS will detect that whether the packet is malicious or not. (For Example if packet is coming from same source again & again the IDS will check the number of packets coming from same source within the specific time duration).

If it is match with set of predefined rules IDS will detect that packet is malicious or not. Different algorithms are used to define set of rules like Fuzzy logic, Genetic Algorithms, Genetic Programming. With the help of crossover & mutation techniques available in genetic algorithm we can update number of rules &for better protection of SDN networks. If Intrusion Detection Scheme identifies a malicious flow of packets it generates an alert which will send to the controller. When the controller is notified by the IDS, it lists all the flows installed in the OpenFlow switches and set a drop action to all the flows that matches the malicious one. As per the IDS results, the malicious packets get block at switch level itself. Our first proposed architecture of Intrusion Detection Scheme with Software Define Network is shown in Fig. 2

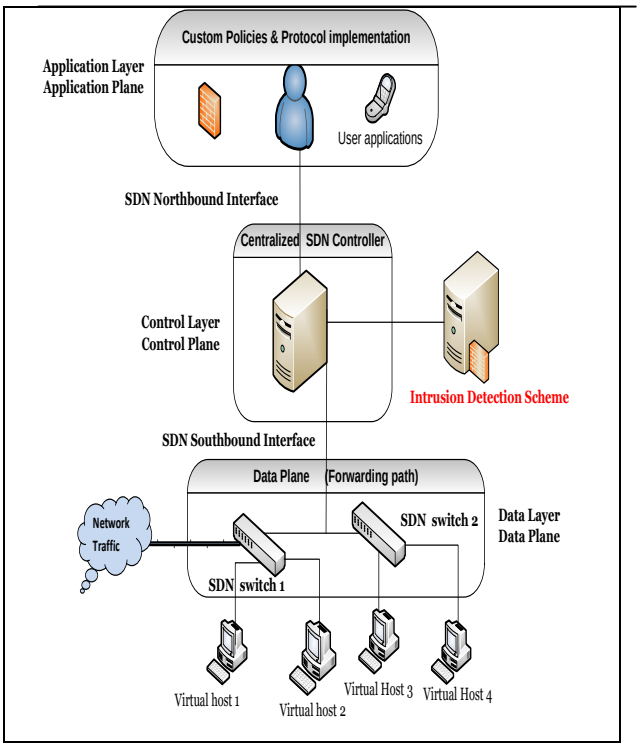

Fig. 2 Intrusion Detection Scheme with Software Defined Networks

4.3 Benefits of Implementing SND with IDS

Intrusion Detection Scheme is the most important tools that analyze & protect networks from inside as well as outside attacks, malicious attacks & monitor network behavior or patterns which look suspicious & detect them as an intrusion.

- SDNs lower operating expenses: - Implementing SDN with IDS requires less expense to design a SND networks which avoid all burdens of network developing team.
- Flexible: - The development tools available make it easy to reconfigure the network very smoothly & it depends on user, how they want their own networks to be.

- Provides virtual management for computing & storage resources so that resellers can also plan IT strategies more effectively for their customers & apply security policies to the given networks.
- The biggest advantage of SND network is infrastructure savings, because of separation of control & data plane reduces hardware prices as routers and switches must compete on price-performance features.

5. PROPOSING GENERIC FRAMEWORK FOR IDS IN SDN FOR 5G NETWORKS

The unpredictable growth in wireless Internet use is showing that it not going to end in any case & no signs of slowing down. Existing cellular networks shows insufficiency in meeting this demands, due to their inflexible and expensive equipment as well as complex and non-agile control plane. As discussed in previous section Software defined networking is emerging as a natural solution for next generation cellular networks as it enables further network function virtualization opportunities and network programmability. The 5G terminals will have software defined radios and modulation schemes as well as new error-control schemes that can be downloaded from the Internet.
The 5G terminals have ability to combine different wireless technologies & flows from different technologies for handling user-mobility; terminal will make the final selection among different wireless as well as wired access network providers for a given service. Mobile networks are composed of two components: the radio access network (RAN) and the core network (CN). While the RAN provides connectivity of the User Equipments (UEs) to the network via base stations (eNBs), the Core Network provides paths between eNBs and various services as well as outside networks. Generic programmable framework for IDS in SDN for 5G networks is shown in Fig. 3

5.1 Research Methodology

The proposed work required installation of *mininet* emulator on Ubentu 14.10 along with Virtual Box. Then need to add programmability on SDN controller according to rules controller sends instructions to different hosts & to the IDS upon receiving data packets from controller IDS (Genetic Algorithm to detect malicious traffic) will check whether packets look suspicious or not.
If it matches with predefined set of rules IDS will generate & alert signal & send it to controller for further action. Controller sent & instruction to block the packets at SDN switch. In this way the malicious traffic get blocked into SDN network with the help of IDS in SDN.

- To find the 5G networks simulation tools & combines it with *mininet* SDN network.
- To find the 5G networks conversion tools & techniques to combine it with SDN networks.

5.2 Outcome

- Proposed methodology helps network administrator to design programmable software Defined Network wants to access many applications, database of different servers which are located at different remote locations, without creating machine to machine traffic before it returns to the intended user.
- With proposed methodology user can access their applications from any devices smart phones, tablets & notebooks, anywhere, anytime & from any networks whether it is wired or wireless. Once the user set networks policies with programmable SDN to allow only that packet which are not malicious into their networks which can avoid additional data traffic across wide area network.
- We can also protect our data traffic whether it is on wired or wireless network. The proposed architecture of 5G conversion with SDN IDS helps to keep track on increasing network traffic also find the threat from both the networks

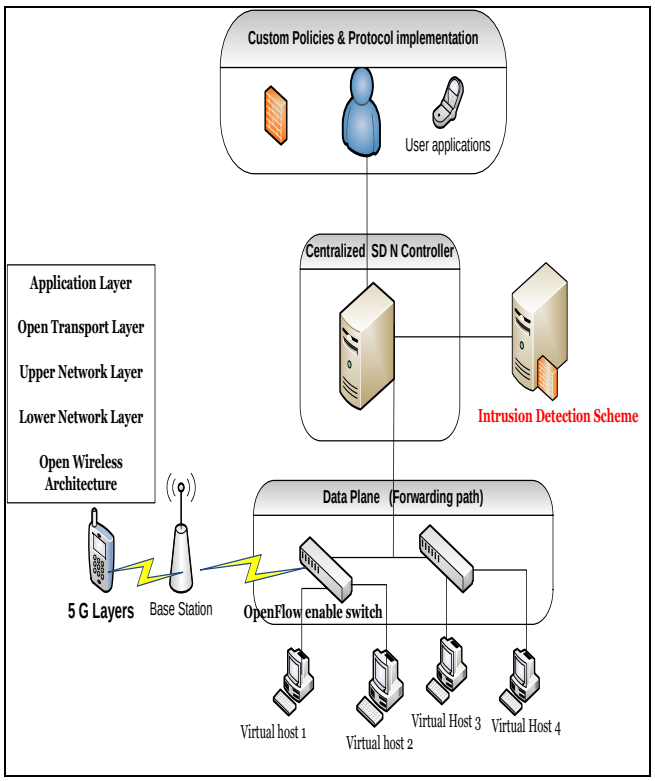

Fig.3 Intrusion Detection Scheme in SDN for 5G Networks

6. CONLCUSION AND FUTURE SCOPE

The proposed architecture of Software Defined Network with IDS is useful tool for an Intrusion Detection, which will block the malicious flow of the network traffic & notifies to controller. The 5G architecture with SDN IDS helps to track the increasing network traffic of wired as well as wireless network. Our future work is to define methodology for 5G conversion techniques in SDN & apply intrusion detection algorithm, to monitor the network traffic & also allowing multiple IDS virtual machines running in the same network.

We will further study the attack pattern, characteristics of various malwares, finding out malware detection techniques and explore the possibilities of employing them in the

context of SDN with IDS. The proposed method is trying to simulate on *mininet* & with combination of different wireless tools available. I addition to that want to take better advantage of infrastructure and test our Scheme at a larger scale in order to give good optimization & scalability to our Scheme design. Future work is to find the conversions techniques of SDN with 5G.

REFERENCES

[1] Open Networking Foundation "SDN architecture" Issue 1 June, 2014.

[2] ONF White Paper "Software-Defined Networking: The New Norm for Networks" April 13, 2012.

[3] Manar Jammal, Taranpreet Singh, et.al "Software-Defined Networking: State of the Art and Research Challenges", Department of Electrical and Computer Engineering, Western University, Canada.

[4] Nick Mckeown, Tom Anderson, et.al "OpenFlow: Enabling Innovation in Computer Networks, 2008.

[5] Chiwook Jeong, Taejin Ha, Jargalsaikhan Narantuya et.al **"**Scalable Network Intrusion Detection on Virtual SDN Environment**"** IEEE third International conference on clod networking, 2014.

[6] Antonio Gonzalez Pastana Lobato et.al "An Architecture for Intrusion Prevention using Software Defined Networks" Universidade Federal do Rio de Janeiro - GTA/COPPE - Rio de Janeiro, Brazil.

[7] Richard Skowyra et.al "Software-Defined IDS for Securing Embedded Mobile Devices" IEEE 2013.

[8] S. Scott-Hayward et.al "SDN Security: - A Survey" IEEE SDN for Future Networks and Services (SDN4FNS) 2013.

[9] Toni Janevski "5G Mobile Concept" University "Sv. Kiril i Metodij", Faculty of Electrical Engineering and Information Technologies, IEEE 2009.

[10] Volkan Yazıcı, Ulas¸ C. Kozat, et.al *"*A New Control Plane for 5G Network Architecture with a Case Study on Unified Handoff, Mobility, and Routing Management*"* IEEE Communications Magazine November 2014.

[11] HSIN-HUNG CHO et.al "Integration of SDR & SDN for 5G", IEEE October 21, 2014.

[12] CARLOS J. BERNARDOS et.al "An Architecture for software defined wireless networking" IEEE Wireless Communications June 2014.