Cooperative Diversity in Wireless Networks: A Survey

Manju Lahare[l] Mr. Kauleshwar Prasad[2]
[1]M.Tech. Student [2]Assistant Professor
[1,2]Department of Computer Science & Engineering
[1,2]Bhilai Institute of Technology, Bhilai, India

Abstract— Computer networks are stereotypically constructed from a number of network devices such as routers, switches, hubs and abundant types of devices with numerous complex protocols employed on them. The old-fashioned method of controlling and managing the network is not acceptable due to the incorporation of various types of networks. Software defined network acts as a challenging solution for this problem. In SDN, each and every decision is monitored, configured and changed by the software. This becomes possible because the control is transferred from number of distributed devices to the one or more general purpose servers called controllers. In this paper we have proposed a custom topology based on SDN, which will improve packet delivery time over network, we have also compared custom topology with hybrid topology based on packet delivery factor.

Key words: SDN

I. INTRODUCTION

Networks of the twenty first century offer immense flexibility to the business and individual users, but at the cost of higher complexity. Controlling and managing such networks have become highly complex and specialized activities. In this context Software defined networking (SDN) is being looked upon as a promising paradigm that has the power of changing the networking world. Through SDN, network administrators would be able to get a better control over the traffic flows. They would also be able to easily program and modify network policies to manage these flows according to the user requirements. This becomes possible because SDN transfers control and policy functions from a large number of distributed devices to one or more general-purpose servers. There has been heightened interest in recent years in the academia, industry and the network operators in research and implementation of SDN. It now appears that the time for SDN has finally arrived.

Though the concepts that evolved into SDN have been around for over 20 years, the developments that are more directly attributable to SDN are relatively recent. The development of General Switch Management Protocol (GSMP) by Ipsilon , in 1996, Cambridge's The Tempest in 1998, IETF Forwarding and Control Element Separation (FORCES) in 2000 and IETF Path Computation Element (PCE) in 2004 are important landmarks. PCE is centralized element for computing path for the network nodes. Along with Open flow it is one of the main approaches towards SDN. Also important were the Princeton's Routing Control Platform in 2004 and 4D (decision, dissemination, discovery, and data) approach to separation of control logic from networking elements, in 2005. For many experts, SDN started evolving when the concepts of SDN were first explored in the Ethane project at Stanford University in 2007 [Stanford]. Standardization of Open flow as the first communication interface for SDN by the Open Network Foundation in 2009 was the game changer.

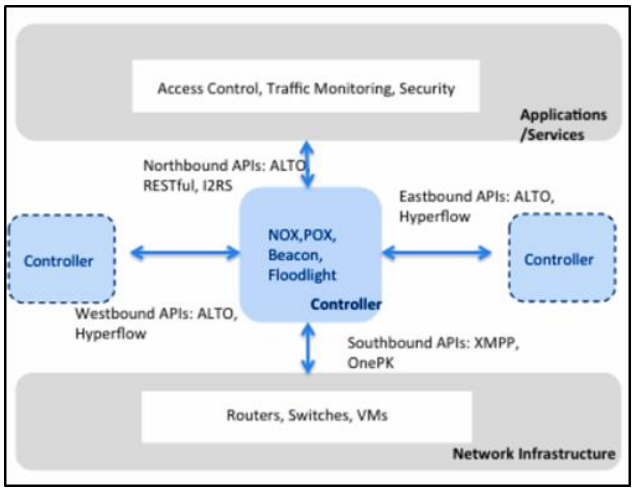


Fig. 1: SDN Architecture

In traditional network with network nodes that have control and data planes integrated, they have institutionalized ways to offer services. A key challenge in SDN is maintaining carrier grade service within the framework of separation of control and data planes. There have been new developments in the traditional networks, like increasing stress on energy efficiency and reducing the carbon footprint, which SDN and Open flow will have to cope with right from the beginning.

A full security specification for the controller-switch interface must be defined to secure the connection and protect data transmitted across it. When there are multiple controllers in the network, potential for unauthorized access to nodes and alteration of its configuration and traffic rerouting may take place. It could lead to Denial of Service (DoS), which could have crippling effect on the network. SDN strength in open interfaces and known protocols become a boon for attackers.

II. LITERATURE SURVEY

We have gone through several literature which are as follows.

Jinyong Jo et. al. said that Existing home-networking protocols do not robustly incorporate universal connectivity among multiple homes, which leaves their use restricted to a single home. In addition, even in a single home network, new functional requirements ask for more diversified forms of networking control. This paper presents in-home consumer electronic devices that incorporate the emerging SDN (Software Defined Networking) paradigm. The proposed devices enable ondemand provisioning for protocol-agnostic home networking and thus provide a high degree of flexibility for intra-home networking as well as wider connectivity for inter-home networking. The feasibility of the prototype devices is verified by realizing a

All rights reserved by www.ijsrd.com

multi-home visual-sharing scenario and by supporting diverse future scenarios [IEEE 2014].

Marc Mendonca et. al. said that The idea of programmable networks has recently re-gained considerable momentum due to the emergence of the SoftwareDefined Networking (SDN) paradigm. SDN, often referred to as a "radical new idea in networking", promises to dramatically simplify network management and enable innovation through network programmability. This paper surveys the state-of-the-art in programmable networks with an emphasis on SDN. We provide a historic perspective of programmable networks from early ideas to recent developments. Then we present the SDN architecture and the OpenFlow standard in particular, discuss current alternatives for implementation and testing SDN-based protocols and services, examine current and future SDN applications, and explore promising research directions based on the SDN paradigm [IEEE 2014].

Nick McKeown et. al. proposes OpenFlow: a way for researchers to run experimental protocols in the networks they use every day. OpenFlow is based on an Ethernet switch, with an internal flow-table, and a standardized interface to add and remove flow entries. Our goal is to encourage networking vendors to add OpenFlow to their switch products for deployment in college campus backbones and wiring closets. We believe that OpenFlow is a pragmatic compromise: on one hand, it allows researchers to run experiments on heterogeneous switches in a uniform way at line-rate and with high port-density; while on the other hand, vendors do not need to expose the internal workings of their switches. In addition to allowing researchers to evaluate their ideas in real-world traffic settings, OpenFlow could serve as a useful campus component in proposed large-scale testbeds like GENI. Two buildings at Stanford University will soon run OpenFlow networks, using commercial Ethernet switches and routers. We will work to encourage deployment at other schools; and We encourage you to consider deploying OpenFlow in your university network too [ACM SIGCOMM 2008].

Heng Cui et. al. said that Software-defined networking (SDN) eases network management by centralizing the control plane and separating it from the data plane. The separation of planes in SDN, however, introduces new vulnerabilities in SDN networks, since the difference in processing packets at each plane allows an adversary to fingerprint the network's packet-forwarding logic. In this paper, we study the feasibility of fingerprinting the controller-switch interactions by a remote adversary, whose aim is to acquire knowledge about specific flow rules that are installed at the switches. This knowledge empowers the adversary with a better understanding of the network's packet-forwarding logic and exposes the network to a number of threats. In this paper, we collect measurements from hosts located across the globe using a realistic SDN network comprising of OpenFlow hardware and software switches. We show that, by leveraging information from the RTT and packet-pair dispersion of the exchanged packets, fingerprinting attacks on SDN networks succeed with overwhelming probability. We additionally show that these attacks are not restricted to active adversaries, but can also be mounted by passive adversaries that only monitor traffic exchanged with the SDN network. Finally, we discuss the implications of these attacks on the security of SDN networks, and we present and evaluate an efficient countermeasure to strengthen SDN networks against fingerprinting. Our results demonstrate the effectiveness of our countermeasure in deterring fingerprinting attacks on SDN networks.

S.No.	Author/Title/Publication	Description
1.	Dimitri Staessens et. al./Software Defined Networking: Meeting Carrier Grade Requirements/ IEEE 2011	Show that Openflow can restore traffic quite fast, but its dependency on a centralized controller means that it will be hard to achieve 50 ms restoration in large networks serving many flows. In order to achieve 50 ms recovery, protection will be required in carrier grade networks
2.	Keshav Sood et. al./ Software-Defined Wireless Networking Opportunities and Challenges for Internet-of-Things: A Review/ IEEE 2016	Presented the current key research efforts on SDWN. Author emphasize that integration of SDN in IoT network can potentially bring exciting opportunities. Author also highlighted that the traditional network tools to collect, store, process, and forward massive data are inefficient to meet critical future IoT network needs.
3.	Danda B. Rawat et. al./Software Defined Networking for Reducing Energy Consumption and Carbon Emission/ IEEE 2016	Presented steps toward converting a typical network set-up into an OpenFlow controlled Software Defined Network (SDN); to reduce the power consumption used by the network. Mininet is useful in visually representing a physical network to optimize power consumption using Software Defined Network
4.	Shibo Luo et. al. /A Multi-stage Attack Mitigation Mechanism for Software-defined Home Networks/ IEEE 2016	A multi-stage attack mitigation mechanism is proposed for SDHN using Software-Defined Networking (SDN) and Network Function Virtualization (NFV). Firstly, an evidence-

All rights reserved by *www.ijsrd.com*

		driven security assessment method using SDN factors and NFV-based detection is designed to perform security assessment along with observed security events. Secondly, an attack mitigation countermeasure selection method is proposed. The evaluation shows that the proposed mechanism is effective for multi-stage attack mitigation in SDHN.
5.	Ann Sabeeh et. al./ A Hybrid Intelligent Approach for Optimising Software-Defined Networks Performance/ IEEE 2016	A hybrid intelligent system has been proposed for modeling and optimizing the Software-Defined Network (SDN). An artificial neural network (ANN) with a single layer in the hidden zone has been trained to map the inputs and the performance of the network. The results have shown that the network gives a very acceptable MSE, we hereby this has been demonstrated as being less than 2.466×10-8.

Table: 1

III. MOTIVATION

In traditional networks control and data planes are tightly integrated in the network devices like switches and routers. Once the forwarding policy has been defined, the only way to change it is by changing the configuration of all the affected devices. This is time consuming and puts a limit on scalability and also meeting challenges of mobility and big data. The actual networks have by now become complicated and expensive to maintain. At the same time, revenues are globally declining. Operators are, therefore, looking for solutions that can unify network management and provisioning across multiple domains. SDN has been developed to take care of what is missing in the traditional networks. This has been done by moving control out of the network nodes and keeping it centralized in a server called controller, which has the complete view of the network. This controller can then use the complete knowledge of the network to optimize flow management and support service-user requirements of bandwidth, scalability and flexibility. The separation of the forwarding hardware from the control logic allows easier deployment of new protocols and applications, simplifies network visualization and management.

IV. PROBLEM IDENTIFICATION

With the emergence of new protocol and technologies, the network is getting complex. It's a difficult task to meet the needs of the network with the increasing traffic and data. A key challenge in SDN is maintaining carrier grade service within the framework of separation of control and data planes. There have been new developments in the traditional networks, like increasing stress on energy efficiency and reducing the increasing traffic, which SDN and Open flow will have to cope with right from the beginning. Open Flow (OF) is considered one of the first SDN standards. It originally defined the communication protocol in SDN environments that enables the SDN Controller to directly interact with the forwarding plane of network devices such as switches and routers, both physical and virtual (hypervisor-based), so it can better adapt to changing business requirements. In order to have the maximum benefit, the controller would be expected to power up/down parts of the switch on demand. Open flow currently has limited support for the control of power management in the switches and would need extra messages for controlling individual ports. The controller should also be able to query the nodes and find out the available energy efficiency features.

- In traditional network with network nodes that have control and data planes integrated, they have institutionalized ways to offer services.
- More developmental work is required to achieve a hybrid SDN infrastructure in which SDN enabled and traditional integrated nodes inter-operate.
- It has to be ensured that the performance of SDN in terms of packet delivery is commensurate with the traditional networks if not better.
- Cost is very high in traditional network.

V. PROPOSED METHODOLOGY

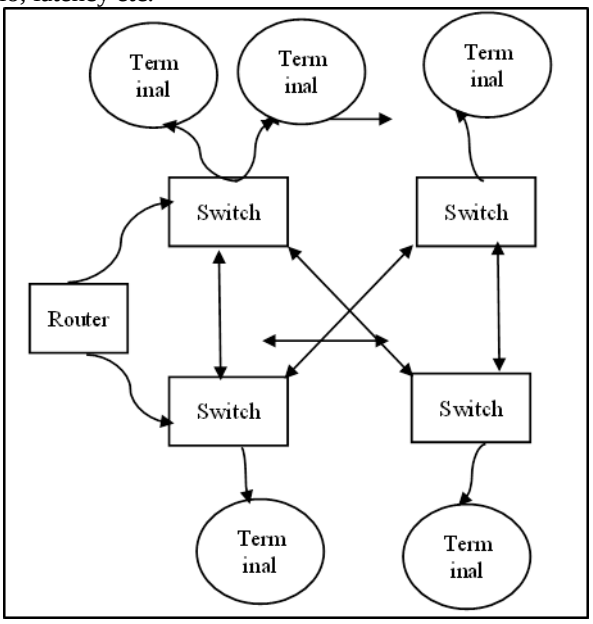
SDN provides a new, dynamic network architecture that transforms traditional network backbones into rich service-delivery platforms. By decoupling the network control and data planes, SDN-based architecture abstracts the underlying infrastructure from the applications that utilize it. This makes the networking infrastructure programmable and manageable at scale. SDN adoption can improve network manageability, scalability and dynamism in enterprise data center. The flexibility provided through SDN has allowed its users to efficiently route their flows in networks and conveniently build security applications on top of their networks. SDN-enabled core and edge nodes with a proper SDN controller and network application can be considered as a novel cloud federation mechanism.

To overcome the problem identified we have proposed a custom topology which will improve the packet delivery ratio over network in comparison with hybrid topology.

Custom topology means a user defined computer network, i.e. user can design a network by means of different network entities so as to improve the several

All rights reserved by *www.ijsrd.com*

network parameters such as throughput, packet delivery ratio, latency etc.



VI. PROPOSED ALGORITHM

1) Step-1. Input as different network elements.
2) Step-2. Add router and switches and design network.
3) Step-3. Add different parameter to each network elements.
4) Step-4. Evaluate the performance of network.
5) Step-5. If optimal network found with improved packet delivery ratio then suggest the topology for network.
6) Step-6. Else again change the network entities and their parameters.
7) Step-7. Repeat step-5, 6 still optimal result.

VII. RESULT & DISCUSSION

For simulation of our proposed scheme i.e. steps to design an optimized network centered on optimizing packet delivery ratio, we have used Mininet framework and check the network we have used Wireshark and plot graph and compared our custom topology with hybrid topology.

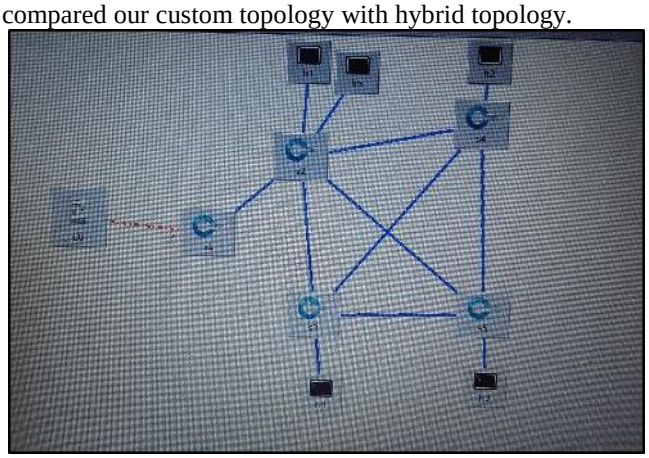


Fig. 3: Proposed Custom Topology

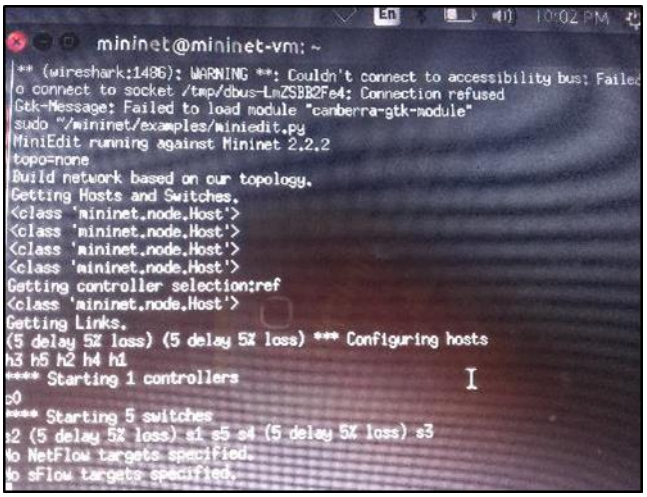


Fig. 4: Custom Topology Network Parameters

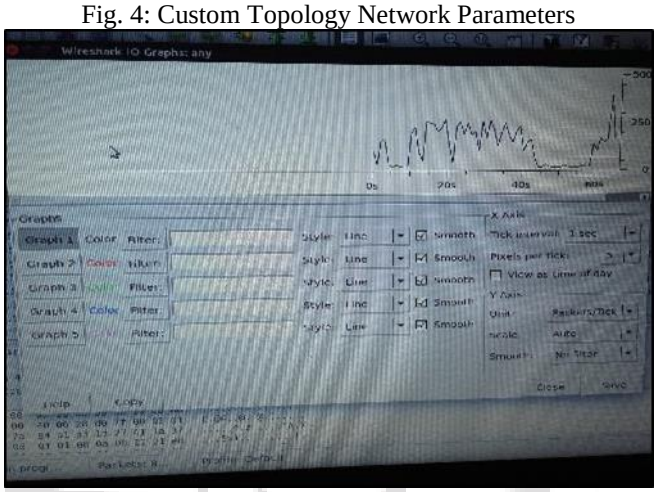


Fig. 4: Packet Delivery Ratio Graph

VIII. CONCLUSION

Networks of the twenty first century offer immense flexibility to the business and individual users, but at the cost of higher complexity. The coexistence of various protocols for current network equipment leads to extremely complex network systems, which not only limit the development of network technologies, but also cannot meet the growing demands for cloud computing, big data, and service visualization applications, just to name a few. Proposed topology improves the packet delivery over network. By means of SDN cost also reduces.

REFERENCES

[1] Dimitri Staessens et. al./Software Defined Networking: Meeting Carrier Grade Requirements/ IEEE 2011
[2] Keshav Sood et. al./ Software-Defined Wireless Networking Opportunities and Challenges for Internet-of-Things: A Review/ IEEE 2016
[3] Danda B. Rawat et. al./Software Defined Networking for Reducing Energy Consumption and Carbon Emission/ IEEE 2016
[4] Shibo Luo et. al. /A Multi-stage Attack Mitigation Mechanism for Software-defined Home Networks/ IEEE 2016
[5] Ann Sabeeh et. al./ A Hybrid Intelligent Approach for Optimising Software-Defined Networks Performance/ IEEE 2016.

All rights reserved by *www.ijsrd.com*

[6] Seizer , S. et al, Are We Ready For SDN? Implementation Challenges for Software-Defined Networks, IEEE Communications Magazine, Volume: 51, Issue: 7, 2013 , Page(s): 36- 43
[7] P. M. Julia and A. F. Skarmeta. Extending the Internet of Things to IPv6 With Software Defined Networking, White Paper, 2014
[8] Shibo Luo, Jun Wu, Member, IEEE, Jianhua Li, and Longhua Guo A Multi-stage Attack Mitigation Mechanism for Software-defined Home Networks IEEE Transactions on Consumer Electronics, Vol. 62, No. 2, May 2016
[9] Keshav Sood, Shui Yu, and Yong Xiang, Software-Defined Wireless Networking Opportunities and Challenges for Internet-of-Things: A Review, IEEE Internet of Things journal, VOL. 3, No. 4, August 2016
[10] J. Wang, Z. Zhang, B. Li, S. Lee, and R.S. Sherratt , "An enhanced fall detection system for elderly person monitoring using consumer home networks," IEEE Trans. Consumer Electronics, vol. 60, no. 1, pp. 23-29,Feb. 2014
[11] Jo, S. Lee, and J. Kim, "Software-defined home networking devices for multi-home visual sharing," IEEE Trans. Consumer Electronics, vol. 60, no. 3, pp. 534-539, Aug. 2014.
[12] Ei, H., and W. V.W.S., "Bandwidth allocation and pricing for SDN enabled home networks," in Proc. 2015 IEEE International Conference on Communications, London, UK, pp. 5342-5347, Jun. 2015.

All rights reserved by *www.ijsrd.com*