PERFORMANCE ANALYSIS OF WIRELESS TRUSTED SOFTWARE DEFINED NETWORKS

Angel Antonette Keziah .J [1], Rajarajeshwari.K.C [2], M.Kirubha[3]

[1,2,3] *Assistant Professor, Dept. of Electronics and Communication Engineering, Sri Ramakrishna Institute of Technology, Tamil Nadu, India*

---***---

Abstract - *Software defined network (SDN) provides a centralized intelligence and control model by the separation of the data plane and the control plane that is well suited to provide much needed flexibility to network security deployments. Secured networks are critical to all businesses, especially with their increased migration to the cloud and the wave of innovation being unleashed by SDN. This paper focuses on performance analysis of wireless trusted software defined networks by considering performance matrices like energy consumption, throughput, end-to-end delay, packet delivery ratio for a particular topology model. Results show that the performance of SDN networks is better than the conventional networks which operate without SDN. Furthermore, comparison of energy consumption for different topology models which uses SDN is done.*

Key words— Authentication, End-To-End Delay, Packet Delivery Ratio, Throughput, SDN-Software Defined Network

1. INTRODUCTION

Recently, Data centres have received significant attention as a very important infrastructure for its ability to store large amount of data and hosting large-scale service applications. Today large companies use data centres for their large scale computations and IT businesses. SDN offers a dynamic approach to networking by separating (decoupling) the control plane and data forwarding plane of network devices. The data plane is responsible for the actual forwarding of the data packets through the network using the paths chosen by the control plane. The control plane realizes the intelligence of a network. By decoupling the data and control planes routing decisions can be centralized and made by software, rather than decentralized decisions at every router within the network.

As SDN has better features than conventional networks more research and development study are being done as regards to securing SDN by providing security key. Wide usage of SDN in enhancing fields like underwater sensor nodes, IOT has better prospects. This project began with a literature study to provide relevant background information about the SDN networks and their security issues. SDN architectures were developed to provide improved routing and networking performance, however it changes the network's communication patterns, allowing new types of attacks, and necessitating a new approach to securing the network .The SDN architectures have not focused on security.SDN security challenges are a combination of SDN, and network security vulnerabilities. The highly secure SDN Networks remains an open problem

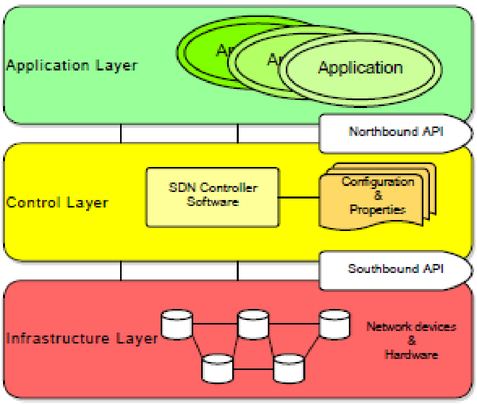

Fig -1: The SDN Stack.

As seen from the Fig 1, SDN architecture is divided into three layers: application layer, control layer, and infrastructure layer. This architecture provides the possibility to centralize the state of the network and the intelligence into one part of the network. This, enhances the property of network programmability, the network industry can start to innovate and enable differentiation in the developing process. Therefore, SDN can make networks become more scalable, flexible and proactive. SDN architecture stack abstracts and decouples hardware from software, control plane from forwarding plane, and physical from logical configuration.

2. SDN BENEFITS AND CHALLENGES

SDN, with its inherent decoupling of control plane from data plane, offers a greater control of a network through programming. This combined feature would bring potential benefits of enhanced configuration, improved performance, and encouraged innovation in network architecture and operations, as summarized in Table 1. Moreover, with an ability to acquire instantaneous network status, SDN permits a real-time centralized control of a network based on both instantaneous network status and user defined policies. This further leads to benefits in optimizing network configurations and improving network performance. The potential benefit of SDN is further evidenced by the fact that SDN offers a convenient platform for experimentations of new techniques and encourages new network designs, attributed to its network programmability and the ability to define isolated virtual networks via the control plane. In the subsection, we dwell on these afore mentioned benefits of SDN

TABLE -1: Comparison Between SDN And Conventional Networks

CHARACTERISTICS	SDN	CONVENTIONAL NETWORKING
Features	Decoupled data and control plane and programmability	A new protocol per problem, complex network control
Configuration	Automated configuration with centralized validation	Error prone manual configuration
Performance	Dynamic global control with cross layer information	Limited information and relatively static configuration
Innovation	Easy software implementation for new ideas, sufficient test environment with isolation, and quick deployment using software upgrade.	Difficult hardware implementation for new ideas, limited testing environment, long standardization process.

In comparison from table 1, SDN encourages innovation by providing a programmable network platform to implement, experiment, and deploy new ideas, new applications, and new revenue earning services conveniently and flexibly. High configurability of SDN offers clear separation among virtual networks permitting experimentation on a real environment. Progressive deployment of new ideas can be performed through a seamless transition from an experimental phase to an operational phase.

Given the promises of enhanced configuration, improved performance, and encouraged innovation, SDN is still in its infancy. Many fundamental issues still remain not fully solved, among which security is the most urgent ones. Common concerns include SDN interoperability with legacy network devices, performance and privacy concerns of centralized control, and lack of experts for technical support.

3. Performance Metrics

The following are the metrics that are used for performance analyses.

- End-to-end delay is the average time it takes a data packet to reach the destination. This includes all possible delays caused by buffering during route discovery latency, queuing at the interface queue. This metric is calculated by subtracting time at which first packet was transmitted by source from time at which first data packet arrived to destination. Mathematically, it can be defined as: Avg.EED=S/N Where S is the sum of the time spent to deliver packets for each destination, and N is the number of packets received by the all destination nodes.
- Packet delivery ratio is defined as the total number of packets delivered over the total simulation time. Packet delivery ratio Packet delivery ratio is defined as the ratio of data packets received by the destinations to those generated by the sources. Mathematically, it can be defined as: PDR= S1÷ S2 Where, S1 is the sum of data packets received by the each destination and S2 is the sum of data packets generated by the each source.
- Throughput is a measure of how many units of information a system can process in a given amount of time. Throughput is usually measured in bits per second (and sometimes in data packets per second or data packets per time slot.

4. Security Analyses Of SDN

The basic properties of a secure communications network are: confidentiality, integrity, availability of information, authentication and non-repudiation. In order to provide a network protected from malicious attack or unintentional damage, security professionals must secure the data, the network assets (e.g. devices) and the communication transactions across the network. The alterations to the network architecture introduced by SDN must be assessed to ensure that network security is sustained. Systems are becoming increasingly complex. This complexity in turn has led to increased risk and severity of bugs and errors in implementations. This complexity increases with virtualization within networks, as increasing numbers of traditional hardware functions are realized by software. This puts a large amount of pressure upon programmers to deliver flawless software solutions. Additionally, this pressure is increasing due to the business trend towards cloud computing. The aim is to ensure that networks are protected from attack by malicious intruders. Networks that are built according to SDN architecture principles need to protect a number of key security assets:

- Availability – the network should remain operational even under attack.
- Performance – the network should be able to guarantee a baseline bandwidth and latency in the event of an attack
- Integrity and confidentiality – control plane and data plane integrity and isolation should be upheld between tenants.

To assure protection of these assets, a number of processes need to be in place. They are authentication and authorization, resiliency, multi-domain isolation and repudiation. Authentication and authorization are the processes used to identify an unknown source and then determine its access privileges. Implemented correctly, these processes can protect networks from certain types of attack, such as Provision of false (statistical) feedback to the system, Modification of a valid on-path request, Forwarding Traffic that is not meant to be forwarded or not forwarding, Gaining control access to any component. The critical nature of the SDNC dictates that additional security measures need to be taken to protect it.And so, all communication within the control plane must be mutually authenticated. Security protocols like TLS and IPSEC provide a means for mutual authentication as well as for replay attack protection, confidentiality, and integrity protection. Encryption and integrity protection without mutual authentication are less useful from a security point of view. The problem with mutual authentication is that it requires previous knowledge of the remote communicating endpoint – unless a commonly trusted third party exists.

The major security threats are denial of service attack, vulnerability attack, connection flooding and bandwidth flooding. Due to these security threats there is an urging need to focus on the security issues of SDN as SDN is the current emerging technology.

5. Proposed Methodology

The SDN architectures have not focused on security.SDN security challenges are a combination of SDN, and network security vulnerabilities. The highly secure SDN Networks remains an open problem. The need of the hour is to develop a secured SDN to overcome the security issues by providing a secure networking architecture that secures the data within each layer of communication packet utilizing SDN centralized controller for secure routing and performance management.

While advantage of the SDN framework has been recognized, solutions to tackle the challenges of securing the SDN network are fewer in number. SDNs provide us with the ability to easily program the network and to allow for the creation of dynamic flow policies. It is, in fact, this advantage that may also lead to security vulnerabilities. Within this dynamic environment, it is vital that network security policy is enforced. The promises of agility, simplified control, and real-time programmability offered by software-defined networking (SDN) are attractive incentives for operators to keep network evolution apace with advances in virtualization technologies. But the capabilities that undermine the security is a question to be answered. The aim is to ensure that networks are protected from attack by malicious intruders.

The proposed methodology is a secured SDN which focuses on the one of the three assets of security; Authentication which secures the communication between nodes. Various wireless topologies like grid, random and tree are developed based on the SDN concepts. In these topologies the data plane and control plane are separated and one node is made to act as SDN controller which controls the entire network. This approach provides us with the ability to easily program the network.

AODV is used for authentication .One distinguishing feature of AODV is its use of a destination sequence number for each route entry. The destination sequence number is created by the destination to be included along with any route information it sends to requesting nodes. Given the choice between two routes to a destination, a requesting node is required to select the one with the greatest sequence number. Requests (RREQs), Route Replies (RREPs), and Route Errors (RERRs) are the message types defined by AODV. When a route to a new destination is needed, the node broadcasts a RREQ to find a route to the destination. A route can be determined when the RREQ reaches the SDN controller. The route is made available by unicasting a RREP back to the origination of the RREQ. Each node receiving the request caches a route back to the originator of the request, so that the RREP can be unicast from the destination along a path to that originator, or likewise from any intermediate node (SDN controller) that is able to satisfy the request. When a link break in an active route is detected, a RERR message is used to notify other nodes that the loss of that link has occurred. The RERR message indicates those destinations which are no longer reachable by way of the broken link.

The Fig 2 gives a flow graph of the proposed work. The topologies with SDN controller are authenticated by using the above mentioned process and various analyses are considered based on the energy consumption, packet delivery, throughput and the time delay. Of which SDN out beats the conventional network in terms of energy consumption and the time taken

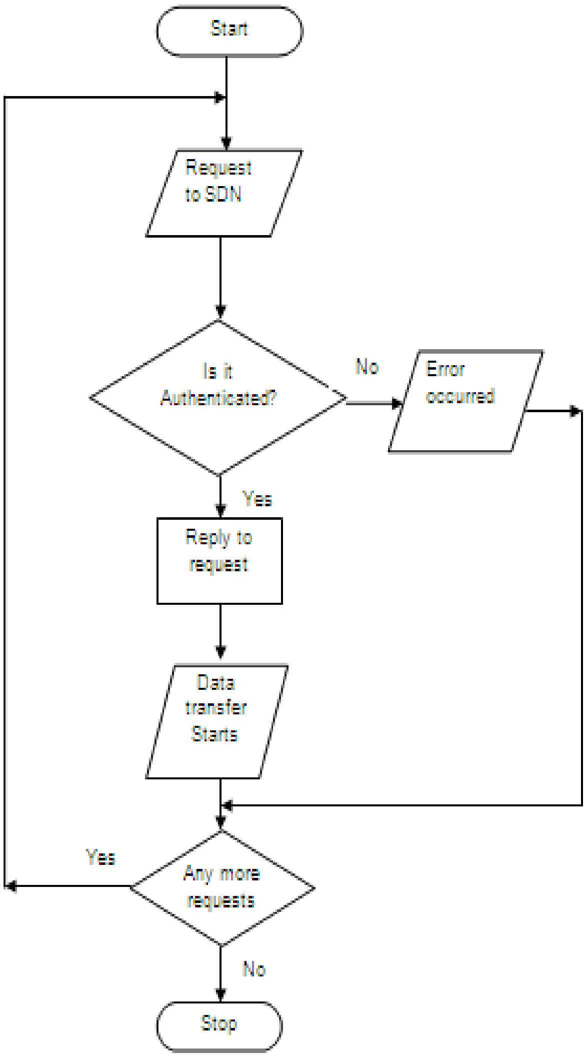

Fig- 2: Flow Chart for Authentication Process

6. EXPERIMENTAL RESULTS

In this project the SDN concept is considered especially from the perspective of network authentication and the Data Plane and Control plane is separated in three wireless topologies and the performance metrics are calculated. Fig 3 illustrate wireless Grid Topology based on SDN concept wherein separation of Data Plane and Control plane is done by using one of the nodes as SDN Controller. The other nodes that wish to send their data have to obtain authentication from the SDN controller

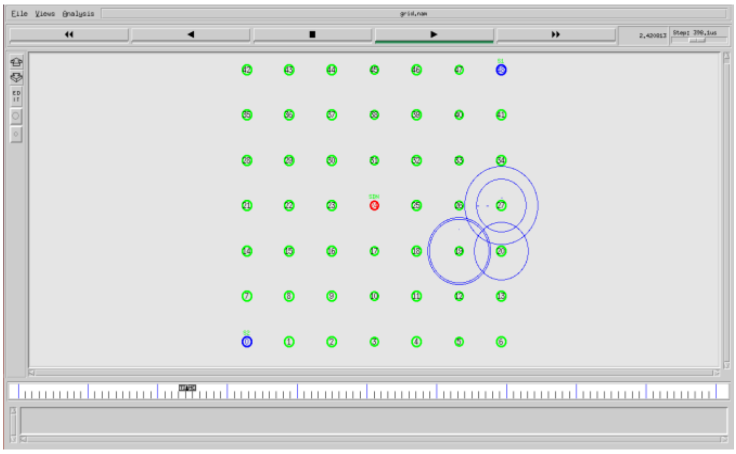

Fig-3: Grid Topology

Random Topology is elaborated in Fig 4 by separating Data and Control Planes. In fig 5 Packet Drop is seen at times when more number of nodes send request to the controller at the same time. This Topology is less preferred owing to the packet drop.

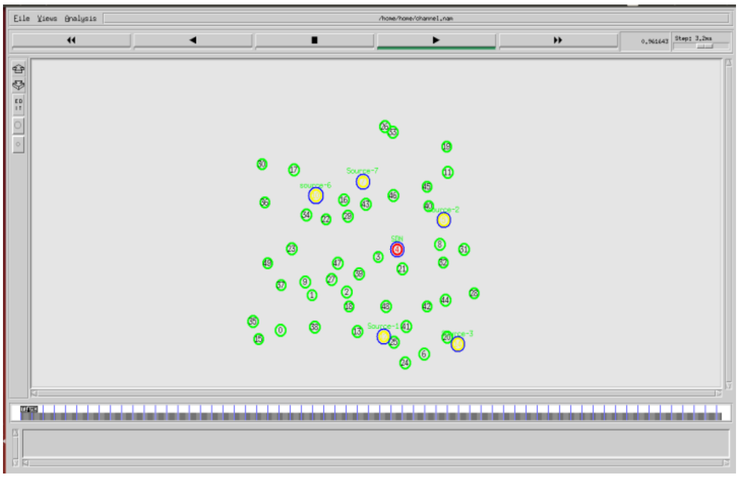

Fig 4: Random Topology

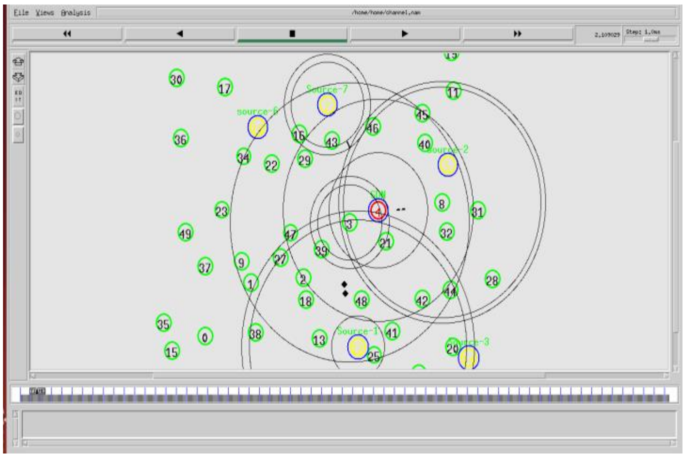

Fig -5: Packet Drop In Random Topology

In the Tree Topology is shown in Fig 6. The Root Node is considered as SDN. Nodes C1, C2 and C3 are nodes which initiate transmission. C1 first seeks authentication from SDN, followed by C2 and C3

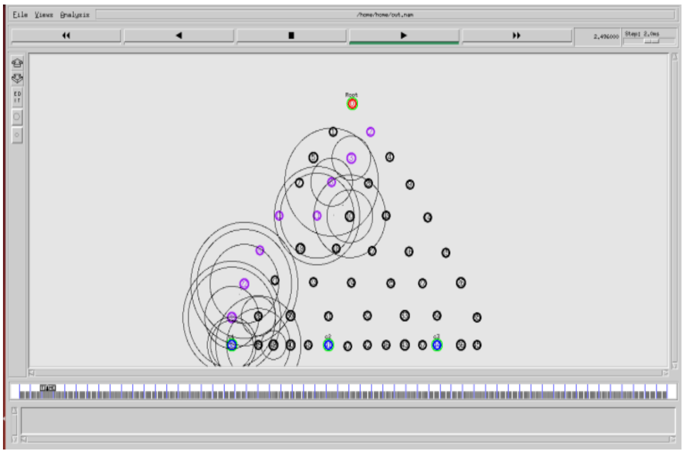

Fig -6: Tree Topology

The following graph in Fig 7 illustrates energy consumption against time taken in grid topology .It elaborates that energy consumption in SDN networks is much lesser compared to the conventional networks Values varied to evaluate energy consumption by using upto 50 nodes.

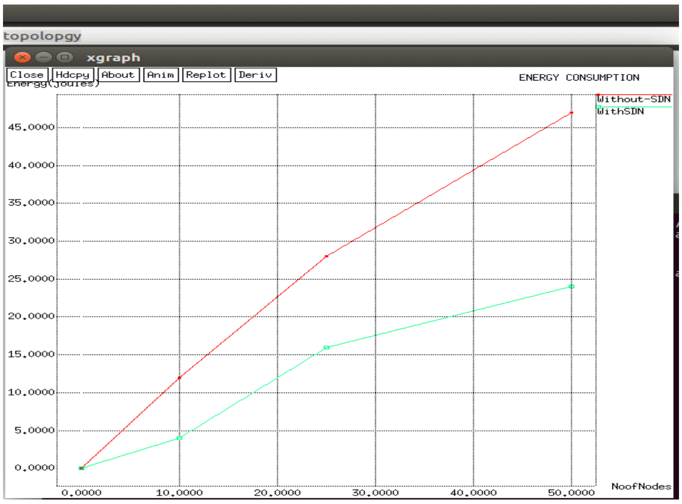

Fig -7: Energy Consumption With and Without SDN

The below figure illustrates packet delivery ratio versus time in grid topology. The Packet delivery Ratio in network with SDN is higher in the given time compared to without SDN according to the graph obtained in Fig.8

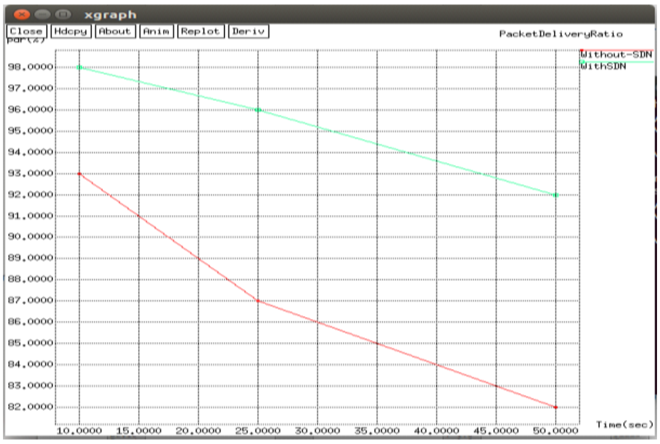

Fig -8: Packet Delivery Ratio With and Without SDN

The Fig 9 shows graph against end-to end delay and time with and without SDN using grid topology. The End-To-End Delay is observed to be less in SDN compared to traditional network without SDN

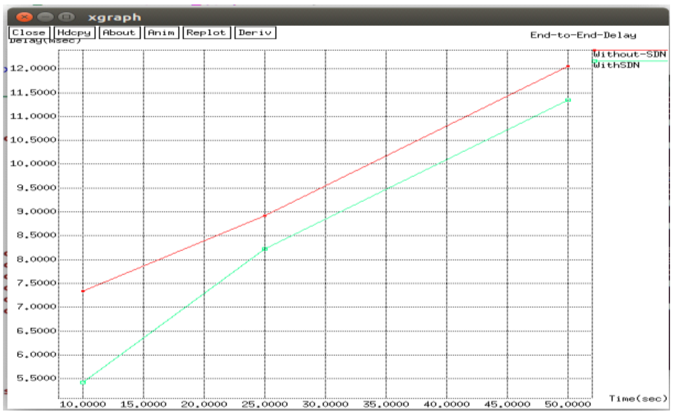

Fig -9: End-To-End Delay with SDN and Without SDN

In fig 10 throughputs versus time is plotted and as seen in the figure throughput in SDN is high when compared to without SDN.

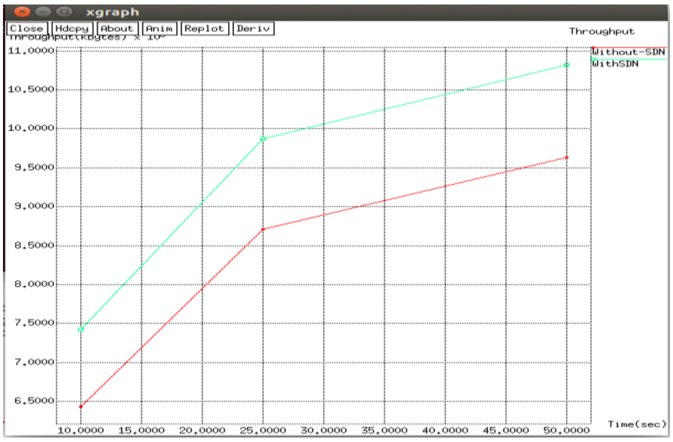

Fig 10: Throughput With and Without SDN

The below Fig 11 shows comparison of three topologies with SDN against energy consumption and number of nodes by varying up to 50 nodes. Comparatively Random Topology has seen to consume highest energy followed by Tree and then Grid. As a result it has been observed that only Grid topology consumes less energy.

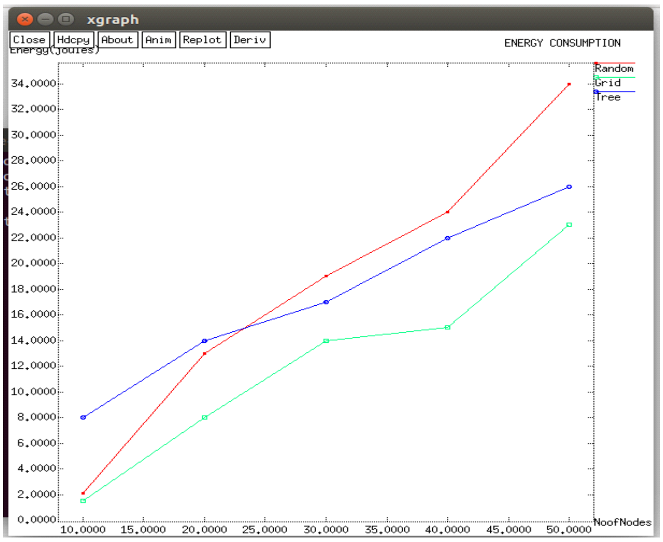

Fig 11: Energy Consumption of Different Topologies With SDN

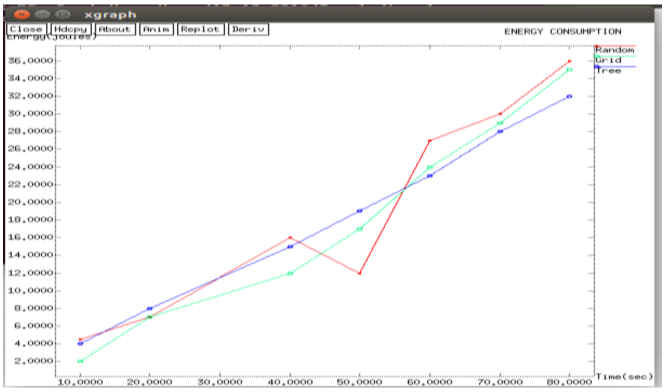

Fig -12: Energy Consumption of Different Topologies with SDN against Time

The graph in Fig 12 elucidated, compares energy consumption versus time taken in random, grid and tree topology. The graph elucidates that in the given time, Random Topology consumes more energy while there is a slight variation in the Grid and tree topologies.

7. Conclusion And Future Work

Software-defined networking is a new concept to manage and configure computer networks. The main idea of the SDN concept is to separate the controlling layer of the computer network from the network switches and centralize it to the SDN controller. The centralized management brings a new way to control network functionality with one single application instead of configuring hundreds and thousands of devices independently.

In this paper the SDN concept is addressed especially from the perspective of network security. The security improvements are explored and solutions are proposed for an enhanced security. But, still more research needs to be done to obtain highly secured network.NS2 software is used to study the parameters involved and to develop the proposed solution. Authentication mechanism is provided which secures the communication between nodes, thereby providing security. Different wireless topologies like grid, tree and random has been created with SDN controller and performance metrics like energy consumption Vs number of nodes, energy Vs time, throughput, end to end delay and packet delivery ratio are analyzed for the same. Energy consumption and the time taken is analyzed and compared with SDN and without SDN .Wherein, without SDN, consumes less energy than the normal conventional networks which is a great advantage for SDN and another advantage is the lesser time consumed. Although this paper gives out some advantages based on the project work, still security can be enhanced to provide a highly secured network. The SDN will be the leading networking technology in the future but it still needs a little more time to evolve.

However the future perspective of usage of SDN is very high. As SDN has better features than conventional networks more research and development study shall be done as regards to securing SDN by providing security key. Wide usage of SDN in enhancing fields like underwater sensor nodes, IOT has better prospects

8. BIBLIOGRAPHY

1. Diogo Menezes Ferrazani Mattos, Lyno Henrique Gonc¸alves Ferraz,Otto Carlos Muniz Bandeira Duarte, “AuthFlow: Authentication and Access Control Mechanism for Software Defined Networking,”IEEE International conference on computer networks, 2013.

2. Feliksas Kuliesius, and Vainius Dangovas, “SDN Enhanced Campus Network Authentication and Access Control System”,IEEE International Conference on Computer Science and Network Technology, 2015.

3. Ruikang Zhou,Yingxu Lai,Zenghui Liu,Jing Liu,“Study on authentication protocol of SDN trusted domain”, IEEE Twelfth International Symposium on Autonomous Decentralized Systems, 2015.

4. Caraguay ALV, Lopez LIB, Villalba LJG,“Evolution and Challenges of Software Defined Networking”, IEEE Communications Magazine,2012.

5. Patouni E, Merentitis A, Panagiotopoulos P, Glentis A, Alonistioti N, “Network Virtualisation Trends: Virtually

Anything Is Possible by Connecting the Unconnected", IEEE SDN for Future Networks and Services (SDN4FNS),2013.

6. CasadoM, Koponen T, Shenker S, Tootoonchian A, "Fabric: A retrospective on evolving SDN", International journal on SDN, 2012.

7. Monteleone G, Paglierani P,"Session Border Controller Virtualization Towards Service-Defined Networks Based on NFV and SDN",IEEE SDN for Future Networks and Services (SDN4FNS), 2013.

8. Gelberger A, Yemini N, Giladi R, "Performance Analysis of Software-Defined Networking (SDN)",IEEE 21st International Symposium on Modeling, Analysis & Simulation of Computer and Telecommunication Systems (MASCOTS),2013

9. Lara A, Kolasani A, Ramamurthy B, "Network Innovation using OpenFlow: A Survey", IEEE Communications Surveys & Tutorials,2014

10. Akyildiz IF, Lee A, Wang P, Luo M, Chou W, "A roadmap for traffic engineering in SDN-OpenFlow networks",International conference on Computer Networks,2014

11. Jin D, Nicol DM, "simulation of software defined networks",springer,2013

12. Raghavan B, Koponen T, Ghodsi A, Casado M, Ratnasamy S, Shenker S,"Software-defined internet architecture: decoupling architecture from infrastructure",ACM Hotnets '12,2012

13. Bhattacharya B, Das D,"SDN based Architecture for QOS Enabled Services across Networks with Dynamic Service Level Agreement",IEEE ANTS, 2013.

14. Kobayashi M, Seetharaman S, Parulkar G, Appenzeller G, Little J, van Reijendam J, Weissmann P, McKeown N,"Maturing of Open Flow and Software-defined Networking through deployments",IEEE Conference on Computer Networks,2014

15. Galis A, Clayman S, Mamatas L, Rubio Loyola J, Manzalini A, Kuklinski S, Serrat J, Zahariadis T,"Softwarization of Future Networks and Services - Programmable Enabled Networks as Next Generation Software Defined Networks", IEEE SDN for Future Networks and Services(SDN4FNS),2013.

16. Caraguay ALV, Lopez LIB, Villalba LJG,"Evolution and Challenges of Software Defined Networking", IEEE Communications Magazine,2012.

17. Cahn A, Hoyos J, Hulse M, Keller E,"Software-Defined Energy Communication Networks: From Substation Automation to Future Smart Grids",IEEE Smart Grid Communication 2013 Symposium - Smart Grid Services and Management Models,2013

18. Wang J, Wang Y, Hu H, Sun Q, Shi H, Zeng L,"Towards a Security-Enhanced Firewall Application for OpenFlow Networks",Springer LNCS CSS,2013.