Journal of Ubiquitous Computing and Communication Technologies (UCCT) (2019)
Vol.01/ No. 02
Pages: 110- 120
https://www.irojournals.com/jucct/
DOI: https://doi.org/10.36548/jucct.2019.2.005

DESIGN AND DEVELOPMENT OF SECURE AND SUSTAINABLE SOFTWARE DEFINED NETWORKS

J.V. Anand
Department of Electronics and Communication Engineering,
PACE Institute of Technology and Sciences,
Ongole, India

Abstract: Nowadays the technological advancements have made the internet ubiquitous and linked a wide group of people to be through it, paving way for a network transferal, causing the applications to be shifted from its local servers to the cloud ecosystem. The shifting of the computer applications led to entailment of enormous network connectivity that caused difficulties in the operations of the network. The software defined networks emerged as capable solution for the managing the difficulties arising due to the paradigm shift, and enriched the network operators with high flexibility programming in accessing as well as controlling the multiple routing paths. However the security and the sustainability in the SDN is still an open issue. So the paper looks forward to design and develop a secure and a sustainable software defined networks. The proposed method is simulated with the NS2 to verify the enhanced quality of service provided in terms of security, throughput and the Packet drop rate.
Keywords: Software Defined Networks**,** Flexible Network Operation, Security, Sustainability, Internet and Cloud Computing

1. INTRODUCTION

The advancement in the information and the communication technology has bought the access of the entire world into our fingertips. The further tremendous progress in the processing capacities and the enormous growth in the communication technologies for the devices that are hand held have turned the computational resources ubiquitous. The paradigm shift of the applications from the local server to the cloud networking has still improved the accessing capability towards the computer resources at a much reduced cost.

But the paradigm shift does not go in hand with the network operations as the traditional networks finds hard to manage the enormous with the enormous network connectivity. This was well handled by the software defined networks that emerged as the promising solution for the long –standing problems in the networking. The fig .1 below shows the frame work of the software defined network.

ISSN: 2582-337X (online)

Ubiquitous Computing & Communication Technologies

Journal of Ubiquitous Computing and Communication Technologies (UCCT) (2019)
Vol.01/ No. 02
Pages: 110- 120
https://www.irojournals.com/jucct/
DOI: https://doi.org/10.36548/jucct.2019.2.005

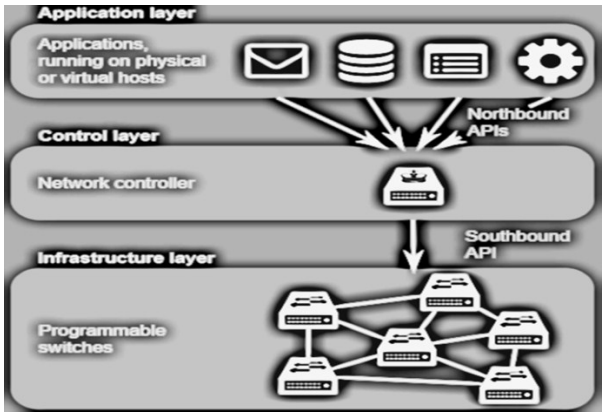


Fig .1 Software Defined Network-Frame Work [1]

The Traditional network functions integrating the data and the control plane, but the SDN separates the control plane from the data plane and ensures an enhancement in the functioning of the network. The data plane in the software defined network is distributed through the network/sub-network and the control plane is managed centrally. The table .1 below provides the difference between the traditional and the software defined networks.

ISSN: 2582-337X (online)

Journal of Ubiquitous Computing and Communication Technologies (UCCT) (2019)
Vol.01/ No. 02
Pages: 110- 120
https://www.irojournals.com/jucct/
DOI: https://doi.org/10.36548/jucct.2019.2.005

Traditional Network	Software Defined Net work
It is hardware based	It is soft ware –based
traditional networks use switches, routers and other physical infrastructure to create connections and run the network.	Highly flexible, manages the resources virtually throughout the control plane
traditional networking uses protocol	developers can directly program the network,
Traditional network uses dedicated hardware's	SDN lets users use software to provision new devices
The physical location of the control plane hinders an IT administrator's ability to control the traffic flow.	SDN virtualizes your entire network, and generates an abstract copy of your physical network, provides resources from a centralized location.
Requires new hardware to improve the network capacity	Does not require an additional physical infrastructure
They have a distributed control plane	They have a central control plane and a distributed data plane
Maintenance Cost is higher , resource utilization is less	Maintenance Cost is less, resource utilization is high
Updation and the error handling takes time	Updation and the error handling is easy
Authenticity, integrity and the consistency of the controller is not important	Authenticity, integrity and the consistency of the controller is important

Table .1 Difference Between Traditional and Software Defined Network

Despite the capabilities in the SDN, they hold certain limitations in terms of the information security and the quality of service. So in-order to develop a high reliable SDN, that is robust and efficient. The paper looks forward to design and develop a secure and a sustainable software defined network.

The paper is organized with the related works described in the section 2, proposed work done in section 3 and the description of the results obtained in section 4 and the conclusion in section 5.

2. RELATED WORKS

The author Raj, Jennifer S et al [2] and [3] presents the "virtual structure for sustainable wireless networks in cloud services and enterprise information system." Management using the SDN and the "a comprehensive survey on the computational intelligence techniques and its applications." in the traditional wireless networks the author Smys, S.,

ISSN: 2582-337X (online)

Journal of Ubiquitous Computing and Communication Technologies (UCCT) (2019)
Vol.01/ No. 02
Pages: 110- 120
https://www.irojournals.com/jucct/
DOI: https://doi.org/10.36548/jucct.2019.2.005

et al [4] details the utilization of the SDN in the “stochastic mobile data traffic model for vehicular ad hoc networks." Pandian, M. Durai et al [5] elaborates the “enhanced network selection and handover schema for heterogeneous wireless networks” that are conventional. Mugunthan et al [6] elaborates the security and the privacy provisioning in the wireless sensor network. Neelaveni, R et al [7] and Karunakaran, et al [8] explains the essentiality of the security assistance in the VANET and the a “stochastic development of cloud computing based task scheduling algorithm." Joy Iong-Zong Chen and Smys, S., et al [9] provides the details of the “software-defined control for next-generation wireless systems” and Smys, S., et al [10] further provides the “Analysis of localized virtual structure constructions in wireless networks." Ananthi, J. Vijitha, and Jennifer S. Raj et al [11] in the paper provides the "A Peer to Peer Overlay Approach for Topology Maintenance in Wireless Networks." Korniak, et al [11] puts forth the “The GMPLS controlled optical networks as industry communication platform.” The author Praveena, A., and S. Smys et al [15] details the "Efficient cryptographic approach for data security in wireless sensor networks using MES VU."

2.1. PROBLEM STATEMENT

The dual properties of the software defined networks that include the capability to handle the network operation using the software and the centralization of the network intelligence allowing anybody to access the host serves, who hold the control software ,have become the loop hole for the hackers and the unauthorized users. More over this has caused much head ache to the network operations that commence with low level of preparations. The table.2 below shows the potential treats vectors identified in the Software defined Networks.

ISSN: 2582-337X (online)

Journal of Ubiquitous Computing and Communication Technologies (UCCT) (2019)
Vol.01/ No. 02
Pages: 110- 120
https://www.irojournals.com/jucct/
DOI: https://doi.org/10.36548/jucct.2019.2.005

Table .2 Threat vectors of the Software Defined Network

The proposed methodology is to develop a security system for the software defined network that guarantees the SDN with the fault and the intrusion tolerance along with the trusted relationships between its layers. To develop a robust system the proposed method scopes in framing a secure control layer, enhancing the resilience of the system.

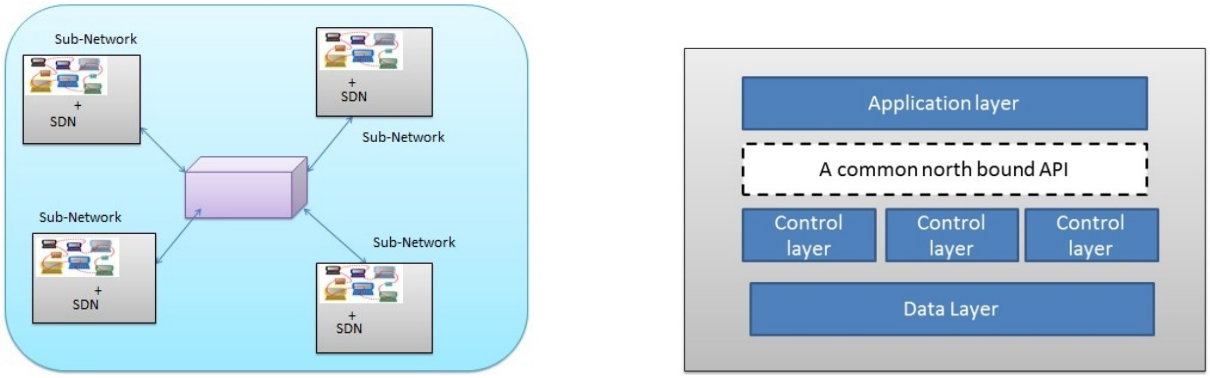
3. PROPOSED FRAME WORK

The methods also enhances the self-adaptability of the system to the changing network conditions and self-healing in case of threats, by automatically increasing the number of replications and the key length. The paper presents the overall design of the Secure SDN control layer along with back restoration scheme deployed and connected to the

ISSN: 2582-337X (online)

Journal of Ubiquitous Computing and Communication Technologies (UCCT) (2019)
Vol.01/ No. 02
Pages: 110- 120
https://www.irojournals.com/jucct/
DOI: https://doi.org/10.36548/jucct.2019.2.005

core of the network to address the security issues in the SDN and handling the failures encountered in the stand alone controller respectively. The fig.2 shows the overall proposed architecture and the Modified SDN frame work.



(a) (b)

Fig.2. (a). Proposed Architecture, (b) Modified SDN frame work

This is mainly developed for the network that holds multiple sub-networks with each sub- network holding multitudes of nodes that is taken care by a dedicated software defined network. To manage the threats and the failures encountered in a single controller in the sub-net of the network the backup restoration scheme along with the replication of the controllers, the common interface handling the integration and the interoperation of the controllers to provide a dynamic association and diversity in the switches is utilized in the software defined network as shown in the fig.2

3.1. ENHANCED SECURITY FOR THE SDN

The replication of the controllers ensures to maintain the network in the healthy state, even on the failures of the particular controller or the when one of the controller gets compromised. The common interface, the common north bound API and the common replication capabilities used between the controllers assures that they are framed with replication done at ease along with the capability of interoperating. Further the switches maintain a trustworthy relationship with the controllers in a secure manner. By utilizing the symmetric cryptography algorithms [14] [15]

ISSN: 2582-337X (online)

Journal of Ubiquitous Computing and Communication Technologies (UCCT) (2019)
Vol.01/ No. 02
Pages: 110- 120
https://www.irojournals.com/jucct/
DOI: https://doi.org/10.36548/jucct.2019.2.005

the dangerous flows are identified. This trusted relationship among the switches and the controllers are retained by maintaining the list in the controller that holds the details of the trusted devices. The anomaly behavior of the devices is identified applying the trust based detection algorithm [17]. If the trustworthiness of the devices goes beyond the threshold level immediately the device is isolated from all the other devices and the controller. The diversity is introduced in the system to avoid relying on the single controller make for replications, bugs and the anomaly that is very high possibility of affecting the entire occurrence simultaneously.

3.2. CONTROLLER FAILURE MANAGEMENT IN SDN

The failure in the stand alone controller is managed by the back-up restoration scheme [BURS] that is deployed into the core of the network that holds multitudes of the sub-networks and connected to the dedicated SDN that controls each sub –network. The BURS [13] serves as a solution to fill the gap that is caused when a controller fails. The replicated controllers, though they take care of the flow, on situations under heavy traffic the BURS is eludes the gap in service provisioning until the controllers are restored. The BURS affords to provide a better quality of service by load balancing and proper controller placement [16], thus managing the failures in the controller.

4. RESULTS EVALUATION

The Evaluation of the proposed system with the security and the back-up restoration scheme is performed using the network simulator-2 with diverse parameters. The experiment is done using the 100 –500 numbers of the nodes for the sub-network with and without the BURS. The table.3 below shows the parameter that is used in the simulation.

ISSN: 2582-337X (online)

Journal of Ubiquitous Computing and Communication Technologies (UCCT) (2019)
Vol.01/ No. 02
Pages: 110- 120
https://www.irojournals.com/jucct/
DOI: https://doi.org/10.36548/jucct.2019.2.005

Parameters	Values
Queue Type	Drop tail
TRAFFIC Type	TCP
Simulation Time	1000ms

Table.3 Simulation Parameters

The table.4 below provides the comparative analysis of the proposed method in terms of security, PDR, throughput for varying number of nodes with and without the Security framework and the BURS (S-BURS)

Number of Nodes	With S-BURS			Without S- BURS		
	Throughput in Mbps	Security %	PDR %	Throughput in Mbps	Security %	PDR %
100	1.4	95.65	95.24	.835	89.4	75.4
200	1.38	97.87	95.41	.723	88.4	67.7
300	1.39	94.26	95.43	.784	78.34	63.2
400	1.35	97.75	95.56	.698	75.5	50.1
500	1.4	98.53	95.78	.654	73.2	52.4

ISSN: 2582-337X (online)

Ubiquitous Computing & Communication Technologies

Journal of Ubiquitous Computing and Communication Technologies (UCCT) (2019)
Vol.01/ No. 02
Pages: 110- 120
https://www.irojournals.com/jucct/
DOI: https://doi.org/10.36548/jucct.2019.2.005

Table.4 Comparative Analysis

The results obtained shows the enhanced resilience, robustness and the failure management by the SDN deployed with the S-BURS, when compared with the network without the deployment of the S-BURS.

5. CONCLUSION

To manage the complex connectivity in the network operations and provide with the flexible connections for the network with paradigm shift and multiple routing paths and enhance the security and the failure management, the software defined network is modified with the replication of the controllers, by extending a trust based relation between the devices and the controller along with the Back-up and restoration scheme to address the security issues in the SDN and handling the failures encountered in the stand alone controller respectively. The controllers are built with the symmetric cryptography methods to avoid the malicious traffic flow. The trust based intrusion detection is utilized to manage the trusted relationship between the devices and the controllers. This enables the network to have a simultaneous network access even on the failure of the components and secure the network during the anomaly detection in the network. The future work of the paper is to continue with the context aware trust management for the component based software systems to ensure the trustworthiness of the relationship among the applications and controllers.

References

[1] https://qmonnet.github.io/whirl-offload/2016/07/08/introduction-to-sdn/

[2] Raj, Jennifer S., and S. Smys. "VIRTUAL STRUCTURE FOR SUSTAINABLE WIRELESS NETWORKS IN CLOUD SERVICES AND ENTERPRISE INFORMATION SYSTEM." *Journal of ISMAC* 1, no. 03 (2019): 188-205..

[3] Raj, Jennifer S. "A COMPREHENSIVE SURVEY ON THE COMPUTATIONAL INTELLIGENCE TECHNIQUES AND ITS APPLICATIONS." *Journal of ISMAC* 1, no. 03 (2019): 147-159.

ISSN: 2582-337X (online)

[4] Smys, S., and Jennifer S. Raj. "A STOCHASTIC MOBILE DATA TRAFFIC MODEL FOR VEHICULAR AD HOC NETWORKS." *Journal of Ubiquitous Computing and Communication Technologies (UCCT)* 1, no. 01 (2019): 55-63.

[5] Pandian, M. Durai. "ENHANCED NETWORK SELECTION AND HANDOVER SCHEMA FOR HETEROGENEOUS WIRELESS NETWORKS." *Journal of ISMAC* 1, no. 03 (2019): 160-171.

[6] Mugunthan, S. R. "SECURITY AND PRIVACY PRESERVING OF SENSOR DATA LOCALIZATION BASED ON INTERNET OF THINGS." *Journal of ISMAC* 1, no. 02 (2019): 81-91.

[7] Neelaveni, R. "PERFORMANCE ENHANCEMENT AND SECURITY ASSISTANCE FOR VANET USING CLOUD COMPUTING." *Journal of trends in Computer Science and Smart technology (TCSST)* 1, no. 01 (2019): 39-50.

[8] Neelaveni, R. "PERFORMANCE ENHANCEMENT AND SECURITY ASSISTANCE FOR VANET USING CLOUD COMPUTING." *Journal of trends in Computer Science and Smart technology (TCSST)* 1, no. 01 (2019): 39-50.

[9] Karunakaran, V. "A STOCHASTIC DEVELOPMENT OF CLOUD COMPUTING BASED TASK SCHEDULING ALGORITHM." *Journal of Soft Computing Paradigm (JSCP)* 1, no. 01 (2019): 41-48.

[10] Smys, S., Joy Iong-Zong Chen, and Robert Bestak. "Introduction to the special section on software-defined control for next-generation wireless systems." *Computers & Electrical Engineering* 100, no. 57 (2017): 91-92.

[11] Smys, S. "Analysis of localized virtual structure constructions in wireless networks." (2012).

[12] Ananthi, J. Vijitha, and Jennifer S. Raj. "A Peer to Peer Overlay Approach for Topology Maintenance in Wireless Networks."

[13] Korniak, Janusz. "The GMPLS controlled optical networks as industry communication platform." *IEEE Transact*

[14] Song, Il-Keun, Won-Wook Jung, Ju-Yong Kim, Sang-Yun Yun, Joon-Ho Choi, and Seon-Ju Ahn. "Operation schemes of smart distribution networks with distributed energy resources for loss reduction and service restoration." *IEEE Transactions on Smart Grid* 4, no. 1 (2012): 367-374. *ions on Industrial Informatics* 7, no. 4 (2011): 671-678.

[15] Pritchard, Sean W., Gerhard P. Hancke, and Adnan M. Abu-Mahfouz. "Cryptography methods for software-defined wireless sensor networks." In *2018 IEEE 27th International Symposium on Industrial Electronics (ISIE)*, pp. 1257-1262. IEEE, 2018.

ISSN: 2582-337X (online)

[16] Praveena, A., and S. Smys. "Efficient cryptographic approach for data security in wireless sensor networks using MES VU." In *2016 10th international conference on intelligent systems and control (ISCO)*, pp. 1-6. IEEE, 2016.

[17] Heller, B., R. Sherwood, and N. McKeown. "Ithe controller placement problem." *ACM HotSDN, New Yor>, USA, pp. 7Y12* (2012).

[18] Anguraj, Dinesh Kumar, and S. Smys. "Trust-based intrusion detection and clustering approach for wireless body area networks." *Wireless Personal Communications* 104, no. 1 (2019): 1-20.

ISSN: 2582-337X (online)