ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

Handling Malicious Switches To Reduce Delay in Software-Defined Networking (SDN)

P.Premadevi[1] , P.Deepika[2] , S.Priya[3] , R.Swarnamuki[4] , R.Udayavarsheni[5]

AP, Department of CSE, Angel College of Engineering and Technology, Tirupur, TamilNadu, India [1] ,

IV year, Department of CSE, Angel College of Engineering and Technology, Tirupur, TamilNadu, India [2,3,4,5]

ABSTRACT: Software-Defined Networking is a novel network topology that enables decoupling of the data plane from the control plane on network devices. This approach differs from the traditional networking architecture. In which both planes reside on the same network device. SDN offers flexibility, centralized control, reduced complexity and a decrease in network systems and equipment costs. The goals of constructing the SDN network are to achieve faster service deployment and greater flexibility in managing the networks. OpenFlow(OF) is a widely used protocol for establishing the communication between the control and data planes for SDN. To increase the consistency and reliability of the SDN network the fault tolerance issue needs to be studied. Because the routing path between source and destination switch may have faulty influence. The traditional solution is not suitable as Path Agreement Protocol(PAP) discuss about the path fault even when there are some malicious switches exist in the SDN. In this paper,Trust Secure Energy Optimized Aggregation Protocol (TSEOAP) is proposed to identify and eliminate the malicious switches which helps all the data be transmitted to the destination in the SDN network.

KEYWORDS: Software-Defined Network, fault tolerance, malicious switches, aggregation.

I. INTRODUCTION

With the rapid development of Internet technologies, network architectures have been improved continuously. The main challenges are to satisfy the various services of customers by high quality of service delivered by virtualization technologies. An energy-efficient and high security networking for supporting the multiple concurrent tasks will be of increasing importance.

In traditional network architecture, each network device comprises a control plane and a data plane. The control plane is responsible of configuring and managing the device and routing, and the data plane is responsible for forwarding the data according to the rules from the control plane, and the traditional architecture is shown in Figure 1.However, the SDN network architecture separates the control plane and the data plane of the network. Under the architecture, the centralized controller manages the control plane, and the data plane is only responsible for the packet transmission. In addition, the controller defines the network behaviour by software, and the switches have different behaviours based on different demands. It can also deploy different network environments quickly without replacing network devices. Thus, SDN can reduce the time of deployment, decrease human resources and achieve the network virtualization. The SDN architecture is shown in Figure 2.

However, in the real situation, the faulty component can influence the communication data to make the function of network topology down. In other words, these faulty switches may do some faulty behaviour to make other switches not to work correctly. Hence, the faulty diagnosis is also an important topic to be studied under SDN network.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

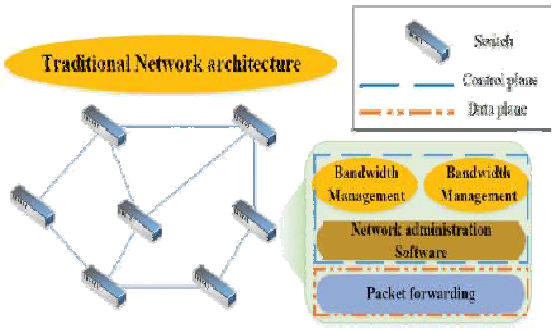

FIGURE 1.Traditional architecture.

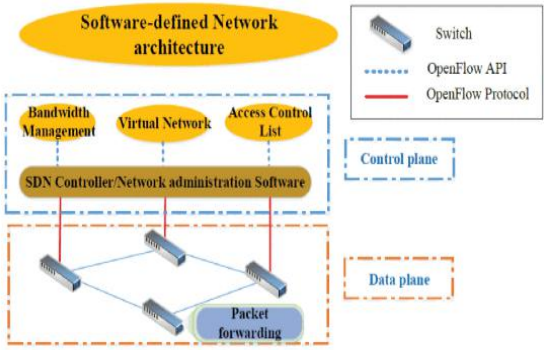

FIGURE 2.SDN architecture.

Thus, in this paper, a Trust based evaluations defined. It is an efficient technique to detect malicious switches in the network. For this, threshold value is defined for each switch. If the threshold value is less than the computed trust value then it will be the malicious switch and it is to be discarded from the network.

The remaining section of the paper is organized as follows. In Section II we discuss related work, while in Section III presents about the proposed algorithm and the parameters. In Section IV is about our implementation. Section V describes about simulation setup and simulation results, Finally, Section VII is conclusion and the future works.

II. RELATED WORK

Antonio Capone et al. [1] illustrated a failure management mechanism. It uses MPLS crackback routing, it respond to the failure by rerouting the tagged packets and by enabling a detour for all subsequent packets. For managing the failure it takes an longest path.

Carmelo Cascone et al. [2] used spider provides a fully programmable abstraction to execute the programmed failure reaction behaviours directly in the switches, minimizing the recovery delay and guaranteeing the failover even when the controller is not reachable.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

Tzu-Weichao et al. [3] proposed to locate and mitigate malicious SDN switches using active probing, statistics checking and packet obfuscation. This helps to forward the packets securely among malicious switches. It minimizes performance overhead with high probability and low delay.

Mao-Lun Chiang et al. [4] illustrated that to improve the consistency and reliability of the SDN network, a new failure type path fault was defined to solve the BA problem. Path-based Agreement Protocol (PAP) is used. It requires minimum number of rounds for message exchange and can tolerate the maximum faulty paths to make the destination switch fault-free decision. Unfortunately, it only tolerate the failures. It does not apply any faulty diagnosis method to identify and eliminate the faulty switches.

Gang-Song Dong et al. [5] proposed a fast failure recovery mechanism for control flow and data flow. Loss Of Signal(LOS) and Bidirectional Forwarding Detection(BFD) are used to recover from the faults within 50ms.For large network, it cannot able to recover from failures within 50ms.

Karim Eldefrawy et al. [6] used a BFT-SMaRT consensus protocol to replicate to original controller to ensure the fault tolerance of the entire system. However, it cannot confirm the correctness of transmission result on the switch.

Rami Ghannam et al. [7] proposed to identify the various malicious behaviour using sphinx and LLDP. By analysing the effectiveness of strategies 10-15% of the switches are only compromised. More work has to be done to handle the malicious switches.

Shella S.Rana et al. [8] uses ipath algorithm to find the optimal set of paths to support reliable communication. The source node maintains the conflict graph which keeps the conflicts occur in the nodes helps to reduce overhead. Minimum vertex cover for larger network cannot be computed.

Vignesh Renganathan Raja et al. [9] proposed to handle the node or link failures by dividing the tree into subtrees. If any failures occurred in any of the node in subtree the corresponding subtree is modified. It does not handle the failures quickly.

Hin-sing siu et al. [10] proposed a mixed sum algorithm to solve the arbitrary and omission faults. The algorithm can tolerate any fault in a system provided $n > 3m + b$ and $c > 2m + b$, where n is the total number of processors, c is the system connectivity, m is the number of arbitrary faults, and b is the number of dormant fault. It cannot handle both the faults at a time.

Xitao Wen et al. [11] inspect forwarding behaviour using customized probe regator Investigate incremental forwarding inspection toward monitoring dynamic networks in real time. Rulescope achieves accurate fault detection within 16 s.

III. PROPOSED ALGORITHM

Wireless networks are very easy to move because there is no need to establish any physical path. This feature results into birth of various attacks. In the wireless network, the attacker targets some nodes and then drop the packets sent towards the intended nodes. They try to drop/delay the packets in the routine manner so it's very difficult to detect. The packet drop will further results into the high false positive rates and ultimately breaks the security of wireless networks. The objective of our model is to identify and eliminate threats in the switch.

A. ARCHITECTURE DIAGRAM

Data is transmitted from source to destination, to transmit the data there may be 'n' sources and 'n' destinations. The set of paths is identified in route discovery using neighbour

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

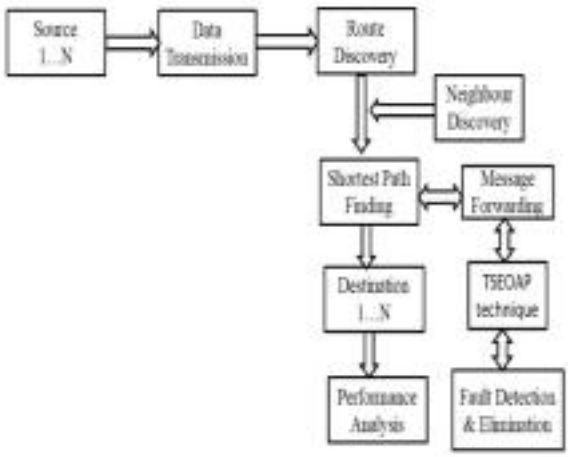

FIGURE 3.Architecture Diagram

nodes and the shortest path is found to transmit the data. While forwarding the packets there are "n" nodes in a path and the nodes may be faulty. TSEOAP protocol is used to identify the faulty nodes and eliminate the faulty nodes. Again the shortest path is found and the packets are forwarded to the destination.

B. ALGORITHM

1. For each mobile node Mi i=1,2,….,n
    - Measure the identification factor IDi.
    - Measure the mobility result MRi.
    - Measure the consistency value MRi.
    - Estimate the CTVi.

    End for
2. Choose the aggregator node Aj with the highest CTV .
3. For each aggregator Aj,j=1,2,….
    - When A receives the data packet from node Mi, it measures its trust value CVi.
    - If CTVi < CTVthr, then Aj will not aggregates the packet

      Else:

      Aj aggregates the packet and increments its counter Ctj as:

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

Ctj=Ctj+α

Where α is the number of packets successfully aggregated by Aj.

End if.

- Aj generates a random hash value [MAC(agg,Ctj)] to the sink.
- Aj transmits [MAC(agg,Ctj)] to the sink.

End For

4.When all the aggregated data from Aj reaches the sink,it checks the counter value Ctj.

5.If Ctj > Cthr,then;

Aj is well behaving

Else

Aj is misbehaving

End if:

6.Aj is prohibited from further transmission.

C. PARAMETERS DISTANCE

We need to find the distance between nodes by considering a link between nodes A and B, let D be the distance between the two nodes. Let (x1, y1) and (x2, y2) are the coordinates of nodes A and B, respectively, the distance can be calculated by using the following formula:

$$\mathbf{D = ((x2 - x1)^2 + (y2 - y1)^2)}$$

ENERGY

Energy is consumed when a packet is received or sent or when a node is idle overhearing traffic from neighbouring nodes. The remaining energy in a node can be calculated by:

ER(n) = EI(n) – EC(n) EI(n) - initial energy of a node, EC(n) -consumed energy of the node

THROUGHPUT

In data transmission, throughput is the amount of packets successfully moved from one place to another in a given unit of time. It can be calculated as follows:

Throughput=received data * 8 / data transmission period

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

IV. IMPLEMENTATION

A. NETWORK DEPLOYMENT

Nodes can be deployed randomly in wireless network. Each node in a MANET is free to move independently in any direction and will therefore change its links to other devices frequently. To properly route traffic, equipping each device to continuously maintain the information required.

B. DATA COMMUNICATION

In this module, data communication between nodes is established using ipath algorithm by calculating the distance between the nodes.Each data has a steady size of 512 bytes. The IEEE 802.11 are used to boost wireless throughput and reduce power consumption.

C. BINARY SCHEME

The probabilistic approach is used to identify two node failure detection. This scheme identifies the location, transmission range and node collaboration for mobile wireless networks. Binary feedback algorithm is used to identify the failure in nodes based on probability value.

D. TRUST COMPUTATION

In order to find the malicious node, trust value is calculated for every node. By depending upon the value, the nodes will get discarded from the network. While calculating, we will get the value with the help of threshold value. By comparing that value, if the node value is more than that then it will be a malicious node and the node gets discarded.

E. PERFORMANCE ANALYSIS

Trace file is generated that shows the result of the Wireless network performance.

Average End to End Delay

Packet Delivery Ratio

Routing Overhead

Throughput Ratio

V. SIMULATION

NS2 is used for implementation and it generates a TCL (Tool Command Language) file. When running the tcl file it results into two more files, first the trace file which contains all the information regarding the network and second the NAM (Network animator) file is a visual aid showing how packets flow along the network. It also shows the virtualization of the network corresponding to the trace file. All routing protocols in NS2 are mounting in the directory of “ns-2.28”.We create a tiny size network that has nodes and generate a UDP link connection between the nodes and attach CBR (Constant Bit Rate) function that produce constant packets in the course of the UDP connection.

A. SIMULATION SETUP

The performance of TSEOAP protocol is evaluated through ns2 simulation. A random network deploy in an area of 500 x 500 m is considered. Initially 59 mobile nodes are placed in a square grid area by placing each mobile in a 50 x 50 grid cell. The Distribution Coordination Function(DCF) of IEEE 802.11 is used for wireless LANs as the MAC layer protocol. CBR is used with UDP to design the traffic source and sink behavior.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

Table 1 : Simulation Parameters

No. of Nodes	60
Area Size	500 x 500
MAC	802.11
Routing Protocol	AODV
Simulation Time	50 s
Traffic Source	CBR
Packet Size	50 bytes
Speed of Events	2 m/s

B. SIMULATION RESULTS

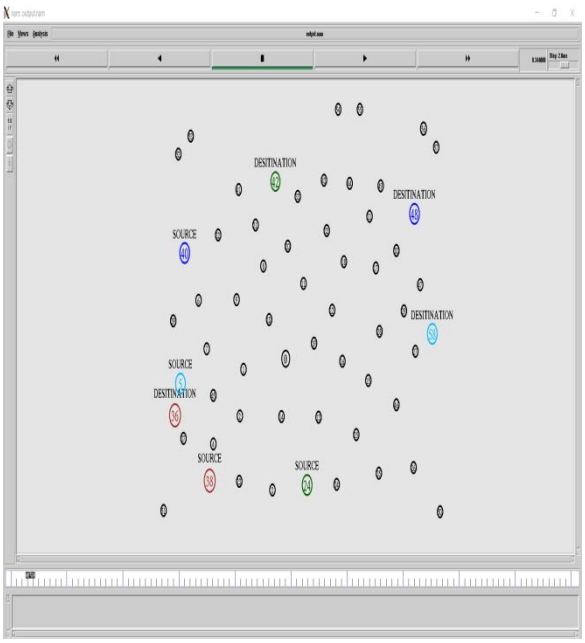

FIGURE 4.Node Deployment

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

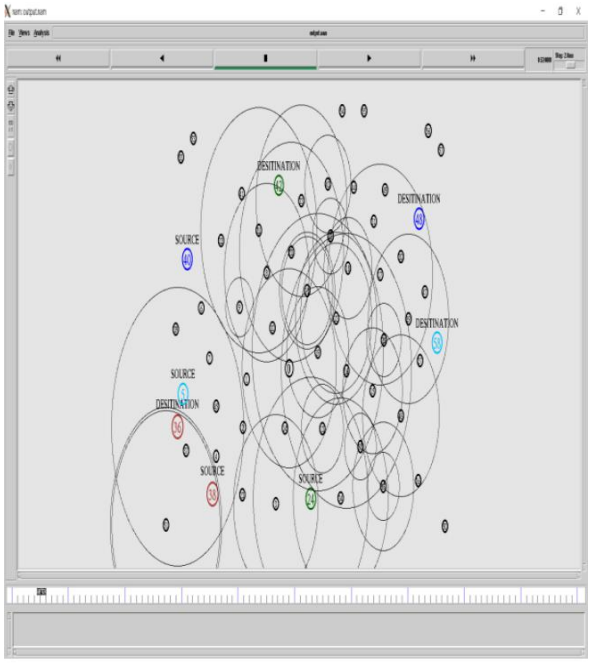

FIGURE 5.Radio Propagation

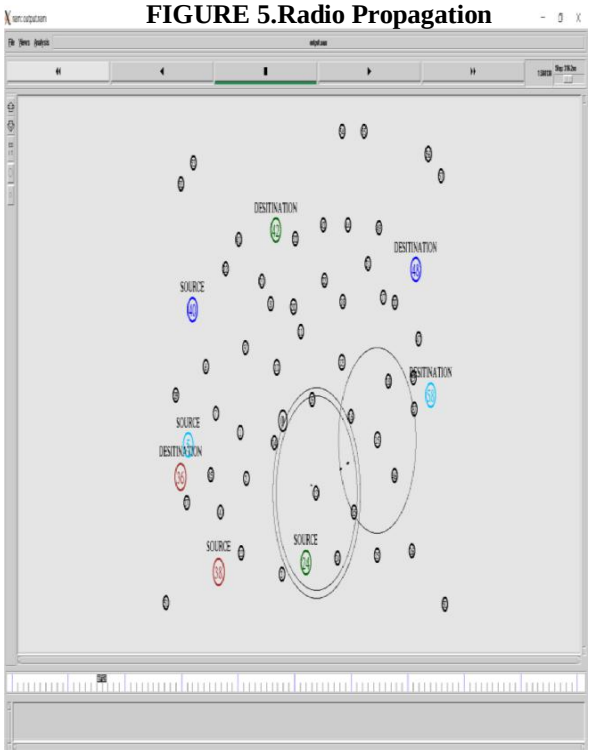

FIGURE 6.Data Transmission

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

VI. CONCLUSION

Software Defined Network(SDN) supports dynamic nature of current network functions and applications. We proposed TSEOAP protocol to identify and eliminate the malicious switches. In other words the overall network environment can have better execution environment after applying the proposed protocol. Thus, each fault free switch can maintain the performance, integrity and reliability of the SDN to provide a steady environment.

In the future, security enhancements can be done in SDN framework research.

REFERENCES

1. A. Capone, C. Cascone, A. Q. T. Nguyen and B.Sanso, "Detour Planning for Fast and Reliable Failure recovery in SDN with OpenState", in *Proc.11th INT. conf. Desing Reliable commun. Netw. (DRCN)*, Mar.2015, pp.25-32.
2. C.Cascone, L.Pollini, D. Sanvito, A.Capone, B.Sansó, "SPIDER: Fault resilient SDN pipeline with recovery delay guarantees", *NetSoft Conference and Workshops (NetSoft) 2016 IEEE*, pp. 296-302, 2016.
3. T.-W. Chao, Y.-M. Ke, B.-H. Chen, J.-L. Chen, C. J. Hsieh, S.-C. Lee, and H.-C. Hsiao, "Securing data planes in software-defined networks", in *IEEE NetSoft Conference and Workshops (NetSoft), 2016.*
4. M. -L. Chiang , H. -C. Hsiehand and C. -W. Wang , "Improving the Fault Tolerance Under Software- Defined Network Based on New
5. Agreement Protocol", *Access IEEE*, vol. 6, pp. 40898-40908, 2018.S. Dong, J. Shen and L. –Q. Sun , "Fast
6. Failure Recovery in Software-Defined Networking", in *Proc. 5th INT. conf. on Frontiers of Manufacturing Science andMeasuring Technology (FMSMT)*,Apr.2017.
7. K. EIDefrawy and T. Kaczmarek , "Byzantine Fault Tolerant SDN controller", in *Proc. IEEE 40th Annu. Comput. Softw. Appl.Conf.(COMPSAC)*,vol.2,Aug.2016, pp.208-213.
8. R. Ghannam and A. Chung , "Handling Malicious switches in Software Defined Networking" in *Proc.IEEE Netw. Oper. Manage. Symp . (NOMS)*, Apr.2016, pp. 1245-1248.
9. S. S. Rana and N. H. Vaidya , " IPATH : Intelligent and optimal path Selection for BYZANTINE Fault tolerant communication",in
10. *Proc.IEEE Conf. Comput. Commum. (INFOCOM)*, Apr.2015, pp. 1095-1103.
11. V.R.Raja,C. -H.Lung,A.Pandey,G. -M.Wei and
12. A.Srinivasan,"A Subtree based approach to failure detection & protection for multicast in SDN", *Frontiers of Information Technology and Electronic Engineering*, Jul.2016, pp. 682-700.
13. H.-S.Siu,Y.-H.Chin and W.-P. Yang, "A note on consensus on Dual Failure models", *IEEE Trans. Parallel Distrib. Syst .*, vol. 7, no. 3,pp. 225-230,Mar.1996.
14. X.Wen, K.Bu, B.Yang, Y.Chen , L.Erran Li, X.Chen, J.Yang and X.Leng,"RULESCOPE: Inspecting forwarding faults for Software
15. Defined Networking", *IEEE/ACM Trans. on Netw.*,Apr 2017,pp. 2347-2360.