Survey of optimizing dynamic virtual local area network algorithm for software-defined wide area network

Talah Oday Alani, Ameer Mosa Al-Sadi
Computer Engineering Department, University of Technology - Iraq, Baghdad, Iraq

Article Info

Article history:

Received Jul 07, 2021
Revised Oct 26, 2022
Accepted Nov 06, 2022

Keywords:

Dynamic VLAN
Open-Flow
SD-WAN
Software-defined network
Virtual local area network

ABSTRACT

Software-defined network (SDN) is one of the most predominant technologies for networking in the existing and next-generation networks. Therefore, this paper is conducted to introduce a survey for researchers who are interested in exploiting the dynamic tunneling technique to optimize software-defined wide area network (SD-WAN). The main purpose of this survey is not only to investigate the related works of dynamic tunneling with SD-WAN but also to classify this related work according to the aim of each research into the practicable categories and present the most dominated employments for tunneling with SD-WAN, specifically virtual local area network (VLAN). The performed classification accompany dynamic tunneling in SDN can be summarized into four categories as following: exploring VLAN in SDN; management of multi VLAN in SDN; recover link failure of SDN; and development of SDN by using VLAN. Finally, the intensive study of the literature in this paper discovers that the dominant path of research falls in the class that covers SDN's link failure. This class takes full advantage of SD-WANs due to offering more robust networking and restoring most communication failures. In the event of a fault, the controller could respond and recover quickly by switching to a pre-computed backup route.

Corresponding Author:

Talah Oday Alani
Computer Engineering Department, University of Technology - Iraq
Al-Sinaa Street, Baghdad, Iraq
Email: ce.19.03@grad.uotechnology.edu.iq

1. INTRODUCTION

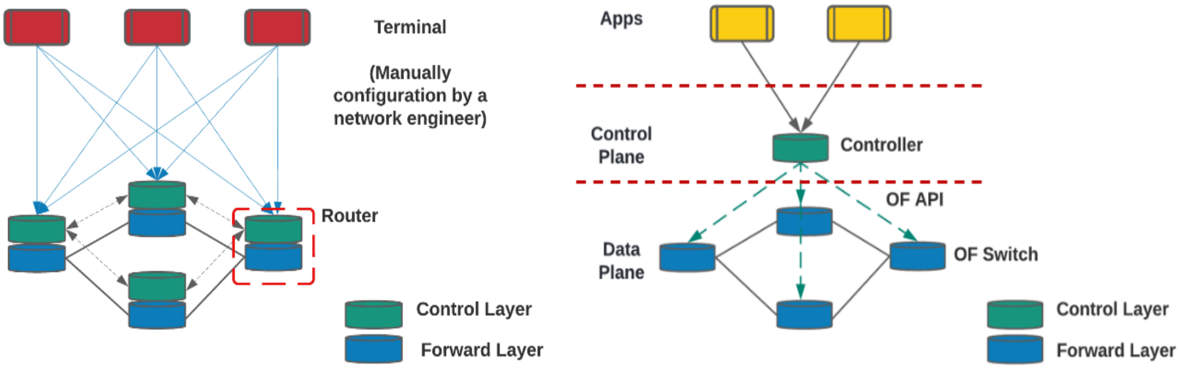
Today's society relies largely on technology to carry out daily tasks. Technology development has improved the way information is transferred to solve many issues in traditional networks by inventing software-defined network (SDN). The deployment of SDN with its powerful abilities in creating, managing, and terminating any type of customization or tunneling leads the researcher to employ it for many purposes. Tunneling can improve many features such as quality of services (QoS), security and privacy. The wide spectrum of this implementation motivates to write literature that investigates this hot topic [1].

Traditional networking hardware becomes imperfect by growing the social media, mobile devices, and cloud computing technologies because it experiencing several cons [2], [3]. The first one, these networks have too many types of equipment, such as proxy, load balancers, firewalls, and intrusion detection systems (IDS), in addition to the primary devices such as routers and switches. The second cons, the control of the network is distributed to be run on all routers and switches of this network. In addition, the operating system and protocols of network devices are usually closed and obligated by device manufacturers. The last cons, a human is needed to administrate the network devices by utilizing some programming interfaces [4], [5] (see Figure 1(a)).

One of the main problems which have been driven from the premonition cons of traditional networks is missing an end-to-end path reservation mechanism. That is because, each switching function in traditional networks is responsible for packet forwarding logic based on rules defined in its local software [6]. The traffic engineering solved this issue by utilizing some tunneling techniques such as virtual local area network (VLAN). VLAN is a technology that, is separated from the physical core network, which could configure logical networks on layer 2 (data link layer) [7]. This technique allows making a reservation for some network resources for specific traffic. The VLAN application aims to increase security, control the network, and simplify the network [8].

The advent of new services such as the internet of things, cloud integration and cloud services, big data, and IT consumerization and mobility, escalated the network demands. This escalation restricts VLAN techniques to solve all these new challenges. That, call the necessity of handling a new solution can provide more management flexibility by supporting the programming language, which is represented by a new model called, SDN [9]–[12].

The way of building and managing the network is being changed by SDN [13], as shown in Figure 1(a). SDN has two characteristics that distinguish it as a leading paradigm of the network. First, the SDN separates the control plane (which defines how traffic can be managed) from the data plane (which directs traffic based on decisions made by the control plane) has been illustrated in Figure 1(b) [14]. Second, the SDN centralizes the control plane such that various data-plane components can be controlled by a single software control function [15]. The SDN control plane exerts direct control over the state of the network's data plane elements (i.e. routers, switches, and other middleboxes) through a well-defined application programming interface (API). A popular example of such an API is OpenFlow (OF). The OF switch has one or maybe more packet-handling rules tables. Each rule fits a traffic subset and conducts such traffic acts that conform to a rule; behavior involves dropping, forwarding, or flooding. For improved automation, scalability, and stability, SDN offers better strategies for unified dynamic management and control configurations. The OF switch will act like a router, switch, firewall, network address converter, or anything, based on the rules configured by the controller application [16], [17]. The new ability of controller rules and OF switches escalates the motivation to use VLAN with SDN. Doubtlessly, the above explanation can demonstrate the motivation to use VLAN with SDN and consider it as a focus of this paper, which prospect to assist another researcher. The rest of this paper is arranged as the following: section 2, briefly revises the related work; section 3, show the main differences between VLAN-SDN and VLAN-traditional network; section 4, discusses research challenges and future work/ research trends. Finally, this paper is concluded in section 5. All section try to identify the evolution of tunneling in presence of SDN.



(a) (b)

Figure 1. The difference between the traditional network and SDN (a) traditional network and (b) software-defined network [18]

2. LITERATURE REVIEW

This study presents the research related to using VLAN with SDN. These researches have been categorized into four classes according to the aim of the research. These four classes are exploring VLAN in SDN, management of multi VLAN in SDN, recover link failure in SDN, and development SDN by using VLAN.

2.1. Exploring virtual local area network in software-defined network

Xu and Xu [19] explore VLAN in SDN by proposing an SDN model supporting VLANs, which provide significant characteristics to create a scalable layer 2/3 network for data centers. The proposed network employs the physical OpenFlow switches characterized by routing paths, which will be pre-computed. Also, the operation of encasing and unpacking packets is not necessary. It uses an entirely different operation style for the controller, which highly releases its workload, and forwards flow more efficiently.

Hameed and Wasim [20] achieve four VLAN functions by using SDN and VLAN networks. These functions include broadcast inclusion, QoS, security policy enforcement, and traffic grasp. This research uses two types of experimental networks: for VLANs and for checking SDN-capable switches. The mininet SDN emulator to create network tests. Open vSwitches are the switches on the SDN network, and virtual machines (VMs) are the hosts. After that, the performance is evaluated by the iPerf tool, and the packets are captured and analyzed by Wireshark.

Maeda *et al.* [21] propose a method that derived quantity features from the traffic data. These features are extracted for every session and separate the infected computer after detecting malicious behavior using the deep learning multilayer perceptron (MLP) model. The tests are conducted to distinguish botnet and dangerous traffic from regular traffic, then check that the rules for lookup SDN compromised terminals have been evolved and accommodated. A firmware (FW) and VLAN are used to isolate an infected interface via SDN. Botnet traffic was identified by monitoring the behavior of flow operation using machine learning and network control (FW and VLAN) could be dynamically activated using SDN. The Ryu SDN system for the OpenFlow controller and Open vSwitch for the OpenFlow switch were used for the SDN quarantine experiment. As a result, the detection rate of this work was better than the rate of the existing methods.

Gheisari *et al.* [22] provide a platform for internet of thing (IoT) and SDN integration. Then, they provide a way for resolving the data privacy issue. Some advantages can be realized with the use of VLAN such as clients that are distributed over a network are grouped together, a smaller number of routers are required to broadcast traffic, and fewer conflicts and traffic congestion. This technique provides flexibility, easier network management, network maintenance, and a level of privacy protection that is acceptable.

Rauf *et al.* [23] suggest a communication architecture that integrates both enterprise integration patterns (EIP) and SDN in an enterprise setting. The proposed communication framework’s design includes an adaptive VLAN module that uses EIP to deploy and remove VLANs in a reactive manner. This framework also includes a packet forwarding module that hides the host’s IP addresses from each other to enable communication between applications from different networks in a corporate context. The Ryu SDN controller serves as the foundation for the whole system. The network mapper (NMAP) network scanner was used to evaluate the framework, and the findings reveal that it delivers dependable, secure, and smooth communication across multiple hosts.

Pawar and Kataoka [24] propose the use of SDN to provide segmented proactive flow rule injection (SPFRI). The suggested SPFRI stores the contextual information for service chaining in the VLAN header using the VLAN ID. Even if one or more middleboxes change packets in both the outbound and inbound directions of a flow, SPFRI preserves the service chain’s consistency. Theoretically verifiable service chaining via SPFRI can be achieved, even in the presence of changing middleboxes.

As a conclusion of this class, by developing an SDN model that supports VLANs, in [19]–[21] investigate VLAN in SDN, also improve SDN service and traffic management. Also, in [22]–[24] use VLAN ID and VLAN module to segment SDN by deploying and removing VLANs in a reactive fashion and employ SDN to take advantage of VLAN features. To sum up, the research of this calss explored the abilites SDN to improve its management and segmentation using dynamic VLAN.

2.2. Management of multi virtual local area network in software-defined network

Mathew and Prabhu [25] multi VLAN managed in SDN that present the concept of VLAN and inter VLAN routing, a configuration with four switches layer 2 (L2) and two switches layer 3 (L3) together with a router. The technologies associated with VLAN formation and VLAN maintenance have also been explained. Static routing is required to provide traffic routing between various VLANs. This paper used VLAN to provide connect switches with two different layers.

Lehocine and Batouche [26] aim to provide large networks with effective VLAN segmentation, as well as minimal input data provided by the network administrator and minimal overhead processing for the switches. The Ryu SDN controller was selected to validate the suggested technique for deploying VLAN filtering and segmentation on SDN networks. The SDN network is emulated using mininet to build an entire OpenFlow network.

Aziz [27] default native and management VLANs were viewed as three distinct VLAN types. The effects of the packet tracer software confirm that VLAN-based network isolation isolates the transmitted traffic of the devices regardless of their existence in the exact location with separate network classifications, even if all of the systems in the regions will share the same cable and switch. The creation of VLANs is needed for data and traffic management as the LAN expands and more network devices are introduced to keep the broadcast frequency valid.

Sandhya *et al.* [28] solve the challenge of implementing waypoint enforcement in a multi-VLAN hybrid-SDN that isn't limited by these constraints. The suggested technique uses the idea of gratuitous address resolution protocol (ARP) to damage the ARP tables of all hosts in the network to direct traffic packets to an SDN switch. SDN creates a hybrid SDN system in which legacy and SDN computers coexist in the same network. Mininet was used to perform the experiments.

Poncea *et al.* [29] in SDN, multi-VLAN management is achieved by introduce a new source routing approach to SDN that uses stacked VLAN tags, and it proved to have many benefits over other forwarding approaches. In mininet, this approach was tested using the Ryu controller. This solution can be allowed by default across the data center, simplifying flow tables in core switches, or only when the number of flows exceeds the total capacity if the packet size is a problem. When to do it is up to the controller. This technique was used to improve multipath routing because packets can be led on different paths from the source using fine-grained distribution algorithms, and switches in the center would be unaware of it.

In conclusion of this class, Sandhya *et al.* [28] and Poncea *et al.* [29] improve multipath routing by using VLAN tags compared to other forwarding methods, they have several advantages. While studies [25]–[27] have handled many VLAN in SDN and many techniques for the configuration and maintenance of VLAN. Finally, all of the researchers in this class demonstrated how effective SDN for managing VLANs.

2.3. Recover link failure in software-defined network

Zhang *et al.* [30] present a local fast reroute (LFR) method with flow aggregation in the SDN with VLAN ID. When a connection failure is identified in LFR, all traffic flows affected by the breakdown are combined into a new "large" flow. The SDN controller then deploys a local redirect path for the aggregated traffic dynamically. Mininet can be used to simulate network topology. According to the results, LFR offers quick recovery while reducing the overall amount of flow entries in SDN.

Chen *et al.* [31] propose a fast, low memory consumption protection-based recovery mechanism for link failures using the VLAN tag. In case of a malfunction occurs, this method can respond and restore rapidly without the interference of the controller by transitioning to the backup route that has been pre-computed. The reconstruction takes 50 milliseconds to complete in the simulation, while this process takes just 20 milliseconds. In comparison, this approach can save more ternary content addressable memory (TCAMs) than other protection approaches. Mininet, a simulation platform based on the ubuntu operating system, is used.

Liaoruo *et al.* [32] present a technique of link protection based on source routing in SDN. When a link fails, this solution uses source routing to manage the flow's route and guides the packet onto the backup path by modifying the source routing header. Route information is encoded in the VLAN ID field. Because researchers store route information in the packet's header instead of flow entries stored in switches, this strategy can greatly minimize the complexity of building and maintaining backup pathways after implementation and assessment.

Vadivelu and Malathy [33] in SDN link failure recovering to examine a definition of layer 2-switching and its load-balancing system. Aggregation and linking are achieved through the network of the (VLAN). The switch connects multiple hosts and defines an appropriate network route. Then, the router allows the sharing of the VLAN with external users. Information sharing is possible on the network's host, switch, and router. Link aggregation is carried out to enhance QoS and results. Connect aggregation is a technique for combining several network connections in parallel to increase throughput above what a single link can handle while still providing continuity in the case of a link collapse. It is well known that the mechanism boosts performance and is made possible by actual network equipment.

Chen *et al*. [34] propose a protection VLAN (pro-VLAN) solution that determines an exact backup path and assigns a single VLAN ID to each network connection that the security system supports. It takes advantage of the most critical features of SDN and can recover one connection loss in SDN, all while offering high performance, scalability, and applicability. Both pro VLAN and protection path (pro-PATH) achieve a fast failure recovery, according to the simulation results.

In conclusion, it's noticeable that the researches [30]–[34] of this class have many benefits, because they provide a very fast response and restoration for link failure without the interference of the controller. One benefit is increasing the software-defined wide area network (SD-WAN) reliability. Another benefit of preserving the latency of packet retransmission due to supply of alternative paths for packets of the failed link. In addition, little research has proposed a way to help the controller to forecast the node mobility and link failure probability.

2.4. Development software-defined network by using virtual local area network

Nguyen and Kim [35] used VLANs to develop SDN by incorporating SDN and OpenFlow into the campus and enterprise network environments. An application was built and implemented in this architecture for quickly controlling and flexibly troubleshooting the VLANs. This program provides both static VLAN and dynamic VLAN settings. Answer the hybrid mode service, which requires packet processing from both the OpenFlow control plane and the traditional control plane.

Jerome *et al.* [36] explain the multi-path transmission control protocol (MPTCP) transport layer protocol, increasing network load management and use. The overall network throughput improves even more as MPTCP traffic is directed using specific VLAN paths without clear VLAN paths. The internet protocol (IP) aliasing concept can also be used to bind several IP addresses to a single host, allowing OpenFlow to construct additional MPTCP sub-flows.

Saenko and Kotenko [37] introduce the concept of VLAN "roles" and use the role-based method to simplify VLAN-based access control schemes. An enhanced genetic method is presented to tackle the optimization problem. An improved genetic algorithm is proposed. Changes are linked to a multi chromosome human representation, a modern version of the exercise function, a two-dimensional method of crossover action, and many other factors. The results of the tests show that the genetic algorithm proposed is highly effective.

Sowjanya and Anitha [38] were constructing an appropriate VLAN to reduce network traffic loads. A concept known as VLAN has been created to minimize the traffic load. This study illustrates the advantages of improving a network's efficiency by reducing the traffic load by adding additional network protection by limiting the exchange of information by users. Notice that only the expected devices are forwarded to the data packets since the VLAN was created in the switches. The traffic load on the network has therefore decreased because data is not spread across the existing network.

Almalki [39] states that the visual simulation platform provides fifth generation (5G) IoT smart buildings using a virtual network in the cisco packet tracer. Protection, fire safety, and energy management are regarded in the 5G IoT architecture. The results of the VLAN simulation show that allowing 5G IoT to buildings shows protection, comfort, improves energy efficiency, and reduces costs, there is a great potential to apply this model in real life in different domains.

In conclusion of this class, many studies in [38], [39] create VLAN to optimize and segregate the traffic load of the network. This optimization depends on the SDN's promising capabilities. Studies [35]–[37] reduce cost, and time of service and discover the error early, by creating and executing the application to control the VLAN depending on the SDN.

3. THE DIFFERENCES BETWEEN VLAN-SDN AND VLAN-TRADITIONAL NETWORK

First, SDN enables dynamic configuration VLAN that makes better utilization of the network and makes changes on operations (add, delete, edit) on VLAN, but traditional network generates fixed VLAN that cannot be modified [40], [41]. SDN also improves service availability due to the controller's ability to calculate backup pathways in the event of a failure, as well as a faster convergence time as compared to a traditional network [42], [43]. Moreover, it has been noticed that VLANs with traditional networks are established to accomplish certain tasks and that alterations or modifications cannot be made to meet the needs of the user. On the other hand, SDN has a faster configuration that is a viable approach to deal with the issues of VLAN administration since it is characterized by centralized network management and network programmability [44]-[46]. Another noteworthy point, although VLANs are an excellent traffic management tool, they do not provide network security in a traditional network. On the contrary, SDN can enhance network security and fewer risks of misconfiguration [47]-[49]. Finally, increase network efficiency through centralized administration and control, as well as more orchestration and automation. The controller may dynamically set policies and offer access control [50], [51].

4. RESEARCH CHALLENGES AND FUTURE WORK / RESEARCH TRENDS

The aim of this study is to guide the researcher to the resources and publishers whose interested in this topic. At the same time, the table can confirm that the resources of this paper depend on authorized materials. The content of Table 1 (see appendix) shows the methodology of each research and the challenges, in addition to, showing the future work of each one and its publication year. From Table 1, it is noticed that most of the research analyzed present networks theoretically, including issues, drawbacks, solutions, simulation tools, algorithms, and results. After that Table 2 (see appendix) is added to show the most popular journals that have the papers published on this topic and sorted the number of used papers from each of them.

5. CONCLUSION

SD-WAN provided an opportunity to solve many issues of a traditional network. This paper presents a survey for researchers who are curious about using dynamic tunneling to improve SD-WAN performance. This study summarizes the research that has been done on advancing SDN technologies through tunneling mechanisms. According to the research's aim, these studies have been divided into four categories (exploring VLAN in SDN; management of multi VLAN in SDN, link failure of SDN; and development of SDN by using VLAN).

To summarize the result of study, many of the studies offered a theoretical analysis of current networks, challenges, difficulties, solutions, and algorithms. In class 1, some researchers investigate VLANs in SDN by presenting a VLAN-supporting SDN paradigm and utilizing the VLAN module to get dependable, secure, smooth results, and minimize the broadcast domain in SDN. Several researchers in class 2, multi VLAN managed in SDN that explains VLAN and inter VLAN routing as well as VLAN maintenance. In class 3, the numbers of the research measure the recovery times for link failures using the VLAN. Other researchers in class 4, increase energy efficiency and lowers expenses by creating and running an application to construct a VLAN based on SDN. A few researchers increase and optimize the QoS and performance, solve the scalability problem, and traffic management.

In a conclusion, the intensive investigating of the literature which presented at the conclusion of each class. The class of link failure takes full advantage of SD-WANs by improving the process of restoring many communication failures and improving the system reliability. These researchers prove this outcome by comparing and contrasting the time it takes for three distinct approaches for recovering (restoration, pro-flow, and pro-VLAN). Other studies that use VLAN tags in SDN present a unique method for source routing, and some of them use link aggregation to increase the QoS and performance. Furthermore, other researchers establish a precise backup path and allocate a specific VLAN ID to each network connection. Also, it's essential to refer that, each research presented in our classification has been determined a specific niche and its solution. A lot of hope that this review will be helpful to many future researchers.

ACKNOWLEDGEMENTS

This work was supported in part by the Iraqi ministry of higher education and scientific research the University of Technology Iraq, which represents the institution of the first and second authors.

APPENDIX

Table 1. Summary table of research

Author name	The class (aim)	How to optimize (methodology)	Research challenges	Future work	Publish year
F. Xu and Y. Xu [19]	Exploring VLAN in SDN	Auxiliary VLANs are used by isolating the telephones on an auxiliary VLAN with native VLANs to ensure the efficiency of voice over internet protocol (VoIP) traffic.	In the implementation of fabric in the network topology, construction is dynamic: switches and connections may all be added or withdrawn. Following notification of such events, the controller must compute the consequences and repair the impacted pathways.	- Test the architecture and encourage its success within the entire network. - The components of traffic engineering will be developed and tested. - Because the controller is the only one who can resolve the ARP, how can the controller's stresses be relieved?	2016
P. Pawar and K. Kataoka [24]	Exploring VLAN in SDN	Devised and implemented a technique that ensures accurate middlebox traversal without requiring any middlebox software modifications the proposed SPFRI stores the contextual information for service chaining in the VLAN header using the VLAN ID.	Because middleboxes change packet headers and the service context is lost, service chaining is challenging.	The suggested SPFRI will Implement and investigate its integration with the current network functions virtualization (NFV) software architecture for real-world deployment and performance and operational overhead analysis.	2016
M. Gheisari *et al*. [22]	Exploring VLAN in SDN	Aggregation, encryption, and VPN are three privacy-preserving ways that any device in the network might use to convey data to the SDN controller. If the device should use encryption, there are four different encryption rules that may be used. Overall, the SDN controller assigns six different privacy-preserving approaches for an application to each device.	- The term "computation cost" refers to the expense of estimating the level of system overload. - This strategy causes the system to be overloaded by at least 15%.	Using a number of assessment indicators, such as computational cost and penetration rate, to assess the suggested solution. Proposing an application-specific privacy-preserving approach in the IoT-SDN context is another possible future effort.	2018

Table 1. Summary table of research (*continue*)

Author name	The class (aim)	How to optimize (methodology)	Research challenges	Future work	Publish year
S. Maeda *et al*. [21]	Exploring VLAN in SDN	Analyze malware traffic data obtained from an internal network and use deep learning to distinguish regular traffic and malicious traffic. Can work with malware in a scalable way by programming. Deep learning runs on a software-defined network to avoid host identification after infection and secondary damage detection of an infected host.	The botnet detection module applies the classifier learned by MLP to the feature set supplied by the feature extraction module and uses pre-assigned labels to classify malicious or regular traffic.	It is essential to investigate whether network isolation is often used on an infected phone number.	2019
A. Hameed and M. Wasim [20]	Exploring VLAN in SDN	The network is divided into a particular set of categories (broadcast containment, QoS, security policy implementation, and traffic capturing). The experimental network's hosts are all set to send out transmitted packets.	- SDN's changing nature. - New VLANs standards improved performance and scalability for bigger carrier networks. - Current investments in VLAN-based network architecture.	VLANs are expected to flourish in the presence of SDN, allowing networks to take advantage of the benefits of both technologies.	2019
B. Rauf *et al*. [23]	Exploring VLAN in SDN	To support message communication structure, built numerous SDN modules (host registration, adaptive VLAN management, ARP req resolution, and packet forwarding). Created two distinct host setup situations and designed a series of tests to assess the communication framework's accuracy, efficiency, and security. The NMAP network scanning tool is used to do the security assessment.	Suggested a module to provide adaptive VLAN setups and administration by using SDN's features.	- To fully leverage all of EIP's characteristics in SDN networks for secure, fault-tolerant, reliable, and efficient communication, more research is needed. - Aim to look into the suggested framework's flaws in order to improve the overall security of the business SDN network.	2021
A. I. Mathew and S. R. B. Prabhu [25]	Management of multi VLAN in SDN	This technique divides a single extensive broadcast domain into several domains. This means that a single switch can perform many functions.	Break broadcast domains to create a virtual LAN and connect with one another.	/	2017
M. B. Lehocine and M. Batouche [26]	Management of multi VLAN in SDN	When a switch receives a non-tagged frame with no corresponding rule, a packet-in message is sent to the controller, which will respond to the receiving switch by forwarding the received frame through physical port x, flooding the received frame to all physical ports except the receiving port, and dropping the received frame, depending on the information stored in the private VLANs database (PVLAN - DB).	The concentration of intelligence and control has made it possible to deploy applications in vast networks with high reliability and cheap cost.	Extend the current study to more complex use cases, such as handling tagging systems such as multiprotocol label switching protocol (MPLS) and virtual extensible local area networks (VXLAN), by communicating the inheritance principle between incoming switches, allowing for complete control of traffic flows at the ingress edge-switches with the least amount of computing overload.	2017
O. M. Poncea *et al*. [29]	Management of multi VLAN in SDN	Stacked VLAN tags are used to present a novel approach to source routing in SDN.	Streamlining flow tables in core switches, or only when the number of flows approaches the maximum capacity if the packet size is a concern.	It is possible to build specific and fast hardware that only needs VLAN port-switched based source routing (PSSR) support, resulting in a substantial cost reduction per switching unit.	2017
D. A. Aziz [27]	Management of multi VLAN in SDN	The network was divided into separate VLANs to display the performance of three distinct VLAN types specified by default, native and management VLANs. While computer transmission traffic is divided between computers, the same cable and switch will connect multiple locations.	- The broadcast traffic of computers acting in separate departments but belonging to the same network classification can be segregated, although the same cable and switch can be shared across regions. - Set up the security policy to monitor attackers and hackers from the sub-networks indicated by the student data and management VLANs.	/	2018

Table 1. Summary table of research (*continue*)

Author name	The class (aim)	How to optimize (methodology)	Research challenges	Future work	Publish year
Sandhya, *et al*. [28]	Management of multi VLAN in SDN	All network traffic was put under the jurisdiction of the unified SDN controller while maintaining existing VLAN configurations. Gratuitous ARP (GARP) packets were used to poison each host's ARP table, causing all packets from that host to be routed to the nearest SDN switch to poison all the hosts' ARP table multi-homed host computer was used instead of an SDN switch.	- To poison the ARP table of all the hosts, utilize a multi-homed host machine instead of an SDN switch.	Various heuristics can be developed to improve SDN reachability while reducing overhead and minimizing end-to-end delay.	2018
X. Zhang *et al*. [30]	Link failure in SDN	The data plane switches immediately activate the backup path when a connection breaks, by passing the SDN controller. As a result, SDN protection allows for quick recovery in the event of a connection breakdown.	By lowering the number of flow operations between the SDN controller and switches, LFR provides quick recovery.	/	2017
J. Chen *et al*. [31]	Link failure in SDN	Compare and contrast the recovery times of three different strategies (restoration, pro-flow, and pro-VLAN)	- As the protection method is utilized, the system recovers fast and reliably from link failures. - Instead of each flow, creates backup pathways based on each connection as a consequence, before any failure, each connection has its own backup computed.	/	2016
R. Vadivelu and S. Malathy [33]	Link failure in SDN	Link aggregation is used to increase the QoS and performance. Layer 2 exists most frequently through switch ports, which can be physical or virtual and is handled by VLAN, Hot standby router protocol (HSRP), and the connection.	Link aggregation is used to improve QoS and performance.	Improves efficiency Networks that have more complex topologies on a broader scale.	2017
H. Liaoruo *et al*. [32]	Link failure in SDN	When a link fails, a packet is transmitted to the fast failover group table, and the switch adjusts the original port's status based on the failure detection result. The switch then updates the old packet header with a new one using pop and push VLAN tags in accordance with the established action list so that packets can be transported over a new path, similar to the packet header programming procedure.	- It is capable of performing local connection failure recovery in less than 50 milliseconds. - It has the ability to recover quickly from connection failures while consuming relatively little flow. - It is simple to implement flexible and dynamic backup path design based on network state.	This research will deal with the finer points of the installation procedure and look into the use of source routing SDN in other sectors.	2016
J. Chen *et al*. [34]	Link failure in SDN	When backup paths are determined instead of each flow for each connection, high reliability is achieved, and group tables are used to dynamically and locally swap backup paths when errors occur.	Pro-VLAN, the protection mechanism, generates both functioning and backup routes and saves them in switches before problems occur.	As the network size expands, the number of working flow entries per switch grows as well.	2018
V. -G. Nguyen and Y. -H. Kim [35]	Development SDN by using VLAN	Create two VLAN networks with the same VLAN ID for two pairs of hosts. The average network delay for dynamically building a VLAN segmented network for a couple of hosts was calculated by dynamic VLAN.	- Create a VLAN management application that supports both static and dynamic VLAN configurations. - Provide an interactive graphical user interface (GUI).	- This analysis can be expanded to include multi-domain support. - The rule placement problem, which refers to the correctness of rule installation in switches and introducing a new spanning tree protocol (STP) algorithm, requires further research.	2015
A. Jerome *et al*. [36]	Development SDN by using VLAN	For hosts and routers, VLAN-specific route formation was used. Also, without using any path formation, the output was calculated using standard MPTCP.	- Design and build an SDN framework that allows network managers to investigate how MPTCP can help them create VLANs that use OpenFlow. - Develop heuristics that would help direct MPTCP flows across the network in an efficient manner that would further help in improving load balancing and network utilization across the network.	- At the switch stage, automation of the path calculation process may be valuable and cost-effective.	2018

Table 1. Summary table of research (*continue*)

Author name	The class (aim)	How to optimize (methodology)	- Research challenges	- Future work	Publish year
I. Saenko and I. Kotenko [37]	Development SDN by using VLAN	Introduces the idea of VLAN "roles" and uses the role-based approach to optimize VLAN-based access control schemes.	- The mathematical underpinnings for the role-based VLAN access control strategy are provided. - The developed testbed considers the condition of guaranteed availability of a solution to the problem, which allows for increasing the reliability of the estimates.	- The suggested approach's used in other fields of access management. - Examining the impact of different decompositions focused on a hierarchy of functions.	2019
N. L. Sowjanya and R. Anitha [38]	Development SDN by using VLAN	three departments were created to act like three separate networks, although they are present only in a single switch. VLANs provide additional security to the networks.	Static VLAN, which is based on port numbers, is being implemented. A distinct broadcast domain is created for each current VLAN.	- The routing pathways between the routers are automatically changed in dynamic routing.	2020
F. A. Almalki [39]	Development SDN by using VLAN	The Cisco Packet Tracer is used to demonstrate the deployment of the projected 5 G IoT intelligent buildings.	Give a thorough 5G IoT deployment to smart buildings utilizing the Cisco Packet Tracer tool from many smart viewpoints.	- Apply this model in real life in various domains for security, comfort, improving energy efficiency, and reducing costs.	2020

Table 2. Resources of researches

Resources	No. of papers	Total inclusion rate in %
IEEExplore	6	17
International conference on communication systems and networks	6	17
International journal of current engineering and scientific research (elsevier)	4	11
Telkomnika (telecommunication computing electronics and control)	3	8
Springer nature	2	5
ACM digital library	2	5
Journal of information processing system	2	5
International conference on information and communication technologies	1	2
International conference on computer communications and networks	1	2
International symposium on networks, computers, and communications	1	2
Electrical engineering and computer science	1	2
International journal of printing, packaging, & allied sciences	1	2
Journal of circuits, systems, and computers	1	2
International conference on transparent optical networks	1	2
Proceedings of the genetic and evolutionary computation conference companion	1	2
International journal of advanced trends in computer science and engineering	1	2
International journal of electronics communication and computer engineering	1	2
Total	35	100

REFERENCES

[1] A. M. Al-Sadi, A. Al-Sherbaz, J. Xue, and S. Turner, "Developing an asynchronous technique to evaluate the performance of SDN HP aruba switch and OVS," *SAI 2018: Intelligent Computing*, 2019, pp. 569–580, doi: 10.1007/978-3-030-01177-2_41.

[2] K. Benzekki, A. E. Fergougui, and A. E. Elalaoui, "Software-defined networking (SDN): a survey," *Security and Communication Networks*, vol. 9, no. 18, pp. 5803–5833, 2017, doi: 10.1002/sec.1737.

[3] R. Masoudi and A. Ghaffari, "Software defined networks: A survey," *Journal of Network and Computer Applications*, vol. 67, pp. 1–25, 2016, doi: 10.1016/j.jnca.2016.03.016.

[4] P. Göransson, C. Black, and T. Culver, "SDN futures," in *Software Defined Networks*, Elsevier, 2017, pp. 353–374, doi: 10.1016/B978-0-12-804555-8.00015-6.

[5] X. Wu, K. Lu, and G. Zhu, "A survey on software-defined wide area networks," *Journal of Communications*, pp. 253–258, 2018, doi: 10.12720/jcm.13.5.253-258.

[6] O. S. Al-Heety, Z. Zakaria, M. Ismail, M. M. Shakir, S. Alani, and H. Alsariera, "A comprehensive survey: benefits, services, recent works, challenges, security, and use cases for SDN-VANET," *IEEE Access*, vol. 8, pp. 91028–91047, 2020, doi: 10.1109/ACCESS.2020.2992580.

[7] D. A. J. Al-Khaffaf and M. G. Al-Hamiri, "Performance evaluation of campus network involving VLAN and broadband multimedia wireless networks using OPNET modeler," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 19, no. 5, pp. 1490-1497, 2021, doi: 10.12928/telkomnika.v19i5.18531.

[8] Y. A. Makeri, G. T. Cirella, F. J. Galas, H. M. Jadah, and A. O. Adeniran, "Network performance through virtual local area network (VLAN) implementation &amp; enforcement on network security for enterprise," *International Journal of Advanced Networking and Applications*, vol. 12, no. 06, pp. 4750–4762, 2021, doi: 10.35444/IJANA.2021.12604.

[9] V. Balasubramanian, M. Aloqaily, and M. Reisslein, "An SDN architecture for time sensitive industrial IoT," *Computer Networks*, vol. 186, 2021, doi: 10.1016/j.comnet.2020.107739.

[10] T. Huang, F. R. Yu, C. Zhang, J. Liu, J. Zhang, and Y. Liu, "A survey on large-scale software defined networking (SDN) testbeds: approaches and challenges," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 2, pp. 891–917, 2017, doi: 10.1109/COMST.2016.2630047.

[11] R. Deb and S. Roy, "A comprehensive survey of vulnerability and information security in SDN," *Computer Networks*, vol. 206, 2022, doi: 10.1016/j.comnet.2022.108802.

[12] S. K. Keshari, V. Kansal, and S. Kumar, “A systematic review of quality of services (QoS) in software defined networking (SDN),” *Wireless Personal Communications*, vol. 116, pp. 2593–2614, 2021, doi: 10.1007/s11277-020-07812-2.

[13] H. Tussyadiah, R. M. Negara, and D. D. Sanjoyo, “Distributed gateway-based load balancing in software defined network,” *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 18, no. 5, pp. 2352-2361, 2020, doi: 10.12928/telkomnika.v18i5.14851.

[14] V. Monita, I. D. Irawati, and R. Tulloh, “Comparison of routing protocol performance on multimedia services on software defined network,” *Bulletin of Electrical Engineering and Informatics*, vol. 9, no. 4, pp. 1612–1619, 2020, doi: 10.11591/eei.v9i4.2389.

[15] T. A. Assegie and P. S. Nair, “A review on software defined network security risks and challenges,” *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 17, no. 6, pp. 3168-3174, 2019, doi: 10.12928/telkomnika.v17i6.13119.

[16] A. L. Aliyu, P. Bull, and A. Abdallah, “Performance implication and analysis of the 0penflow SDN protocol,” in *2017 31st International Conference on Advanced Information Networking and Applications Workshops (WAINA)*, 2017, pp. 391–396, doi: 10.1109/WAINA.2017.101.

[17] M. Alsaeedi, M. M. Mohamad, and A. A. Al-Roubaiey, “Toward adaptive and scalable openflow-SDN flow control: A survey,” *IEEE Access*, vol. 7, pp. 107346–107379, 2019, doi: 10.1109/ACCESS.2019.2932422.

[18] G. Liang and W. Li, “A novel industrial control architecture based on Software-Defined Network,” *Measurement and Control*, vol. 51, no. 7–8, 2018, doi: 10.1177/0020294018784310.

[19] F. Xu and Y. Xu, “A SDN network based on VLANs for data centers,” *Proceedings of the 2016 International Conference on Engineering Science and Management*, 2016, doi: 10.2991/esm-16.2016.15.

[20] A. Hameed and M. Wasim, “On the study of SDN for emulating virtual LANs,” in *2019 8th International Conference on Information and Communication Technologies (ICICT)*, 2019, pp. 162–167, doi: 10.1109/ICICT47744.2019.9001947.

[21] S. Maeda, A. Kanai, S. Tanimoto, T. Hatashima, and K. Ohkubo, “A botnet detection method on SDN using deep learning,” in *2019 IEEE International Conference on Consumer Electronics (ICCE)*, 2019, pp. 1–6, doi: 10.1109/ICCE.2019.8662080.

[22] M. Gheisari, G. Wang, S. Chen, and A. Seyfollahi, “A method for Privacy-preserving in IoT-SDN integration environment,” in *2018 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Ubiquitous Computing & Communications, Big Data & Cloud Computing, Social Computing & Networking, Sustainable Computing & Communications (ISPA/IUCC/BDCloud/SocialCom/SustainCom)*, 2018, pp. 895–902, doi: 10.1109/BDCloud.2018.00132.

[23] B. Rauf, H. Abbas, A. M. Sheri, W. Iqbal, and A. W. Khan, “Enterprise integration patterns in SDN: A reliable, fault-tolerant communication framework,” *IEEE Internet of Things Journal*, vol. 8, no. 8, pp. 6359–6371, 2021, doi: 10.1109/JIOT.2020.3034350.

[24] P. B. Pawar and K. Kataoka, “Segmented proactive flow rule injection for service chaining using SDN,” in *2016 IEEE NetSoft Conference and Workshops (NetSoft)*, 2016, pp. 38–42, doi: 10.1109/NETSOFT.2016.7502439.

[25] A. I. Mathew and S. R. B. Prabhu, “A study on virtual local area network (Vlan) and inter-vlan routing,” *International Journal of Current Engineering and Scientific Research (IJCESR)*, vol. 4, no. 10, 2017. [Online]. Available: https://deliverypdf.ssrn.com/delivery.php?ID=0160130060950210220941251201271180290380200280040630101260241270750301171250281041240361180010320560560021160691140661050230890410610690870490981050800870931141110860170660150040860070771081040270020911161220870001021270680081200260940671250780080840 93&EXT=pdf&INDEX=TRUE

[26] M. B. Lehocine and M. Batouche, “Flexibility of managing VLAN filtering and segmentation in SDN networks,” in *2017 International Symposium on Networks, Computers and Communications (ISNCC)*, 2017, pp. 1–6, doi: 10.1109/ISNCC.2017.8071999.

[27] D. A. Aziz, “The importance of VLANs and trunk links in network communication areas,” *International Journal of Scientific & Engineering Research*, vol. 9, no. 9, pp. 10–15, 2018. [Online]. Available: https://www.researchgate.net/profile/Dlnya-Aziz-4/publication/327824310_The_Importance_of_VLANs_and_Trunk_Links_in_Network_Communication_Areas/links/5ba69acc299bf13e6045f14f/The-Importance-of-VLANs-and-Trunk-Links-in-Network-Communication-Areas.pdf

[28] Sandhya, M. Swamy, K. Haribabu, and A. Bhatia, “Achieving waypoint enforcement in multi-VLAN hybrid SDN,” in *2018 10th International Conference on Communication Systems & Networks (COMSNETS)*, 2018, pp. 519–521, doi: 10.1109/COMSNETS.2018.8328260.

[29] O. M. Poncea, F. Moldoveanu, and V. Asavei, “VLAN-PSSR: Port-switching based source routing using Vlan tags in SDN data centers,” *University Politehnica of Bucharest Scientific Bulletin Series C -Electrical Engineering and Computer Science*, vol. 79, no. 2, pp. 15–24, 2017. [Online]. Available: https://www.scientificbulletin.upb.ro/rev_docs_arhiva/full3f7_291525.pdf

[30] X. Zhang, Z. Cheng, R. Lin, L. He, S. Yu, and H. Luo, “Local fast reroute with flow aggregation in software defined networks,” *IEEE Communications Letters*, vol. 21, no. 4, pp. 785–788, 2017, doi: 10.1109/LCOMM.2016.2638430.

[31] J. Chen, J. Chen, J. Ling, and W. Zhang, “Failure recovery using vlan-tag in SDN: High speed with low memory requirement,” in *2016 IEEE 35th International Performance Computing and Communications Conference (IPCCC)*, 2016, pp. 1–9, doi: 10.1109/PCCC.2016.7820627.

[32] H. Liaoruo, S. Qingguo, and S. Wenjuan, “A source routing based link protection method for link failure in SDN,” in *2016 2nd IEEE International Conference on Computer and Communications (ICCC)*, 2016, pp. 2588–2594, doi: 10.1109/CompComm.2016.7925166.

[33] R. Vadivelu and S. Malathy, “Design and performance analysis of complex switching networks through VLAN , HSRP and link aggregation,” *International Journal of Printing, Packaging & Allied Sciences*, vol. 5, no. 1, pp. 139–148, 2017.

[34] J. Chen, J. Chen, J. Ling, J. Zhou, and W. Zhang, “Link failure recovery in SDN: high efficiency, strong scalability and wide applicability,” *Journal of Circuits, Systems and Computers*, vol. 27, no. 06, 2018, doi: 10.1142/S0218126618500871.

[35] V. -G. Nguyen and Y. -H. Kim, “SDN-based enterprise and campus networks: A case of VLAN management,” *Journal of Information Processing Systems*, Vol. 12, No. 3, pp. 511-524, 2016. [Online]. Available: https://koreascience.kr/article/JAKO201633055670755.pdf

[36] A. Jerome, M. Yuksel, S. H. Ahmed, and M. Bassiouni, “SDN-based load balancing for multi-path TCP,” in *IEEE INFOCOM 2018 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 2018, pp. 859–864, doi: 10.1109/INFCOMW.2018.8406943.

[37] I. Saenko and I. Kotenko, “A role-base approach and a genetic algorithm for VLAN design in large critical infrastructures,” in *Proceedings of the Genetic and Evolutionary Computation Conference Companion*, 2019, pp. 1643–1650, doi: 10.1145/3319619.3326853.

[38] N. L. Sowjanya and R. Anitha, “An efficient VLAN implementation to decrease traffic load in a network,” *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 9, no. 2, pp. 2147–2153, 2020, doi: 10.30534/ijatcse/2020/189922020.

[39] F. A. Almalki, “Implementation of 5G IoT Based Smart Buildings using VLAN Configuration via Cisco Packet Tracer,” *International Journal of Electronics Communication and Computer Engineering*, vol. 11, no. 4, pp. 56–67, 2020. [Online]. Available: https://ijecce.org/administrator/components/com_jresearch/files/publications/IJECCE_4379_FINAL.pdf

[40] Y. Xu *et al.*, “Dynamic switch migration in distributed software-defined networks to achieve controller load balance,” *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 3, pp. 515–529, 2019, doi: 10.1109/JSAC.2019.2894237.

[41] Z. Yang, Y. Cui, B. Li, Y. Liu, and Y. Xu, “Software-defined wide area network (SD-WAN): architecture, advances and opportunities,” in *2019 28th International Conference on Computer Communication and Networks (ICCCN)*, 2019, pp. 1–9, doi: 10.1109/ICCCN.2019.8847124.

[42] R. Amin, M. Reisslein, and N. Shah, “Hybrid SDN networks: A survey of existing approaches,” *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3259–3306, 2018, doi: 10.1109/COMST.2018.2837161.

[43] X. Huang, S. Cheng, K. Cao, P. Cong, T. Wei, and S. Hu, “A survey of deployment solutions and optimization strategies for hybrid SDN networks,” *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1483–1507, 2019, doi: 10.1109/COMST.2018.2871061.

[44] B. Gorkemli, S. Tatlicioglu, A. M. Tekalp, S. Civanlar, and E. Lokman, “Dynamic control plane for SDN at scale,” *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 12, pp. 2688–2701, 2018, doi: 10.1109/JSAC.2018.2871308.

[45] T. Semong *et al.*, “Intelligent load balancing techniques in software defined networks: A survey,” *Electronics*, vol. 9, no. 7, 2020, doi: 10.3390/electronics9071091.

[46] I. S. Petrov and R. L. Smeliansky, “Minimization of multicast traffic and ensuring its fault tolerance in software-defined networks,” *Journal of Computer and Systems Sciences International*, vol. 57, pp. 407–419, 2018, doi: 10.1134/S1064230718030085.

[47] C. Lin, K. Wang, and G. Deng, “A QoS-aware routing in SDN hybrid networks,” *Procedia Computer Science*, vol. 110, pp. 242–249, 2017, doi: 10.1016/j.procs.2017.06.091.

[48] M. Paliwal, D. Shrimankar, and O. Tembhurne, “Controllers in SDN: A review report,” *IEEE Access*, vol. 6, pp. 36256–36270, 2018, doi: 10.1109/ACCESS.2018.2846236.

[49] M. H. Rehmani, A. Davy, B. Jennings, and C. Assi, “Software defined networks-based smart grid communication: A comprehensive survey,” *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2637–2670, 2019, doi: 10.1109/COMST.2019.2908266.

[50] J. Bailey and S. Stuart, “Faucet: deploying SDN in the enterprise,” *Communications of the ACM*, vol. 60, no. 1, pp. 45–49, 2016, doi: 10.1145/3009828.

[51] X. Ma and T. Yu, “An algorithm of physical network topology discovery in multi-VLANs,” *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 14, no. 3A, 2016. [Online]. Available: https://123dok.com/document/4yrnon8z-algorithm-physical-network-topology-discovery-multi-vlans.html

BIOGRAPHIES OF AUTHORS

Talah Oday Alani received the B.Sc. in Computer Engineering from the University of Technology, Baghdad, Iraq, in 2018, and she is currently pursuing the M.SC. in Computer Engineering at the university of technology, Baghdad, Iraq. The interests of the researcher include Software Define Network, Network, Internet-of-Things. She can be contacted at email: ce.19.03@grad.uotechnology.edu.iq and talatota61@gmail.com.

Ameer Mosa Al-Sadi received the B.Sc. in Electrical and Electronic Engineering/ Computer from the University of Technology, Baghdad, Iraq, in 2002, and M.Sc. in Computer Engineering from Slovak University of Technology in Bratislava, Slovak Republic in 2009. Finally, he accomplished Ph.D. degree in computer and distributed system engineering with the University of Northampton, Northampton, U.K. This author became a Member (M) of IEEE in 2016. His research interests include software-defined networks, network function virtualization and distrusted systems, Internet-of-Things, smart cities, and 5G cellular network. He can be contacted at email: Ameer.M.AlSadi@uotechnology.edu.iq.