Summer 6-2-2021

Recent Trends in Software-Defined Networking: A Bibliometric Review

Jones Jefferson
jones.jefferson.mtech2020@sitpune.edu.in

Harikrishnan R
dr.rhareish@gmail.com

Recent Trends in Software-Defined Networking: A Bibliometric Review

Jones Jefferson, Harikrishnan R

Symbiosis Institute of Technology (SIT) affiliated to Symbiosis International (Deemed University) Pune, India.
Corresponding author: dr.rhareish@gmail.com

Abstract. Software-Defined Networking is referred to as the next big thing in the field of networking. Legacy networks contain various components such as switches, routers, etc. with a variety of complex protocols. A network administrator is responsible for configuring all these various components. Apart from complex network management, network security is also a persistent issue in the field of networking. SDN promises simplicity in network management while also dramatically improving the security of networks. This paper gives an analysis of the current trends in in SDN as well as Security challenges with SDN. A bibliometric review on SDN has also been outlined in this paper. We have also mentioned some of the challenges posed by the SDN architecture and also some of the solutions to combat them.

Keywords: Software-Defined-Networking, OpenFlow, Security, Cloud, Challenges

1. Introduction

Normal computer networks contain various devices such as Switches, routers, hubs, repeaters, etc. There are a variety of complex protocols that are used with these devices. It is the job of a network administrator to configure and manage all these devices. They try to accomplish this despite having only minimal access to the tools required to do the above-mentioned functions. This makes network management and tuning of the network a big challenge. Flexibility is one of the obstacles that traditional networks pose. In a traditional network, the devices like switches, routers have to make the call as to what traffic goes where.

Hardware ruled the world of networking until Software-Defined Networking emerged. The key principle behind SDN is the separation of control plane from the data plane. This allows all the traffic to flow through a single consolidated controller. This type of centralized network control allows all traffic to flow through a single entity thus improving the security aspect of SDN as well. So, by using SDN technology, all the traffic now can flow through a single firewall, thus making the capture of unwanted traffic using Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) more efficient. The separation of the control plane from the data plane also opens doors to automation. In traditional networks, the management and configuration of VLANs is an intricate task. SDN allows for the automation of these configurations while simultaneously improving the aspect of traceability of these configurations. One of the important protocols with respect to SDN is OpenFlow. Now the advantage with the OpenFlow protocol is that it makes the routing of traffic among switches and routers possible irrespective of the vendor that manufactures it. It also allows the enforcement of security policies at a high and a central level compared to physical configuration of the devices.

Now, this paper gives a brief review of some of the advancements as well as the vulnerabilities in SDN. The rest of the paper is organised as follows:

1. Review of the various papers
2. Bibliometric review
3. Challenges in SDN and solutions
4. Conclusion

Table 1 Summary of Acronyms

Sr No	Acronyms	Full form of Acronyms
1	SDN	Software-Defined Networking
2	VLAN	Virtual Local Area Network
3	IPS	Intrusion Prevention System
4	IDS	Intrusion Detection System
5	DDoS	Distributed Denial of Service
6	TCP	Transmission Control Protocol
7	WSN	Wireless Sensor Network
8	QoS	Quality of Service
9	VNE	Virtual Network Embedding
10	IOT	Internet of Things
11	MITM	Man in the Middle
12	LDS	Link Discovery Service
13	MAC	Media Access Control
14	IP	Internet Protocol

2. Literature review

The legacy network that are in use today are difficult to manage [1]. To enforce network policies, administrators would have to configure the devicies manually. These devices are usually speciic to the different vendors and support own low level commands for configuration. Tranditional networks are also integrated vertically. This means that the control plane as well as the data plane are coupled together. SDNs break this arrangement and decouple the data and the control plane giving more flexibility. This means that the the data plane devices act as devices that just forward traffic while the controlling logic is what drives them. The controller has the controlling logic [2]. Using SDNs, load balancing is possible to avoid problem of overloading. By load balancing, placement of network services in network is simplified [3]. Management of a variety of wireless networks becomes easier with SDNs [4]. In the current networking scenario, SDNs can be used to improve the aspect of security [5] [6].

Computer networks are made up of a plethora of devices like switches, routers, firewalls, etc. A network administrator handles the management of all these devices. The management of this network, configuring, turning, etc. is a very tedious and prone to human error as well. Here is where software defined networking comes into play. This can simplify network configuration as well as management. They key idea in which SDN is based on is: It allows programmability of network architecture of the cloud-based control plane which is detached from the data plane. The control plane handles deciding the path between two nodes to send the packets. So, the control plane is tasked with decision making. The other part of SDN is the data plane, which deals with forwarding traffic. This part can be programmed using Open Standard Protocols. Transition from traditional legacy networks to SDN is still taking time as there are a few concerns like: security, scalability, complexity. So, hybrid SDN's have been proposed where traditional network nodes and SDN can exist harmoniously. Hybrid SDN can interface the centralized (logically) SDN and legacy distributed Routing Information Base (RIB) [7].

In SDN, the functions of control and transmission are separated. This uses cloud platforms for the distribution of control plane. However, protection of cloud computing systems is a critical issue that needs to be take care of due to the increasing number of attacks on it like DDoS attacks, spreading malicious code on cloud platforms, compromised passwords, etc. Therefore, software-based Intrusion Detection Systems (IDS) are vital to SDNs. The intrusions are detected by the IDS

by processing data in the network. So, by combing machine learning with IDS, we can prevent attacks on the network as well as assure a high detection rate. The authors have used google cloud hosted OpenDayLight software as the SDN controller. They have used Support vector machines in conjunction with Gridsearch to detect attacks. They were trained on UNSW-NB-15 and NSL-KDD datasets and have proven that their technique is effective against attacks on SDN based cloud environments [8].

Service providers make use of mechanisms like balancing load as well as saving energy to meet the requirements of today's networks. Network providers generally leave routers as well as switches on 24/7 irrespective of the traffic because they need to satisfy the demands of the users as well as to account for the occasional traffic spikes. This results in increased energy consumption. Network providers can leverage SDN to manage the use of resources and lower the cost of operation. Load balancing distributes the network traffic across multiple accessible links. Shutting down as many networking links as well as devices as possible reduces energy. The authors in this paper have proposed a model to save energy and balance load to maximize use of resources as well as save energy [9].

SYN flood attacks are a major threat to SDN infrastructures. The IDS that try to detect these attacks result in performance deterioration and reduced response time. The centralized SDN controller is a potential target for SYN flooding attacks with the malicious motive of exhausting the controller's resource, exhaust control plane bandwidth. This attack is based on exploiting the TCP 3-way handshake mechanism by sending a large number of TCP connections that are half open thus preventing the completion of the 3-way handshake. The earlier techniques that were used to prevent these attacks were based on static thresholds which are set by users to analyze data and generate results when a violation occurs at specific intervals. So, the authors in this paper have proposed an IDPS solution called SYNGuard which dynamically calculates and updates the thresholds to seize the SYN flooding attacks. They have also mentioned that their proposed method outperforms existing IDPS solutions such as Zeek and Snort with respect to consumption of resources, response time, and accuracy [10].

The use of SDNs in networks that have limitations such as Wireless Sensor Networks (WSN) is very scarce as a result of certain factors such as excessive pressure on control plane and lossy medium. WSN contain sensors that have resource constraints. These sensors are used to monitor the conditions in a particular environment. The use of SDN in wireless sensor networks led to the rise of a new field called SD-WSNs, Software-defined Wireless Sensor Networks. Flow management in SDN is very flexible and less complex. So, the functions of control plane such as Load balancing, Quality-of-Service (QoS) are performed by the SDN controller while the actual forwarding of packets is done by the individual nodes. The entire network is partitioned into clusters containing minimal border nodes. The SDN controller performs the traffic flow between clusters while the flow within the clusters is done by the WSN routing algorithm. By performing clustering, the communication cost for flow configuration is reduced with no effect on packet delivery rate [11].

One of the major hurdles in a 5G network is the increasing number of mobile users and the resultant increase in network traffic. Therefore, the 5G network is less flexible and scalable. To combat this, a 5G architecture based on SDN could be the solution to the above-mentioned networks. By using the SDN controller the data plane can be programmed using OpenFlow. The authors in this paper have implemented their proposed architecture in a network simulator and found that their architecture performs better than traditional 5G architectures [12].

Introducing new network services into the architecture of the internet is a very costly business. Hence the solution is to use network virtualization. Embedding these virtual networks into the actual physical network infrastructure is still an area that researchers are trying to understand. The main problem with Virtual network embedding is efficiently mapping the request from the virtual network to the substrate resources. So VNE algorithms may be enacted in a centralized or distributed manner to solve this problem. In centralized method, a single entity receives all the requests from the virtual networks. But this requires current information about the substrate network. This is the problem with the centralized approach. Hence in distributed approach multiple entities receive requests from multiple virtual networks. Therefore, by using a distributed VNE called DVSDNE using multi-agent systems the load can be distributed across physical substrate network [13].

IOT devices are growing at a rapid pace and efficient management of these devices is a huge concern. This paper deals with the integration of SDN and blockchain technology to ensure secure communication as well as secure network infrastructures. Blockchain is used to store digital transaction data and distributes them across the network and does not allow any editing by third parties. So, a SDN-Blockchain framework can be implemented in an IOT ecosystem in order to mitigate constraints such as end-to-end delay and energy utilization. Blockchain allows for decentralization and eliminates the risk of single point failures. Blockchain with SDNs allows for information-based transactions between network devices [14].

One of the issues with 5G is due to the increasing traffic, management of the network has become complex in nature. Thus, with the introduction of SDN combined with Network Function Virtualization (NFV), this complexity of the network can be reduced and resource sharing can be done more efficiently. With SDN, the network control functions can be isolated from the devices that operate in the data layer, thus allowing for automation of management of 5G networks. Network Function Virtualization allows for the use of virtualization of network components such as firewalls, traffic control, etc. and running them as software on virtual machines rather than running them on hardware. In multi-control SDN architecture, placing the controller, quantity of controllers, and assignment of functions to the switches is major challenge and is known as the Controller Placement Problem (CPP). These three parameters need to be effectively managed to obtain an efficient control plane. Thus, the authors in this paper have proposed a heuristic approach to determine the allocation of controllers in SDN/NFV architecture. By using their proposed framework, the authors were able to achieve high resource assignment efficiency [15].

Smart cities aim to promote sustainable development while improving the quality of life of its citizens. Smart cities rely on a vast network of sensors to collect data in real time to make intelligent decisions. Secure transmission of this vast amount of data is extremely critical to smart cities. Here is where SDNs come into play and can provide a secure communication infrastructure. SDN characteristics such as centralized control plane, virtualization and programmability make them appealing to smart cities. The programmability characteristics of SDN can prove to be cost-effective as well as dynamic in the configuration of the networks in smart cities. SDN can also greatly improve the security of a network infrastructure due to its centralized control plane making the enforcement of security policies much easier. This benefit however is not obtained in a distributed control plane architecture. SDN makes the implementation of security policies as well as applications much easier as they allow for attachment of security modules onto the controllers without having to update the firmware or change the hardware. However, with the adoption of SDN, it opens the door to new threats such as DDoS, Man-in-the-middle attacks (MITM), Link Discovery Service (LDS). SDNs also only consider some parts of the entire network

infrastructure, therefore in the future, hybrid SDNs would gain more attention [16].

Moving target defense is a mechanism which is used to confuse an attacker who is trying to attack a network. The aim is to confuse the person trying to compromise a network by changing the surface of the network such as system or network configurations. So, the attacker obtains false information about a network. Using this in combination with SDN technology, shuffling of network configuration such IP, MAC address, port number is done. Attackers usually use this information to enter and perform attacks on network. By using MTD in conjunction with SDN secure networks can be created [17].

As people become increasingly dependent on technology, attackers exploit this dependency on technology by launching ransomware attacks on them which denies them access to their own networks and granting restoration in return for ransom. BadRabbit is one such ransomware attack that is launched on networks. WannaCry, Petya are some of the most common ransomwares. Solutions based on SDN have been provided by studying the impact of these types of ransomwares on traditional networks. However, BadRabbit is still an active area of study. The authors of this paper have enacted an IDPS system based on SDN to detect and prevent ransomwares such as BadRabbit. The authors in this paper have enacted deep packet inspection, ARP scanning, inspection of the header of packets to block SMB access as well as honey pots to detect attack attempts. SMB is a communication protocol used by the nodes in a network to gain access to shared files [18].

As an increasing number of devices are being connected in an IOT ecosystem, the demand for QoS is also increasing. The proposed method in this paper exploits the flexibility and flow-based nature of SDNs to improve the QoS of every flow in the network. By implementing QoS routing strategies such as delay-sensitive and loss-sensitive to deal with the delay and loss type flows in network, the end-to-end delay as well as the QoS of the network can be vastly improved [19].

This article deals with security of SDN. There are certain vulnerabilities in the SDN architecture that attackers can exploit. In the layer 7 a variety of applications run with a variety of protocols. The network administrator must have knowledge about the types of communication protocol that are running in the 7^{th} layer. Here is where application-aware firewalls come into play which can allow certain types of traffic to pass while blocking traffic that is a known vulnerability. So, the authors in this paper propose running an application-aware firewall on top of the SDN controller to filter out unwanted traffic. This may however hinder the performance of the network at times. All the security policies are contained in the controller while the application-aware firewall inspects the traffic and enforces the policies contained in the controller [20].

Energy concern is a key concern when it comes to networking. In SDN networks, the controller handles the decision-making process. The controller communicates its decisions to the data layer devices using a protocol called OpenFlow. Ambience aware routing protocol which routes data through the best possible path to arrive at the destination with no delay can be used to minimize energy consumption [21].

Network Function Virtualization can revolutionize the telecommunication industry. It basically separates the network functions from the actual hardware. This can really bring down operating as well as capital expenditure. By using Network Function Virtualization for example, a firewall can be sent to a Telecommunication service provider as a software. One major challenge with the scalability of NFV is standardization [22].

There are two key issues with the current networking scenario. One is the dynamic nature of the network as it is changing rapidly. The other is difficulty in configuration of devices at the lower

levels. Network administrators as a result find it difficult to enforce policies at the higher level. Procera is a framework based on SDN which can be used to implement reactive network rules[23].

ONOS stands for Open Network Operating System. ONOS is an open-source project based on the SDN platform that can be used to create network services across a variety of Hardwares. Some applications that have been tried out on ONOS are: BGP interfacing and route maintenance. It is still a prototype. ONOS provides Abstraction, Isolation, as well as security. ONOS being open source, it can be analyzed as well as improved by the Open-source community [24].

3. Bibliometric survey for Software-Defined Networking

Bibliometric analysis is done to analyze the research published that is published in various formats. This helps us to understand the amount of impact that the publications have on a global scale [25]. The bibliometric analysis was done on the Scopus database. The goal of this bibliometric study is to comprehend the volume of research and trends in the area of Software-Defined Networking. We hope this paper would give researchers an idea of the trends and challenges in this area and bridge the gaps in the existing literature. The time frame chosen for this bibliometric survey is 2016-2021.

Choosing the right keywords is critical as it helps us narrow down the area of focus. So, this is done by using basic Boolean logic such as “AND” & “OR”. This helps us in refining our search. The key words chosen for this survey are: “Software Defined Networking” AND “OpenFlow” AND “Security” OR “Cloud” OR “Challenges”.

Table 2: Top 10 keywords and their corresponding NOP

Top 10 keywords	Number of Publications
Software Defined Networking	523
Software Defined Networking (SDN)	379
Openflow	359
OpenFlow	331
Network Security	292
SDN	217
Network Architecture	180
Controllers	171
Denial-of-service Attack	131
Network Function Virtualization	89

Table 2 shows the top 10 keywords that were used in research related to Software-Defined Networking and their corresponding number of Publications. It can be observed from the above table that “Software Defined Networking” is the most used keyword and has been used in over 523 publications. Also keywords like “Openflow”, “Network Security”, “controllers”, “Denial-of service Attack” indicate the tends of research in SDN. So, researchers are interested in learning and contributing to how the controller configurations can affect the performance of SDN, how to improve the network architecture and the security of SDN. These are some fields that can be explored and solve the challenges that they may face.

Table 3: Number of publications according to Publication languages

Publication Languages	NoP	Publication Languages	NoP
English	736	Japanese	1
Chinese	19	Spanish	1
Portuguese	2	Turkish	1

It can be seen from the table 3 that English is the language in which most of the publications have been done, followed by Chinese, and the other languages.

Table 4: Publication type

Publication type	NoP
Conference	476
Article	241
Review	27
Book Chapter	12
Conference review	2
Short survey	1
Undefined	1

Table 4 shows the different publications such as Conference, Article, Review, Book Chapter, Conference Review, and short survey. The number of publications made in article form is the highest comprising of around 62.63% of the documents published. The next highest number of publications was made in article form comprising of 31.7% of the documents published. 27 review papers, 12 book chapters, and 1 short survey were also published. One document remains undefined.

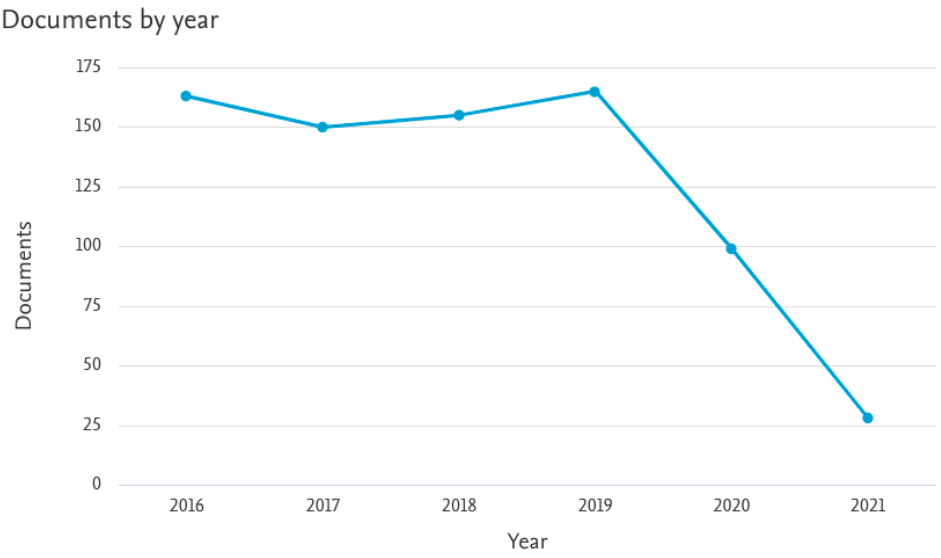

Figure 1: Documents published year-wise

Figure. 1 shows us the papers that were published year wise from 2016 to 2021. From the graph we observe that in the year 2016, 162 publications were made. In the following years, the number of published documents was around the same range with the highest being in 2019 with 165 documents. However, since then till present day there has been a huge dip in publications due to the pandemic.

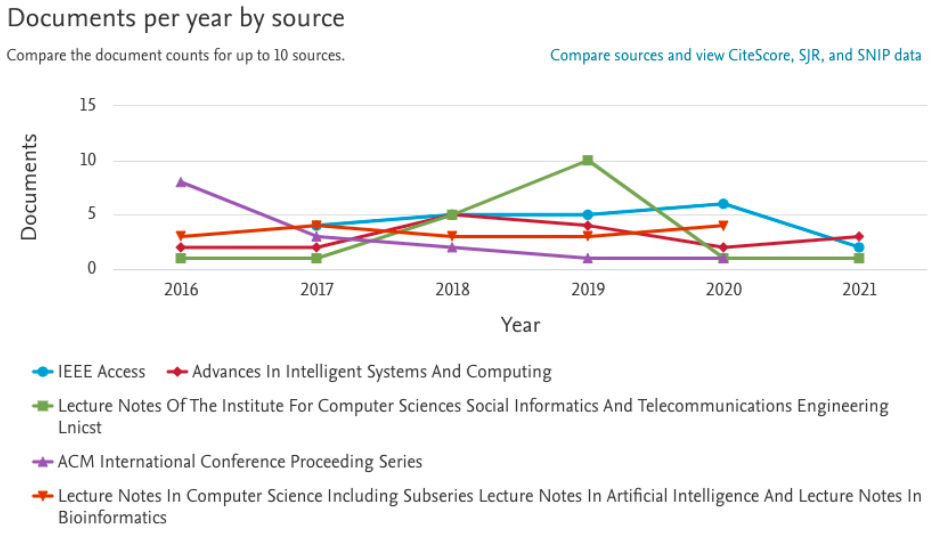

Figure 2: Documents per year by source

Based on the key words that we have chosen, the journals mentioned in Figure 2 are the ones that researchers are publishing to. We had chosen the following keywords, Software Defined Networking" AND "OpenFlow" AND "Security" OR "Cloud" OR "Challenges". It can be observed that researchers have been publishing to all journals at a steady rate every year. Due to the pandemic, there was a sudden halt in 2020, but the rate of publishing is slowly picking up.

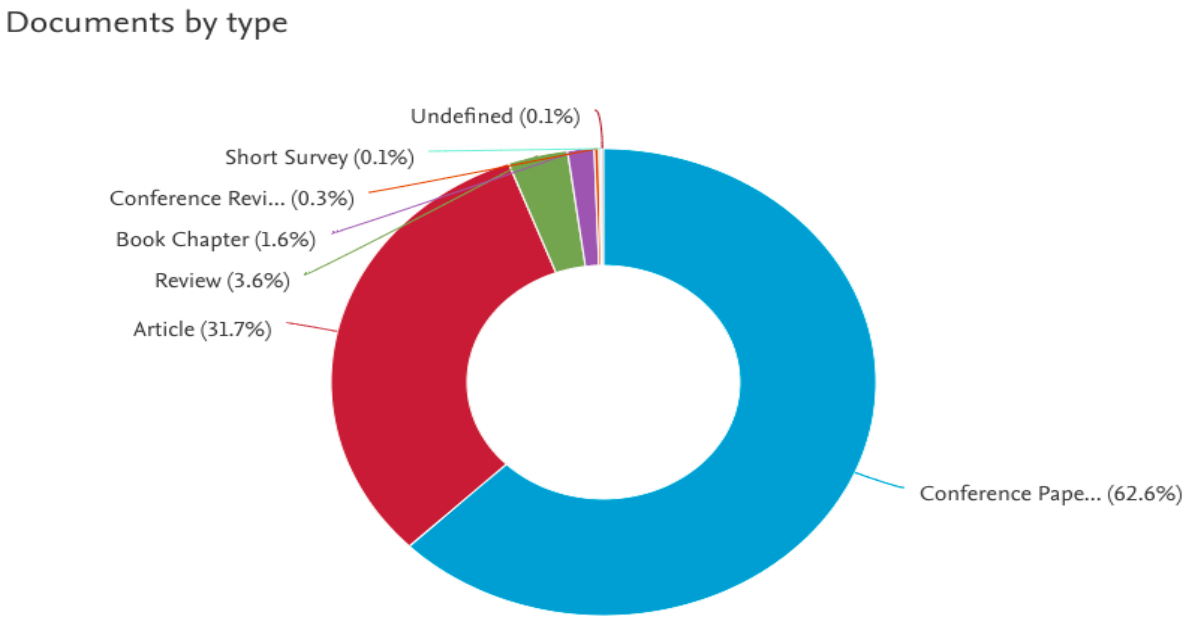

Figure 3: Distribution of documents by type

Figure. 3 shows us how the documents are distributed according to their type. Out of all the documents published, conference papers account for 62.6% of the documents published followed by Articles at 31.7%. The number of review papers published is 3.6%. Publication of review papers is essential as the amount of conference papers and articles published are huge. So, review papers can consolidate the data in these documents and give the readers a detailed summary of the current trends in Software defined networking.

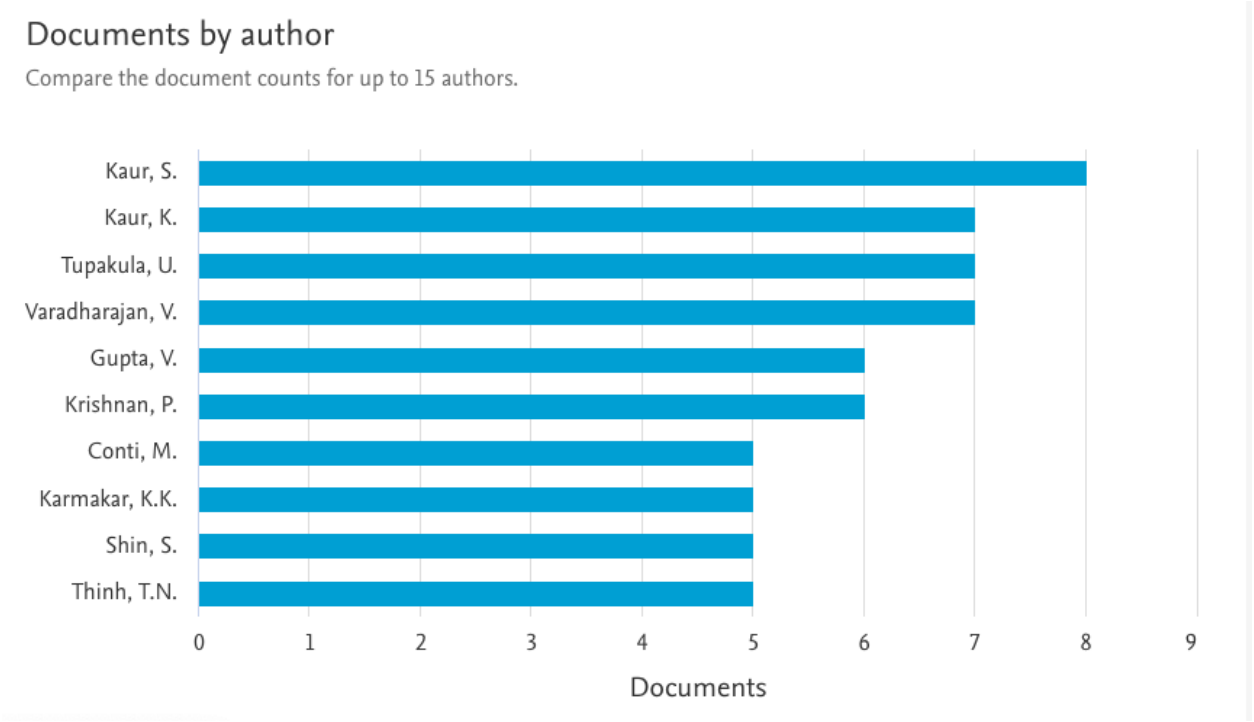

Figure 4: Documents by author

Figure 4 shows the number of publications made by the top 10 authors. Kaur, S. is stands out as the author with the greatest number of publications with 8 documents published. Authors with many publications generally tend to be technically inclined in the area of research and following their work can help us gain more insights.

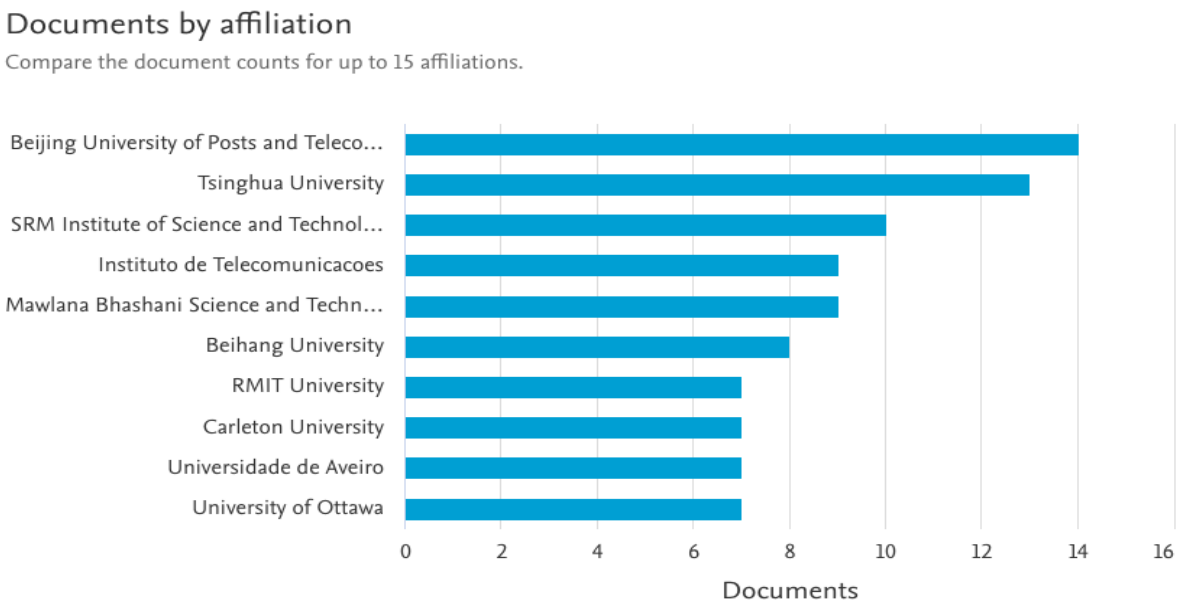

Figure 5: Documents by affiliation

Authors that publish papers may be affiliated to different Universities. Figure 5 shows the bar chart of number of documents published in relation with the top 10 affiliated Universities. It can

be observed that 14 publications were affiliated to Beijing University of Posts and Telecommunications which is the highest.

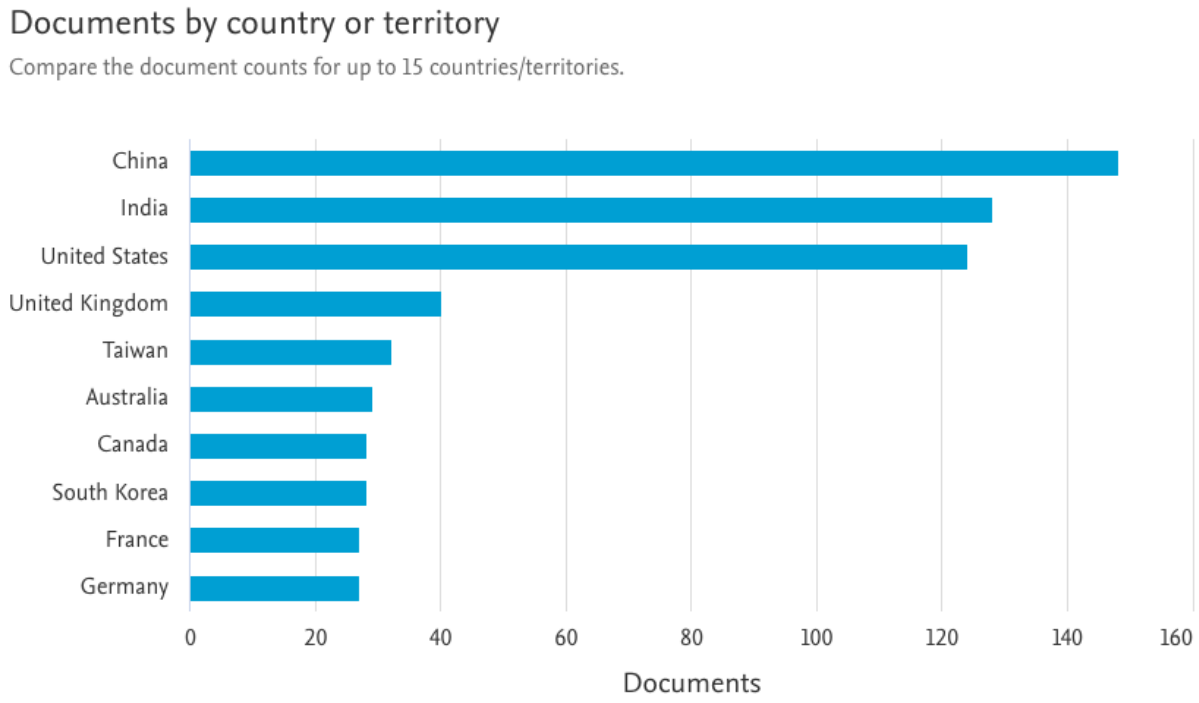

Figure. 6 Publication of documents Country-wise

Figure 6 shows us the bar chart of the documents published Country-wise. It can be observed that China stands out with the most number of publications at 148 documents published to the Scopus journals followed by India, the United States, and the United Kingdom.

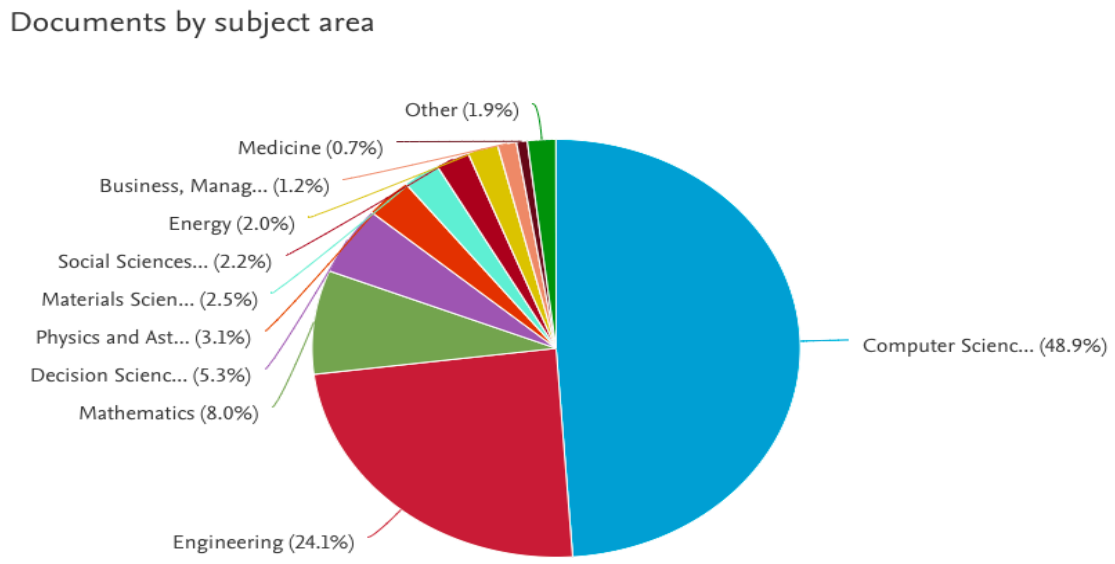

Figure. 7 Pie chart of Distribution of documents by subject area

From Figure 7 shown above, the subject area when it comes to Software Defined Networking is concentrated in computer science. Various techniques related to computer science such as machine learning and deep learning can be applied to SDNs to develop more robust SDN architectures. The other subject areas that the documents were concentrated towards are Engineering and Mathematics.

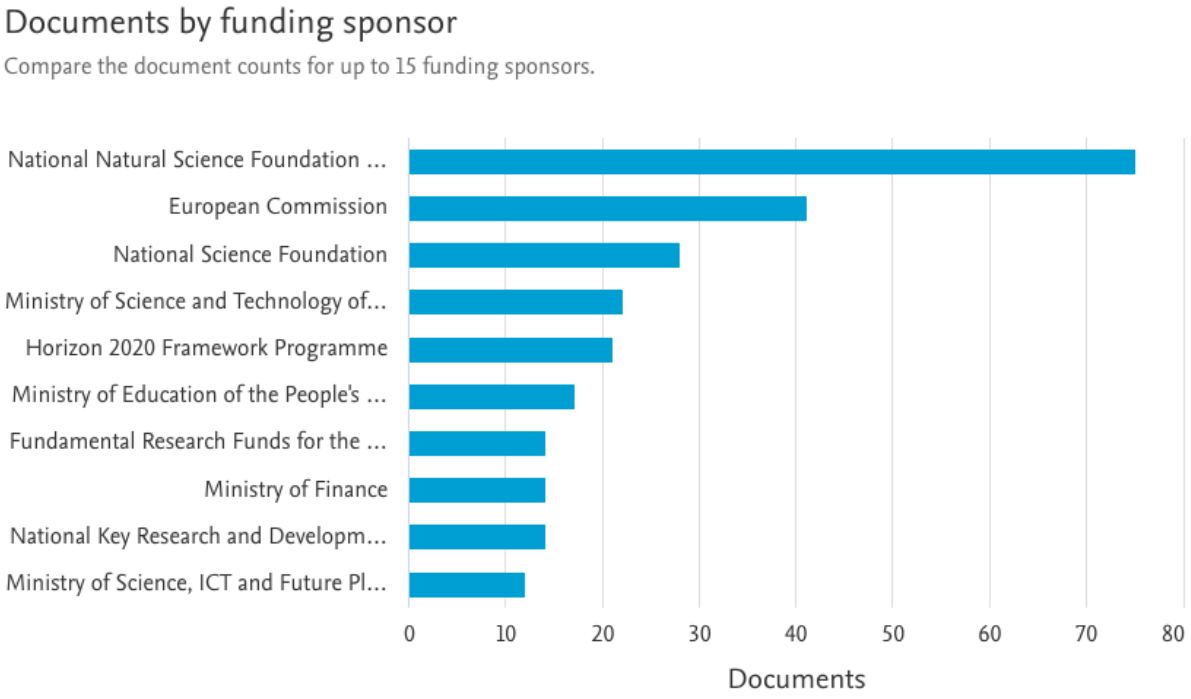

Figure 8: Documents distribution with respect to funding sponsor

Research documents are funded by different funding sponsors. Figure 8 depicts the top 10 funding agencies that are actively sponsoring for research related to Software-Defined Networking. A. National Natural Science Foundation of China is the funding agency with the most number of publications with 75 documents in Scopus. This could also be the reason for China being the country with most number of publications.

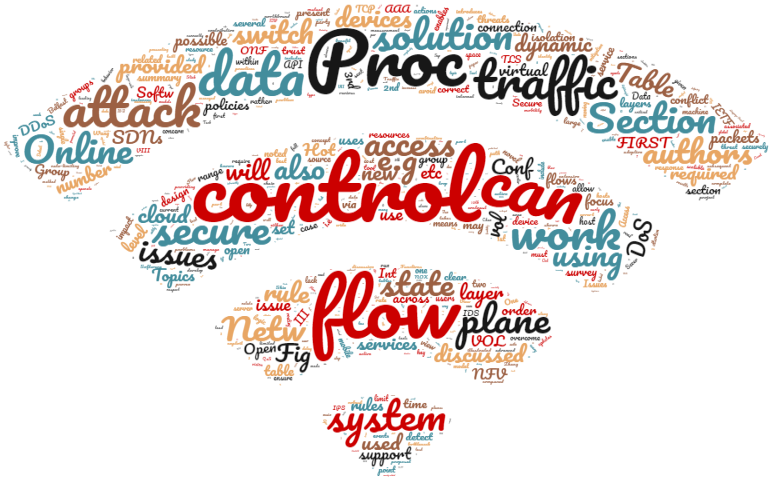

Figure 9: Popular keywords used in research

Figure 9 shows the most used keywords by authors when doing research in Software-Defined-Networking. The above image was generated by "Word Cloud", which is a software used to represent the most used words in a document in a picture as shown above. We obtain the most-cited document related to Software-Defined Networking. We then upload that paper into the software which parses the document and gives us a pictorial representation of the frequently used words. We can observe that flow, control, attack, online, traffic are some of the hottest keywords in the area of Software-Defined Networking.

Table 5: Citations of the publications for Software-Defined Networking

Year	<2017	2017	2018	2019	2020	2021	Subtotal	>2021	Total
No: of Citations	44	452	952	1775	2048	871	6098	0	6142

Table 6: Table of citations for top 10 publications in Scopus for Software-Defined Networking

Serial number	**Title of Publication**	**Annual Citations**								
		<2017	**2017**	**2018**	**2019**	**2020**	**2021**	**Subtotal**	**>2021**	**Total**
1	A survey of security in software defined networks	9	48	60	68	56	14	246	0	255
2	A survey: Control plane scalability issues and approaches in Software-Defined Networking (SDN)	0	4	35	47	55	18	159	0	159
3	Software Defined Networking Architecture, Security and Energy Efficiency: A Survey	0	15	40	52	41	11	159	0	159
4	Quality of Service (QoS) in Software Defined Networking (SDN): A survey	0	8	21	45	54	24	152	0	152
5	DDoS Attack Detection and Mitigation Using SDN: Methods, Practices, and Solutions	0	1	18	45	39	11	114	0	114
6	Software defined networks: A survey	3	18	22	20	27	16	103	0	106
7	A survey on OpenFlow-based Software Defined	0	10	23	25	20	15	93	0	93

	Networks: Security challenges and countermeasures									
8	SD-Anti-DDoS: Fast and efficient DDoS defense in software-defined networks	0	7	25	22	28	10	92	0	92
9	Software-defined networking (SDN): a survey	0	1	7	30	37	16	91	0	91
10	A Survey on the Security of Stateful SDN Data Planes	0	1	22	30	23	10	86	0	86

Table 5 shows the total citations that the Scopus based publications have received on a yearly basis. We can observe that the total number of citations in 2017 was just 44. It has been steadily increasing and touched an all-time high of 2048 citations in the year 2020 followed by a huge dip in 2021. Table 6 gives the number of citations that the top 10 most-cited papers in the Scopus database have received on a yearly basis as well as the total number of citations. It can be seen that "A survey of security in software defined networks" is the document with the greatest number of citations with up to 255 citations. By referring the top 10 cited papers we can understand how the trend is moving towards in our area of research.

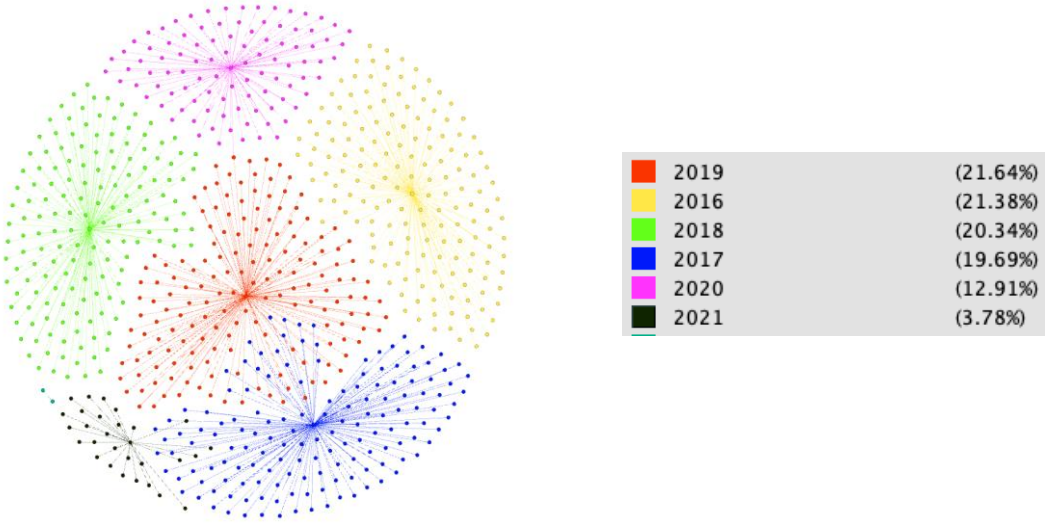

Figure 10: Cluster of Publication year and Paper title

Figure 10 shows the relationship between the year of publication and the Title of Publication in the form of clusters. The different colors in the cluster stand for the different years and each cluster has a node which connects to the different papers published during that year. This was visualized using an open-source software known as Gephi. This software basically takes an excel file consisting of the various values and presents a visual representation of the data. The Fruchterman Reingold layout was used to visualize the data. It can be seen that 2019 has the highest number of connections which means that it was the year with the highest number of publications. The cluster of 2021 is very small indicating a smaller number of published documents.

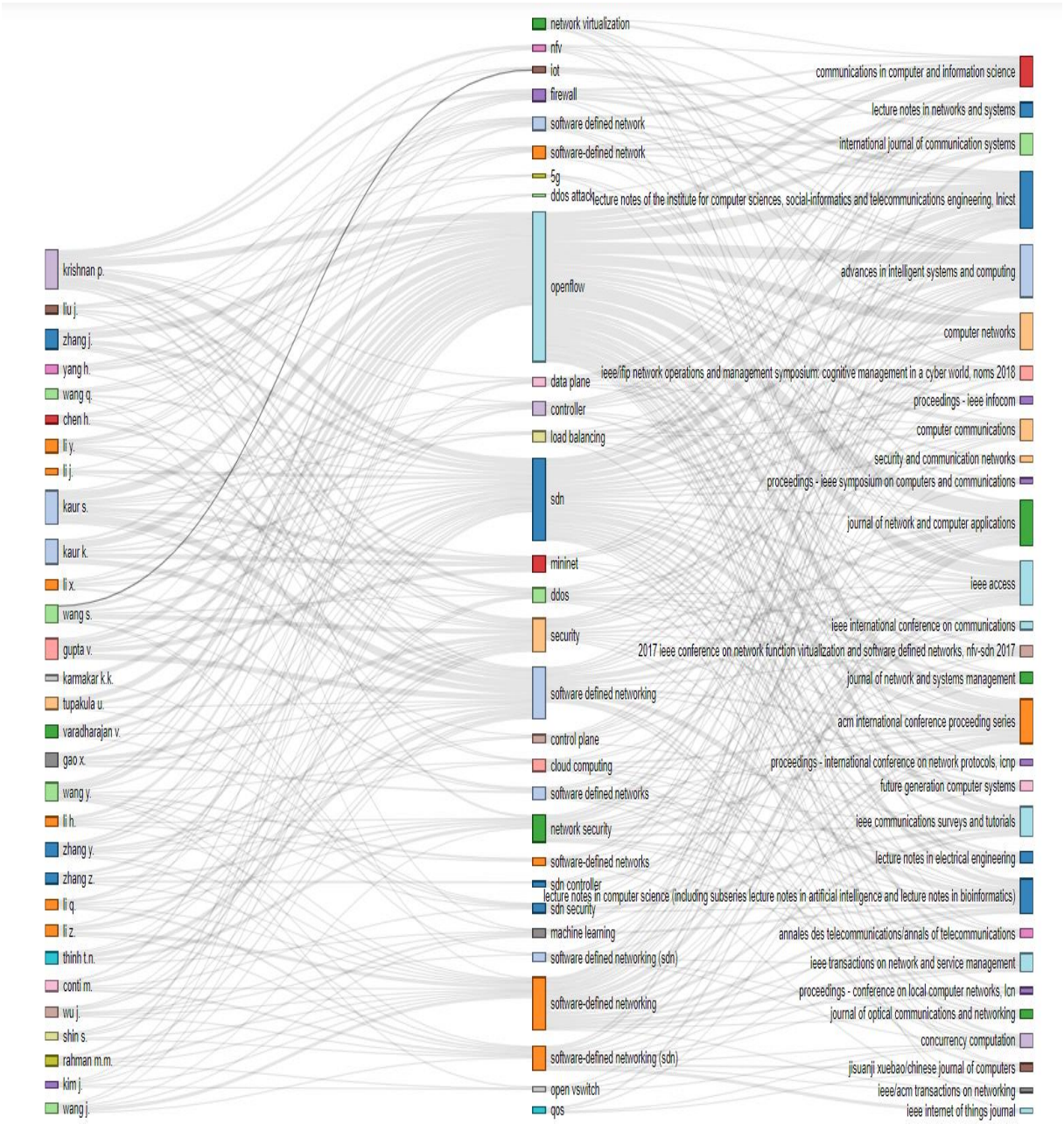

Figure 11: A-K-J Sankey graph

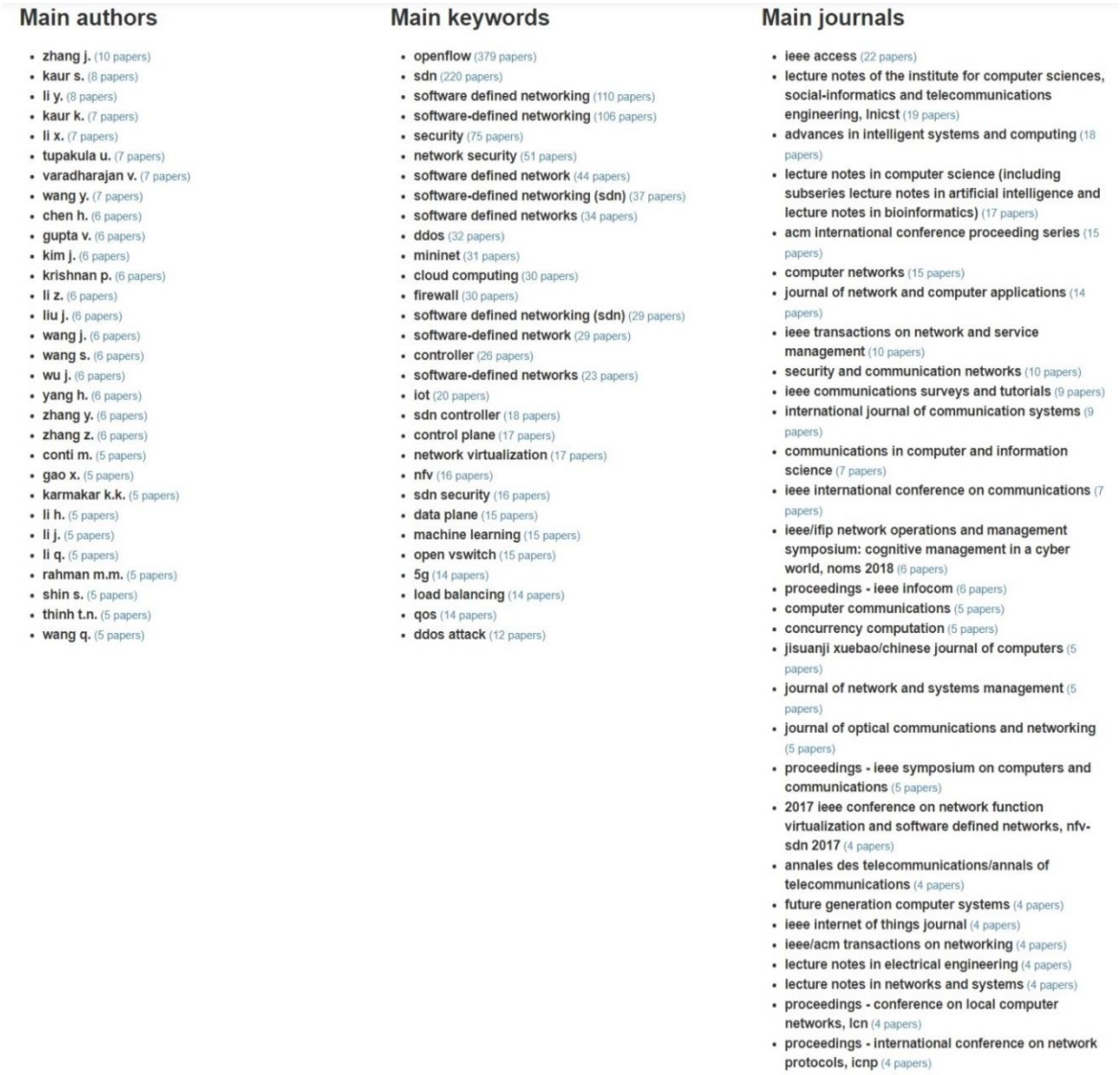

Figure 12: Relationship between authors, keywords, and journals

Figure 11 shown above is a graph showing the relationship among the authors, the keywords they use, and the journals they publish to. The graph is known is an A-K-J Sankey graph. The scope of this graph is limited to the data obtained from the Scopus database from the year 2016 to 2021. The first column of figure 11 shows the authors who have a considerable amount of influence in the number of publications. The middle column depicts the significant keywords that they have used. The final column shows the names of the journals to which the authors who use the various keywords mentioned in the second column publish to. The whole graph is an interconnection of the data in these three columns, so it is helpful for viewers to track the main authors, the keywords they use, and the journals they publish to. Figure 12 shows the same information shown in the Sankey graph in tabular form. So, it is helpful to have this table and the graph side by side when doing the analysis. It can be inferred from the graph that “OpenFlow “, is the keyword that most of the authors have used and published over 379 papers to various journals.

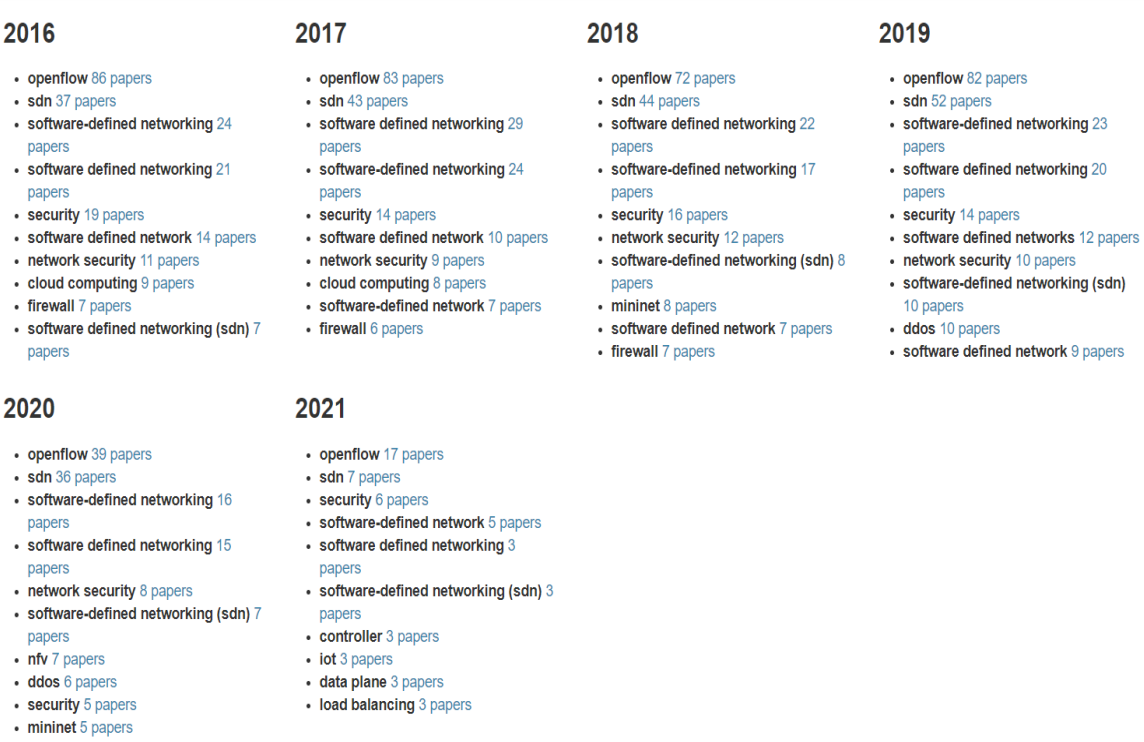

Figure 13: Top keywords used year-wise

Figure 13 shows the top keywords that authors have used year-wise. It can be observed that all authors in the last 6 years including the present year have shown interest in the keyword “OpenFlow”.

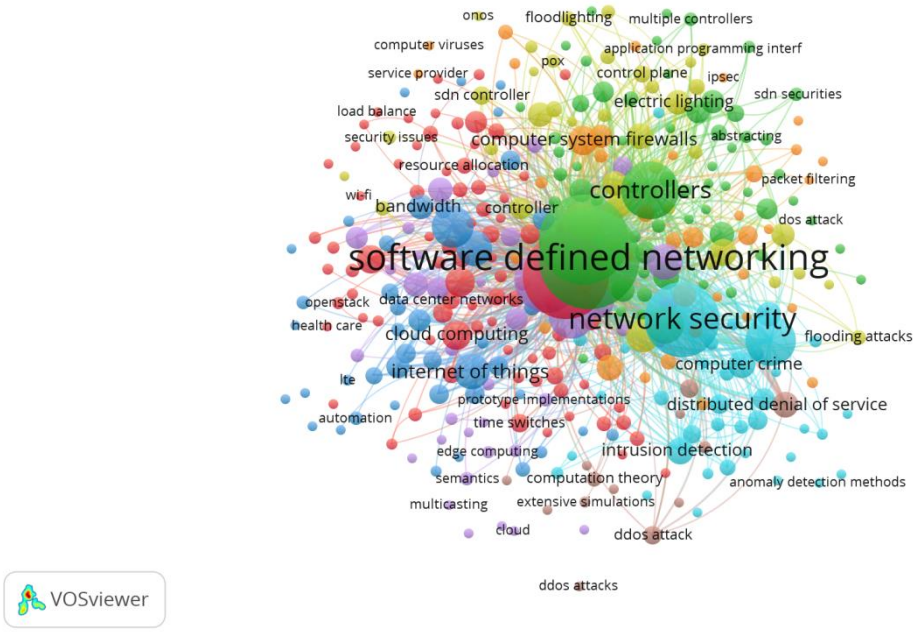

Figure 14: Clusters of keywords that co-occur in Scopus Publications

Figure 14 shown above shows the clusters of keywords that co-occur in Scopus publications that we have considered. The biggest clusters from the above image are “Software defined networking”, “Network security”, and “Controller”. These are the main keywords that are employed in research related to Software-Define Networking.

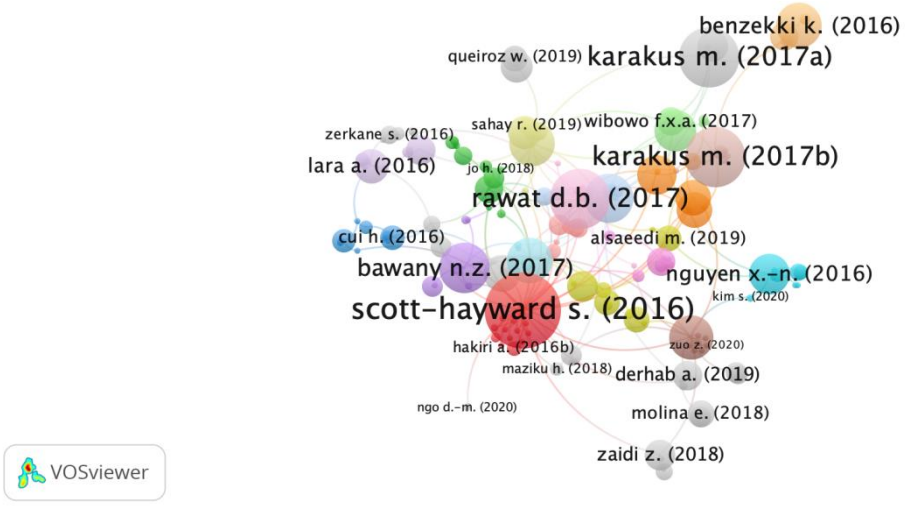

Figure 15: Cluster of citations in documents in Scopus publications

Figure 15 shows the clusters of the citations of the documents that were obtained from the Scopus publications. Scott-haward et al, in 2016 published “A survey of security in software defined networks” was cited a total of 255 times by other publishers. Thus, this graph shows how the different documents are connected with respect to citations.

4. Discussions

In this paper, we have seen the different trends in SDN as well as some of the challenges it poses. Some of the key concerns regarding SDN are Security, Scalability, and migration to SDN. The SDN architecture, with its decoupled control plane opens new challenges such as Scalability reliability, and interoperability. The controller can handle only a limited number of requests at any given time. They are expected to process flows in the rate of millions without compromising the quality of service. Scalability can be improved by reducing overhead on control plane by delegating some functions to the data plane. Another way is to increase the output of the control plane itself. In case of making the data plane more scalable, Devoflow [26]and SDCs [27] can be used. By implementing the above-mentioned methods, overhead on control plane can be reduced as well as the ability of the control plane to process flows can also be increased, thereby improving the scalability factor. In order to make the control plane more scalable, controllers such as Beacon [28] and Kandoo [29] can be used to improve controller performance. To improve scalability, implementing different architectures such as distributed, hierarchical architectures can help prevent controller bottlenecks. The controller is vulnerable as it is equivalent to putting all the eggs in one basket. Hence efficiently using the controller’s resources is crucial to maintain network reliability. In SDN’s, separating the controller plane from the data plane opens doors to security issues such as MITM, DDoS attacks, etc. Some attacks are possible due to the inherent architecture of SDN such as attacks on the centralized controller. A compromised controller leads to a compromised network. Other attacks that are common on SDNs are DDoS [29] and spoofing attacks [29]. Packet dropping can be done based on thresholding such as rule based or load on system, thus detecting DDoS attacks. Implementing trust management between controllers and the forwarding devices ensures that no attack goes undetected [31]. Encryption of data with SSL certificates can be done to provide secure transmission between the data plane and the control

plane. Brute force attacks on SDNs can be avoided by using stronger passwords, time-bound logins, captcha, TFA, and so on. Now here comes the major hurdle when it comes to implementation, transitioning the legacy networks present today to SDN. People may also refuse to migrate to SDNs fearing job security. Using controllers such as OpenDaylight [32] and OpenContrail [33], legacy networks can be interfaced with SDN. ClosedFlow is an SDN like controller that can be used with legacy networks [34]. Hence backward compatibility must be ensured in SDNs to support legacy networks as well.

5. Conclusion

Traditional networks that are in use today are not able to keep up with the rapid development of business applications. A variety of trends has emerged in the past few decades such as IOT, Cloud computing, Virtualization and so on. Traditional networks are not that flexible to support these modern technologies. SDNs with their separation of the two planes can provide this flexibility while reducing costs, boosting productivity, and handling network resources generously. In the future SDNs can be implemented in a variety of network scenarios. Even though SDN is software oriented, the hardware required to run it cannot be ignored. So, both hardware and software portion of SDNs will evolve to support a multitude of applications. SD-WANs is also something that the future holds, where the SDNs can be used to connect multiple LANs. Even though there are a few challenges like Security, scalability, controller problems and so on, SDN has an enormous potential in the upcoming years.

References

[1] T. Benson, A. Akella, and D. Maltz, “Unraveling the complexity of network management,” in Proceedings of the 6th USENIX Symposium on Networked Systems Design and Implementation, ser. NSDI’09, Berkeley, CA, USA, 2009, pp. 335–348.

[2] H. Kim and N. Feamster, “Improving network management with soft-ware defined networking,” Communications Magazine, IEEE, vol. 51,no. 2, pp. 114–119, 2013.

[3] N. Handigol, S. Seetharaman, M. Flajslik, N. McKeown, and R. Johari, ‘‘Plug-n-serve: Load-balancing web traffic using OpenFlow,’’ 2009.

[4] A. Gudipati, D. Perry, L. E. Li, and S. Katti, “SoftRAN,” presented at the the second ACM SIGCOMM workshop, 2013, doi: 10.1145/2491185.2491207.

[5] M. Casado, T. Garfinkel, A. Akella, M. J. Freedman, D. Boneh,N. McKeown, and S. Shenker, “SANE: a protection architecture for enterprise networks,” in Proceedings of the 15th conference on USENIX Security Symposium - Volume 15, ser. USENIX-SS’06, Berkeley, CA,USA, 2006.

[6] D. Kreutz, F. M. V. Ramos, P. E. Veríssimo, C. E. Rothenberg, S. Azodolmolky and S. Uhlig, "Software-Defined Networking: A Comprehensive Survey," in *Proceedings of the IEEE*, vol. 103, no. 1, pp. 14-76, Jan. 2015, doi: 10.1109/JPROC.2014.2371999.

[7] S. Khorsandroo, A. G. Sánchez, A. S. Tosun, J. Arco, and R. Doriguzzi-Corin, “Hybrid SDN evolution: A comprehensive survey of the state-of-the-art,” Computer Networks, vol. 192, p. 107981, Jun. 2021, doi: 10.1016/j.comnet.2021.107981.

[8] O. J. Ibrahim and W. S. Bhaya, “Intrusion Detection System for Cloud Based Software-Defined Networks,” J. Phys.: Conf. Ser., vol. 1804, no. 1, p. 012007, Feb. 2021, doi: 10.1088/1742-6596/1804/1/012007.

[9] M. R. Çelenlioğlu and H. A. Mantar, “Energy aware adaptive resource management model for software-defined networking-based service provider networks,” IET Networks, vol. 10, no. 2, pp. 88–100, Jan. 2021, doi: 10.1049/ntw2.12006.

[10] M. Rahouti, K. Xiong, N. Ghani, and F. Shaikh, “SYNGuard: Dynamic threshold-based SYN flood attack detection and mitigation in software-defined networks,” IET Networks, vol. 10, no. 2, pp. 76–87, Jan. 2021, doi: 10.1049/ntw2.12009.

[11] Q. Liu et al., “Cluster-based flow control in hybrid software-defined wireless sensor networks,” Computer Networks, vol. 187, p. 107788, Mar. 2021, doi: 10.1016/j.comnet.2020.107788.
[12] A. Abdulghaffar, A. Mahmoud, M. Abu-Amara, and T. Sheltami, “Modeling and Evaluation of Software Defined Networking Based 5G Core Network Architecture,” IEEE Access, vol. 9, pp. 10179–10198, 2021, doi: 10.1109/access.2021.3049945.
[13] A. A. Nasiri, F. Derakhshan, and S. S. Heydari, “Distributed Virtual Network Embedding for Software-Defined Networks Using Multiagent Systems,” IEEE Access, vol. 9, pp. 12027–12043, 2021, doi: 10.1109/access.2021.3050922.
[14] A. Rahman *et al*., "SmartBlock-SDN: An Optimized Blockchain-SDN Framework for Resource Management in IoT," in *IEEE Access*, vol. 9, pp. 28361-28376, 2021, doi: 10.1109/ACCESS.2021.3058244.
[15] A. A. Z. Ibrahim, F. Hashim, N. K. Noordin, A. Sali, K. Navaie and S. M. E. Fadul, "Heuristic Resource Allocation Algorithm for Controller Placement in Multi-Control 5G Based on SDN/NFV Architecture," in *IEEE Access*, vol. 9, pp. 2602-2617, 2021, doi: 10.1109/ACCESS.2020.3047210.
[16] M. Rahouti, K. Xiong and Y. Xin, "Secure Software-Defined Networking Communication Systems for Smart Cities: Current Status, Challenges, and Trends," in *IEEE Access*, vol. 9, pp. 12083-12113, 2021, doi: 10.1109/ACCESS.2020.3047996.
[17] S. Yoon, J. -H. Cho, D. S. Kim, T. J. Moore, F. Free-Nelson and H. Lim, "Attack Graph-Based Moving Target Defense in Software-Defined Networks," in *IEEE Transactions on Network and Service Management*, vol. 17, no. 3, pp. 1653-1668, Sept. 2020, doi: 10.1109/TNSM.2020.2987085.
[18] F. M. Alotaibi and V. G. Vassilakis, "SDN-Based Detection of Self-Propagating Ransomware: The Case of BadRabbit," in *IEEE Access*, vol. 9, pp. 28039-28058, 2021, doi: 10.1109/ACCESS.2021.3058897.
[19] N. Saha, S. BERA and S. Misra, "Sway: Traffic-Aware QoS Routing in Software-Defined IoT," in IEEE Transactions on Emerging Topics in Computing, vol. 9, no. 1, pp. 390-401, 1 Jan.-March 2021, doi: 10.1109/TETC.2018.2847296.
[20] Nife, F. N. and Kotulski, Z. (2020) “Application-aware firewall mechanism for software Defined networks,” *Journal of network and systems management*, 28(3), pp. 605–626.
[21] H. B. Valiveti, S. Ganesh, B. A. Kumar and D. K. Yadav, "Energy efficient ambience awake routing with openflow approach," *Computers, Materials & Continua*, vol. 67, no.2, pp. 2049–2059, 2021.
[22] R. Mijumbi, J. Serrat, J. Gorricho, N. Bouten, F. De Turck and R. Boutaba, "Network Function Virtualization: State-of-the-Art and Research Challenges," in IEEE Communications Surveys & Tutorials, vol. 18, no. 1, pp. 236-262, Firstquarter 2016, doi: 10.1109/COMST.2015.2477041.
[23] H. Kim and N. Feamster, "Improving network management with software defined networking," in IEEE Communications Magazine, vol. 51, no. 2, pp. 114-119, February 2013, doi: 10.1109/MCOM.2013.6461195.
[24] P. Berde et al., “ONOS,” presented at the SIGCOMM’14: ACM SIGCOMM 2014 Conference, Aug. 2014, doi: 10.1145/2620728.2620744.
[25] Shivali. A. Wagle and R. Harikrishnan, DigitalCommons @ University of Nebraska - Lincoln “A Bibliometric Analysis of Plant Disease Classification with Artificial Intelligence,” pp. 1–12, 2021.
[26] A. R. Curtis, J. C. Mogul, J. Tourrilhes, P. Yalagandula, P. Sharma, and S. Banerjee, “DevoFlow,” presented at the the ACM SIGCOMM 2011 conference, 2011, doi: 10.1145/2018436.2018466.
[27] J. C. Mogul and P. Congdon, “Hey, you darned counters!,” presented at the the first workshop, 2012, doi: 10.1145/2342441.2342447.
[28] D. Erickson, ‘‘The Beacon OpenFlow controller,’’ in Proc. 2nd ACM SIGCOMM Workshop Hot Topics Softw. Defined Netw., 2013, pp. 13–18.
[29] S. Hassas Yeganeh and Y. Ganjali, ‘‘Kandoo: A framework for efficient and scalable offloading of control applications,’’ in Proc. 1st Workshop Hot Topics Softw. Defined Netw., 2012, pp. 19–24.

[30] R. Kloti, ‘‘OpenFlow: A security analysis,’’ M.S. thesis, Dept. Inf. Tech. Elec. Eng., Swiss Fed. Inst. Technol. Zurich (ETH), Zurich, Switzerland, 2013.
[31] D. Kreutz, F. M. Ramos, and P. Verissimo, ‘‘Towards secure and dependable software-defined networks,’’ in Proc. 2nd ACM SIGCOMM Workshop Hot Topics Softw. Defined Netw., 2013, pp. 55–60.
[32] OpenDaylight, A Linux Foundation Collaborative Project, 2013. [Online]. Available: http://www.opendaylight.org
[33] Juniper Networks, ‘‘Opencontrail,’’ 2013. [Online]. Available: http://opencontrail.org/
[34] R. Hand and E. Keller, ‘‘ClosedFlow: OpenFlow-like control over proprietary devices,’’ in Proc. 3rd Workshop Hot Topics Softw. Defined Netw., 2014, pp. 7–12.