ISSN 2278-3091

Volume 9, No.1.2, 2020

International Journal of Advanced Trends in Computer Science and Engineering

Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse3191.22020.pdf

https://doi.org/10.30534/ijatcse/2020/3191.22020

Feasibility of Software Defined Network in a SOHO Network

Nitheesh Murugan Kaliyamurthy[1], Dr. SwapneshTaterh[2], Dr. Suresh Shanmugasundaram [3]

[1] PhD Scholar, Amity Institute of Information Technology,
Amity University, Jaipur, India

[2] Associate Professor, Amity Institute of Information Technology,
Amity University, Jaipur, India

[3] Professor, Faculty of Engineering and Applied Sciences, Botho University, Botswana

ABSTRACT

A spotlight concept for the researchers in today's technology driven world is Software Defined Networking. Before a few decades, considered as extremely diverged domains, Software and Networking concepts are now converging itself to bring out feasible, effective, cost-efficient and easy solutions to the existing challenges in the networking domain. Due to the arrival of latest user-friendly technologies, IoT applications, the legacy networking domain is facing a drastic and dramatic growth with respect to the size and complexity. This brings in a whole lot of new challenges in managing, controlling and securing the existing legacy networks. Software Defined Networking, because of its decoupled architecture, will be a better alternative approach from the legacy network to provide a feasible solution for the existing challenges. This paper focuses on the existing challenges in the SOHO networks and the available options in Software Defined Networking to overcome the challenges. This paper is designed with an Introduction part describing the challenges in a SOHO Network continued with the pure SDN Architecture following with the industry approach on SDN implementation, SDN Standardization strategies and Cisco ONE SDN Architecture. This paper concludes with a comment on the feasibility of implementing SDN in SOHO networks replacing legacy network.

Key words : SOHO, Software Defined Networking, SDN, Data Plane, Control Plane, DDoS, TAN, Traditional Architecture Network, OpenFlow, ONE.

1. INTRODUCTION

Software Defined Networking, the emerging trend in today's networking domain is one of the hot topics for researchers to work-on with. This is because of its entirely different prototype approach. The SDN Architecture decouples the control and the data plane proposing an entire turn from the traditional network architecture. This attracts the researchers over the last decade to talk more about the pros and cons of Software Defined Networking Architecture.

During the initial development of Software Defined Networking, it was considered as a theoretical approach rather than finding feasible solutions to implement in the existing network architecture. However, Software Defined Networking architecture facilitates the users to move from a closed vendor- specific scenario in to an open user-specific or network-specific scenario. Software Defined Networking enables a centralized control over the network (Nitheesh Murugan Kaliyamurthy & Dr. SwapneshTaterh, 2018). This initiated few industrial enterprise giants like Google to move their operations from traditional network architecture to a software defined networking architecture which eventually created a view that Software Defined Networking architecture is efficient in a large enterprise network. Google's WAN (S. Jain, A. Kumar, S. Mandal, J. Ong, L. Poutievski, A. Singh, S. Venkata, J. Wanderer, J. Zhou, M. Zhu, J. Zolla, U. H¨ olzle, S. Stuart, and A. Vahdat, 2013) implemented a Software Defined network with OpenFlow proved that Software Defined Networking is not a theoretical approach, but could be more efficient in dynamic routing and traffic controlling aspects (Haque, I. T., & Abu-Ghazaleh, N, 2016).

Various research works have been done in the recent past not only considering the architecture of Software Defined Networking, but also its other features like Latency, Quality of Service and Load balancing. However, Security perspectives in the network are always challenging because of the nature of Software Defined Networking Architecture by decoupling control and data plane allowing the switching devices only to forward the packets and a centralized controller to make decisions of network flow. A lot of researches are on-going in improving the security aspects of a Software Defined Networking (Nitheesh Murugan Kaliyamurthy, Dr. Swapnesh Taterh & Dr. Suresh Shanmugasundaram, 2019).

Major research works focuses on the specific aspects and functionalities of Software Defined Networking, like the SDN controllers, the managing capabilities, the Quality of Service etc. There are also research works deep diving into the security challenges of SDN networks. However, all these aspects addresses the challenges and functionalities based on the enterprise networks, Data Centre, cloud management which puts in a lot of servers in the network, requires agile decision making process in packet filtering and forwarding (Abdalkrim M. Alshnta, MohdFaizalAbdollah & Ahmed AlHaiqi, 2018). On a true note, Software Defined Networking architecture is very resourceful and attractive for the above stated network infrastructure, overcoming the vendor specific devices, protocol and proprietary functionality challenges, level of complexity in achieving the expected outcomes and much more.

This paper is efficiently classified to focus on the feasibility of implementing Software Defined Networking Architecture in SOHO Networks. This paper concludes with comments on feasibility of implementation. Part 2 of this paper discusses on the challenges in SOHO networks followed by Part 3 detailed view of Software Defined Networking Architecture and Part 4 focusing on the Industries contribution towards Software Defined Networking. Part 5 gives a generic overview on standardization consortiums of SDN architecture and part 6 discusses the Cisco's SDN ONE Architecture. In the final Part, the viability of SDN implementation in SOHO networks is discussed

2. SOHO NETWORKS AND ITS CHALLENGES

The day-to-day increase in the amount of incoming and outgoing data in the network scenario raises the complexity in handling them efficiently, effectively and more important securely. In the process of mitigating the above said parameters raises the performance bottlenecks within a network. (J. Y. Hailong Zhang, 2015). The devices in traditional legacy network architecture deals with a whole lot of information focusing from source till the destination, its formats, transmission and much more (P. P. R. B. Ameen Banjar, 2015). The increase in data flow precisely requires more resources which in term is more expensive for SOHO networks to meet the basic requirement. Moreover, the additional controls required in effective management of the SOHO networks using traditional network infrastructure are most probably vendor-specific and complex in nature which further raises the management issues in the networks (Rajni Aron, Inderveer Chana & Ajith Abraham, 2015). Based on interviews conducted with the IT Managers dealing with day-to-day challenges in SOHO networks, allocation of internet bandwidth to the users based on their roles, managing and controlling Intranet access, securing the network from inside and outside attacks, local file servers (ftp servers), access to the available resources such as printers, scanners, copiers in an efficient manner, desktop user management were the top listed challenges in SOHO networks.

Focusing on securing the network, there are a lot of attacks happened in the past targeting the SOHO networks (Adrian Pastor, 2007). The SOHO network is vulnerable in various aspects such as buffer overflows (Website: Embedded Device Hacking, 2013), denial of service attacks, cross-scripting attacks etc (Nadav Rotenberg, Haya Shulman, Michael Waidner& Benjamin Zeltser, 2017). To cope up with today's advancing technology the networks are forced to allow BYOD policies which further makes the network vulnerable. Social Engineering is another big security concern which puts forth in training the users at a high cost and a weak output. Creating policies for every challenges faced in day-to-day scenario is the most common practice measures followed in the network management perspective (David Longenecker, 2016). The real problem arises at this juncture. To implement the policies in a network requires complex configurations which are more specific proprietary features provided by vendor specific devices. They shall be achieved only by an expensive resource implementation.

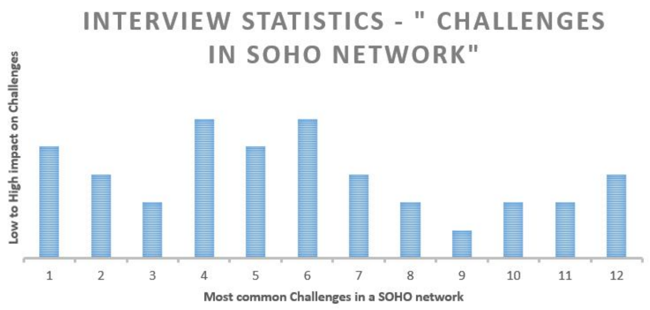

Figure 1: Summation of Challenges in SOHO network

The chart in Fig 1 is the summation of the output given by personnel's in the position of managers or above in a SOHO network management ranging from low to high impact. The collection of data was anonymous enabling the personnel's to answer the true fact without hesitation (Mrutyunjaya Panda & Ajith Abraham, 2015). The challenges are listed in table 1. As per the above analysis, the highest concern for the managerial personnel's of SOHO networks is the security and BYOD policies. Though security concerns are given highest priority in managing any sort of networks, the attacks over a SOHO networks are widespread (Nadav Rotenberg, Haya Shulman, Michael Waidner & Benjamin Zeltser, 2017). It is inevitable to avoid BYOD policies in today's rapid growth of technology. This scenario brings in the two factors to be listed in the top above the other listed challenges. However, it does not mean that the other challenges shall be ignored or given less priority. All the challenges considered in this parameter is a union factor interlinked to each other. To achieve an efficient, effective and secured SOHO network management, all the challenges are to be addressed regardless of its impact factors. Researching on a new feasibility to achieve the above factors does not mean that they are unachievable in the current traditional network architecture. It is achievable but expensive, vendor dependent and complex.

Table 1: List of Challenges and summation of impact

Listed Challenges	Impact (1-5)
(1)Allocation of Internet Bandwidth based on user roles	4
(2) Internet issues within the network	3
(3) Wireless device connectivity	2
(4) BYOD Challenges	5
(5) Intranet access	4
(6) Security	5
(7) FTP File Server	3
(8) Resource Management	2
(9) Design and management of Access Points	1
(10) Antivirus installation and management	2
(11) Software installation and management	2
(12) Users with pirated software usage	3

3. SOFTWARE DEFINED NETWORKING – DETAILED VIEW

Software defined networking is now in discussion over the past 10 years. The basic variance from a traditional network is its architecture of separating control plane from the data plane. By now, almost all the vendors in the market are turning themselves towards SDN. We will be discussing more in detail about the vendors and their market approach towards SDN in the next part. However, we will classify SDN architecture in such a way to analyze its feasibility towards the challenges listed above in a SOHO network.

Software defined networking, otherwise a pure/ open SDN (Global IPD week, 2017) decouples control plane and data plane from the managing devices. In a traditional network, the manageable devices work together with control and data plane. The control plane is responsible to maintain a routing table and the data plane is responsible to maintain a forwarding information base. The control and the data plane works based on the configured protocols in a network. The best routes are registered in the routing table which is the control plane and based on the information registered in the routing table, a forwarding information base is created which is the data plane. The data traffic will move in and out of a network based on the information in the forwarding information base and not the routing table. However, the forwarding information base is created based on the routing table. The idea of SDN is to put the control plane in a controller which has a centralized control over the network and put the data plane in the manageable devices which will receive the information about the data flow from the centralized controller. This will enable the manageable devices to focus only on forwarding the data in a network and the decisions are based on controllers (C. B. Paul Göransson, 2014). The other advantage of SDN is that various applications shall be created which shall help the controllers to take various decisions in forwarding the data in a network.

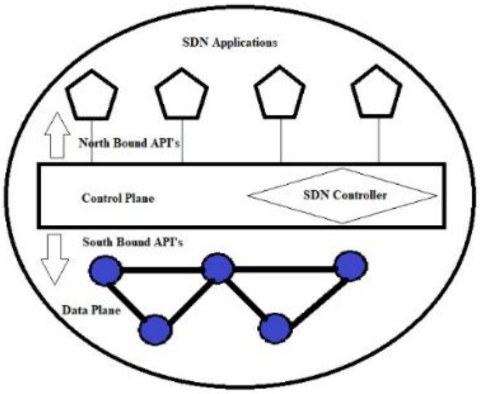

Figure 2: Brief SDN Architecture

Based on the Fig. 2, the SDN Architecture has moved the control plane from the manageable devices to the controller, a separate control in the top of the network, having the view of the entire topology of the network, enabling itself to define control over the network, based on the Applications through the North Bound APIs. The Controller in the control plane based on its routing information base (routing table) will create a forwarding information base at the devices in the data plane to forward the data in the network through the South Bound APIs. There are different controllers like ONOS, onePK, Big Network Controller, OPENDAYLIGHT, RYU, Rosemary (Nitheesh Murugan Kaliyamurthy & Dr. SwapneshTaterh, 2018). The interaction between the control and the data plane will happen based on the South Bound API's like Openflow. The North bound API's establishes communication with the controllers to the applications. Based on the controller used in the network, supporting programming languages shall be used to create applications as per the network requirements. The SDN Applications and the SDN controllers communicate through the North Bound API's and the controller controls the network through the South Bound API's. This decoupled architecture of control and data plane from the devices with a centralized view of the network with the controller adding the programmability feature (Sezer, S., Scott-Hayward, S., Chouhan, P., Fraser, B., Lake, D., Finnegan, J & Rao. N, 2013) in a network makes Software Defined Networking a special effect to address the existing challenges in the traditional or legacy network.

4. INDUSTRIES CONTRIBUTION TOWARDS SDN

Industries play a very vital role in the existing traditional network architecture which impulse them to concentrate more on the Software Defined Networking Architecture. The main role of the Industries in Software Defined Networking is to mold and modify their business plans from a traditional network architecture to a SDN architecture without a high impact on their business scheme. Their participation in the SDN is also one of the main reason for the rapid growth of SDN concepts in the recent past. Even though Software Defined Networking is a new name for the decoupling technology coined in the recent past (Sezer, S., Scott-Hayward, S., Chouhan, P., Fraser, B., Lake, D., Finnegan, J & Rao. N, 2013), the original concept of SDN evolved in the late 1990's. AT&T's GeoPlex, a middleware for managing networks (P. Dutta, 1998) was implemented in 1997 followed by Ericson in 2001 with its first soft switch Supranet Transaction Server (Nitheesh Murugan Kaliyamurthy & Dr. SwapneshTaterh, 2018).

The concept of programmability, separating control and data plane was attempted in the late 1990's and early 2000's (Network Security, Online). This made the academic and industry researchers to focus their study over the concept which was revived as Software Defined Networking. Large enterprise Organisations like Google has implemented SDN in their private WAN to mitigate the issues on the existing traditional network (Nitheesh Murugan Kaliyamurthy & Dr. SwapneshTaterh, 2018). After the implementation of SDN by these large enterprises left the part of considering SDN as a theoretical approach and both the industry and academia started concentrating more seriously on the implementation part of SDN.

Other Organisations like Cisco, Juniper, IBM, VMWare, NEC, Brocade, HP, BigSwitch are also keen in implementing Software Defined Network (Nitheesh Murugan Kaliyamurthy & Dr. SwapneshTaterh, 2018) based on their own strategies and business impacts. Cisco is concentrating on onePK controller with OpenFlow as a South Bound API. Cisco's onePK is discussed more in detail in the following part. Juniper is also working on API based controllers with OpenFlow as a South Bound API. IBM focuses on Programmable Network Controller as a SDN Controller with OpenFlow, Rack Switch and Flex System as South Bound API. VMWare is working on NVP (NSX) as a SDN Controller with OpenFlow Open vSwitch as South Bound API. NEC is working on Programmable Flow Controller as its SDN Controller and Programmable Flow 5240 and 5820 as its South Bound API (Zahra Pooranian, Mohammad Shojafar, JemalAbawajy & Ajith Abraham, 2015). Brocade has introduced its own Brocade SDN Controller and OpenFlow as South Bound API (Dataswitchworks, Online). HP is working on VAN SDN Controller which works with an OpenFlow enabled network. BigSwitch is working on Big Network Controller as its SDN Controller with OpenFlow Indigo, Switch Light as South Bound API (Nitheesh Murugan Kaliyamurthy & Dr. SwapneshTaterh, 2018). These are the few key industries which contribute towards the implementation of Software Defined Networking. However, these industries are part of different organization standards which set a common platform towards implementation of Software Defined Networking.

5. STANDARDIZATION OF SDN

Software Defined Networking, a hot topic both in today's industrial and academia sector has updates on a day to day basis. In order to maintain the accessibility and flexibility of the topic, which is its one big advantage as stated, researchers and industrial sector felt of its standardization. In the early stage of today's Software Defined Networking concepts, in 2008 after the introduction of OpenFlow protocol, there was a wide variance in defining and structuring the SDN concepts (Álvaro Herrero, VáclavSnášel, Ajith Abraham, Ivan Zelinka, HéctorQuintián & Emilio Corchado, 2015). In the focus of standardizing SDN architecture and proceed further in a beneficial path, various consortiums were formed.

In the year 2011, Open Networking Foundation (ONF) (Open Networking Foundation, Online) was formed. ONF partners with industry sectors starting from big enterprise not limited to a small start-up company based on their interest and contribution towards SDN. Industrial Giant's like Google, Infosys, Juniper, Intel, AT&T, DELL EMC and much more are partnering Open Networking Foundation (Open Networking Foundation, Online).

ONF started from the point where SDN was in 2011 and published the first standard and detailed SDN architecture in the year 2014. ONOS (Open Network Operating System), an operating system for SDN service providers was introduced. Followed by an update in the SDN architecture in the year 2016 (Schaller, S., & Hood, D, 2017). These consequent tasks by the ONF paved a path way to take SDN concepts from a basic decoupled and compatible packet forwarding mechanism into resource utilization and alignment of virtual and physical environment (Mrutyunjaya Panda, Ajith Abraham & ManasRanjan Patra, 2015). This created a new face to the SDN concept. Focused on industrial purpose and considered as a large enterprise solution, SDN architecture turned into a structure to be implemented in any category of a network not limited to enterprise networks, WAN's, data centers, campus networks and much more (Schaller, S., & Hood, D, 2017).

There are other consortiums such as IETF (Internet Engineering Task Force), OpenDayLight which also talks about the various layers and applications in the architecture of SDN such as its infrastructure, various interfaces like south bound, north bound, east and west bound, the SDN Controllers, programming languages, various applications used in formulating SDN architecture in the aspect of network implementation (F. M. V. R. P. E. V. C. E. R. S. A. S. U & Diego Kreutz, 2015). Based on the given standards and innovative approaches by various enterprises and the researchers further funneling up with the SOHO network challenges Cisco's SDN approach, the onePK SDN controller is taken in the next part to discuss on the feasibility of addressing the SOHO network challenges. It does not implicate that other SDN controllers are not viable in addressing the existing SOHO network challenges, but as an initiative to cope up with the challenges, the next part analyses the architecture of Cisco's onePK controller to mitigate the challenges in SOHO network

5. CISCO'S ONE ARCHITECTURE

All the way talking about the advantages of OpenFlow protocol, there are a lot of areas in which more research works are required in the implementation of SDN networks. While focusing on SDN architecture, we compile and list out the disadvantages of the traditional networks, wherein the actual fact is that the traditional networks also have seen a tremendous growth in the last few decades listing out good numbers of advantages behaving as a consistent and stable network architecture withstanding the new generation challenges. Few advantages in the traditional networking devices in terms of device management and device monitoring in a network, capability of directly manipulating routes and device advertisements, data packet payload manipulation are areas in which more clarity and functionalities are required in a SDN implemented network. On stating the areas of improvement, Cisco also accepts the true advantages in the ONF SDN architecture and has developed a full-fledged OpenFlow controller Cisco Extensible Network Controller. Cisco steps ahead with a wider and broader approach of SDN concept keeping in mind a flexible and compatible network programmability along with creating feasible applications to gather real-time intelligence of a network and attain multiple models of network programmability (White Paper: Cisco, 2013). Cisco's perspective of network programmability endorses acquiring intelligence from the network, analyzing them further to provide a real-time intelligence about the network enabling the applications and the developers to have a broader view on the happenings (data flow, device inclusions and much more) within the network focusing on reducing the existing and maximizing today's cyber security challenges. This also focuses on improving the performance of a network and ensuring reliable security to the network by directing the data flow analyzed in the real-time scenario to stateful services like firewalls (White Paper: Cisco, 2013).

Cisco, focusing on wider and broader range of network programmability feature, has come up with Cisco Open Network Environment (ONE) architecture. The Open Network Environment includes programmatic API's, agents and controllers and Network virtualization Infrastructure (White Paper: Cisco, 2013). The ONE architecture is developed not keeping in focus a specific network infrastructure which is the existing problem in any architecture feasible to fit into different structures and sizes of the network. The challenges faced by WAN, data centers, campus networks are entirely different and requires a speculative insight to address these challenges. ONE architecture is developed keeping all the above factors as a criteria and it is believed to support programmable actions towards device discovery, device management, routing protocols and policy enhancements (ONE Architecture, Online)

6. CONCLUSION AND FUTURE WORK

On a conclusive note based on the above list of challenges faced in the SOHO networks and the rapid development in the scope of Software Defined Networking trying to address the recent challenges in the real time scenarios, the feasibility of implementing SDN architecture in a SOHO network is viable. To aggregate the suggestion further, SDN architecture is developed to simplify the network operations befitting programming capability to control over the network in a centralized environment gives the management a God's eye perspective towards the network. The top listed challenges like security, BYOD, bandwidth management and intranet access in a SOHO network could be easily mitigated using the standards and programmability features of SDN architecture. Few scenarios make SDN architecture to suite better for a big enterprise networks and WANs. Stepping ahead, Cisco's ONE architecture will be a tailor made structure to suite the SOHO networks mitigating almost all the challenges listed above because of its agile approach to optimize network as per the emerging and volatile requirements. To further move towards implementation of SDN architecture in SOHO networks, adoption of network programmability, setting up policies to step further in implementation, will ensure a productive operational cost and feasible control over the network to mitigate the above challenges.

REFERENCES

1. Abdalkrim M. Alshnta, MohdFaizalAbdollah & Ahmed AlHaiqi. (2018). SDN in the home: A survey of home network solutions using Software Defined Networking. Cogent Engineering (2018), 5: 1469949. https://doi.org/10.1080/23311916.2018.1469949
2. Haque, I. T., & Abu-Ghazaleh, N. (2016). Wireless software defined networking: A survey and taxonomy. IEEE Communicable Survey Tutorials, 18(4), 2713–2737. doi:10.1109/COMST.2016.2571118
3. S. Jain, A. Kumar, S. Mandal, J. Ong, L. Poutievski, A. Singh, S. Venkata, J. Wanderer, J. Zhou, M. Zhu, J. Zolla, U. H¨ olzle, S. Stuart & A. Vahdat, (2013). B4: Experience with a globally-deployed software defined

WAN. SIGCOMM Comput. Commun. Rev., vol. 43, no. 4, pp. 3–14. https://doi.org/10.1145/2534169.2486019

4. Nitheesh Murugan Kaliyamurthy & Dr. SwapneshTaterh. (2018). Understanding software defined networking – A study on the existing software defined networking technologies and its security impact. Journal of Biology and Today's World. 2476-5376(Print), 2322-3308 (Online). Volume 7, 2018, Issue 1, Pages 36-40; Paper doi: 0.15412/J.JBTW.01070107; Paper ID: 16566
5. Rajni Aron, Inderveer Chana, Ajith Abraham, A hyper-heuristic approach for resource provisioning-based scheduling in grid environment, The Journal of Supercomputing, 71(4): 1427-1450, 2015. https://doi.org/10.1007/s11227-014-1373-9
6. J. Y. Hailong Zhang. (2015). Performance of SDN Routing in Comparison with Legacy Routing Protocols. International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery. https://doi.org/10.1109/CyberC.2015.30
7. Kaliyamurthy, Nitheesh Murugan, SwapneshTaterh and Suresh Shanmugasundaram. “Vulnerability of SDN Network Architecture and Proposed Countermeasures on Enhancing Security”, International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-4, November 2019, Retrieval Number: D5266118419/2019©BEIESP, (doi:10.35940/ijrte.D5266.118419).
8. P. P. R. B. Ameen Banjar. (2015). Comparison of TCP/IP Routing Versus OpenFlow Table and Implementation of Intelligent Computational Model to Provide Autonomous Behavior. Computational Intelligence and Efficiency in Engineering Systems, Part II, vol. 595, Z. C. W. J. T. Ł. Grzegorz Borowik, Ed., Springer International Publishing. pp. 121-142. https://doi.org/10.1007/978-3-319-15720-7_9
9. Nadav Rotenberg, Haya Shulman, Michael Waidner& Benjamin, Zeltser. (2017). Authentication-Bypass Vulnerabilities in SOHO Routers. In Proceedings of SIGCOMM Posters and Demos ’17, Los Angeles, CA, USA, August 22–24, 3 pages. https://doi.org/10.1145/3123878.3131989.
10. Website: Embedded Device Hacking, 2013. Reverse Engineering a D-Link Backdoor. (2013).http://www.devttys0.com/2013/10/reverse-engineering-a-d-link-backdoor/
11. David Longenecker. (2016). ARRIS (Motorola) SURFboard modem unauthenticated reboot flaw. http://www.securityforrealpeople.com/2016/04/arris-motorola-surfboard-modem.html
12. Mrutyunjaya Panda, Ajith Abraham, Development of a Reliable Trust Management Model in Social Internet of Things, International Journal of Trust Management in Computing and Communications, 2015.
13. Adrian Pastor. 2007. BT Home Flub: Pwnin the BT Home Hub. (2007). http://www.gnucitizen.org/blog/bt-home-flub-pwnin-the-bt-home-hub/
14. Global IPD week, (2017). Cisco Networking Academy, SDN Fundamentals 1
15. Sezer, S., Scott-Hayward, S., Chouhan, P., Fraser, B., Lake, D., Finnegan, J. & Rao, N. (2013). Are we ready for SDN? Implementation challenges for software-defined networks. IEEE Communications Magazine, 51(7), 36–43. doi:10.1109/mcom.2013.6553676
16. P. Dutta. (1998). Internet object caching. Intelligent Network Workshop,Proceedings of 7th IEEE. https://doi.org/10.1109/INW.1998.713263
17. Zahra Pooranian, Mohammad Shojafar, Jemal Abawajy, Ajith Abraham, An efficient meta-heuristic algorithm for grid computing, Journal of Combinatorial Optimization, 30(3): 413-434, 2015. https://doi.org/10.1007/s10878-013-9644-6
18. Network Security, (Online). Available: http://www.networxsecurity.org/members-area/glossary/s/sdn.html.
19. Open Networking Foundation, (Online). Available: https://www.opennetworking.org/about/onf-overview.
20. C. B. Paul Göransson, (2014). Software Defined Network, A Comprehensive Approach. 1 ed., Morgan Kaufmann.
21. Mrutyunjaya Panda, Ajith Abraham and Manas Ranjan Patra, Hybrid Intelligent Systems for Detecting Network Intrusions, Journal of Security and Communication Networks, 8(16): 2741-2749, 2015. https://doi.org/10.1002/sec.592
22. Dataswitchworks, (Online). Available: http://www.dataswitchworks.com/SDN-Controller.asp
23. Álvaro Herrero, Václav Snášel, Ajith Abraham, Ivan Zelinka, Héctor Quintián and Emilio Corchado, Computational Intelligence in Security for Information Systems, Logic Journal of the IGPL, 23:1, 1-3, 2015. https://doi.org/10.1093/jigpal/jzu041
24. Schaller, S., & Hood, D. (2017). Software defined networking architecture standardization. Computer Standards & Interfaces, 54, 197–202. doi:10.1016/j.csi.2017.01.005
25. F. M. V. R. P. E. V. C. E. R. S. A. S. U & Diego Kreutz. (2015). Software-Defined Networking: A Comprehensive Survey. Proceedings of the IEEE, vol. 103, no. 1, pp. 14-76. https://doi.org/10.1109/JPROC.2014.2371999
26. White Paper: Cisco. (2013). Software-Defined Networking: Why We Like It and How We Are Building On It.
27. ONE Architecture, (Online). Available: www.cisco.com/go/one
28. Jalal A. Sultan &amp; Raghad M. Jasim, “Demand Forecasting using Artificial Neural Networks Optimized by Artificial Bee Colony”, BEST: International Journal of Management, Information Technology and Engineering (BEST: IJMITE), Vol. 4, Issue 7, pp. 77-88

29. A. Jaya Lakshmi, J. Swetha &amp; G. N. Swamy, “Enhanced Multi-Transmitter Based Channel Selection Matching System for Cognitive Radio Ad Hoc Network”, IMPACT: International Journal of Computational Sciences and Information Technology (IMPACT: IJCSIT), Vol. 1, Issue 1, pp. 1-12
30. Vinay Bhatia, Dushyant Gupta &amp; H. P. Sinha, “Implementing Comparative Analysis of Wireless LAN Security Protocols in NS2”, International Journal of Electronics and Communication Engineering (IJECE), Vol. 2, Issue 2, pp. 1-8
31. S. Gayathri Devi, A. Marimuthu &amp; A. Kavitha, “Multicast Routing in Mobile Ad Hoc Networks: Issues and Techniques”, International Journal of Computer Science and Engineering (IJCSE), Vol. 3, Issue 3, pp. 1-8
32. Shawqi Ali Daghem Mohammed &amp; Shaikh Samad, “Irish and Irishness in G. B. Shaw’s “John Bull’s Other Island””, International Journal of English and Literature (IJEL), Vol. 5, Issue 4, pp. 23-30
33. Vishal Sharma &amp; Navneet Kaur, “Performance Estimation of OFDM -Wimax Network”, International Journal of Computer Networking, Wireless and Mobile Communications (IJCNWMC), Vol. 4, Issue 5, pp. 33-40