Proc. of the Third Intl. Conf. on Advances in Information Processing and Communication Technology - IPCT 2015

ISBN: 978-1-63248-077-4 doi: 10.15224/ 978-1-63248-077-4-07

Can Security Be Built Intrinsically into SDN?

(A Survey of Existing Scenario and the Way Forward)

[Naveen Bindra, Manu Sood]

***Abstract*—In traditional networks, the threats owing to cyber-attacks, Trojans/ viruses, botnet based attacks, DoS/DDoS attacks etc. have posed challenges to the networks around the globe. In SDN scenario, decoupling of control and data planes along with the programmability of control plane have brought flexibility in contrast to existing ossified networks. Most of the limiting factors of traditional networks can effectively be addressed through a relatively new networking paradigm i.e. Software Defined Networks (SDN). The programmability feature of SDN presents opportunities to shape the future networking. However, while proposing new architecture for SDN, security aspects must be given due attention. In this paper, the authors present a snapshot of the existing status of security aspects of SDN and also highlight the issues that are yet to be addressed.**

Keywords—SDN, DoS attack, network vulnerabilities, security, security threats, secure SDN architecture

I. Introduction

With the advent of Software Defined Networks (SDN), the perception of networks' functioning has changed. Researchers are now more interested in leveraging the power of programmable networks and to explore new frontiers for innovations. SDN decouples data, control and management planes and removes control plane from network hardware by implementing it in software. A network administrator can easily shape traffic from centralized console without having to touch individual switches. SDN is a paradigm shift from static, inflexible hardware to a flexible, agile and virtualized network. Both wired and wireless networks can be managed by SDN based Controllers.

SDN provide research opportunities which were missing in traditional. BigData, BYOD (Bring Your Own Device), Internet of Things (IoT) can be handled efficiently by programmable networks. Data centres and Clouds are areas. Aspects of security concerns due to heterogeneity of IT infrastructure in cloud have been looked into by [1].

SDN is still an evolving technology. New models and designs for an efficient, agile and scalable network are being proposed by many. The journey covered in this area till date has been well presented in [2]. Security is still a neglected domain in SDN research as not much work can be found in literature on the security plane of SDN. This paper tries to identify gaps in some of the proposed existing solutions in security and finally highlights to mitigate most, if not all, threats and attacks.

SDN though has the ability to solve age old problems of agility, flexibility and complexity, but at the same time, also exposes the networks to new threats. Botnet based DDoS attacks carried out intelligently are very difficult to even detec t. Centralized controller can be a single point of failure. Dependability apart from security is another challenge [3]. Wireless networks are even more vulnerable as they do not have the secure channel as implemented in their peer wired networks. Problems in wireless networks e.g. Intelligent jamming attacks that go beyond applying brute-force at the physical link; exploiting configuration or protocol specific vulnerabilities have been discussed in [4]. This paper is an attempt to accentuate on the need to a) have a Secure SDN and b) build a cost effective, integrated and Secure SDN model based on basic security principles. It entails the security requirement and advocates for having an integrated, adaptive and cognitive system which can deal with new security challenges and threats. Section II of this paper elaborates what SDN has to offer to the networking world, be it wired or wireless. It tries to summarize security requirement and parameters on which secure SDN model can be built. It further; list out the existing security threats. Section III critically examines the existing literature in SDN security and highlights the extent of conformity to security requirements in SDN. Section IV provides a) an argument to build security intrinsic to SDN rather than bolting it later on, and b) an overview of the limitations that exist in SDN security. It is followed by the conclusion and scope for future work in Section V.

II. Offerings by SDN

A. *Need of SDN*

In traditional networks, new protocols are written from scratch and traffic engineering is handled with ad-hoc mechanisms. Security implementations typically require Access Control List (ACL), VLANs(Virtual LAN), Middle boxes, Intrusion Detection System (IDS), Intrusion Prevention System (IPS) and firewall, which have rigid set of rules.

Kreutz et al. in [4] have looked into the possible threats that can be posed by benign, buggy and other malicious applications. It uses customized permission set and threat based isolation mechanism.

SDN offer test beds to probe and implement new ideas. The virtual network infrastructure described in [5] can be used to develop and deploy new SDN solutions. A number of open source tools have made this kind of experimentation possible. NoX [6] is an open source controller that can be used to program and control switches using OpenFlow. GENI [7] is virtual programmable network and a natural choice for researchers. It offers simulated environment for routers, end-hosts and network links.

Naveen Bindra
Himachal Pradesh University
India

Manu Sood
Himachal Pradesh University
India

Proc. of the Third Intl. Conf. on Advances in Information Processing and Communication Technology - IPCT 2015

ISBN: 978-1-63248-077-4 doi: 10.15224/ 978-1-63248-077-4-07

[8] proposes a new SDN based architecture with centralized controller and extremely simple flow based Ethernet switches for an enterprise. Organizations cannot afford to lose money due to mis-configurations and security issues in the networks. [9,10,11,12] proposed solutions to provide reliability and scalability in networks.

OpenFlow [13] is a set of standard protocols for communication between centralized controller and dumb switches over secure channels. The switch can be programmed using OpenFlow. Intrusion Detection system and network monitoring are proposed to be implemented as controller application in [14].

Byzantine fault tolerance is another concept proposed in [15]. It may happen that systems come crashing down due to incorrect process request, corrupting their local state and other inconsistencies that may come up in other arbitrary ways. Security in SDNs can be enforced in better ways as proposed in [10] & [13]. They propose to focus on network level goals rather than configuration of individual routers which induces mistakes and compromise security. As shown in Figure 1, the traditional networks are no match for SDN when it comes to issue e.g. management and innovation.

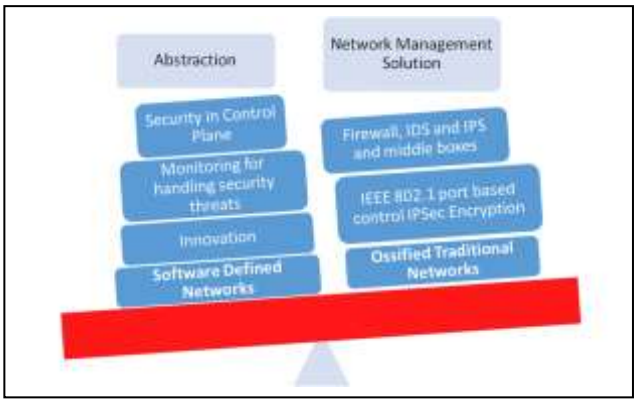

Figure 1. Contrast in SDN and Traditional Networks

B. *Security Parameters and Requirements*

To come up with a model that can detect and mitigate security threats, the requirements for the security need to be defined in the first place. Mere detection of threat does not serve our purpose if same are not mitigated. Security includes but not limited to:

a) Confidentiality
b) Integrity: The system should be able to provide integrity assurance before storing the data.
c) Robustness and Availability
d) Compliance to Regulatory framework
e) Authentication, Authorization and Accounting:
f) Adaptive/ Cognitive: The system should support adaptive and learning capabilities.
g) Redundancy
h) Cost effectiveness: The solution should be cost effective for its wider acceptance by commercial vendors and for the sake of standardization.
i) Auto-healing: A device or system that has the ability to perceive that it is not operating correctly and, without human intervention, make the necessary adjustments to restore itself to normal operation.
j) Detection: of abnormal behavior/ malicious activity or threats inside a network

C. *Threats in SDN*

Forged or faked traffic flow, DoS and DDoS attacks top the list of threats. A DoS or DDoS attack is initiated by rouge elements to suspend temporarily or indefinitely the services of host connected over Internet. The genuine users are denied services being rendered to by these websites. Following are the major vulnerabilities in traditional networks and Software Defined Networks:

- Attack on vulnerabilities of switches and controller include attack on controller's operating system and APIs.
- Lack of mechanism to ensure trust among controller and management applications.
- Lack of trusted resources for forensic remediation.
- Vulnerabilities of wireless networks are liable to pose potential threats.
- Malware/ Trojans/ viruses
- IP Spoofing done by packets posing as legitimate in DoS attacks and are undetected as their true source remains unknown.
- Disaster Management and recovery processes are also prone to threats.

III. Work Done In Security-A Comparative Analysis

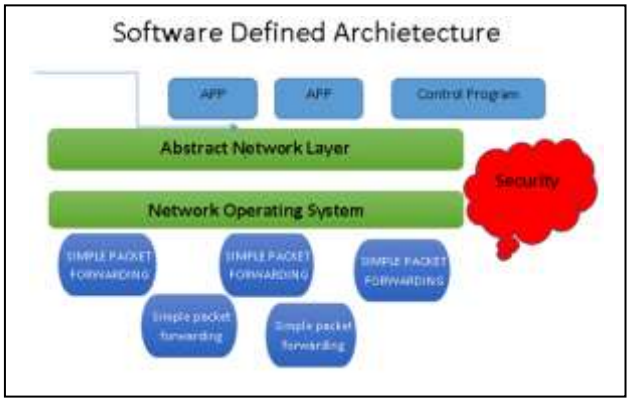

Figure 2. Security in SDN Architecture

In this section, the authors critically analyze various SDN models and highlight their strengths and weaknesses. The exact place of security in SDN is still evasive as depicted in Figure 2. In this paper authors have tried to undertake minute study of various SDN models from the security prospective and have put forward their standpoint. We first presented ways in which most occurring DoS/ DDoS attacks have been tackled by various researchers and then the methods to detect to intrusion/ infection in SDN have been emphasized. Later in this section potential threats in wireless networks and mobile devices have been touched upon. Imposing network wide policies in SDN can be a layer of defence as mentioned towards the end of this section. Active monitoring of network status and using the

Proc. of the Third Intl. Conf. on Advances in Information Processing and Communication Technology - IPCT 2015

ISBN: 978-1-63248-077-4 doi: 10.15224/ 978-1-63248-077-4-07

way to discourage attackers are other mechanism stressed upon.

OpenFlow [13] was designed for routing applications, primarily deals with flow and not with individual packets. The paper proposes a flexible sampling extension of OpenFlow that helps controller to access packet level information thus overcoming the drawback of OpenFlow. Shirali-Shahreza and Ganjali in [14] recommend Intrusion Detection System (IDS) and network monitoring as controller applications in SDN. Using middle box can result in huge cost savings. IDS access packet level information but this information is not readily available in SDN controllers.

Lim et al [11] and Krishanan et al. [16] looks into the possible situation that can arise due to DDoS and Dos attacks. Drawback of this work can be a situation during the attack on the server, it's interaction with DBA is not possible, as the secure channel is not able to receive response from the server then. Krishnan et al. in [16] have put forward some suggestions about dealing with DoS attacks in data centres. The authors suggest a low cost solution to detect such behavioral threats and their mitigation. Phemius et al. in [17] propose a distributed control plane for WAN and constrained networks based on message oriented communications bus. Wen et al. in [18] promote the idea of using fine grained permission system as first line of defence. Dotcenko et al. in [19] look into the security aspect in SDN by proposing to implement security detection and intrusion prevention algorithm as OpenFlow applications. The obvious limitation of this work is the idea of collection and analysis of network traffic on the switch instead of the controller which seems to be in variance to ideology of SDN. Many limitations in current architecture of SDN have been touched upon by S. Sezer et al. in [20]. Secure channel proposed for communication with controller using TLS is a good option for point to point communication between controller and a node. However, if multiple controllers communicate with single node or multiple control processes communicate with single controller, same can lead to a potential manipulation of network traffic

One more possible way to have a secure SDN model as proposed by Chen et al. in [21] is OSTMA (Optimal Security Traversal with Middlebox Addition) mechanism which dynamically monitors network condition and reconfigures the security in traversal path. Discouraging an attacker can be good strategy as illustrated in [22] known as 'Moving Target Defence (MTD)'. The authors here propose to use adaptive environment in order to delay or prevent attacks. Various techniques used in the MTD are virtualization, workload migration, network redundancy, instructions set and address space.

Braga et al. in [23] suggest an SDN based method to detect DDoS attacks based on traffic flow feature to distinguish between a legitimate packet and useless one. Unlike ossified traditional IDS, Skowyra et al. in [24] present L-IDS Learning Intrusion Detection System, a network security service for protecting embedded mobile devices e.g. embedded biomedical devices and robotic material handling where denial of service can be loss of human life. Zaalouk et al. in [25] propose separate control and monitoring to reduce overhead on the controller and thus claim to improve performance. The authors propose four iterations of designs of SDN. What to choose amongst these designs in a particular situation has not fully been explained.

Wang in [26], Chaudet and Haddad in [27] address challenges in SDN based wireless networks. Wang in [26] proposes a secure and efficient way of policy distribution over insecure wireless channel, where SDN can be used to control the flow of packets to ensure that it does not cross the country's border. Link isolation and channel estimation are the identified problems of SDN application in wireless paradigm. Nonetheless, the globally underutilized wireless spectrum can be used by SDN based radio opportunistically with the challenges like slicing and channel isolation [27].

Song et al. in [28] address the issues of network management, accuracy, reliability and scalability. The authors have proposed to manage network wide disaster events. CPU utilization measurements on each router can be an indicator for DoS attack. However this prediction cannot be reliable. In practice, the ability to handle abrupt event in real time is difficult.

Jin and Wang in [29] propose a malware detection algorithm system based on SDN in the mobile devices. The system makes real-time analysis of network traffic. However, the threshold calculation has not been substantiated and it may happen that a genuine host is removed from the network. Moreover, the system has been tested on a very small scale. Bouet et al. in [30] discusses the need to have fine-grained, flexible, adaptable and cost optimized monitoring mechanisms for cyber security. In [31], Zhang et al. compare implementations of Intrusion Prevention System (IPS) in traditional network and SDN. A collaborative and rapid application development platform has been suggested by Shin et al. in [32].

The models discussed in this section has been studied vis- a –vis the security parameters suggested in section II B, generating scenario as depicted in Table I below:

TABLE I. COMPLIANCE TO SECURITY PARAMETERS

	Security Parameters									
SDN Models	***a***	***b***	***c***	***d***	***e***	***f***	***g***	***h***	***i***	***j***
[1]	✓		✓			✓		✓		
[3]	✓				✓					
[4]	✓					✓	✓			
[8]	✓				✓			✓		
[10]			✓		✓	✓				
[11]		✓			✓			✓		✓
[13]		✓			✓					
[14]						✓		✓		✓
[15]					✓		✓	✓		✓
[17]		✓	✓		✓	✓	✓	✓		✓
[18]					✓					✓
[19]	✓					✓		✓		
[20]			✓		✓	✓				
[21]					✓		✓			
[22]	✓		✓			✓		✓		✓
[23]				✓				✓		
[25]						✓	✓	✓		
[28]	✓		✓							
[29]					✓					
[30]			✓		✓			✓		✓
[31]					✓		✓			
[33]	✓	✓			✓					
[36]			✓							
[37]										
[40]			✓			✓				✓
[41]				✓				✓		

Proc. of the Third Intl. Conf. on Advances in Information Processing and Communication Technology - IPCT 2015

ISBN: 978-1-63248-077-4 doi: 10.15224/ 978-1-63248-077-4-07

Table I shows that the models suggested in [1], [17] and [22] are the ones which address maximum number of security requirements parameters. However, no one seems to score 100%. An SDN architecture will be more secure which scores more.

IV. Secure SDN Architecture & it's Possible Ingredients

A. *Security in existing SDN Architecture*

Many SDN models have been suggested by authors under current study of literature. The researchers propose different protocols, security functions and platform to develop secure applications to deal with various threat/ attacks in SDN based network. However, the need is to have a holistic approach in creating SDN based model which have security per say not only from threat vectors discussed in previous sections but from intrinsic faults too. The ultimate goal of network is to have a network with all-time availability, confidentiality, integrity, authentication, non-repudiation, scalability and fault tolerance and thus secure SDN architecture should be designed in a way that not only tackles the attacks on major components e.g. Controller and channels in SDN but also stresses upon the need to detect and attacks and infection due to Trojans and virus etc. Furthermore the management and mitigation of threats should do away the complexities in current SDN models proposed to date. This is very much possible by using the basic principles as mentioned in section II

Efforts are required to develop simple SDN and secure APIs. Ghafoor and Muftic in [34] propose a software protection against reverse engineering, break once run everywhere attack by using cryptographic techniques. These techniques can also be very efficient in developing APIs in SDN modeling. SDN is an evolving field and innovations require platform for experimentation. Bavier et al. in [37] provide VINI Veritas which gives opportunities to the researchers to test their protocols in realistic network infrastructure. Ahmed et al. in [40] propose a platform for development of various security detection and mitigation modules. It gives all in one solution to develop security applications with ease and abstracts away the complexities. Skowyra et al. in [24] have rightly raised the issue of challenges in adoption of SDN and advocate its interoperability with traditional network for smooth transition to SDN. Though IDS and IPS are integral part of a network and are expected to provide software assurance and protection but are neither satisfactory and nor fully reliable, illustrated well by K. Govindarajan et al. in [36]. Keeping in mind, software vulnerabilities, the authors propose software based on encryption technique which cannot be intruded even using reverse engineering, illegal tempering, program based attacked and even Break Once Run Everywhere kind of attacks. Such technique can prove a boon for development of not only various SDN based API but also Network Operating System and other secure software application for SDN functionalities. Lastly, Sabnis et al. elaborate in [41] that in present multivendor environment, end to end security can only be achieved through use of standards.

B. *Limitations in Existing Work*

Many researchers have proposed excellent ideas to strengthen the security in SDN as described in previous section of this paper. There is still need to work on various aspects of SDN so as to develop a comprehensive security model. SDNs are capable of solving a number of long pending security related concerns but they also pose some challenges due to its architecture and 'software' nature. Existing standard models can be used to overcome software related vulnerabilities. Inter SDN communication is another area which require more consideration. Traditional and SDN networks will coexist for some time as transition is not possible overnight and thus compatibility between the two also require attention which is missing in the work studied here. A secure SDN architecture should conform to all the security requirements/ parameters and provide solution to most, if not all the vulnerabilities. Most of the works studied here also lack the description and ways to include security parameters in these SDN models.

V. Conclusion

This paper is an attempt to review the security aspects of SDN and it has been found that none of the models proposed for provide a comprehensive solution to security threats. The authors suggest that the security requirements and parameters should be the integral part of the development of new SDN architecture(s) so that it can be made intrinsic to these models. There is an urgent need to have an agile, flexible, adaptive and cognitive system which can take on security challenges leading to development of a secure SDN architecture. The authors are at present working on the development of a comprehensive secure model for SDN which can prevent, detect and mitigate most threats as outlined in this paper.

Acknowledgment

We really thank all the authors who have done fabulous work in the field of SDN. In the times to come, SDN will change the way we manage our networks. Security aspect will make it more adaptable and implementable. This idea has kept us going.

References

[1] S. Shin and G. Gu, "CloudWatcher: Network Security Monitoring Using OpenFlow in Dynamic Cloud Networks (or: How to Provide Security Monitoring as a Service in Cloud," 20th IEEE International Conference on Network Protocols (ICNP), 2012, pp 1-6.

[2] http://queue.acm.org/detail.cfm?id=2560327

[3] C. Corbett, J Uher, J. Cook and A. Dalton, "Countering Intelligent Jamming with Full Protocol Stack Agility," Security & Privacy, IEEE Volume 12 , Issue 2, 2014, pp 44 – 50.

[4] D. Kreutz, Fernando M.V. Ramos and P. Verissimo, "Towards Secure and Dependable Software-Defined Networks," HotSDN'13, August 16,2013, Hong Kong, China.

[5] https://www.cisco.com/web/strategy/docs/gov/cis13090_sdn_sled_white_paper.pdf

[6] http://www.noxrepo.org

[7] https://www.geni.net/

[8] M. Casado, M. J. Freedman, J. Pettit, J. Luo, N. Mckeon and S. Shenker, "Ethane: Taking Control of the Enterprise, SIGCOMM '07'", August 27-31, Kyoto, Japan.

ISBN: 978-1-63248-077-4 doi: 10.15224/ 978-1-63248-077-4-07

[9] A. Dixit, F. Hao, S. Mukherjee, T.V. Lakshman and R. Kompella, "Towards an Elastic Distributed SDN Controller, HotSDN'13," August16, 2013 Hong Kong, China.

[10] A. Greenberg, G. Hjalmtysson, D. A. Maltz, A. Myers, J. Rexford, G. Xie, J. Zhan, H. Zhang, "A Clean Slate 4D Approach to Network Control and Management," http://www.cs.cmu.edu/~4D/papers/greenberg-ccr05.pdf

[11] S. Lim, J. Ha, H. Kim, Y.Kim, and S.Yang, "A SDN-Oriented DDoS Blocking Scheme for Botnet-Based Attacks," Ubiquitous and Future Networks (ICUFN), 2014, 8-11 July 2014, pp 63 - 68

[12] L. Vanbever, J. Reich and T. Benson, N. Foster and J. Rexford, "Hot Swap: Correct and Efficient Controller Upgrades for Software-Defined Networks," HotSDN'13 August, 2013, Hong Kong, China

[13] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker and J. Turner , "OpenFlow: Enabling Innovation in Campus Networks A Whitepaper archive.openflow.org/documents/openflow-wp-latest.pd"

[14] S. Shirali-Shahreza and Y. Ganjali,"FleXam: Flexible Sampling Extension for Monitoring and Security Applications in OpenFlow," HotSDN'13, August 16, 2013, Hong Kong, China.

[15] H. Li, P. Li, S. Guo and A. Nayak, Byzantine-Resilient Secure Software-Defined Networks with Mutiple Controllers in Cloud, IEEE Transactions on Cloud Computing, 5 September 2014,pp 436 – 447.

[16] R. Krishnan, D. Krishnaswamy and D. Medysan, "Behavioral Security Threat Detection Strategies of Data Center Switches and Routers," 34th International Conference on Distributed Computing Systems Workshops (ICDCSW), 2014 IEEE, June 30 2014-July 3 2014, pp 82-87.

[17] K. Phemius, M. Bouet and J. Leguay, "DISCO- Distributed Multi-domain SDN Controllers," Network Operations and Management Symposium (NOMS), 2014 IEEE, 5-9 May 2014, pp 1-4.

[18] X. Wen, Y. Chen, C. Hu,C. Hu, C. Shi and Y Wang, "Towards a Secure Controller Platform for OpenFlow Applications," HotSDN'13, August 16, 2013 HongKong, China.

[19] S. Dotcenko, A. Vladyko and I. Latenko, "A Fuzzy Logic-Based Information Security Management for Software-Defined Networks," 16th International Conference on Advanced Communication Technology (ICACT), IEEE,2014, 16-19 Feb. 2014,pp 167 – 171.

[20] S. Sezer, S. Scott-Hayward and P. K. Chouhan, B. Fraser, D. Lake, J. Finnegan, N. Viljoen, M. Miller and N. Rao, "Are We Ready for SDN? Implementation Challenges for Software-Defined Networks," Communications Magazine, IEEE, July 2013, pp 36 – 43.

[21] Y.J. Chen, F. Lin, L. Wang and B. Lin, "A Dynamic Security Traversal Mechanism for Providing Deterministic Delay Guarantee in SDN," 15th International Symposium WoWMoM, IEEE, June 19 2014, pp 1-6.

[22] P. Kampanakis, H. Perros and T. Beyene, "SDN-based solutions for Moving Target Defense network Protection," ," 15th International Symposium WoWMoM, IEEE, June 19 2014, pp 1-6.

[23] R. Braga, E. Mota and A. Passito, "Lightweight DDoS Flooding Attack Detection using NOX/ OpenFlow," 35th Conference on IEEE Local Computer Networks (LCN), 10-14 Oct. 2010, pp 408 – 415.

[24] R. Skowyra, S. Bahargam and A. Bestavros, "Software-Defined IDS for Securing Embedded Mobile Devices", High Performance Extreme Computing Conference (HPEC), 2013 IEEE, 10-12 Sept. 2013, pp 1-7.

[25] A. Zaalouk, R. Khondoker, R. Marz and K. Bayarou, "OrchSec: An Orchestrator-Based Architecture For Enhancing Network-Security Using Network Monitoring And SDN Control Functions, Network Operations and Management Symposium (NOMS)," 2014 IEEE, 5-9 May 2014, pp 1-9.

[26] H. Wang, "Authentic and Confidential Policy Distribution in Software Defined Wireless Network," International Wireless Communications and Mobile Computing Conference (IWCMC)," IEEE, 4-8 Aug. 2014, pp 1167 - 1171

[27] C. Chaudet and Y. Haddad, "Wireless Software Defined Networks: Challenges and Opportunities," 2013 IEEE International Conference on Microwaves, Communications, Antennas and Electronic Systems (COMCAS2013) Tel Aviv, Israel, 21-23 October 2013, pp 1-5.

[28] S. Song, S. Hong, X. Guan, B. Choi and C. Choi, "NEOD: Network Embedded ON-line Disaster Management Framework for Software Defined Networking," IFIP/IEEE International Symposium on Integrated Network Management, 27-31 May 2013, pp 492 – 498.

[29] R. Jin and B. Wang, "Malware Detection for Mobile Devices Using Software-Defined Networking," Second GENI Research and Educational Experiment Workshop (GREE), IEEE, 20-22 March 2013, pp 81 – 88.

[30] M. Bouet, J. Leguay and V. Conan, "Cost-based placement of virtualized Deep Packet Inspection functions in SDN," Military Communications Conference, MILCOM 2013, IEEE, 18-20 Nov. 2013, pp 992 – 997.

[31] L. Zhang, G. Shou, Y. Hu and Z. Guo, "Deployment of Intrusion Prevention System Based on Software Defined Networking," Proceeding of ICCT2013 Networks and Services (SDN4FNS), 2013 IEEE, 17-19 Nov. 2013, pp 26 – 31.

[32] S. Shin, P. Porras, V. Yegneswaren, M. Fong, G. Gu1 and M. Tyson, "Fresco- Modular Composable Security Services for Software-Defined Netowrks ISOC Network and Distributed System," Security Conference in San Diego, CA, February 2013.

[33] S. Namal, I. Ahmed, A. Gurtov and M.Ylianttila, "Enabling Secure Mobility with OpenFlow," SDN for Future Networks and Services (SDN4FNS), IEEE, 11-13 November 2013, pp 1-5.

[34] A. Ghafoor and S. Muftic, CryptoNET: Software Protection and Secure Execution Environment, International Journal of Computer Science andNetwork Security, VOL, 10 No,2, February 2010.

[35] S. S. Hayward, G. O'Callaghan and S. Sezer, "SDN Security: A Survey," SDN for Future Networks and Services (SDN4FNS), 2013 IEEE, 11-13 November 2013, pp 1-7.

[36] K. Govindarajan, K. C. Meng and H. Ong, A Literature Review on Software-Defined Networking (SDN) Research Topics, Chllenges and Solutions, Fifth International Conference on Advanced Computing (ICoAC), 2013, IEEE, 18-20 Dec. 2013, pp 293 – 299.

[37] A. Bavier, N. Feamster, M. Huang, l. Peterson and J. Rexford, "In VINI Veritas: Realistic and Controlled Network Experimentation," SIGCOMM '06, September 11-15, 2006, Pisa, Italy

[38] I. Monga, E. Pouyoul and C. Guok, Software Defined Networking for big-data science Architectural models from campus to the WAN, SC Companion:High Performance Computing, Networking, Storage and Analysis (SCC), IEEE, 10-16 Nov. 2012, pp 1629 – 1635.

[39] R. Kioti, V. Kotronis and P. Smith, "OpenFlow: A Security Analysis, 21st IEEE International Conference on Network Protocols (ICNP)," 7-10 Oct. 2013, pp 1 – 6.

[40] M. F. Ahmed, C. Talhi, M. Pourzandi and M. Cheriet, "A software-Defined Scalable and Autonomous Architecture for Multi-tenancy, International Conference on Cloud Engineering (IC2E)," 2014 IEEE, 11-14 March 2014, pp 568 – 573.

[41] S. Sabnis, U. Chandrashekhar, S. Sabnis and F. Bastry, "Challenges of Securing and Enterprise and Meeting Regulatory Mandates," 12th International Telecommunications Network Strategy and Planning Symposium, November 2006, pp 1-6.

About Author (s):

Naveen Bindra has done Master of Computer Application and MBA. Currently pursuing Ph.D in computer Science. He is presently working on Security aspect in SDN.

Dr. Manu Sood is a Professor in the Department of Computer Science, HPU, India. He is Chairman of the Department with an additional charge of the Director, UIIT, HPU, Shimla. He is an Engineering graduate, has an M.Tech. degree in Information Systems from University of Delhi (DU). He also holds the degree of Ph.D, from the Faculty of Technology, DU, India. He possesses around 5 years of Industry experience and more than 22 years of academics as and administrative experience. His areas of interest in research are Software Engineering, e-Learning, MANETs and SDNs.