Indian Journal of Science and Technology, *Vol 9(32), DOI: 10.17485/ijst/2016/v9i32/100214, August 2016*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Is SDN the Real Solution to Security Threats in Networks? A Security Update on Various SDN Models

Naveen Bindra* **and Manu Sood**

Department of Computer Science, Himachal Pradesh University, Summer Hill Shimla, Himachal Pradesh, India; naveenjb@hotmail.com, soodm_67@yahoo.com

Abstract

Objectives: The concept of Software Defined Networks (SDNs) has changed the way the traditional networks used to function. The security mechanisms for these SDNs are evolving very fast. The objective of this paper is to evaluate existing significant security mechanism and to propose an inclusive secure architecture for this new generation networking. **Method/Statistical Analysis:** Network security requires a laser focused approach to tackle ever increasing vulnerabilities/ threat perceptions. With significant advances in Software Defined Networks (SDNs) research, a number of network threat mitigation mechanisms have been proposed by the researchers. The authors have evaluated these security solutions along the three important dimensions namely area of focus, mitigation solutions and drawbacks.**Findings:** This paper has attempted to highlight the prevalent threat mitigation strategies, their strongpoint features and limitations for adoption of a mitigation strategy for corresponding SDN model(s). The study divulges that no single model can tackle all the prevalent security issues and thus there is need to develop a model which can tackle most, if not all security issues. This analysis has helped the authors to propose a generalized rational security model for SDNs. **Application/Improvements:** This paper intends to initiate a debate in the community of researchers and academicians, to build a consensus on the must have security ingredients of an inclusive SDN architecture. These must-ingredients can become basis of an inclusive SDN model.

Keywords: SDN, SDN Model, SDN Architecture, Security Ingredients, Security Threats

1. Introduction

SDN has been successful in changing our perception about the networks. Decoupling of control and management planes and development of APIs, to manage and control the networks opens new frontiers to probe the unexplored areas. Network Management has really reached the next level and so are the security/vulnerability issues. A network administrator can easily shape traffic from centralized console without having to touch individual switches. Same implies to Wireless networks. Other major reasons behind its adoption at faster pace are its agility, flexibility and scalability unlike in traditional networks.

Security in SDN can be divided into three areas namely 1. Existing network threats like DoS/ DDos attacks, Trojan Worms, Hacking, stealing of sensitive information, 2. Vulnerabilities due to software used in SDNs, and c. Single point of failure due to centralized controller. A number of models have been chosen based on these three criteria. In the quest of designing new architecture for SDN, security demands utmost importance.

Section 2 of this paper elaborates on what makes SDN an ideal candidate to address security issues in the networking world, be it wired or wireless. It tries to sum up security aspects that can be addressed by SDN only and thus justifies the premise that SDN provides security solutions. Section 3 critically examines various secure SDN models and highlights the possible gaps in threat mitigation strategies used therein. The SDN solutions have been examined from the security prospective. Section 4 highlights the drawbacks of the existing secure SDN models. It further,

*Author for correspondence

propose an architecture with must have ingredients of security. Section V concludes this paper and also indicates the future plans in this direction.

2. SDN - Security Provisions for Real

2.1 Vulnerabilities in Traditional Networks and SDN

Today's network can be brought down or made ineffective by a number of threat vectors. Forged or faked traffic flows, DoS/DDoS attacks top the list of threats. A DoS or DDoS is a very common sight wherein the network comes under attack by rouge elements. This situation can suspend network services temporarily or indefinitely to the hosts connected over that network. Botnet based DDoS attacks carried out intelligently are very difficult to even detect. Single point failure of centralized controller by DoS attack or virus infection is a known problem in SDN architecture. Services are denied even to the genuine users.

Malware/Trojans/viruses are quite common in networks. IP Spoofing is creation of IP packets with dummy source in order to conceal its true source. Such packets posing as legitimate packets in DoS attacks are not detected by filters.

SDN on the other hand can have vulnerabilities which though can be taken care of. The major vulnerabilities faced by today's network have been depicted in Figure 1.

2.2 Why SDN?

Security and management issues in current networks have been discussed in this section and choosing SDN over current networks has been debated upon.

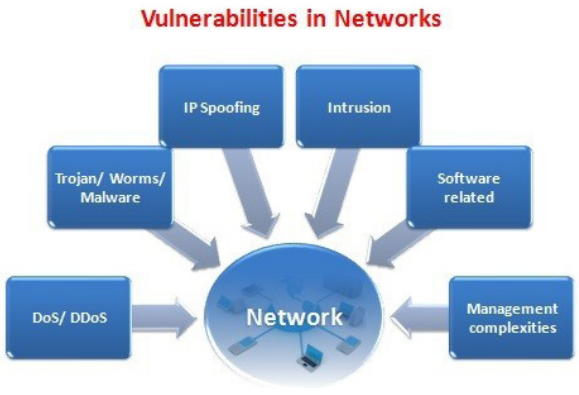

Figure 1. Vulnerabilities in traditional networks and SDN.

Managing Traditional networks is not easy. Configuring the equipment such as Access Control List (ACL), VLANs (Virtual LAN), Middle boxes, Intrusion Detection System (IDS), Intrusion Prevention System (IPS) and firewall is really a task. Any required change in the Network policy need individual changes in each equipment. The requirement to deploy fine grained policies makes it even worse. Absence of flexibility in shaping network traffic is another challenge.

Cloud computing, Wireless networks, Internet of Things (IoT) are widely used/proposed for new requirements. Clouds have heterogeneous infrastructure to manage and SDN can be an effective solution to setup and manage clouds based infrastructure[1]. Easy management of such networks is intrinsic to SDN as new feature can be built by writing new APIs.

Vulnerabilities in Wireless networks are even more intricate as compared to peer wired networks. Wireless network doesn't have the secure channel. Problems in wireless networks range from intelligent jamming attacks to exploiting configuration[2]. Benign, buggy and other malicious applications are other possible threats[3].

Intrusion Detection system and network monitoring unlike in traditional network are proposed to be implemented[4] as controller applications. Implementing network wide goals instead of individually configuring routers provides security from possible induction of errors in configuration. Thus SDN provides easy management, better security, better network wide visibility, use of less resources and increased uptime.

In traditional networks, attack on vulnerabilities of switches is a threat vector and in SDN scenario as well. An attack on control plane communication can lead to disruption of directions being given by the controller to the switches. Vulnerabilities of controller include attack on controller operating system and Controller APIs. However, these can be managed in SDN by using redundancy at controller level.

Distributed controllers[6] can be of great help to counter the possible single point of failure of controller during an attack. Elasticon, elastic distributed controller architecture addresses the scalability and reliability issues of networks. Here the controller pool works in a cluster depending on temporal and spatial network load. The mechanism[7] proposed to manage a single network device using multiple controllers in cloud scenario is even a better solution than just having multiple controllers. This approach has been effective to tackle Byzantine-Resilient faults. This paper

also talks about tackling legitimate looking DoS attacks. The facility of hot swapping can be used in preserving the status of flow table and the possible packet loss[8].

All above scenarios make SDN as a natural choice for setting up secure networks. Flexibility in SDN networks is also paving way for its adoption. All these reasons support the argument that SDN is not a fad and is likely to stay for long.

3. Security through SDN

In this section, many SDN models have been chosen and their proposed threat countering mechanisms have been analyzed. Table 1 presents a summary of the methods used

Table 1. Analysis of security in SDN models

#	Analysis of security in various SDN models		
	Vulnerability covered/ Focus area	**Mitigation Solution Proposed**	**Drawback**
1	Monitors packet flow	Security monitoring as a Service	Performance overhead
2	Attack on physical layer and DLL layer in wireless network	Moving Target Defence	Performance overhead
3	Forged faked traffic flows, vulnerabilities in switch, controller and administrative stations	Automatic trust solution for software, Oligarchic trust models, Replication of controller/ switches etc Credential verification	Proposed Solutions are not verified
4	Network packet	Flexible Sampling	*
5	Secure SDN network	Use of explicit permission set between end hosts and packet forwarding strictly according to directive of controller	Security from network threats is not proposed
6	Scalability and Reliability aspects of SDN	Dynamic Load Distribution	*
7	Legitimate looking Botnet based DDoS attacks	Application based DDoS blocking scheme using standard OpenFlow	Known vulnerabilities of OpenFlow
8	Packet loss, latency and correctness	Use of hypervisor to keep history for trouble free up gradation of controller/ switches	Problems can arise in case host OS crashes then hypervisor would not work. Redundancy should be included in the solution
9	Inter controller communication	Distributed Multi domain SDN controllers	Security of communication channel should have been proposed
10	Malware: Trojan, virus worms etc.	High speed packet detection and centralized view of network threats	Performance analysis in real scenario not done
11	Malware in Mobile	Traffic information system detects malware using SDN	Performance with bigger scale can be an issue
12	SYN Flood attack, UDP Flood attack, Christmas Tree Flood Attack, Tenant Misbehaviour	DDoS detection application using sampling Algorithm	Performance issues due to need of separate pre-filters for each DDoS type
13	Distributed Denial of Services attacks	Technique based on artificial neural network trained with features	Black box nature of artificial neural networks
14	Attacks/ hacking attempts in networks	Moving Target Defence network protection	Performance overhead
15	Privacy and network attacks	IPV6 based Moving Target Defence network protection	Performance overhead
16	Byzantine Faults happens due to failure of components of a system in an arbitrary manner	Use of cloud based multi controller system and self-healing mechanism	*
17	Integrity of workflow models	Model analysis method	*

(*Continued*)

*No Significant drawback proposed by the author

for effectively handling the threats by these SDN models and their possible drawbacks.

In SDN, centralized controller is main component which pass instructions to the dumb packet forwarding devices. But same can be prime target for disrupting network services in an organization. Further, the controller in SDN design can be a single point of failure due to target by attackers, faults or technical glitches happening over a period of time. Various mechanisms have been proposed to prevent thwart at controller[3]. The paper proposes handling of these problems by using multi-controller system and self-healing mechanism. The redundancy at controller's level[6] is proposed to ensure working of controller under all circumstances. Extensible distributed control plane[9] has been used to deal with distributed nature of networks. Controllers communicate with each other over a communication channel.

Malware is another threat for networks. They perform many unwanted activities from infecting network, steal information, sending spam to disrupting the network services. Malware is a broader term and include virus, Trojans, works, viruses, rootkit, and botnets etc. Malware detection is still a challenge in current network[10]. Campus network still find it hard to deal with speedy mitigation of malwares on the network. The author here proposes to detect the malware by correlating the distributed load. Similarly, SDN based malware detection algorithm can be used for the mobile devices[11]. The system makes real-time analysis of network traffic. The threshold calculation has not been substantiated though and it may happen that a genuine host is removed from the network. Besides, the system has been tested on a very small scale.

DDos Blocking Application (DBA)[7] is used to not only detect DDoS attacks but also resume the services after detection of attacks. These attacks are carried out targeting a specific service, utilizing only a small portion of legitimate looking traffic. Drawback of this work can be a situation like disruption of interaction of server with DBA during an attack. In this situation, the proposed secure channel would not be able to receive response from the server. In[12] have put forward some suggestions about dealing with DoS attacks in data centres. A low cost solution to detect such DDoS attacks and their mitigation in Data centers. In[13] suggest a NoX/Openflow based method to detect DDoS attacks based on traffic flow feature to distinguish between a legitimate packet and useless one. This method is efficient than others as the overhead is very small. Self-organizing maps- an artificial neural network is used for detection of DoS attacks. Thus, this mechanism goes beyond packet header analysis. The only drawback of this model is black box nature of artificial neural networks and computational burden.

An intelligent way to deal an attacker is to discourage him by using 'Moving Target Defence (MTD)'[14]. The authors here proposed to use adaptive environment in order to delay or prevent attacks. MTD is implemented here using virtualization, workload migration, network redundancy, instructions set and address space. MT6D[15] is another flavour of MTD which hides and rotates IPV6 assignments by implementing MT6D tunnelled packets. Address rotation is done to prevent the attacker from identifying host communicating with each other. The scheme cannot be used for IP V4.

Byzantine fault tolerance is another concept[16]. It may happen that systems come crashing due system fault originating due to incorrect process request, corruption of state and other inconsistencies that may come up in arbitrary ways. Such faults are known as Byzantine faults. In this scheme each switch is controlled by multiple controllers in cloud. This scheme guarantees that each switch update its forwarding table correctly even if they receives instructions from compromised controllers.

The security of network can be improved by adopting a workflow based approach[17]. Authors highlight here a very genuine issue about the existing work done in SDN. However, only processes are defined here and no emphasis has laid on workflow, which otherwise can improve the security and performance of the system. A very novel idea is where the system senses the existing state and adjusts configurations and counters the threats[18]. The counter attack on the resources of attacker though seems a radical idea but should be debated upon as miscalculation of attacking source can land one in legal tangles.

Matsumoto et al.[19] has touched upon a very critical and frequent problem of mis-configuring the controller by chance or deliberately. Such mis-configuration can, not only downgrade the performance of network significantly but also jeopardizes the network's security.

Intrusion Detection System can be made more effective in SDN scenario. Shahreza and Ganjali[4] recommend Intrusion Detection System (IDS) and network monitoring as controller applications in SDN. Use of middle box can result in huge cost savings. IDS require to access packet level information but same is not readily available in SDN controllers. Security increases by using network monitoring and SDN based control functions[20].

The authors proposed four iterations of designs of SDN. What to choose amongst these designs in a particular situation has not fully been explained.

Use of fine grained permission system can be used in order to apply minimum privilege on applications which can act as a first line of defence[21]. Security detection and intrusion prevention algorithm as OpenFlow applications[22] can be second layer of security. This algorithm combined with decisions based on fuzzy rules has shown better results. Fuzzy rules are in abundance and are arbitrary which can be possible limitation of this work.

To look into the problem of secure communication channel in SDN, a secure channel[23] for communication with controller can be used for point to point communication between controller and a node. However, problem can arise when multiple controllers communicate with single node or multiple control processes communicate with single controller, leading to a potential manipulation of network traffic. The real time monitoring via deep packet inspection has also been used for cyber security[24]. The authors used genetic algorithm for optimizing the costs and number of Deep Packet Inspection engine and network load. The obvious drawbacks of genetic algorithm are optimization problems and absence of assurance to find a global optimum etc.

The issues of network management, accuracy, reliability and scalability can also be addressed by using NEOD (Network Embedded On-line Disaster Management)[25]. Network wide disaster events' correlation is performed by NEOD manager for the applications such as verification of customer SLA and DoS attack detection. CPU utilization measurements on routers are used as an indicator for DoS attack. However this prediction cannot be reliable. In practice, the ability to handle abrupt event in real time is difficult.

The challenges in wireless networks have been addressed by Wang[26], Chaudet and Haddad[27]. Wang[26] proposes a secure and efficient way of policy distribution where SDN can be used for controlling the flow of packets to prevent them from crossing 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].

Intrusion Prevention System (IPS) can be more effective in SDN scenario than in traditional networks. Zhang et al. evaluate both scenarios[28]. IPS in SDN, is not required at ingress/egress points like in traditional networks. A secure multi-party computational framework to counter DDoS attacks[29] can be effective in situations where the possibility to detect a compromised controller is not much.

The Various SDN models discussed in this section have been studied with regard to security mechanisms; generate the scenario illustrated in Table 1 below:

4. Proposed Secure SDN Model

4.1 Limitations of Existing Work

After the analysis in the previous section, it is concluded unless we develop an inclusive architecture for security in SDN and deal with the known drawbacks of various algorithms/ solutions proposed in various SDN models, these solutions will only be partially effective.

Malware detection and mitigation though have been tackled in[10-11] by fast and efficient packet inspection mechanism. Improvement is needed in proposed packet selection method to overcome the possible performance issues.

DDoS is not only malicious in intent but can wreak havoc on networks. It can attack both application and network layers. Sabotaging a network using a botnet based DDoS attack, does not require advanced skills. Plenty of tools presently available on internet make the situation even worse. Many scenarios of DDoS attacks and have come up with many mitigation schemes namely; application based, artificial neural network with training capabilities, and use of multi-party computational network etc[7,13,28,29]. But their potential shortcomings as shown in Table 1 have scope of overcoming same.

Right now, most of SDN models are based on OpenFlow which uses TLS/ SSL channel for communications. There are known vulnerabilities of TLS/SSL and those should be dealt carefully. The vulnerabilities of TLS/SSL in OpenFlow can be overcome by using cryptographic techniques.

The threat detection is the most important amongst all the mitigation strategies as without threat detection, no mitigation mechanism works. Many solutions[1-5] are proposed for threat detection by inspection of network packets to 'permission sets' for packet forwarding and communications between two end hosts. Ways to tackle possible wrong configuration (either intentional or otherwise) has also been worked upon[19-20]. Byzantine fault tolerant system using cloud is also an important aspect

covered[16]. Disaster recovery[25], Hotswap capabilities for networking components[8] and last but not the least, the issues of wireless networks[26-27] have also been considered for this SDN architecture.

4.2 Proposed Generalized Rational Secure SDN Architecture

Table 1 expounds a number of threats covered by various models and mitigations strategies. The critical analysis of the work done in SDN has paved the way to work on an inclusive SDN architecture.

Figure 2 illustrates the extent up to which the SDN models under study have adhered to the areas of focus i.e. network threats/ vulnerabilities and mitigation strategies. The authors have used these criteria to propose the ingredients of a generalized rational architecture which are: 1. Proactive threat detection, 2. Appropriate adaptive threat mitigation strategy and 3. Resilient and fault free services even after the threat has entered the system. No single model is able to tackle all the threats and work only in a particular threat situation.

The Architecture of generalized rational secure SDN shown in Figure 3, present the 'must have ingredients'. After the extrapolation of the mitigation strategies proposed in various models, we suggest that our model, not only deals with the most possible network threats but also capable of implementing the efficient mitigation strategies. These mitigation strategies will use the optimal trade-offs between performance and effectiveness of algorithms used. Redundancy has been proposed to tackle single point of failure of SDN components e.g. controllers. Moreover, this architecture takes into account the auto-healing mechanism which makes it work, even

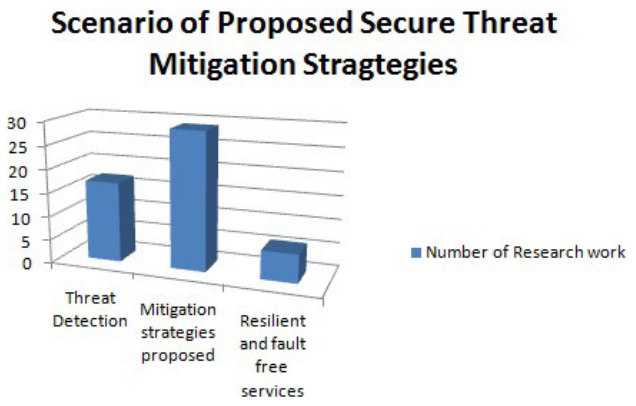

Figure 2. Overall scenario of mitigation strategies studied in section III.

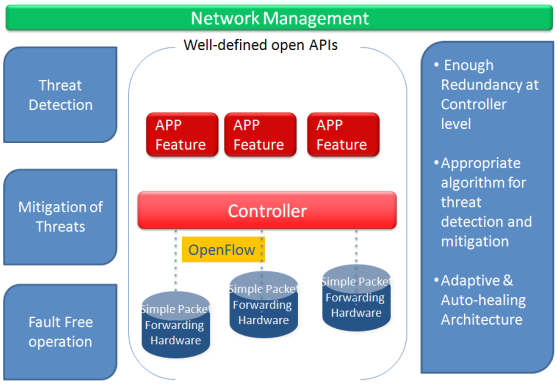

Figure 3. Generalized rational secure SDN architecture

same gets infected or comes under attack. Security follows management and network management layer will thus be designed with utmost care and without any complexities. This makes them fault free and management friendly. In a nutshell, this architecture may stand out from the models analyzed in this paper for the security related issues, as it is intended to be more inclusive and able to handle the most of the threats.

5. Conclusion and Future Work

The proposed work was aimed to develop a comprehensive secure SDN model. Various security aspects related to SDN were found in the literature but none of the models can qualify for same. The existing work in security of SDN was evaluated against the three axis plane namely 1. Threat Detection 2. Mitigation Strategies and 3. Fault Free Services. It has been gaged that most of the vulnerabilities covered are Malwares, IP Spoofing, DDoS attacks, Byzantine faults, possible single point of failures and intrusions etc. The mitigation strategies include the redundancies at controller level, deep packet inspection, sampling techniques for efficient threat detection, secure channel for intra controller communications, network flows, moving target defence for discouraging the attack, and DDoS blocking schemes. The main drawbacks are the overhead and performance issues for using a particular threat mitigation strategy besides the already known limitations of algorithms on which these solutions are founded.

Based on these inputs, the authors were inclined to propose a 'generalize rational secure SDN model'. The salient features of this model are 1. Proactive threat detection, 2. Appropriate adaptive threat mitigation

strategy and 3. Resilient and fault free services even if the threat enters the system. Presently the authors are working on this secure SDN model which can mitigate most of the network threats.

6. References

1. Shin S, Gu G, CloudWatcher: Network security monitoring using openflow in dynamic cloud networks. Proceedings of 20th IEEE International Conference on Network Protocols (ICNP); 2012. p. 1–6.
2. Corbett C, Uher J, Cook J, Dalton A. Countering intelligent jamming with full protocol stack agility, security and privacy. IEEE. 2014; 12(2):44–50.
3. Kreutz D, Ramos FMV, Verissimo P. Towards secure and dependable software-defined networks. Proceedings of HotSDN'13; Hong Kong, China. 2013 Aug 16.
4. Shirali-Shahreza S, Ganjali Y, FleXam: Flexible sampling extension for monitoring and security applications in openflow. Proceedings of HotSDN'13; Hong Kong, China. 2013 Aug 16.
5. Casado M, Freedman MJ, Pettit J, Luo J, Mckeon N, Shenker S. Ethane: Taking control of the enterprise. Proceedings of SIGCOMM 07; Kyoto, Japan. 2007 Aug 27–31.
6. Dixit A, Hao F, Mukherjee S, Lakshman TV, Kompella R. Towards an elastic distributed SDN controller. Proceedings of HotSDN 13; Hong Kong, China. 2013 August 16.
7. Lim S, Ha J, Kim H, Kim Y, Yang S. A SDN-oriented DDoS blocking scheme for botnet-based attacks. Proceedings of Ubiquitous and Future Networks (ICUFN); 2014. p. 63–8.
8. Vanbever L, Reich J, Benson T, Foster N, Rexford J. Hot swap: Correct and efficient controller upgrades for software-defined networks. Proceedings of HotSDN'13; Hong Kong, China. 2013 Aug.
9. Phemius K, Bouet M, Leguay J. DISCO-distributed multi-domain SDN controllers. IEEE Network Operations and Management Symposium (NOMS); 2014 May 5-9. p. 1–4.
10. Abaid Z, Rezvani M, Jha S. Monitor malware: An SDN-based framework for securing large netowrks. CoNext Student Workshop; Sydney, Australia. 2014.
11. Jin R, Wang B. Malware detection for mobile devices using software-defined networking. IEEE 2nd GENI Research and Educational Experiment Workshop (GREE); 2013 Mar 20-22; p. 81–8.
12. Krishnan R, Krishnaswamy D, Medysan D. Behavioral security threat detection strategies of data center switches and routers. Proceedings of IEEE 34th International Conference on Distributed Computing Systems Workshops (ICDCSW); 2014. p. 82–7.
13. Braga R, Mota E, Passito A. Lightweight DDoS flooding attack detection using NOX/ openflow. Proceedings of 35th Conference on IEEE Local Computer Networks (LCN); 2010 Oct 10-14. p. 408–15.
14. Kampanakis P, Perros H, Beyene T. SDN-based solutions for moving target defense network protection. IEEE Proceedings of 15th International Symposium WoWMoM; 2014 Jun 19. p. 1–6.
15. Dunlop M, Groat S, Urbanski W, Marchany R, Tront J. MT6D: A moving target IPv6 defens. Proceedings of Military Communication Conference; Baltimore, MD. 2011 Nov 10. p. 1321–6.
16. Li H, Li P, Guo S, Nayak A. Byzantine-resilient secure software-defined networks with multiple controllers in cloud. IEEE Transactions on Cloud Computing. 2014 Sept 5; 436–47.
17. He J, Guand Z, Xu F. Role-based modeling and analysis of workflow for SDN. Proceedings of International Conference on Business Management and Electronic Information (BMEI); Guangzhou, China. 2011. p. 254–8.
18. Hand R, Ton M, Keller E. Active security. Proceedings of Hotnets; USA. 2013 Nov 21-22. p. 7–12.
19. Matsumoto S, Hitz S, Perrig A. Fleet: Defending SDNs from malicious administrators. ACM Proceedings of HotSDN; Chicago II, USA. 2014. p. 103–8.
20. Zaalouk A, Khondoker R, Marz R, Bayarou K. OrchSec: An orchestrator-based architecture for enhancing network-security using network monitoring and sdn control functions. IEEE Network Operations and Management Symposium (NOMS); 2014. p. 1–9.
21. Wen X, Chen Y, Hu C, Shi C, Wang Y. Towards a secure controller platform for openflow applications. Proceedings of ACM SIGCOMM HotSDN'13; Hong Kong, China. 2013 Aug 16. p. 171–2.
22. Dotcenko S, Vladyko A, Latenko I. A fuzzy logic-based information security management for software-defined networks. IEEE 16th International Conference on Advanced Communication Technology (ICACT); 2014. p. 167–71.
23. Sezer S, Scott-Hayward S, Chouhan PK, Fraser B, Lake D, Finnegan J, Viljoen N, Miller M, Rao N. Are we ready for SDN? Implementation challenges for software-defined networks. IEEE Communications Magazine. 2013 Jul. p. 36–43.
24. Bouet M, Leguay J, Conan V. Cost-based placement of virtualized deep packet inspection functions in SDN. IEEE Proceedings of MILCOM; 2013 Nov 18-20. p. 992–7.
25. Song S, Hong S, Guan X, Choi B, Choi C. NEOD: Network embedded on-line disaster management framework for software defined networking. IFIP/IEEE International Symposium on Integrated Network Management; 2013 May 27-31. p. 492–8.
26. Wang H. Authentic and confidential policy distribution in software defined wireless network. IEEE Proceedings

of International Wireless Communications and Mobile Computing Conference (IWCMC); 2014. p. 1167–71.
27. Chaudet C, Haddad Y. Wireless software defined networks: Challenges and opportunities. IEEE Proceedings of International Conference on Microwaves, Communications, Antennas and Electronic Systems (COMCAS); Tel Aviv, Israel. 2013 Oct 1-5. p. 21–3.
28. Zhang L, Shou G, Hu Y, Guo Z. Deployment of intrusion prevention system based on software defined networking. IEEE Proceeding of ICCT Networks and Services (SDN4FNS); 2013 Nov 17-19. p. 26–31.
29. Jagadeesan NA, Pal R, Nadikuditi K, Huang Y, Shi R, Yu M. A secure computation framework for SDNs. Proceedings of HotSDN; 2014. p. 209–10.