Penerbit Akademia Baru

Journal of Advanced Research in Computing and Applications

Journal homepage: www.akademiabaru.com/arca.html
ISSN: 2462-1927

A security trending review on software define network (SDN)

Open Access

Mohd Zafran Abdul Aziz [1,2,*], Koji Okamura [3]

[1] Faculty of Electrical Engineering, Universiti Teknologi Mara, 40450, Shah Alam, Selangor, Malaysia
[2] Department of Advanced Information Technology, Graduate School of Information Science and Electrical Engineering, Kyushu University, Japan
[3] Research Institute Information Technology, Kyushu University, Japan

ARTICLE INFO

Article history:
Received 17 March 2017
Received in revised form 31 March 2017
Accepted 1 April 2017
Available online 9 May 2017

Keywords:
SDN, Security Trending Review, Software Define Network, SMTP, Spam, Botnet, SDN Security, OpenFlow, Mininet

ABSTRACT

This work presents a comprehensive literature review on security for SDN. We revisit the existing works for network security in the SDN such as mitigation attack from D/DoS, botnet, spam etc. Later, we discuss the SDN and its hype cycle for emerging technologies. SDN offers a high level of network abstraction management as well as a centralized security solution. Due to robustness and flexibility of SDN architecture, many researchers have chosen SDN. It can help to prevent D/DoS attacks in a single SDN domain (e.g. LAN, WAN) or multiple integrated SDN domains (e.g. MAN). This review paper will drive a research topics on network security using SDN technologies. Various study on SDN communication and infrastructure, but this paper focuses more on network security based on technical analysis and machine learning using Artificial Intelligent. Based on research and development trending in the literature review, SDN is considered for the Gartner's hype cycle for emerging technologies.

1. Introduction

SDN is an architecture for multi devices communication in integrated networks. It provides manageable network infrastructures that consist millions of computing devices and software. In this work, we present a comprehensive literature review on SDN with consideration of security in the architecture. We revisit the existing works on security for the SDN such as D/DoS, botnet, spam etc. Later, we discuss the SDN and its hype cycle for emerging technologies. We divided this work into four sections. The first Introduction section provides an introduction to this work. It follows the Related Works section that discusses SDN, D/DoS, botnet and spam attacks. It also shows detection and prevention methods in a comparison table. After that, we discuss the comparison table as well as SDN's hype cycle in the Discussion section. Finally, we conclude this work and propose a suggestion in the Conclusion section.

* *Corresponding author.*
E-mail address: zafran.fke@gmail.com (Mohd Zafran Abdul Aziz)

2. Literature Review

This section will discuss SDN background and related literatures. The following subsection revisits the SDN architecture. After that security reviews on SDN will be discussed.

2.1 Software Define Network (SDN)

SDN is an architecture for multi devices communication in integrated networks. In the initial stage, it allows multiple LANs devices and systems to be integrated into WAN networks. The first SDN began after Java language released by Sun Microsystem, which AT&T Labs Geoplex project that used Java to program APIs for implementation middleware networking [1]. The Geoplex provided open networking standard for network integrations and communications such as system managements and provisions, integrated security and system authentication, network monitoring etc. By 2011, Open Networking Foundation (ONF) develops OpenFlow for SDN [2]. The ONF provides SDN resources (e.g. switch specification) for product manufacturer and software developer to implement SDN using the OpenFlow standard and protocol [3].

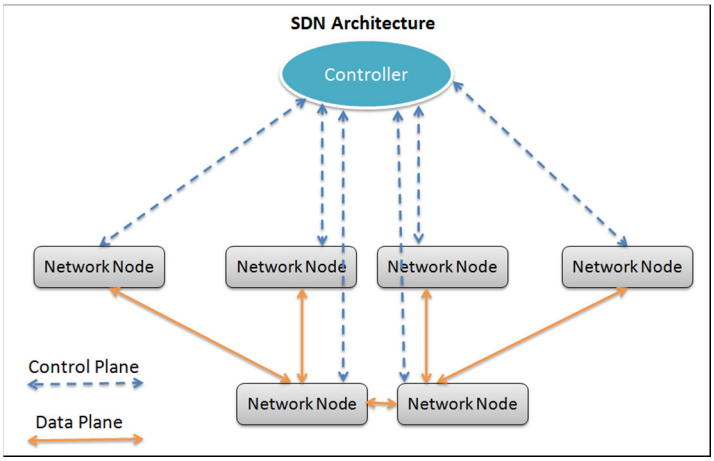

Fig. 1. SDN architecture [6]

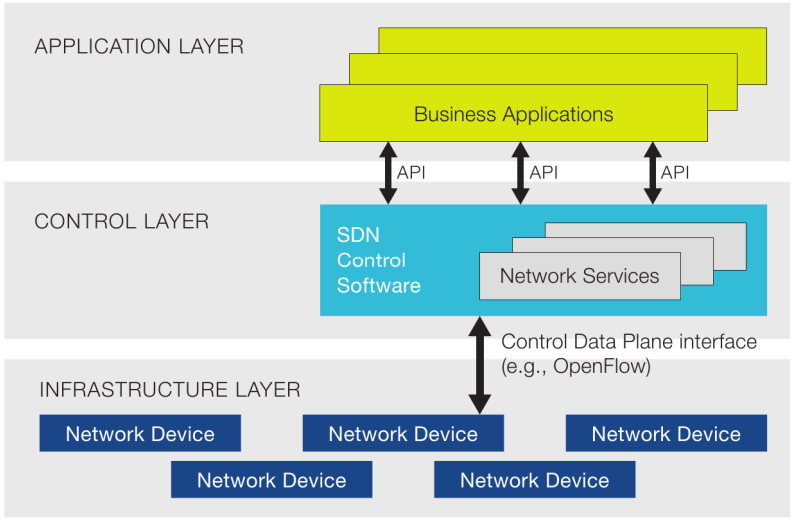

Fig. 2. SDN's stacks [7]

Figures 1 and 2 show a general SDN architecture and stacks. In SDN topology, all network nodes or devices are controlled using a control plane. The architecture splits the control plane from actual network data and routing process (data plane). The infrastructure layer communicates with SDN Controller using Control Data Plane (CDP) API (e.g. OpenFlow). All nodes or routers in the SDN network will use the CDP API for all control plane communication. The control layer consists of SDN Control Software or Controller, which extract information from the infrastructure layer such as a list of all devices in the SDN network and its states. It does not provide the entire information of all connected devices, but it provides an abstract view of the SDN network and topology. The application layer uses information from the control layer for a network abstraction administrative such as network analytics; network, system and topology managements etc [4, 5].

2.2 SDN Security review

Distributed systems such as cloud computing and Internet of Things (IoT) are not the main factors for organizations to migrate theirs network infrastructure into SDN, another main reason is a network security that offered by the SDN [8, 9]. The SDN allows an abstraction of network security that provides a central authority in a network, which previously hard to be done by traditional distributed networking systems and infrastructures [2, 3]. There are also new security problems introduce by an implementation the SDN in network infrastructure, but we are not going to discuss in this publication. One may refer to [9–12] for further examinations regarding these security problems. The following paragraphs will discuss security threats and countermeasures that are related to SDN.

Kim *et al*. [13] proposed a prototype for abnormal network traffic detection. It uses an aggregation of packets that using identical flow, which can be used to detect an attack when there are changes in traffic patterns. Changes in traffic patterns such as port number and payload can be detected using this method. Xiao *et al*. [14] present a method to identify attacker signature using an active probing scheme. It analyzes delay in TTL for each router in networks that can use to identify SYN flooding. Luo *et al*. [15] proposed a method to detect SMTP anomaly using collection and aggregation of packet deviations. The method does not require to store all traffic data, it uses a leaky integrate-and-fire model (or weightage sum) to maintain previous traffic knowledge. Naksomboon *et al*. [16] proposed a behavior method to filter known spammer's behaviors in filtering rules. The authors used random forest algorithm and Spam Assassin Corpus database in their works. Kakavelakis *et al*. [17] implemented a botnet analysis using machine learning, SMTP Mail Transport Agent (MTA). It (or named SpamFlow) can be integrated into transport-layer for packet analysis. Still *et al*. [18] revisited the state of the art in DDoS for attack, detection, protection and mitigation in SMTP server.

Sahu *et al*. [19] have explored a performance analysis on DoS attack using SYN flooding attack. The results have shown that memory and CPU usage burst heavily when attacked. Duan *et al*. [20] monitored outgoing message by zombie machines for spam detection, which used sequential probability ratio test algorithm. Nevlud *et al*. [21] proposed a method to detect network anomaly using machine learning systems. The authors used data mining framework, namely WEKA. It is used for network analysis by two algorithms: decision tree and Bayesian networks. The purpose of this work is to find and build efficient knowledge structures of network attacks. Petkov *et al*. [22] investigated an entropy of aggregated network traffics for entropy fingerprints. Channegowda *et al*. [23] proposed service on demand (SoD) architecture in SDN. Shin *et al*. [24] developed an OpenFlow security application (named FRESCO) for managing security modules in SDN. The FRESCO provides security architecture as well as API for security scripting and translation, database and event management, and instance execution.

Hoque *et al*. [25] discussed tools used by attackers and security admin in SDN. The authors revisit machine learning algorithm, flow-based features for botnet detection using a predefined dataset. The dataset consists of SMPT Spam and UDP Storm and it successfully detected with rate 75%. Ioanidis *et al*. [26] showed an implementation of Pushback router to reduce DDoS attacks in a network. The implementation was done in FreeBSD. It uses congestion control problems as a sign for DDoS attacks and flash crowds. Lim *et al*. [27] proposed to utilize SDN for DDoS attack detection and prevention. The authors discuss a method to block the DDoS attack using OpenFlow in SDN controller. It was simulated in POX controller using Mininet emulator. Schafer [28] used geolocation and country to detect an anomaly that can be used to identify spam email. A novel contribution, Theoretical Geographical Travelling Speed (TGTS) method is proposed in his work. Sochor [29] revisited the existing methods to detect and prevent spam messages. Multi-layer protection technique such as blacklisting and greylisting was discussed. Beigi *et al*. [30] reexamined flow-based for botnet detection, which also studies its effectiveness in detection using a predefined dataset. Ouyang *et al*. [31] studied spam filtering pipeline for finding its accuracy and tradeoff in four layers. The authors used three decision trees: packet features, flow features and the combination of both features.

Chen *et al*. [9] integrated entropy measurement for flooding detections in mail systems. It studies an entropy in round-trip time (RTT) and retransmission timeout (RTO) to detect dangerous traffics. The entropy can help to improve malicious mail analysis and detection for protocols: SMTP, IMAP4, POP3 and HTTPS. Sahay *et al*. [32] proposed an implementation of a distributed collaboration framework for sharing information that can be used to mitigate DDoS in SDN. A client can request from Internet Service Provider (ISP) for a mitigation service by downloading (and installing) security middleboxes in a client-side. The security middleboxes will perform attack detection and analysis at the client-side, while sharing collected information on attack with ISP. It can be done in autonomous communication, which to protect the entire SDN infrastructures from DDoS attacks. Jeong *et al*. [33] propose security services in SDN for a centralized firewall and DDoS mitigation systems. Yan *et al*. [34] reviewed DDoS attacks on cloud computing and then how to prevent the DDoS attacks by implementing SDN in the cloud computing. Holl [35] discussed multiple methods to detect and prevent DDoS attacks in SDN such proactive and reactive defenses, and post-attack analysis. Yan *et al*. [36] presented a survey on SDN, DDoS in cloud computing. The authors found that DDoS attacks on cloud computing are increasing because of "On-Demand Self-Service Leading to Botnets Outbreak… Broad Network Access and Rapid Elasticity Leading to More Immense, Flexible, and Sophisticated DDoS Attacks… Resource Pooling Leading to the Victims More Vulnerable to DDoS Attacks" [36]. To reduce such attacks, the authors have suggested implementing SDN in cloud computing because its capability to deal with dynamic network architectures.

The summary of literature reviews is presented in Table 1. The Table 1 also included many literatures that are not discussed in the previous paragraphs.

Table 1
A summary of literature discusses D/DOS and spam attacks

Authors	Attacks	Detection and Prevention
Kim [13]	D/DoS, abnormal network traffic	Packets aggregation and identical flow
Xiao [14]	SYN flooding	Active probing scheme
Luo [15]	SMTP spam	Weightage sum of traffics
Bencsáth [37]	DoS, SMTP spam	Content filtering applications harm server performance
Beverly [38]	Spam	Extraction of email TCP features, SpamFlow
A. Al-Bataineh [39]	Reviews on: Botnet, spam	Monitoring outgoing traffic, DBSpam, SpamFlow, signatures

Hu [40]	DoS and Worms	Cisco NetFlow, entropy based adaptive flow aggregation algorithm, detect source of attack in clusters
Smith [41]	Spambots	Entropy of packets distribution skewness
Naksomboon [16]	Email spam	Spammer's behaviors, random forest algorithm
Ehrlich [42]	Email spam, spam bots	Network flow data, entropy-based traffic analysis
Kakavelakis [17]	D/Dos, SMTP spam	Machine learning analysis
Still [18]	DDoS, zombie spoofs, SMTP spam, SYN flooding etc.	Detections: pattern, anomaly and 3rd party database. Defenses: over provisioning, routing control, currency assumption and authentication, Push back.
Sahu [19]	DoS, SYN flooding	Exhaustive memory and CPU usage
Duan [20]	DDoS, spam, zombie	Monitoring outgoing messages by sequential probability ratio test algorithm
Suwa [43]	Botnet, spam mail	DNS record characteristics and behavior of DNS servers, blacklist
Nevlud [21]	Abnormal network traffic	Machine learning systems, WEKA, decision tree and Bayesian networks
Petkov [22]	-	Entropy fingerprints
Channegowda [23]	-	Service on demand (SoD) in SDN
Lin [44]	SMTP spam	Tools: Bro IDS, Bloom filters
Jian-Qi [45]	DoS	Dynamic entropy-based model for anomalies detection
Gada [46]	Spam	Dynamic whitelist in layer 3 switch.
Zempoaltecatl-Piedras [47]	Network anomaly	Anomaly traffic filtering - Method of Entropy Spaces (MES), flow-level entropy space
Navaz [48]	DDoS	Combine entropy and anomaly detection for multilevel DDoS, share signatures with Cloud Service Provider (CSP)
Phemius [49]	Network attacks	Distributed SDN Control plane (DISCO) for WAN, analysis on inter-domain topology disruption
Shin [24]	-	Security framework in SDN, FRESCO
Sochor [50]	Spam	Blacklisting
Phemius [51]	Measure link latencies	OpenFlow controller
Cartier [52]	DDoS, SMTP flooding	Optimize connection timeout (TTL) configuration
Scott-Hayward [8]	Survey on: SDN security	Attacks and security on SDN
Rathi [53]	Spam flooding	Analyze existing methods for spam mail detection e.g. support vector machine, naïve Bayes, decision tree, feature selection, classification and prediction
Hoque [19]	Reviews on: SDN security, botnet	machine learning algorithm, flow-based
Beigi [30]	Botnet, DDoS, SMTP Spam, UDP Storm	Flow-based features
Ioannidis [26]	DDoS, flash crowds	Congestion-control problems, Pushback
Lim [27]	DDoS	POX/SDN controller, Mininet
Schafer [28]	Spam email	Geo location and country
Sochor [29]	Reviews on: Spam message	Blacklisting and greylisting
Beigi [30]	Botnet, SMTP spam	Flow-based
Ouyang [31]	Spam email	Spam filtering pipeline. Packet features, flow features and combined both
Chen [54]	Botnet, IRC	Two-level correlation for the same anomaly
Vizváry [55]	Reviews on: DDoS in SDN	Malicious traffics
Giotis [56]	Network anomaly and DDoS in SDN	OpenFlow with Remote Triggered Black-Hole (RTBH) routing

Oktian [57]	DoS, IP/MAC spoofing, bulky/garbage message	Simulation of attacks by OpenFlow in Mininet, block all known unused resources in SDN
Hoque [25]	Reviews on: attacks and defensive techniques in networks	Anomaly detection, scanning tools, attacking tools
Smeliansky [10]	-	Security by SDN architecture
Geetha [58]	DoS, SYN flooding attack	Analysis on SYN flooding attack
Özçelik [59]	Vulnerability in entropy based detection method	Attacker avoids detection
Chen [14]	SYN flooding	Entropy RTT and RTO
Sahay [32]	DDoS	Distributed collaboration framework in SDN, ISP and its client sharing information
Jeong [33]	DDoS	Centralized firewall and mitigation systems in SDN
Graham [60]	Botnet	Flow export for identification botnet command control
Yan [34]	DDoS	Existing method to prevent DDoS in SDN e.g. attacks on application, control and infrastructure layers
Holl [35]	DDoS, botnet	Proactive and reactive defenses, and post-attack analysis
Kim [61]	DDoS	Implementation of centralized firewall and mitigation system in SDN
Seeber [62]	DDoS	Redirect identified suspicious traffics to IDS for further inspection in SDN.
Yan [36]	Survey on: DDoS in SDN and cloud computing	Implementation of SDN helps to minimize DDoS in cloud computing – based on SDN features.
Ruffy [63]	Security threat modeling	Implementation of STRIDE threat model to test SDN security.
Mir [64]	Network performance	Scalability and performance of SDN for Data Center Network (DCN).
Teo [65]	Campus network security policies	SDN controllers deployment experience at Cornell University. Limitation of SDN in the actual deployment.
Saxena [66]	SDN architecture vulnerability	New security vulnerability by SDN whereby it does not exist on traditional architectures.

3. Discussion

This section will summarize the literatures. From the Table 1, one may observe the trends of research works by various researchers. In the earliest stage, all methods to detect and prevent D/DoS attacks by botnets are not centralized. It happened because, at that moment, there is no open standard for the entire network (e.g. WAN) to be properly managed (in term of security). Due to independence and incompatible with each other, it is hard to prevent botnet attacks on the Internet. A new paradigm emerging, and it begins to change traditional networking architecture, namely SDN. In 2011, OpenFlow which is an implementation of the SDN [4] is available for multi devices communication in centralized and integrated networks.

One may observe in 2013, researchers began to integrate SDN for a high level of network abstraction management as well as a centralized security solution. Due to robustness and flexibility of SDN architecture, researchers or information security officers can implement the existing detection and prevention methods as an application or services in SDN controller. This is a blessing,

and many researchers have seized it by re-innovate (or integrate) the existing security methods into the SDN. This is nothing news, but it helps to prevent D/DoS attacks in a single SDN domain (e.g. LAN, WAN) or multiple integrated SDN domains (e.g. MAN). When a network is transparently less vulnerable to the D/DoS attacks (e.g. botnet or zombie), it will produce a correlation in reducing spam email in the SDN domains. That can be a reason why researchers focusing on detecting and preventing D/DoS in SDN. One may see this security trending using SDN in the Table 1.

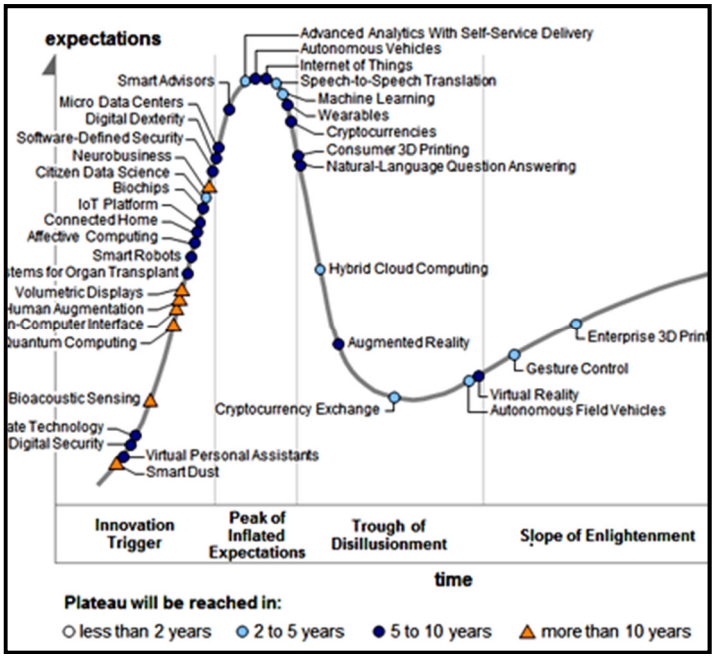

Fig. 3. Gartner's hype cycle for emerging technologies (August 2015) [63].

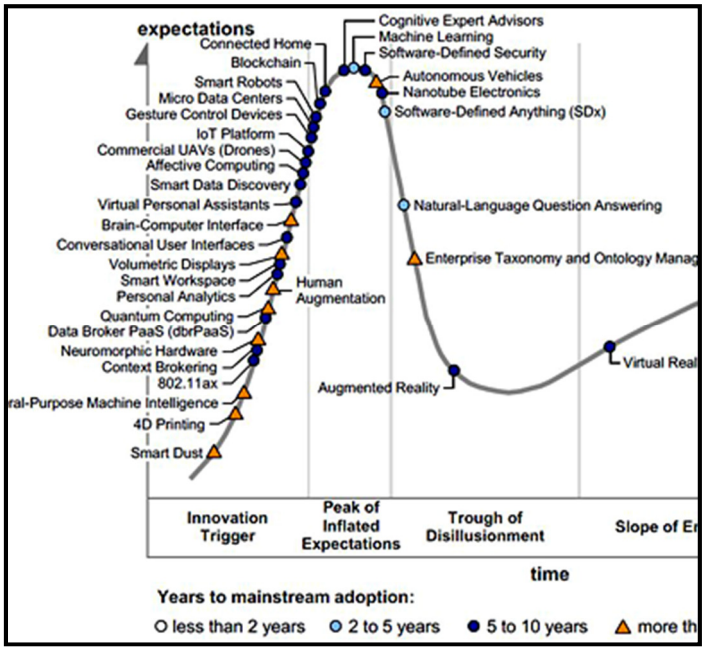

Fig. 4. Gartner's hype cycle for emerging technologies (August 2016) [69].

The purpose of this works is to explore information security research works before and during SDN period. Based on the literature, SDN's paradigm and its developer, Open Networking Foundation (ONF) having a good momentum. Network developers and researchers are believed in it, and continue to devote their effort. We believe that, by this or in the next year, SDN will be still near to the peak of a hype cycle for emerging technologies. It is because Software-defined Security (SDS) [67] (refer to Table 1 is a sibling of SDN and it can be implemented in SDN [68] as well as Software-defined Anything (SDx) (Refer to Figure 4). Both used similar paradigm in their design.

4. Conclusion

We have presented the literature review on SDN from 2004 until 2016. After three years of OpenFlow being deployed, many research works that related to D/DoS, spam and botnet are moving toward SDN security based model. SDN offers a high level of network abstraction management as well as a centralized security solution. Due to robustness and flexibility of SDN architecture, many researchers have chosen SDN. We also believe that, by the next year, SDN will be included in the Gartner's hype cycle for emerging technologies. To be in the mainstream, we hope fellow researchers will continue to investigate security on SDN. One must take this opportunity before SDN begin to fall in the hype cycles before it too late.

References

[1] G. Vanecek, "GeoPlex: Universal Service Platform for IP Network-based Services," 1997.
[2] Fundation, Open Networking. "Software-defined networking: The new norm for networks." *ONF White Paper* 2 (2012): 2-6.
[3] O. N. Foundation, "OpenFlow," 2016. [Online]. Available: https://www.opennetworking.org/sdn-resources/openflow/57-sdn-resources/onf-specifications/openflow?layout=blog. [Accessed: 29-Jan-2016].
[4] Park, Sae Hyong, Byungjoon Lee, Jaeho You, Jisoo Shin, Taehong Kim, and Sunhee Yang. "RAON: Recursive abstraction of OpenFlow networks." In *Software Defined Networks (EWSDN), 2014 Third European Workshop on*, pp. 115-116. IEEE, 2014.
[5] Gurbani, Vijay K., Michael Scharf, T. V. Lakshman, Volker Hilt, and Enrico Marocco. "Abstracting network state in Software Defined Networks (SDN) for rendezvous services." In *Communications (ICC), 2012 IEEE International Conference on*, pp. 6627-6632. IEEE, 2012.
[6] Mouli, "Why SDN Concepts Need To Extend Into The Wan," 2016. [Online]. Available: http://www.aryaka.com/blog/why-sdn-concepts-need-to-extend-into-the-wan/. [Accessed: 31-Jan-2016].
[7] SDxCentral, "Inside SDN Architecture," 2016. [Online]. Available: https://www.sdxcentral.com/resources/sdn/inside-sdn-architecture/. [Accessed: 31-Jan-2016].
[8] Scott-Hayward, Sandra, Gemma O'Callaghan, and Sakir Sezer. "SDN security: A survey." In *Future Networks and Services (SDN4FNS), 2013 IEEE SDN For*, pp. 1-7. IEEE, 2013.
[9] Kloti, Rowan, Vasileios Kotronis, and Paul Smith. "Openflow: A security analysis." In *Network Protocols (ICNP), 2013 21st IEEE International Conference on*, pp. 1-6. IEEE, 2013.
[10] Smeliansky, R. L. "SDN for network security." In *Science and Technology Conference (Modern Networking Technologies)(MoNeTeC), 2014 First International*, pp. 1-5. IEEE, 2014.
[11] Lange, Stanislav, Steffen Gebert, Thomas Zinner, Phuoc Tran-Gia, David Hock, Michael Jarschel, and Marco Hoffmann. "Heuristic approaches to the controller placement problem in large scale SDN networks." *IEEE Transactions on Network and Service Management* 12, no. 1 (2015): 4-17.
[12] Wang, Shu-ling, Ji-han Li, Yun-yong Zhang, and B. Fang. "Research on SDN architecture and security." *Telecommunications Science* 29, no. 3 (2013): 117-122.
[13] Kim, Myung-Sup, Hun-Jeong Kong, Seong-Cheol Hong, Seung-Hwa Chung, and James W. Hong. "A flow-based method for abnormal network traffic detection." In *Network operations and management symposium, 2004. NOMS 2004. IEEE/IFIP*, vol. 1, pp. 599-612. IEEE, 2004.
[14] Xiao, Bin, Wei Chen, Yanxiang He, and EH-M. Sha. "An active detecting method against SYN flooding attack." In *Parallel and Distributed Systems, 2005. Proceedings. 11th International Conference on*, vol. 1, pp. 709-715. IEEE, 2005.

[15] Luo, Hao, Binxing Fang, and Xiaochun Yun. "Anomaly detection in SMTP traffic." In *Information Technology: New Generations, 2006. ITNG 2006. Third International Conference on*, pp. 408-413. IEEE, 2006.
[16] Naksomboon, S., C. Charnsripinyo, and N. Wattanapongsakorn. "Considering behavior of sender in spam mail detection." In *Networked Computing (INC), 2010 6th International Conference on*, pp. 1-5. IEEE, 2010.
[17] Kakavelakis, Georgios, and Joel Young. "Auto-learning of SMTP TCP Transport-Layer Features for Spam and Abusive Message Detection." In *LISA*, pp. 18-18. 2011.
[18] Still, Michael, and Eric C. McCreath. "DDoS protections for SMTP servers." *International Journal of Computer Science and Security (IJCSS)* 4, no. 6 (2011): 537.
[19] Sahu, Rakesh Kumar, and Narendra S. Chaudhari. "A performance analysis of network under SYN-flooding attack." In *Wireless and Optical Communications Networks (WOCN), 2012 Ninth International Conference on*, pp. 1-3. IEEE, 2012.
[20] Duan, Zhenhai, Peng Chen, Fernando Sanchez, Yingfei Dong, Mary Stephenson, and James Michael Barker. "Detecting spam zombies by monitoring outgoing messages." *IEEE Transactions on dependable and secure computing* 9, no. 2 (2012): 198-210.
[21] Garcia-Teodoro, Pedro, J. Diaz-Verdejo, Gabriel Maciá-Fernández, and Enrique Vázquez. "Anomaly-based network intrusion detection: Techniques, systems and challenges." *computers & security* 28, no. 1 (2009): 18-28.
[22] Petkov, Vladislav, Ram Rajagopal, and Katia Obraczka. "Characterizing per-application network traffic using entropy." *ACM Transactions on Modeling and Computer Simulation (TOMACS)* 23, no. 2 (2013): 14.
[23] Channegowda, M., R. Nejabati, S. Peng, N. Amaya, G. Zervas, Y. Shu, M. Rashidifard, and D. Simeonidou. "Design and demonstration of multi-domain, multi-technology software defined networks for high-performance cloud computing infrastructure." In *Optical Communication (ECOC 2013), 39th European Conference and Exhibition on*, pp. 1-3. IET, 2013.
[24] S. Shin, P. Porras, V. Yegneswaran, and M. Fong, "FRESCO: Modular Composable Security Services for Software-Defined Networks.," in *ISOC Network and Distributed System Security Symposium* 2, 2013.
[25] Hoque, Nazrul, Monowar H. Bhuyan, Ram Charan Baishya, D. K. Bhattacharyya, and Jugal K. Kalita. "Network attacks: Taxonomy, tools and systems." *Journal of Network and Computer Applications* 40 (2014): 307-324.
[26] Ioannidis, John, and Steven M. Bellovin. "Implementing Pushback: Router-Based Defense Against DDoS Attacks." In *NDSS*. 2002.
[27] Lim, Sharon, J. Ha, H. Kim, Y. Kim, and S. Yang. "A SDN-oriented DDoS blocking scheme for botnet-based attacks." In *Ubiquitous and Future Networks (ICUFN), 2014 Sixth International Conf on*, pp. 63-68. IEEE, 2014.
[28] Schäfer, Carlo. "Detection of compromised email accounts used by a spam botnet with country counting and theoretical geographical travelling speed extracted from metadata." In *Software Reliability Engineering Workshops (ISSREW), 2014 IEEE International Symposium on*, pp. 329-334. IEEE, 2014.
[29] Sochor, Tomas. "Overview of e-mail SPAM elimination and its efficiency." In *Research Challenges in Information Science (RCIS), 2014 IEEE Eighth International Conference on*, pp. 1-11. IEEE, 2014.
[30] Beigi, Elaheh Biglar, Hossein Hadian Jazi, Natalia Stakhanova, and Ali A. Ghorbani. "Towards effective feature selection in machine learning-based botnet detection approaches." In *Communications and Network Security (CNS), 2014 IEEE Conference on*, pp. 247-255. IEEE, 2014.
[31] Ouyang, Tu, Soumya Ray, Mark Allman, and Michael Rabinovich. "A large-scale empirical analysis of email spam detection through network characteristics in a stand-alone enterprise." *Computer Networks* 59 (2014): 101-121.
[32] Sahay, Rishikesh, Gregory Blanc, Zonghua Zhang, and Hervé Debar. "Towards autonomic ddos mitigation using software defined networking." In *SENT 2015: NDSS Workshop on Security of Emerging Networking Technologies*. Internet society, 2015.
[33] Jeong, Jaehoon, Jihyeok Seo, Geumhwan Cho, Hyoungshick Kim, and Jung-Soo Park. "A Framework for Security Services based on Software-Defined Networking." In *Advanced Information Networking and Applications Workshops (WAINA), 2015 IEEE 29th International Conference on*, pp. 150-153. IEEE, 2015.
[34] Yan, Qiao, and F. Richard Yu. "Distributed denial of service attacks in software-defined networking with cloud computing." *IEEE Communications Magazine* 53, no. 4 (2015): 52-59.
[35] Holl, Patrick. "Exploring DDoS Defense Mechanisms." *Network* 25 (2015).
[36] Yan, Qiao, F. Richard Yu, Qingxiang Gong, and Jianqiang Li. "Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges." *IEEE Communications Surveys & Tutorials* 18, no. 1 (2016): 602-622.
[37] Bencsáth, Boldizsár, and Miklós Aurél Rónai. "Empirical analysis of denial of service attack against smtp servers." In *Collaborative Technologies and Systems, 2007. CTS 2007. International Symposium on*, pp. 72-79. IEEE, 2007.
[38] Beverly, Robert, and Karen Sollins. "Exploiting transport-level characteristics of spam." (2008).
[39] Al-Bataineh, Areej, and Gregory White. "Detection and prevention methods of botnet-generated spam." In *Proc. MIT Spam Conf.*, pp. 1-10. 2009.

[40] Hu, Yan, Dah-Ming Chiu, and John Lui. "Entropy based flow aggregation." *NETWORKING 2006. Networking Technologies, Services, and Protocols; Performance of Computer and Communication Networks; Mobile and Wireless Communications Systems* (2006): 1204-1209.
[41] Smith, Kyle, Ehab Al-Shaer, and Khalid Elbadawi. "Information theoretic approach for characterizing spam botnets based on traffic properties." In *Communications, 2009. ICC'09. IEEE International Conference on*, pp. 1-5. IEEE, 2009.
[42] Ehrlich, Willa K., Anestis Karasaridis, David A. Hoeflin, and Danielle Liu. "Detection of Spam Hosts and Spam Bots Using Network Flow Traffic Modeling." In *LEET*. 2010.
[43] Suwa, Shuji, Nariyoshi Yamai, Kiyohiko Okayama, Motonori Nakamura, and Keita Kawano. "Spam mail discrimination system based on behavior of DNS servers associated with URLS." In *Applications and the Internet (SAINT), 2012 IEEE/IPSJ 12th International Symposium on*, pp. 381-386. IEEE, 2012.
[44] Lin, Po-Ching, Ping-Hai Lin, Pin-Ren Chiou, and Chien-Tsung Liu. "Detecting spamming activities by network monitoring with Bloom filters." In *Advanced Communication Technology (ICACT), 2013 15th International Conference on*, pp. 163-168. IEEE, 2013.
[45] Jian-Qi, Zhu, Fu Feng, Yin Ke-Xin, and Liu Yan-Heng. "Dynamic entropy based DoS attack detection method." *Computers & Electrical Engineering* 39, no. 7 (2013): 2243-2251.
[46] Yamai, Nariyoshi, Kiyohiko Okayama, Keita Kawano, and Motonori Nakamura. "E-Mail Priority Delivery System with Dynamic Whitelist in the Layer 3 Switch." In *Computer Software and Applications Conference Workshops (COMPSACW), 2013 IEEE 37th Annual*, pp. 581-586. IEEE, 2013.
[47] Zempoaltecatl-Piedras, Rafael, Pablo Velarde-Alvarado, and Deni Torres-Roman. "Entropy and flow-based approach for anomalous traffic filtering." *Procedia Technology* 7 (2013): 360-369.
[48] Navaz, A. S., V. Sangeetha, and C. Prabhadevi. "Entropy based anomaly detection system to prevent DDoS attacks in cloud." *arXiv preprint arXiv:1308.6745* (2013).
[49] Phemius, Kevin, Mathieu Bouet, and Jeremie Leguay. "Disco: Distributed multi-domain sdn controllers." In *Network Operations and Management Symposium (NOMS), 2014 IEEE*, pp. 1-4. IEEE, 2014.
[50] Sochor, Tomas, and Radim Farana. "Improving efficiency of e-mail communication via spam elimination using blacklisting." In *Telecommunications Forum (TELFOR), 2013 21st*, pp. 924-927. IEEE, 2013.
[51] Phemius, Kevin, and Mathieu Bouet. "Monitoring latency with openflow." In *Network and Service Management (CNSM), 2013 9th International Conference on*, pp. 122-125. IEEE, 2013.
[52] Cartier, Gabriel, Jean-François Cartier, and José M. Fernandez. "Next-generation dos at the higher layers: A study of smtp flooding." In *International Conference on Network and System Security*, pp. 149-163. Springer Berlin Heidelberg, 2013.
[53] Rathi, Megha, and Vikas Pareek. "Spam Mail Detection through Data Mining-A Comparative Performance Analysis." *International Journal of Modern Education and Computer Science* 5, no. 12 (2013): 31.
[54] Chen, Chia-Mei, and Hsiao-Chung Lin. "Detecting botnet by anomalous traffic." *journal of information security and applications* 21 (2015): 42-51.
[55] Vizváry, Martin, and Jan Vykopal. "Future of DDoS attacks mitigation in software defined networks." In *IFIP International Conference on Autonomous Infrastructure, Management and Security*, pp. 123-127. Springer Berlin Heidelberg, 2014.
[56] Giotis, Kostas, Georgios Androulidakis, and Vasilis Maglaris. "Leveraging SDN for efficient anomaly detection and mitigation on legacy networks." In *Software Defined Networks (EWSDN), 2014 Third European Workshop on*, pp. 85-90. IEEE, 2014.
[57] Oktian, Yustus Eko, SangGon Lee, and HoonJae Lee. "Mitigating denial of service (DoS) attacks in openflow networks." In *Information and Communication Technology Convergence (ICTC), 2014 International Conference on*, pp. 325-330. IEEE, 2014.
[58] Geetha, K., and N. Sreenath. "SYN flooding attack—Identification and analysis." In *Information Communication and Embedded Systems (ICICES), 2014 International Conference on*, pp. 1-7. IEEE, 2014.
[59] Özçelik, İlker, and Richard R. Brooks. "Deceiving entropy based DoS detection." *Computers & Security* 48 (2015): 234-245.
[60] Graham, Mark, Adrian Winckles, and Erika Sanchez-Velazquez. "Botnet detection within cloud service provider networks using flow protocols." In *Industrial Informatics (INDIN), 2015 IEEE 13th International Conference on*, pp. 1614-1619. IEEE, 2015.
[61] Kim, Jinyong, Mahdi Daghmehchi Firoozjaei, Jaehoon Paul Jeong, Hyoungshick Kim, and Jung-Soo Park. "SDN-based security services using interface to network security functions." In *Information and Communication Technology Convergence (ICTC), 2015 International Conference on*, pp. 526-529. IEEE, 2015.
[62] Seeber, Sebastian, Lars Stiemert, and Gabi Dreo Rodosek. "Towards an SDN-enabled IDS environment." In *Communications and Network Security (CNS), 2015 IEEE Conference on*, pp. 751-752. IEEE, 2015.

[63] Ruffy, Fabian, Wolfgang Hommel, and Felix von Eye. "A STRIDE-based Security Architecture for Software-Defined Networking." *ICN 2016* (2016): 107.
[64] Mir, Nader F., Jayashree N. Kotte, and Gokul A. Pokuri. "Implementation of Virtualization in Software Defined Networking (SDN) for Data Center Networks." *ICN 2016* (2016): 136.
[65] Teo, Zhiyuan, Ken Birman, and Robbert Van Renesse. "Experience with 3 SDN controllers in an enterprise setting." In *Dependable Systems and Networks Workshop, 2016 46th Annual IEEE/IFIP International Conference on*, pp. 97-104. IEEE, 2016.
[66] Saxena, Mudit, and Rakesh Kumar. "A recent trends in software defined networking (SDN) security." In *Computing for Sustainable Global Development (INDIACom), 2016 3rd International Conference on*, pp. 851-855. IEEE, 2016.
[67] Linden, Alexander. "Gartner's 2002 Hype Cycle for Emerging Technologies." *Cited from www. gartner. com on March* 4 (2002): 2008.
[68] J. T. Johnson, "Why you need software-defined security for your SDN," 2016. [Online]. Available: http://searchtelecom.techtarget.com/tip/Why-you-need-software-defined-security-for-your-SDN. [Accessed: 03-Mar-2016].
[69] I. Gartner, "Hype Cycle for Emerging Technologies 2016," 2016. [Online]. Available: http://www.gartner.com/newsroom/id/3412017. [Accessed: 21-Nov-2016].