Secure Multipath Mutation SMPM in Moving Target Defense Based on SDN

Article *in* Procedia Computer Science · January 2019

DOI: 10.1016/j.procs.2019.04.137

4 authors:

Karim Zkik
Université Internationale de Rabat
17 PUBLICATIONS **46** CITATIONS
SEE PROFILE

Anass Sebbar
Université Internationale de Rabat
3 PUBLICATIONS **6** CITATIONS
SEE PROFILE

Youssef Baddi
Université Chouaib Doukkali
27 PUBLICATIONS **47** CITATIONS
SEE PROFILE

Mohammed Boulmalf
Université Internationale de Rabat
91 PUBLICATIONS **694** CITATIONS
SEE PROFILE

Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 151 (2019) 977–984

Procedia Computer Science

www.elsevier.com/locate/procedia

International Symposium on Machine Learning and Big Data Analytics for Cybersecurity and Privacy (MLBDACP)
April 29 – May 2, 2019, Leuven, Belgium

Secure Multipath Mutation SMPM in Moving Target Defense Based on SDN

Karim ZKIK[a,*], Anass Sebbar[a,b], Youssef Baddi[c], Mohammed Boulmalf[a]

[a]*Université Internationale de Rabat, Faculté d'Informatique et de Logistique, TICLab, Morocco*
[b]*ENSIAS-Mohammed V Rabat University, Morocco*
[c]*STIC,ESTSB-Chouaib Doukkali University, Morocco*

Abstract

Software-defined networking (SDN) refers to a network architecture where the transfer state in the data plane is managed by a remote control plane in a centralized manner. SDN offer many advantage in terms of flexibility and automation to administrator but it suffer from many security issues. In other hand, Random Route Mutation (RRM) and path diversity represent one of the important research focuses about moving target defense (MTD). The main idea of using this technic, is to change periodically (or basing on events) used routes between sender and receiver in order to enhance mutation efficiency and decrease attackers capabilities to launch effective eavesdropping, denial of service or man in the middle attack. Using RRM and multi path technics can be very interesting in order to secure SDN and to detect and prevent intrusions. In this paper it is propose a new framework called SMPM which aims to secure and prevent intrusion by modeling SDN architectures and using a pathfinder algorithm called RRM-Pathfinder. The proposed framework calculates all possible paths from given source to destination and then, based on some criteria such as capacity, Overlap, Security and QoS, it selects and identifies the most cost-effective routes. The use of SMPM allow also to dynamically route packets using all pre-calculated paths which will permit to avoid sniffing and poisoning attacks such as Arp spoof and the man in the middle attacks and to ensure more confidentiality, integrity and privacy.

Keywords: Moving target defense; Random Route Mutation; Software-defined networking; Pathfinder; Multipath Mutation; Security and Privacy.

* Corresponding author. Tel.: +212-6-68541985; fax: +212-5-30103100
E-mail address: karim.zkik@uir.ac.ma

10.1016/j.procs.2019.04.137

1. Introduction

In recent years, with the popularization of smartphones and new technologies such as Cloud and IoT, the number of services offered by different service providers and operators has grown phenomenally [1]. Internet services contribute to the greater amount of traffic flowing through the networks, which means that the bandwidth limits of networks are constantly increasing. In the coming years, with the commercialization of 4k mobile terminals and mobile video services, bandwidth of the traffic network will continue to increase significantly. Moreover, with the development of the Internet of Things (IoT), more than 50 billion new equipment's will be connected to the network by 2020 [2]. Experts in networks and information systems estimate that traditional networks can no longer support this increase in terms of the number of service and bandwidth [3]. Thus, to meet the needs of users and to support technological development, networks have to evolve and to embrace new challenges to adapt to more increase in data transmission. To meet the growing needs in terms of services; new technologies such as Network function virtualization (NFV) [4] and Software-defined networking (SDN) [5] have emerged. NFV is trying to rebuild "vertically" the network architecture by deploying virtualized network elements (NEs) on an X86-based universal server using hardware resources to provide more resources in terms of computing, storage and bandwidth. On the other side, SDN rebuilds the network "horizontally"; of such kind that the operations of calculation and controls are centralized. The SDN dissociates the control plane from the data plan, allowing a more flexible adjustment of network resources and control capabilities.

Despite the various advantages of using the SDN; there are various challenges [6] facing his deployment such as: Interfaces and protocol standardization and interoperability, Performance and reliability, fault tolerance and security. Security is considered by experts as the biggest challenge on SDN [7]. There are many solutions to secure SDN architectures in literature [8-10], but there are some attacks that are very difficult to stop such as network scanning, spoofing and listening on the communication channels [11]. Moving Target Defense (MTD) [12] is a new security solution that aims to create asymmetric uncertainty on the attacker side, to increase complexity and cost of attacks and limit exposure to vulnerabilities. This technique aims to continuously and randomly modify the attack surface of a system (for example change the paths of flows and streams, change IP addresses, change ports numbers) to prevent or stop attacks. So, MTD can be used to change the routes in the network periodically; this technique of MTD is called Random Route Mutation (RRM) [13]. RRM is based on the path diversity or the ability to provide multiple physical and/or virtual paths between sender and receiver. In other hands Multipath routing [14-15] is a technique that allows using multiple paths simultaneously on a network. The algorithm generates one or more paths between nodes based on certain characteristics; packets are then routed according to percentages by these multiple predefined paths.

In this paper we propose a Random Route Mutation (RRM) using a multi-Pathfinder algorithm called SMPM suitable to software defined networks (SDNs). The basic idea of SMPM is allowing the control plan to select and to change the routes in the network periodically (or based on some specific events). To do this we will implement two new modules in SDN controllers (RRM-Pathfinder flow management Module and RRM-Pathfinder calculation Module) which calculate all possible paths between a source and a destination and selects the most cost-effective path. The SDN controller can then automatically calculate the suitable paths based on the algorithms results. The main goal of this work is to increase the complexity of attacks on SDNs environments and to detect and prevents some specific attacks such as scanning, spoofing, man in the middle (MitM) and denial of services (DoS).

This paper is organized as follows: in section I we present some preliminaries, motivations, related works and research scoop. Section II discusses and analyses the RRM-Pathfinder algorithms and introduces our proposed model. The Experimental results are presented in Section III. Section IV concludes the paper.

2. Problematic and Related Work

Software-defined networking (SDN) [5] is an emerging networking paradigm that allows network administrators to manage the whole network through abstraction of higher-level functionality. SDN is characterized by five fundamental traits: Plane separation, a simplified network architecture, centralized control, network automation and virtualization, and openness. In general, SDN bring many benefits to operators and network administrators in terms

of service such as rapid service introduction and profit making, service automation and automated service provisioning and network optimization.

Despite the apparent benefits of using SDN architectures, several challenges are slowing down its deployment such as configuration standardization, topology discovery, performance management, fault tolerance, resiliency, scalability, and security issues. Security is one of the most problematic challenges for the deployment of SDN. SDN's centralized architecture and multi-layered design makes it vulnerable to multiple types of attacks and subject to multiple security vulnerabilities. So, in the SDN architecture, there are several security issues that affect its operation. The more common SDN security concerns include attacks at the various SDN architecture layers. The figure 1 illustrates a typical SDN architecture and the main SDN threat vector.

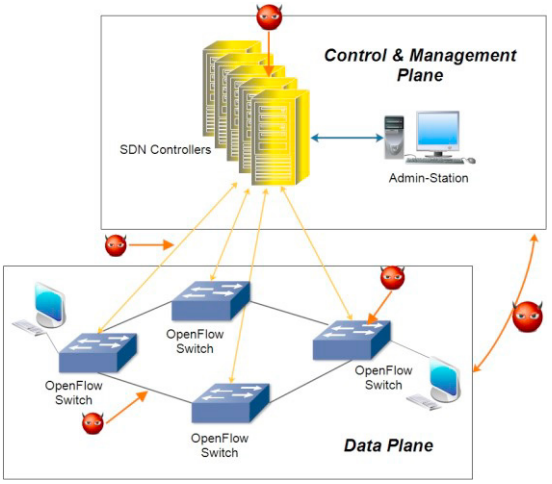

Fig. 1. Threat vectors in SDN architecture

From this figure, we can divide the security problems in the SDN architectures in 7 major categories: Controller Security, Controllers Communication Security, Data Plan Security, Management Plan Security, Control Plan Security, Applications and end users Plan Security, and Communications Channel Security. These vulnerabilities can be exploited by several attacks such as Scanning, Spoofing, Hijacking, Man in the Middle and DDoS attacks.

To overcome these issues, several research projects have proposed secure solutions and frameworks [16-18]. Zhu et al. [19] propose SFA; a dynamic transfer abstraction processor in an SDN data plane. The main goal of this work is to extend the functionality of the SDN controller and to filter malicious connections. Xiao Feng Qiu et al. [20] propose GFT; a mechanism that provides security appliances with information about the paths of all SDN flows and gives a global view of the network. Kamisinski and Fung [21] propose FlowMon; a model that limits the impact of poisoning attacks. Lara and Ramamurthy [22] propose OpenSEC; a security models that enables deep packet inspection, intrusion detection, and malware detection.

Despite the various proposals and solutions offered by these research projects, most of them are complex, which reduces performance and increases latency and they only focus on some security aspects of SDN. Considering solutions including Moving target Defense techniques; a few amount of related work is available. Jafarian et Al. [23] present a random host mutation as moving target defense technique using on software defined networking. In their work, they describe how host virtual addresses can be updated following an algorithm that assigns free addresses. Dunlop et Al. [24] implements an IPv6 address update scheme in similar context. Kampanakis et Al. [25] propose an SDN framework that incorporates MTD functionality. On their paper, authors introduce a moving target technique called OpenFlow Random Host Mutation (OF-RHM) which mutates IP addresses of end-hosts randomly and frequently so that the attackers' premises about the static IP assignment of network fails. Al-Shaer et Al. [26] propose changing routes that connect a source and a destination. It describes how a random route mutation (RRM) scheme can be formulated and optimized according to MTD requirements and costs. Then the most effective route is implemented without disrupting any ongoing traffic or violating security integrity.

Even though these researches propose MTD-based solutions but they usually choose the best path which will always allow to a Dolev-Yao attacker to recover the data that transits in the network. In addition, the fact that packets pass through the same path makes the MitM attack always possible. The proposed solutions also need some extra computing power which could affect the SDN nodes and increase latency.

In this paper, we will investigate how SDN can be used in Random Route Mutation based MTD techniques by taking the advantages of centralization and automation. So, we will be interested to modeling SDN network, and developed an algorithm which calculates all possible paths from given Source to Destination given a Multi-pathfinder algorithm. The chosen paths must correspond to a valid system configuration (Suitable to controller rules) and make route change without interrupting on-going traffic.

3. A new secure Multipath flow management Mutation SMPM

3.1. Proposed model and Conceptual design

In order to implement the RRM-Multipath techniques, there are two main problems need to take on considerations, explained as below:

Next Valid system configuration: The main problem of an MTD system is to move the system from current valid state to a new valid state, that's mean we need to answer the question, how to select the next valid configuration state of the MTD system?

Adaptation election problem: Moving the system from current valid and stable configuration to the next valid configuration state requires solving the adaptation selection problem, which can be stated informally as applying a multiple sequence of actions to can transition the system from old configurations to next configuration with minimum of impact in normal work of system, the optimal solution would require to take constraints such as time and costs into consideration.

To overcome these limitations we propose to implement two new modules in SDN controllers who calculate all possible paths from an SDN node to another. Figure 2 represents the conceptual design of our proposed model.

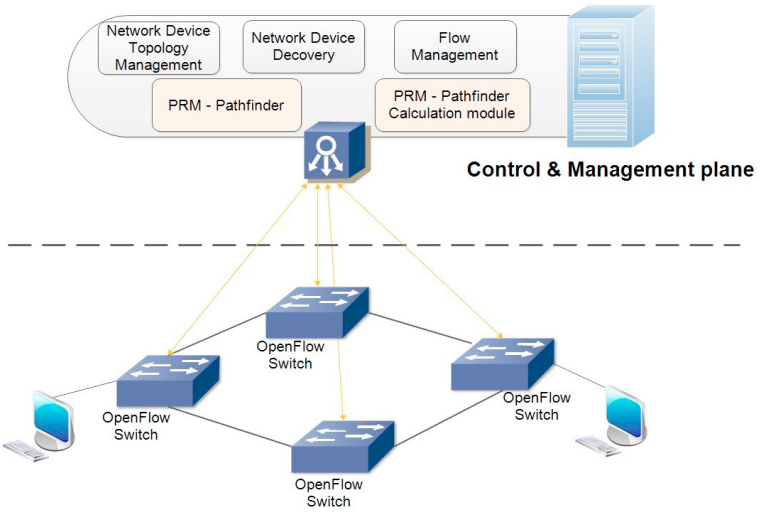

Fig. 2. Conceptual design of SDN architecture using RRM-Mutipath modules

SDN controllers usually consist of several modules that allow them to choose the best paths between the nodes. This choice does not take into account security risks. For this we will detail the proposed modules and some existing modules to explain how a controller can choose multiple paths in order to send packages safely.

- **Network Device Discovery:** This module is responsible of discovery of network devices which comprise the infrastructure of the network, such as switches, routers, and wireless access points.

- **Network Device Topology Management**: This module maintain information about the interconnection details of the network devices to each other, and to the end-user devices to which they are directly attached, such as laptops, desktops, servers and mobile devices.
- **Flow Management:** Maintain a database of the flows being managed by the controller and perform all necessary coordination with devices to ensure synchronization of the device flow entries with that database.
- **RRM-Pathfinder:** This module will calculate all the possible paths from a source node to a source destination. To implement our modules we will simplify our network as a set of linked nodes. In our case nodes represent the open flow switches.
- **RRM-Path Calculation:** This module will be responsible for sending multiple packets by different path according to their weight.

3.2. RRM-Multipath Flow Management Execution Detail

A computer network is modeled as a simple directed and connected graph F_N=(N ,E), where N (n_1,…, n_i) is a finite set of nodes and E(l_1,…,.l_i), is the set of edges (or links) connecting the nodes. Let |N| be the number of network nodes and |E| the number of network links. An edge l ∈ E connecting two adjacent nodes i ∈ N and j ∈ N will be denoted by $l_{(i,j)}$, the fact that the graph is directional, implies the existence of a link l(j,i) between j and i. Each edge is associated with a positive real value: a cost function W(e) = W(l(i,j)) represents link utilization, which may be either monetary cost or any measure of resource utilization. To represent our network, figure 3, we will use an adjacency matrix $A_{i,j}$, where i and j represent the nodes, and w_{ij} represents the link's weight between them.

$$A = w_{ij} \begin{pmatrix} w_{00} & \cdots & \\ \vdots & \ddots & \vdots \\ w_{i0} & \cdots & \end{pmatrix} \quad \text{Where } w_{ij} = \begin{cases} =0 \{i,j\} \notin E \\ \neq 0 \{i,j\} \in E \end{cases}$$

In order to build the adjacency matrix, we'll need to define the weight of each path; In our case we will use weight=1 (equivalent to 10Gb), and weight=2 (equivalent to 1Gb), in this case (we will use 10 nodes), the global adjacency matrix will be presented as shown in table 1.

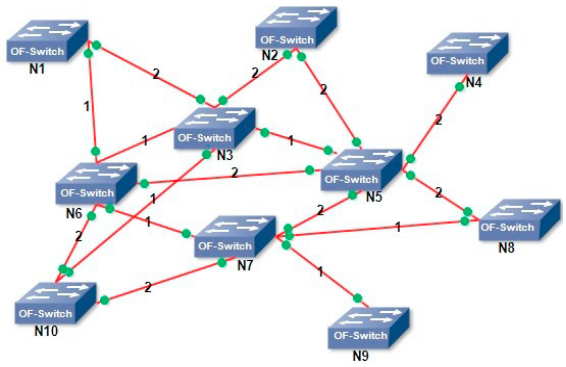

Fig. 3. SDN nodes

Table. 1. Example of an Adjency matrix for 10 SDN nodes

	N1	N2	N3	N4	N5	N6	N7	N8	N9	N10
N1	0	0	2	0	0	1	0	0	0	0
N2	0	0	2	0	2	0	0	0	0	0
N3	2	2	0	0	1	1	0	0	0	1
N4	0	0	0	0	2	0	0	0	0	0
N5	0	2	1	2	0	2	2	2	0	0
N6	1	0	1	0	2	0	1	0	0	2
N7	0	0	0	0	2	1	0	0	1	2
N8	0	0	0	0	2	0	1	0	0	0
N9	0	0	0	0	0	0	1	0	0	0
N10	0	0	1	0	0	2	2	0	0	0

Initial Setup:

1- Choose a source node, Src= the starting open flow switches
2- Choose a destination node, Dst=the destination open flow switches
3- Define a weight in each link, W_{ij}= weights of each link
4- Initiate the number of possible jump from source to destination to 0. Jmp= number of jumps.
5- Define Max_jmp as the maximum jumps value before reaching destination
6- Construct a table of all possible path and initiate it to 0, Path [i]= A possible path from source to destination

Display paths Algorithm: In this part we will calculate the different paths according to the following algorithm:

```
Function Path_Display()
IF (position==DST) THEN
          jmp= 0 // initiate total distance.
          FOR(i= 0 ; i <= Max_jmp ; i++)
                    DISPLAY path[i]
          IF (i==0) continue;
          Jmp = A[path[i-1]][path[i]] + jmp;
          END FOR
END IF
```

Let's take as example the study of the possibilities for Source node1=N1 and Destination node8=N8. The algorithm, when executed, will take into consideration all the possibilities. We will then calculate the weights of all possible paths based on our constructed Adjency Matrix. The different results are presented in table 2.

Table. 2. Path selection results

Paths	Weights	Paths	Weights
Path1: N1 N3 N2 N5 N8	W_Path1: 8	Path11: N1 N6 N3 N5 N8	W_Path11: 5
Path2: N1 N3 N2 N5 N7 N8	W_Path2: 9	Path12: N1 N6 N3 N5 N7 N8	W_Path12: 6
Path3:N1 N3 N6 N5 N8	W_Path3: 7	Path13: N1 N6 N3 N2 N5 N8	W_Path13: 8
Path4:N1 N3 N6 N5 N7 N8	W_Path4: 8	Path14: N1 N6 N3 N2 N5 N7 N8	W_Path14: 9
Path5: N1 N3 N6 N7 N5 N8	W_Path5: 8	Path15: N1 N6 N3 N10 N7 N5 N8	W_Path15: 9
Path6: N1 N3 N6 N10 N7 N5 N8	W_Path6: 10	Path16: N1 N6 N3 N10 N7 N8	W_Path16: 6
Path7: N1 N3 N6 N10 N7 N8	W_Path7: 7	Path17: N1 N6 N7 N5 N8	W_Path17: 6
Path8: N1 N3 N5 N8	W_Path8: 5	Path18: N1 N6 N7 N8	W_Path18: 3
Path9: N1 N3 N5 N7 N8	W_Path9: 6	Path19: N1 N6 N10 N7 N5 N8	W_Path19: 9
Path10: N1 N3 N10 N7 N5 N8	W_Path10: 9	Path20: N1 N6 N10 N7 N8	W_Path20: 6

The best path is the path with the lowest weight. Using these results, we will choose some of the best past and we will send our packets using these multi-paths.

RRM Bests Multi Paths calculation Algorithm:

Firstly, we will calculate an amount of best paths to route packets from source to destination according to a percentage of best paths selected beforehand by the administrator. So, we will select the best paths according to the following algorithm:

```
Function RRM_PathCalculation()
Begin
          n_paths = paths.length
          n_selectedPaths_weight = prc * n_paths
          sortedPath = new Path[n_paths]
          bestPaths = new Path[n_selectedPaths_weight]
          sortedPath = sortByWeight(paths)
          for i = 0 to n_selectedPaths_weight-1 do
          begin for
                    bestPaths[i] = sortedPath[i]
                    if(bestPaths[i_p]==bestPaths[i_p+1] and i_p!=0) then
                    p=bestPaths[i_p].Random();
                    p.Out_time();
                    end if
          sendPacket(p, bestPaths[i_p])
                    i_p++;
                    i++;
          end for
End function
```

In the case where we have several paths with the same weight, we will choose our paths randomly. We will run this algorithm periodically so we will have new paths selections on each execution. In this case we will have a change of path according to MTD based on RRM techniques and a multipath selection according to the pathfinder algorithm.

Packets Redirection Algorithm:

The main idea of our proposition is sending packets using multiple paths. To do this we will calculate packets' rate "quota_packets" to send by each path. The calculation will be made dynamically according to the weight of

each path. To increase performance in the network, we will send the highest rate using the best path and the lowest rate by the worst path. So, we will calculate the percentage of packets to send per path according to the following algorithm:

```
for i = 0 to n_selectedPaths-1 do
          begin for
                    real_Weights[i] = sumWeights - bestPaths[i].weight
                    sumReal_Weights += realWeights[i].weight
                    quota_packets[i] = real_Weights[i] / sumReal_Weights * 100
          end for
          while i < n_packets
                    if i_p = n_selectedPaths then i_p = 0
                    p = packets[i]
                    if(quota_packets[i_p]==0 and i_p != 0) then i_p = 0 continue
                    end if
                    sendPacket(p, bestPaths[i_p])
                    quota_packets[i_p]--
                    i++
```

Let's take as example the study of the possibilities for Source node1=N1 and Destination node8=N8 with a selection of 20% from validated paths. Let be Ep (p1 …. pm) the set containing the 20% of paths with minimum weights sorted in increasing order. Let be Np the total number of packets to be routed from source to destination. The result of the RRM_PathCalculation is shown in table 3.

Table. 3. Paths selection and packets redirection

Parameters	**Results**
sortedPath[i]: Selected Paths with corresponding weigh	Path18 → 3 Path11 →5 Path9 → 6 Path8 → 5
sumWeights: the sum of the weights of the selected paths	19
real_Weights[i] : Selected Paths with corresponding Real weigh	Path18 →19-3=16 Path11 →19-3=14 Path9 → 19-3=13 Path8 → 19-5=14
sumReal_Weights: the sum of the real weights of the selected paths	57
quota_packets[i] : For each path we have the following rate:	Path18 → 28,070175438596491228070175438596% Path8 → 24,561403508771929824561403508772% Path11 → 24,561403508771929824561403508772% Path9 → 22,807017543859649122807017543 86%

We have demonstrated in the following that our algorithm allows choosing a range of some best paths to route the packets and that it spreads the data using several paths at once and randomly. Man-in-the-middle spoofing or listening attacks will become very complicated to perform, because the attacker will no longer know by which path the data was routed from the source to the destination.

4. Conclusion

Random Route Mutation is a technic that permit routes mutation in the network periodically or basing on triggered events in order to enhance efficiency and decrease attacker capabilities to launch eavesdropping, denial of service or sniffing's attack. In this paper, we focused our work on modeling SDN network, and developing two new modules based on pathfinder algorithm and MTD/RRM technics, called RRM-Pathfinder. These modules calculates all possible paths from given source to destination, choose a range of best paths, and send data using randomly and simultaneously all these paths. Our RRM-Pathfinder modules are based on some criteria such as capacity, overlap, security and QoS, in order to selects and identifies the most cost-effective route. In this paper we demonstrate that our algorithm is efficient and that increase complexity of attacks such as scanning and poisoning and it is able to improve the capacity of defending attacks such as scanning, eavesdropping, MitM, and DoS attacks.

References

[1] BITTENCOURT, Luiz, IMMICH, Roger, SAKELLARIOU, Rizos, et al. The internet of things, fog and cloud continuum: Integration and challenges. Internet of Things, 2018.

[2] EVANS, Dave. The internet of things: How the next evolution of the internet is changing everything. CISCO white paper, 2011, vol. 1, no 2011, p. 1-11.

[3] SEZER, Sakir, SCOTT-HAYWARD, Sandra, CHOUHAN, Pushpinder Kaur, et al. Are we ready for SDN? Implementation challenges for software-defined networks. IEEE Communications Magazine, 2013, vol. 51, no 7, p. 36-43.

[4] Walter Goralski, "Chapter 29 - Cloud, SDN, and NFV", The Illustrated Network (Second Edition), How TCP/IP Works in a Modern Network, p. 731-757, 2017.

[5] T. D. Nadeau, K. Gray, "SDN: Software defined networks", (O'REILY), 2013.

[6] KATSALIS, Kostas, ROFOEE, B., LANDI, Giada, et al.Implementation experience in multi-domain SDN: Challenges, consolidation and future directions. Computer Networks, 2017, vol. 129, p. 142-158.

[7] AHMAD, Ijaz, NAMAL, Suneth, YLIANTTILA, Mika, et al.Security in software defined networks: A survey. IEEE Communications Surveys & Tutorials, 2015, vol. 17, no 4, p. 2317-2346.

[8] ALSMADI, Izzat et XU, Dianxiang. Security of software defined networks: A survey. computers & security, 2015, vol. 53, p. 79-108.

[9] SEBBAR, Anass, BOULMALF, Mohammed, EL KETTANI, Mohamed Dafir Ech-Cherif, et al. Detection MITM Attack in Multi-SDN Controller. In : 2018 IEEE 5th International Congress on Information Science and Technology (CiSt). IEEE, 2018. p. 583-587.

[10] ZKIK, Karim, HAJJI, Said EL, et ORHANOU, Ghizlane. Design and Implementation of a New Security Plane for Hybrid Distributed SDNs. Journal of communications. 2019, Vol 14, Issue 1, pp. 26-32.

[11] YOON, Changhoon, PARK, Taejune, LEE, Seungsoo, et al.Enabling security functions with SDN: A feasibility study. Computer Networks, 2015, vol. 85, p. 19-35.

[12] AYDEGER, Abdullah, SAPUTRO, Nico, et AKKAYA, Kemal. A moving target defense and network forensics framework for ISP networks using SDN and NFV. Future Generation Computer Systems, 2019, vol. 94, p. 496-509.

[13] DUAN, Qi, AL-SHAER, Ehab, et JAFARIAN, Haadi. Efficient random route mutation considering flow and network constraints. In : 2013 IEEE Conference on Communications and Network Security (CNS). IEEE, 2013. p. 260-268.

[14] BANNER, Ron et ORDA, Ariel. Multipath routing algorithms for congestion minimization. IEEE/ACM Transactions on networking, 2007, vol. 15, no 2, p. 413-424.

[15] CHLIAH, Mouhcine, ORHANOU, Ghizlane, et EL HAJJI, Said. Countering MitM Attacks Using Evolved PathFinder Algorithm. International Journal of Cloud Applications and Computing (IJCAC), 2017, vol. 7, no 2, p. 41-61.

[16] TRIPATHY, Bata Krishna, DAS, Debi Prasad, JENA, Swagat Kumar, et al. Risk based Security Enforcement in Software Defined Network. Computers & Security, 2018, vol. 78, p. 321-335.

[17] ZKIK, Karim, TACHIHANTE, Tarik, ORHANOU, Ghizlane, et al. A Modular Secure Framework Based on SDMN for Mobile Core Cloud. In : International Conference on Mobile, Secure, and Programmable Networking. Springer, Cham, 2016. p. 137-152.

[18] ZKIK, Karim, HAJJI, Said EL, et ORHANOU, Ghizlane. A centralized secure plan for detecting and mitigation incidents in hybrid SDN. In : MATEC Web of Conferences. EDP Sciences, 2018. p. 10015.

[19] ZHU, Shuyong, BI, Jun, et SUN, Chen. {SFA}: Stateful Forwarding Abstraction in {SDN} Data Plane. In : Presented as part of the Open Networking Summit 2014 ({ONS} 2014). 2014.

[20] QIU, Xiaofeng, ZHANG, Kai, et REN, Qiuzheng. Global Flow Table: A convincing mechanism for security operations in SDN. Computer Networks, 2017, vol. 120, p. 56-70.

[21] KAMISIŃSKI, Andrzej et FUNG, Carol. Flowmon: Detecting malicious switches in software-defined networks. In : Proceedings of the 2015 Workshop on Automated Decision Making for Active Cyber Defense. ACM, 2015. p. 39-45.

[22] LARA, Adrian et RAMAMURTHY, Byrav. OpenSec: A framework for implementing security policies using OpenFlow. In : 2014 IEEE Global Communications Conference. IEEE, 2014. p. 781-786.

[23] JAFARIAN, Jafar Haadi, AL-SHAER, Ehab, et DUAN, Qi. Openflow random host mutation: transparent moving target defense using software defined networking. In : Proceedings of the first workshop on Hot topics in software defined networks. ACM, 2012. p. 127-132.

[24] DUNLOP, Matthew, GROAT, Stephen, URBANSKI, William, et al.Mt6d: A moving target ipv6 defense. In : 2011-MILCOM 2011 Military Communications Conference. IEEE, 2011. p. 1321-1326.

[25] KAMPANAKIS, Panos, PERROS, Harry, et BEYENE, Tsegereda. SDN-based solutions for moving target defense network protection. In : Proceeding of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks 2014. IEEE, 2014. p. 1-6.

[26] AL-SHAER, Ehab, MARRERO, Will, EL-ATAWY, Adel, et al.Network configuration in a box: Towards end-to-end verification of network reachability and security. In: 2009 17th IEEE International Conference on Network Protocols. IEEE, 2009. p. 123-132.