APTIKOM Journal on Computer Science and Information Technologies
Vol. 2, No. 3, 2017, pp. 97~105
ISSN: 2528-2417
DOI: 10.11591/APTIKOM.J.CSIT.68

Research trends and solutions for secure traffic management of SDN

Ravi Shankar Pandey, Vivek Srivastava*, Lal Babu Yadav
Department of Computer Science & Engineering,
Birla Institute of Technology, Uttar Pradesh, India
*Corresponding author, e-mail: viveksrivastava@united.ac.in

Abstract

Software Defined Network (SDN) decouples the responsibilities of route management and data transmission of network devices present in network infrastructure. It integrates the control responsibility at the centralized software component which is known as controller. This centralized aggregation of responsibilities may result the single point of failure in the case malicious attack at the controller side. These attacks may also affect the traffic flow and network devices. The security issues due to such malicious attacks in SDN are dominating challenges in the implementation and utilization of opportunities provided by this new paradigm. In this paper we have investigated the several research papers related to proposal of new research trends for security and suggestions which fulfil the security requirements like confidentiality, integrity, availability, authenticity, authorization, nonrepudiation, consistency, fast responsiveness and adaptation. We have also investigated the new future research for creating the attack free environment for implementing the SDN.

Keywords: *quality of service, security requirements, security, software defined networking, traffic engineering*

1. Introduction

A data transfer from one place to another place without delay is a major challenge. The network system facilitates the data transfer from one place to another place. Traditional network system consists of network devices with control management module which is responsible for forwarding data packets and managing routing of the data in optimum time. Radius and AAA (Authentication, Authorization and Accounting) based security systems [1] are used for traditional network systems. A secure routing protocol for integrated UMTS and WLAN are used to improve jitter sensitivity of video streaming traffic for ad-hoc networks [2]. The control management and actual data transfer are tightly coupled in traditional network system. Any change in topology of the network, device configuration or routing strategies may demand change in firmware software which incur cost and delay in data transmission. SDN concept decouples the responsibility of control management and actual data transfer with the help of software component. This software component is called as controller and is responsible for control management. Any change in network topology or routing strategies can be easily managed by controller without involving the cost and delay.

SDN emerges as future network technology. This technology provides better management of communications among the network devices. This architecture has three layers as shown in Figure 1. These layers are infrastructure layer, control layer and application layer. The infrastructure layer consists of network devices like: router, switches, wireless access point etc. The control layer has controller (like floodlight, NOX, POX, OpenDaylight etc.). The application layer has application like access control, security, monitoring, and network management tools etc. The role of controller finds the congestion free path between requests and responses. The controller may have several paths for one request and one response. The controller decides any one optimal path from the set of available path on the basis of load balancing algorithms. So many network devices approach to controller for providing the optimal path at any time. So controller is always heavily loaded from this work.

In traditional network systems network devices/forwarding devices have responsibilities of routing and data transmission. In this structure malicious attacks cannot fail entire network system because each network devices have its own control and data transmission module. SDN is based on centralized control responsibility which can easily affect from malicious attacks and may result a single point of failure. The security of SDN is a major challenge. These malicious attacks can be affected on

Received August 3, 2017; Revised September 1, 2017; Accepted September 15, 2017

traffic flow, network devices, control plane and at controller due to trust deficit between controller and application management etc. The DoS attack can be exhausted the resource of forwarding devices and controller. This can be overcome by authentication process. Azeem Mohammed Abdul et.al [3] have also worked on denial of service attacks in the context of wireless sensor networks to improve the utilization of network resources, they have investigated DOS attack at every level of the protocol by using state of flow of traffic to detect DOS attack. The malicious attack can slow down or de-active the network devices or change the actual data transmission route decided by the controller or increase the controller load by the fake and forged requests. The improvement of trust between application and controller are implemented by different certification techniques. The SDN security has some requirements like confidentiality, integrity, availability, authenticity, authorization, non-repudiation, consistency, fast responsibility and adaptation. The security system is installed on controller to stop single point of failure, like firewall system, intrusion prevention system, intrusion detection system etc. A naive bayes decision tree concept is used to develop intrusion detection system to deal with attack from internet for computer systems [4]. This research investigation is organised as follows: Section –2 describes different security issues in SDN and also summarizes the different types of attacks along with solution in tabular form. Section –3 describes is used for summarizing the research trends and solutions in security of the SDN. Section –4 concludes the research investigation.

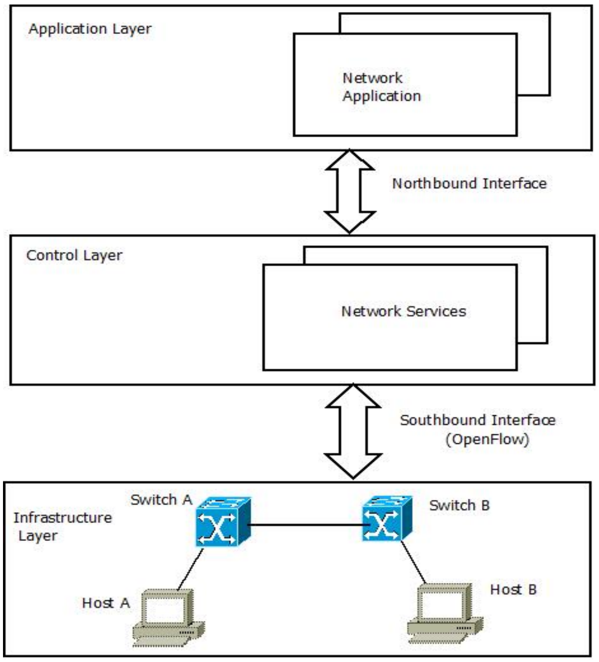

Figure 1. SDN architecture

2. Security Issues in SDN

In SDN request and response between the hosts take place with the help of switches, controller and application as shown in Figure 2. The threats can damage at the switch level or at the controller side or at the application layer as shown in Figure 2 by the labels. The forged or faked traffic flow attacks take place between the switches and controller as shown by label-1. These attacks are in the category of denial of services attacks (DoS). The individual switches can also be damaged by the attacks as shown by label-2. These attacks are known as SSL/TLS attacks. The control plane communication may also be infected by the threats as mentioned by label-3. These threats are in the category of DoS. The controller may be disturbed due attacks and this is in the area of DoS labelled as 5. The trust deficit between the controller and management application can cause the malicious attacks and is labelled as 5, 6, and 7. The Table 1 is summarised the attacks and respective solutions.

Centralization of the control management of the SDN creates opens doors for new attacks. These attacks may create problems at the controller side, at data plane, or at applications. These attacks are classified in seven categories as list in Table 1. These attacks may occur due to forged traffic flow, on switches, on control planes, due to trust deficit in controller and application, administrative station attached with controller. The consequences of the attacks and tentative solution are also described in the Table 1. The security of the SDN can be improved by implementing the solution. These solutions should be satisfied the security requirement authentication, authorization, consistency, integrity etc.

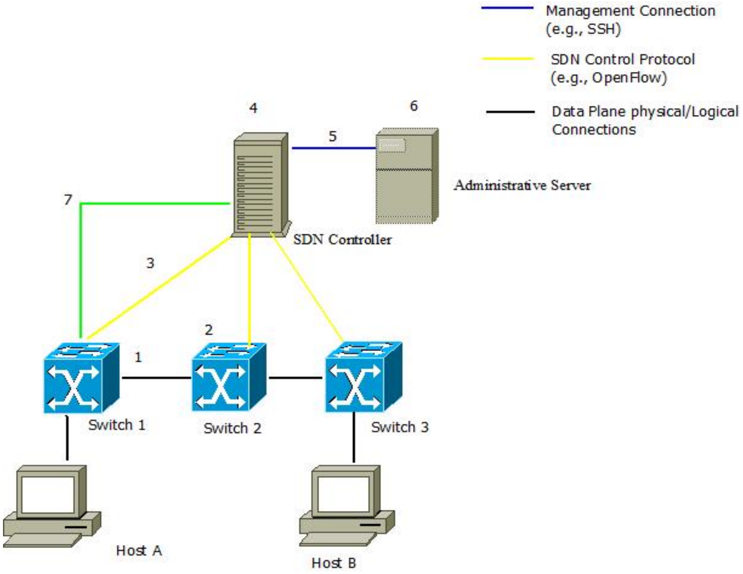
Management Connection (e.g., SSH)
SDN Control Protocol (e.g., OpenFlow)
Data Plane physical/Logical Connections
4
6
5
Administrative Server
7
SDN Controller
3
2
1
Switch 1
Switch 2
Switch 3
Host A
Host B

Figure 2. A model of attacks on SDN

Table 1. Summary of Types of Attacks, Solutions and Properties Satisfy

Vector Name	Consequence in SDN	Solution/Mechanism	Property
Forged or traffic flows	Can be a door for DoS attack.	Replication, trust between controller and devices	Authentication
Attacks on vulnerabilities in switches	But now the impact is potentially augmented.	trust between controller and devices, Fast and reliable update and patching, self-healing	Authentication, fast responsiveness
Attacks on control plane communications	Communication with logically centralized controllers can be explored.	Diversity, Dynamic switch association, Trust between controllers and devices	Adaptation
Attacks on and vulnerabilities in controllers	Controlling the controller may compromise the entire network.	Replication, Diversity, Self-healing, Dynamic switch association, Trust between controllers and apps, Security domains, Secure components, Fast and reliable update and patching	Adaptation, authorization, availability, fast responsiveness, nonrepudiation, authenticity
Lack of mechanisms to ensure trust between the controller and management applications	Malicious applications can now be easily developed and deployed on controller.	Replication, Trust between controllers and apps, Security domains, Secure components	Authorization, availability, nonrepudiation
Attacks on and vulnerabilities in administrative stations	But now the impact is potentially augmented.	Diversity, , Self-healing, Fast and reliable update and patching	Fast responsiveness
Lack of trusted resources for forensics and remediation	It is still critical to ensure fast recovery and diagnosis when faults happen.	Replication, Secure components	Availability

3. Research Trends and Solutions

SDN concept is implemented using three layers: application, control & infrastructure layer. These layers loosely coupled together. The security issue in SDN has two actors' security at network devices & security at controller. Host security & controller security simultaneously/together make complex interaction with protocols which are responsible for the communication & cause incorrect behaviour in the case of attacks. The several researches have been made to develop a better security feature at controller side & network side. Some research efforts have been also made which use man-in-the-middle approach which is installed between controller & hosts. These approaches also increase the trust level between network devices & controller.

3.1. MITM Attacks

Man-in-middle attacks may be infected network topology, switches and generate false certificate. In this kind of attack one or more attacker may be present in the path of network connection. When any user wants to send their data packets to another user these attackers change the information of the destination host with the information of itself. The Figure 3 describes the MITM attack. In this two hosts are connected with the router and with internet and one attacker present in the route of user A and user B. User A sends the data packet to user B through router and attacker changes the user destination information. The packet travels from user A and it reaches to attacker in place of user B. The attacker changes the MAC address of destination in address resolution protocol of user A if A is source of the data transmission. In the case of user B attacker is again updated information of the user A in ARP table of as shown in Table 2. The several research efforts have been done to stop such attacks by implementing tools like TopoGuard, Resonance, and Crossbear etc.

Table 2. Description of change due to attacks in ARP

ARP entry of User A				ARP entry is updated to		
IP address	MAC address	type		IP address	MAC address	Type
10.1.1.3	3-3-3	dynamic	⇨	10.1.1.3	2-2-2	Dynamic
ARP entry of User B				ARP entry is updated to		
IP address	MAC address	type		IP address	MAC address	Type
10.1.1.1	1-1-1	dynamic	⇨	10.1.1.1	2-2-2	Dynamic

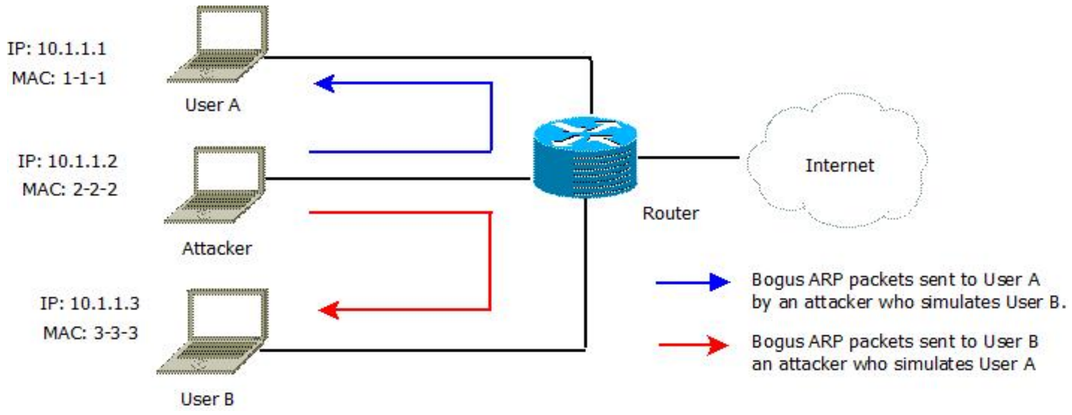
IP: 10.1.1.1
MAC: 1-1-1
User A
IP: 10.1.1.2
MAC: 2-2-2
Attacker
IP: 10.1.1.3
MAC: 3-3-3
User B
Router
Internet
Bogus ARP packets sent to User A
by an attacker who simulates User B.
Bogus ARP packets sent to User B
an attacker who simulates User A

Figure 3. A model of middle-man attacks

Network topology plays important role in fundamental building block for core SDN component and in the topology aware SDN applications. The attacks can also disturb the network information. Incorrect network topology information which is present at upper layer open flow controller services/application may create a serious problem in SDN like hijacking, DOS, MITM attacks. They have studied all current major SDN controllers do not have (POX, Beacon, Floodlight) system for stopping such kind of attacks. S. Hong et al. [5] have proposed a new security extension for SDN controllers which prevents in Real-Time environment from network topology poisoning attacks. They have named this extension TopoGuard and implementation this extension with the help of Floodlight controller. This extension provides secure network topology for the SDN controller. They have also mentioned two kinds of network topology poisoning attacks like host location hijacking attack and link fabrication attack. In host location hijacking attack, attackers can hijack the location of network server to correct the service of subscribers. In link fabrication attack the infected or false link are launched in MITM to manipulate the messages in the network. The traditional attack is also corrupt ARP table like the above tool attacks. TopoGuard prevents the SDN network to apply the precondition and post condition for the verification of host and switches. They have analysed the security issues for the topology management system and suggested to new kind of security issues like (link fabrication and host location) and demonstrated the feasibility of these attacks using mininet evaluation environment. They have also suggested TopoGuard tool can easily implement with other available controller easily.

Ankur Nayak et al. [6] have developed the security system for securing the enterprise network using MITM approach called as resonance. This tool is implemented for dynamic network monitoring & access control for Georgia University. They have argued that network devices are also responsible for a secure enterprise network as well as controller. In this approach they have used programmable switches for controlling the traffic al lower layers by dropping or redirecting traffic and security is enforced at higher level. The resonance improves dynamic access control. Resonance application is used for controlling the traffic with the help of policies installed at the programmable switches by the controller. These applications automatically detect & quarantine automatically the threats. They have used the concept of the security classes which detect the access of the traffic for resources on the network. Each security class has a predefined set of states registration state, authentication, operation & quarantine state. Each state has polices/action that which execution will varies on the basis of network traffic. They have modelled every mac addresses in the form of state machine. The controller uses this state machine for updating flow table entry & corresponding switches. Every state machine has four states.

R. Holz et al. [7] have proposed a tool Crossbear for detecting MITM attacks on SSL/TSL & fixing the problem at local level in the networks. The large number of trace routes is installed on internet for localising the problem called as hunters. Several hunters are distributed over the internet which is deployed by the Crossbear tool. These hunters compare certificates which they receive in SSL/TSL handshake & record the IP route. All these activities are reported to central server where certificates & for further hunting processes are available. This information is used in proposed adaptive attacker model.

C. Soghoian et al. [8] and I Dacosta et al. [9] have proposed method for detection of malicious attacks (MITM) without third party at the SSL/TSL level. The security of network traffic is enforced via secured protocol like SSL/TLS. The security provided by this protocol is based on authentication of servers using the certificates issued by trusted authority. The attackers illegally are creating forged certificates which interrupt secure communication between request and response and such kind of attacks are called as MITM attack. They have used direct validation of certificate protocol which allows domains directly and security watch of their certificate on the basis of history of the user authentication credentials without the third party certificate validation. They have done experimental analysis for desktop and mobile phone to show the performance of DVCERT. Their proposed protocol enhances server authentication and protect web application from MITM attacks SSL/TLS. Their proposals based on simple observation of stack web users. They have established a secure connection using password with most important web application. The proposed protocol allows using to secrete directly and security authentication their certificates without exposing secrete to offline attacks.

3.2. MiddleBox

Middlebox plays important role in networking of enterprises for improving security issues with the implementation of secure traffic routing. The configuration and traffic flow should be correct in MB device to secure connection. The research issues are arising in the implementation of middle boxes with the SDN like implementation of MB operations in dynamic environment, change of traffic load, migrations of application form the deployment etc. A. Gember et al. [10] have argued that current MB managements are clumsy & unsuitable for fully utilization of MB deployment. They have proposed a mechanism which improves MB mechanism which is based on unified control. They have also discussed challenge involved in representing, manipulating & knowledgeably control MB states. The MB operations are classified in four classes: action, supporting, tuning & monitoring. Action class defines operations for applying packet/flow. Supporting class is used to decide one action from multiple possible actions. Tuning class is used for improving MB algorithm performance. They have store three parameters in MB states: key, action & supporting. The value of key depends upon header information of a packet like source destination TCP & source destination port. The action has two values either accept or drop for firewall. The controller maintains state machine for each MAC address using following states: registration state, authentication state operation & quarantine state.

3.3. Security at Controller

In SDN controller plays dominant role in the data transmission. The attacker tries to create destination at controller side using the forged traffic flow. This forged traffic flow creates congestion in the channel increase the load in controller sides which creates controller use responsive. DOS in the case of forged traffic flow is one of the tools for securing the controller from attack. The Figure 4 consists of three switches and one controller and controller is infected by the forged traffic flow which is indicated by red arrow.

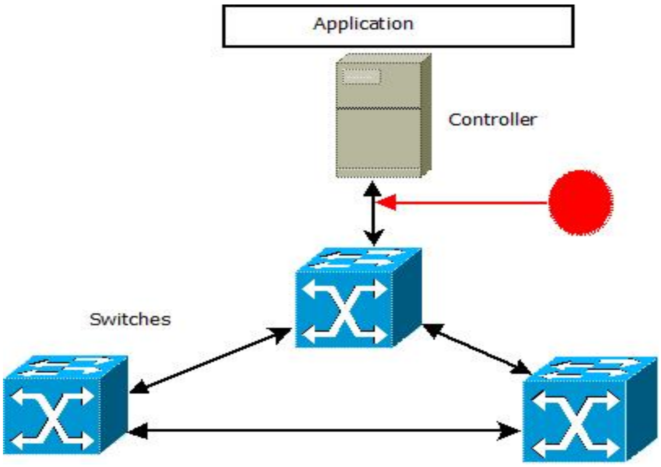

Figure 4. A model of attacks on controller

K. Cabaj et al. [11] have advocated installation of hybrid security management system for SDN. The security system at the controller side provides global view of network security system which governs from the switches. Some security system can also install at the switches side to reduce malicious traffic rate at controller side. They have distributed security system. This security system has two modules local frequent sets analyser (LFSA) and global frequent sets analyser (GFSA). LFSA is placed at on the SDN switches. This module finds the threads which generate large amount of traffic. These malicious activities can be locally stoped without any delay. They have advocated this implementation reduces the amount of malicious traffic at the controller side. They have again argued that all type of malicious activities cannot be stopped at the switch level. These undetected malicious activities can be detected using the global network view of the SDN. GFSA is used for detecting the undetected malicious activities by the switch. This module is placed at controller side and connected with NBI. The role of LFSA module is to analyse the malicious pattern and insert the additional rule for drop malicious packet. GFSA module is used to detect the massive scanning activities which cannot be detected by the switch.

P. Pinto et al. [12] have proposed an algorithm for anomaly detection on controller of SDN. They have also given a methodology for finding the changes in SDN due to DOS attacks with the help of statistical analysis of data provided by the controller. They have considered two parameters for deciding the network state in SDN load of channel and number of flows. They have also detected the next network state after the DOS attack. They have used two tables. First table contains the data in normal conditions with the properties number of flows and duration. Another table stores same data under the simulated attack. They have argued that in the normal condition. There is no association among the data of traffic flows while under the DOS attacks some relations may be present between the traffic flow data. In SDN controller receives large amount of data packet with high rate. D. Kotani et al. [13] have proposed filtering mechanism for dropping unimportant packets from the controller without using important data packets. Packets which match flow entries are process with high speed and in the case of miss match packets are process loosing controller. If controller receives message, then it installs entry in flow table and packets are forwarded to the host with the packet messages.

Syed Akbar Mehdi et al. [14] have proposed an algorithm for detecting traffic anomalies to improve network security in SDN. Their hypothesis is used for home network, routers and advocated this router is ideal platform and suitable place for detecting security level problem. They have also examined several anomaly algorithms and mentioned the two major problem low detection rate and inability to runs Anomaly Detection System (ADS**)** algorithm at line rates in the network. They have used OpenFlow protocol using NOX controller for implementing algorithms. These algorithms are 1. Threshold random walk credit rate limiting. 2. Rate limiting 3. Maximum entropy rate detects or 4. NETAD (Network Traffic Anomaly Detector).

1. This algorithm finds worm on a host on the basis of probability of connection attempt being a success should be much higher for benign host malicious.
2. Rate limiting algorithm based on observation that in the case of virus propagation infected machine attempts to connect two different machines in small time interval which uninfected machine at lower rate and more likely to repeat connection attempt to recently.
3. Maximum entropy detector is algorithm based on estimation of traffic distribution using maximum entropy estimation. They have used 2,3,4,8 packet classes.
4. NETAD–this algorithm is based on rule based traffic model the filter removes uninterested traffic. The traffic anomaly detects on the basis of first few connection of the packet request which include all non IP packet, all TCP packets.

SDN suffers from lack of security at the control layer which creates hindrance in interaction between application layer and the network infrastructure layer. P. Porras et al. [15] have advocated that there is no concrete security model which implements key security feature trust model and policy mediation logic in the presence of multiple SDN application in sensitive computing environment. They have proposed a security extension at control layer which manages the security issues and resolve the conflicting flow rule which arises in the case of multiple SDN application. They have implemented their security extension with OpenFlow protocol with the Floodlight controller which is named as SE-Floodlight. This SE-Floodlight has included secure management application feature, authentication of services, roll based authorization, permission model for managing configuration changes request for data plane, conflict in flow rule, resolution of flow rule and security audit service.

D. Kreutz et al. [16] have also investigated solution for threat vectors. Replication is one of solution for stopping the threats like which are associated to the controller. Diversity is another techniques tool stopping the threats due to communication with controller. SDN paradigm creates new opportunities and challenges. The security is one of the major challenges in SDN. The security issues can be arising at different levels of security issues of controller, switches and in data transfer. They have categorized security threat vectors in seven categories on the basis of their attacking places. They have also summarized the solution for these attacks in Table 1 which describes the types of security threats, effect of the threats in SDN or consequence in SDN, tentative solution for respective threats and properties fulfil by the solution of respective threats.

3.4. Security for OpenFlow

OpenFlow protocol is used to implement the control management of SDN at controller. This OpenFlow protocol consists of master table, group table, secure channel, flow table as shown in Figure 5. Flow table entry contains rules for taking action for forwarding data. Group table consists of more complex forwarding behaviours which may be applied to a set of flows. In the case of multiple controllers, they act as master/slave. This protocol does not support the security management. The researchers have also proposed solution to secure the OpenFlow protocol.

S. Shin et al. [17] have developed a security module for detecting and securing the network in SDN using OpenFlow. They have named this module FRESCO. It is a security application development frame work using OpenFlow protocol which allows security researchers to implement share and compose different security module. They have claimed that FRESCO implementation reduces the code writing up to 90%. Each FRESCO module has five interfaces: input, output, event, parameter and action. This tool replicates essential security function such as firewall, scan detector, attack deflector after just providing the volume to above mentioned interface. It also produces flow rule and provide a way to implement security directive to counter threads which are represented as FRESCO module. This tool has several security functions like: simple address blocking to complex flow redirection procedure. This tool also incorporates API which allows the addition of existing security tools.

OpenFlow protocol is used for implementing the SDN it creates a standard interface for connecting the switches to controller. This protocol does not provide secure communication between switch and controller. D. Samociuk [18] has compared different authentication and access control mechanism for a secure channel in OpenFlow. Some of the protocols are TLS, SSL, and IPsec. TLS another its predecessor are based on cryptography for securing the communication and provides and satisfied security requirements like confidentiality, integrity, authentication and nonrepudiation. It works into more centralized approach and distributed approach. X.509 is based on public key infrastructure (PKI) cryptosystem while of trust architecture uses decentralized authentication method. SSH protocol is also uses encryption based technology and user recognition. IPsec is a set of protocols and based on encryption based technology and protecting the transmission between host to host, network to network, host to network.

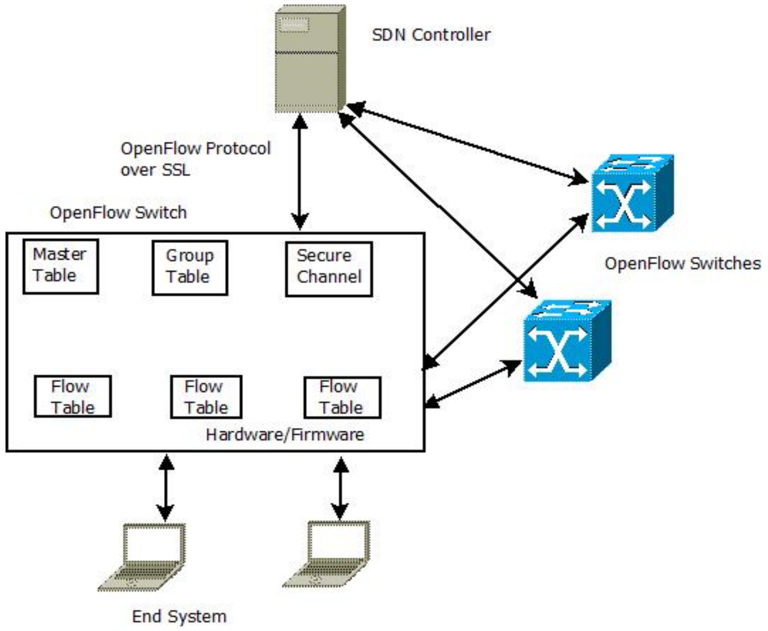

Figure 5. A model of attacks on OpenFlow switch

4. Conclusion

SDN is new paradigm for improving the existing network infrastructure. It separates the management related activity from the devices and uses the centralized approach for route discovery and other management related issues. The centralization of the management activities is silent feature of the SDN. This feature is major challenge for the security issues. The centralization is going to create a single point failure in case of malicious attack at the controller. The new security features should be added for strengthen the concept of SDN. In this paper we have included solutions for the problems of malicious attack due to spoofing, tempering, Denial of Service, authorization, single point of failure etc. provided by the researchers to fulfil the security requirements like authentication, integrity, authorization etc. We have also categorized the solutions provided by the researchers on the basis of their security requirements.

References

[1] Yuyang Lu, et. al. Based on Radius and AAA Authentication of the Campus Networks Security System Design and Implementation. *TELKOMNIKA Indonesian Journal of Elecrical Engineering*. 2014; 12(4): 3040-3045.

[2] Shashank Tripathi, et. al. Secure Routing Protocol for Integrated UMTS and WLAN Adhoc Networks. *Bulletin of Electrical Engineering and Informatics*. 2016; 5(4): 469-488.

[3] Azeem Mohammed Abdul, et. al. Attacks of Denial of Service on networks layer of OSI model and maintaining of security. *Indonesian Journal of Electrical Engineering and Computer Science*. 2017; 5(1): 181-186.

[4] Bekti Maryuni Susanto. Naïve Bayes Desicision Tree Hybrid Approach for Intrusion Detection System. *Bulletin of Electrical Engineering and Informatics*, 2013; 2(3): 225-232.

[5] S Hong, et al. *Poisoning Network Visibility in Software Defined Networks: New Attacks and Countermeasures*. NDSS, 2015.

[6] Ankur Nayak, et al. *Resonance: Dynamic Access Control for Enterprise Networks*. In Proceeding of the workshop on Research on Enterprise Networking (WREN). 2009: 11-18.

[7] R Holz, et al. *X.509 Forensics Detecting and Localising the SSL/TLS Men-in-the-Middle*. Proc. ESORICS. 2012: 217-34.

[8] C Soghoian, et al. *Certified Lies: Detecting and Defeating Government Interception Attacks Against SSL*. In Proceeding of Financial Cryptography and Data security. 2011: 250-259.

[9] I Dacosta, et al. *Trust No One Else: Detecting MITM attacks Against SSL/TLS without Third-Parties*. ESORICS 2012: 199-216.

[10] Aaron Gember, et al. *Toward Software-defined Middlebox Networking*. In Proceeding of the ACM Workshop on HOT Topics in Networks (HotNets), Redmond, WA, USA. 2012: 7-12.

[11] K Cabaj, et al. SDN Architecture Impact on Network Security. *ACSIS*. 2014; 3: 143-148.

[12] P Pinto, et al. DoS Detection on SDN Architectures Using Parametric Statistical Tests. *Advances in Applied and Pure Mathematics*. pp. 206-209.

[13] D Kotani, et al. A packet in message filtering mechanism for protection of control plane in OpenFlow networks. *ACM New Yark USA* 2014: 29-40.

[14] S A Mehdi, et al. *Revisiting traffic Anomaly Detection Using Software defined Networking*. In proceeding of the 14th International Symposium on Recent Advances in Intrusion Detection (RAID). 2011; 6961: 161-180.

[15] P Porras, et al. *Securing the Software Defined Network Control Layer*. Proceedings of the 2015 Network and Distributed System Security Symposium (NDSS), 2015.

[16] D Kreutz, et al. *Towards secure and dependable Software-Defined networks*. Proceeding of the second ACM SIGCOMM workshop on Hot topics in software defined networking – HotSDN'13. 2013: 55-60.

[17] S Shin, et al. *FRESCO: Modular Composable Security Services for Software Defined Networks*. In ISOC Network and Distributed System Security Symposium (NDSS), 2013.

[18] D Samociuk. *Secure Communication between OpenFlow Switches and Controllers*. The Seventh International Conference on Advances in Future internet. 2015.