July – August 2020
ISSN: 0193-4120 Page No. 395 - 401

Prevention of Address Spoofing Attacks in Software-Defined Networking: A Review

Ramesh Chand Meena
Scientist, STPI,
Ministry of Electronics and IT,
GoI,Jaipur–302022, India
rameshrmz@yahoo.com

Mahesh Bundele
Principal &Director,
Poornima College of Engineering,
Jaipur-302022, India
maheshbundele@poornima.org

MeenakshiNawal
Associate Professor,
SET, Poornima University,
Jaipur–303905,
Indiameenakshi.nawal@poornima.edu.in

Article Info
Volume 83
Page Number: 395 - 401
Publication Issue:
July - August 2020

Article History
Article Received*: 06 June 2020*
Revised*: 29 June 2020*
Accepted*: 14 July 2020*
Publication*: 25 July 2020*

Abstract

Software-defined networking technology advantages are attracting for its implementation in enterprises rapidly. It separates the data and control planes of network and OpenFlow protocol enabled simple forwarding devices forwards data packets. SDN control takes the responsibility of control plan. The source host generates data packet,and forwarding device forwards the packet to its destination taking details of destination address form such packet. Usually, the device does verify the genuinely of source host address. SDN controller monitors the data packet flows by making necessary flow entry the device. Initially,the device does not have flow entry, and it cannot send data packet of hosts. This data packet is forwarded to the controller by the forwarding device. The controller examines the packet field values and sets up required flow entry into the flow table of the device. In this condition, the attacker can carry out source address forged attacks and creates hindrance in network operations.The researchers have offered few techniques for the identification&prevention of such attacks. In this article, we propose anappraisal of methods of prevention of address spoofing attacks (PASA)developed for security of SDN setup. Our study describes different characteristics and limits of PASAsolutions. It offers research areas in SDN security for researchers.

Keywords: Spoofing, Address, Source, Attack,SDN, PASA, Prevention, Security

I. INTRODUCTION

SDN is an emerging technique and segregatesthe data and control planes from the existing switched networking. The routers and switches are generally forwarding devices.In the conventional network, these devices work with incoming packets and dependon the target host address[1]. In SDN,flow incoming packet is controlled with the help of flow entryof the OpenFlow forwarding device and the flow entry is based on various fields and their values of the packet header. SDNnetwork setup maintains the traffic statistics. SDN setup provides the simplicity, elasticity and programmability to the network managers. Several big data

July – August 2020
ISSN: 0193-4120 Page No. 395 - 401

centres are using this network technology to take the benefits of its features.

Initially, the OpenFlowforwarding device does not have monitoring &safety rules. It does not know the way to handle a data packet coming from a host. Generally, the device forwards the packet after checking the target host address. It does not verify the source host address authenticity[2]before sending the packet to next hop until it reaches to the target host. An attacker performs source address forging attacks taking advantage of such a situation and causes for chocking the network resources, making unavailable the network services to the legitimate users and man-in-the-middle attacks.

The researchers have offered several solutions to deal with this issue. In SAVSH[3], authors provide an IP prefix-based solution to prevent address spoofed attacks. In SDN-SAVI [4], authors offer an SDN security technique based on Address Assignment Messages (AAM) and binding of IP with switch port for validation at switch port level. In ISAVA [5], researchers present the extension of SAVSH for the inter-domain environment by adding an authentication header with the user packet. In SIPAV-SDN [6], authors givethe use of the ARP messages for creating binding of host address with switch port for the SDN setup. In PacketChecker[7], authors present the use of PacketIn messages to check the spoofed packets at the port level. In a study[8], the authors also compare the few source address validation techniques.

There are several mechanisms for mitigation and prevention of such attacks. In this article, we present ananalysis of techniques of prevention of address spoofing attacks (PASA) offered by researchers for the SDN environment. It identifies characteristics, limits and gapsofthe approaches. It also provides prospective areas for research in SDN security.

This paper is arranged into sections. In Sec-II,we present brief SDN background. In Sec-III, we describe the techniques of prevention of address spoofing attacks (PASA). In Sec-IV, we present comparison SDN PASA techniques.Sec-Vdescribes the findings and gaps found in SDN PASA techniques. In Sec-VI,we suggest research works for researchers in future. Finally, in Sec-VII,we conclude the study.

II. SDNBACKGROUND

SDN is dynamic, flexible, profitable, programmable, and fulfils high throughput bandwidth requirements. The nature of the latest network utilitiesis dynamic and requires repeated changes in it. The OpenFlow protocol is the base for the SDN system. The Open Network Foundation (ONF) promotes the use of the protocol and provides standards for connection between the controller and forwarding devices. RFC-7426[9] of IEFT describes the components of SDN architecture. The packet forwarding devices such as OpenFlow enabled routers, switches and hosts come under Infrastructure Layer (IL).Management Abstraction Layer (MAL)and Control Abstraction Layer (CAL)are two sub-layers of Control Layer (CL). IL connects with CAL using Management Plane (MP) and Control Plane (CP) southbound interfaces. Control Layer is between Application Layer (AL) and IL in SDN architecture. The secure service connectivity called as the northbound interface connects to AL and CL. Fig.1 shows the architectural diagram of the SDN system.

The Control Layerdecides the control message and forwards them to the forwarding devices to make entry into the flow table. The CL monitors; configures and keeps a record of attached forwarding devices. The Application Layer decides the behaviour of the network device, and it is applied in the form of a module. The Infrastructure Layer works to manage packets according to the instructionsof the CL, and it also manages recentsettings and status of forwarding devices.

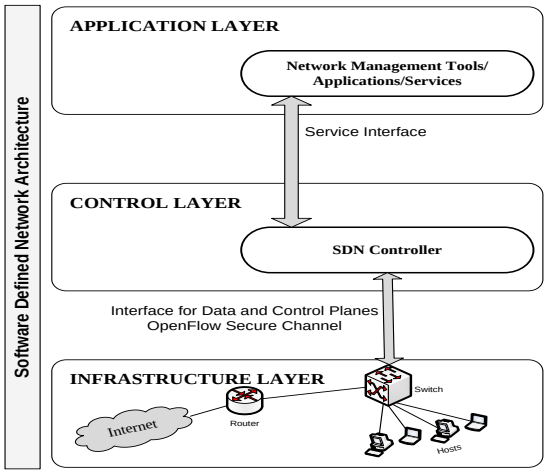

Fig. 1: Architecture of SDN

The features of SDN, such as abstraction of control from forwarding devices, network device programmability, centralization of net intelligence at the controller, network operations simplification, elimination of proprietary devices, andopen standardof the protocol are continuously increasing its suitability. The users are adopting it quickly to avail the benefits of thefeatures described above.

In IDH-SDN [10], the authors state that switch and controller greet for starting an OpenFlowlink. They exchange messages with each other using its TCP port& IPto start a secure &encrypted connection. Initially, the controller generates an OfptFeatureRequestmessage and sends to the forwarding devices. The device generates an OFPT_FEATURE_REPLY message with details switch and its active ports. It sends this message to the controller to

July – August 2020
ISSN: 0193-4120 Page No. 395 - 401

establish a connection. This handshaking process discloses the presence of forwarding devices but not interlinks between them. The controller needs details of network topology for the execution of several network monitoring and administrationoperations. It performs the critical task to identify devices, links between them, and configures paths into devices to make able them for sending packets the destination.

The OpenFlowforwarding device has a flow table and a group of sub-tables. The controller used OfptFlowMod messages to manage the flow tables. It is used to add, remove and modify the entry of the flow table. The flow has several fields, an actionand a set of counters in its structure. The arriving packet's fields values are matched with fields values of flow. After matching these values of the flow and packet, the related counter is increased, and related action is taken. In case these values do not match, then it raises an event. This table miss event directs to forwarding device about the packet to drop or forward to the controller. The forwarding device sends the packet to the controller by raising PacketInevent for its evaluation. The controller then decides appropriate action to the packet; it generates control packets using OfptFlowMod for the forwarding device and takes action as per security policy.

III. TECHNIQUES OF PASA

In this section, we present various approaches offered by researchers in SDN and traditional network environments. An approach supports and works only in the traditions network; such an approach is known as non-SDN approach. First, we discuss non-SDN methods.

The authors in mechanism[11]offer source address validation (SAV)for IPv6 network setupsto mitigate forged address attacks. It is built on First-Come-First-Serve (FCFS) to balance the ingress filtering method. It detects and prevents from spoofed IP attacks. It determines the source address of a host-based on FCFS until next change happens in it. It binds to the binding anchor the address of source hostsent in the first data packet. Its FCFS-SAVI-DB keeps binding details like source address, binding anchor, creation time,lifetime, status, prefix, binding anchor and interface. The authors discussed many SAV improvement (SAVI)methods to process transit packets and local packets, along with identifying the on-link prefixes. The SAV improvementmethodmainly works for local traffic with anchoring MAC&IPto switch port. The authors in [12] also suggest the use of Access control lists (ACLs) for checkingthe source and filter the packets with forged source IP in the network. The nature of ACLs is complex, and some time it creates collision with other safety rules in the network.

The researchers in[2]examine the efficiency and utilization of resources during the execution of the SAVI. They describe the system of SAVI,such as DHCP-SAVI [13]and FCFS [11]are offered to protect the first hop. The binding table is created using the tracking of network devices and neighbourdiscovery (ND) messages. The IP forged traffic is filtered using the same table. Most of the PASA approaches are offered in a traditional network and do not support SDN environment.

Non-SDN techniques provide two types of protections. The first method suggests a protocol redesign & encryption, and the second method suggests an IP filtering method. The PASA schemes like SANE[14], Passport[15], SPM[16], SEND SAVI[17]come under protocol redesign & encryption as they offer redesign of the protocol and use of encryption for the protection of forged IP attacks.

The PASA schemes like Ingress/Egress Filtering [3], DPM[18]/Traceback/iTrace[19], ACL[12], FCFS SAVI[11], uRPF [3]&DHCP SAVI [13] fall under IP filtering method as they offer IP filtering for the protection of forged IP attacks at various level of the network. The non-SDN PASA techniques are summarized in Table 1. We describe non-SDN schemes of PASA here for the background of the prevention of such attacks. It also provides a list of methods for trying in the SDN environment after some modifications.

The researchers offer some PASA techniques for the SDN setup. In this category, SAVSH [3] claims the maximum mitigation of the address spoofed attacks for SDN network. In this scheme, the essentialcomponents are topology detection, filtering rule generation and checkpoint selection. The topology detection and creation of a sink tree are limited to the discovery of links connecting the forwarding devices. It does not detect and keep the details of live hosts. This scheme uses IPs prefix in flow entry to mitigate attacks. An attacker can perform address forged attack within the same network due to use of the IP prefixes.

July – August 2020
ISSN: 0193-4120 Page No. 395 - 401

Table 1:
Non-SDN PASA Techniques (6=IPv6. 4=IPv4, G=Good, H=High, M=Moderate, F=Flexible, I=Inflexible, C=Complex, S=Simple)

Parameter	Source IP Address Filtering						Protocol Redesign/ Encryption			
	DHCP SAVI[13]	FCFS SAVI[11]	Ingress/ Egress Filtering [3]	ACL[12]	Traceback/ iTrace [19] /DPM[18]	uRPF[3]	SEND SAVI[17]	SPM [16]	Passport[15]	SANE[14]
IP Support	6, 4	6	4	6, 4	6, 4	4	6	6	4	6, 4
Messages Used	NS, NA, RA DHCP	NS, NA, RA	NS, NA, RA	ACL Commands	ICMP Messages	All Packets	Secure NS, NA, RA	Key association messages	Secret Keys Packets	SANE Header & Encrypted Source Route
Complexity	Easy with SAVI enabled Switches	Easy with SAVI enabled switches	C	C and conflicts with other policies	S	C	C; need Cryptographic enabled	C; Source and IPSec enabled target host	C; need execution at Source & Target Hosts	C
Filtering Accuracy	H	H	M	M	G	G	G	G	G	G
Dynamic Network	F with SAVI enabled device	F with SAVI enabled device	I	I	I	I	F using Cryptographic enabled device	F	F	F
Validation at	Source Port	Source Port	Edge Network	Switch	Router	Router	Destination	Destination	Destination	Domain Controller
Development Cost	SAVI enabled device	SAVI enabled device	Router/ Firewall	Network Admin cost	Router	uRPF at Router	Cryptographic enabled device	IPSec enabled device	Passport execution at Host & Router	Protocol execution & Domain Controller

Table 2
SDN PASA Techniques (S=Supported, C=SDN Programming/ Applications/ Services Development, 4=IPv4)

Parameter	SAVSH[1]	SDN-SAVI[4]	SIPAV-SDN[6]	ISAVA [5]	PacketChecker [7]	INSPECTOR [20]	DosDefender [21]	Literature [22]	Literature [23]
IP Support	4	4	4	4	4	4	4	4	4
Messages Used	SNMP packets	AAM packets	ARP packets	SNMP packets	PacketIn messages	PacketIn messages	PacketIn messages	ARP messages	TTL Value
Complexity	Moderate	Simple	Simple	Moderate	Moderate	Moderate	Moderate	Moderate	Moderate
Binding/Filter Parameter	Network IP-Prefixes	IP & Switch Port	IP, MAC & Switch Port	IP-Prefixes /IGuarantee header & Encryption	IP, MAC	IP, MAC	IP, MAC	MAC, IP	MAC, IP
Filtering Accuracy	Less	Moderate	High	Less	High	Moderate	High	High	High
Dynamic Network	S	S	S	S	S	S	S	S	S
Validation At	Network	Switch Port	Switch Port	Network	Switch Port	Special Device	Switch Port	Switch Port	Host Level
Development Cost	C	C	C	C	C	C & Inspector	C	C	C

Expended name of the acronym given in table 1:

ACL: *Access Control List*
DHCP: *Dynamic Host Configuration Protocol*
DPM: *Deterministic Packet Masking*
ICMP: *Internet Control Massage Protocol*
iTrace: *ICMP Traceback*
SANE: *Secure Architecture for the Networked Enterprise*
SEND: *Secure Neighbor Discovery*
SAVI: *Source Address Validation Implementation*
SLAAC: *Stateless Address AutoConfiguration*
SPM: *Spoofing Prevention Method*
uRPF: *Unicast Reverse Packet Forwarding*

TEST Engineering & Management

July – August 2020
ISSN: 0193-4120 Page No. 395 - 401

The authors in SDN-SAVI [4] present a scheme to bind IP with switch port for validation of source address at the first hop of network traffic. The prevention of forged IP attack is achieved by the authors with matching the IP of the source host with the address of flow entry. The packet is dropped at switch port level, which is not matching with flow entry field values. Since it uses the switch port and source IP for anchoringbut without MAC of the source host, it does not identify the host completely. The source IP, MAC, and switch port binding can provide fine-grain filtering.

In SIPAV-SDN[6], researchers present a scheme addressing the issues of [3]&[4]by utilizing the 1stARP message from the host. It updates HostTableextracting the host informationsuch as MAC, IP and switch port from ARP message and sets up the flow entry regarding the data packets of a host. Since it is utilizing ARP messages to discover the host and extract the details for matching flows. Anillicit usercan generate ARP messages with the forged source address and mislead the scheme. This issue affects the approach working,and the system extractsincorrect host information from such ARP messages.

The authors in ISAVA[5] present a scheme for the protection of inter-domain by sharing a secret key with the help of IGuarantee 40 bytes header. The use of IGuarantee header increases the size of the packet, and sometime it may cross the maximum transmission unit (MTU) size. It is not permitted in most of the IPv4 networks. It also increases the bandwidth utilization and processing overheads for the SDN controller at the sender side and receiver side. It uses SAVSH for intra-domain security.

The authors in PacketChecker[7] present a scheme for the protection of packet injection attacks with a spoofed address. It maps a switch port with the MAC address of a host and provides security at switch port level. The authors in Inspector [20] present a technique with a device which inspects the malicious packets to ensure a solution against attacks of forged IP packets. This technique uses PacketIn messages. In DosDefender[21]method, authors present a module for online protection of malicious packet to SDN setup. It uses PacketIn messages and MAC_Port table to provide security at switch port level. The authors in [22] present an event-based scheme to detect the forged IP traffic and protect the SDN network. The authors in[23]give a system for mitigation the attacks of IP spoofing in hybrid SDN setup.

IV. SDN PASATECHNIQUES

This section compares the techniques of prevention of address spoofing attacks developed for SDN environment. In the above section, we describedseveral SDN approaches for PASA,and now we present the comparison based on messages used; complexity and filtering accuracy.

The SAVSH is using SNMP packets for collecting topology details, and its complexity is moderate. The accuracy of the approach is less as it is using IP prefixes. The SDN-SAVI is using the address assignment message (AAM) for the collection host details, and complexity-wise it is simple. The accuracy of the approach is moderate as it is using the binding between IP and switch port.The SIPAV-SDN is using ARP message for the collection host details, and complexity-wise it is simple. The accuracy of the approach is high as it is using the anchoringof switch port with source IP, MAC. The ISAVA is using SNMP packets for the collection intra-domain host details, and it is also using IGuarantee header & encryption key for the authentication of inter-domain hosts. The complexity-wise it is moderate. The accuracy of the approach is less as it is using IP prefixes. It also increases the packet size. It requires more bandwidth and processing resources.

The PacketChecker is using PacketIn message for the collection host details, and complexity-wise it is moderate. The accuracy of the approach is high as it is using the binding between source MAC and the switch port.The Inspector is using PacketIn message for the collection host details, and complexity-wise it is moderate. The accuracy of the approach is average as it is using the binding between source MAC and switch port but using an additional device-Inspector.The PacketChecker is using PacketIn message for the collection host details, and complexity-wise it is moderate. The accuracy of the approach is high as it is using the anchoring of switch port with source MAC. The comparison of the SDN PASA techniques is given in table 2.

Most of the SDN PASA techniques are supporting IPv4 and dynamic networks. The development cost of the approaches is SDN application & service programming. The Inspector needs an additional device.

V. FINDINGS AND GAPS INPASA MECHANISMS

Findings:

- ISASA, SIPAV-SDN and SAVSH techniques are proposed to implement in hybrid SDN networks.
- Anchoring is created based on host traffics. The port binding with IP & MAC provides high accuracy and performance for filtering of malicious packets.
- Some approaches use particular messages such as AAM in such a way that offered SDN-SAVI cannot be protected from IP forging.
- The detection and transformation of topology into a sink tree of SAVSH is not detecting the live host, and it is detecting only interlinks in forwarding devices.
- ISAVA is using IGuarantee 40 byteslong header and encryption key for inter-domain validation of source address. The IP prefixes are used in the flows of SDN switch by the SAVSH approach.An attacker can generate traffic with a forged origin address within the same network.
- The size of network may be dynamic for most of PASA approach.
- Most of the approaches are executed at the controller level.
- SIPAV-SDN does not propose any modificationat the packet or host level.
- Network-level verification is offered by SAVSH& ISAVA whereas others are proposing checkat the ingress point of packets (host or switch port level).
- Inspector requires an additional device for its execution.

July – August 2020
ISSN: 0193-4120 Page No. 395 - 401

Gaps

- In SAVSH & ISAVA, Sink tree generation is restricted to the detection of interlinks connecting forwarding devices. The live hosts are not included in the sink tree. It is known that without host details fine-grain filtering is not achieved.
- In SAVSH & ISAVA, the IP prefixes in flow entry are used, and it indicated the group of IPs. It checks that the source host belongs to this group or not. The use of IP prefixes in the flows provides a change to an attacker to perform spoofing attacks within the same network.
- In SDN-SAVI, AAM packers are used to create a binding table. In SIPAV-SDN, the ARP messages used to create HostTabledetails. An illicit host can produceaddress spoofed ARP/AAM messages to mislead the generation of binding information.
- In SDN-SAVI, researchers use the anchoring in the IP &Switch Port for validation of packet source. The validation of source without MAC of the host does not provide fine-grain filtering and not identify the complete host details.
- In Inspector, authors propose an additional device as Inspector for validation of source. This device has its capacity of processing and bandwidth.
- In ISAVA, an IGuarantee header and encryption key are proposed. The extra header increases the size of the packet and needs more bandwidth and processing power. Sometimes, it increases the size of the packet more than MTU size, which is not permitted in some networks.

VI. Future Works

In this section, we suggest some research areas in SDN security. The researchers may work on them in future. The sink tree of SAVSH does not keep connected hostsinformation. The approach does not offer any scheme for the discovery of hosts. Any scheme does not propose a mechanism for setting up the controls and rules before the generation of actual traffic of the connected host. The researcher may develop a new tool to detect a live host beforegenerating real traffic by it. The researcher may develop a method for proactive setting up of safety rules and control policies beforereal traffic generated bythe hosts.

The ARP/AAM messages produced by the connected host are used in SIPAV-SDN and SDN-SAVI to identify the details of the host. The researchers may work on developing a technique for the generation of secure packets internally to ascertain the host details like IP, MAC, switch port etc.

The SDN-SAVI and SIPAV-SDN are using IP, MAC and switch port for anchoring and validation. The techniques are generating a vast number of flows. It causes the exhaustion of the limit of the flow table. Therefore, the studies are necessary to examine the resource utilization and effects of massive flow generation. It also needs optimization of flow rule generation to increase the efficiency of the flow table.

We also suggest the development of PASA and source address validation techniques for IPv6 networks. The researcher may also implement the non-SDN PASA techniques in SDN set up after the required modifications.

VII. Conclusion

We present a review of the techniques of prevention of address spoofing attacks in SDN. This paper also discusses non-SDN prevention techniques with summery. We offer the categorization of PASA techniques as SDN supported methods and traditional network techniques. Our study compares the SDN based techniques on various parameters such as IP support, messages used, binding/filtering parameters, and filtering accuracy. It is observed that most of the mechanisms support IPv4, and there is a requirement to develop such techniques for IPv6 environment. The findings and gaps section mentions various features and limitation of PASA techniques. The future work section describes the research areas for researchers based on gaps identified during the review.

References

[1] M. Z. Masoud, Y. Jaradat, and I. Jannoud, “On preventing ARP poisoning attack utilizing Software Defined Network (SDN) paradigm,” in *2015 IEEE Jordan Conference on Applied Electrical Engineering and Computing Technologies (AEECT)*, 2015, pp. 1–5.

[2] O. Strugaru, A. D. Potorac, and A. Graur, “The impact of using Source Address Validation filtering on processing resources,” in *2014 10th International Conference on Communications (COMM)*, 2014, pp. 1–4.

[3] G. Chen, G. Hu, Y. Jiang, and C. Zhang, “SAVSH: IP source address validation for SDN hybrid networks,” in *2016 IEEE Symposium on Computers and Communication (ISCC)*, 2016, pp. 409–414.

[4] B. Liu, J. Bi, and Y. Zhou, “Source address validation in software defined networks,” *SIGCOMM 2016 - Proc. 2016 ACM Conf. Spec. Interes. Gr. Data Commun.*, no. Dc, pp. 595–596, 2016.

[5] C. Zhang *et al.*, “Towards a SDN-Based Integrated Architecture for Mitigating IP Spoofing Attack,” *IEEE Access*, vol. 6, pp. 22764–22777, 2017.

[6] R. C. Meena, M. Nawal, and M. M. Bundele, “SIPAV-SDN: Source internet protocol address validation for software defined network,” *Int. J. Innov. Technol. Explor. Eng.*, vol. 8, no. 12, pp. 3386–3393, 2019.

[7] S. Deng, X. Gao, Z. Lu, and X. Gao, “Packet injection attack and its defense in software-defined networks,” *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 3, pp. 695–705, 2018.

[8] R. C. Meena, M. M. Bundele, and M. Nawal, “Appraisal of Source IP Validation Techniques in SDN,” in *2019 4th International Conference and Workshops on Recent Advances and Innovations in Engineering (ICRAIE)*, 2019, pp. 1–5.

[9] E. Haleplidis, K. Pentikousis, S. Denazis, J. H. Salim, D. Meyer, and O. Koufopavlou, “Software-Defined Networking (SDN): Layers and Architecture Terminology,” *IEFT*, vol. 1, no., pp. 1–35, 2015.

[10] R. C. Meena, M. Nawal, and M. Bundele, “Instant detection of host in SDN (IDH-SDN),” *Int. J. Recent Technol. Eng.*, vol. 8, no. 3, pp. 5603–5608, 2019.

[11] C. P. G. Machado, “FCFS SAVI: First-Come, First-Served Source Address Validation Improvement for Locally Assigned

July – August 2020
ISSN: 0193-4120 Page No. 395 - 401

IPv6 Addresses," *Internet Eng. Task Force*, vol. 3, no. September, pp. 1–47, 2012.

[12] B. Liu, J. Bi, and A. V. Vasilakos, "Toward incentivizing anti-spoofing deployment," *IEEE Trans. Inf. Forensics Secur.*, vol. 9, no. 3, pp. 436–450, 2014.

[13] J. Bi, J. Wu, G. Yao, and F. Baker, "Source Address Validation Improvement (SAVI) Solution for DHCP," *Internet Eng. Task Force*, pp. 1–54, 2015.

[14] M. Casado *et al.*, "SANE : A Protection Architecture for Enterprise Networks," in *Proc. USENIX Secur. Symp.*, 2006, vol. 49, p. 50.

[15] X. Liu, A. Li, and X. and W. D. Yang, "Passport : Secure and Adoptable Source Authentication University of California, Irvine," in *USENIX Symposium on Networked Systems Design and Implementation*, 2008, pp. 365–378.

[16] A. Bremler-Barr and H. Levy, "Spoofing prevention method," in *Proceedings - IEEE INFOCOM*, 2005, vol. 1, pp. 536–547.

[17] M. Bagnulo, "SEcure Neighbor Discovery (SEND) Source Address Validation Improvement (SAVI)," *Internet Eng. Task Force M. Bagnulo*, pp. 1–38, 2014.

[18] A. Belenky and N. Ansari, "IP traceback with deterministic packet marking," *IEEE Commun. Lett.*, vol. 7, no. 4, pp. 162–164, 2003.

[19] S. Bellovin, M. Leech, and T. Taylor, "ICMP Traceback Messages," *Internet Eng. Task Force*, pp. 1–18, 2003.

[20] A. S. Alshra'a and J. Seitz, "Using INSPECTOR Device to Stop Packet Injection Attack in SDN," *IEEE Commun. Lett.*, vol. 23, no. 7, pp. 1174–1177, 2019.

[21] S. Deng, X. Gao, Z. Lu, Z. Li, and X. Gao, "DoS vulnerabilities and mitigation strategies in software-defined networks," *J. Netw. Comput. Appl.*, vol. 125, pp. 209–219, 2019.

[22] N. Hubballi and N. Tripathi, "An event based technique for detecting spoofed IP packets," *J. Inf. Secur. Appl.*, vol. 35, pp. 32–43, 2017.

[23] F. Ubaid, R. Amin, F. Bin, and M. Muwar, "Mitigating Address Spoofing Attacks in Hybrid SDN," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 4, pp. 562–570, 2017.

AUTHOR'S BIOGRAPHY

Ramesh Chand Meena is working as a Scientist in Software Technology Parks of India, Ministry of Electronics and Information Technology, Government of India and pursuing a PhD degree in Computer Engineering with Poornima University, Jaipur, India. He completed Master of Technology (M.Tech.) in Computer Engineering in 2006 from Sam Higginbottom University of Agriculture, Technology & Sciences (formerly Allahabad Agricultural Institute), Allahabad, India, Master of Science (M.Sc.) in Computer Science in 2003 from MaharshiDayanand University, Rohtak, India. He has more than 22 years of working experience at various organizations of Government of India in the field of Computer Software Development, Computer Network Management and Implementation of Government of India schemes like Software Technology Park (STP) & Electronic Hardware Technology Park (EHTP). He has published more than 6 research papers in international/national journals and conferences. His research interests include Network Architecture and Security, Computer Programming, Software Defined Networks, etc.

Dr Mahesh Bundele is currently working as Principal and Director of Poornima College of Engineering, Jaipur since 1st September 2018. He has a total of 33 years of experience in teaching and research. He has developed many unique research methodology concepts and implemented. He is the mentor and controller of quality research and publications at the University. He is also responsible for the inculcation of innovative and critical analysis concepts across the University and the Poornima Foundation involving three other campuses. He did his doctoral degree in Wearable Computing and guiding research in Pervasive & Ubiquitous Computing, Computer Networks, and Software-Defined Networking. His areas of interests are also Wireless Sensor Networks, Algorithmic research, Mathematical Modeling, and Smart grids. He has more than 50 publications in reputed journals and conferences. He has been a reviewer of few IEEE Transactions. He is actively involved in IEEE activities in Rajasthan Subsection and Delhi Section and holding the responsibility on Standing Committee of IEEE Delhi Section for Technical & Professional activities for controlling the quality of conferences and publications in IEEE. He is also holding the position of vice-chair in Jaipur ACM professional chapter.

DrMeenakshiNawal is currently working as Associate Professor with the Poornima University, Jaipur, India. She is Gold Medalist in M.Sc (IT) from MDS University Ajmer. She has completed Ph. D (Computer Science) from BanasthaliVidhyapith, Jaipur. She is having 13 years of experience in Academics and Research.Her area of research is "Patient Authentication and Security measures in Remote Health Monitoring". She has attended many National and International Workshops, Conferences and Published papers in National conference.Her areas of research interest are Machine Learning, Deep Learning, Image Processing, Big Data Analytics and Software Defined Networks etc.