IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON RESEARCH CHALLENGES AND OPPORTUNITIES IN SECURITY AND PRIVACY OF BLOCKCHAIN TECHNOLOGIES

Received November 1, 2017, accepted December 6, 2017, date of publication December 19, 2017, date of current version May 9, 2018.

Digital Object Identifier 10.1109/ACCESS.2017.2785236

Towards a SDN-Based Integrated Architecture for Mitigating IP Spoofing Attack

CHAOQIN ZHANG[1,2], GUANGWU HU[3], GUOLONG CHEN[4], ARUN KUMAR SANGAIAH[5], PING'AN ZHANG[3], XIA YAN[3], AND WEIJIN JIANG[6]

[1]National Digital Switches System Engineering and Technological Researcher Center, Zhengzhou 450002, China
[2]School of Computer and Communication Engineering, Zhengzhou University of Light Industry, Zhengzhou 450001, China
[3]School of Computer Science, Shenzhen Institute of Information Technology, Shenzhen 518172, China
[4]Huawei Technologies, Shenzhen 518055, China
[5]School of Computing Science and Engineering, VIT University, Vellore 632014, India
[6]College of Computer and Information Engineering, Hunan University of Commerce, Changsha 410205, China

Corresponding author: Guangwu Hu (hugw@sziit.edu.cn)

This work was supported in part by the 863 Project of China under Grant SS2015AA010203, in part by the National Natural Science Foundation of China under Grant 61472136 and Grant 61772196, in part by the Natural Science Foundation of Guangdong Province under Grant 2015A030310492, Grant 2015A030313592, and Grant 2014A030310299, in part by the Fundamental Research Project of Shenzhen Municipality under Grant JCYJ20160301152145171, Grant JCYJ20170817115335418, and Grant 20160415113927863.

ABSTRACT Current Internet packet delivery only relies on packet's destination IP address and forwarding devices neglect the validation of packet's IP source address, it makes attackers can leverage this flaw to launch attacks with forged IP source address so as to meet their vicious purposes and avoid to be tracked. In order to mitigate this threat and enhance Internet accountability, many solutions have been proposed either from the intra-domain or the inter-domain aspects. However, most of them faced with some issues hard to cope with, e.g., low filtering rates, high deployment cost. And most importantly, few of them can cover both intra-domain and inter-domain areas at the same time. With the central control and edge response pattern, the novel network architecture of software defined networking (SDN) possess whole network intelligence and distribute control rules directly to edged SDN switches, which brings a good opportunity to solve the IP spoofing problem. By taking advantage of SDN, in this paper, we propose an SDN-based integrated IP source address validation architecture (ISAVA) which can cover both intra- and inter-domain areas and effectively lower SDN devices deployment cost, while achieve desirable control granularities in the meantime. Specifically, within autonomous system (AS), ISAVA relies on an SDN incremental deployment scheme which can achieve IP prefix (subnet)-level validation granularity with minimum SDN devices deployment. While among ASes, ISAVA sets up border server and establishes a vouch mechanism between allied ASes for signing outbound packets so as to achieve AS-level validation granularity. Finally, conducted experiments confirm that ISAVA intra-domain scheme can get beyond 90% filtering rates with only 10% deployment in average, while the inter-domain scheme can get high filtering rates with low system cost and less storage usage.

INDEX TERMS Cyber-security, IP address validation, software-defined networking.

I. INTRODUCTION

IP source address spoofing or IP spoofing attack, it refers to attackers release packets with forged IP source addresses so that they can conceal their real identities and launch attacks, e.g., reflect network traffics to flood victim hosts. Once suffering such attack, it is hard for victim to trace back to perpetrators and identify their real identities, which severely compromises Internet accountability indeed. From the perspective of technique, IP spoofing threat is derived from the design that Internet packet forwarding in routers only relies on packet's destination IP address, but neglects the validation of packet's IP source address to verify sender authenticity. Taking this vulnerability, attackers can launch serious attacks against specified targets, and as a matter of fact, most of attack directly related with this volubility, i.e., TCP-SYN flooding [1], DDoS [2] and Smurf [3].

Despite anti-IP spoofing has been studied extensively in the past decade, however, feasible and integrated solutions

that cover both of intra-domain and inter-domain scopes still under the way of research. As a matter of fact, the IP spoofing phenomena in Internet did not improve much in the last few years. According to the Center for Applied Internet Data Analysis (CAIDA)'s statistics [4], by end of October 2017, the spoofable address space, prefix, and AS have up to 26.7%, 33.6% and 34.1%, respectively. Also, the global cyber-security event recording proves that the number of IP spoofing and related attacks has sharply increased in last few years [5]. More than that, the annual report [6] regarding Chinese Internet security status confirms that the new IP spoofing-related attack means, such as Distributed Reflection Denial of Service (DRDoS) [7], DNS request reflection, Network Time Protocol (NTP) synchronization reflection, are thrived and abused to target at many high-value websites.

In order to mitigate this threat, many intra-domain or inter-domain solutions have been proposed. The former mainly solve the issue within Autonomous System (AS), while the latter cover the area between ASes. In Detail, solutions within domain for anti-IP-spoofing can be categorized into packet filtering, address encryption and protocol modification. Packet filtering is a common practice for anti-spoofing in many domain networks, e.g., configuring Access Control List (ACL) rules onto intra-domain routers or switches so that they can drop packets with unexpected/illegal IP source addresses or prefixes. As to the legal IP address set, it may be defined by admins (e.g., allowable IP prefix list) or machine learning based approaches (e.g., hop-count history and bloom filtering). But such methods share three aspects of drawbacks at least: (1) ACL is proved to be complex and may conflict with existing rules; (2) It is inflexible and hard to cope with situations such as topology dynamics and routing asymmetry; (3) Filtering accuracy is also a big concern since the way of self-learning would incur false positive or false negative problems to some degrees. In addition, the rest two types of solutions are also faced with common challenges in system implementation and deployment cost, since either IP address encryption or protocol/host-stack modification will inevitably introduce extra costs, e.g., Public Key Infrastructure (PKI) systems and router/host software upgrades.

Inter-domain solutions mainly concentrate on three directions: end-based, end-to-end and path-based filtering. End based filtering method specifies AS border device drops the inbound packets with source addresses belong to the local AS and the outbound packets whose source addresses belong to other domain. End-to-end filtering idea establishes a connection between two ASes' border devices and ignores ASes along the path. And each source-destination pair ASes shares a secret key so that the source AS can tag the packets header to destination AS and the destination AS can verify the packets authenticity. Path based filtering proposal verify the packets by the paths they flow through as the attacker usually cannot manipulate the forwarding path. Although these solutions achieve good effect for anti-spoofing between ASes, they still face many issues to solve. For example, end-based filtering methods are hard to satisfy network admins' filtering accuracy demands since the filtering space is divided into local domain and outside domain areas, and end-to-end filtering could be suffered attacked in the situation of shared keys compromised, while path-based filtering may encounter the system scalability issue since routing in inter-domain is dynamic.

As Software Defined Networking (SDN) owns the capacity of global topological view and central control pattern, it has gained much attention from both academic and industrial communities in recent years. With SDN, traditional ACL can be interpreted by flow rules in SDN-supported switches (or SDN switches), which can be issued by logically centralized controllers based on network real-time situations. Thus, SDN offers us an opportunity to solve the IP spoofing issue and overcome defections existing in traditional solutions. Inspired by this motivation, in this paper, we propose an SDN-based Integrated IP Source Address Validation Architecture (ISAVA) which can cover both intra- and inter-domain areas and effectively lower SDN devices deployment cost but achieve desirable control granularities. Specifically, within Autonomous System (AS), ISAVA propose an SDN incremental deployment plan which can achieve IP prefix (subnet)-level validation granularity with minimum SDN devices deployment. Thus the most exciting advantage of this plan is that it can gain the maximal IP source address validation effect by deploying the minimal SDN switches into traditional networks, which can keep existing network assets to the maximal degree that can promote system incremental deployment. While among ASes, ISAVA sets up SDN controller in each AS's border and establishes a vouch mechanism between allied AS controllers for outbound packets so as to achieve AS-level validation granularity. What's more, since the topological information of each AS is partly visible to other allied ASes, and the packet's original source address is replaced by its SDN border controller's IP address, our inter-domain solution also can get trade-off between privacy and security. Finally, through our conducted experiments, we confirm that ISAVA intra-domain scheme can get at least 90% filtering rates with only 10% deployment in average, while ISAVA inter-domain scheme can get high filtering rates with low system cost and less storage usage. Compared to existing studies, our main contributions are as follows:

1. We propose an integrated IP spoofing validating solution named ISASA, which can cover both intra- and inter-domain areas effectively with lower SDN devices deployment cost. It is a novel design that combines SDN architecture and protocol redesign to realize IP source address validation purpose.

2. In intra-domain scenario, we leverage the SDN control pattern to computes key nodes location and takes SDN switches to replace traditional devices in these nodes, so that it can gain a balance between fake packets filtering rate and deployment cost. To the best of knowledge, it's the first idea to use SDN technology to realize this purpose

3. In Inter-domain part, we propose a time-synchronized packet signature signing and verification protocol between

AS alliances. Through the established allied relationship, two ASes can exchange secret key, network abstract view and other information. Eventually, packets shuttle between one pair of allied AS will be tagged signature header in source AS and removed after they have been verified in the destination AS.

The rest of this paper is organized as follows. Section II summarizes related work. Section III depicts the attacking model in intra- and inter-domain scenario separately. Section IV elaborates on ISASA's architecture and mechanisms in details. Section V evaluates system performance. Finally, we conclude the whole paper in Section VI.

II. RELATED WORK

A lot of related work that focuses on the subject of intra- and inter-domain IP source address validation approaches gives us many aspirations. We will elaborate them in the following section.

A. INTRA-DOMAIN SOLUTIONS

1) IP SOURCE ADDRESS FILTERING

Depending on the acting positions, filtering solutions can be divided into three types: ingress-, egress- and router-based filtering, which checks packet legitimacy in router's ingress ports, egress ports and internal modules, respectively. For instance, the unicast Reverse Path Forwarding (uRPF) [8] is a deployable ingress filtering solution, which was advocated by Cisco and applied to its products. When uRPF function is enabled, for every packet, router's ingress port first looks up its Forwarding Information Base (FIB) with packet's IP source address, so that it can verify the packet's legality based on whether the forwarding port matches the current ingress port or not. However, uRPF is proprietary mechanism and it is hard to cope with the situations when both the victim and the attacker are in the same direction, routing asymmetry and etc. In order to overcome this drawback, SAVI [9] sets up a Layer2 (L2) switch in a user access subnet, which can filter spoofing packets by establishing a binding relationship between the IP source address, the MAC address and the ports of each access host. Thus, the filtering granularity in SAVI is single hosts rather than IP prefixes, which is much more accurate than uRPF. By Utilizing SAVI switch, we also proposed a general IP source validation and traceback framework for almost IPv4/IPv6 transition scenarios [10]. Still, the deployment cost is the biggest concern in this proposal since all legacy L2 switches have to be replaced by the SAVI switches. In addition, researchers also propose packet filtering solutions based on the bloom filtering [11], hop-count expectation [12] and even history IP filtering record [13], but all of which have confirmed that they either have the false positives or false negatives issues.

2) IP SOURCE ADDRESS ENCRYPTION

In order to authenticate communication correspondents, some researchers give their solutions from the angle of replacing the IP source address with the encrypted one. For example, Cryptographically Generated Addresses (CGA) [14] and Accountable Internet Protocol (AIP) [15] encrypt IP source address with the asymmetric key cryptography so that keys sharing both ends can verify each other. But such designs need extra secure key agreement protocols because key generation and public-key distribution are accomplished by individual hosts without Certificate Authority (CA), which is non-suitable for large-scale networks. To address this issue, TrueIP [16] takes IP source address as the public key and utilizes the Identity Based Cryptography (IBC) to produce the private key, so that correspondents can verify the authenticity of each other directly without public-key acquirements. However, it is uneasy to revoke IBC keys since all keys need to be regenerated if one private key is compromised.

3) PROTOCOL AND HOST-STACK REDESIGN

There are also some other schemes showing their merits from the aspect of protocol/host-stack redesign. For instance, SPM [17] and Base [18] solve this problem by leveraging some rarely used fields (e.g., ToS) in the IP header and replacing them with customized tags. But this design may disturb other special applications (e.g., Quality of Service). Additionally, SANE [19] redesigns the TCP/IP stack and introduces an isolation layer between networks and data link layers so as to achieve its purpose of traffic redirection and host authentication enforcement. Moreover, the Host Identity Protocol (HIP) [20] sets up a new layer named Host Identity (HI) in the middle of IP and transportation layers. It obtains reliable host identities through asymmetrically encrypting the HI data. But in the meantime, it complicates system implementation as it has to modify client's host-stack. More importantly, it needs to install a DNS-like system to resolve the mapping relationship between HI and IP addresses. Therefore, the largest overhead comes from their implementation and deployment.

4) SDN-BASED SOURCE ADDRESS VALIDATION

Till now, only few SDN-based approaches have focused on IP source address validation problem, e.g., Virtual source Address Validation Edge (VAVE) [21] and O-CPF [22]. The purpose of the former is to protect users under the SAVI switch being spoofed by other users within the same domain. To do so, VAVE establishes an IP source address protection zone comprising by all of Layer3 (L3) OpenFlow switches (OF-switch) and L2 SAVI switches. And the legacy network assets are posited outside this zone. Thus, any flows originated from the legacy switches and passed through this zone will be redirected to the controller to verify their IP source addresses authenticity, except that matching rules explicitly exist in the boundaries of the OF-switch. On the contrary, the goal of O-CPF is anti-IP-spoofing with the granularity of subnet prefixes in intra-domain. It leverages the SDN controller to compute the forwarding path for each prefix pair and tries to upgrade domain routers to accommodate

OpenFlow specification. By doing this, the OF-routers can check the validity for each packet passing by and drop illegal ones via issued rules from controller. Nevertheless, both of them incur large deployment cost and re-computation overhead in the topological dynamic situations. Besides that, our solution of SuperFlow [23] presented a novel idea by integrating L3 OpenFlow switch with L2 SAVI switch functions together so as to achieve effect of accept central controllers' commands to bind/report host binding information. Also, our previous work SAVSH [24] shows great merit on IP source address validation by deploying minimal SDN switches into networks within domain. Based on SAVSH, this paper extends working scenario into both intra-domain and inter-domain area, and integrates them so as to achieve better effect for spoofing packets filtering.

B. INTER-DOMAIN SOLUTIONS

1) END-BASED SOURCE ADDRESS FILTERING

The main idea of end-based filtering method is to drops the inbound packets whose IP source addresses belong to the local domain or the IP destination addresses do not belong to local. So it is usually used in domain boundary devices. The two classic proposes, ingress/egress filtering [2] and CatchIt [25], give us a lot of inspiration. For example, CatchIt proposes a way of validating inter-domain packets authenticity by enabling inter-domain routing system cooperation via an intelligent routing choice notification mechanism. However, CatchIt still has the implementation issue, thus it is hard to deploy and that hampers its promotion as well.

2) PATH-BASED SOURCE ADDRESS FILTERING

The Path-based filtering method verifies the forwarding path to identify the spoofing packets since attackers may modify packets' IP source addresses but they cannot manipulate packets' forwarding path in general. There are some work concentrates on path-based verification, like DPF [26] and IDPF [27]. DPF associates each source AS to a set of valid upstream ASes so that it can validate packets attribution by check their incoming AS. Theoretically, DPF can be very effective in inter-domain IP spoofing scenario, and it is extensively studied by other path based defense proposals. However, its filtering accuracy relies on the filtering sets' complete and accurate (i.e. a perfect filter), but how to quickly construct the perfect filters, the paper is not specified. By overcoming DPF's drawback, The IDPF constructs filters set by inferring feasible paths for every source AS. Detailly, it constructs feasible path set by analyzing routing entries or route export rules. For example, supposing AS u is a feasible upstream AS v for v reach to source AS s, if and only if u has exported to v via Border Gateway Protocol (BGP) protocol and v declares it as the best route towards s. Thus, an IDPF-enabled router can independently infer feasible paths by monitoring BGP update messages. However, since a feasible path is assembled by a lot of path segments, some involved path segments may not be taken by genuine packets.

3) END-TO-END (E2E)-BASED SOURCE ADDRESS FILTERING

The E2E-based filtering is on the basis of corporation between two ends (ASes) or two ASes composed alliance. Each alliance pair shares a secret key or establishes one particular communication protocol. Some studies, e.g., SAVE [28], SPM [17], Passport [29], DIA [30] and APPA [31], are the typical representatives. By learning the routing knowledges, SAVE introduces a new protocol and builds a filtering table into inter-domain routers. Through optimizing data structures and algorithms, the authors prove that the computation, storage, and network overhead can be handled by existing routers. However, since SAVE has to modify router devices' core software function so as to accommodate its protocols and filtering tables, the implementation and deployment cost are huge. Different SAVE, Spoofing Prevention Method (SPM) associates a unique temporal key with every AS pair and add tags into packets travel between the two ASes, so that receiver AS border routers can verify packets' authenticity and remove tags. But it shares the drawback with SAVE, the router software's upgrade hampers its promotion. Passport requires per packet cryptographic computation so as defy attackers' counterfeiting, but which makes it impossible to perform high-speed packet processing without new hardware. Therefore, the deployment cost of Passport is high. Similarly, DIA uses the same idea to form inter-domain anti-spoofing alliances. By adding and verifying MAC message in the packet, so the ASes belong to the party can identity the fake packets. Finally, APPA is a signature-based IP source address prevention method. It takes advantage of an automatically synchronizing state machine to exchange generate secrete state code (password) in a fixed time interval, and generate signatures for outbound packets based on current password.

III. THREAT MODEL

In this section, we first give the system model and related mathematic descriptions which covers both intra- inter-domain environments. Then we depict the threat scenarios in detail.

A. FORMALIZED DESCRIPTION

For better understand the IP spoofing problem and our system, we first give some formalized description in this section. Assuming in a domain network named D, the topology can be denoted as: $Topo_D = G(V, E)$, where V is the node/router set and E is the links between routers/edge collection. Also, we use the set $HOST_D = \{H_1, H_2, \ldots H_S\}$, $USER_D = \{U_1, U_2, ..U_Q\}$ and $IP_D = \{IP_1, IP2, ..IP_M\}$ to represent the collection of host, user and IP address in domain D, where S, Q and M are the total number of hosts, number of users and number of IP address, respectively.

Further, according to the IP packet's format, we can describe a IP packet as $packet = \{\text{version, length, IP}_{\text{src}},$

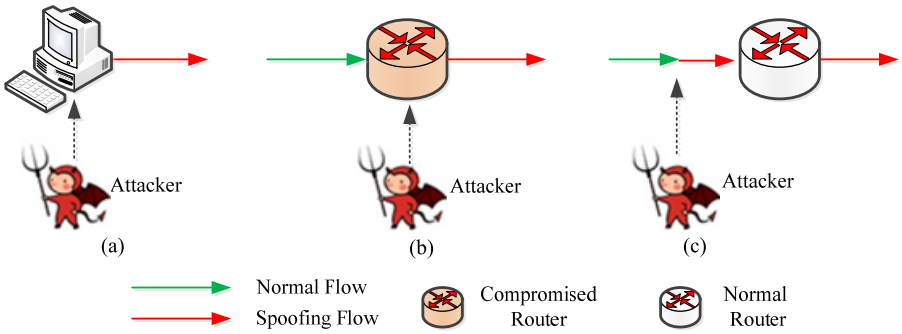


FIGURE 1. IP source address spoofing scenarios. (a) Host-based attack. (b) Router-based attack. (c) Flow-based attack.

IP_{dst}, data..}, items in which represent packet fields, such as packet version, length, IP source address, IP destination address, upper layer data and etc. Thus, all packet collection that source from domain D can be denoted as $Packet_D = \{\text{packet}|IP_{src} \in IP_D\}$.

In order to get the packet reliability, we believe that system needs to achieve both IP source address credibility and user credibility. The former one refers to every host has its own IP address or vice versa, which can be describe as $Host_D \leftrightarrow IP_D$. While the latter one states each packet's IP source address should be consistent with packet's true sender, which can be expressed as $IP_D \leftrightarrow User_D$. Thus, packet reliability can be denoted as $Host_D \leftrightarrow IP_D \leftrightarrow User_D$, *which* means elements in the end host set, IP address set and user identity set has a unique mapping relationship.

B. THREAT MODEL

Based on the attacker's location, we category the IP spoofing scenarios as three types: host-based attack, router-based attack and flow-based attack, as shown in Fig.1.

1) HOST-BASED ATTACK

Attackers forge packets with specified or random IP source address in IP header so as to launch attack and shift responsibility to other innocent people. This type of attack is very common in current Internet and it evolves a lot of versions till now, such as DDoS, reflected amplification DDoS and etc.

2) ROUTER-BASED ATTACK

Attackers may leverage routers' or key routing devices' vulnerability to take over their control privilege or even modify forwarding function so that attackers can pollute flowing through packets with false IP source address. Compare to the host-based attack, this kind of attack is much harder since network admins will pose enhanced security protection to these devices.

3) FLOW-BASED ATTACK

This kind of attack also knows as man-in-the middle attack, which refers to attackers posit half-way of packets flow through and conquer some key routing devices (e.g., wireless access point) so that they can capture, alternate and then replay them with forged IP source address to meet their vicious purpose.

Considering last two attack tricks are relative rare, we mainly consider the first threat in this paper.

C. ATTACK SCENARIOS

Also, according to the locations of spoofing source host and spoofing packets' destination, we summary the two attack scenarios that are intra-domain and inter-domain spoofing.

1) INTRA-DOMAIN SPOOFING

Intra-domain spoofing means both attacker and destination host are in the same domain, so the checkpoint in the domain border cannot effect and filter forged packets. Taking the scenario in Fig.2 as example, the spoofing host 10.192.123.2 pretends to be the host 10.192.123.10 and conduct an attack to victim host 10.192.123.11. If the router has not deployed any anti-spoofing measures, the attack could be harmed to destination host and pretending host both. Thus, this threat reminds us that anti-spoofing measures have to impose to intra-domain area, instead of domain border only.

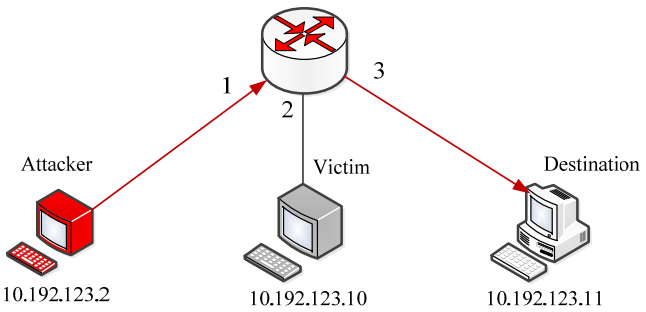


FIGURE 2. The illustration of intra-domain spoofing attack scenario.

2) INTER-DOMAIN SPOOFING

As various management policies exist in different ASes and routing flapping phenomenon happens occasionally between ASes, attacker could posit in any ASes and launch attack without traceback risk, which indicates deploying anti-IP-spoofing solution in inter-domain area is much difficulty than intra-domain area. For example, as Fig. 3 depicted, the spoofing host 14.19.80.30 in AS3 can

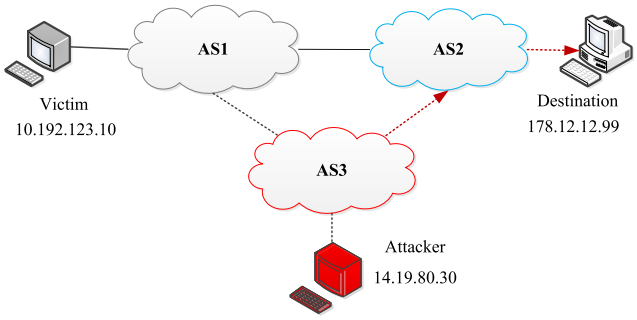


FIGURE 3. The illustration of inter-domain spoofing attack scenario.

emit packets with victim's address 10.192.123.10 and attack host 178.12.12.99 in AS2. Even worse, if attacker and victim are in the same direction, e.g., BGP routing flapping makes AS 3 needs to traverse AS 1 to reach AS 2, it will hard to distinguish normal flows from vicious flows in the destination AS or end-host.

IV. SYSTEM OVERVIEW

A. SYSTEM GOALS

Based on the above analytical formulation and attack scenario illustration, we learn that anti-IP-spoofing solution has to consider both intra-domain and inter-domain dimensions. For intra-domain dimension, even though we can get high filtering accuracy for spoofing packets if we deploy anti-measures into first-hop devices or replace these first-hop devices with anti-spoofing features devices for all access users, the deployment cost will too huge to bear to most networks. Thus the most difficulty in this dimension is how to balance filtering accuracy and deployment cost. While in inter-domain dimension, the most difficulty is how to distinguish normal flows from vicious flows because of complex BGP relationships between ASes and unfixed routing path. Thus our system has three goals as following:

(1) Covering both intra-domain and inter-domain dimensions: system has to build an integrated architecture that can cover two dimensions and impose measures for mitigating anti-IP-spoofing issue; otherwise single dimension coverage will compromise system ability and effectiveness.

(2) Balancing filtering accuracy and deployment cost: since high filtering accuracy and low deployment cost cannot achieve in the same time for traditional networks, thus system has to get a trade-off between desired accuracy and device deployment cost.

(3) High performance: system should possess high process capability so as to fit large-scale networks.

B. SYSTEM ARCHITECTURE

In order to realize above system goals, we propose an SDN- based Integrated IP Source Address Validation Architecture (ISAVA) with the help of SDN's centralized control capability. It can cover both intra- and inter-domain dimensions and effectively lower SDN devices deployment cost but owns desirable control granularities. Specifically, within AS area, ISAVA supports an SDN incremental deployment scheme which can achieve IP prefix (subnet)-level packet validation granularity with minimum SDN devices deployment. While among ASes, our architecture provides a packet signing and verification mechanism to achieve AS-level packet validation granularity. As Fig.4 shows, ISAVA relies on SDN controller in each AS that acts as a center intelligent brain to control all information and guides the inter-domain modules (IDM) and intra-domain module (DM) to meet requirements. The two part of modules work together and response to domain area and inter-domain area packet verification, respectively. Specifically, the IDM communicates with peer module to exchange key information, e.g., encryption key, topology information, and then guides SDN-enabled AS border device to sign outbound packets or verify packets' signatures for allied ASes. As DM, it computes intra-domain checkpoints node based on real-time substrate network topology, then generates filtering rules and distributes onto these checkpoint nodes so as to filtering spoofing packets within domain.

V. INTRA-DOMAIN SOLUTION

A. SYSTEM OVERVIEW

SAVSH (Source Address Validation for SDN Hybrid network) is our intra-domain proposal for filtering spoofing packets within domain. Its aim is to prevent the packets with forged IP source address to leave out domain or attack hosts within domain. As SDN technology has achieved great success and accepted by lots of networks, now most networks has partially deployed or considered to deploy SDN devices to meet their diversified purposes. Under such circumstances, the goal of SAVSH is to take advantage of SDN patterns to maximally filter spoofing packets but with minimal SDN devices deployment. In other words, SAVSH aims to obtain the best trade-off between filtering accuracy and deployment overhead. As illustrated in the topology of Fig.5 (a), all the nodes in the unprotected tradition network are unable to detect the spoofing flows originated by vicious host H1' which spoofs legitimate host H1's IP source address. With SAVSH design in Fig. 5 (b), we replace node A with a SDN device and takes it as a checkpoint to perform IP address filtering function.

Certainly, the node A still needs to be deployed some rules to perform filtering function. The rules are defined like pair ⟨Import, SIP, DIP, Action⟩. The "Import" item in the pair states the device port through which packets enters the device, then the SIP and DIP items are the source address and destination address separately, and the last item Action could be output(forward to appropriate port), drop and other options.

Although the above scenario is not complex, the main challenges come from three aspects as we stated: (1) locate deployment nodes (checkpoints) and prioritize them; (2) design controller application to distribute appropriate rules onto these SDN nodes; (3) adapt to network dynamics. Next we will explain how we solve these issues.

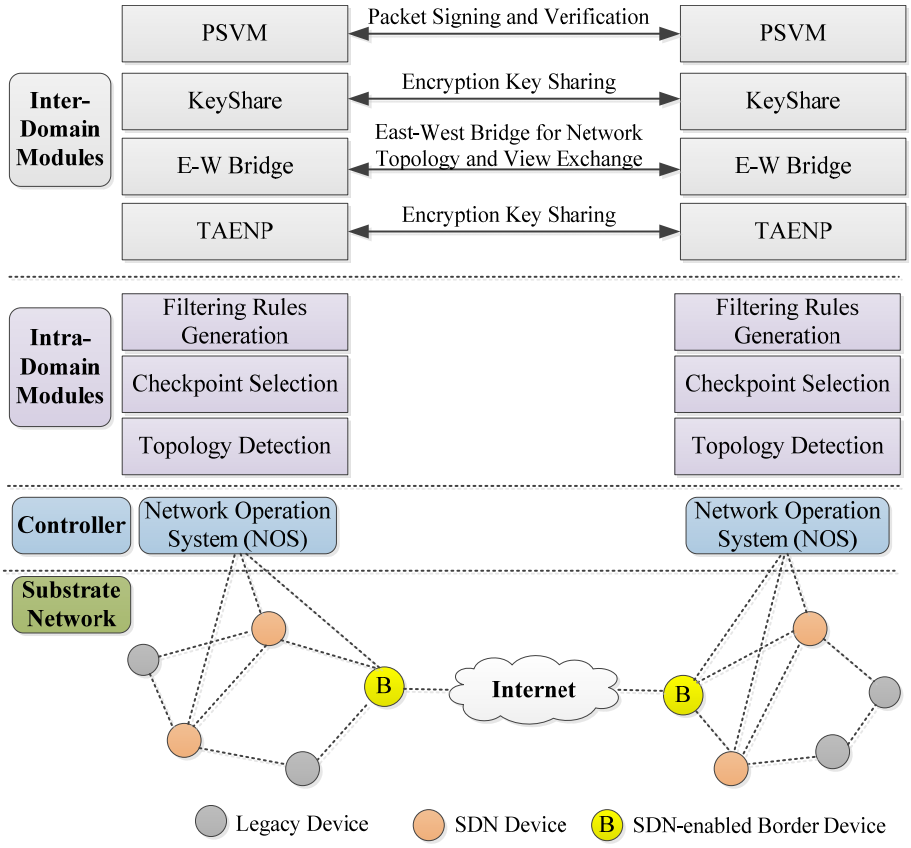


FIGURE 4. The logical diagram of system architecture (In each allied AS, there is a SDN controller that includes domain and inter-domain modules. The former one exploits global topology and computes checkpoints' location and distribute SDN rules onto these checkpoints so as to filter spoofing flows within domain area; Differently, the latter module communicates peer module between allied ASes so as to verdict inbound packets' legitimacy or sign signature for outbound packets to peer AS, this function is performed by SDN border device with yellow circle).

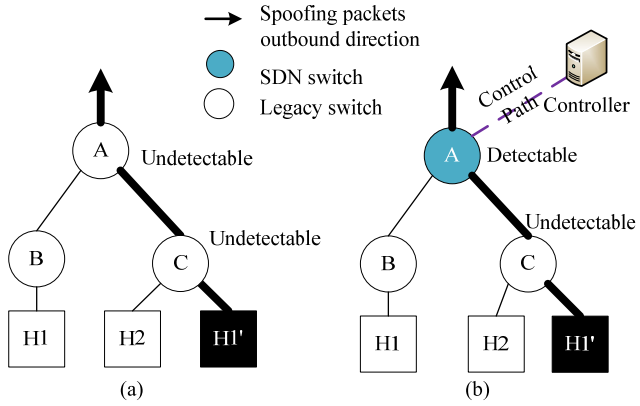


FIGURE 5. Intra-domain scheme overview. (a) Before SDN deployment. (b) After SDN deployment.

B. CONVERTING TOPOLOGY INTO SINK-TREE

In order to accurately find the deployment nodes, we first need to convert complex intra-domain network topology into a simple export-based sink-tree, which takes the domain border router as the root and other L3 switches/routers as nodes. To do that, we assume that: (1) multiple links (e.g., port trunk) bet- ween two nodes are treated as one; (2) we do not take link bandwidth or quality into consideration (we argue that this assumption is reasonable since most domain networks usually take hop-count as link quality. Otherwise, we can assign links with corresponding weights in the following topological matrix); (3) we only focus on the single-homing scenarios (Actually, for multi-homing cases, we can take the nearest concentration border router as the root node to apply our proposal). In such sink-tree, each leaf node can follow the shortest path to reach the root and intra-domain other nodes. Next we treat the initial topology as a directed acyclic graph (DAG) with the border router as root node. Then we can get a $N * N$ (N is the total number of all nodes) adjacent topological matrix according to the link connection relationship between nodes. The value of the matrix can be assigned as the following:

$$A[i][j] = \begin{cases} 1 & \textit{direct link between node i and j} \\ 0 & \textit{no direct link between node i and j} \end{cases}$$

Eventually, we can take this matrix as the parameter of the Dijkstra algorithm to shape this tree, and Fig.6 shows an example of this idea.

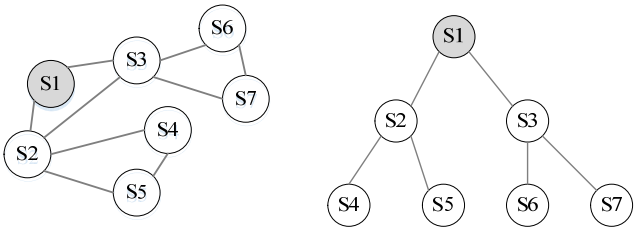


FIGURE 6. Export based sink tree conversion (assuming S1 as the border router).

C. LOCATING SDN DEPLOYMENT NODES

Technically, border routers and all of the L3 access switches deployment can address the IP source address spoofing issue. However, considering most networks are still traditional networks with legacy devices, the biggest concern of them is how to lower down the front-end investment and achieve this anti-spoofing purpose. Thus, within the legacy and SDN device hybrid network, minimizing SDN device deployment ratio but satisfying the desirable IP prefix-level anti-spoofing coverage ratio in the same time becomes our optimal goal. To realize this, we establish a network model to formulize this problem, and Table I explains its related notations.

TABLE 1. Key notations in SASSH formulation.

Notation	Meaning
AM(v,e)	Matrix, the adjacency matrix of topology with node set V and link set E.
ST(v,e')	Matrix, sink-tree converted by topology matrix, and the nodes are indexed from 1 in the root node.
N	Integer, total number of nodes, equal to $\|V\|$.
pc_i	Array, set of IP prefixes covered by node i (set of prefixes in the subtree with root node i, which includes all IP prefixes in this subtree and node i).
pc_{all}	Array, total set of IP prefixes within domain.
$\boldsymbol{\sigma_i}$	Binary, indicates whether node i is an SDN node or not.
child[i]	Integer Array, set of child nodes with root node i.
$\boldsymbol{\beta_i}$	Ratio, proportion of unspoofable IP prefix pair when node i is an SDN node.
$\propto$	Ratio, proportion of SDN nodes in all of nodes.
$\boldsymbol{\lambda}$	Ratio, requirement of unspoofable IP prefix rate in total.
$\mathbf{u_i}$	Integer, utility/prefix pair that can be checked by node i.
distinct()	Function, used to eliminate overlapped utilities when multiple nodes are selected for deployment.

SAVSH first introduces the notations pc_i which represents the prefixes collection issued by node i and its subtree nodes, while pc_{all} notates the collection of all prefixes within domain. Once one node is replaced by an SDN switch, its utility can be expressed by the number of prefix pairs that transit through the node, which indicates all possible paths from source prefix to destination. Thus this utility not only includes the valid prefix pairs within the subtree with root node i, but also contains the prefix pair combinations inside and outside this subtree. Nevertheless, the whole formulation should meet user's predefined requirement λ, and this constraint expresses the ratio of unspoofable prefix pair as a whole.

$$\min \alpha = \frac{\sum_{i=1}^{N} \sigma_i}{N} \tag{1}$$

$$\forall \mathrm{pc}_s, pc_t \in Child\,[i]\,,\ s \neq t : u_i = pc_s \cdot pc_t + pc_i \cdot \overline{pc_i} \tag{2}$$

$$\forall pc_s, pc_t \in V,\ s \neq t : \lambda = \frac{\sum_{i=1}^{N} distinct(\mu_i \cdot \sigma_i)}{pc_s \cdot pc_t} \tag{3}$$

$$\alpha \in [0, 1]\,,\ \lambda \in [0, 1] \tag{4}$$

However, such optimization goal with multiple constraints is a problem of integral linear programming, which is proved to be an NP-hard problem that cannot be solved in a mathematic way. Alternatively, we consider adopting a heuristic algorithm to locate SDN nodes, whose details are shown in Algorithm 1. With this algorithm, we first calculate the utility of prefix pair coverage and sort them in a decreased order for each node. Then we sum and eliminate the overlapped utilities from the first node to the last one until the utility requirement is satisfied.

Algorithm 1 SDN Deployment Nodes Selection Algorithm

Input: AM, N ∗ N topology adjacent matrix;
Output: α, proportion of SDN nodes in all nodes;

```
ST = Dijstra(AM)
for i = 1 to N do
    for j = 1 to N do
        u_all += ||pc_i|| · ||pc_j||
    end for
end for
for i = 1 to N do
    β_i = u_i / u_all
end for
sort(β)
for i = 1 to N & λ_temp < λ do
    λ_temp += Distinct(β_i)
end for
α = i/N
return α
```

D. DISTRIBUTING FILTERING RULE GENERATION

After we locate the SDN nodes and replace them with SDN switches, rules for each individual SDN switch should be generated from the controller and deployed onto them. Controller generates corresponding rules for each SDN node according to following three steps: (1) Relying on the generated sink-tree, SAVSH sorts out all legal prefixes in all of its downlink ports and aggregates prefixes in the same port as much as possible; (2) System organizes all possible prefix pairs between these prefixes in different downlink ports, and then forms corresponding forwarding rules; (3) Besides, system needs to produce forbidden rules to block illegal prefix pair to get through. Thus once spoofing packets reach these SDN

checkpoints, they will be matched with these defined rules and executed by related actions.

E. COPING WITH NETWORK DYNAMICS

How to deal with network dynamics is an important issue that matters solution's success, since topology changes would affect the shape of the sink-tree and the rule for SDN nodes. Unfortunately, sink-tree reshaping and rule recalculation will incur relative large latency than other procedures. To address this problem, we take the proactive and reactive combined way to cope with it. That is, for one link or one node failure situation, the system calculates new tree and store related rules into database in advance, so that system can directly distribute them if one of such cases happens. While for the rest of situations, system has to recalculate in time because multiple links and nodes failure combined situations are too complex to simulate. As the issue of rules redistribution would cause packets loss in the air, it is beyond the agenda of this paper and many studies (e.g., zUpdate) have focused on this issue.

VI. INTER-DOMAIN SOLUTION

A. SYSTEM OVERVIEW

As we depicted in the Fig.4, the inter-domain module mainly consists four components. From above to top they are: the trust alliance establishment & negotiation protocol (TAENP), east-west bridge, keyshare and packet sign and validation mechanism (PSVM). Given each pair of SDN controllers, TAENP responses to communicate with them to exchange system fundamental information, such as peer identity verification, domain IP address list, leader AS election in each pair AS and etc. Based on TAENP, east-west bridge can exchange domain abstract network view with peer ASes so as to meet high-level requirement, e.g., path-based packet verification. Then the keyshare component has two very important functions, time synchronization and encryption key exchange with fixed intervals between allied ASes. Lastly, the PSVM relies on shared keys to tag packets and forward to allied ASes, or verify legitimacy and remove tags for the packets from allied ASes as well.

B. TRUST ALLIANCE ESTABLISHMENT & NEGOTIATION PROTOCOL

TAENP is use to establish alliance relationship and negotiation some information between SDN controllers in different allied AS. In the first beginning, it will connect peer AS controller and identify peer's identity. When authenticated each other, two peers will form a pair and they will exchange some key information, for example, AS number, range list of domain IP address, for other component to perform their function. Besides that, they will elect a leader for initiatively launch connection in the subsequent interactions. The following simple algorithm decides how to select the leader in a pair.

$$Peer_{leader} = \begin{cases} \max(AS1, AS2) & where\ AS1 + AS2\ is\ odd \\ \min(AS1, AS2) & where\ AS1 + AS2\ is\ even \end{cases}$$

Where *AS1* and *AS2* are the AS numbers of two peers, and their sum decides leader peer selection. If the two allied peers are two networks instead of two domains, then we can assign their AS number with value 0.

C. NETWORK VIEW AND SECRET KEY SHARING

In the meantime, allied peers maybe need to exchange topology view for inter-domain innovations, e.g. cross-domain multicast application. However, since different domains have different policies and their admins usually not willing to expose full topology information but partial or abstract network topology views to their peers due to commercial benefits and security reasons. With the help of EW-Bridge [32], we can abstract physical topology as a virtual network view with only virtual links and nodes (e.g., a small network in domain can be abstract as a router node), so that we can achieve our purpose in a privacy and security manner. For the paper length reason, we will not elaborate EW-Bridge's detail in this paper.

Another important function in our system is the key sharing component for packets signing between allied AS. Thus symm- etric encryption key will be securely shared between each pair of peers with the help of Diffie-Hellman algorithm [33]. Besides that, network time protocol (NTP) will facilitate to synchronize two peers' time and keep secret key update with a fixed time interval, which can defer attacker to perform replay attack or brutal force attack to analyze secret key in a short time.

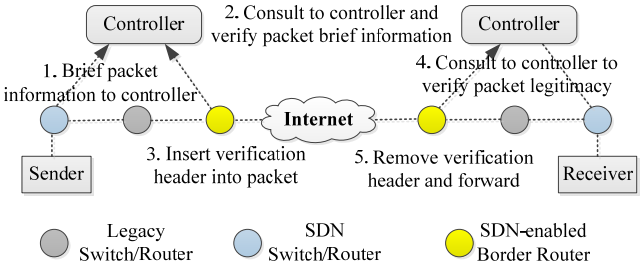


FIGURE 7. The workflow of packet signing and verification.

D. PACKET SIGNING AND VERIFICATION

As we stated, in order to verify packets authenticity between two allied ASes, packets travelling between two allied peers will be tagged signatures by source peer and verified by destination. Detailly, as illustrated in Fig.7, once a packet released to network, its first-hop SDN device will brief controller with packets' hash result. When the packet arrives to the border of network, the SDN-enabled domain border router will consult to its controller to verify packet's brief information. Once positive result returned, the border routers will insert an extra header we named as IGuarantee header into the packet. Also, when packet arrives to destination AS, peer SDN-enabled border router will take shared key and re-compute the signature so that it can compare the two signatures and verify the packet's authenticity. For inbound legitimate packets, the

border router will remove the IGuarantee header and forward to next-hop. Thus the whole processes are transparent to end users.

As packet's brief generation, as illustrated in the following algorithm, we take the first-hop SDN router's IP address, packet's IP header and body parts, the three components as parameters of hash algorithm (e.g., SHA-256) so as to avoid packet's key data to be modified in the route.:

$$Brief\,(P) = H(IP_{SDN-router}||P_{body}||P_{IP\_header})$$

E. IGuarantee HEADER

In order to compatible with IPv4 option field that cannot exceed 40 bytes limitation, we design IGuarantee header's fields as Fig.8 shown. This design is derived from following considerations.

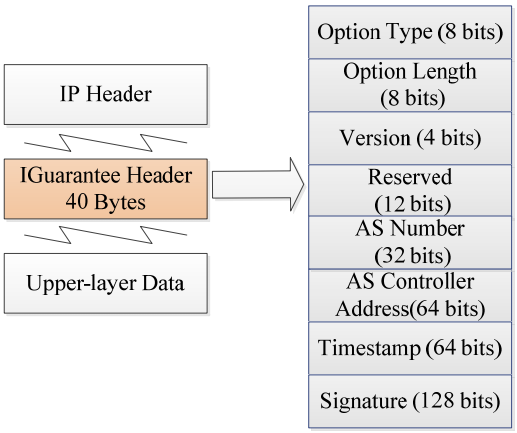


FIGURE 8. IGuarantee header format.

(1) **Option Type**: we assign the value "00011111" for this new type of option header. According to the IPv6 specification, the first two bits indicate "skip over this option and continue processing the header," while the third bit means "option data does not change en-route." The other five consecutive bits with customized value 1 is for device identification and processing convenience. Certainly, this value needs to be approved from the Internet Assigned Numbers Authority (IANA);

(2) **Option Length:** this field indicates the while option length. Currently, our header length is fixed size of 40 bytes, but 8 bits can maximally hold 64 bytes data in this header.

(3) **Version**: this field is for identify different option version when this header has multiple updates.

(4) **Reserved** filed is reserved for future consideration.

(5) **AS number:** 32 bits space is for compatible with new version AS number in IPv6 networks that is up to 32 bits.

(6) **AS controller Address** field is for hold domain AS controller's IP address, which can facilities peer AS to verify packets.

(7) **Timestamp** is aim to prevent reply attack, since receiving domain can drop inbound packets with outdated timestamp.

(8) **Signature** field is use to hold packet's signature so that end domain can re-calculate and compare it so as to decide packet's legitimacy. The signature is generated with a hash and encryption combined way:

$$Signature\,(P) = HMAC\,(K \oplus\ opad|(K \oplus ipad|M))$$

The K is the key shared by both ends in a pair, and HMAC is the encryption hash function (e.g., HMAC-MD5). Then the *opad* and *ipad* are the outside and inside padding for HMAC function. Last M is the message, which includes IGuarantee header, upper-layer data, and IP source and IP destination fields in IP header as well.

F. DISCUSSION

1) PACKET FRAGMENTATION ISSUE

Since our proposal needs to add extra header into packets head to allied ASes, it will enlarge packets' size slightly. However, Maximum Transmission Unit (MTU) does not allow oversized packets to be transmitted. In IPv4 networks, we can arrange a layer 3 device outside SDN-enabled border router so that it can perform packets' fragmentation function for oversized packets. While in IPv6 networks, we can decrease the MTU value in the MTU announcement if necessary.

2) SYSTEM SECURITY ISSUE

Considering system feasibility and performance, we take symmetric encryption algorithm and shared key to generate signature for packets between each pair of allied ASes. Thus, the key's security is the biggest concern in system security. First of all, we utilize Diffie-Hellman algorithm to distribute encryption key with a security manner. In the meantime, in order to avoid attacker perform sniff and replay attack, we setup the timestamp field and update key in every fixed interval that makes attacker cannot decryption the key in a short time.

3) COMPUTING OVERHEAD ISSUE

Indeed, computing signature and adding new header into a normal packet will incur extra overhead. However, since these operations are very common and they can be implemented by hardware, thus it can be achieve full line-rate speed.

VII. EVALUATION

In this section, we first establish a prototype to assess some quantitative indications that can prove our solution's feasibility. Further, we evaluate the relationship between our proposal's deployment ratio and unspoofable IP prefix proportion with some typical topologies, which can demonstrate our solution's advancement.

A. PROTOTYPE SETUP

1) SDN CONTROLLER

We build our controller application based on the open source controller Floodlight, its modules diagram is shown

in Fig.9 and it consists of two parts: intra-domain module and inter- domain module.

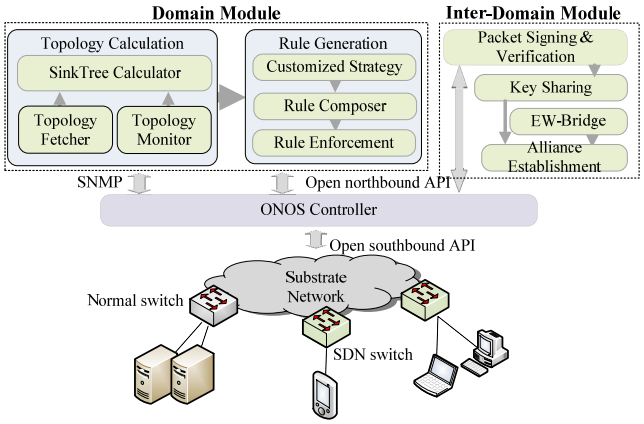


FIGURE 9. System prototype modules in SDN controller.

The inter-domain module comprised of four components and their function we have explained in section 6.1. Then the intra-domain module contains two components: topology calculation and rule generation. The former monitors topology changes and calculates the sink-tree promptly, while the latter combines network strategy and global topology knowledge to generate control rules. Once the system starts, the topology fetcher model retrieves routing information of the whole network from key routers via Simple Network Management Protocol (SNMP), and then it delivers this information to the sink-tree calculator module to shape the routing forwarding tree appropriately. After that, the topology monitor module detects topology changes so that it can translate topology to export-based tree according to network dynamics.

2) SDN-ENABLED BORDER ROUTER

We developed a SDN-enabled router prototype with Net Magic card [34] to fulfill packets signing and verification jobs, which is very similar with NetFPGA card-based application development

B. INTRA-DOMAIN SCHEME PERFORMANCE

We take Fig.6(a) illustrated topology to evaluate our domain scheme's performance, and we assume only one subnet prefix in the leaf nodes S4 to S7.

1) PROTOTYPE EXPERIMENT

SDN Node Deployment Rate: the ratio of SDN node number in total nodes number. Although large SDN switches deployment rate can increase unspoofable IP prefix coverage, investment is increased as well. Thus, our trade-off is to maximize prefix coverage under given deployment rate. In our case, we only need 28.6% deployment rate to replace S2 and S3 with SDN switches while trading 85.7% unspoofable IP prefix coverage.

Number of SDN Rule: the number of filtering rule in SDN nodes which depends on the shape of the sink-tree, as well as the location of the SDN node and the number of IP prefix it covered. To a modern SDN switch with the space of at least thousands of flow entries, this cost is ignorable. Besides, we can utilize JumpFlow's [35] method to reduce the number of rules under the circumstance of large flow table.

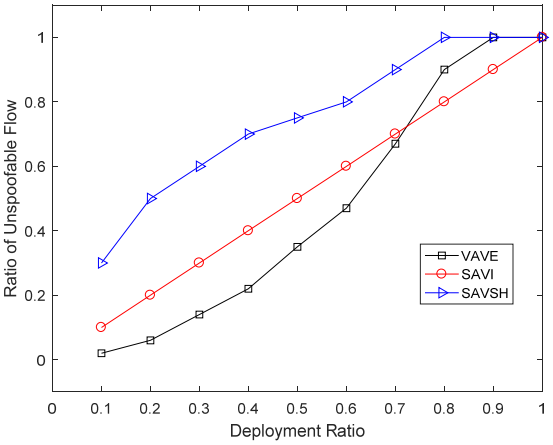


FIGURE 10. The ratio of unspoofable flows with different deployment rates.

Filtering Latency: the period of time from illegal host sending out a forged packet to system filtering it. The value of the latency depends on the distance from the vicious host to its nearest SDN checkpoint, the link bandwidth and traffic situation. In our experiment, we have the IXIA traffic generator attached in node S4 and injected 100 packets to S1. The average packet delay tested in the controller forwarded by node S2 is 0.024s.

Rule Re-Computation Latency: the delay from topology change to control rule recalculation and redistribution to SDN nodes. First, we disconnect the link between S5 to S2. Since such case is pre-stored in system, the average latency of rule redeployment in node S2 is 3.25s. Further, we randomly disconnect two links in different nodes but keep the whole topology without any isolated node. This average latency reaches to 20.46s, which is much longer than the previous situation mainly caused by rule recalculation we believe.

Filtering Effect Comparison: We also compare the spoofing packets filtering effect with SAVI and VAVE proposals under different SDN deployment rates. From the Fig 10, we can see that our solution can get better effect with the same SDN node deployment ratios than other two solutions.

2) TYPICAL TOPOLOGY SIMULATION

To evaluate the required number of SDN switches in different topology models, we also conduct a deployment simulation with four typical topologies in Rocketfuel project [36], which are all ISP topologies in the global caught by traceroutes. The basic profiles of these topology models are shown in Table II. Each topology owns different nodes and links which can be represented by undirected graph. And we assume that each leaf node attached five prefixes in these topologies.

TABLE 2. Topology details.

Topology Name	Nodes	Links
Exodus	79	294
Telstra	104	306
Abovenet	138	745
Sprintlink	315	1944

Next we apply our node selection algorithm into these topologies. The relationship between deployment ratio and IP prefix coverage is demonstrated in Fig.11.

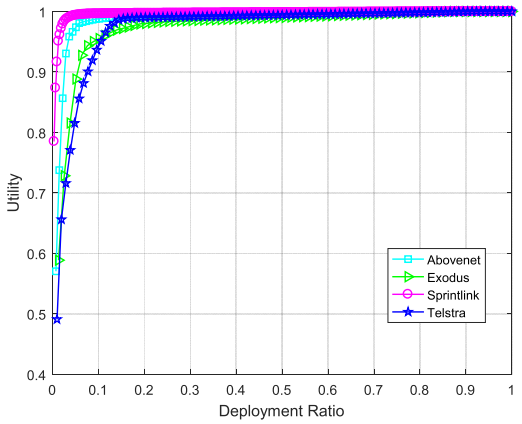


FIGURE 11. The utility comparison for intra-domain scheme with different ratios of SDN deployment.

We can observe that the percentage of required SDN switches in Sprintlink is smaller than the other three networks since Sprintlink network presents a larger link aggregating as a whole. But even for the worst case in the Telstra network, we still have the satisfactory result that 10% SDN node deployment ratio can exchange nearly 95% utility in IP prefix-level anti-spoofing effect.

C. INTER-DOMAIN SCHEME PERFORMANCE

Also, based on the illustrated topology in Fig.3, We simulate three ASes and evaluate our inter-domain scheme performance from two aspects: filtering accuracy and end-to-end delay.

1) FILTERING ACCURACY

We take IXIA traffic generator produce different amounts of packets and a fixed ratio of spoofing packets as well. Then we compare our proposal with the classic inter-domain anti-spoofing proposal Passport, and the baseline that has not any anti-spoofing measurements. From the Fig.12 we can see that our scheme is outperform than Passport before the packets number gets too large. However, as packet number increasing, the accuracy of our proposal and passport are both decrease sharply. We guess our PC-based border router has limited computing resource and lacks of resource optimization design are the main reasons.

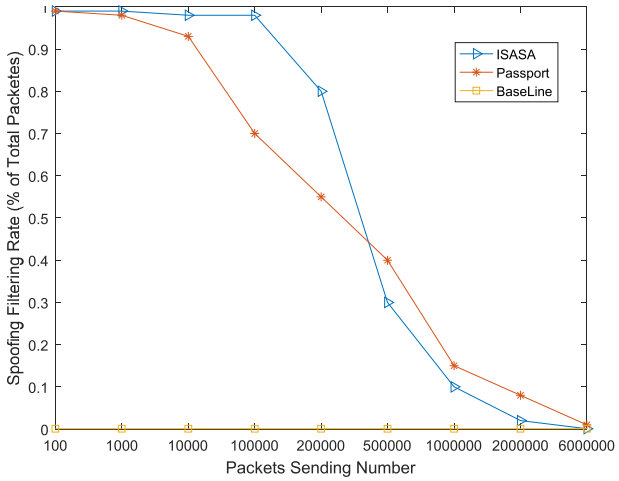


FIGURE 12. The spoofing packet filtering rate comparison with different schemes.

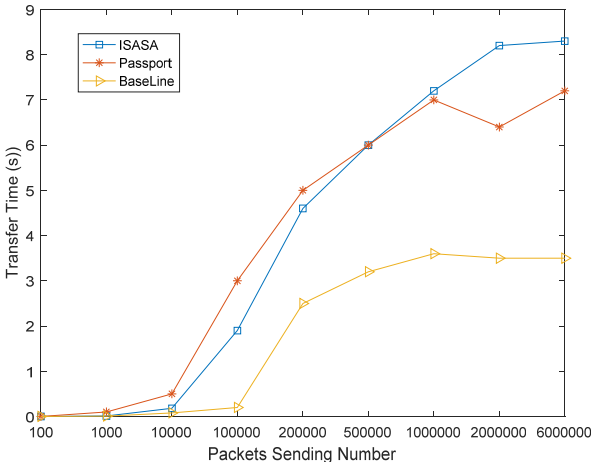


FIGURE 13. The end-to-end delay comparison with different schemes.

2) END-TO-END DELAY

We also evaluate the end-to-end delay from a normal packet being sent out to it arrives destination host. In Fig.13, we can observe that the transfer time increases with the number of packet increases, but our proposal is still faster than the Passport and baseline schemes.

D. INCREMENTAL DEPLOYMENT BENEFIT

We collect the Internet AS links data form CAIDA. [37] and generate the AS-level topology. The topology contains 25 ASes, and we assume each AS has only one host with an IP address. The deployment ratio will increases slowly and the AS who will deploy is chosen randomly. Then we evaluate the deployment benefits of Ingress Filtering (IEF), SPM and our proposal ISASA with an IP spoofing attack simulator.

As we can see in Fig.14, SPM shows advantage in the smaller deployment, but the more AS deployed only result in less effective at the later stage. While our ISASA can gain more benefit with the increase of deployment, since only

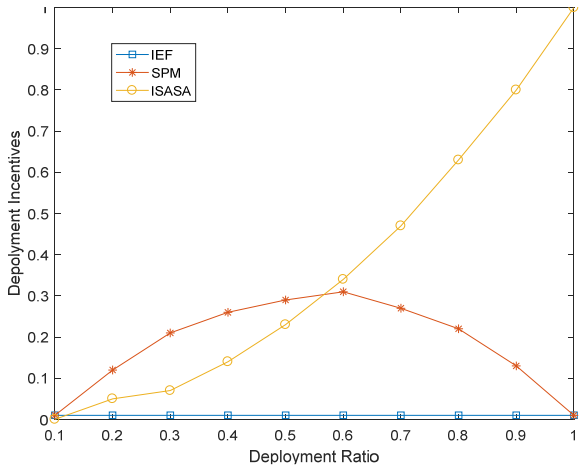


FIGURE 14. The deployment Incentives comparison with different schemes.

alliances having implemented our protocol can work out, and it will encourage the ISP providers to adopt the new idea to reality.

VIII. CONCLUSION

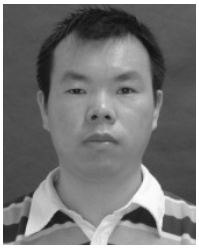
In this paper, we present an integrated IP spoofing validating solution named ISASA for both intra-domain and inter-domain scenarios. The intra-domain part scheme first computes key network nodes and takes SDN switches to replace traditional devices in these nodes, so that it can gain a balance between fake packets filtering rate and deployment cost. Further, taking advantage of SDN pattern, filtering rules can be generated and distributed by central controller based on network real-time topology. In the meanwhile, the inter-domain part scheme proposes a time-synchronized packet signature signing and verification protocol between AS alliances. Through the established allied relationship, two ASes can exchange secret key, network abstract view and other information. Eventually, packets shuttle between the two ASes will be tagged signature header and removed after they have been verified in the destination AS. Lastly, we have implemented the system prototype, and our conducted experiments prove ISASA poses desirable performance. In the future, based on some new research [38], [39], we plan to enhance the system architecture design and joint with network equipment manufacturer, so that we can release related products onto market and apply them into real network scenarios.

REFERENCES

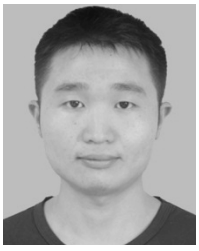
[1] W. M. Eddy, "Defenses against TCP SYN flooding attacks," *Internet Protocol J.*, vol. 9, no. 4, pp. 2–16, 2006.
[2] D. Senie and P. Ferguson, *Network Ingress Filtering: Defeating Denial of Service Attacks Which Employ IP Source Address Spoofing*, document RFC 2267, 1998.
[3] The Indian Computer Emergency Response Team. *CERT Advisory Smurf IP Denial-of-Service Attacks*. Accessed: Dec. 6, 2017. [Online]. Available: http://www/cert.org/advisories/CA-1998-01.html
[4] CAIDA, *State of IP Spoofing*. Accessed: Dec. 6, 2017. [Online]. Available: https://spoofer.caida.org/summary.php
[5] Hackmageddon. *Cyber Attacks Timeline Master Indexes*. Accessed: Dec. 6, 2017. [Online]. Available: http://www.hackmageddon.com/cyber-attacks-timeline-master-indexes/
[6] CERT. *China Internet Network Security Report in 2016*. Accessed: Dec. 6, 2017. [Online]. Available: http://www.cert.org.cn/publish/main/upload/File/2016_cncert_report.pdf
[7] *Wikipedia. DR-DOS*. Accessed: Dec. 6, 2017. [Online]. Available: https://en.wikipedia.org/wiki/DR-DOS
[8] Cisco. *Unicast Reverse Path Forwarding*. Accessed: Dec. 6, 2017. [Online]. Available: http://www.cisco.com
[9] J. Wu, J. Wu, M. Bagnulo, C. Vogt, and F. Baker, *Source Address Validation Improvement (SAVI) Framework*, document RFC 7039, 2013.
[10] G. Hu, K. Xu, J. Wu, Y. Cui, and F. Shi, "A general framework of source address validation and traceback for IPv4/IPv6 transition scenarios," *IEEE Netw.*, vol. 27, no. 6, pp. 66–73, Nov./Dec. 2013.
[11] W. Chen and D.-Y. Yeung, "Defending against TCP SYN flooding attacks under different types of IP spoofing," in *Proc. IEEE ICN/ICONS/MCL Int. Conf. Netw., Int. Conf. Syst., Int. Conf. Mobile Commun. Learn. Technol.*, Apr. 2006, p. 38.
[12] C. Jin, H. Wang, and K. G. Shin, "Hop-count filtering: An effective defense against spoofed DDoS traffic," in *Proc. 10th ACM Conf. Comput. Commun. Secur.*, 2003, pp. 1–15.
[13] T. Peng, C. Leckie, and K. Ramamohanarao, "Protection from distributed denial of service attacks using history-based IP filtering," in *Proc. IEEE Int. Conf. Commun. (ICC)*, vol. 1. May 2003, pp. 482–486.
[14] T. Aura, *Cryptographically Generated Addresses (CGA)*, document RFC 3972, 2005.
[15] D. G. Andersen, H. Balakrishnan, N. Feamster, T. Koponen, D. Moon, and S. Shenker, "Accountable Internet protocol (AIP)," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 38, no. 4, pp. 339–350, 2008.
[16] C. Schridde, M. Smith, and B. Freisleben, "TrueIP: Prevention of IP spoofing attacks using identity-based cryptography," in *Proc. ACM 2nd Int. Conf. Secur. Inf. Netw.*, 2009, pp. 128–137.
[17] A. Bremler-Barr and H. Levy, "Spoofing prevention method," in *Proc. INFOCOM, 24th Annu. Joint Conf. IEEE Comput. Commun. Soc.*, vol. 1. Mar. 2005, pp. 536–547.
[18] H. Lee, M. Kwon, G. Hasker, and A. Perrig, "BASE: An incrementally deployable mechanism for viable IP spoofing prevention," in *Proc. 2nd ACM Symp. Inf., Comput. Commun. Secur.*, 2007, pp. 20–31.
[19] M. Casado *et al.*, "SANE: A protection architecture for enterprise networks," in *Proc. USENIX Secur. Symp.*, vol. 49. 2006, p. 50.
[20] P. Nikander and R. Moskowitz, *Host Identity Protocol (HIP) Architecture*, document RFC 4423, 2006.
[21] G. Yao, J. Bi, and P. Xiao, "Source address validation solution with OpenFlow/NOX architecture," in *Proc. 19th IEEE Int. Conf. Netw. Protocols (ICNP)*, Oct. 2011, pp. 7–12.
[22] P. Xiao, J. Bi, and T. Feng, "O-CPF: An OpenFlow based intra-AS source address validation application," in *Proc. CFI*, Beijing, China, 2013, pp. 1–2.
[23] G. Hu, Y. Jiang, W. Chen, T. Chen, and J. Wu, "SuperFlow: A reliable and scalable architecture for large-scale enterprise networks," *Chin. J. Electron.*, vol. 25, no. 6, pp. 1134–1140, 2016.
[24] G. Chen, G. Hu, Y. Jiang, and C. Zhang, "SAVSH: IP source address validation for SDN hybrid networks," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Jun. 2016, pp. 409–414.
[25] J. Li, J. Bi, and J. Wu, "Towards a cooperative mechanism based distributed source address filtering," in *Proc. IEEE 22nd Int. Conf. Comput. Commun. Netw. (ICCCN)*, Jul./Aug. 2013, pp. 1–7.
[26] K. Park and H. Lee, "On the effectiveness of route-based packet filtering for distributed DoS attack prevention in power-law internets," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 31, no. 4, pp. 15–26, 2001.
[27] Z. Duan, X. Yuan, and J. Chandrashekar, "Constructing inter-domain packet filters to control IP spoofing based on BGP updates," in *Proc. IEEE INFOCOM*, Apr. 2006, pp. 1–12.
[28] J. Li, J. Mirkovic, M. Wang, P. Reiher, and L. Zhang, "SAVE: Source address validity enforcement protocol," in *Proc. 21st Annu. Joint Conf., IEEE Comput. Commun. Soc. INFOCOM*, vol. 3. Jun. 2002, pp. 1557–1566.
[29] X. Liu, A. Li, X. Yang, and D. Wetherall, "Passport: Secure and adoptable source authentication," in *Proc. NSDI*, vol. 8. 2008, pp. 365–378.
[30] B. Liu, J. Bi, and Y. Zhu, "A deployable approach for inter-AS anti-spoofing," in *Proc. 19th IEEE Int. Conf. Netw. Protocols (ICNP)*, Oct. 2011, pp. 19–24.

[31] J. Bi, B. Liu, J. Wu, and Y. Shen, "Preventing IP source address spoofing: A two-level, state machine-based method," *Tsinghua Sci. Technol.*, vol. 14, no. 4, pp. 413–422, Aug. 2009.
[32] P. Lin, J. Bi, and Y. Wang, "East-west bridge for sdn network peering," in *Frontiers in Internet Technologies*. Berlin, Germany: Springer, 2013, pp. 170–181.
[33] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. 22, no. 6, pp. 644–654, Nov. 1976.
[34] Netmagic. *Netmagic Card*. Accessed: Dec. 6, 2017. [Online]. Available: http://www.netmagic.org/
[35] Z. Guo, *et al.*, "JumpFlow: Reducing flow table usage in software-defined networks," *Comput. Netw.*, vol. 92, pp. 300–315, Dec. 2015.
[36] N. Spring, R. Mahajan, and D. Wetherall, "Measuring ISP topologies with Rocketfuel," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 32, no. 4, pp. 133–145, 2002.
[37] CAIDA. *The IPv4 Routed/24 AS Links Dataset*. Accessed: Dec. 6, 2017. [Online]. Available: http://www.caida.org/data/active/ipv4_routed_topology_aslinks_dataset.xml
[38] X. Li, J. Niu, M. Z. A. Bhuiyan, F. Wu, M. Karuppiah, and S. Kumari, "A robust ECC based provable secure authentication protocol with privacy protection for industrial Internet of Things," *IEEE Trans. Ind. Informat.*, to be published.
[39] X. Li, J. Niu, S. Kumari, F. Wu, A. K. Sangaiah, and K.-K. R. Choo, "A three-factor anonymous authentication scheme for wireless sensor networks in Internet of Things environments," *J. Netw. Comput. Appl.*, vol. 103, pp. 194–204, Feb. 2018.

CHAOQIN ZHANG is currently pursuing the Ph.D. degree with the State Key Laboratory of Mathematical Engineering and Advanced Computing, China. He is also an Associate Professor with the Zhengzhou University of Light Industry. His research interests include Internet architecture, data mining, and network security.



GUANGWU HU received the Ph.D. degree in computer science and technology from Tsinghua University in 2014. He held a post-doctoral position at the Graduate School at Shenzhen, Tsinghua University. He is currently an Assistant Professor with the Shenzhen Institute of Information Technology. His research interests include software-defined networking, next-generation Internet, and Internet security.



GUOLONG CHEN received the master's degree in computer science and technology from Tsinghua University in 2017. He is currently with Huawei Technologies Co., Ltd., where he is involved in Linux Kernel Virtualization and RTOS.

ARUN KUMAR SANGAIAH received the Ph.D. degree in computer science and engineering from VIT University, Vellore, India. He is currently an Associate Professor with the School of Computer Science and Engineering, VIT University. His area of interest includes software engineering, computational intelligence, wireless networks, bioinformatics, and embedded systems.

PING'AN ZHANG received the M.S. and Ph.D. degrees in computer science from Xi'an Jiaotong University, China, in 1991 and 1996, respectively. He is currently a Full Professor with the Shenzhen Institute of Information Technology. He is the Dean of the Computer School of Shenzhen Institute of Information Technology. His research interests include computer network, intelligent control, and computer applications.

XIA YAN received the M.S. degree in computer science from the Harbin Institute of Technology, China, in 2006. She is currently an Associate Professor with the Shenzhen Institute of Information Technology. His research interests include Internet architecture and cyber-security.

WEIJIN JIANG received the Ph.D. degree in computer science from the National University of Defense Technology, China, in 2009. He is currently a Full Professor with the Hunan University of Commerce, China. His research interests include complex system modeling and system simulation.