Coordination of Anti-Spoofing Mechanisms in Partial Deployments

Hyok An, Heejo Lee, and Adrian Perrig

Abstract: **Internet protocol (IP) spoofing is a serious problem on the Internet. It is an attractive technique for adversaries who wish to amplify their network attacks and retain anonymity. Many approaches have been proposed to prevent IP spoofing attacks; however, they do not address a significant deployment issue, i.e., filtering inefficiency caused by a lack of deployment incentives for adopters. To defeat attacks effectively, one mechanism must be widely deployed on the network; however, the majority of the anti-spoofing mechanisms are unsuitable to solve the deployment issue by themselves. Each mechanism can work separately; however, their defensive power is considerably weak when insufficiently deployed. If we coordinate partially deployed mechanisms such that they work together, they demonstrate considerably superior performance by creating a synergy effect that overcomes their limited deployment. Therefore, we propose a universal anti-spoofing (UAS) mechanism that incorporates existing mechanisms to thwart IP spoofing attacks. In the proposed mechanism, intermediate routers utilize any existing anti-spoofing mechanism that can ascertain if a packet is spoofed and records this decision in the packet header. The edge routers of a victim network can estimate the forgery of a packet based on this information sent by the upstream routers. The results of experiments conducted with real Internet topologies indicate that UAS reduces false alarms up to 84.5% compared to the case where each mechanism operates individually.**

Index Terms: **DDoS attacks, Internet protocol (IP) spoofing prevention, network security, packet filtering, packet marking.**

I. INTRODUCTION

A. Background

INTERNET protocol (IP) spoofing continues to be used effectively in network-based attacks. Attackers exploit IP spoofing to forge untraceable IP addresses. Because anonymity is guaranteed [1], attackers can bypass source-based filtering and defeat resource-allocation mechanisms [2]. A massive distributed reflective denial-of-service (DRDoS) using the reflection of the network time protocol (NTP) with 400 Gbps was reported by the BBC [3]. We must focus on the fact that the attacks are launched using IP spoofing. Recently, distributed denial-of-service (DDoS) attacks have been increasingly launched. Because of large-scale botnets, it may appear that IP spoofing is no longer required. However, IP spoofing is an attractive technique for botnet owners to obfuscate the identity of bots and the necessary conditions to amplify the attack traffic against a victim network [4], [5]. IP spoofing is frequently observed on the captured backscatter messages from UCSD Network Telescopes [6], [7]. New types of attacks including amplification attacks, in-window-TCP-reset, and spam filter circumvention attacks can also be launched using IP spoofing [8].

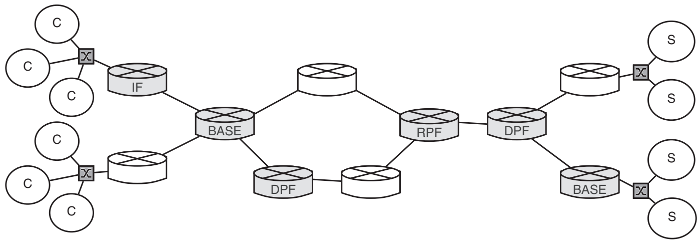


Fig. 1. Deployment of four different anti-spoofing mechanisms on a 10-node network between clients (C) and servers (S). Ingress filtering (IF), BASE, DPF, and RPF are deployed at six nodes individually; however, the resulting performance is not the sum of their individual performances. Alternatively, their cooperation could increase their accuracy.

Although many approaches against IP spoofing attacks have been proposed, how to prevent these attacks remains an unsolved problem. First, the majority of anti-spoofing mechanisms are ineffective filters because they have not been widely deployed on the Internet, given the lack of deployment incentives for adopters [9]. For example, reverse path forwarding (RPF) [10] and distributed packet filtering (DPF) [11] do not provide any incentives for early adopters. In Arbor Networks' recent annual report [12], the proportion of the report respondents implementing ingress filtering dropped from 50% in 2013 to 33% in 2014. Secondly, existing anti-spoofing mechanisms have limitations (e.g., false positives). RPF functions properly for only a specific network environment (i.e., symmetric routing paths). Finally, an autonomous system (AS) can select its own defense mechanism and policy independently from other ASes and each anti-spoofing mechanism functions individually of other mechanisms. Such practical issues cause filtering to remain inefficient and limit the effectiveness of defenses against IP spoofing attacks.

None of the previously proposed mechanisms has been widely deployed. Fig. 1 illustrates one example of the coexistence of multiple anti-spoofing mechanisms. Each of these techniques works individually and their effects are doubtful given the large attacks currently occurring. We believe that if existing

Manuscript received February 23, 2016; approved for publication by B. Byunghoon Kang, Division III Editor, August 1, 2016.

This work was supported by Institute for Information & Communications Technology Promotion (IITP) grant funded by the Korea government (MSIP) (No.R0190-16-2011, Development of Vulnerability Discovery Technologies for IoT Software Security). A preliminary version of this paper was presented at the 38th IEEE Local Computer Networks (LCN 2013) [46].

H. An and H. Lee are with the Department of Computer Science and Engineering, Korea University, Republic of Korea, email: {anhyok, heejo}@korea.ac.kr.

A. Perrig is with the Department of Computer Science, ETH Zurich, Zurich, Switzerland, email: adrian.perrig@inf.ethz.ch.

H. Lee is a corresponding author.

Digital object identifier: 10.1109/JCN.2016.000129

anti-spoofing mechanisms that operate individually can be integrated into a new mechanism with a higher deployment ratio, the anti-spoofing efficacy will increase substantially.

B. Overview

We propose a universal anti-spoofing (UAS) mechanism that incorporates existing mechanisms to thwart IP spoofing attacks. UAS utilizes packet marking [13] to deliver the opinions of the upstream routers that forward packets. Individual routers that use a single anti-spoofing mechanism inscribe a mark in the IP packet header indicating whether they consider the packet to be spoofed or not. Edge routers on a victim network receive the packet with marks from multiple routers and compare it with a predefined threshold value for filtering.

UAS incorporates various anti-spoofing mechanisms while considering all necessary properties. This approach can support not only existing but also future mechanisms that adhere to the proposed minimum requirements. The conventional method is to drop packets that are identified as spoofed by a single prevention mechanism. Conversely, we propose that individual mechanisms should not be allowed to drop packets; instead, spoof identifications from individual mechanisms should be treated as opinions. These opinions can be collated into a comprehensive assessment to determine packets that should be dropped.

Thus, our first requirement is that the deployed prevention mechanisms record their determination as to whether a packet has been spoofed or not in the received packets; it is much easier than designing a new control protocol and there is no additional traffic. Our second requirement is that the packets transport the opinions of all the deployed mechanisms on the path to the victim network. Finally, the opinions in the received packets are used to determine if a packet should be dropped according to a predefined threshold value. It may seem advisable to drop all doubtful packets; however, this is not always true. If individual mechanisms are not deployed widely, they can make false decisions. A lack of deployment is difficult to solve. Therefore, integrating mechanisms is a superior option compared to solving the difficulty of deployment.

C. Main Contributions

UAS provides a platform to cooperate other mechanisms and reduces false alarms more than in the case of the individual operation of other mechanisms in a network.

In experiments using four existing mechanisms, with only 25% deployment over the entire network, we found that false alarms were reduced by 72.9% compared to the cases where each mechanism operated individually. In one of these experiments, false alarms were reduced up to 84.5%. The contributions of our work are twofold:

1. UAS provides a platform that can incorporate existing anti-spoofing mechanisms. Any anti-spoofing mechanism alone is difficult to deploy widely on the network; however, the alliance of low-deployed mechanisms can occupy a wide area.
2. UAS reduces false alarms more effectively than the individual operation of anti-spoofing mechanisms given the same deployment ratio. UAS provides a method for cooperation of mechanisms for higher accuracy and improved defensive power.

The remainder of this paper is organized as follows. In Section II, we discuss related work on anti-spoofing mechanisms. In Section III, we define IP spoofing problems and discuss the limitations of the current anti-spoofing mechanisms. In Section IV, we outline the UAS operations, including marking and filtering. We present a basis upon which to evaluate the performance of UAS in Section V and discuss the results in Section VI. We conclude this paper in Section VII.

II. RELATED WORK

There are several studies involving IP spoofing prevention mechanisms. S. T. Zargar *et al.* in [14] present the classifications of the prevention mechanisms. The studies were categorized according to the deployment location as source-based, destination-based, and network-based.

A. Source-Based Mechanisms

Ingress/egress filtering [15] operates on the border routers of networks. It is called either ingress or egress depending on where it is applied. It verifies that the outbound packets received use one of the available IP addresses in its network. The scheme has two problems [16]. The first is that if not all ISP providers deploy this mechanism, IP spoofing can occur from the networks where it has not been deployed. The other is that this mechanism requires overhead in terms of additional router configuration and processing.

RPF [10] is similar to ingress filtering. RPF operates on the basis that the source address of incoming packets should be available as the origin address in the IP routing table. To do this, it assumes that a network is a symmetric routing environment. However, numerous networks now use asymmetric routing on the Internet [16]. Furthermore, the IP routing table must be up to date, incurring additional overhead for the routers. Because of these requirements, RPF cannot be deployed in many places.

B. Network-Based Mechanisms

DPF [11] has a proactive and reactive approach to DDoS attack prevention based on route-based distributed packet filtering. It uses routing information for spoofed packet filtering, as the interface of a router is used for specific source IP addresses. Thus, it assumes that routers know the routing information.

Border gateway protocol (BGP) anti-spoofing extension (BASE) [2] uses an incrementally deployable mechanism that relies on BGP. Each router that uses BASE records the incoming interface in the incoming packets. BASE focuses on a viable solution; thus, it is designed to satisfy the incremental deployment properties necessary for adoption along with distributed filtering, cryptographic packet marking, and on-demand filtering for the destination addresses of the victim network.

Virtual anti-spoofing edge (VASE) [17] is an intra-domain spoofing filtering mechanism based on calculating the forwarding path of flows. It makes use of a forwarding table and interface table to calculate the path of a part of flows and generates filtering rules to protect such flows. VASE uses sampling and on-demand filter configuration to detect IP spoofing attacks and reduce unnecessary overhead due to the existence of intermittent attacks.

Mutual egress filtering (MEF) [18] is an egress filtering-based anti-spoofing mechanism. Instead of filtering all the spoofed traffic identified by egress filtering, a MEF deployer only filters for its peers. Using selective filtering, MEF enlarges the difference between the protection gained by deployers and non-deployers and thus provides ASes with high deployment incentives. MEF can also work in on-demand filtering mode. In this mode, MEF precisely protects the subnetworks or prefixes under attack, instead of filtering for all peer prefixes all the time.

C. Destination-Based Mechanisms

Hop-count filtering [19] records a source IP address and its corresponding hops from a destination at the victim network when it is not under attack. It cannot ensure the integrity and accuracy of the source IP addresses and their corresponding hops from the victim [14]. Furthermore, legitimate packets can be discarded as spoofed if their IP to hop-count mappings are inaccurate or if the hop-count update has a delay [20].

Pi [13] is a per-packet deterministic mechanism. This means that each packet travels along the same path carrying the same identifier. A path fingerprint is embedded in each packet that enables a victim to identify packets traveling the same paths, whether the source IP address of the packets is spoofed or not. Pi demonstrates effective performance if it is deployed over about approximately half of the routers in the Internet.

Marking on demand (MOD) [21] is based on the deterministic packet marking (DPM) mechanism to dynamical distribute marking IDs in both temporal and space dimensions. It can trace back to all possible sources of DDoS attacks, which is not possible for the existing DPM schemes. Because of the enormous amount of attack information in the MOD database, it is a challenge to the performance of information retrieval from victims or other potential clients.

D. Advantages of IP Spoofing for Attackers

Some researchers believe that IP spoofing is no longer being used for attacks owing to the prevalence of ingress/egress filtering and the widespread use of botnets. However, an analysis of backscatter traffic [6], [22] reports several hundred DDoS attacks with IP spoofing per day. Further, a massive DRDoS attack using IP spoofing was launched against Spamhaus, a spam-fighting group based in Europe, on Mar. 19, 2013 [23], [24]. This DRDoS attack was based on DNS amplification and peaked at 300 Gbps, six times greater than similar attacks of approximately 50 Gbps against normal sites such as major banks [25]. In addition to DNS amplification, NTP queries have been used for recent DRDoS attacks [26], [27]. These attacks are strong evidence that IP spoofing remains an effective method to launch attacks.

According to the Spoofer Project [28], IP spoofing continues to be used with a significant number of Internet addresses. The Spoofer Project monitors the state of source IP address spoofing on the Internet using volunteers. According to the project report, the IP addresses that can be used by the volunteers as forged source addresses when sending packets to the project server can all be spoofed by attackers. As of Feb. 2, 2016, their results indicate that 13.5% of the IP addresses — approximately 309,150,000 out of 2,290,000,000 — enable spoofing. This does not mean that attackers can spoof only 13.5% of IP addresses; some attackers are able to spoof all IP addresses [29]. Furthermore, Arbor Networks [12] reported that the proportion of the report respondents implementing ingress filtering has dropped from 50% in 2013 to 33% in 2014. IP spoofing attacks are evolving into new forms of attack such as DRDoS attacks.

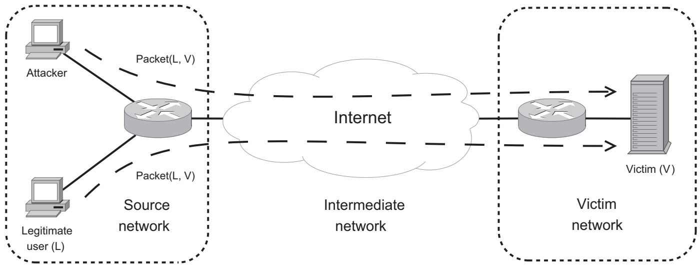


Fig. 2. Network overview: Packets are sent from the source network to the victim (V) network through the intermediate network. The attacker can send packets with the source address of the legitimate user (L).

IP spoofing is also proving useful to botnet owners who want to hide their business base and conceal the identity of their zombie machines for as long as possible [29]. If there are many botnets, their owners perform better, allowing for more powerful attacks that can be more profitable. Thus, they use IP spoofing tactically to conceal their botnets.

From the above arguments, it is clear that IP spoofing continues to be a major unresolved threat.

III. PROBLEM STATEMENT

In this section, we discuss the deployment problem of existing anti-spoofing mechanisms and suggest the requirements for a universal anti-spoofing mechanism that incorporates existing mechanisms.

We can model the Internet as three groups of networks: Source, intermediate, and victim networks as indicated in Fig. 2. The source network has a legitimate user and/or an attacker, both sending packets to the victim network through the intermediate network. The legitimate user sends the target server a packet that has his/her own source IP address. The attacker also sends a packet through the intermediate network to the victim. These packets have a spoofed source IP address of a legitimate user and the destination IP address of the victim. Source IP spoofing is possible because Internet global routing is based on looking up only the destination address, without verification of the source address [30]. Although the attacker sends spoofed packets with the source address of a legitimate user, the victim cannot recognize if the packets are spoofed. The victim cannot trace back to a source located out of its own ISP network [31].

To hinder IP spoofing attacks, many anti-spoofing mechanisms have been proposed. However, every mechanism has limitations that hinder its widespread deployment on the Internet. Furthermore, ASes can adopt their own mechanism and each anti-spoofing mechanism functions individually from other ASes.

- **Anonymity**: The victim cannot recognize the source even though the attacker sends spoofed packets with the source address of a legitimate user.
- **Deployability**: The lack of solutions to solve the limitations that hinder a mechanism's widespread deployment makes network administrators reluctant to deploy them.

As we explained above, the anonymity of packets and the deployability of anti-spoofing mechanisms are the main problems that we must consider to develop solutions. We consider an alternative approach that works within the current limitations. We suggest a universal anti-spoofing mechanism that incorporates existing mechanisms. There are three essential properties, i.e., coordination (C), synergy (S), and incrementality (I). CSI is required for a viable incorporative mechanism design:

1. **Coordination**: The proposed mechanism should ensure the proper operation of each mechanism and address the peculiarities that arise because of the interactions among the individual mechanisms.
2. **Synergy**: The performance of a universal anti-spoofing mechanism depends on the performance of the individual mechanisms; however, the filtering strength of the integrated mechanisms should be enhanced.
3. **Incrementality**: The proposed mechanism should operate in a fashion of incremental deployment and the performance should improve as the deployment ratio increases.

To achieve these aims, the proposed universal mechanism considers the decision of each mechanism as an opinion and the accumulated opinions are used for making a final decision. Our goal is to combine individually operating anti-spoofing mechanisms into one and improve the universal performance result.

Because there is also no single mechanism that is broadly deployed and no single mechanism to defeat the threats, a new approach must be implemented to coordinate the existing mechanisms and achieve highly accurate of anti-spoofing decisions. This new approach should provide adoption incentives to existing mechanisms. It is not acceptable for a new approach to require significant changes to existing networks [32], [33]. Rather, it is necessary to design an approach that functions with only minor modifications to the existing networks. Thus, integrating mechanisms is a superior option compared to waiting for a new approach that could resolve the difficulty of deployment.

IV. MECHANISM DESCRIPTION

In this section, we propose the UAS mechanism and explain its marking and filtering operations. A marking field is utilized for integrating multiple mechanisms and we discuss how its use solves various limitations. In the subsection on marking and filtering operations, we describe a method to integrate multiple mechanisms and enhance filtering strength.

A. Mechanism Concepts

There are several methods for transporting the opinions of each anti-spoofing mechanism. Control protocol design, additional data packets, data attached to the packets, or marks in the packet header are some examples. Instead of devising a new control protocol or sending additional packets, we record the opinion of each mechanism into a field of the IP packet header. This has three advantages over the other methods:

1. We are not required to design an alternative control plane prototype;
2. There is no additional traffic incurred;
3. The individual anti-spoofing mechanisms can function together by contributing their own opinion.

Two steps are performed in UAS: Marking and filtering. The first step, marking, is performed to help assess if the received packets are spoofed and executes on the routers in the intermediate network between the source and victim networks. There is no requirement to know where the routers are located or the number of hops they are away from the source. The second step, filtering, is executed on the edge routers of the victim network for which the packets are destined. The edge routers determine whether to discard the received packets according to a predefined threshold value. The marking bit f is set to "1" if the marking router determines that the received packet is spoofed, otherwise it is set to "0".

$$f = \begin{cases} 1, & \text{the router decides that the packet is spoofed;} \\ 0, & \text{otherwise} \end{cases} \quad (1)$$

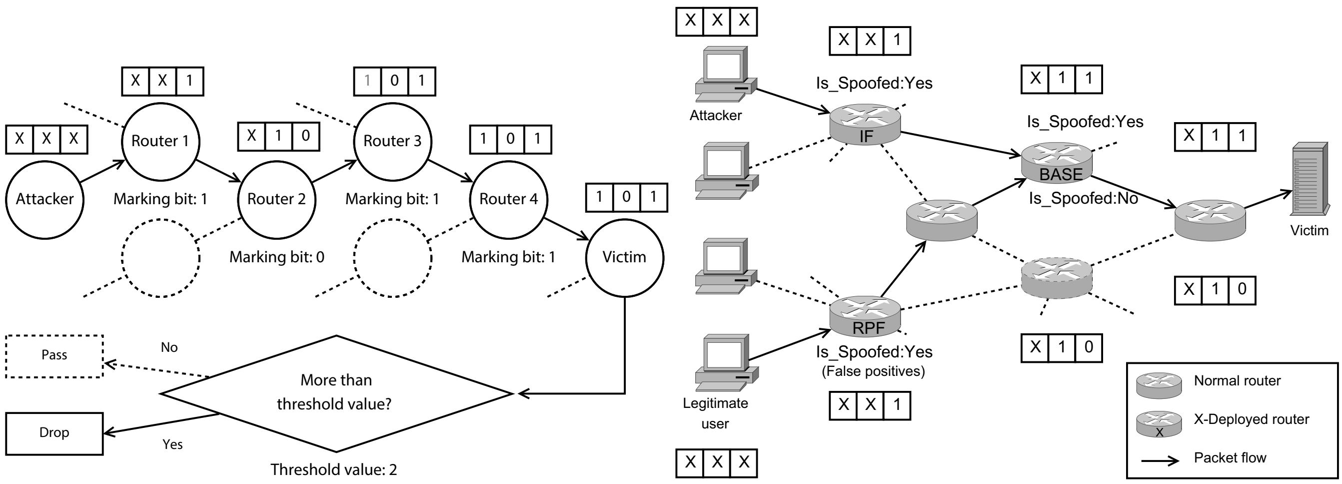
Fig. 3 depicts the operation of a three-bit marking field. Fig. 3(a) indicates the marking and filtering to ensure the proper operation of each mechanism. Fig. 3(b) displays an example of the low accuracy of an individual operating anti-spoofing mechanism with false positives, e.g., RPF. The received packet at the RPF-deployed router is legitimate, however, processed as spoofed. If the packet is discarded by the router, we cannot solve this mistake. In UAS, this mistake could be mitigated by the opinion of the BASE-deployed router. We provide detailed information of the interference in Section V.E.

B. Marking Field Design

The marking field is used to collect the opinions of deployed mechanisms and allow comprehensive decisions to be made. The identification field of the IP packet header is a good candidate for the deployed mechanisms on the routers to mark. This 16-bit field is used by many anti-spoofing mechanisms because it is rarely used on the Internet for other purposes. Savage *et al.* [34], [35] first argued that the IP identification field is a suitable candidate because it is used only for packet fragmented packets that constitute less than 0.25% of the packets on the Internet [36]. For this reason, several prevention mechanisms [2], [13], [16], [37] and IP traceback mechanisms [35], [38]–[40] use the IP identification field.

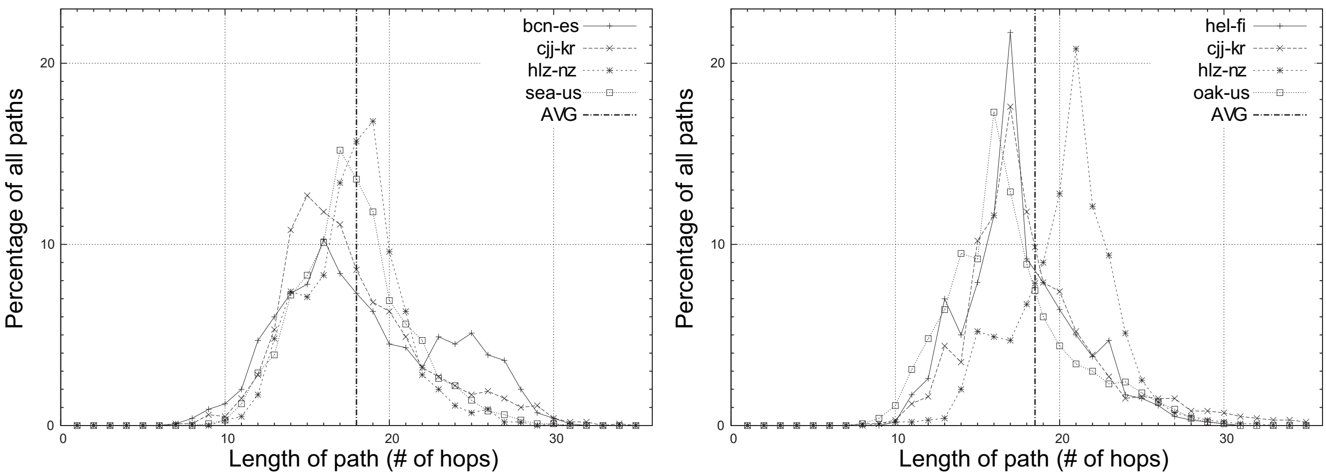
However, although the IP identification field can be used for marking, the maximum path length between the source and destination node can be longer than 16 hops. Fig. 4 displays the distribution of IP path lengths over Europe, Asia, Oceania, and North America. It indicates that the average length was 17.5 hops and the maximum length was 39 hops as of Jan. 22, 2016 [41]. These lengths will increase as the Internet grows.

In cases where the network path length is *less than 16* hops, the marking information can be recorded completely. However,



(a) (b)

Fig. 3. Examples of UAS operations between an attacker and a victim. Each router that adopts an anti-spoofing mechanism marks its determination into a marking bit. In this example, we illustrate the marking values stored in a three-bit marking field: (a) Marked values is used at the victim router for filtering and (b) a mistake at the RPF-deployed router could be mitigated by the opinion of the BASE-deployed router.



(a) (b)

Fig. 4. Distribution of IP path lengths: (a) Apr. 09, 2012 (AVG 17, MAX 34) and (b) Jan. 22, 2016 (AVG 17.5, MAX 39) where (1) bcn-es: Universitat Politecnica de Catalunya, Spain, Europe; (2) cjj-kr: KREONET, Republic of Korea, Asia; (3) hlz-nz: University of Waikato, New Zealand, Oceania; (4) sea-us: University of Washington, USA, North America; (5) hel-fi: Aalto University, Finland, Europe; (6) oak-us: International Computer Science Institute, USA, North America.

when it is *greater than 16* hops, given the limitation of 16 bits, we must determine other methods to record the information. Hence, the marking procedure must consider the limitations of the marking field length.

C. Marking Operations

There are three possible marking operations: bounded-shift-add (BSA), squash-zero (SZ), and plus-one (PO). BSA shifts and adds the marking bit to the n-bit marking field; marking terminates if the routing path is longer than n hops. SZ is similar to BSA; however, if the routing path is longer than n hops, it removes a legitimate packet mark and adds a spoofed packet mark. PO simply adds the marking bit to the marking field. Intermediate routers utilize the same marking operations. The victim network has two options for the filtering operation and can select one for performance in terms of accuracy.

Fig. 5 depicts these operations with a three-bit marking field. In the case where the routers use BSA, Routers 1 to 3 add their opinions to the marking field, however, Router 4 does not add its opinion because the marking field is already full. If the routers use SZ, Router 4 can add its opinion to the marking field after removing a legitimate packet mark. If the routers use PO, all routers add their opinions and one bit of the marking field remains unused.

1. **Bounded-shift-add (BSA)** shifts and adds the marking bit f_i to the n-bit marking field. Marking terminates if the routing path is more than n hops. This means that the most significant bit (MSB) of the marking field is "1".

$$m_i = (2 - MSB) \cdot m_{i-1} + (1 - MSB) \cdot f_i \quad (2)$$

2. **Squash-zero (SZ)** operates similarly to BSA. It removes a legitimate packet mark and adds a spoofed packet mark if the

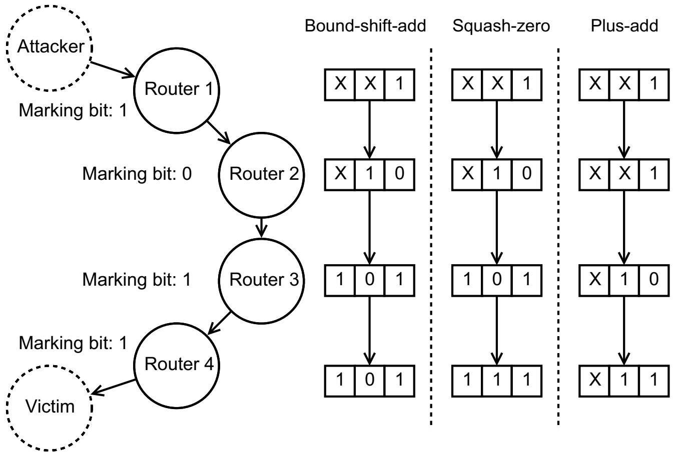


Fig. 5. Example of marking operations in the intermediate network. The packet travels from the attacker to the victim across Routers 1 to 4. Each router marks its own determination using a marking bit.

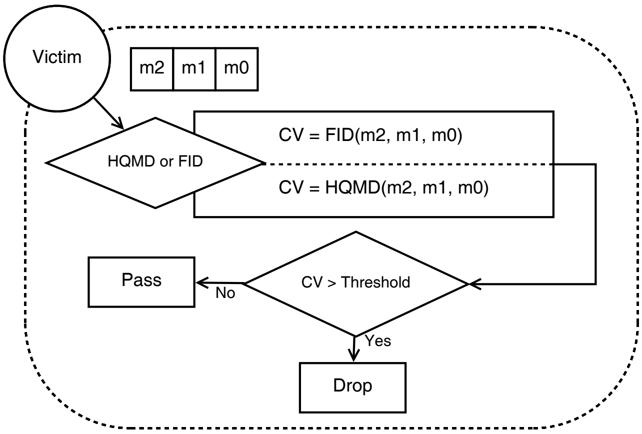


Fig. 6. Filtering operations of the victim network. When an edge router of the victim network receives the marked packets, it calculates the CV and compares it with a predefined threshold.

routing path is more than n hops. Index k is the highest-order legitimate bit ($1 \leq k \leq n$).

$$m_i = 2 \cdot m_{i-1} - MSB \cdot (2^n - 2^k) + f_i \tag{3}$$

3. **Plus-one (PO)** simply adds the marking bit to the marking field.

$$m_i = m_{i-1} + f_i \tag{4}$$

After these operations in the intermediate network, the raw data for the marked values for the packets must be processed to form a comprehensive assessment.

D. Filtering Operations

When an edge router in a victim network receives the marked packets, it calculates a comprehensive value (CV) from the marked values and compares this with a predefined threshold to decide whether the packets are spoofed. A higher CV value translates into a higher likelihood that the packet is spoofed. There are two possible operations for computing a CV from a marked value: First influence decision-making (FID) and host-near qualified majority decision-making (HQMD).

Fig. 6 depicts the filtering operations for calculating the CV to decide if the packets are spoofed. The marked values [m2, m1, m0] are converted into a CV by the FID or HQMD methods and compared with a predefined threshold θ. If the CV is greater than θ, the received packet is discarded. That is, packets are dropped at the victim network based on the CV calculated from the marking field of the packet and the threshold value of the victim network.

1. **First influence decision-making (FID)** uses the ordinary binary-coded (2^n weight-coded) decimal notation such that early marking has a higher impact on the result.

$$CV = \sum_{k=0}^{n-1} (2^k \times m_k) \tag{5}$$

2. **Host-near qualified majority decision-making (HQMD)** uses an n weight-coded decimal notation such that earlier determinations may be overturned by later (lower) bits.

$$CV = \sum_{k=0}^{n-1} \{(k+1) \times m_k\} \tag{6}$$

In the FID method, the binary marked values are processed as a binary number, converted to a decimal number and compared with the threshold. If the marked value is [1, 1, 1], the CV is $2^2 + 2^1 + 2^0 = 7$. This method is easy to calculate. In this approach, however, the earlier marked bits have a higher weight than the sum of the later bits. It is $2^q > \sum_{k=0}^{q-1} 2^k$ where $0 < q \leq n$.

This is always true from the definition of the binary number because the weight of each bit is 2^n, meaning that the results of FID are disproportionately influenced by the first marks. Values marked close to the attacker are more likely to be correct, however, this method does not implement a majority rule if the later bits cannot overturn the earlier result.

HQMD is a method that follows a qualified majority rule. It reduces the weight of each bit from 2^n to n, which is sufficient to overturn earlier results by the sum of later bits, remedying FID's defect (i.e., q can be less than $\sum_{k=0}^{q-1}(k+1), 0 < q \leq n$).

Another method to overturn the early results is to assign the weight of every bit to "1", however, a new method is unnecessary because PO with FID operates in this manner. In PO, marked values have a binary number indicating the number of routers that described bits and FID converts this to a decimal number.

E. Operation Algorithms

When an intermediate router receives a packet, the router determines if the packet is spoofed using its deployed anti-spoofing mechanism and records this determination (or opinion) using BSA, SZ, or PO. If the marking field has been filled by previous routers, the packets are transferred normally.

The detailed algorithm for the marking operations is presented below. It illustrates the operations of an intermediate router when a packet arrives. Let N be the number of marking bits, m be the marked value of the received packet, and *op* be the marking operation used.

If we utilize BSA as the marking operation and a router receives packets, the marked value is shifted to empty the least significant bit (LSB) and a flag f is added, "1" if the packet is regarded as spoofed, otherwise "0". As the marking bit is close to the MSB, it is the decision of the router that is closest to the packet sender. If we utilize SZ, the router shifts the marked value and adds a flag similar to BSA. If MSB is "1", however, the highest-order legitimate bit ($= 0$) is removed and the lower bits (than the highest-order legitimate bit) are shifted. Then, f is added to the LSB. SZ can records spoofed-decisions more than BSA. If we utilize PO, f is simply added. This means that the marked value is increased by one when the router decides the packets are spoofed.

$N \leftarrow$ Number of marking bits;
$m \leftarrow$ Marked value of a received packet;
$op \leftarrow$ Current used marking operation;
$f \leftarrow 1$ if the packet is regarded as spoofed, otherwise 0;
if $op = BSA$ **then** // Marking op.: Bound-shift-add
  if $m[N-1] \neq 1$ **then**
    $m \leftarrow m \ll 1$;
    $m[0] \leftarrow f$;
  end if
else if $op = SZ$ **then** // Marking op.: Squash-zero
  if $m[N-1] \neq 1$ **then**
    $m \leftarrow m \ll 1$;
    $m[0] \leftarrow f$;
  else
    for $i \leftarrow (N-2)$ **to** 1 **do**
      if $m[i] = 0$ **then**
        $m[i] \leftarrow m[i-1]$;
        $m[i-1] = 0$;
      end if
    end for
    if $m[0] = 0$ **then**
      $m[0] \leftarrow f$;
    end if
  end if
else if $op = PO$ **then** // Marking op.: Plus-one
  if $m < (2^N - 1)$ **then**
    $m \leftarrow m + f$;
  end if
end if

When a victim router receives a packet, the router determines if the received packet is spoofed based on a predefined threshold. Before packet filtering, the marked value is converted into a CV using either FID or HQMD and compared with a threshold θ for filtering.

$N \leftarrow$ Number of marking bits;
$m \leftarrow$ Marked values of a received packet;
$op \leftarrow$ Used filtering operation;
$\theta \leftarrow$ Predefined threshold value;
$cv \leftarrow \emptyset$;
for $i \leftarrow 0$ **to** $N-1$ **do** // CV by FID or HQMD
  if $op = FID$ **then**
    $cv = cv + \{2^i \times m[i]\}$; // A binary-coded decimal
  else if $op = HQMD$ **then**
    $cv = cv + \{(i+1) \times m[i]\}$; // An n weight-coded decimal
  end if
end for
if $cv \geq \theta$ **then** // Filtering with threshold
  $Drop\_Packet()$;
else
  $Pass\_Packet()$;
end if

The above algorithm details the filtering operations of a victim network when the packets arrive at its routers. If we utilize FID as the filtering operation, the marked value of the received packet is considered a binary number and calculated. This means that the weight of each bit is 2^i (let i be an index number of the marking field); the weight of the LSB is 2^0. If we utilize HQMD, each weight is changed to $(i + 1)$. The weight of the LSB is one. The result is stored in cv as a CV. Then, the packet is bypassed when CV is less than the threshold θ, otherwise the packet is discarded.

Marking operations provide a method to collect the opinions of the intermediate routers. Filtering operations provide a method to make comprehensive decisions. We must define a performance measure to determine if these operations are sufficient to integrate into existing mechanisms.

V. PERFORMANCE MEASURE

To evaluate and compare the performance of the mechanisms, a performance measure was defined. False positive and false negative ratios are meaningful measures that can be used to compare two or more anti-spoofing mechanisms. A *positive* occurs when a packet is spoofed. Thus, a *false positive* indicates that a packet that is not spoofed has been discarded as spoofed, whereas a *false negative* indicates that a packet that is spoofed is accepted as non-spoofed. That is, false positives and false negatives are misjudgments made by a prevention mechanism. Prevention mechanisms must attempt to minimize misjudgments.

For example, consider a scenario where two mechanisms, α and β, attempt to prevent IP spoofing. If mechanism α generates fewer false positives than β, then α can be considered to be superior to β. However, if α generates more false negatives than β, it is difficult to decide what mechanism is superior. The relative importance of false positives and false negatives depends on the situation. Hence, we must determine performance by considering both false positives and false negatives.

A. False Decision Percentage Function

In cases where we consider the online service to be more important than the victim server, false positives must be avoided at any cost, whereas some false negatives can be accepted. This is because reducing the false positive rate results in dropped legitimate packets and disrupted network operation. Conversely, in cases where protecting the victim is more important than providing the service, false negatives may be much more dangerous. If the victim is related to national security, even a single attack can cause a significant amount of damage [42]. If we assume that both are equally important and the weight of false positives is equal to the weight of false negatives, the amount of misjudgment at deployment percentage x is given by the false decision percentage (FDP) function as follows:

$$F_\theta(x) = FP_\theta(x) + FN_\theta(x), \tag{7}$$

where $FP_\theta(x)$ is the false positive percentage, $FN_\theta(x)$ is the false negative percentage, θ is the threshold value belonging to $T = \{\theta \mid \theta > 0\}$, and x is the deployment percentage belonging to $R = \{x \mid x > 0 \text{ and } x \leq 100\}$.

In the case where the threshold value $\theta = 1$, the comparison between UAS and multiple individual mechanisms acquires a special meaning; the UAS result is the same as that of the original deployed mechanisms running individually on the network. When the threshold value is one, the packets are filtered by the first marked value indicating a spoofed packet and hence, the result is the same as that when filtering using only the first prevention mechanism. Therefore, $F_1(x)$ signifies the sum of false positives and false negatives for a given deployment percentage x of the individual mechanisms without UAS. If we let $F(x)$ be the FDP function without UAS, then $F(x) = F_1(x)$ is true.

B. False Decision Rate for Threshold Value θ

The overall amount of misjudgment is the sum of misjudgments for all x, and can be defined using the FDP function $F_\theta(x)$ as follows:

$$S_\theta = \int_{x \in R} F_\theta(x), \tag{8}$$

where S_θ is the sum of $F_\theta(x)$ for a given threshold value θ and the deployment percentage belongs to $R = \{x \mid x > 0 \text{ and } x \leq 100\}$. Thus, this value indicates the overall amount of misjudgment by the prevention mechanisms on the network when the threshold value is θ.

Eq. (8) enables us to accurately compare performance between S_a and S_b, where $a, b \in T$ and $a \neq b$. A result of $S_a < S_b$ signifies that S_a has fewer false positives and false negatives than S_b. That is, it has a higher overall accuracy for threshold value a. In particular, we can state that it always has a higher accuracy if $F_a(x) < F_b(x)$ is true for all x.

C. Minimized False Decisions

The FDP function $F_\theta(x)$ changes according to θ and a minimized FDP (mFDP) function can be defined as follows to measure the accuracy of UAS against existing mechanisms operating individually.

$$F_{\min}(x) = \min_\theta F_\theta(x) \tag{9}$$

Therefore, the overall amount of minimized misjudgment can be defined using mFDP as follows:

$$S_{\min} = \int_{x \in R} F_{\min}(x), \tag{10}$$

where θ belongs to the T that minimizes the result for all x.

For example, let $R = \{k, l\}$ and $k < l$. Then, $F_m(k)$ is greater than $F_n(k)$, although $F_m(l)$ may be less than $F_n(l)$. In this case, $S_{\min}$ is $F_n(k)+F_m(l)$. By altering the threshold value, $S_{\min}$ minimizes the number of inaccurate decisions.

D. Properties of Minimized False Decisions

From the equations defined above, we can identify several properties. For all x, $F_{\min}(x) \leq F_\theta(x)$ is true from Eq. (9). If $F_1(x) \leq F_\theta(x)$ is true for all x and for all θ, then $F_1 = F_{\min}$ is also true from Eq. (9). Hence, $F_{\min}(x) \leq F_1(x)$ is always true for all x and for all θ.

$$F_{\min}(x) \leq F_1(x) \tag{11}$$

The amount of minimized misjudgment for x is always equal to or less than the amount of misjudgment of individually operating mechanisms. Further, for all θ, $S_{\min} \leq S_1$ is true.

$$S_{\min} \leq S_1 \tag{12}$$

The overall amount of minimized misjudgment is always equal to or less than the overall amount of misjudgment of individually operating mechanisms. If UAS incorporates existing mechanisms, the results of the experiments should satisfy (11) and (12).

E. Interference by Low Accuracy

Let anti-spoofing mechanisms A, B, and C be deployed on Router 1, Router 2, and Router 3 between a user and a server without UAS. If we let their packet dropping ratio by their own false positives be 0.2, the packet's reaching ratio to the server against the false dropping is $(1-0.2)^3 = 0.512$. This means that the overall false dropping ratio is 0.488, which is greater than each false dropping ratio 0.2 and half of the legitimate packets will be discarded. Furthermore, the overall false dropping ratio becomes 0.672 with five routers and 0.892 with ten routers. If an upstream router detects IP spoofing and thus drops the packet, the packet will not arrive at the remaining downward routers. Thus, false positives are dependent and can be greater under the coexistence of multiple anti-spoofing mechanisms.

If B and C are the same anti-spoofing mechanisms in different locations, they are dependent on each other and provide improved operation. The false dropping ratio in the dependent case is less than or equal to that of the case above. This means that the overall false dropping ratio is also less than or equal. However, the overall false dropping ratio is greater than each false dropping ratio unless each ratio is equal to zero or there is not another mechanism A.

Individually operating anti-spoofing mechanisms on the network are dependent and cause interference by low accuracy, which is their own false dropping ratio. Thus, the overall false dropping ratio P_{all} can be defined using each false dropping ratio P_n where n is equal to the number of anti-spoofing mechanisms operating on the routers between a user and a server ($n \geq 2$).

$$P_{\text{all}} = 1 - \prod_{i=1}^{n}(1 - P_i) \tag{13}$$

If the number of routers n increases to ∞, P_{all} converses to one. $\prod_{i=1}^{n}(1 - P_i)$ is the overall reaching ratio, which is equal to or less than every routers' reaching ratio $(1 - P_n)$ because $(0 \leq P_n \leq 1)$.

$$\prod_{i=1}^{n}(1-P_i) \leq \min(1-P_1,\cdots,1-P_n) \tag{14}$$

Then, we can redefine (14) using (13) as follows:

$$P_{\text{all}} \geq 1-\min(1-P_1,\cdots,1-P_n). \tag{15}$$

Eq. (15) indicates that the overall false dropping ratio P_{all} is always equal to or greater than the greatest false dropping ratio P_n. If one of P_n is equal to one, P_{all} is also equal to one. From (13), if all of P_n is equal to zero, P_{all} is also equal to zero. Otherwise, P_{all} is definitely greater than all of P_n because $\prod_{i=1}^{n}(1-P_i)$ becomes smaller than all of $(1-P_n)$ where $0 < P_n < 1$ and $n \geq 2$. This is the reason we must have a platform that can incorporate existing anti-spoofing mechanisms. We next evaluate the performance of UAS in terms of false positives and false negatives to demonstrate that UAS provides a sufficient manner to incorporate existing mechanisms.

VI. EVALUATION AND DISCUSSION

In this section, we evaluate the performance of UAS with a simulation program using Internet topologies and four anti-spoofing mechanisms: Ingress filtering [15], RPF [10], DPF [11], and BASE [2]. First, we discuss the result of a simple dual scheme. We follow this with a discussion of the correlation between the two selected mechanisms in the dual scheme. Next, we examine the results of a mixed scheme using the four mechanisms mentioned above. Finally, we evaluate the accuracy of UAS by comparing it with a non-UAS case.

We modified the simulation program by Parno *et al*. [43] to incorporate UAS. The Internet topology used in the simulation was derived from CAIDA Skitter [44] probe results that depict a router-level topology. The Skitter map is a rooted tree. We used a 3,000-node map and a randomly chosen end node sent packets to the root node at a rate of 20,000 packets per unit time.

A. Dual Scheme

In this section, we first study the results of a dual scheme integrated by UAS on a network and explain how to interpret these results. In our simulation, to compare the performance of marking methods given the limitations of the marking field length, we assumed that $R = \{x \mid x = 10, 20, 30, \cdots, 90, 100\}$ and $T = \{\theta \mid \theta = 2^n,\ n = 0, 1, 2, 3\}$ and the marking field was four bits long.

Fig. 7 depicts the relation between mechanism deployment percentage and false decision by changing the threshold value. In Fig. 7(a), $F(x)$ is plotted for RPF, BASE, and a dual scheme (RPF and BASE deployed in equal numbers). Fig. 7(b) displays $F_\theta(x)$ for $\theta \in T = \{2^0 = 1,\ 2^1 = 2,\ 2^2 = 4,\ 2^3 = 8\}$ for the dual scheme for $x \in R$ and $F_1(x)$ indicates the result without UAS.

Fig. 7(a) indicates that there is an increase in the number of false decisions because of the interference from the low accuracy of the operating mechanisms individually as we explain in Section V.E. In this result, RPF has low accuracy for the entire deployment ratio. The performance falters (i.e., the FDP rises) as the deployment percentage increases when RPF and BASE are deployed in equal amounts. This indicates that one detrimental deployment mechanism can cause the interference; increasing the deployment can impair the results and each method's misjudgment restrict the growth potential of the other.

However, Fig. 7(b) indicates that UAS can mitigate the interference and reduce the false decisions in the dual scheme. As can be observed, $F_{\min}(x)$ is less than $F_1(x)$. The scheme using $F_2(x) \in \{30, \cdots, 100\}$ has lower false decision percentages than $F_1(x)$ without UAS. This means that we can realize improved accuracy when we adopt UAS with only a minimum threshold, $\theta = 2$. Furthermore, $F_3(x) \in \{60, \cdots, 100\}$ has the lowest false decision percentages. The result of BASE 100% from Fig. 7(a) is better than $F_{\min}(x)$; however, the problem is that any anti-spoofing mechanism alone is difficult to deploy widely on a network such as Fig. 7(a). These results indicate that UAS reduces interference and improves accuracy. Further, S_1 is 310.9 and $S_{\min}$ is 175.8, indicating a decrease of 43.5% when using UAS.

UAS addresses the peculiarities that arise because of the interactions among the individual mechanisms. The filtering strength of the integrated mechanisms is enhanced by modifying the threshold value. The results demonstrate that UAS cooperates effectively with the existing mechanisms

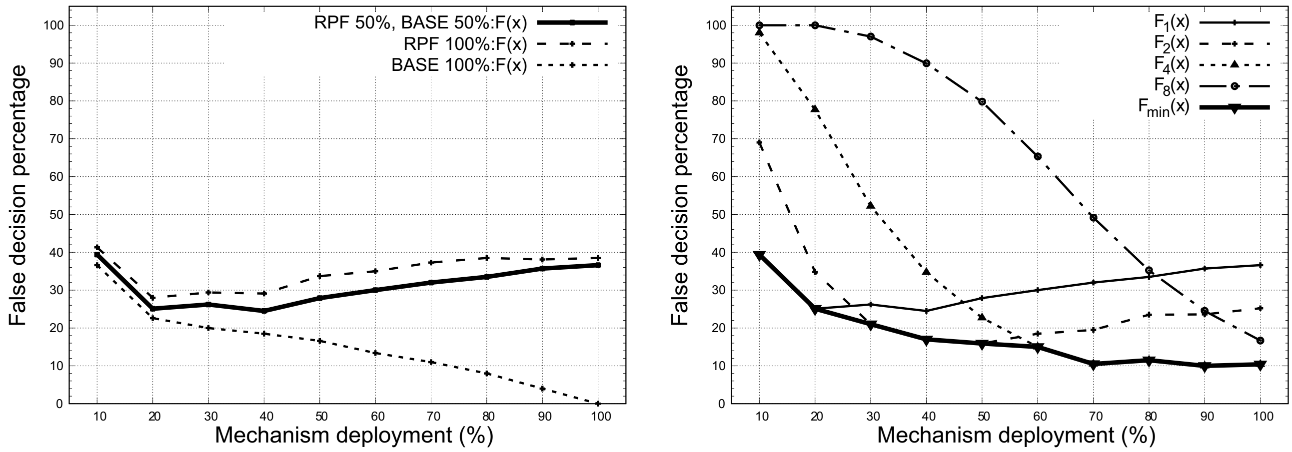
B. True Positives of Marking Field between BSA and SZ

The marking operation SZ is designed to improve the efficiency of the limited marking field length when it uses BSA as explained in Section IV.B. Fig. 8 displays the true positive percentage of each bit of a packet's marking field. Fig. 8(a), a result using BSA, indicates that the true positives of the 1st marking bit only, increase in an arc as the deployment percentage of the anti-spoofing mechanism continues to increase. Fig. 8(b) indicates that all marking bits move up in an arc. These results demonstrate that SZ manages the marking field effectively and improves the accuracy of the marking operations more than BSA.

C. Sensitivity and Specificity of FID and HQMD

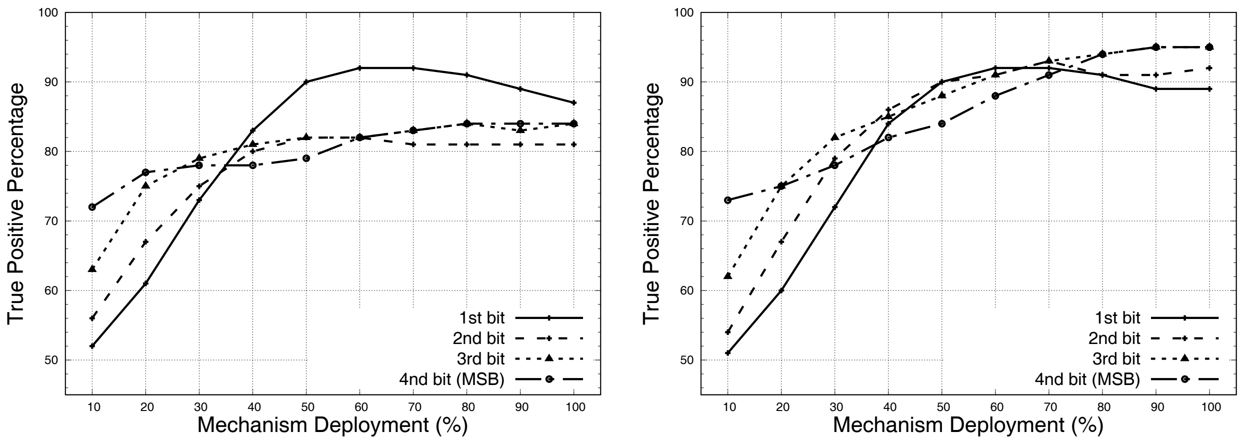
Previously, we described FID and HQMD and how they filter. HQMD is designed to remedy FID's defect. Fig. 9 displays the relation between false positive ratio (1 − Specificity) and true positive ratio (Sensitivity) of FID and HQMD for $R = \{x \mid x = 10, 20, 30, \cdots, 90, 100\}$ and $T = \{\theta \mid \theta = 2^n,\ n = 0, 1, 2, 3\}$. HQMD depicts less false positives and more true positives than FID as we attempt to overturn earlier marking bits by the sum of later bits for accuracy.

Fig. 10 presents the receiver operating characteristic (ROC) curve; the relation between false positive ratio (1−Specificity) and true positive ratio (Sensitivity) for $R = \{x \mid x = 10, 20, 30, \cdots, 90, 100\}$ and $T = \{\theta \mid \theta = 2^n,\ n = 1, 2\}$. The results have three groups of false positives and true positives: [PO (FID or HQMD)], [BSA or SZ (HQMD)], and [BSA or SZ (FID)]. BSA or SZ using HQMD demonstrate superior performance in terms of the accuracy compared to using FID. As we discussed, HQMD provides a remedy to FID's defect. This means that HQMD is more effective for filtering and improves the accuracy of UAS operations compared to FID when we use BSA or SZ as the marking operation.



(a) (b)

Fig. 7. Results for the dual scheme (RPF and BASE). The false decision percentage is the sum of the FP and FN percentages: (a) Interference without UAS and (b) coordination with UAS using PO and FID.



(a) (b)

Fig. 8. True positives of each marking bit for IF 25%, RPF 25%, DPF 25%, and BASE 25%: (a) Using BSA and (b) using SZ.

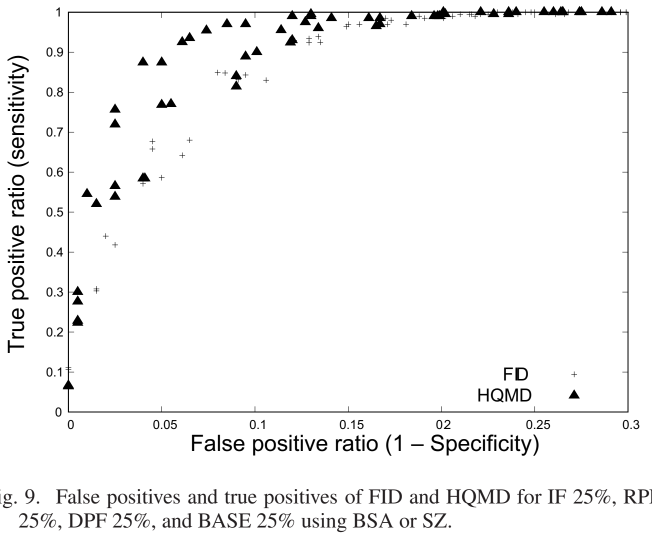


Fig. 9. False positives and true positives of FID and HQMD for IF 25%, RPF 25%, DPF 25%, and BASE 25% using BSA or SZ.

Fig. 10 indicates that PO is the best marking operation for false positives and true positives. When we use PO as the marking operation, the two filtering methods do not seem to have a significant difference. The results of PO with FID or HQMD are similar where θ is equal to 2^1 or 2^2. The average path length was approximately 14 hops and the maximum length was approximately 26 in this evaluation. We used a four-bit as limitation for the marking field. This indicates that PO is an effective option to record the maximum number of router opinions with a limited marking field.

D. Mixed Scheme

We evaluated the performance of UAS using four mechanisms in mixed schemes of 19 different proportions as presented in Table 1. The proportions were used to consider various network environments with several anti-spoofing mechanisms and to demonstrate that UAS operates properly with existing mechanisms. Moreover, we can identify the marking and filtering operations that are more effective under various deployment conditions.

Fig. 11(a) exhibits the results of one of the experiments, where S_1 is 251.5 and $S_{\min}$ is 168.2, indicating a decrease of 33.1%. With UAS, if each mechanism is deployed only on 25% of the network, the number of false decisions made by those

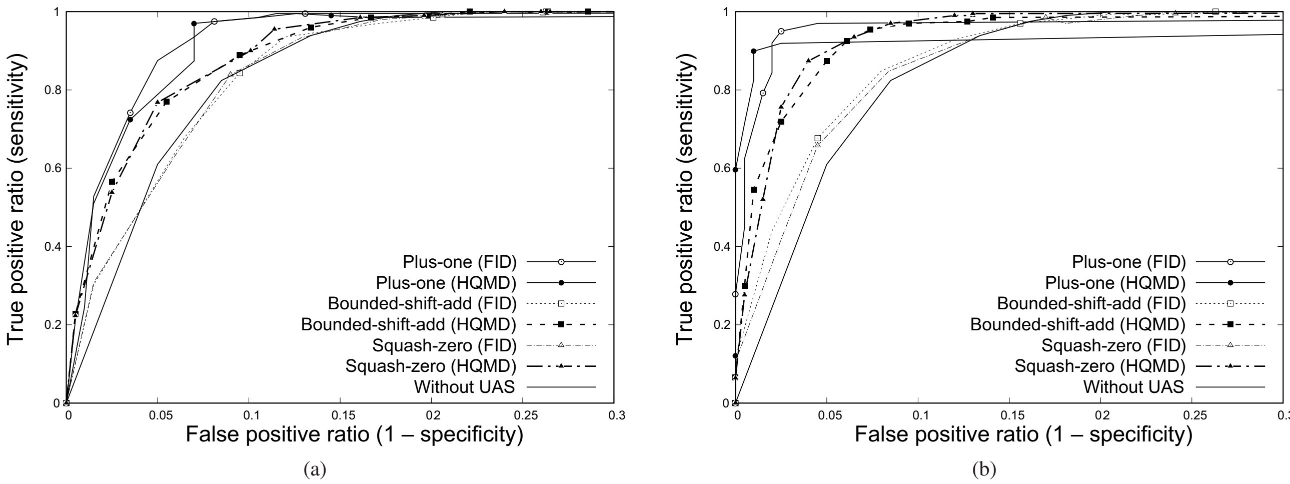


Fig. 10. ROC Curve: false positives and true positives by threshold for IF 25%, RPF 25%, DPF 25%, and BASE 25% using BSA or SZ: (a) Threshold = 2^1 and (b) threshold = 2^2.

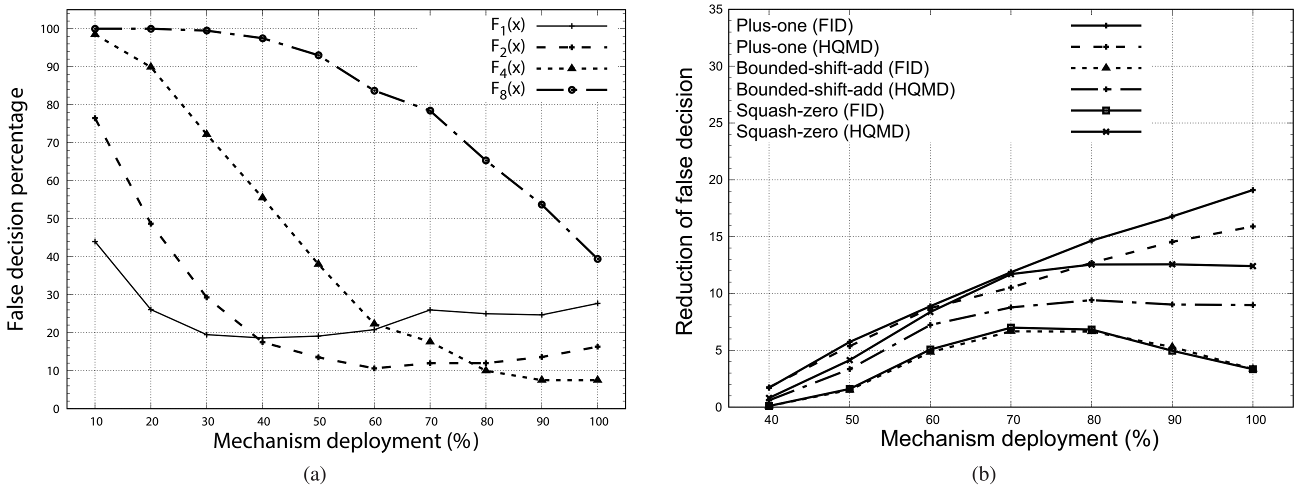


Fig. 11. Mixed Scheme: (a) Sum of FP and FN for IF 25%, RPF 25%, DPF 25%, and BASE 25% using Plus-one and FID and (b) average reduction of false decisions with UAS using 19 different mechanism deployment proportions.

mechanisms is reduced by 72.9% and the sum of false decisions is reduced by 33.1% compared to the case where each mechanism operates separately, as indicated in Tables 2 and 3. Furthermore, false decision rates were reduced up to 84.5% in the case of 10% for ingress filtering, 40% for RPF, 40% for DPF, and 10% for BASE using PO and FID. These decreases confirm that the proposed mechanism can significantly reduce false alarms by incorporating multiple schemes. Fig. 11(b) plots the average reduction of false decisions for marking and filtering operations using the 19 different proportions in Table 1. This result demonstrates that UAS is desirable to decrease false decisions and that the combination of PO / FID is the best case in terms of false decision.

E. Deployment Ratio and Threshold Value

As illustrated in Fig. 11(a), even if the threshold value is two, UAS demonstrates superior performance compared to the result without UAS. However, as indicated in Fig. 11(b), changing the threshold value is a dominant factor for overall performance. Threshold selection will be a future work for us. However, we would like to provide a concise idea on how this can function.

If we utilize the unused field of an IPv4 packet, there is the possibility of a field of 25 bits to record information [39]. In this evaluation, UAS demonstrates effective operation using only four bits for marking. If each UAS router adds "1" using the other field, the victim can determine how many UAS routers were in the path of the arrived packets. Moreover, we can figure out a hop count from an attacker according to [32]. Then, the victim network could calculate (number of UAS routers / hop count) a deployment ratio of the arrived packet's path dynamically and could change the threshold value based on the dynamic deployment ratio.

F. Incremental Deployment

UAS is sufficient to be deployed on a real network. As we explained in Section IV, the marking operations use only bit-shift and flag-add and the filtering operations use the multiply and sum of natural numbers. Computation overhead is the same level as TTL of a IPv4 packet. Routers of intermediate and victim networks require only small changes. Many existing mechanisms already use simple calculations such as TTL; hence, this is not a significant issue for deployment.

UAS provides deployment incentives to ISPs and is adoptable for incremental deployment.

- **Initial deployment**: Routers utilize their own existing mechanism. In [45], ingress filtering is adopted for a similar case of incremental deployment — ($F(x) = F_1(x)$).
- **Partial deployment**: UAS-ready intermediate routers, which know UAS, record their own opinions into the packets. UAS-ready victim routers with filtering operations receive the packets with recorded opinions. As the deployment ratio increases, the victim receives more opinions and achieves a higher accuracy of anti-spoofing decisions. The evaluation results demonstrate that only four-bit marking values can be used to adopt UAS to operate effectively. A non-UAS victim router that does not know UAS, can discard the packets with a rule (threshold = 1). Those routers operate as if there were no UAS evaluation results, $F_1(x)$. This rule is simple and can be adopted by the victim easily. The non-UAS intermediate routers utilize their own existing mechanism to drop the spoofed packets. The packets are discarded by the existing mechanism or the filtering operation of the victim networks — ($F_1(x) \geq F(x) \geq F_{\min}(x)$).
- **Full deployment**: If the routers of the intermediate and victim networks know UAS, operations will be as explained above — ($F(x) = F_{\min}(x)$).

Table 1. Proportions of mechanisms used in the simulation.

#	IF	RPF	DPF	$BASE$
1	25%	25%	25%	25%
2	40%	20%	20%	20%
3	20%	40%	20%	20%
4	20%	20%	40%	20%
5	20%	20%	20%	40%
6	40%	40%	10%	10%
7	40%	10%	40%	10%
8	40%	10%	10%	40%
9	10%	40%	40%	10%
10	10%	40%	10%	40%
11	10%	10%	40%	40%
12	30%	30%	30%	10%
13	30%	30%	10%	30%
14	30%	10%	30%	30%
15	10%	30%	30%	30%
16	0%	34%	33%	33%
17	34%	0 %	33%	33%
18	34%	33%	0%	33%
19	34%	33%	33%	0%

Table 2. Decrease of $F_\theta(100\%)$ when deployment percentage of each mechanism is 25%.

Operations	$F_1(100\%)$	$F_{\min}(100\%)$	Decrease
PO and FID	27.7	7.5	72.9%
BSA and FID	30.3	26.4	12.9%
SZ and FID	29.6	26.6	10.1%
PO and HQMD	29.7	10.6	64.3%
BSA and HQMD	29.1	15.6	46.4%
SZ and HQMD	27.5	13.5	50.9%

Table 3. Decrease of S_θ when deployment percentage of each mechanism is 25%.

Operations	S_1	$S_{\min}$	Decrease
PO and FID	251.5	168.2	33.1%
BSA and FID	261.1	232.1	11.1%
SZ and FID	259.0	231.5	10.6%
PO and HQMD	258.6	180.4	30.2%
BSA and HQMD	254.6	195.9	23.1%
SZ and HQMD	255.6	193.4	24.3%

G. Changing UAS Marking Values

Owing to the lack of integrity of marking bits, a malicious router can change marking bits to degrade the destination's ability to mitigate spoofing attacks. Instead of attacking a victim, an attacker can attack the intermediate routers in the path to the victim, potentially causing a disruption in the paths packets select to reach the victim. A clever victim may be able to identify the router under attack by comparing the marking values of the traffic before and after the attack begins, such as StackPi [16].

VII. CONCLUSION

In this paper, we proposed a novel scheme that integrates existing and already deployed anti-spoofing mechanisms. Although there are many schemes to prevent IP spoofing, they have not achieved widespread deployment. The limitations of each mechanism hamper its deployment and the low deployment ratio of these mechanisms results in false positives and false negatives. These individually operating anti-spoofing mechanisms on the network cause interference from low accuracy, which are their own false positives.

For this reason, we require a platform that can incorporate existing anti-spoofing mechanisms. Integrating mechanisms is a superior option than wider deployment of one mechanism. Therefore, we propose UAS, which integrates existing mechanisms on the network for effective defense against IP spoofing attacks. In the proposed mechanism, existing anti-spoofing mechanisms with marking and filtering processes enable each mechanism to be integrated with others for coordination (C) and work in synergy (S) to significantly reduce false alarms. Furthermore, UAS provides incrementality (I) to operate in cases of initial, partial, and full deployment.

The results of the experiments indicate that the proposed mechanism reduces false decisions. That is, UAS increases the accuracy of existing mechanisms. In the experiments using four pre-deployed mechanisms with UAS, with each mechanism deployed on 25% of the network, the number of false decisions was reduced by 72.9% compared to the case where each mechanism operated individually. The false decision rate was found to be reduced by as much as 84.5% in one experiment. These decreases indicate that UAS significantly reduces false alarms by incorporating multiple schemes.

In our future work, we will determine an approach to place UAS-aware routers in the intermediate network for location optimization. Furthermore, we will theoretically calculate the optimum time to switch the threshold value of a victim network to minimize false decisions. Deployment strategies with real networks such as software defined network (SDN) will also be targeted to confirm that UAS is an adoptable anti-spoofing mechanism in the real world.

REFERENCES

[1] CERT, "Cert advisory ca-1996-21 TCP SYN flooding and IP spoofing attacks," Sept. 1996.

[2] H. Lee, M. Kwon, G. Hasker, and A. Perrig, "BASE: An incrementally deployable mechanism for viable IP spoofing prevention," in *Proc. ACM AsiaCCS*, 2007, pp. 20–31.

[3] D. Lee. (2014, Feb.). Huge hack 'ugly sign of future' for Internet threats. BBC. [Online]. Available: http://www.bbc.com/news/technology-2613 6774.

[4] C. Rossow, "Amplification hell: Revisiting network protocols for DDoS abuse," *NDSS*, Feb. 2014, pp. 23–26.

[5] A. Mangla. (2006). Distributed reflection denial of service: A bandwidth attack. [Online]. Aviliable: http://palpapers.plynt.com/issues/2006Apr /ddos-reflection/

[6] G. Yao, J. Bi, and A. V. Vasilakos, "Passive IP traceback: Disclosing the locations of IP spoofers from path backscatter," *IEEE Trans. Inf. Forensics and Security*, vol. 10, no. 3, pp. 471–484, 2015.

[7] CAIDA. (2016). The UCSD Network Telescope. [Online]. Available: https://www.caida.org/projects/network_telescope/

[8] R. Beverly, A. Berger, Y. Hyun, and k. claffy, "Understanding the efficacy of deployed Internet source address validation filtering," *ACM SIGCOMM IMC*, Nov. 2009, pp. 356–369.

[9] J. Kwon *et al.*, "An incrementally deployable anti-spoofing mechanism for software-defined networks," *Comput. Commun.*, vol. 64, pp. 1–20, 2015.

[10] F. Baker and P. Savola, "Ingress filtering for multihomed networks," BCP 84, RFC 3704, Mar., Tech. Rep., 2004.

[11] K. Park and H. Lee, "On the effectiveness of route-based packet filtering for distributed DoS attack prevention in power-law internets," in *Proc. ACM SIGCOMM*, Aug. 2001, pp. 15–26.

[12] D. Anstee, J. Escobar, C. Chui, and G. Sockrider, "Worldwide infrastructure security report volume X," Arbor Networks, Tech. Rep., 2015.

[13] A. Yaar, A. Perrig, and D. Song, "Pi: A path identification mechanism to defend against DDoS attacks," *IEEE S&P*, pp. 93–107, 2003.

[14] S. T. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks," *Commun. Surveys Tuts.*, vol. 15, no. 4, pp. 2046–2069, 2013.

[15] P. Ferguson and D. Senie, "Network ingress filtering: Defeating denial of service attacks which employ IP source address spoofing," BCP 38, RFC 2827 May, Tech. Rep., 2000.

[16] A. Yaar, A. Perrig, and D. Song, "StackPi: New packet marking and filtering mechanisms for DDoS and IP spoofing defense," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 10, pp. 1853–1863, 2006.

[17] G. Yao, J. Bi, and P. Xiao, "VASE: Filtering IP spoofing traffic with agility," *Comput. Netw.*, vol. 57, no. 1, pp. 243–257, 2013.

[18] B. Liu, J. Bi, and A. Vasilakos, "Towards incentivizing anti-spoofing deployment," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 3, pp. 436–450, Mar. 2014.

[19] H. Wang, C. Jin, and K. G. Shin, "Defense against spoofed IP traffic using hop-count filtering," *IEEE/ACM Trans. Netw.*, vol. 15, no. 1, pp. 40–53, Feb. 2007.

[20] M. Abliz, "Internet denial of service attacks and defense mechanisms," *Tech. Rep. TR-11-178*, 2011.

[21] S. Yu, W. Zhou, S. Guo, and M. Guo, "A dynamical deterministic packet marking scheme for DDoS traceback," in *Proc. IEEE GLOBECOM*,2013, pp. 729–734.

[22] D. Moore, C. Shannon, D. J. Brown, G. M. Voelker, and S. Savage, "Inferring internet denial-of-service activity," *ACM Trans. Comput. Syst.*, vol. 24, no. 2, pp. 115–139, 2006.

[23] J. Markoff and N. Perlroth. (2013, Mar.). Firm is accused of sending spam, and fight jams Internet. The New York Times. [Online]. Available: http://www.nytimes.com/2013/03/27/technology/internet/online-dispute-becomes-internet-snarling-attack.html?smid=pl-share

[24] M. Anagnostopoulos, G. Kambourakis, P. Kopanos, G. Louloudakis, and S. Gritzalis, "DNS amplification attack revisited," *Computers & Security*, vol. 39, pp. 475–485, 2013.

[25] D. Lee. (2013, Mar.). Global Internet slows after 'biggest attack in history'. BBC. [Online]. Available: http://www.bbc.co.uk/news/technology-21954636

[26] R. Lemos. (2014, Jan). Amplified DDoS attacks broke bandwidth records in 2013: Arbor report. eWeek. [Online]. Available: http://www.eweek.com/security/amplified-ddos-attacks-broke-bandwidth-records-in-2013-arbor-report.html

[27] A. Liska. (2013, Dec.). Hackers spend Christmas break launching large scale NTP-reflection attacks. Symantec. [Online]. Available: http://www.symantec.com/connect/blogs/hackers-spend-christmas-break-launching-large-scale-ntp-reflection-attacks

[28] R. Beverly and S. Bauer. (2016). ANA Spoofer Project. [Online]. Availble: http://spoofer.cmand.org/

[29] T. Ehrenkranz and J. Li, "On the state of IP spoofing defense," *ACM Trans. Internet Technol.*, vol. 9, no. 2, p. 6, 2009.

[30] F. Baker *et al.*, "Addressing the challenge of IP spoofing," Internet Society, Tech. Rep., 2015.

[31] S. Yu, G. Wang, and W. Zhou, "Modeling malicious activities in cyber space," *IEEE Netw.*, vol. 29, no. 6, pp. 83–87, 2015.

[32] D. Seo, H. Lee, and A. Perrig, "APFS: Adaptive probabilistic filter scheduling against distributed denial-of-service attacks," *Computers & Security*, vol. 39, pp. 366–385, 2013.

[33] L. Feinstein, D. Schnackenberg, R. Balupari, and D. Kindred, "Statistical approaches to DDoS attack detection and response," *DISCEX*, 2003, pp. 303–314.

[34] S. Savage, D. Wetherall, A. Karlin, and T. Anderson, "Network support for IP traceback," *IEEE/ACM Trans. Netw.*, vol. 9, no. 3, pp. 226–237, 2001.

[35] S. Savage, D. Wetherall, A. Karlin, and T. Anderson, "Practical network support for IP traceback," in *Proc. ACM SIGCOMM*, 2000, pp. 295–306.

[36] I. Stoica and H. Zhang, "Providing guaranteed services without per flow management," in *Proc. ACM SIGCOMM*, Aug. 1999, pp. 81–94.

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

[38] M. Adler, "Trade-offs in probabilistic packet marking for IP traceback," *J. ACM*, vol. 52, no. 2, pp. 217–244, 2005.

[39] D. Dean, M. Franklin, and A. Stubblefield, "An algebraic approach to IP traceback," *ACM Trans. Inf. Syst. Security*, vol. 5, no. 2, pp. 119–137, 2002.

[40] A. C. Snoeren, C. Partridge, L. A. Sanchez, C. E. Jones, F. Tchakountio, B. Schwartz, S. T. Kent, and W. T. Strayer, "Single-packet IP traceback," *IEEE/ACM Trans. Netw.*, vol. 10, no. 6, pp. 721–734, 2002.

[41] CAIDA. (2016). The CAIDA IPv4 Routed /24 Topology Dataset - April 9, 2012 and May 19, 2013. [Online]. Available: http://www.caida.org/data/active/ipv4_routed_24_topology_dataset.xml

[42] S. McClure, S. Shah, and S. Shah, *Web hacking: Attacks and defense*. Addison-Wesley Longman Publishing Co., Inc., 2002.

[43] B. Parno *et al.*, "Portcullis: Protecting connection setup from denial-of-capability attacks," in *Proc. ACM SIGCOMM*, Aug. 2007, pp. 289–300.

[44] CAIDA. (2014). The CAIDA UCSD Macroscopic Topology Dataset. [Online]. Available: http://www.caida.org/tools/measurement/skitter/

[45] B. Liu, J. Bi, and Y. Zhu, "A deployable approach for inter-AS anti-spoofing," in *Proc. IEEE ICNP*. IEEE, 2011, pp. 19–24.

[46] H. An, H. Lee, and A. Perrig, "UAS: Universal anti-spoofing by incorporating existing mechanisms," in *Proc. IEEE LCN*, 2013, pp. 448–451.

Hyok An earned his Bachelor of Science in Engineering degree at Kumoh National Institute of Technology (KIT) at Gumi, Republic of Korea in 2007. He was the recipient of "very best" awards twice at KIT in 2006. He worked at Saehan Information Systems as an Assistant Researcher from 2006 to 2010. In 2010, he joined the integrated master-doctoral program in Computer Science at Korea University at Seoul. He is a member of the Computer and Communication Security Lab supervised by Dr. Heejo Lee. He was as Visiting Researcher at Saisei Networks in Sunnyvale, CA, USA in January-February, 2014 and 2015, and at the Network Security Group of the Swiss Federal Institute of Technology (ETH) in Zurich in February-March, 2016.

Heejo Lee is a Professor in the Department of Computer Science and Engineering, Korea University, Seoul, Korea. Before joining Korea University, he was at AhnLab, Inc. as the CTO from 2001 to 2003. From 2000 to 2001, he was a Post-doctorate Researcher at CERIAS Purdue University. In 2010, he was a visiting professor at CyLab/CMU. Dr. Lee received his B.S., M.S., and Ph.D. degree in Computer Science and Engineering from POSTECH, Pohang, Korea. Dr. Lee serves as an Editor of the Journal of Communications and Networks, and the International Journal of Network Management. He has been working on the consultation of the cyber security in the Philippines (2006), Uzbekistan (2007), Vietnam (2009), Myanmar (2011), Costa Rica (2013) and Cambodia (2015). He is a recipient of the ISC^2 ISLA award of community service star in 2016.

Adrian Perrig is a Professor of Computer Science at the Department of Computer Science at the Swiss Federal Institute of Technology (ETH) in Zurich, where he leads the network security group. From 2002 to 2012, he was a Professor of Electrical and Computer Engineering, Engineering and Public Policy, and Computer Science (courtesy) at Carnegie Mellon University. He served as the Technical Director for Carnegie Mellon's Cybersecurity Laboratory (CyLab). He earned his Ph.D. degree in Computer Science from Carnegie Mellon University under the guidance of J. D. Tygar, and spent three years during his Ph.D. degree at the University of California at Berkeley. He received his B.Sc. degree in Computer Engineering from the Swiss Federal Institute of Technology in Lausanne (EPFL). He is a recipient of the NSF CAREER award in 2004, IBM Faculty Fellowships in 2004 and 2005, the Sloan Research Fellowship in 2006, the Security 7 award in the category of education by Information Security Magazine in 2009, the Benjamin Richard Teare teaching award in 2011, and the ACM SIGSAC Outstanding Innovation Award in 2013. His research revolves around building secure systems-in particular secure future Internet architectures.