UAS: Universal Anti-Spoofing by Incorporating Existing Mechanisms

Hyok An and Heejo Lee
Div. of Computer and Communication Engineering
Korea University
Seoul, Korea
Email: {anhyok, heejo}@korea.ac.kr

Adrian Perrig
Institute of Information Security
ETH Zurich
Zurich, Switzerland
Email: adrian.perrig@inf.ethz.ch

***Abstract*—IP spoofing is attractive to amplify network attacks and to provide anonymity. Many approaches have to prevent IP spoofing attacks; however, they do not address a significant deployment issue: filtering inefficiency caused by lack of incentives for early adopters. Practically, no mechanism has been widely deployed and none successfully blocks IP spoofing attacks. 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 ascertains whether a packet is spoofed or not, and inscribes this information in the packet header. The edge routers at a victim network can estimate the forgery of a packet based on the information sent by the upstream routers. The results of experiments conducted with Internet topologies indicate that UAS reduces false alarms up to 84.5% compared to cases where each mechanism operates separately. Our evaluation shows that incorporating multiple anti-spoofing mechanisms reduces false alarms significantly.**

***Index Terms*—Network security; IP spoofing prevention; packet marking; packet filtering; DDoS attacks.**

I. Introduction

Attackers exploit IP spoofing to forge IP address in order to be untraceable. Since anonymity is guaranteed, attackers can bypass source-based filtering and defeat resource-allocation mechanisms [5]. Recently, distributed denial-of-service (DDoS) and distributed reflection denial-of-service (DRDoS) [6] attacks utilized spoofed packets to obfuscate bots and to amplify the attack traffic. A massive DRDoS attack using DNS was launched against Spamhaus in March 19, 2013, peaking at 300 Gbps [7]. New types of attacks such as DNS amplification attacks, in-window-TCP-reset, and spam filter circumvention attacks are launched using IP spoofing [3].

Although many approaches against IP spoofing attacks have been proposed, no single anti-spoofing mechanism has been widely deployed on the Internet. For example, ingress filtering [4], reverse path forwarding (RPF) [2], and distributed packet filtering (DPF) [8] do not provide incentives for early adopters. RPF works properly only for a specific network environment, i.e., symmetric routing path. Moreover, autonomous systems (ASes) operate their own mechanisms and policies independently from other ASes. Such practical issues result in filtering inefficiency and limited effectiveness against IP spoofing attacks. Hence we believe that if the existing anti-spoofing mechanisms that operate independently, can be integrated into a new one with a higher deployment ratio, the anti-spoofing efficacy will be substantially improved.

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 decision. Intermediate routers, operating a single anti-spoofing mechanism, inscribe a mark in the IP header, indicating whether they consider the packet spoofed or not. Edge routers at a victim network receive a packet with marks, which will be converted into a numeric value, called Comprehensive Value (CV), and compare it with a predefined threshold for filtering.

In experiments using four existing mechanisms, with 25% deployment of the overall network, we found that false alarms were reduced by 72.9% compared to the cases in which each mechanism operated separately. Furthermore, in one of these experiments, false alarms were reduced by 84.5%. The contributions of our work are twofold:

1) UAS provides a platform to incorporate existing anti-spoofing mechanisms. It includes not only existing mechanisms, but also new mechanisms considering UAS.
2) UAS reduces false alarms more effectively compared to the independent operation of the anti-spoofing mechanisms for the same deployment ratio.

II. Problem Statement

We can model the Internet as three groups of networks: source network, intermediate network, and victim network. The source network has a legitimate user and an attacker, both sending packets to the victim network through the intermediate network. The legitimate user sends the target server a packet that has source IP address. The attacker sends a packet through the intermediate network to the victim. These packets have a spoofed source IP address of the legitimate user and the destination IP address of the victim. Although the attacker sends spoofed packets, the victim cannot recognize that packets are spoofed.

In order to hinder IP spoofing attacks, many anti-spoofing mechanisms have been proposed and utilized. However, each mechanism has limitations that hinder its widespread deployment on the Internet. The lack of solutions to solve the filtering inefficiency problems makes network administrators reluctant to deploy such anti-spoofing solutions. Since it is not feasible to widely deploy a single mechanism, we consider an alternative approach. We suggest a universal anti-spoofing mechanism that incorporates existing mechanisms. The essential considerations follow:

- The performance of the universal anti-spoofing approach depends on the performance of the individual mechanisms and we derive a sum of the filtering strength.
- The proposed solution has to ensure proper operation of each mechanism and to deal with peculiar situations that arise because of the interactions.

To achieve these aims, the proposed approach treats the decision of each mechanism as an opinion and the accumulated

978-1-4799-0537-9/13/$31.00 ©2013 IEEE

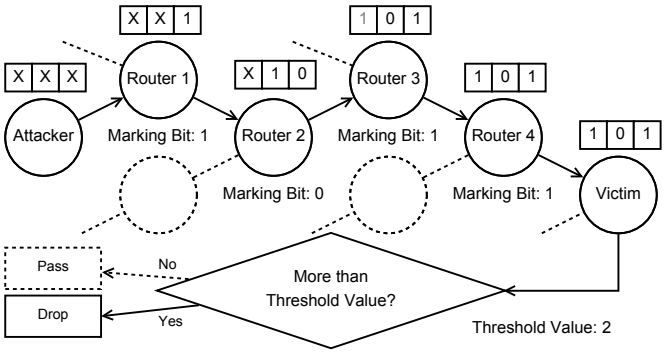


Fig. 1. An example of the UAS operation between an attacker and a victim. Each router from Router 1 to Router 4 marks its own decision in the form of a marking bit. In this example, we show the value in a three-bit marking field.

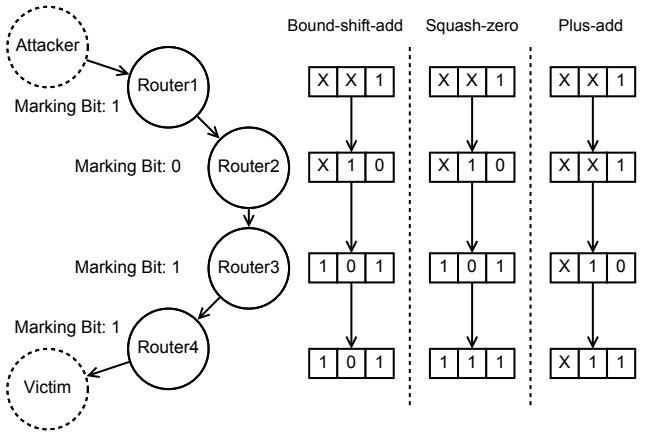


Fig. 2. An example of marking operations in the intermediate network. The packet travels from the attacker to the victim across the routers 1 to 4. Each router marks its own decision in the form of a marking bit.

opinions are used for decision-making. Our goal is to combine individually operating anti-spoofing mechanisms into one and to derive one universal performance result.

III. Mechanism Description

In this section, we explain the operations of UAS and discuss the limitations of a marking field.

A. Mechanism Overview

UAS incorporates the anti-spoofing mechanisms by overall considering. This approach is able to support not only existing but also future mechanisms that adhere to our minimum requirements. Traditionally each prevention mechanism drops packets that are determined as spoofed. Individual mechanisms should not be allowed to decide about dropping packets, and hence such decisions should be treated as opinions. These opinions will be collated to derive a comprehensive assessment about dropping packets or not. Thus, our first requirement is that the deployed prevention mechanisms record their decision as to whether a packet has been spoofed or not in the received packets. Our second requirement is that the packets carry the opinions by all the deployed mechanisms to the victim network. Finally, the opinions in the received packets are used to make a decision as to whether to drop or not according to a predefined threshold value. There are two operational steps that are carried out to achieve this goal in UAS: marking and filtering. Fig. 1 depicts the operations in case of a three-bit marking field value. It is 1 for a spoofed packed and 0 otherwise.

B. Marking Field

The marking field is used to collect opinions of deployed mechanisms and to allow comprehensive decision-making. The identification field of the IP packet header is a marking field candidate for the deployed mechanisms on the routers. This 16-bit field is used by many mechanisms because it is rarely used on the Internet. Savage et al. [10], [11] first argued that the IP identification field is a suitable candidate for this use because it is used only for packet fragmentation, which constitutes less than 0.25% of the packets on the Internet [12].

In cases where the network path length is *less than 16* hops, the marking information can be recorded completely. On the other hand, in cases where it is *more than 16* hops, given the limitation of the 16 bits, we have to find other ways to make it work properly. Hence, marking operations need to consider the limitations of the length of the marking field.

C. Marking Operations

There are three possible marking operations: bounded-shift-add, squash-zero, and plus-one. Fig. 2 depicts these operations with a three-bit marking field.

1) **Bound-shift-add** shifts and adds a marking value (f_i) to the marking field that is n-bits. Marking stops if the routing path is more than n-hops. It means that the most-significant-bit (MSB) of the marking field equals to the 1.

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

2) **Squash-zero** operates similar to Bound-shift-add. It removes a legitimate packet mark and adds a spoofed packet mark if the routing path is more than n-hops. k is an index of the high-order legitimate bit ($1 \leq k \leq n$).

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

3) **Plus-one** adds a marking value to the marking field.

$$m_i = m_{i-1} + f_i \qquad (3)$$

After these operations of the intermediate network, the marking value of the packets that is raw data, needs to be processed for comprehensive assessment.

D. Filtering Operations

Fig. 3 depicts the filtering operations that use the marking values to decide whether the packets are spoofed. When an edge router at a victim network receives the marked packets, it calculates a Comprehensive Value (CV), and compares it with a pre-defined threshold. A higher CV value translates into a higher spoofing possibility. At the victim network, packets are dropped based on the CV calculated from the marking of each packet and the threshold value of the victim network. There are two possible filtering operations to compute a CV from a marking value. First Influence Decision-making (FID) and Host-near Qualified Majority Decision-making (HQMD).

The marked value is binary data, which can be converted to a decimal value and compared with the threshold. This is FID. In this approach, the early marked bit has always higher weight than the sum of the other bits because the weight of each bit is 2^n ($2^q > \sum_{k=0}^{q-1}(2^k \times m_k), 0 < q \leq n$), meaning that the results of filtering operations with FID are dependent on early

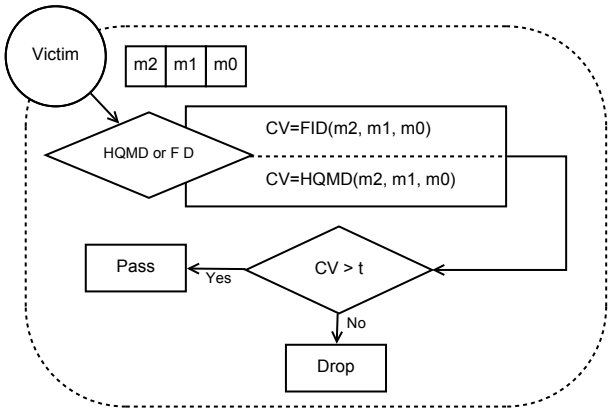


Fig. 3. The filtering operations of the victim network. When on edge router of the victim network receives the marked packets, it calculates a CV, and compares it with a pre-defined threshold (t).

marking. The marked value close to the attacker is likely to be correct but it is not majority rule. HQMD reduces the weight of each bit from 2^n to n, and it is sufficient to overturn the results by the sum of lower bits to remedy that defect of FID (q can be less than $\sum_{k=0}^{q-1}\{(k+1)\times m_k\}, 0 < q \leq n$). Another way to overturn the results is to assign the weight of every bit to 1, but this is unnecessary because Plus-one is able to operate likewise.

1) **FID** uses a binary-coded (2^n-weight-coded) decimal notation to make early marking have a higher impact on the result.

$$CV = \sum_{k=0}^{n-1}(2^k \times m_k) \tag{4}$$

2) **HQMD** uses n-weight-coded decimal notation to make a decision to overturn the result by lower bits.

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

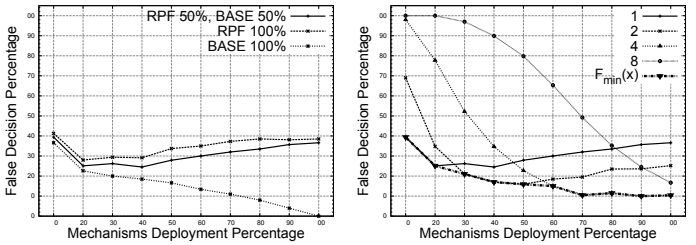
We have to define how to evaluate the performance in terms of false positives and false negatives, and to show that UAS is sufficient to incorporate existing mechanisms.

IV. Evaluation and Discussion

In this section, we evaluate the performance of UAS by means of a simulation program using Internet topologies and four anti-spoofing mechanisms: ingress filtering [4], RPF [2], DPF [8], and BGP Anti-Spoofing Extension (BASE) [5]. We modified the simulation program by Parno et al. [9] to adopt UAS. The Internet topology used in the simulation was derived from CAIDA Skitter [1] probe results, which depict a router-level topology. The Skitter map is a rooted tree and we used a 3,000-node map. A randomly chosen end node sent packets to the root node at a rate of 20,000 packets per unit time.

A. Definition of Performance Basis

In order to evaluate and compare the performance of the mechanisms, a performance basis was established. False positives and false negatives are misjudgments made by a prevention mechanism when it determines whether the received packets are spoofed or not. It means that prevention mechanisms should try to reduce misjudgment as much as possible.



(a) Without UAS (b) With UAS using Plus-one and FID

Fig. 4. Dual scheme (RPF and BASE): Sum of FP and FN.

For instance, given a scenario in which two mechanisms, α and β, try to prevent IP spoofing; if the mechanism α gives less false positives than β, then α can be considered to be better than β. However, if α gives higher false negatives than β, it is difficult to make a decision which mechanism is better. The importance of false positives and false negatives depend on the situation. This means that we need to determine the performance by considering both false positives and false negatives. Thus, we consider that false positives and false negatives are equally important.

1) False decision percentage function:

$$F_t(x) = FP_t(x) + FN_t(x) \tag{6}$$

$F_t(x)$ is the sum of false positive percentage ($FP_t(x)$) and false negative percentage ($FN_t(x)$), where t is the threshold value belonging to $T = \{t \mid t > 0\}$ and x is the deployment percentage belonging to $R = \{x \mid x > 0 \; and \; x <= 100\}$. If we assume that the weight of false positives is equal to the weight of false negatives, the amount of misjudgment when the deployment percentage is x, can be defined by Eq. (6). $F_1(x)$ means not only that the threshold value is 1 in UAS, but also that the result is the same as with the original behavior of the deployed mechanisms running separately on the network because the result is the same with that of filtering using only the first prevention mechanism.

2) False decision for threshold value t:

$$S_t = \sum_{x \in R} F_t(x) \tag{7}$$

S_t is the sum of $F_t(x)$ for a given threshold value t, where the deployment percentage belongs to R. Thus, it shows the overall amount of misjudgment by the prevention mechanisms on the network when the threshold value is t.

3) Minimized false decision:

$$F_{min}(x) = \min_t F_t(x) \tag{8}$$

$$S_{min} = \sum_{x \in R} F_{min}(x) \tag{9}$$

S_{min} is the sum of minimum $F_t(x)$, where t belongs to the T that makes the least result for x. For instance, let $R = \{k, l\}$ and $k < l$. $F_m(k)$ 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.

TABLE I
15 PROPORTIONAL SETS 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	0%	34%	33%	33%
13	34%	0 %	33%	33%
14	34%	33%	0%	33%
15	34%	33%	33%	0%

B. Dual Scheme

In our simulation, in order to compare the performance of marking methods in the limitations of the length of the marking field, we assumed that the marking bit was four bits. $R = \{x \mid x = 10, 20, 30, ..., 90, 100\}$ and $T = \{t \mid t = 2^n,\ n = 0, 1, 2, 3\}$.

Fig. 4 shows the sum of false positive percentage and false negative percentage of a dual scheme (50%:50%) with RPF and BASE. In Fig. 4(b), the result shows $F_t(x)$, $t \in T = \{2^0 = 1,\ \ 2^1 = 2,\ \ 2^2 = 4,\ \ 2^3 = 8\}$, which are the results for a given x and a threshold value t. $F_1(x)$ shows the result without UAS.

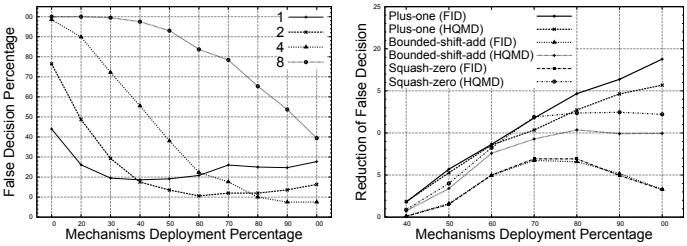
Fig. 4(a) shows that there is an increase in the number of false decisions due to an interference phenomenon in the dual scheme. The result of RPF 50% and BASE 50% begins to falter or rise as the deployment percentage increases. Fig. 4(a) indicates that increasing deployment can impair results. Their misjudgment restricts the growth potential of each other.

However, Fig. 4(b) shows that UAS is able to mitigate the interferences to reduce false decisions in the case of the dual scheme. As can be seen, $F_{min}(x)$ is less than $F_1(x)$. S_1 is 310.9 and S_{min} is 175.8. This indicates a decrease of 43.5% using UAS.

C. Mixed Scheme

We evaluated the performance of UAS using 15 proportional sets of mechanisms using four mechanisms for a mixed scheme as shown in Table I. Fig. 5(a) shows the results of one of the experiments. S_1 is 251.5, while S_{min} is 168.2 which indicates a decrease of 33.1%.

Fig. 5(b) is the average reduction of false decisions, which shows that Plus-add and FID help to achieve the best efficiency. With UAS, if each mechanism is deployed only on 25% of a network, the number of false decisions made by those mechanisms is reduced by 72.9% and the sum of false decisions is reduced by 33.1% compared to the case in which each mechanism operates separately. Furthermore, false decision rate was found to have been reduced up to 84.5% in the case of ingress filtering 10%, RPF 40%, DPF 40% and BASE 10% using Plus-one and FID. The decrease signifies that our proposed mechanism greatly reduces false alarms by incorporating multiple schemes.



(a) Sum of FP and FN (b) Reduction of false decision

Fig. 5. Mixed Scheme: (a) IF 25%, RPF 25%, DPF 25%, and BASE 25% using Plus-one and FID. (b) Performance of UAS in 15 proportional sets.

V. CONCLUSION

In this paper, we proposed a novel scheme that integrates existing, possibly already deployed, anti-spoofing mechanisms. Although there are many schemes to prevent IP spoofing, they have not achieved widespread deployment. In proposed mechanism, existing anti-spoofing mechanisms with marking and filtering according to a pre-defined threshold value enables each mechanism to be integrated with others and work in synergy to reduce false alarms greatly.

ACKNOWLEDGMENT

This research was funded by the MSIP(Ministry of Science, ICT & Future Planning), Korea in the ICT R&D Program 2013 and supported by the Public welfare & Safety research program through the National Research Foundation of Korea(NRF) funded by the Ministry of Science, ICT & Future Planning (NRF-2012M3A2A1051118).

REFERENCES

[1] "The CAIDA UCSD macroscopic topology dataset," http://www.caida.org/tools/measurement/skitter/, 2013.
[2] F. Baker and P. Savola, "Ingress filtering for multihomed networks," RFC 3704, 2004.
[3] R. Beverly, A. Berger, Y. Hyun *et al.*, "Understanding the efficacy of deployed internet source address validation filtering," *9th ACM SIGCOMM IMC*, pp. 356–369, 2009.
[4] P. Ferguson and D. Senie, "Network ingress filtering: Defeating denial of service attacks which employ IP source address spoofing," *Internet Request for Comments*, 2000.
[5] H. Lee, M. Kwon, G. Hasker, and A. Perrig, "BASE: An incrementally deployable mechanism for viable IP spoofing prevention," *the 2nd ACM symposium on information, computer and communications security*, pp. 20–31, 2007.
[6] A. Mangla, "Distributed reflection denial of service: A bandwidth attack," http://palpapers.plynt.com/issues/2006Apr/ddos-reflection/, 2006.
[7] J. Markoff and N. Perlroth, "Firm is accused of sending spam, and fight jams internet," http://www.nytimes.com/2013/03/27/technology/internet/online-dispute-becomes-internet-snarling-attack.html?smid=pl-share, The New York Times, March 2013.
[8] K. Park and H. Lee, "On the effectiveness of route-based packet filtering for distributed dos attack prevention in power-law internets," *ACM SIGCOMM*, 2001.
[9] B. Parno, D. Wendlandt, E. Shi, A. Perrig, B. Maggs, and Y.-C. Hu, "Portcullis: Protecting connection setup from denial-of-capability attacks," *ACM SIGCOMM*, 2007.
[10] S. Savage, D. Wetherall, A. Karlin, and T. Anderson, "Practical network support for IP traceback," *ACM SIGCOMM*, 2000.
[11] ——, "Network support for IP traceback," *IEEE/ACM Transactions on Networking*, vol. 9, no. 3, pp. 226–237, 2001.
[12] I. Stoica and H. Zhang, "Providing guaranteed services without per flow management," *ACM SIGCOMM*, vol. 29, 1999.
[13] A. Yaar, A. Perrig, and D. Song, "Pi: A path identification mechanism to defend against ddos attacks," *the 2003 IEEE Symposium on Security and Privacy*, p. 93, 2003.