Fine-Grained Intra-domain Bandwidth Allocation Against DDoS Attack

Lijia Xie[1,2,3], Shuang Zhao[4], Xiao Zhang[1,2,3(✉)], Yiming Shi[1,2,3], Xin Xiao[1,2,3], and Zhiming Zheng[1,2,3]

[1] LMIB and School of Mathematical Sciences, Beihang University, Beijing, China
{xielijia,xiao.zh,ymshi,xinxiao}@buaa.edu.cn, zzheng@pku.edu.cn
[2] Peng Cheng Laboratory, Shenzhen, China
[3] Beijing Advanced Innovation Center for Big Data and Brain Computing, Beihang University, Beijing, China
[4] China Academy of Information and Communications Technology, Beijing, China
zhaoshuang@caict.ac.cn

Abstract. Multiple bandwidth reservation mechanisms based on network capability have been proposed to resolve Distributed Denial of Service (DDoS) attacks towards the transit-link. However, previous capability-based techniques are insufficient to provide accurate protection towards legitimate users of contaminated domains. In this paper, we present FIBA, an intra-domain bandwidth allocation mechanism with fine-grained accessing control granularity. FIBA enables source domains to locally differentiate the capability requests by state measuring according to two attributing factors. Moreover, FIBA can establish hierarchical channels for capability requesting packets to realize the isolation of traffic from the same source domain. Our scheme is integrated with existing methods and can be optionally deployed by source domains. Finally, through network experiments, we evaluate FIBA can realize user-level DDoS protection even in 90%-contaminated domain.

Keywords: DDoS attack · Network capability · Fine-grained · Intra-domain · Bandwidth allocation

1 Introduction

A recent Neustar report (2020) [5] pointedly indicates that Distributed Denial of Service (DDoS) attacks, as a menace of network availability, are becoming increasingly intense and sophisticated. As the rapidly rising of attacking volume (up to 2.3 Tbps [4]) of transit-link flooding attack (e.g., coremelt and crossfire attack [14,24]), how to avoid target network infrastructure collapsing has been a significant challenge. To mitigate a large-scale volumetric DDoS attack, researchers are actively exploring capability-based resource reservation mechanisms [7,28–32] to manage an effective admission control of transit-link.

An important issue is to select the *allocating granularity*. The *network capability*, which is constituted of a series of authentication tokens, enables legitimate

J. Garcia-Alfaro et al. (Eds.): SecureComm 2021, LNICST 398, pp. 399–417, 2021.
https://doi.org/10.1007/978-3-030-90019-9_20

pairs of end hosts to acquire a guaranteed accessing admission of prioritized bandwidth. In this way, DDoS prevention is realized through capability-based bandwidth allocation by degrading the malicious flows. However, massive attackers may send traffic to flood the capability-setup channel to prevent the legitimate pairs from obtaining capability, namely Denial of Capability (DoC) attacks. Fair resource allocation using granularity such as per-flow [28], per-user [29] is inadvisable, resulting in tragedy of the network-link commons [7]. Thus, recent approaches adopt Autonomous System (AS) as the allocating granularity to confine attacking effects in the source domain.

Several fine-grained inter-domain allocating techniques [30–32] aim to priovide differential bandwidth guarantees among heterogeneous ASes by domain characterizing. Tumbler [31] considers utilization and reputation to compute the allocation. D4 [32] employs a state-defined reservation by adding popularity and locality aspects. STBA [30] introduces the spreader metric to protect influential ASes. Nonetheless, the above domain-level bandwidth gurantee is necessary to protect legitimate ASes, but are insufficient to protect legitimate users within contaminated source ASes. Moreover, uncontaminated source ASes also needs differential accessing control to the internal users. To explain in more detail, if a source AS locally allocate resources to their internal end hosts by simple per-client fair sharing, it will lead to:

- inadequate protection to *legitimate users* (complying with the allocation) located in the same source AS with *attackers* (over-requesting/over-using) in an attacking scenario;
- unreasonable allocation between *active users* (with high bandwidth demand) and *ordinary users* (with medium bandwidth demand) in a normal scenario.

In this paper, we present FIBA, a fine-grained intra-domain bandwidth allocation mechanism with user-level DDoS resistance. The key insight of FIBA is to manage differential accessing control of network capability to intra-domain users by *state measurement* and *hierarchical channels*. Upon the domain-level allocation, source ASes locally perform the traffic control to their internal bandwidth-requesting entities. First, FIBA leverages the *allocating index* to quantitatively measure the state of each capability request to determine the accessing priority. Thus, we combine two key attributing factors to enforce the compution the allocating index according to the topological effects and traffic features, namely (1) centrality factor, and (2) legitimacy factor. The legitimate request from an active user tends to obtain a larger allocating index and vice versa. Based on the attributing factors, the source ASes maintain the periodical renewal of allocating index for each request. Then, FIBA enables transit ASes to build hierarchical channels for the multi-state capability requests by unspoofable accessing priority tag and weight-customized hierarchical queue. The bandwidth guarantees of legitimate users/attackers and active users/ordinary users can be differentiated due to their diverse allocating indexes. Futhermore, the user-level DDoS protection is realized by intra-domain traffic isolation.

Hereby, we list the main contributions of FIBA as follows.

- We propose FIBA, a novel capability-based DDoS protection that realizes intra-domain state measurement and fine-grained accessing control of capability. By measuring state, FIBA enables each user to obtain reasonable capability accessing priority (Sect. 3.2–3.4).
- Our scheme is built with hierarchical channel to separate multi-state capability requests. Through intra-domain traffic isolation, FIBA is able to provide user-level DDoS resistance upon the domain-level DDoS protection (Sect. 3.5–3.7).
- FIBA is established with existing network methods, protocols and cryptographic algorithms. We demonstrate the effectiveness of FIBA through multiple simulations (Sect. 4).

2 Problem Definition

2.1 Network and Threat Model

In this paper, our aim is to protect legitimate flows against the volumentric transit-link DDoS attack, in which the victim link is traversed by legitimate pairs (source-to-destination) and malicious pairs (bot-to-bot (e.g. Coremelt [24]) or bot-to-server (e.g. Crossfire [14])). Our DDoS prevention is established upon inter-domain capability-based bandwidth allocation [18,30–32], which is another active, but orthogonal problem to this paper.

Compling with the current network architectures, each user is managed by a certain domain (i.e., AS). The distribution of botnets is unlimited to launch the transit-link DDoS attack. In other words, any AS may be contaminated with an arbitrary proportion of malicious bots by sending large amounts of traffic (network capability requests and data packets) to congest the link and prevent legitimate pairs from acquiring bandwidth resource. And the attackers can flood the capability-setup channel or data-transmit channel, which corresponds to DoC attack and DDoS attack, respectively. However, the attack that misbehaving routers intentionally delay/drop packets is out of our scope. Note that the network links may fail, resulting in naturally loss of capability request packets or data packets.

2.2 Assumptions

We make the following assumptions. First, the bandwidth-requesting sources are able to acquire the AS-path to include the inter-domain path in the packet headers, which is feasible by several routing protocols (e.g. BGP [21] and Pathlet routing [11]). Second, every flow can be assigned a unique flow identifier and AS identifier (e.g., IP address [25] and Autonomous System Number (ASN) [1], respectively). Third, multiple approaches can be leveraged to make the flow identifier further non-hijackable [6,12] and the AS identifier further unforgettable [15,27]. In addition, the source AS can utilize traffic features to detect the attacking flows originated from malicious entities [16,26].

2.3 Desired Goals

Under the defined threat model, we specify the desired goals of fine-grained bandwidth reservation mechanism as follows.

- **User-level DDoS resistance.** The scheme should establish hierarchical channels for capability requesting packets to realize the traffic isolation between benign users and misbehaving users, even when they are from the same source AS.
- **Allocating reasonability.** Source domains are able to realize differential local intra-domain bandwidth allocation. Namely, the mechanism should be able to provide differential bandwidth guarantees for active users/ordinary users from a certain source domain.
- **Deployability.** The mechanism is able to be integrated with existing network protocols and cryptographic algorithms.

3 The Design of FIBA

In this section, we first give a overview to introduce the key insight of FIBA. Then we describe FIBA' s design of state measurement in detail. Finally, we present how FIBA processes with allocating index to achieve fine-grained accessing control by establishing hierarchical channels.

3.1 Overview

The overall goal of FIBA is to enforce fine-grained accessing control of network capability. The capability enables legitimate user pairs to acquire a guaranteed accessing admission of prioritized bandwidth. *Fine-grained* means that the source domain can differentially control the accessing priority of capability to its internal users. More specifically, FIBA manages differential accessing control by **state measurement** (in source ASes) and **hierarchical channels** (in transit ASes). Source ASes leverage state measuring to determine the accessing priority and tramit the information to transit ASes. Then thansit ASes can accordingly establish hierarchical channels for multi-state capability requests.

First, to quantitatively measure the state of capability request, source ASes calculate **allocating indexes** for the internal users by making use of two attributing factors: (1) **centrality** factor and (2) **legitimacy** factor. The allocating index describes the priority of accessing the target link. The two factors are related to normal scenario and attacking scenario. In normal scenario, FIBA employs the centrality factor to differentiate active users and ordinary users (Sect. 3.3). In attacking scenario, FIBA employs the legitimacy factor to differentiate legitimate users and attackers (Sect. 3.4). The centrality factor describes the spreading influence of an end host from the aspect of topological effects. The legitimacy factor describes whether the capability requesting flows is malicious from the aspect of traffic features. After the two-factor integration, source ASes are able to compute allocating indexes for every capability requests. Moreover,

requests from the users that behave inactively or illegally will obtain low accessing priority with low allocated indexes. Then, the request packet is attached with an *accessing priority tag* (Sect. 3.5), which indicates the state of capability requests. By carrying the tag, source ASes are able to transmit the preference information to transit ASes.

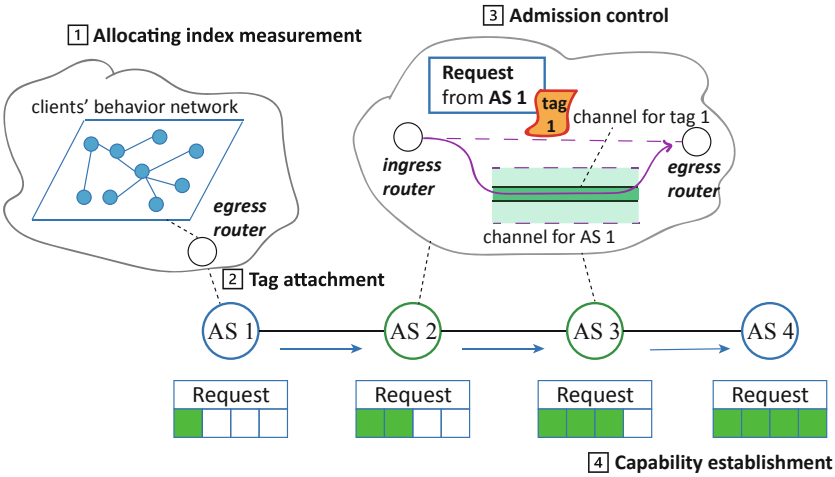

Fig. 1. The overview of FIBA. First, source ASes enforce the allocating index measurement by considering two attributing factors. Second, source ASes (blue) attach a suitable tag for each capability request. Third, transit ASes (green) leverage the hierarchical queue to execute the admission control for capability request. Finally, the capability initiated by bandwidth-requesting client is established hop-by-hop. (Color online figure)

Then, transit ASes establish hierarchical channels for multi-state capability requests. Specifically, transit ASes fair-queue the capability requests from multiple source ASes. Furthermore, according to the accessing priority tag, transit ASes will accordingly fair-queue the capability requests from the same source AS in sub-queues via the tags. The capability requests in different sub-queues are differentially processed. For instance, the sub-queue of requests possessing higher allocating indexes acquires a higher weight. Therefore, the accessing priority of diverse end hosts can be distinguished, even from the same source AS. In this way, transit ASes do not need to maintain allocating index information for every end host, which can greatly reduce storage costs.

Intuitively, the overall process of FIBA is shown as in Fig. 1. Based on aforementioned ideas, the fine-grained accessing control of network capability can be achieved: For each source AS, FIBA aims to establish hierarchical channels during capability establishment to differ the accessing priority for its internal users. Thanks to the state measurement for each capability request, the reasonable allocation is realized from two aspects. On the one hand, each benign user is able to be guaranteed with deserved accessing priority according to its centrality

factor. Namely, the accessing priority of ordinary users is no more than active users from the same source AS. On the other hand, the attacking effects will be confined in the low-priority channel. With low legitimacy factor, attackers cannot compress the accessing priority of active legitimate users possessing high allocating indexes, even from the same source AS. Futhermore, if attackers flood the given link with low-rate attacking flows, FIBA can also confine the attacking effects through low centrality factor. Therefore, fine-grained accessing control of network capability is achieved.

Note that if a user is not satisfied with its accessing priority, the user can send a purchase request of premium service to its AS manager. The additional charge motivates source ASes to deploy FIBA. However, the premium service can only work for the centrality factor, not the legitimacy factor. Besides, if the source AS is weakly supervised and unable to deploy FIBA, transit ASes can also confine the attacking effects in the domain-level channel by deploying inter-domain allocation, not influencing other source ASes.

3.2 State Measurement by Allocating Index

To fine-grained reasonable bandwidth allocation, FIBA leverages the allocating index to numerically measure the state of each capability request. The allocating index is a one-byte parameter with a value between 0 and 255 (which can be extended). Users with a larger allocating index can get better accessing priority of capability.

Specifically, the allocating index (A) is constituted of centrality factor (C) and legitimacy factor (L).

- Centrality factor (C) is an attribute collected from the normal state of the request to represent activeness of the user. We define C as a one-byte parameter between 0 and 255.
- Legitimacy factor (L) is an attribute collected from the attacked state of the request to represent compliance of the user. We define L as a one-byte parameter between 0 and 255.

The combination of the two factors represents the state of capability-requesting packets. Source ASes locally calculate the user-level data packet allocating index for their internal clients based on topological effects from the user and traffic features from the data packet sent by the user. We denote $req_{i,j}$ as the jth capability-requesting packet sent by the user i. The allocating index of $req_{i,j}$ is calculated and updated by the egress router of the source AS where the user is located.

The allocating index reflects the state of each capability request. And the allocating index is utilized to determine the accessing priority levels. We now define the computation of allocating index $A_{i,j}$ of $req_{i,j}$ as:

$$A_{i,j} = \lceil xC_{i,j}^{\alpha} \cdot L_{i,j}^{1-\alpha} + (1-x)A_{i,j-1} \rceil, \tag{1}$$

where $C_{i,j}$ and $L_{i,j}$ are the centrality factor and legitimacy factor of $req_{i,j}$, $A_{i,j-1}$ is allocating index of last request packet $req_{i,j-1}$, and x $(0 < x < 1)$ is a constant

smoothing factor. And α is an adjustable coefficient between 0 and 1. When the centrality and legitimacy factor become smaller, the corresponding allocating index will accordingly become smaller.

Note that users' state is dynamic, resulting in changeable centrality factor and legitimacy factor. Thus, source ASes can periodically update two attributing factors and allocating index. For example, the update period can be set to 30 s by default. According to the allocating index, the state of request packets is quantitatively measured in each source AS. On the basis of allocating index, how to differ the accessing priority of capability request is described with detail in Sect. 3.5 and Sect. 3.6.

3.3 Centrality Factor Calculation

We determine the users' centrality factor according to the *spreading influence* collected from the normal state of the users. The end hosts utilize bandwidth to process information dissemination with each other. The remove of structural nodes (called spreaders) will have a strong impact on information spreading capability in the behavioral network [19]. Thereby, in order to perform reasonable bandwidth allocation, FIBA leverages the thought of spreading influence to estimate the activeness of end hosts. Users with strong spreading influence deserve a greater bandwidth demand, and users with weak spreading influence deserve a smaller bandwidth demand. In FIBA, the allocated bandwidth is proportional to the spreading influence.

Then, the problem is how to efficiently evaluate the spreading influence of end hosts with acceptable computational costs. In information network, multiple centrality approaches are used for topological effects measurement and spreader identification. Inspired by this, we employ the topological characteristics of users to measure the spreading influence. The topological characteristics of users within the AS are different, resulting in different spreading influence of users. Intuitively, users with higher topological centrality will be connected to more users or routers. For the measurement of node users' spreading influence, academia has proposed multiple calculation methods (e.g., degree centrality [9], k-shell centrality [17], betweenness centrality [10]). Among those, several centrality methods are easy-to-compute, yet effective and local, which are suitable for FIBA state measurement. In our simulation, we simply select degree centrality as a measure of the spreading influence (SI_i) of user node i.

To obtain the centrality factor $C_{i,j}$ of $req_{i,j}$, we specify the calculation as:

$$C_{i,j} = \lceil 255 \cdot \frac{SI_i}{max(SI_i)} \rceil, \tag{2}$$

where $max(SI_i)$ is the maximum value SC_i of the users in the source AS where the user is located. Note that the centrality factor computed for the capability-requesting packet sent by the same user i is consistent. Moreover, considering the connections of end hosts in the network can be disconnected and reconnected, the network topology is dynamic and changeable. Source ASes periodically update the centrality factors of users based on the dynamic topology.

Consequently, in FIBA, active users with strong spreading influence can get more bandwidth guarantee than ordinary users, maximizing the information dissemination of behavioral network and ensuring reasonable bandwidth allocation.

3.4 Legitimacy Factor Calculation

We determine the legitimacy factor according to the malicious behavior information collected from the the users. The distribution of bot hosts within the AS is uneven. Previous mechanisms enable the transit ASes to isolate the traffic from uncontaminated ASes and contaminated ASes. Likewise, it is necessary to classify the benign users and attackers within a contaminated AS to guarantee the bandwidth allocation of legitimate users. The goal of legitimacy factor is to control the traffic flooding by limiting the bandwidth allocation of malicious bots. To do this, the packets flow of end hosts are evaluated to determine maliciousness of users. Therefore, FIBA defines the legitimacy factor as a one-byte number to reflect whether the user over-requests or over-uses, namely compliance.

Several detections are proposed to employ traffic features to distinguish the attacking flows from the normal flows [13,16,18,26]. In FIBA, the traffic features of packets are used to observe the abnormality of the data packets and estimate the legitimacy factor. According to those attacking flow identification methods, FIBA extracts five features, namely *packetCount*, *byteCount*, *durationSeconds*, *ipv4_src*, *ipv4_dst*, to distinguish legal packets and malicious packets. Based on these features, the scoring of data packets is achieved [13,16]. And we use $m_{i,j}$ to denote the attacking score obtained by $req_{i,j}$, which is a number between 0 and 1. Misbehaving flows will obtain higher attacking scores than legitimate flows. During a period of time, when data packets pass through the egress router, the egress router will extract the attributes of the data packets to perform statistical analysis. Then the legitimacy factor $L_{i,j}$ of $req_{i,j}$is calculated according to the score as the following.

$$L_{i,j} = \lceil 255 \cdot \frac{1}{m_{i,j}} \rceil. \tag{3}$$

However, the above method may misidentify slight legitimate requests as attacking requests, which is acceptable. Once the users of those flows decreases the request rate, the mistake can be eliminated. Note that statistical analysis is an optional technique here. Source AS can use additional techniques to improve the accuracy of malicious flow identification and we leave it as a future work.

3.5 Accessing Priority Tags

To distinguish the accessing priority of network capability, source ASes attach adaptable tags for the capability requests originated from the internal users. First, according to the allocating indexes, the source AS determines how many types of tags to be set. Note that the distribution of allocating index is non-uniform. Temporally, the internal users of the source ASes maintains dynamic allocating index. Spatially, even in a same source AS, the disparity of centrality

factor and legitimacy factor leads to the heterogeneous allocating index. Hence, FIBA involves the definition of network heterogeneity [23] to termly measure the heterogeneity of allocating index.

$$H(\{A_{i,j}\}) = \frac{\sqrt{Variance(A_{i,j})}}{Average(A_{i,j})}, \tag{4}$$

where $A_{i,j}$ is an array of set $\{A_{i,j}\}$ containing the allocating indexes of capability-requesting flows in the source AS. If the source AS obtains a higher heterogeneity, the number of tags' types will be greater to explicitly differentiate the capability request from various user entities.

Next, the source AS adds a tag t for every capability request to indicate the state according to its allocating index (e.g., $t = 1/2/3$ for low/medium/high accessing priority). The source AS can optionally transform the threshold determination for multi-state tags into an optimization problem[1]. Upon receipt of the tags, how the transit AS differs the accessing priority will be demonstrated in Sect. 3.6. Besides, if the heterogeneity of allocating index is small or the number of capability requests is relatively slight, the source AS can simplify the tag as $t = 0$ for all request flows. And when transit AS receives overmuch capability requests from a source AS, the transit AS will send a *tag-request* to request the source AS for multi-state tags. However, if the source AS refuses to deploy multi-tag, transit ASes can also confine the attacking effects in the domain-level channel by deploying inter-domain allocation, not influencing other source ASes. However, attackers may attempt to modify/replay the accessing priority tags on the path from source AS to transit AS. And we will specify how to prevent the modification/replay attacks in Sect. 3.7.

3.6 Hierarchical Queueing

End hosts initiate capability request to access the guaranteed link. However, attackers can over-request to overwhelm the requests from benign users. In order to prevent attackers from overwhelming legitimate requests, transit ASes establish isolated channel for each source AS. Each capability request is placed into a separate queue whose weight could be adjusted by the transit AS according to its preference. Nonetheless, the attackers can still overwhelm the legitimate requests from the attackers' source AS. The reason is that the benign requests and attacking requests from a certain source AS will share a same queue.

In this way, the source ASes are motivated to control the outgoing traffic to enforce local management. However, rate limiting simply on the egress router of source AS is not advisable. In FIBA, we leverage hierarchical fair-queue [8] to isolate the traffic. We demonstrate the queue management in Fig. 2. Transit ASes queue the packets according to the AS identifier and tag after receiving the

[1] For example, 2-state tag problem is to find an interger number a to minimize $H(\{A_{i,j}|A_{i,j} \leq a\}) + H(\{A_{i,j}|A_{i,j} > a\})$. Also, the source AS can determine by itself.

capability request. The AS identifier and tag are used to identify the first-level queue and second-level queue, respectively. Therefore, if the attackers launch a DoC attack by sending a large number of requests, the misbehaving requests will be put into the sub-queue with low priority due to their low legitimacy factor. While the requests from active benign users are put into sub-queue with high priority, the accessing priority of legitimate users will not be influenced. Based on the hierarchical channel, transit ASes can filter unwanted requests flow according to its capacity. Moreover, transit ASes can adjust the weights of first-level queues and second-level queues and reallocate the unoccupied sub-queues.

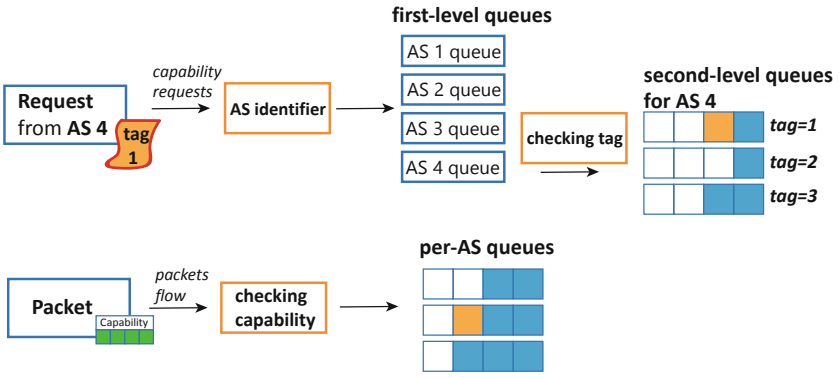

Fig. 2. Queue management at a ingress router of transit ASes. The blue block is occupied by precious packets. The orange block represents the newly added packet. The request from AS 4 with $t = 1$ is added in subqueue of *tag 1* for AS 4 for AS 4. Regular packets with associated capabilities receive preferential forwarding through prioritized per-AS queue. Legacy traffic competes for best-effort bandwidth.

3.7 Capability Requesting

As described in Sect. 3.5, the egress router of a request packet's source AS adds its accessing priority tag into the packet header. Hence, the capability request can be comprised of five components:

$$req = bw \parallel exp \parallel AS\_ID \parallel flow\_id \parallel t. \tag{5}$$

Thereinto, bw is requested bandwidth amount of the user. And exp is expiration time of the requested capability. Then, AS_ID and $flow\_id$, as our assumptions, are the AS identifier and flow identifier, respectively. Besides, t is accessing priority tag of the request according to its allocating index.

However, the basic capability request may be modified or replayed by on-path attackers as in Fig. 3. To solve this problem, the source AS can simply add a digital signature to authenticate the tag. Nonetheless, the per-packet digital signature will incur significant computational overhead. Instead, to counter these attacks, FIBA leverages Message Authentication Code (MAC) as authentication of the requests' tags.

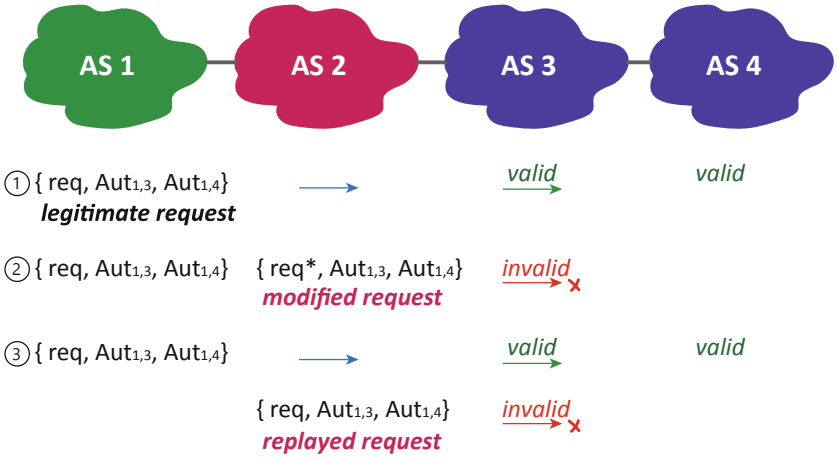

Fig. 3. The authentication process of priority access tags. The clients from *AS* 1 initiates a capability request. *AS* 2 is compromised by attackers, which is able to modify the tag of request or replay a request with high-priority tag. *AS* 3 can authenticate that the initial request from *AS* 1 is valid and the modified/replayed request is invalid.

To construct a unspoofable accessing priority tag, the source AS and the deployed transit AS first establish a shared secret key, which is viable by Diffie-Hellman algorithm. In FIBA, we assume each AS could obtain and authenticate the public keys of other ASes from a trusted certificate authority (e.g., ICANN [22]). In this way, *AS* i can generate a public/private key pair as (a_i, b_i). *AS* i and *AS* j can calculate their shared secret key as $k_{i,j} = a_i^{b_j} = a_j^{b_i}$.

When the source AS sends the request packet, the authentication MAC will be attached in the packet header. And the authentication MAC can be computed with the following equation.

$$Aut_{i,j} = MAC_{k_{i,j}}(req). \tag{6}$$

After receiving the request, transit AS verifies the authentication MAC using the authentication key. Moreover, the generation of authentication MAC includes the expiration time exp to prevent the replay attack. Therefore, the transit AS is able to acquire a unspoofable tag to accurately queue for capability requests.

If the request is approved, the transit AS and the destination AS will compute a cryptographic token to compose the final network capability (similar to [7,30,31]).

$$tok_j = MAC_{k_j}(tok_{j-1} \parallel req), \tag{7}$$

where k_j is the secret key of the *AS* j, and Tok_{j-1} is cryptographic token generated by the last-hop *AS* $j-1$ of *AS* j. The established capability is forwarded back to the end host in source AS. By carrying the capability, the subsequent flows from the client receive preferential forwarding via prioritized bandwidth channel.

4 Evaluation

We evaluate the performance of FIBA using Bene [2] in this section. And we mainly consider two scenarios: (1) both benign clients and attackers compete for bandwidth requesting (attacking); and (2) only legitimate users compete for bandwidth requesting (normal). The attacking scenario is set to verify user-level DDoS resistance. The normal scenario is set to verify allocating reasonability.

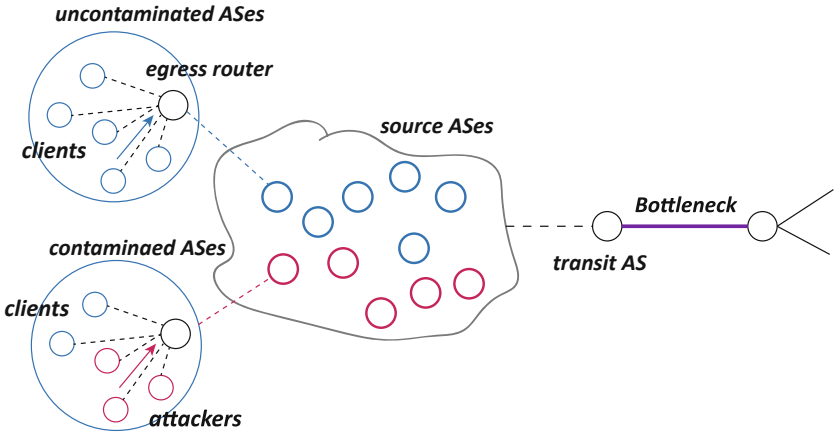

Fig. 4. The network topology of two scenarios.

Without loss of generality, we first demonstrate the network topology of two scenarios as in Fig. 4. We employ a real domain-level network topology from CAIDA AS-relationship dataset [3]. From the constructed topology, we select a link between two high-degree transit ASes as the bottleneck and we randomly select several leaf ASes as the source ASes. The capability request is originated from a certain source AS to request the link access of the bottleneck link. And we consider all source ASes can be deployed with FIBA mechanism. Namely, every source AS is able to measure the allocating index and attach a corresponding tag for the request. The uncontaminated ASes and contaminated ASes are randomly selected from leaf ASes. The end hosts in uncontaminated ASes are all benign users, while the contaminated ASes can include benign clients and attackers simultaneously. And there are 220 end hosts in every source AS.

Besides, we set the coefficient α as 0.2 for each source AS. And the egress routers of source ASes attach *high* tag for packets with allocating index over 128, *low* tag for packets with allocating index less than 108, and *medium* tag for the remaining. In the transit AS, the types of sub-queues is accordingly set as 3: high, medium and low. The weights of three sub-queues is set as 60% for *high* tag queue, 30% for *medium* tag queue and 10% for *low* tag queue. Note that all the aforementioned parameters can be adaptively adjusted. In our experiment, the capacity of bottleneck is set as 9.6 Gbps. Thereinto, 5% of the bandwidth (480

Mbps) is used for capability request. The size of each request packet is fixed as 1 KB. Moreover, in the domain-level, we simply set same share of per-AS bandwidth reservation for multiple source ASes.

4.1 Domain-Level DDoS Resistance

First, we consider the scenario that attackers flood the capability-setup channel by over-requesting the capability. The goal of this experiment is to mainly evaluate the impact of legitimacy factor. In the 10-min simulation, 100 legitimate ASes and 500 contaminated ASes send the bandwidth-requesting packets. And inside the contaminated ASes, there are benign end hosts and attacking end hosts. The number of attackers in each contaminated AS is increasing from 20 to 200. On average, benign users approximately send 1 request per minute, while attackers send 10 requests per second.

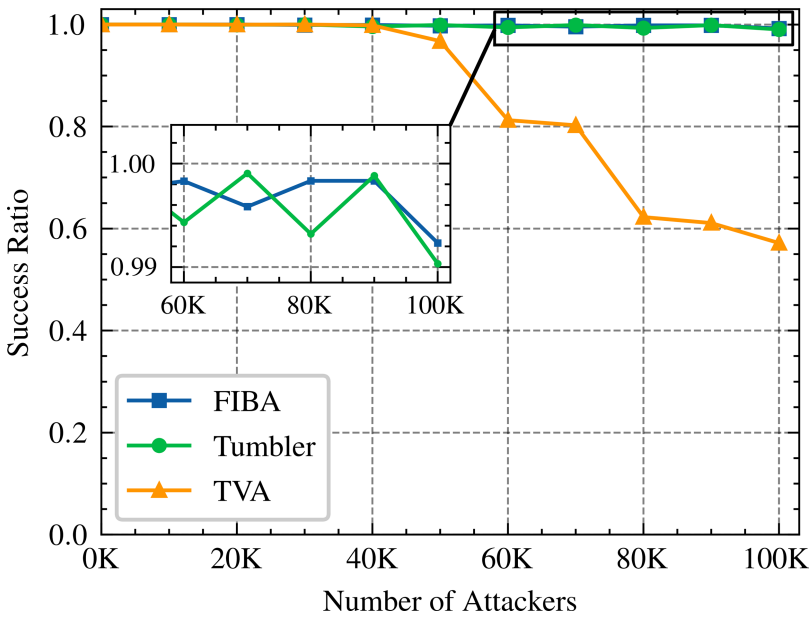

Fig. 5. Comparative simulation results (the average successful ratio of legitimate ASes) for Tumbler, TVA, and FIBA against DoC attack.

According to the above settings, we compare the successful ratio of capability requests from the legitimate ASes with two representative schemes (Tumbler [31] and TVA [29]). Figure 5 presents the change of successful ratio of three approaches. As the number of bots increases, FIBA and Tumbler can maintain the bandwidth guarantee of bottleneck link for legitimate ASes while the curve of TVA witnesses a descent. The slight fluctuation of FIBA and Tumbler is

resulted from naturally loss of packets. Due to a per-AS share strategy, FIBA and Tumbler can establish isolated requesting channels for legitimate ASes. Therefore, even with the explosively increasing of requests from contaminated AS, the requests from the legitimate ASes can be processed by the transit AS.

However, the performance of TVA decreases because of the fair queueing approach based on the path-identifier during the capability establishment. The distances of source ASes are diverse in our simulation. When the path length rises, the requests from remote source ASes will be put into high-level queue. Hence, the link share of remote legitimate ASes is influenced when abundant requests flood the bottleneck. In consequence, FIBA is able to hold the domain-level DDoS resistance.

4.2 User-Level DDoS Resistance

Next, we evaluate the performance of FIBA in user-level DDoS resistance and we focus on the internal allocation in a contaminated AS in FIBA. According to aforementioned experimental settings, we compare the success ratios of legitimate users and attackers in the contaminated ASes and success ratios of uncontaminated ASes.

As observed from Fig. 7, only the success ratio of attackers are decreasing. The dash line indicates the success ratio of legitimate users from contaminated AS in simple per-client fair sharing scheme. Hence, in simple per-client fair sharing scheme, legitimate users from contaminated AS are influenced by attackers. However, FIBA, the curves of legitimate users from both contaminated ASes and uncontaminated ASes are almost 1, while the curve of legitimate users from contaminated AS is marginally lower than uncontaminated AS. The benign users in uncontaminated AS can establish capability with the help of isolated channel for its source AS. And FIBA hierarchical channels contributes to independent channels for benign users in contaminated AS, confining the attacking effects in the *low* tag channel.

To give an intuitive demonstration, we present the distribution of end hosts of source ASes in Fig. 6. The histogram represents the number of different allocating index of users. The curve indicates the Cumulative Distribution Function (CDF) of allocating index in uncontaminated ASes and contaminated ASes. From the Fig. 6, we can observe the dynamic change of clients' distribution as the proportion of attackers increases. Besides, due to the legitimacy factor, almost all of requests from attackers are attached with *low* tags.

Thereby, even in a 90%-contaminated AS, the legitimate users can be identified and guaranteed with deserved bandwidth. Meanwhile, the misbehaving users are controlled by limiting the success ratio (down to about 50%) of over-requesting packets. In a nutshell, FIBA performs the user-level DDoS resistance upon domain-level DDoS resistance by achieving the traffic isolation between legitimate users and attackers from a source AS.

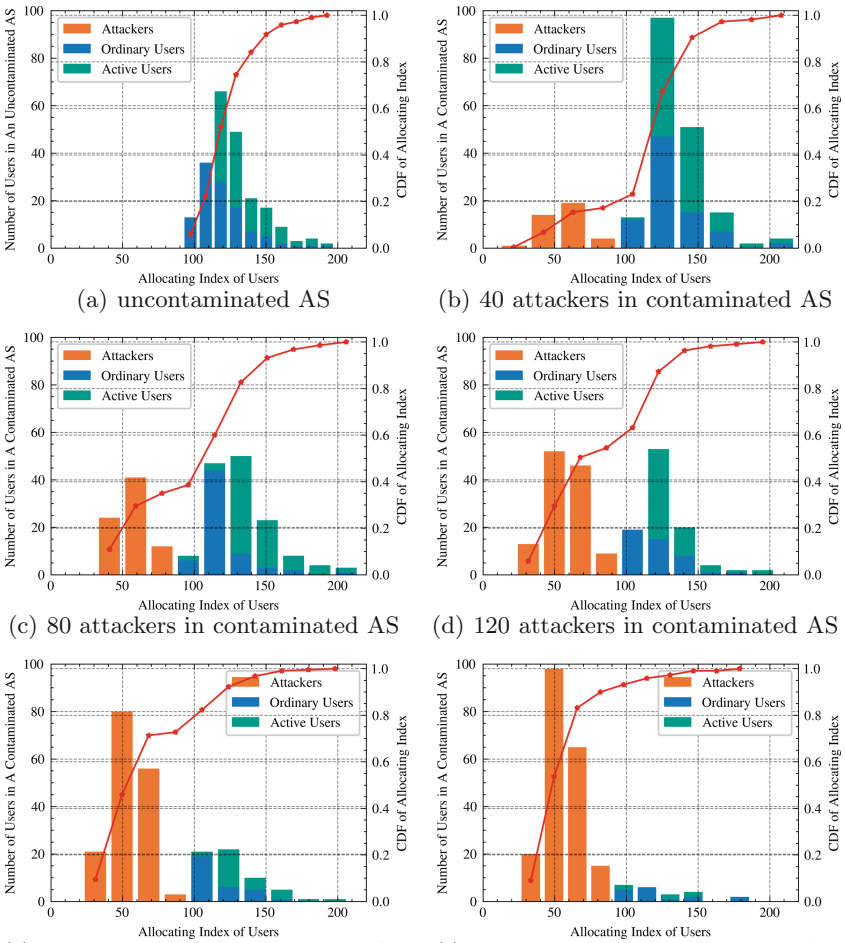

Fig. 6. The allocating index distribution of end hosts in source ASes. The blue and green histogram represents for benign users (ordinary users and active users), and the orange histogram represents for attackers. (Color figure online)

4.3 Allocating Reasonability

In this experiment, we then evaluate that FIBA can allocate different share for diverse legitimate users to realize reasonable bandwidth guarantee. We randomly select 1000 leaf ASes as the source ASes to send the capability request. According to above settings, the source AS divide the legitimate users into *high* tag (active users) and *medium* tag (ordinary users). Per-user sending rate of capability request ranges from 2 packet/s to 10 packet/s. We observe the average successful ratio of capability requesting in 10-min experiment.

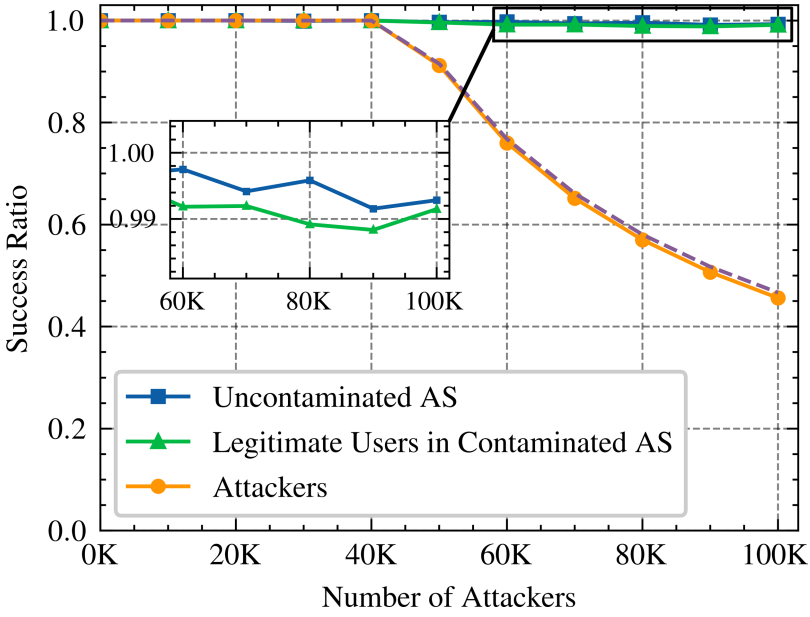

Fig. 7. The average successful ratio of the end hosts from source ASes of FIBA in an attacking scenario.

In Fig. 8, as with the increasing of number of the capability request packets, the successful ratios of both tags' requests witness a decline trend. The dash line is the average successful ratio in per-client fair sharing scheme. The curve of high-tag is consistently higher than the curve of medium-tag, which indicates the requests in high-queue obtain more bandwidth guarantee. Thus, if the end hosts from a legitimate AS maintain prioritized bandwidth demand for capability, the transit AS tends to preferentially process the request from active users with high centrality factor. In addition, as in Fig. 6 (blue and green histogram), the contaminated AS can also perform differential accessing control for legitimate users. Thereby, FIBA can achieve reasonable allocation by providing differential local intra-domain bandwidth guarantees for active users and ordinary users.

5 Related Work

To mitigate DDoS attack, the concept of network capability was proposed, which is an access authentication token related to the access authority. The packets with associated capabilities can transmit data with high priority. With this method, capability-based mechanisms can protect the normal access of legitimate traffic.

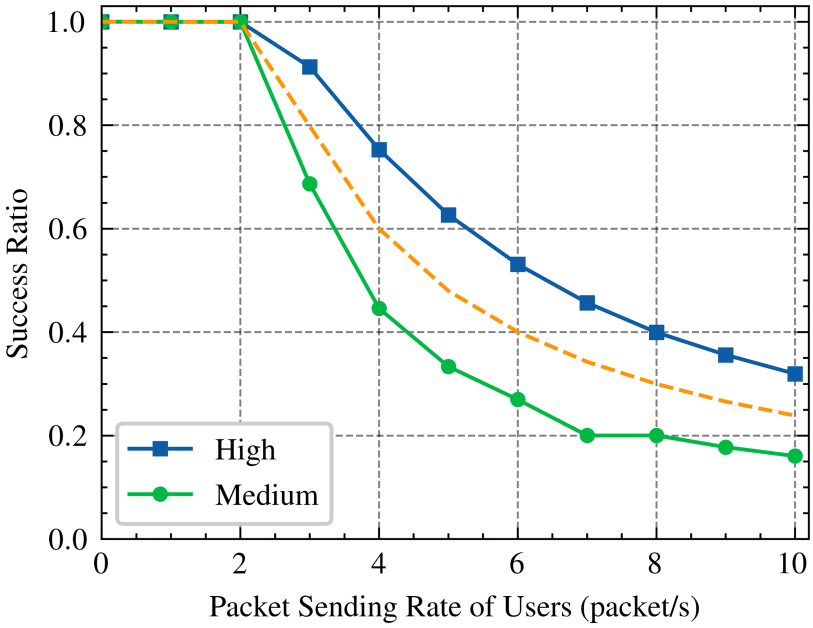

Fig. 8. The average successful ratio of the legitimate end hosts in a normal scenario.

An important part of the capability-based DDoS defense scheme is the research from the perspective of granularity (per-user [29], per-flow [28], per-computation [20], and per-AS [7,18,30,31]). SIFF [28] issues capability in per-flow granularity, and monitors the status of each flow to block or allow issuance. TVA [29] uses WF^2Q+ to process the queues hierarchically, and uses specific routers on the ingress interface to receive and forward traffic with different priority traffic. Portcullis [20] employs proof-of-work to achieve per-computation granularity allocation. Floc [18] differentiates between legitimate and attack flows for a target link. However, Floc is too coarse-grained to differentiate low-rate attacking flows and DoC attack is not considered. SIBRA [7] prioritizes bandwidth to achieve fair bandwidth allocation. SIBRA achieves botnet-size independence together with the scalability of inter-domain resources. Tumbler [31] regards each AS as a unit to allocate bandwidth in its domain on demand, calculates the competition factor considering domain characteristics, and then uses the inter-domain queue to control the packet sending speed. STBA [30] proposes a spatio-temporal heterogeneous bandwidth allocation mechanism, which introduces superspreaders sub-metrics to discriminate the influence of ASes to ensure the bandwidth connection capability of influential ASes.

In addition, several approaches aim to identify and detect DDoS traffic. PacketScore [16] performs statistical analysis to score data packets based on the characteristics of data packets. To distinguish the data packets, PacketScore sets a baseline for data packets to classify the malicious traffic. ScoreforCore[13] pro-

poses a dynamic selection attribute model for different attack types on the basis of PacketScore. However, the false positives are unavoidable in detection mechanisms. Thus, FIBA provides the malevolent-looking packets with low priority queue rather than simply filtering them.

6 Conclusion

We have proposed FIBA, a capability-based DDoS mitigation that realizes fine-grained intra-domain bandwidth allocation. According to the topological effects and traffic features, FIBA measures the state of request packets among diverse clients during capability establishment. FIBA is built with hierarchical channel to achieve differential accessing control of capability and traffic isolation. Upon the domain-level DDoS resistance, FIBA is able to provide a fine-grained protection and user-level DDoS resistance. Through comprehensive network experiments, we verify the performance of FIBA in terms of reasonable bandwidth reservation and user-level DDoS resistance.

Acknowledgement. This work is supported by National Key Research and Development Program of China (2020YFB1005702).

References

1. Autonomous system numbers (2016). http://www.iana.org/assignments/as-numbers/as-numbers.xhtml
2. Bene: A python network simulator (2017). https://github.com/zappala/bene
3. AS relationships (2020). https://www.caida.org/data/as-relationships/
4. AWS said it mitigated a 2.3 Tbps DDoS attack, the largest ever, June 2020. https://www.zdnet.com/article/aws-said-it-mitigated-a-2-3-tbps-ddos-attack-the-largest-ever/
5. DDoS attacks rise in intensity, sophistication and volume, September 2020. https://www.helpnetsecurity.com/2020/09/17/ddos-attacks-rise-in-intensity-sophistication-and-volume/
6. Andersen, D.G., Balakrishnan, H., Feamster, N., Koponen, T., Shenker, S.: Accountable internet protocol (aip). In: Proceedings of the ACM SIGCOMM 2008 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, Seattle, 17–22, August 2008
7. Basescu, C., et al.: SIBRA: scalable internet bandwidth reservation architecture. In: Proceedings NDSS, San Diego, February 2016
8. Bennett, J.C.R., Zhang, H.: Hierarchical packet fair queueing algorithms. IEEE/ACM Trans. Netw. **5**(5), 675–689 (2002)
9. Bonacich, P.: Factoring and weighting approaches to status scores and clique identification. J. Math. Soc. **2**(1), 113–120 (1972)
10. Estrada, E., Rodriguez-Velazquez, J.A.: Subgraph centrality in complex networks. Phys. Rev. E Stat. Nonlin. Soft Matter Phys. **71**(5), 056103 (2005)
11. Godfrey, P., Ganichev, I., Shenker, S., Stoica, I.: Pathlet routing. ACM SIGCOMM Comput. Commun. Rev. **39**(4), 111–122 (2009)

12. Heer, H.: Host identity protocol certificates draft-ietf-hip-cert-12. Technology (2011)
13. Kalkan, K., Alagöz, F.: A distributed filtering mechanism against DDoS attacks. Comput. Netw. **108**, 199–209 (2016). https://doi.org/10.1016/j.comnet.2016.08.023
14. Kang, M.S., Lee, S.B., Gligor, V.D.: The crossfire attack. In: Proceedings IEEE S&P, pp. 127–141, Berkeley, May 2013
15. Kim, T.H.J., Basescu, C., Jia, L., Lee, S.B., Hu, Y.C., Perrig, A.: Lightweight source authentication and path validation. In: Proceedings ACM SIGCOMM, pp. 271–282, Chicago, August 2014
16. Kim, Y., Lau, W.C., Chuah, M.C., Chao, H.J.: Packetscore: a statistics-based packet filtering scheme against distributed denial-of-service attacks. IEEE Trans. Dependable Secure Comput. **3**(2), 141–155 (2006)
17. Kitsak, M., et al.: Identification of influential spreaders in complex networks. Nat. Phys. **6**, 888–893 (2010)
18. Lee, S.B., Gligor, V.D.: Floc : dependable link access for legitimate traffic in flooding attacks. In: IEEE International Conference on Distributed Computing Systems (2010)
19. Morone, F., Makse, H.A.: Influence maximization in complex networks through optimal percolation. Nature **524**(7563), 65 (2015)
20. Parno, B., Wendlandt, D., Shi, E., Perrig, A., Maggs, B., Hu, Y.C.: Portcullis: protecting connection setup from denial-of-capability attacks. ACM SIGCOMM Comput. Commun. Rev. **37**(4), 289–300 (2007). https://doi.org/10.1145/1282427.1282413
21. Rekhter, Y., Li, T.: A border gateway protocol 4 (BGP-4). RFC 1771, March 1995
22. Rouse, M.: ICANN (Internet Corporation for Assigned Names and Numbers) (2016). http://searchsoa.techtarget.com/definition/ICANN
23. Steve, H., Jun, D.: Understanding network concepts in modules. BMC Syst. Biol. **1**(1), 24 (2007)
24. Studer, A., Perrig, A.: The coremelt attack. In: Backes, M., Ning, P. (eds.) ESORICS 2009. LNCS, vol. 5789, pp. 37–52. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-04444-1_3
25. Touch, J.: Updated specification of the IPv4 ID field. RFC 6864, February 2013
26. Xiao, P., Li, Z., Qi, H., Qu, W., Yu, H.: An efficient DDoS detection with bloom filter in SDN. In: 2016 IEEE Trustcom/BigDataSE/ISPA, pp. 1–6. IEEE (2016)
27. Xie, L., Zhang, Y., Zheng, Z., Zhang, X.: TRIP: a tussle-resistant internet pricing mechanism. IEEE Commun. Lett. **21**(2), 270–273 (2017)
28. Yaar, A., Perrig, A., Song, D.: SIFF: a stateless internet flow filter to mitigate DDoS flooding attacks. In: IEEE Symposium on Security and Privacy, 2004. Proceedings, 2004, pp. 130–143 (2004)
29. Yang, X., Wetherall, D., Anderson, T.: Tva: a dos-limiting network architecture. IEEE ACM Trans. Netw. **16**(6), 1267–1280 (2008)
30. Zhang, X., Xie, L., Yao, W.: Spatio-temporal heterogeneous bandwidth allocation mechanism against DDoS attack. J. Netw. Comput. Appl. **162**, 102658 (2020)
31. Zhang, Y., Wang, X., Perrig, A., Zheng, Z.: Tumbler: adaptable link access in the bots-infested internet. Comput. Netw. **105**, 180–193 (2016)
32. Zhang, Y., Xie, L., Zhang, D., Liu, G., Wang, Q.: Scalable bandwidth allocation based on domain attributes: towards a DDoS-resistant data center. In: Proceedings IEEE GLOBECOM, pp. 1–6, Singapore, December 2017