A New Stateless Packet Classification and Filter against DoS Attacks

Guang Jin and Qian Wang
College of Information Science and Engineering, Ningbo University, Ningbo, China
Email: jinguang@nbu.edu.cn, 398077850@qq.com

Xianliang Jiang
College of Computer Science and Technology, Zhejiang University, Hangzhou, China
Email: {jiangxianliang}@foxmail.com

Abstract—Capabilities is a typical scheme of stateless filtering. In order to classify and filter packets effectively, a novel scheme of packet classification and filter based on capabilities is proposed in this paper. In our scheme, a new classifier module is added and a new filter structure is designed. We employ capabilities as verification and introduce new authorization in the communications. All these innovations make packet classification owning good effects in attacking scenario. The experimental results based on large-scale topology datasets and NS2 show that our scheme is better than traditional packet classification algorithms, especially under complex cyber environment.

Index Terms—Packet Classification; Network Security; Capabilities; Filter

I. INTRODUCTION

With the wide application in network monitor, service classification, network measurements, QoS and network security, etc, the packet classification has become a hot topic. Although a number of algorithms for packet classification have emerged, several security flaws still exist. Especially under the current circumstances that security issues occur frequently and the network speed is increasing constantly, the network security deserves more attention.

A. Packet Classification Technology

The packet classification refers to the action that the filter of a router or a host matches the packet header fields and categorizes packets into different flows according to fixed rules, and then performs corresponding operations.

Among most existing packet classification schemes, the rule is often defined as a 5-tuple (SrcIP, DestIP, SrcPort, DestPort, Protocol).


However, there are several inherent issues in existing techniques. Especially under the complicated network environment, most schemes have not yet fully considered security issues, e.g., address spoofing, and relied simply on the classification of the packets’ header fields. It would result in difficulties in resisting cyber attacks. Based on the consideration, we proposed flow trust [10] recently to defend against low-rate or flooding DoS attacks, and now employ packet marking techniques to improve the packet classification.

B. Stateless Filtering with Capabilities

Considering the limited router resources, the Next Generation Internet Infrastructure (NGSI) [11] suggested that the core networks should have minimum or constant-quantity states, as well as routers and firewalls. Even if under the large-scale Distributed Denial-of-Service (DDoS) attack, the size of the filter table should be stable and relatively small. Related studies for the NGSI are analyzed and summarized in [12].

The idea of capabilities was proposed firstly by Anderson et al [13]. They assumed that the capabilities are similar to a token, which emphasizes the request, authorization, carrying, and verifying. And the capability is contained in subsequent packets. Currently, Perrig et al and Yang et al have achieved significant advances respectively. Perrig et al firstly proposed the SIFF [14], emphasizing that when a sender is requesting, the pre-markings should be inserted into request packets by the nodes along the path. Once the destination host accepts...
the request, it would authorize the capabilities to the sender, and allow it to send messages. The nodes along the route would verify the packets carrying authorized capabilities. The packet would be forwarded if the capability is matched, or discarded if the verification is unsuccessful. Yang et al further proposed a more complete Traffic Validation Architecture (TVA) [15], which reduced the computing resource of router processing capabilities and storage requirements effectively, realized incremental deployment and other characteristics. Shue et al [16] suggested building low-cost network capabilities against the deficiencies of capabilities applications. Some researchers raised different views on capabilities. Argyraki et al [17] carried on a comprehensive analysis on capabilities techniques, and made objective evaluations of the drawbacks. We think there is no doubt that the capabilities mechanism has the superiority in aspect of countering DoS attacks, and it can resist spoofing attacks and flooding attacks effectively. We also studied and improved the TVA scheme [18].

The research of this paper will combine the merits of capabilities with the packet classification to design a Packet Classification and Filter based on Capabilities (PCFC).

II. SECURE PACKET CLASSIFICATION AND FILTER

A. The Idea of PCFC

Firstly, the packet classification uses the capabilities marking at the network layer, and is deployed on key routers. The security of the packet classification is determined by the capabilities’ feature against cyber attacks, which prevents the transmission of unauthorized data. Thus the main function of packet classification is to classify the traffic produced by coordinated attacks.

Secondly, the sender should obtain the capabilities authorized by the receiver before sending data, and transmit packets with the capabilities. The packets carrying capabilities would be classified when they arrive at the routers deploying PCFC.

Thirdly, the process of the packet classification is as follows: the routers make decisions according to the actual requirements of service differentiation. If the packet classification plays single defense function, the routers perform classifications of malicious and legitimate packets. Otherwise, the routers need to perform additional service classification operations, according to the packets’ header. For instance, the HiCut [19], a traditional packet classification algorithm, can be used to obtain ordinary classification results. And the combinational outputs of the traditional and attacking packet classification algorithms’ results would present more effective final classifications.

B. The Framework of PCFC

This paper proposes a novel PCFC architecture shown in figure 1.

The core of PCFC includes four parts: controller module, decider module, attacking packet classification module, and service classification module. The principles should be preset by controller to regulate the decider’s decision. The decider includes input and output components. The input controller decides to classify the incoming packets into three categories: attack, service, and mixed combining secure and service ones. The output part makes the decision for attack and service classifications, and produce final classification results. Based on the capability marking and statistical information, the incoming packets can be classified into the malicious or legitimate packets. The service classification based on packet heads employs the traditional packet classification algorithm.

C. The Compatibility of IPv6

Due to limited space, the description of PCFC here is aiming at IPv4, but the main idea also fits IPv6. In IPv6, the IP header of packets includes fixed fields and extension headers. The PCFC scheme carries capabilities mainly in extension headers of IP packets. Therefore, the PCFC can be transplanted easily from IPv4 to IPv6, while the only difference exists in extracting the IP packet header information. Moreover, the filter in this paper also can be designed as the model supporting double protocols, and automatically perform corresponding operation with the IP packets head.

III. DESIGN OF PACKET CLASSIFICATION AND FILTER

A. Design of Controller Module

The classifier allows users to setup configuration files, loaded by the controller at run time. The controller regulates the decisions of input/output decider. The input decider controls the option of packet classification models and the control of output decider is involved with the input decider. Thus the control parameter of output decider can be generated by the control signal of the input decider.

B. Design of Decider Module

The decider module includes two components: input decider and output decider. The input decider decides to adopt which kind of packet classification models, and perform packet classification through calling the corresponding module and setting relevant parameters. The output decider decides to output the result of the attacking/service classification module, and generate the syncretic results.
C. The Design of Attacking Classification Module

Attacking packet classification identifies and classifies attacking packets according to the capabilities. The structure is as shown in Figure 2.

As shown in Figure 2, a packet would experience following steps when arriving at the attacking classification module.

(1) For classification, the module extracts the capabilities and other header’s information from the packet. Go to step (2).

(2) The module finds previous records relating to the capabilities from the filter cache table. Go to step (3).

(3) The module executes the attack classification according to the packet’s header information and the found record. Go to step (4).

(4) The module generates the result of attack classification and updates the filter cache table.

There exist two indefinite issues in the classification process. One is how the attacking classification algorithm uses packet’s header information and locates records to classify packets. Another is how we locate and update the information of the filter’s cache table.

To the first issue, the core of the attacking classification algorithm is searching in the cache table according to the extracted capabilities and judging whether there are records meeting the requirements. If the matched record is found, the module executes the attacking classification and then updates the cache table. Otherwise, a new record is created in the cache table. Meanwhile the packet classification algorithm uses the capabilities and the traffic information to classify packets and then update the new record.

The packet classification module of PCFC is based on the traffic-statistics method and sets up different thresholds to determine whether the packet is legitimate, suspicious or malicious. Equation (1) provides the malicious probability of different flows according to the traffic volume in a constant interval.

\[
P = \begin{cases} 
0 & \text{IF}(Q < \min_q) \\
1 & \text{IF}(Q \geq \max_q) \\
\max(0, \frac{Q - \min_q}{\max_q - \min_q}) & \text{other} 
\end{cases} \quad (1)
\]

In (1), the \( P \) is the probability that packets are malicious. The \( Q \) is the flow’s traffic volume in the constant interval. The \( \min_q \) and \( \max_q \) are the minimum and maximum value of the traffic volume under normal circumstances and the corresponding \( P \) is 0 and 1 respectively.

\[
Q = \frac{fc + cp}{ct - rt} \quad (2)
\]

The \( Q \) can be calculated by (2). The \( fc \) means the statistical flow volume in the cache. The \( cp \) means the size of the current packet. The \( ct \) means current recorded time and \( rt \) means the firstly recorded time.

The filter cache table is changing with the network traffic, and Figure 3 shows the structure of the cache.

In the Figure 3, the LI means the length of index table, and varies from 0 to 31, corresponding to 32 different kinds of capability length passage. The EBF, the extension of Bloom Filter [20], xor the capability firstly to obtain the 64-bit value of combination capability, then execute the Bloom Filter operation. The DM is the address generation module, and determines the final recording address. In the structure, the Bloom Filter is mainly used to determine quickly whether the corresponding records exist in the cache. If a record does not exist, the new record is created and returned. If a record exists, the structure uses the combination of capability hash and LI’s value to execute quick location and return the results.

The related parameters used in the Bloom Filter can be defined by the Equation (3), where \( m \) means the size of bit array; \( n \) means the number of capability; \( \epsilon \) means the upper limit of false positive ratio.

\[
m \geq n \cdot \log_2 e \cdot \log_2(\frac{1}{\epsilon}) \quad (3)
\]

Moreover, the cache table should be updated regularly to occupy as least storage space as possible and the expired records should be deleted in time. Figure 4 provides the pseudo-code of the attack classification.

D. Design of Service Classification

The service classification module adopts the traditional packet classification algorithm, and more optimization is our future work. The paper’s purpose is not to improve the existing algorithms, but to build new packet classification and filter. The following research can adopt typical algorithms, such as decision tree, exhaustive search, and so on.

In PCFC, the existing typical packet classification algorithms can be added to the service module directly, and be well compatible without modifying other parts.
and it possesses good scalability. Figure 5 shows the pseudo-code of the service classification.

```c
Algorithm 1: attacking classification
Input: packets
Output: packets malicious probability
1. double Attack::Classify(packet *p) {
2. get the hdr_filter of packet p;
3. search the cache using capabilities and its length;
4. if (has record) {
5. calculate the probability of malicious packets;
6. } else {
7. create new record;
8. set the probability of malicious packets to zero;
9. }
10. update the record in cache;
11. return P;
12. }
```

Figure 4. The pseudo-code of the attacking classification.

```c
Algorithm 2: service classification
Input: packets
Output: classifying results
1. int Service::Classify(packet *p) {
2. get the head of packet p;
3. call packet classification algorithm;
4. update the record in cache;
5. return result;
6. }
```

Figure 5. The pseudo-code of the service classification.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

A. Experimental Data Set

Our experiments adopt the authoritative CAIDA Internet topology dataset [21]. The experiment described in this paper bases on the “h-r20030507sr” data set, which contains 690,629 Internet paths. 10,000 paths are selected randomly as the final simulation source data.

B. Theoretical Analysis and Evaluation

Security Analysis. The security of packet classification is particularly important in the complex network environment as mentioned before. In PCFC, the capabilities are adopted as the important basis of packet classification and it eliminates the impact caused by spoofing attacks and ensures the security of packet classification.

Analysis of Execution Efficiency. The packet classification and filter are generally deployed in core routers. Therefore the efficiency of the implementation should not be ignored. PCFC allows the attacking classification and service classification to be executed simultaneously on hardware or software. The action is controlled by the controller, and the decider makes the decision of the input and the results, and its efficiency is closed to that of existing packet classification schemes.

Deployment and Expandability. The PCFC operations use capabilities marking, so we assume the capability scheme has been deployed. Then PCFC deployed in key routers can achieve the incremental deployment without depending on other networks and routers, and implement the incentive mechanism.

C. Simulation Experiment

We implemented the PCFC on NS2 [22] and the simulation topology is shown in Figure 6. The scheme is tested separately under two scenarios. The scenario I is without attacks and the scenario II is with spoofing attacks. PCFC is deployed in Ra.

In the experiments, the senders mainly consist of legitimate users and spoofing attackers. The number of legitimate users is 50, and the number of attacker is varying from 1 to 100. The link bandwidth is shown in figure 6. All the delay is 10ms, and the queue management adopts the multi-level queue in TVA [15].

Firstly the simulations on scenario I is described as follows.

Because there are no cyber attacks, the router performs normal classification and the legitimate user sends packets whose sizes is 1000 Bytes. And the transmission time is from 1 to 100 seconds.

Figure 7 compares the efficiency and validity of classification among linear, HiCut [19] and PCFC. Obviously, the efficiency of the PCFC is much close to that of existing classification schemes under normal circumstance. Without cyber attacks, the PCFC can perform the attack classification and service classification in parallel, therefore the execution time is the maximum of attack classification time and service classification time. Generally, the main function of attack classification is to discriminate malicious packets from all, and its execution time is less than that of the service classification. Meanwhile, the PCFC demands hardware and software resources for capability computation and verification to guarantee the secure packet classification.
Therefore, the PCFC requires close but longer execution time of the HiCut. Figure 8 shows the false positive ratio of packet classification algorithms. As we can see, all schemes could acquire low false positive without spoofing attacks. The false positive ratio is mainly determined by the classification algorithm, and PCFC wouldn’t achieve effective results without any attacks.

![Figure 8. The false positive ratio without attacks](image1)

This experiment is conducted as the reference for the following one. The designs of Linear algorithm and HiCut are oriented to general cyber environment, to achieve high performance in classification. Therefore, the ratios fluctuate within a certain range, and PCFC narrowly wins in the comparison.

Then we conduct packet classification experiment with attacks.

In this experiment, to compare the validity of three schemes, the legitimate users and the spoofing attacker send 1000 bytes-size packets respectively and the transmission time varies from 1s to 100s.

![Figure 9. The false positive ratio with attacks](image2)

Figure 9 shows the results of three schemes with spoofing attacks. Obviously, spoofing attacks exert huge impact on classifications, compared to Figure 8. The PCFC can acquire more resistance to the attacks and achieve the best performance.

The algorithms of Linear and HiCut don’t posses effective way to identify and verify forge packets, thus the ratios are up to nearly 70%. With the authentication mechanism of the capability, PCFC can verify the most malicious packets and discard them.

V. CONCLUSIONS

The packet classification has been widely applied in network communications. The PCFC scheme proposed in this paper can achieve secure packet classification, and resist the misclassification caused by spoofing attacks. The experimental results show that PCFC outperform most other schemes. The efficiency of PCFC is close to the packet classification algorithm without attacks, while it would perform better when suffering spoofing attacks. The PCFC aims at the infrastructure of the packet classification at core routers, combines capabilities and other intelligent marking technologies, and can support dual-stack structure of IPv4 and IPv6 well.

We employ the property of the capability in the packet classification for improving the security of the traffic to response to increasingly complicated cyber issues. In conclusion, the PCFC consumes more resources and its complexity of the algorithm increases compared to general algorithms, but it has incomparable advantages on resisting attacking. The PCFC has better overall properties. This paper just provides prototype, and there exist lots deficiencies. For instance, capabilities storage, searching algorithms, scalability and other respects need further improvement and should be tested in actual router measurements.

ACKNOWLEDGMENT

This research was supported in part by Zhejiang Provincial Technology Innovation Team (2010R50009), Natural Science Foundation of Zhejiang Province (LY12F020213), Ningbo Natural Science Foundation (2012A610014), Ningbo Municipal Technology Innovation Team (2011B81002), The Graduate Teaching Innovation on Ningbo University (2011004).

REFERENCES


Guang Jin received his MS and Ph.D degree in Computer Science from Zhejiang University in China. Since 2001, He has been with the College of Information Science and Engineering of Ningbo University in China. He is currently a full professor and his research interests focus on network security and wireless networking. He has published over 30 papers in conferences and journals including IEEE Communications Letters. He also published two books on networking. Especially his new book, the Wireless Networking Technique, has been used as the textbook in over 30 universities or colleges in China.

Qian Wang is a MS candidate in the College of Information Science and Engineering at Ningbo University. His research interests mainly focus on wireless sensor network. Previously, he received his BS degree from Science and Technology of Changsha in 2012.

Xianliang Jiang is a PhD candidate in the College of Computer Science and Technology at Zhejiang University. His research interests are in ad hoc routing protocol, mobile computing and networks security. Previously, he received his BS degree from University of Science and Technology of China in 2009 and MS degree from Ningbo University in 2012.