International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 03 ISSUE 06 Pages: 63-71
SJIF IMPACT FACTOR (2021: 5.478) (2022: 5.636) (2023: 6.741)
OCLC – 1368736135

Journal Website: http://sciencebring.com/index.php/ijasr

Research Article

IMPLEMENTING PACKET CLASSIFICATION USING STANDARD ACL

Submission Date: June 04, 2023, **Accepted Date:** June 09, 2023,
Published Date: June 14, 2023
Crossref doi: https://doi.org/10.37547/ijasr-03-06-12

Nurbek Nasrullayev
Nurafshon Branch Of Tashkent University Of Information Technologies Named After Muhammad Al-Khwarizmi, Tashkent Region, Uzbekistan

Dilnoza Sodikova
Tashkent University Of Information Technologies Named After Muhammad Al-Khwarizmi Cybersecurity And Criminology Department Tashkent, Uzbekistan

Nuriddin Safoev
Tashkent University Of Information Technologies Named After Muhammad Al-Khwarizmi Cybersecurity And Criminology Department Tashkent, Uzbekistan

Qurbonova Kabira Erkinovna
Tashkent State Technical University Named After Islam Karimov, Tashkent, Uzbekistan

ABSTRACT

Packet classification involves the categorization of packets within network systems, such as firewalls and routers, based on their flow. Its primary objective is to match packet headers with a predefined set of filters. In this research, we propose a system that utilizes the source IP address of each incoming packet for packet classification. By employing a rule set, the system can determine whether to grant or deny access to each packet. The algorithm examines the source IP address header field of received packets on a specific link and compares it against a collection of rules. It then outputs the action associated with the highest priority rule that corresponds to the packet header. Ultimately, the classification of individual packets is based on the action specified in the rule set.

KEYWORDS

Packet Classification, Firewalls, Routers, Access Control List (ACL).

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 03 ISSUE 06 Pages: 63-71
SJIF IMPACT FACTOR (2021: 5.478) (2022: 5.636) (2023: 6.741)
OCLC – 1368736135

ISSN-2750-1396

INTRODUCTION

The primary objective of routers and firewalls is to classify packets and direct them to their appropriate destinations. Packet classification is crucial for quality of service (QoS) identification. This classification process involves considering factors such as source and destination ports, addresses, and protocol types. Firewalls, in particular, must rapidly make decisions regarding packet denial or acceptance, prioritizing speed. As router performance requirements increase, there is a need for packet classification algorithms that can efficiently and swiftly classify packets while minimizing storage needs [1].

Evaluating newly published packet classification algorithms can be challenging due to different perspectives and assumptions. Comparing these algorithms directly is nearly impossible without a common framework. This issue is especially pronounced in network routers, as packet classification inherently poses difficulties and existing algorithms rely on heuristics and filter set characteristics. The performance of the packet classification subsystem greatly impacts the overall performance of network routers [1-12].

As network traffic requirements grow and change, larger filters with more complex rules become necessary. This, in turn, leads to the development of various fast packet classification algorithms. A packet comprises header and information data, with the header including MAC addresses, IP addresses, port numbers, and more. When a packet reaches a network device's interfaces, there can be multiple policies that match its specified header fields. Only the action associated with the highest-priority policy is taken [4].

The classifier is a collection of rules that identify each flow and specify the corresponding actions. Network nodes must perform searches over sets of filters using multiple packet fields as search keys in order to classify a packet as belonging to a particular flow or set of flows [10].

PREVIOUS WORK

The development of packet classification algorithms is hindered by the need to balance search time and memory requirements. It is impractical to expect a single algorithm to perform well under all circumstances. Research efforts primarily focus on uncovering inherent structures or characteristics of specific classification problems that allow for the creation of heuristic algorithms that are "fast enough" and consume "not too much" memory.

In general, packet classification involves determining how packets should be categorized and what actions should be taken for each packet after classification. Figure 1 illustrates the process where the packet header is extracted, the packet is checked against a rule set, and a specific action is taken accordingly.

In a study described in [1], the authors propose an algorithm called Dim cut, which is an extension of the Hicut algorithm. This algorithm consists of

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 03 ISSUE 06 Pages: 63-71
SJIF IMPACT FACTOR (2021: 5.478) (2022: 5.636) (2023: 6.741)
OCLC – 1368736135

two distinct levels: a pre-processing level and a search level. The algorithm emphasizes the comprehensive description of data structures and adjustable parameters. When a packet arrives, a tree is constructed, and a search key is generated based on the packet's header fields. The search continues until reaching a leaf node. In this algorithm, buckets are used to store rules within a range. If the same rule is repeated in all nodes at the same level, the algorithm separates that rule and employs a bucket during the search. The buckets are sorted by priority. The advantage of this algorithm is that it provides improved storage utilization and throughput. However, a disadvantage is that if the bucket size increases, it leads to longer linear searches, while smaller bucket sizes require more processing time.

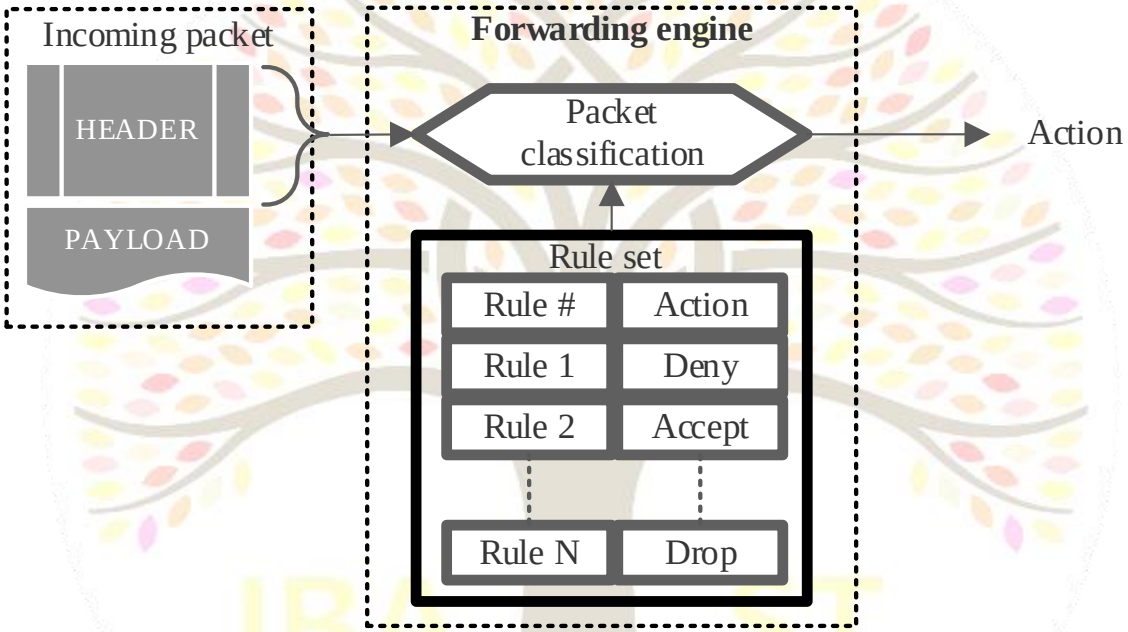

Figure 1. Packet classification in general

In [2], a comparison is made between fast packet classification algorithms, namely HSM and RFC. The focus of the comparison revolves around source and destination IP addresses, as well as source and destination port numbers. The RFC algorithm employs a decomposition-based approach, where it computes multiple fields and condenses them into a single field. On the other hand, the HSM algorithm utilizes four dimensions and consolidates them into a single table. In RFC, the index value can be adjusted based on the internet service provider. When a packet arrives at a network router, both algorithms compare it against a set of rule sets to determine if the information it contains satisfies any of the rules.

Both algorithms offer a versatile solution that can be implemented in software and hardware, making them applicable to various fields of classification. However, a drawback is that an

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 03 ISSUE 06 Pages: 63-71
SJIF IMPACT FACTOR (2021: 5.478) (2022: 5.636) (2023: 6.741)
OCLC – 1368736135

increased number of policies will require more memory.

In [3], a novel algorithm called Hierarchical Intelligent Cuttings (HiCut) is proposed. This algorithm demonstrates fast packet classification and has relatively low storage requirements. It constructs a decision tree data structure, and upon the arrival of a packet, the decision tree is traversed to locate a leaf node that contains a small number of rules. If a node has fewer than a certain threshold of rules, it is not further partitioned and becomes a leaf in the tree. The pre-processing time needed to build the decision tree is an important consideration. The key advantages of this algorithm are its fast average query time and efficient update time when rules change. However, a disadvantage is the use of hashing, which can result in non-deterministic durations for lookups or updates.

In [4], the authors propose a technique called Hierarchical Space Mapping (HSM). This algorithm utilizes a multi-stage reduction scheme. The action to be taken for each packet is determined by selecting the top-priority rule from the matching rule set. The rule set policies can be cached, as the execution order of classification tasks strictly defines the actions to be applied to the packet. The main concept presented in this paper is to minimize the search fields by progressively and hierarchically mapping the lookup domains. By mapping address spaces and port number spaces into non-overlapping segments, a reduced table is obtained. This approach allows for the construction of a policy table that transforms the two-dimensional space into a one-dimensional policy space. The advantages of the HSM technique include its applicability to multiple fields, fast lookup rates, and reasonable memory requirements. However, there are some drawbacks, such as a lengthy pre-processing time and insufficient memory for large policy tables.

In [5], a novel approach to packet classification is presented, known as the Grid of Segment Trees. This method is derived from the Grid of Tries technique and has been implemented to enhance performance. The Grid of Segment Trees modifies the Grid of Tries by replacing binary tries with segment trees. To improve search speed, the authors employ precomputation and introduce the concept of switch pointers in the Grid of Tries. The Grid of Tries is specifically designed to address limitations found in hierarchical tries and set pruning tries. The authors focus on two fields, namely source and destination addresses, when constructing the Grid of Tries, Dynamic Segment Tree, and Grid of Segments. In the Dynamic Segment Tree, the segment tree is constructed by precomputing it in elementary intervals and then building a data structure from the bottom up. However, this approach is not suitable for dynamic routing tables. The Grid of Segment Trees method involves several steps in constructing and processing the trees. These steps include creating a node structure, inserting into the Grid of Segment Trees, constructing switch pointers, and querying the Grid of Segment Trees. The advantage of this technique is that it enables effective multidimensional packet classification [13-30]. The Grid of Segment Trees

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 03 ISSUE 06 Pages: 63-71
SJIF IMPACT FACTOR (2021: 5.478) (2022: 5.636) (2023: 6.741)
OCLC – 1368736135

outperforms the other two approaches. However, a drawback is that packet classification is based on the prefix extracted from the fields in the packet.

CLASSIFICATION USING ACL

In general, there are two main types of access control lists (ACLs): standard control lists and extended control lists. For the purpose of this paper, we will focus on the classification based on standard ACLs. This classification involves analyzing the source/destination addresses, ports, protocol, and packet priority. When an incoming packet arrives, it needs to be compared with a set of rules based on these fields. A packet-filtering router will either block or allow packets based on a predefined set of filtering rules.

Most algorithms for multidimensional packet classification require multiple fields for classification. However, these algorithms often come with increased memory usage and a need for faster search speeds.

Standard Access Lists primarily utilize the source IP address in an IP packet to filter the network. They generally permit or deny an entire suite of protocols. On the other hand, Extended Access Lists consider additional factors such as source and destination IP addresses, as well as the protocol field in the network.

An ACL is essentially a collection of statements that determine whether packets entering or leaving an interface should be accepted or rejected. These statements are processed in a sequential and logical order. If a condition in an ACL statement is matched, the packet is either permitted or denied, and the remaining statements in the ACL are not evaluated. If none of the ACL statements match, an implicit "deny any" statement is typically added to the end of the list as a default action.

IMPLEMENTATION OF CLASSIFICATION USING ACCESS CONTROL LIST

ACLs serve the purpose of packet filtering to manage the flow and destination of packets within a network. They play a crucial role in controlling user and device access, thereby enhancing network security. By carefully defining access rules, ACLs can effectively restrict network access and reduce unnecessary traffic, resulting in resource optimization. Implementation details of the proposed technique can be found in Figure 2.

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 03 ISSUE 06 Pages: 63-71
SJIF IMPACT FACTOR (2021: 5.478) (2022: 5.636) (2023: 6.741)
OCLC – 1368736135

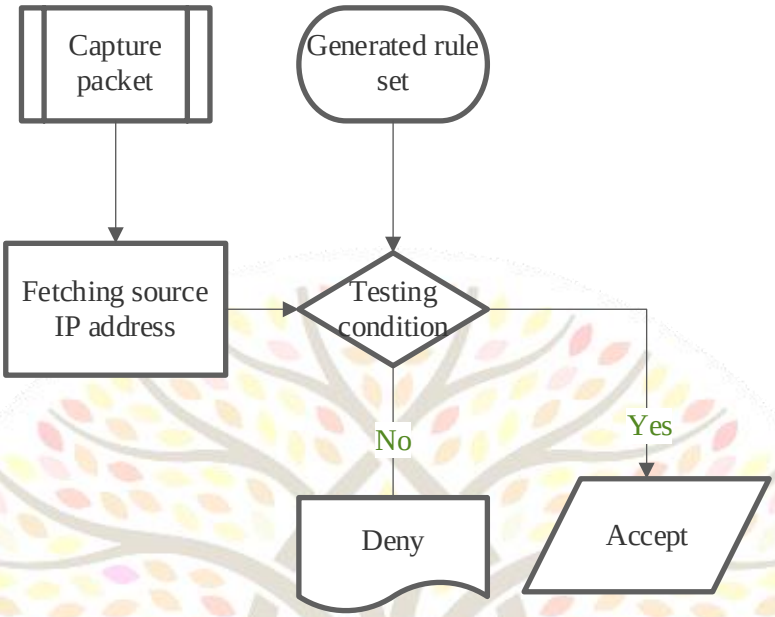

Figure 2. Classification based on ACL

GENERATING RULE SET: The rule set is created to implement security measures by applying an access list. When an access list is applied to a router interface in a specific direction, the router analyzes each packet that traverses that interface and takes appropriate action based on the defined rules. ACLs can be configured on a router to control access to a network or subnet. If a packet contains a single source IP address, the rule set is generated to determine whether to accept or deny the packet. Figure 5 illustrates the representation of the rule set.

DECISION MAKING: ACLs play a vital role in filtering network traffic by allowing or blocking the forwarding of routed packets at the router's interfaces. The router evaluates each packet to decide whether to forward it or drop it, based on the conditions specified in the ACL. These conditions typically involve factors such as the source address of the traffic. The packet is examined against the statements in the ACL, and if a match is found, the packet is either accepted or rejected accordingly.

CONCLUSIONS

Our proposed paper addresses the challenges related to the performance of packet classification algorithms, with a specific emphasis on routers and security concerns in network environments. In the context of packet classification in networks, it is crucial to filter packets in a manner that ensures both security and enhanced search speed. We recognize the importance of flexibility in creating rule sets, as well as in rule specification and implementation. Given that packet classification algorithms predominantly rely on heuristics, the use of

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 03 ISSUE 06 Pages: 63-71
SJIF IMPACT FACTOR (2021: 5.478) (2022: 5.636) (2023: 6.741)
OCLC – 1368736135

different rule sets with varying structures and sizes can yield different outcomes. Additionally, it is important to develop an algorithm that minimizes the effort required for filter set management and can handle frequent filter updates. The primary focus of our paper is to classify packets in real-time environments. We aim to effectively and efficiently determine whether a packet should be accepted or denied, taking into consideration the specific requirements and constraints of the network.

REFERENCES

1. Gupta, P., & McKeown, N. (2001). Algorithms for packet classification. IEEE Network, 15(2), 24-32.
2. Xu B., Jiang D., Li J. HSM: A fast packet classification algorithm //19th International Conference on Advanced Information Networking and Applications (AINA'05) Volume 1 (AINA papers). – IEEE, 2005. – T. 1. – C. 987-992.
3. Gupta P., McKeown N. Packet classification using hierarchical intelligent cuttings //Hot Interconnects VII. – 1999. – T. 40.
4. Gupta P., McKeown N. Packet classification on multiple fields //Proceedings of the conference on Applications, technologies, architectures, and protocols for computer communication. – 1999. – C. 147-160.
5. Taylor, D. E. (2005). Survey and taxonomy of packet classification techniques. ACM Computing Surveys (CSUR), 37(3), 238-275.
6. Bakhodir, Y., Nurbek, N., & Odiljon, Z. (2019). Methods for applying of scheme of packet filtering rules. International Journal of Innovative Technology and Exploring Engineering, 8(11), 1014-1019.
7. Safoev, Nuriddin, and Jun-Cheol Jeon. "Area efficient QCA Barrel shifter." Advanced Science and Technology Letters (2017): 51-57.
8. Safoev, Nuriddin, and Jun-Cheol Jeon. "Full adder based on quantum-dot cellular automata." Proceedings of international conference of trends in engineering and technology. 2017.
9. Safoev, N., and J. C. Jeon. "Reliable design of reversible universal gate based on QCA." Advanced Science Letters 23.10 (2017): 9818-9823.
10. Safoev, Nuriddin, and Jun-Cheol Jeon. "Coplanar QCA adders for arithmetic circuits." International Journal of Engineering & Technology 7.4.4 (2018): 15-16.
11. Gulomov, S. R., & Bakhtiyorovich, N. N. (2016, November). Method for security monitoring and special filtering traffic mode in info communication systems. In 2016 International Conference on Information Science and Communications Technologies (ICISCT) (pp. 1-6). IEEE.
12. Malikovich, K. M., Rajaboevich, G. S., & Karamatovich, Y. B. (2019, November). Method of constucting packet filtering rules. In 2019 International Conference on Information Science and Communications Technologies (ICISCT) (pp. 1-4). IEEE.

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 03 ISSUE 06 Pages: 63-71
SJIF IMPACT FACTOR (2021: 5.478) (2022: 5.636) (2023: 6.741)
OCLC – 1368736135

13. Насруллаев, Н. Б., & Файзиева, Д. С. (2020). Анализ средств службы информационной безопасности в дистанционном обучении. Молодой ученый, (31), 14-18.
14. Baxtiyorovich, N. N., & Ubaydullaevna, H. I. (2019, November). Method of analyzing of antivirus errors when audit provides. In 2019 International Conference on Information Science and Communications Technologies (ICISCT) (pp. 1-3). IEEE.
15. Safoev, N., and J. C. Jeon. "Peres gate realization in QCA for reversible binary incrementer." Advanced Science Letters 23.10 (2017): 9812-9817.
16. Komil, T., & Nurbek, N. (2015). Development method of code detection system on based racewalk algorithm on platform FPGA. In Proceedings of International Conference on Application of Information and Communication Technology and Statistics in Economy and Education (ICAICTSEE) (p. 278). International Conference on Application of Information and Communication Technology and Statistics and Economy and Education (ICAICTSEE).
17. Safoev, N., & Nasrullaev, N. (2021, November). Low area QCA Demultiplexer Design. In 2021 International Conference on Information Science and Communications Technologies (ICISCT) (pp. 01-05). IEEE.
18. Yakubdjanovna, I. D., Bakhtiyarovich, N. N., & Iqbol Ubaydullayevna, X. (2020, November). Implementation of intercorporate correlation of information security messages and audits. In 2020 International Conference on Information Science and Communications Technologies (ICISCT) (pp. 1-4). IEEE.
19. Cohen, M. I., Bilby, D., & Caronni, G. (2011). Distributed forensics and incident response in the enterprise. digital investigation, 8, S101-S110.
20. Mrdovic, S., Huseinovic, A., & Zajko, E. (2009, October). Combining static and live digital forensic analysis in virtual environment. In 2009 XXII International Symposium on Information, Communication and Automation Technologies (pp. 1-6). IEEE.
21. Hay, B., Bishop, M., & Nance, K. (2009). Live analysis: Progress and challenges. IEEE Security & Privacy, 7(2), 30-37.
22. Wang, L., Zhang, R., & Zhang, S. (2009, December). A model of computer live forensics based on physical memory analysis. In 2009 First International Conference on Information Science and Engineering (pp. 4647-4649). IEEE.
23. Alazab, M., Venkatraman, S., & Watters, P. (2009, June). Digital forensic techniques for static analysis of NTFS images. In Proceedings of ICIT2009, Fourth International Conference on Information Technology, IEEE Xplore.
24. Sherzod Rajaboevich, G., Dilmurod Gulamovich, A., & Nurbek Bakhtiyorovich, N. (2019). Method for determination of the probabilities of functioning states of information of protection on cloud

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 03 ISSUE 06 Pages: 63-71
SJIF IMPACT FACTOR (2021: 5.478) (2022: 5.636) (2023: 6.741)
OCLC – 1368736135

computing. International Journal of Mechanical Engineering and Technology, 10(3).

25. Safoev, N., and J. C. Jeon. "Cell interaction based QCA multiplexer for complex circuit design." Advanced Science Letters 23.10 (2017): 10097-10101.

26. Shakarov, M., Safoev, N., & Nasrullaev, N. (2022). Обеспечение безопасности интернет вещей в промышленности 4.0 с использованием WAF. Research and Education, 1(9), 386-393.

27. Насруллаев, Н., Муминова, С., Сейдуллаев, М., & Сафоев, Н. (2022). Внедрение DMZ для повышения сетевой безопасности веб-тестирования. Scientific Collection «InterConf», (110), 641-649.

28. Rajaboevich, G. S., Baxtiyorovich, N. N., & Komilovich, T. S. (2021, November). A model for preventing malicious traffic in DNS servers using machine learning. In 2021 International Conference on Information Science and Communications Technologies (ICISCT) (pp. 1-4). IEEE.

29. Safoev, N., and J. C. Jeon. "Low complexity design of conservative QCA with two-pair error checker." Advanced Science Letters 23.10 (2017): 10077-10081.

30. Rajaboevich, G. S., Baxtiyarovich, N. N., & Salimovna, F. D. (2020, November). Methods and intelligent mechanisms for constructing cyberattack detection components on distance-learning systems. In 2020 International Conference on Information Science and Communications Technologies (ICISCT) (pp. 1-6). IEEE.