Access Control List Provides Security in Network

Chate A.B.
PG Student
Dept of CNE
M.B.E.S.C.O.E.Ambajogai

Chirchi V.R.
Asst.Professor
Dept of CNE
M.B.E.S.C.O.E. Ambajogai

ABSTRACT

A significant component representing network security is access control list inspects values of every packet's field and come to a decision how to implement the network policy. Real-life access control list are naturally four dimensional over fields of four packets such as: IP address of source, destination, port number of destination and type of protocol. In several access control list, the source and destination port number fields make use of a range field constraint while the internet protocol address of source and destination and protocol type fields make use of a prefix or else ternary field constraint. Compression of access control lists is functional for system management of network and optimization for the reason that diminishing large access control lists rule sets to a great extent reduces the difficulty of supervising and optimizing configurations of network. Due to an augment in Internet applications besides enhancement in identified vulnerabilities and attacks, compression lists of access control may perhaps sanction users with outsized access control lists to make use of such devices and moreover this may develop into an increasingly critical concern intended for several users. An algorithm of polynomial time optimal was proposed for the weighted one-dimensional prefix compression problem of Access control lists by means of dynamic programming.

Keywords

Access control list, Dynamic programming, Access control lists compression, polynomial time optimal.

1. INTRODUCTION

Access control lists are organized at every points of entry connecting a concealed network and the outside Internet to supervise all packets of incoming and outgoing packets. A packet can be imagined as a tuple with a limited number of fields for instance IP addresses and port numbers of source/destination, and the type of protocol [4]. In an access control list, each rule has a predicate over header fields of several packets and a decision to be carried out upon the packets that equivalent the predicate. A rule that scrutinizes fields of d-dimensional can be analyzed as a d-dimensional entity. Real-life access control list are naturally four dimensional over fields of four packets such as: IP address of source, destination, port number of destination and type of protocol [8]. When a packet move towards to an access control list, the network device look out for the initial rule of highest priority that matches the packet and carry out the decision of that rule. Two access control list are equal if and only if they have the similar decision for each probable packet [13]. In the general problem of access control list compression given an access control list g, produce an additional access control list g' that is semantically corresponding to g but has the smallest possible number of rules and this was called an access control list compression [10]. Five versions of compression of access control list that be at variance only in the set-up of field constraints of the output access control list were focussed as: range access control list compression where constraints of field are specific by a range of integers; prefix access control list compression where constraints of field are specified by means of a string prefix; ternary access control list compression, where constraints of fields are specified by means of a ternary string; range-prefix access control list compression where several constraints of field are precise by ranges and the lasting field constraints are particular by means of prefix strings and range-ternary access control list compression where field constraints of field are particular by means of ranges and the enduring field constraints are specified by ternary strings. In numerous access control list, the source and destination port number fields make use of a range field constraint while the IP address of source and destination and protocol type fields make use of a prefix or else ternary field constraint [7] [12].

2. METHODOLOGY

Compression of access control lists is functional for system management of network and optimization for the reason that diminishing large access control lists rule sets to a great extent reduces the difficulty of supervising and optimizing configurations of network [1]. Tools of access control list compression on the whole and have been used for exploiting in quite a lot of well-known network management projects. Several network products have solid constraints on the rules that they hold up. Because access control lists are measured confidential due to concerns of security, it is tricky to obtain an outsized sample of real-life access control lists [5]. Compression of access control lists may possibly permit users with larger access control lists to still make use of such devices and this may turn out to be an increasingly vital concern intended for many users as size of access control lists has developed noticeably due to an augment in Internet applications in addition to an enhance in identified vulnerabilities and attacks [2].

Two access control list are equal if and only if they have the similar decision for each probable packet. An algorithm of polynomial time optimal was proposed for the weighted one-dimensional prefix compression problem of Access control lists by means of dynamic programming [6] [15]. This algorithm is on the basis of three explanations such as: initially the last rule of g can forever have its predicate altered to a defaulting predicate and this alteration is potential for the reason that g is absolute and as a result extending the assortment of the interval of last rule cannot modify the semantics of g. An added default rule to g can be appended devoid of altering the semantics of the consequential access control lists [9].

The structure which is imposed by the rules of prefix provides a proficient method to segregate the problem space into secluded sub problems. The solution of dynamic programming subdivides g all along boundaries of prefix until each prefix encloses only a particular decision [3] [14]. These adjoining prefixes are collective onto a negligible rule list of prefix that covers mutually prefixes and this procedure is continual until a single prefix and classifier we are left with. This explanation guides the entirely different formulation of dynamic programming. The NP-hard weighted one-dimensional ternary problem of access control lists compression was addressed by initially producing a finest weighted prefix access control lists and subsequently applying bit merging to additionally compress the prefix access control lists [11]. Bit merging was made used to hold more than two decisions and this algorithm is not definite to produce an optimal access control lists of weighted one-dimensional ternary.

3. RESULTS

It is tricky to obtain an outsized sample of real-life access control lists since access control lists are measured confidential due to concerns of security. Consider five size ACL. To deal with this concern and further estimating the performance of Real life access control lists compressor and access control lists compressor SYN which is a set of synthetic access control lists is generated. This ACL has five fields such as source IP, destination IP, source port, destination port and protocol. Where source IP= 0;destination IP=1;source port=2; destination port=3; protocol=4. For ACL(f) represent 5 permutations. It means 120 permutations(ρ) of five packet fields with these numbers. For any permutation ρ, ACL compressor is represented by AC_P where AC_P(f) denotes ACL produced by applying ACL compressor with ρ on f. for classification we use the best of AC[1]. For each classifier f belongs to set of ACL which is denoted by S.The order of impact variable present on the efficiency of ACL Compressor and one variable order performing ill for numerous classifiers are assessed. Fig.1 shows the range-prefix compression ratio of best of AC for each classifier.

It shows the classification of permutation on compression ratio is near about tenth of their original size. AC best achieves compression ratio near about 80% to 90% of classifiers which compress near about tenth of original size. For each permutation p, the average of compression is computed that AC_p attains on RL and exhibit the growing percentage graph. The average compression ratio of ACL is fall between 57% to 71%. shown in fig2.Ttotal range-prefix ratios of compression is shown in fig3. Where AC_p indicates access control lists Compressor by means of permutation p and RL is selected from a larger set of real-life access control lists obtained from a variety of network service providers. When 120 permutations try in different variable the total ratio of compression is fall between the range 58% to 84%. Variable order does considerably manipulate the efficiency of access control lists Compressor over several of the variable orders are very effectual. For compressing classifiers it takes few minutes for that, measure the complexity of classifiers. ACL compressor spend per nodes increases in roughly a linear fashion with the classifies complexity which is measured by the total number of nodes. in fig.4 shows execution time of total nodes per node.

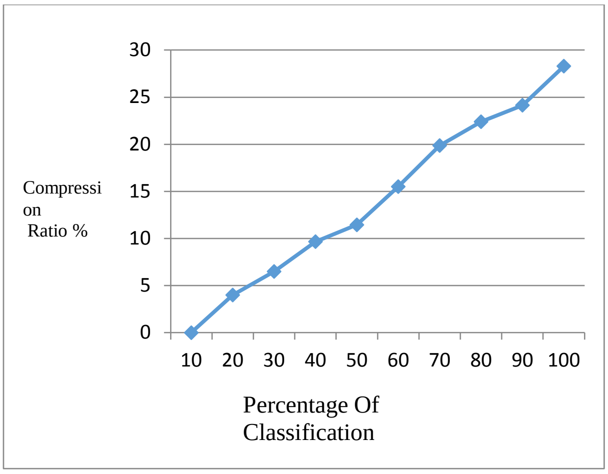

Fig. 1.Range-Prefix compression ratios RL

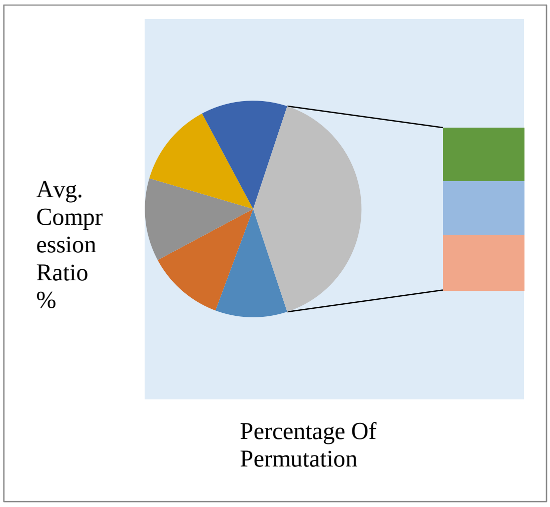

Fig 2: Range-prefix average compression ratio for ACp for RL

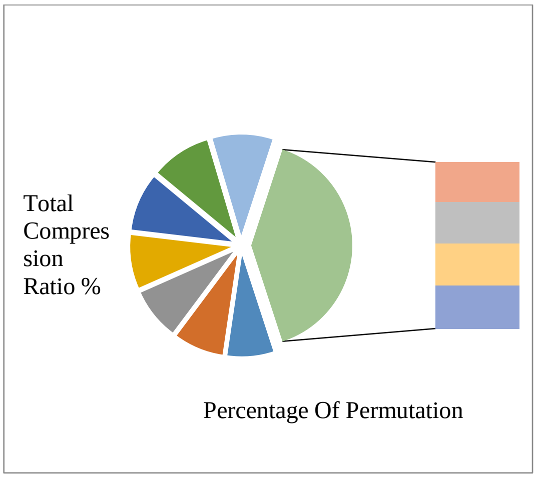

Fig 3: An overview total range-prefix compression ratios that ACp achieves on RL.

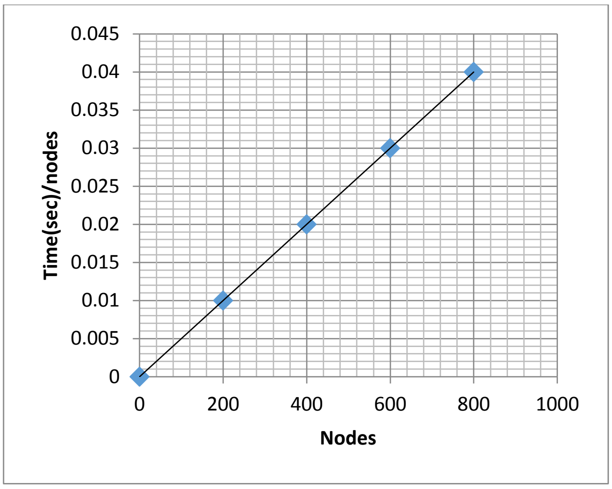

Fig4: Execution time per node to total node size

4. CONCLUSION

Compression of access control lists is functional for system management of network and optimization for the reason that diminishing large access control lists rule sets to a great extent reduces the difficulty of supervising and optimizing configurations of network. Tools of access control list compression on the whole and have been used for exploiting in quite a lot of well-known network management projects. An algorithm of polynomial time optimal was proposed for the weighted one-dimensional prefix compression problem of Access control lists by means of dynamic programming. The NP-hard weighted one-dimensional ternary problem of access control lists compression was addressed by initially producing a finest weighted prefix access control lists and subsequently applying bit merging to additionally compress the prefix access control lists. Access control lists are measured confidential due to concerns of security, it is tricky to obtain an outsized sample of real-life access control lists. To deal with this concern and further estimating the performance of access control lists compressor SYN, a set of synthetic access control lists of seven sizes was generated.

5. REFERENCES

[1] A.X Liu , E.Torng, and C.R. Meiners, ”Compressing Network Access Control List” ,IEEE Transactions On Parallel and Distributed System, vol.22, pp.1969-1977,Dec.2011

[2] A.X. Liu and M.G. Gouda, “Complete Redundancy Detection in Firewalls,” Proc. 19th Ann. IFIP Conf. Data and Applications Security, pp. 196-209, Aug. 2005

[3] D. Rovniagin and A. Wool, “The Geometric Efficient Matching Algorithm for Firewalls,” technical report, http://www.eng. tau.ac.il/yash/ees2003-6.ps, July 2003.

[4] D.A. Applegate, G. Calinescu, D.S. Johnson, H. Karloff, K. Ligett, and J. Wang, “Compressing Rectilinear Pictures and Minimizing Access Control Lists,” Proc. ACM-SIAM Symp. Discrete Algorithms (SODA), Jan. 2007.

[5] Y.-W.E. Sung, X. Sun, S.G. Rao, G.G. Xie, and D.A. Maltz, “Towards Systematic Design of Enterprise Networks,” IEEE Trans. Networking, vol. 19, no. 3, pp. 695-708, June 2011.

[6] A.X. Liu and M.G. Gouda, “Complete Redundancy Removal for Packet Classifiers in TCAMs,” IEEE Trans. Parallel and Distributed Systems, vol. 21, no. 4, pp. 424-437, Apr. 2010.

[7] Q. Dong, S. Banerjee, J. Wang, D. Agrawal, and A. Shukla, “Packet Classifiers in Ternary CAMs Can Be Smaller,” Proc. ACM Joint Int’l Conf. Measurement and Modeling of Computer Systems (SIGMETRICS), pp. 311-322, 2006.

[8] A.X. Liu, Y. Zhou, and C.R. Meiners, “All-Match Based Complete Redundancy Removal for Packet Classifiers in TCAMs,” Proc. IEEE INFOCOM, Apr. 2008.

[9] M.G. Gouda and A.X. Liu, “Firewall Design: Consistency, Completeness and Compactness,” Proc. IEEE 24th Int’l Conf. Distributed Computing Systems, pp. 320-327, Mar. 2004.

[10] C.R. Meiners, A.X. Liu, and E. Torng, “Bit Weaving: A Non-Prefix Approach to Compressing Packet Classifiers in TCAMs,” Proc. IEEE Int’l Conf. Network Protocol (ICNP), 2009.

[11] A.X. Liu, C.R. Meiners, and E. Torng, “TCAM Razor: A Systematic Approach towards Minimizing Packet Classifiers in TCAMs,” IEEE Trans. Networking, vol. 18, no. 2, pp. 490-500, Apr. 2010.

[12] M.G. Gouda and A.X. Liu, “Structured Firewall Design,” Computer Networks: The Int’l J. Computer and Telecomm. Networking, vol. 51, no. 4, pp. 1106-1120, Mar. 2007.

[13] Y.-W. E. Sung, X. Sun, S.G. Rao, G.G. Xie, and D.A. Maltz, “Towards Systematic Design of Enterprise Networks,” Proc. ACM CoNEXT Conf., 2008.

[14] A.X. Liu and M.G. Gouda, “Diverse Firewall Design,” IEEE Trans. Parallel and Distributed Systems, vol. 19, no. 8, pp. 1237- 1251, Sept. 2008.

[15] M. Yu, J. Rexford, M.J. Freedman, and J. Wang, “Scalable Flow- Based Networking with DIFANE,” Proc. ACM SIGCOMM, 2010