

A Heuristic Approach For Firewall Policy Optimization

El-Alfy, ESM

**IEEE, 9TH INTERNATIONAL CONFERENCE ON ADVANCED COMMUNICATION
TECHNOLOGY:**

TOWARD NETWORK INNOVATION BEYOND EVOLUTION, VOLS 1-3; pp: 1782-1787;

Vol: ##

King Fahd University of Petroleum & Minerals

<http://www.kfupm.edu.sa>

Summary

A primary goal of this paper is to develop a heuristic approach based on genetic algorithms to enhance the firewall performance. Typical firewall policies may have thousands of rules and determining an optimal rule order that minimizes the average number of rule comparisons while maintaining the policy integrity is proven to be NP-hard. This problem is formulated as a binary integer program for which an optimal solution is obtained using the branch-and-bound technique. Then, an alternative solution approach is devised based on genetic algorithms. Several experiments are conducted to evaluate the effectiveness of the proposed approach as compared to other rule-ordering techniques. Empirical results show the potential and flexibility of the proposed approach.

References:

1. ADAMIC L, 2002, GLOTTOMETRICS, P143
2. ALSHAER E, 2003, P IEEE IFIP INT MAN, P17
3. ALSHAER E, 2005, IEEE J SEL AREA COMM, V23, P2069
4. BARTAL Y, 2004, ACM T COMPUT SYST, V22, P381
5. BELLOVIN SM, 1994, IEEE COMMUN MAG, V32, P50
6. FULP E, 2005, P 9 IFIP IEEE INT S
7. FULP EW, 2005, P 10 IEEE S COMP COM, P434
8. GEN M, 2000, GENETIC ALGORITHMS E
9. GOUDA MG, 2004, P 24 IEEE INT C DIST, P320
10. HAMED H, 2006, P INFOCOM APR
11. HAZELHURST S, 2000, P INT C DEP SYST NET, P576
12. MAYER A, 2000, P IEEE S SECUR PRIV, P177

13. NEMHAUSER G, 1988, INTEGER COMBINATORIA
14. PREISS B, 1999, DATA STRUCTURES ALGO
15. QIU L, 2001, P 9 INT C NETW PROT, P241
16. YAMADA T, 1997, P MOD HEUR DEC SUPP
17. YUAN L, 2006, P IEEE S SEC PRIV MA
18. ZALENSKI R, 2002, IEEE POTENTIALS, V21, P24

For pre-prints please write to: abstracts@kfupm.edu.sa