# Some Experimental Results About Security Solutions Against DDoS Attacks

In: Proceedings of the International Symposium on Signals, Circuits and Systems (ISSCS 2013), 11 - 12 July, 2013, Iasi, Romania, IEEE Catalog Number: CFP13816-CDR, ISBN: 978-1-4673-6141-5,
IEEEXplore, INSPEC (Accession Number: 13879788), DOI: 10.1109/ISSCS.2013.6651193.

Eugen Petac[1], Abdel Rahman Alzoubaidi[2], Petrut Duma [3]
[1] Faculty of Mathematics and Computer Science, "Ovidius" University of Constanta, Constanta, Romania
epetac@univ-ovidius.ro
[2] Department of Computer Engineering, Al Balqa Applied University (APU), Kingdom of Jordan
alzoubaidi@bau.edu.jo
[3]Faculty of Electronics, Telecommunications and Information Technology, Technical University "Gh. Asachi" Iasi, Romania
pduma@etti.tuiasi.ro

***Abstract*— One of the most currently important security problems on the Internet network is Distributed Denial of Service (DDoS) attacks. There are many solutions [1], [2] for analysis and protection against DDoS attacks at the terminal equipment level (system client, server system), but there is still no universally valid solution for any type of DDoS attack, at the network level. Our proposed method is based on the results of informational correlation [3] to the statistical control study, considering the three partitions of traffic flow defined in [4]. In the second part of the paper we present the technologies and the software solutions we used for the development and implementation of a monitoring application, identification and filtering of DDoS attacks. The theoretical issues that concern the proposed method are presented in the third part of the paper. The application testing made in a virtual and in a real environment is presented in the fourth part of the paper.**

## I. INTRODUCTION

## II. SYSTEM OVERVIEW

## III. SOME THEORETICAL ASPECTS

## IV. EXPERIMENTAL RESULTS

## REFERENCES

[1] B. Xiao, W. Chen, and Y. He, "A novel technique for detecting DDoS attacks at its early stage, " ISPA'04 Proceedings of the Second international conference on Parallel and Distributed Processing and Applications, Springer-Verlag Berlin, Heidelberg, pp. 825-834, 2004

[2] R. Dobbins, and C. Morales, " Worldwide Infrastructure Security Report, " Arbor Networks, vol VII, Massachusetts, USA, 2011.

[3] O. Onicescu, V. Stefănescu, Elements of informational statistics with applications, Bucharest, Technical Press. , 1979.

[4] J. Cheng, B. Zhang, J. Yin, Y. Liu, and Z. Cai, "DDoS Attack Detection Using Three-State Partition Based on Flow Interaction, " FGIT-SecTech, Communications in Computer and Information Science, vol. 58, Springer, pp.176-184, 2009.

[5] C. Douligeris and A. Mitrokotsa, "DDoS attacks and defense mechanisms: classification and state-of-the-art, " Computer Networks, vol. 44, Elsevier B.V., pp. 643–666, 2004.

[6] K. Sourav and D. Prasad Mishra, "DDoS detection and defense: client termination approach, " CUBE '12 Proceedings of the CUBE International Information Technology Conference, ACM New York, NY, USA, pp.749-752, 2012.

[7] J. Roman, B. Radek, V.Radek, and S. Libor, "Launching distributed denial of service attacks by network protocol exploitation, " AICT'11 Proceedings of the 2nd international conference on Applied informatics and computing theory, pp. 210-216, 2011.

[8] R. Anderson, Network Attack and Defense in Security Engineering: A Guide to Building Dependable Distributed Systems, Wiley Publishing Inc., Indianapolis, Indiana, USA 2008, pp. 633-678.

[9] E. Unrein, D. Fish, J. Boeker, W. Sun, "Living in Denial - A Comparison of Distributed Denial of Service Mitigation Methods, " Issues in Information Systems, vol. 13, Issue 1, pp.190-198, 2012.

[10] K. Scarfone, P. Mell, Guide to Intrusion Detection and Prevention Systems (IDPS), NIST Special Publication 800-94, National Institute of Standards and Technology, Gaithersburg, USA, 2007.

[11] M. Alenezi, M. J. Reed, "Methodologies for detecting DoS/DDoS attacks against network servers, " , The Seventh International Conference on Systems and Networks Communications ICSNC 2012, Lisbon, Portugal, pp. 92-98, November 2012.

[12] N. Naoumov and K. Ross, Exploiting P2P Systems for DDoS Attacks, Proc. of INFOSCALE, 2006.

[13] ITU – Free statistics, International Telecomunication Union, Available: http://www.itu.int/ITU-D/ict/statistics/ [February 5, 2013].

[14] BoNeSi - Botnet Network Simulator tool, Apache License, Version 2.0 , Available: http://code.google.com/p/bonesi/ [February 5, 2013].

[15] I. Beijnum, BGP - Building Reliable Networks with the Border Gateway Protocol, O'Reilly Media, USA, 2002.

[16] Cacti - Network Management Suystem tool, GNU General Public License, Available: http://www.cacti.net/ [February 5, 2013].

[17] RRDtool, GNU General Public License, Available: http://oss.oetiker.ch/rrdtool/ [February 5, 2013].

[18] SmokePing, GNU General Public License, Available: http://oss.oetiker.ch/smokeping/ [February 5, 2013].

[19] GNS3 - Graphical Network Simulator, Available: http://www.gns3.net, [February 5, 2013].

[20] Remotely Triggered Black Hole Filtering—Destination Based And Source Based, White Paper, Cisco Systems 2005, http://www.cisco.com/web/about/security/intelligence/blackhole.pdf

[21] H. Liu and M. S. Kim, "Real-Time Detection of Stealthy DDoS Attacks Using Time-Series Decomposition, " in Proceedings of IEEE International Conference on Communications 2010 , May 2010

[22] J. Hall and J. McAdams, Effective Perl Programming: Ways to Write Better, More Idiomatic Perl, Second edition, Addison-Wesley Professional, 2010.

[23] [25] E. L. Thompson and S. D. Nowicki, Professional PHP6, John Wiley & Sons, 2009.

[24] Libes, D., "Expect," Tcl/Tk Extensions, ed, Mark Harrison, O'Reilly & Associates, Inc., 1997.

[25] C. Flynt, Tcl/Tk A Developer's Guide, Academic Press Professional/Morgan Kaufman, 2003.