IEEE ISI 2008 Invited Talk (VI)

Real Time Intrusion Prediction, Detection and Prevention Programs

Dr. Ajith Abraham

Norwegian Center of Excellence, Center of Excellence for Quantifiable Quality of Service
Norwegian University of Science and Technology,
O.S. Bragstads plass 2E, N-7491 Trondheim, Norway
Phone (O): +47 73 59 27 06, Phone (M): +47 45 44 88 62
WWW: http://www.softcomputing.net
ajith.abraham@ieee.org, abraham.ajith@acm.org, ajith.abraham@theiet.org

Abstract

An Intrusion Detection Program (IDP) analyzes what happens or has happened during an execution and tries to find indications that the computer has been misused. In this talk, we present some of the challenges in designing efficient Intrusion Detection Systems (IDS) using nature inspired computation techniques, which could provide high accuracy, low false alarm rate and reduced number of features. Then we present some recent research results of developing distributed intrusion detection systems using genetic programming techniques. Further, we illustrate how intruder behavior could be captured using hidden Markov model and predict possible serious intrusions. Finally we illustrate the role of online risk assessment for intrusion prevention systems and some associated results.

References:

[1] Abraham A., Grosan C. and Martin-Vide C., Evolutionary Design of Intrusion Detection Programs, International Journal of Network Security, Vol.4, No.3, pp. 328-339, 2007.

[2] Chen Y., Abraham A. and Yang B., Hybrid Flexible Neural Tree Based Intrusion Detection Systems, International Journal of Intelligent Systems, John Wiley and Sons, USA, Volume 22, pp. 1-16, 2007.

[3] Abraham A., Jain R., Thomas J. and Han S.Y., D-SCIDS: Distributed Soft Computing Intrusion Detection Systems, Journal of Network and Computer Applications, Elsevier Science, Volume 30, Issue 1, pp. 81-98, 2007.

[4] Haslum K., Abraham A. and Knapskog S., DIPS: A Framework for Distributed Intrusion Prediction and Prevention Using Hidden Markov Models and Online Fuzzy Risk Assessment, Third International Symposium on Information Assurance and Security, IEEE Computer Society press, USA, ISBN 0-7695-2876-7, pp. 183-188, 2007.

Biography: Dr. Ajith Abraham received Ph.D. degree from Monash University, Australia. Currently he is a Visiting Professor in the Norwegian University of Science and Technology, Norway. His primary research interests are in computational intelligence with an application focus including network security, Web services, Web intelligence, multi criteria decision-making, data mining etc.

Dr. Ajith Abraham has authored/co-authored over 300 research publications in peer reviewed reputed journals, book chapters and conference proceedings of which five have won 'best paper' awards. He has given several plenary talks and conference tutorials. He is the editor-in-chief / co-editor in chief of three international scientific journals and also serves the editorial board of several reputed International journals. He has guest edited 23 special issues for International scientific journals. Since 2001, he is actively involved in the Hybrid Intelligent Systems (HIS) and the Intelligent Systems Design and Applications (ISDA) series of International conferences. He was the General Co-chair of the Third International Symposium on Information Assurance and Security (IAS'07), Manchester, UK; Seventh International Conference on Intelligent Systems Design and Applications (ISDA'07), Brazil; and the Program Chair/Co-Chair of the First European International Conference on Data Mining (EICDM'07), Lisbon; Second International Conference on Digital Information Management (ICDIM'07), France; Third International Conference on Next Generation Web Services Practices (NWeSP'07), Seoul; and The Seventh International Conference on Hybrid Intelligent Systems (HIS'07), Germany and 2007 IEEE/WIC/ACM International Conference on Web Intelligence, USA.

More information at: http://www.softcomputing.net