IP Multimedia Communications

ISBN : 978-93-80864-99-3

Year of Publication: 2011

Authors:

Raman Singh

Harish Kumar

R.K. Singla

{bibtex}ipmc012.bib{/bibtex}

Abstract

Soft computing techniques are widely used in malware detection in these days. These techniques have the ability of learning from the past incidences and can categories normal and abnormal behaviour. In this paper we have reviewed various soft computing techniques. A review of application of these soft-computing techniques in malware detection has also been presented in this paper. Despite so much research, techniques with good accuracy and low false alarm rate are still needs attention.

Reference

1. Won Kim n, Ok-RanJeong, Chulyun Kim and Jungmin So, “The dark side of the Internet : Attacks, costs and responses”, Elsevier’s Journal of Information Systems, Volume 36, Issue 3, May 2011, pp 675-705.
2. Faizal, M.A. Mohd, Z.M. Sahib, S. Robiah, Y. Siti, R.S. and Asrul, H.Y., “Time Based Intrusion Detection on Fast Attack for Network Intrusion Detection System”, Second International Conference on Network Applications Protocols and Services (NETAPPS), Kedah, Malaysia, 22-23 Sept. 2010, pp 148 - 152.
3. Dipankar Dasgupta, Senhua Yu and Fernando Nino, "Recent Advances in Artificial Immune Systems: Models and Applications Review", Journal of Applied Soft Computing, Volume 11, Issue 2, March 2011, pp 1574-1587.
4. Shelly Xiaonan Wu and Wolfgang Banzhaf," The use of computational intelligence in intrusion detection systems: A review", Elsevier’s Journal of Applied Soft Computing, volume 10, issue 1 , January 2010, pp 1-35.
5. Gulshan Kumar, Krishan Kumar and Monika Sachdeva , "The use of artificial intelligence based techniques for intrusion detection: a review", Journal of Artificial Intelligence Review, 2010, Volume 34, Number 4, pp 369-387.
6. Alice Este, Francesco Gringoli and Luca Salgarelli, "Support Vector Machines for TCP traffic classification", Journal of Computer Networks, Volume 53, Issue 14, 18 September 2009, pp 2476-2490.
7. Chet Langin and Shahram Rahimi, "Soft computing in intrusion detection: the state of the art", Journal of Ambient Intelligence and Humanized Computing, 2010, Volume 1, Number 2, pp 133-145.
8. Huwaida Tagelsir Elshoush and Izzeldin Mohamed Osman, “ Alert correlation in collaborative intelligent intrusion detection systems—A survey”, Elsevier’s Journal of Applied Soft Computing, volume 11, issue 7 , October 2011, pp 4349-4365.
9. Lanjia Wang, Zhichun Li, Yan Chen, Zhi (Judy) Fu, and Xing Li, " Thwarting Zero-Day Polymorphic Worms With Network-Level Length-Based Signature Generation", IEEE/ACM Transactions on networking, Vol. 18, No. 1, February 2010, pp 53-66.
10. Yong Tang, Bin Xiao and Xicheng Lu, "Signature Tree Generation for Polymorphic Worms", IEEE Transaction on computers, Vol. 60, No. 4, April 2011, pp 565-579.
11. Frederic Massicotte and Yvan Labiche, "Specification-Based Testing of Intrusion Detection Engines using Logical Expression Testing Criteria", 10th International Conference on Quality Software, 14-15 July 2010, Zhangjiajie, China , pp 102-111.
12. Asaf Shabtai, Eitan Menahem, and Yuval Elovici, "F-Sign: Automatic, Function-Based Signature Generation for Malware", IEEE Transaction on system, man and —Part C: Applications and Reviews, Vol. 41, No. 4, July 2011, pp 494-508.
13. Wojciech Tylman, " Misuse-based intrusion detection using Bayesian networks", Int. J. Critical Computer-Based Systems, Vol. 1, Nos. 1/2/3, 2010, pp 178-190.
14. Deguang Kong, Yoon-Chan, Jhi Tao Gong, Sencun Zhu, Peng Liu, and Hongsheng Xi, "SAS: semantics aware signature generation for polymorphic worm detection", International Journal of Information Security, Online First, 21 May 2011 and Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, 1, Volume 50,

Security and Privacy in Communication Networks, Part 1, pp 1-19.

15. Inho Kang and Myong K.," JeongA differentiated one-class classification method with applications to intrusion detection", Expert Systems with Applications, In Press, Uncorrected Proof, Available online 6 July 2011, No. of pp 7.

16. Natalia Stakhanova, Samik Basu and Johnny Wong, "On the symbiosis of specification-based and anomaly-based detection", Elsevier's journal of Computers & Security, Volume 29, Issue 2, March 2010, pp 253-268.

17. Xin Xu, "Sequential anomaly detection based on temporal-difference learning: Principles, models and case studies", Elsevier's Journal of Applied Soft Computing, Volume 10, Issue 3, June 2010, pp 859-867.

18. Francesco Palmieri and Ugo Fiore, "Network anomaly detection through nonlinear analysis ", Elsevier's Journal of Computers & Security, Volume 29, Issue 7, October 2010, pp 737-755.

19. Yi Xie and Shun-Zheng Yu, "A Large-Scale Hidden Semi-Markov Model for Anomaly Detection on User Browsing Behaviors", IEEE/ACM Transaction on networking, Vol. 17, No. 1, February 2009, pp 54-65.

20. Ioannis Ch. Paschalidis and Georgios Smaragdakis, "Spatio-Temporal Network Anomaly Detection by Assessing Deviations of Empirical Measures", IEEE/ACM Transaction on networking, Vol. 17, No. 3, June 2009, pp 685-697.

21. Johannes Kinder, Stefan Katzenbeisser, Christian Schallhart, and Helmut Veith, "Proactive Detection of Computer Worms Using Model Checking", IEEE Transaction on dependable and secure computing, Vol. 7, No. 4, October-December 2010, pp 424-438.

22. Nan Zhang, Wei Yu, Xinwen Fu, and Sajal K. Das, "Maintaining Defender's Reputation in Anomaly Detection Against Insider Attacks", IEEE Transaction on system, man and cybernetics—Part B: Cybernetics, Vol. 40, NO. 3, June 2010, pp 597-611.

23. Satnam Singh, Haiying Tu, William Donat, Krishna Pattipati and Peter Willett, "Anomaly Detection via Feature-Aided Tracking and Hidden Markov Models", IEEE Transactions on system, man and cybernetics—Part A: System and humans, VOL. 39, NO. 1, January 2009, pp 144-159.

24. Andreas Kind, Marc Ph. Stoecklin, and Xenofontas Dimitropoulos, "Histogram-Based Traffic Anomaly Detection" IEEE Transaction on network service management, Vol. 6, No. 2, June 2009, pp 110-121.

25. Vasilis A. Sotiris, Peter W. Tse, and Michael G. Pecht, "Anomaly Detection Through a Bayesian Support Vector Machine", IEEE Transaction on reliability, Vol. 59, No. 2, June 2010, pp 277-286.

26. Gautam Thatte, Urbashi Mitra, and John Heidemann, "Parametric Methods for Anomaly Detection in Aggregate Traffic" IEEE/ACM Transaction on networking, Vol. 19, No. 2, April 2011 pp 512-525.

27. Chi-Yuan Chen, Kai-Di Chang, and Han-Chieh Chao, "Transaction-Pattern-Based Anomaly Detection Algorithm for IP Multimedia Subsystem" IEEE Transactions on information forensics and security, Vol. 6, No. 1, Msrch 2011, pp 152-161.

28. Fu-Hau Hsu, Chang-Kuo Tso, Yi-Chun Yeh, Wei-Jen Wang, and Li-Han Chen, "BrowserGuard: A Behavior-Based Solution to Drive-by-Download Attacks" IEEE Journal on selected areas in communications, Vol. 29, No. 7, August 2011, pp 1461-1468.

29. P. Garcıa-Teodoro, J. Dıaz-Verdejo, G. Macia-Fernandez, and E. Vazquez, "Anomaly-based network intrusion detection: Techniques, systems and challenges" Elsevier's

journal of Computers & Security, Volume 28, Issues 1-2, February-March 2009, pp 18-28.

30. Prasanta Gogoi, B Borah and D K Bhattacharyya, "Anomaly Detection Analysis of Intrusion Data using Supervised & Unsupervised Approach",Journal of Convergence Information Technology Volume 5, Number 1, February 2010, pp 95-110.

31. Dai Geng and Thmohiro Odaka, Jousuke Kuroiwa and Hisakazu Ogura, "An N-Gram and STF-IDF model for masquerade detection in a UNIX environment", Journal in Computer Virology, 2011, Volume 7, Number 2, pp 133-142.

32. Chunfu Jia and Feng Yang, "An intrusion detection method based on hierarchical hidden Markov models", Wuhan University Journal of Natural Sciences, 2007, Volume 12, Number 1, pp 135-138.

33. Davide Ariu, Roberto Tronci and Giorgio Giacinto, " HMMPayl: An intrusion detection system based on Hidden Markov Models", Elsevier's Journal of Computers & Security, Volume 30, Issue 4, June 2011, pp 221-241.

34. Wael Khreich, Eric Granger, Ali Miri, and Robert Sabourin, "Adaptive ROC-based ensembles of HMMs applied to anomaly detection", Elsevier's journal of Pattern Recognition, Volume 45, Issue 1, January 2012, pp 208-230.

35. Federico Maggi, Matteo Matteucci and Stefano Zanero, " Reducing false positives in anomaly detectors through fuzzy alert aggregation", Elsevier's journal of Information Fusion, Volume 10, Issue 4, October 2009, pp 300-311.

36. Gang Wang, Jinxing Hao, Jian Ma and Lihua Huang, " A new approach to intrusion detection using Artificial Neural Networks and fuzzy clustering", Elsevier's journal of Expert Systems with Applications, Volume 37, Issue 9, September 2010, pp 6225-6232.

37. Xuxian Jiang and Xingquan Zhu, " vEye: behavioral footprinting for self-propagating worm detection and profiling", Journal of Knowledge and Information Systems, 2009, Volume 18, Number 2, pp 231-262.

38. Gulshan Kumar, Krishan Kumar and Monika Sachdeva, " The use of artificial intelligence based techniques for intrusion detection: a review", Journal of Artificial Intelligence Review, 2010, Volume 34, Number 4, pp 369-387.

39. Siva S. Sivatha Sindhu, S. Geetha and A. Kannan, " Decision tree based light weight intrusion detection using a wrapper approach", Journal of Expert Systems with Applications, In Press, Corrected Proof, Available online 12 July 2011. No. of pp 13.

40. Chih-Fong Tsai and Chia-Ying Lin, " A triangle area based nearest neighbors approach to intrusion detection", Elsevier's Journal of Pattern Recognition, Volume 43, Issue 1, January 2010, pp 222-229.

41. Ming-Yang Su, " Using clustering to improve the KNN-based classifiers for online anomaly network traffic identification", Journal of Network and Computer Applications, Volume 34, Issue 2, March 2011, pp 722-730.

42. Ming-Yang Su, "Real-time anomaly detection systems for Denial-of-Service attacks by weighted k-nearest-neighbor classifiers", Elsevier's Journal of Expert Systems with Applications, Volume 38, Issue 4, April 2011, pp 3492-3498 .

43. Seyed Hossein Ahmadinejad, Saeed Jalili and Mahdi Abadi, "A hybrid model for correlating alerts of known and unknown attack scenarios and updating attack graphs" Elsevier's journal of Computer Networks, Volume 55, Issue 9, 23 June 2011, pp 2221-2240.

44. Bharanidharan Shanmugam and Norbik Bashah Idris, "Improved Intrusion Detection System using Fuzzy Logic for Detecting Anamoly and Misuse type of Attacks", International Conference of Soft Computing and Pattern Recognition, Malacca, Malaysia, December 4-7,

2009, pp 212-217.

45. Yu-Xin, Min Xiao and Ai-Wu Liu, “ Research and implementation on snort based gybrid intrusion detection system”, Proceedings of the Eighth International Conference on Machine Learning and Cybernetics, Baoding, 12-15 July 2009, pp 1414-1418.

46. Jie Yang, Xin Chen, Xudong Xiang and Jianxiong Wan, "HIDS-DT: An Effective Hybrid Intrusion Detection System Based on Decision Tree", International Conference on Communications and Mobile Computing, April 12-14, 2010, Shenzhen Guest House, Shenzhen, China, pp 70-75.

47. S. I. Handra and H. Ciocârlie, "Anomaly Detection in Data Mining. Hybrid Approach between Filtering-and-Refinement and DBSCAN" 6th IEEE International Symposium on Applied Computational Intelligence and Informatics • May 19–21, 2011 • Timioara, Romania, pp 75-83. Timioara, Romania, pp 75-83.

Index Terms

Computer Science Communications

Key words

malware

malware detection

soft computing

machine learning

anomaly detection