{tag} {/tag}International Journal of Computer Applications
Foundation of Computer Science (FCS), NY, USA

Volume 173
-
Number 1

Year of Publication: 2017

Authors:

Hossein Shapoorifard, Pirooz Shamsinejad

10.5120/ijca2017914340

{bibtex}2017914340.bib{/bibtex}

Abstract

These days, with the tremendous growth of network-based service and shared information on networks, the risk of network attacks and intrusions increases too, therefore network security and protecting the network is getting more significance than before. Intrusion Detection System (IDS) is one of the solutions to detect attacks and anomalies in the network. The ever rising new intrusion or attack types causes difficulties for their detection, therefore Data mining techniques has been widely applied in network intrusion detection systems for extracting useful knowledge from large number of network data to detect intrusions. Many clustering and classification algorithms are used in IDS, therefore improving the functionality of these algorithms will improve IDS performance. This paper focuses on improving KNN classifier in existing intrusion detection task which combines K-MEANS clustering and KNN classification.

References

1. J. Kim, P. J. Bentley, U. Aickelin, J. Greensmith, G. Tedesco, and J. Twycross, “Immune

system approaches to intrusion detection - A review," Natural Computing, vol. 6, no. 4. pp. 413–466, 2007.

2. M. Gupta, "Hybrid Intrusion Detection System: Technology and Development," Int. J. Comput. Appl., vol. 115, no. 9, pp. 975–8887, 2015.

3. M. Panda, A. Abraham, and M. R. Patra, "Procedia Engineering International Conference on Communication Technology and System Design 2011 Detection," vol. 0, no. 2011, 2012.

4. E. Cloe and R. Krutz, Network Security Bible, vol. 1542, no. 9. 2015.

5. R. M. Elbasiony, E. A. Sallam, T. E. Eltobely, and M. M. Fahmy, "A hybrid network intrusion detection framework based on random forests and weighted k-means," Ain Shams Eng. J., vol. 4, no. 4, pp. 753–762, 2013.

6. V. Golmah, "An Efficient Hybrid Intrusion Detection System based on C5. 0 and SVM.," Int. J. Database Theory Appl., vol. 7, no. 2, pp. 59–70, 2014.

7. J. Patel and K. Panchal, "Effective Intrusion Detection System using Data Mining Technique," vol. 2, no. 6, pp. 1869–1878, 2015.

8. W. C. Lin, S. W. Ke, and C. F. Tsai, "CANN: An intrusion detection system based on combining cluster centers and nearest neighbors," Knowledge-Based Syst., vol. 78, no. 1, pp. 13–21, 2015.

9. M. K. Siddiqui and S. Naahid, "Analysis of KDD CUP 99 Dataset using Clustering based Data Mining," Int. J. Database Theory Appl., vol. 6, no. 5, pp. 23–34, 2013.

10. L. Dhanabal and S. P. Shantharajah, "A Study on NSL-KDD Dataset for Intrusion Detection System Based on Classification Algorithms," Int. J. Adv. Res. Comput. Commun. Eng., vol. 4, no. 6, pp. 446–452, 2015.

11. P. Mishra, E. S. Pilli, V. Varadharajan, and U. Tupakula, "Intrusion detection techniques in cloud environment: A survey," J. Netw. Comput. Appl., vol. 77, pp. 18–47, 2017.

12. M. Dashtban and M. Balafar, "Gene selection for microarray cancer classification using a new evolutionary method employing artificial intelligence concepts," Genomics, 2017.

13. A. Taheri and M. Shamsfard, "SBUEI: results for OAEI 2012," in Proceedings of the 7th International Conference on Ontology Matching-Volume 946, 2012, pp. 189–196.

14. S. Olyaee, Z. Dashtban, and M. H. Dashtban, "Design and implementation of super-heterodyne nano-metrology circuits," Front. Optoelectron., vol. 6, no. 3, pp. 318–326, 2013.

15. M. H. Dashtban and P. Moradi, "A novel and robust approach for iris segmentation," Int. J. Comput., 2011.

16. A. Taheri and M. Shamsfard, "Instance coreference resolution in multi-ontology linked data resources," in Joint International Semantic Technology Conference, 2012, pp. 129–145.

17. A. Taheri and M. Shamsfard, "Mapping farsnet to suggested upper merged ontology," in Asia Information Retrieval Symposium, 2011, pp. 604–613.

18. M. Dashtban, M. Balafar, and P. Suravajhala, "Gene selection for tumor classification using a novel bio-inspired multi-objective approach," Genomics, 2017.

19. M. H. Dashtban, Z. Dashtban, and H. Bevrani, "A novel approach for vehicle license plate localization and recognition," Int. J. Comput. Appl., vol. 26, no. 11, 2011.

20. S. Olyaee, Z. Dashtban, M. H. Dashtban, and A. Najibi, "Hybrid analytical-neural network approach for nonlinearity modeling in modified super-heterodyne nano-metrology system," in Telecommunications (ConTEL), Proceedings of the 2011 11th International Conference on, 2011, pp. 525–530.

21. D. Faria et al., "AML results for OAEI 2015.," in OM, 2015, pp. 116–123.

22. H.-J. Liao, C.-H. R. Lin, Y.-C. Lin, and K.-Y. Tung, “Intrusion detection system: A comprehensive review,” J. Netw. Comput. Appl., vol. 36, no. 1, pp. 16–24, 2013.

23. H. Om and A. Kundu, “A hybrid system for reducing the false alarm rate of anomaly intrusion detection system,” in 2012 1st International Conference on Recent Advances in Information Technology, RAIT-2012, 2012, pp. 131–136.

24. W. Pu and W. Jun-qing, “Intrusion detection system with the data mining technologies,” in Communication {Software} and {Networks} ({ICCSN}), 2011 {IEEE} 3rd {International} {Conference} on, 2011, pp. 490–492.

25. D. M. Farid, N. Harbi, E. Bahri, M. Z. Rahman, and C. M. Rahman, “Attacks classification in adaptive intrusion detection using decision tree,” World Acad. Sci. Eng. Technol., vol. 63, no. 3, pp. 86–90, 2010.

26. M. Dhakar and A. Tiwari, “A New Model for Intrusion Detection based on Reduced Error Pruning Technique,” no. September, pp. 51–57, 2013.

27. A. P. Muniyandi, R. Rajeswari, and R. Rajaram, “Network anomaly detection by cascading k-Means clustering and C4.5 decision tree algorithm,” in Procedia Engineering, 2012, vol. 30, pp. 174–182.

28. G. Kim, S. Lee, and S. Kim, “A novel hybrid intrusion detection method integrating anomaly detection with misuse detection,” Expert Syst. Appl., vol. 41, no. 4 PART 2, pp. 1690–1700, 2014.

29. V. Jaiganesh, P. Sumathi, and S. Mangayarkarasi, “An analysis of intrusion detection system using back propagation neural network,” 2013 Int. Conf. Inf. Commun. Embed. Syst., pp. 232–236, 2013.

Index Terms

Computer Science Artificial Intelligence

Keywords

Intrusion Detection System; Data Mining; Network Security; Clustering; IDS system; K-MEANS; K- nearest neighbor; K- farthest neighbor; CANN.