{tag} {/tag}

IJCA Proceedings on National Conference on Innovative Paradigms in Engineering & Technology 2013

NCIPET2013 - Number 2

Year of Publication: 2013

Authors:
Sushilkumar Chavhan

Smita M. Nirkhi

R. V. Dharaskar

{bibtex}ncipet1331.bib{/bibtex}

Abstract

Anomaly detection techniques are widely used in a number of applications, such as, computer networks, security systems, etc. This paper describes and analyzes an approach to anomaly detection using self organizing map classification. We deal with the massive data volumes with the dynamic nature of day to day information networks. So it's difficult to identify the behavior of system. Visualization of data has ability to take into a massive volume of data. In

digital forensics self organizing map has high potential handle large data and observe the behavior of computer. This paper provides an overview of anomaly detection system which able to handle massive real data.

References

- Kohonen, T. 1990, "The self-organizing map", Proceedings of the IEEE, vol. 78, no. 9, pp. 1464-1480.
- B. K. L. Fei, J. H. P. Eloff, H. S. Venter and M. S. Olivier, 2005, "Exploring Data Generated by Computer Forensic Tools with SelfOrganising Maps" Advances in digital forensics, pp. 113-123. Springer.
- V. Chandola,A Banerjee and V. Kumar, July 2009, "Anomaly Detection –A Survey",ACM Computing Survay,vol. 41,no. 3, pp. 1-58.
- Dipankar Dasgupta and Nivedita Sumi Majumdar ,2002. Anomaly Detection in multimedia data using negative selection algorithm, CEC 02. Proceedings on Evolutionary Computation,
- Li Yao , Li ZhiTang, Liu Shuyu 2006. A Fuzzy Anomaly Detection for IPv6 ,SKG '06. Second International Conference on Semantics, Knowledge and Grid,
- Lv, Jun; Li, Xing; Ran, Congsen; Li, Tong. 2006. , A new algorithm for Network anomaly detection, International Multi-Conference on Computing in the Global Information Technology ICCGI 06
- Ning Chen; Xiao-su Chen; Bing Xiong; Hong-wei Lu, 2009, "An Anomaly Detection And Analysis Based on Corelation Coefficient Matrix",. International Conference on Scalable Computing and Communications; Eighth International Conference on Embedded Computing, EMBEDDEDCOM'09, SCALCOM-2009.
- Mian Zhang; Li Zhang, 2010, "Based On Pattern Discovery Network Anomaly Detection Algorithm" 5th International Conference on Computer Science and Education (ICCSE).
- Jinquan Zeng; Tao Li; Xiaojie Liu; Caiming Liu; Lingxi Peng; Feixian Sun, ICNC2007, "A Feedback Negative Selection Algorithm to Anomaly Detection", Third International Conference on Natural Computation.
- E. J. Palomo, J. North, D. Elizondo, R. M. Luque and T. atson,2011, "Visualisation Of Network Forensics Traffic Data With A Self-organising Map For Qualitative Features", Proceedings of International Joint Conference on Neural Networks, pp 1740-1247.
- Chi-Yuan Chen; Kai-Di Chang; Han-Chieh Chao, 2011, Transaction-Pattern-Based Anomaly Detection Algorithm for IP Multimedia Subsystem", IEEE Transactions on Information Forensics and Security, pp 152-161.
- Chee-Wooi Ten; Junho Hong; Chen-Ching Liu, 2011 "Anomaly Detection for Cybersecurity of the Substations", IEEE Transactions on Smart Grid, pp 865-873.
- Zhe Yao; Mark, P. ; Rabbat, M. ,2012, "Anomaly Detection Using Proximity Graph and PageRank Algorithm" IEEE Transactions on Information Forensics and Security, pp 1288-1300.
- Aye, T. T. , 2011, "Web log cleaning for mining of web usage patterns", 3rd

International Conference on Computer Research and Development (ICCRD).

- Ying Zhu, 2011, "Attack Pattern Discovery in Forensic Investigation of Network Attacks", IEEE journal on selected areas in communications, pp 1349-1357
- H. Günes Kayac?k, A. Nur Zincir-Heywood, 2006, "Using Self-Organizing Maps to Build an Attack Map for Forensic Analysis",ACM digital library.
- Correa, Renato Fernandes; Ludermir, Teresa Bernarda 2006, "A Hybrid SOM-Based Document Organization System". Ninth Brazilian Symposium on Neural Networks, SBRN '06.
- Kohonen, T. ; Kaski, S. ; Lagus, K. ; Salojarvi, J. ; Honkela, J. ; Paatero, V. ; Saarela, A. "Self Organization of a Massive Document Collection" , IEEE Transactions on Neural Network
- B. K. L. Fei , J. H. P. Eloff , M. S. Olivier , H. M. Tillwick , H. S. Venter, 2006, "Using Self Organizing Map for Behaviour Detection in computer forensics investigation" Proceedings of the Fifth Annual Information Security South Africa Conference.
- Smita. Nirkhi, 2010, "Potential use of Artificial Neural Network in Data Mining", International conference on Computer and Automation Engineering (ICCAE).
- Kevin Phillip Galloway, 2010, "Intrusion Behavior Detection Through Visualization", M. Sc. thesis.
- Lo?pez-Rubio, E. 2010, "Probabilistic Self-Organizing Maps for Continuous Data"Transactions on Neural Networks, IEEE, pp 1543 - 1554
- Nan Zhang; Wei Yu; Xinwen Fu; Das, S. K. , 2010, "Maintaining Defender's Reutation in Anomaly Detection Aginst Insider Attack", IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics, pp. 597-611.

Index Terms

Computer Science Anamoly Detection

Keywords

Digital Forensic Self Organizing Map (som) Anomaly Detection Visualization