

{tag}

{/tag}

International Journal of Computer Applications

© 2014 by IJCA Journal

Volume 105 - Number 10

Year of Publication: 2014

Authors:

D. P. Jeyepalan

E. Kirubakaran

10.5120/18410-9687

{bibtex}pxc3899687.bib{/bibtex}

Abstract

Detecting intrusions in a network is one of the major functionalities that cannot be overlooked. Even though the intrusion detection systems in networks tend to perform their best, the other side is always ahead conjuring new attacks every time. Further, detecting an attack earlier or at least as soon as the attack has occurred is the only way to counter it. Detecting it at a later point in time proves to be useless. But the current systems available are not able to live up to the needs of the real time scenario. This paper presents an Ant Colony Optimization based intrusion detection system that uses agents to perform the process of detection, storage and monitoring. The network is not considered as a whole, instead, it is divided into clusters and detection is performed on the nodes within the cluster alone. Hence the workload of the detection system is reduced considerably, providing faster results. Another added advantage is that all the agents can run in parallel, hence parallelized detection becomes possible. Experiments were carried out using multi core CPUs and many core GPUs and the comparison shows that the CPUs shows twice the increase in performance when compared to single core machines, while GPUs show thrice the increase in performance when compared to multi core CPUs.

Refer

ences

- VaibhavGowadia ,CsillaFarkas , Marco Valtorta. 2005 Paid: A probabilistic agent-based intrusion detection system. *Computers & Security* 24(7):529–545.
- Garcia-Teodoro, Pedro, et al. 2009 Anomaly-based network intrusion detection: Techniques, systems and challenges. *Computers& security* 28. 1: 18-28.
- Dasgupta, D. , et al. 2005. CIDS: An agent-based intrusion detection system. *Computers & Security* 24. 5: 387-398.
- Wang, Lingyu, Anyi Liu, and SushilJajodia. 2006 Using attack graphs for correlating, hypothesizing, and predicting intrusion alerts. *Computer communications* 29. 15: 2917-2933.
- P. Ammann, D. Wijesekera, S. Kaushik. 2002 Scalable, graph-based network vulnerability analysis, in: *Proceedings of the 9th ACM Conference on Computer and Communications Security (CCS'02)*, pp. 217–224.
- O. Sheyner, J. Haines, S. Jha, R. Lippmann, J. M. Wing. 2002. Automated generation and analysis of attack graphs, in: *Proceedings of the 2002 IEEE Symposium on Security and Privacy (S& P'02)*, pp. 273–284.
- D. P. Jeyepalan, E. Kirubakaran. 2014. A Co-operative Game Theoretic Approach to Improve the Intrusion Detection System in a Network using Ant Colony Clustering. *International Journal of Computer Applications*, Volume 87 - Number 14.
- Foschini, Luca, et al. 2008. A parallel architecture for stateful, high-speed intrusion detection. *Information Systems Security*. Springer Berlin Heidelberg, 203-220.
- Vasiliadis, Giorgos, Michalis Polychronakis, and Sotiris Ioannidis. 2011. MIDeA: a multi-parallel intrusion detection architecture. *Proceedings of the 18th ACM conference on Computer and communications security*. ACM.
- Abadeh, Mohammad Saniee, Jafar Habibi, and Emad Soroush. 2008. "Induction of Fuzzy Classification systems via evolutionary ACO-based algorithms. " *computer* 35: 37.
- Feng, Wenying, et al. 2014. Mining network data for intrusion detection through combining SVMs with ant colony networks. " *Future Generation Computer Systems* 37: 127-140.
- Koliass, Constantinos, Georgios Kambourakis, and M. Maragoudakis. 2011. Swarm intelligence in intrusion detection: A survey. *Computers& security* 30. 8: 625-642.
- Catania, Carlos A. , and Carlos García Garino. 2012. Automatic network intrusion detection: Current techniques and open issues. *Computers & Electrical Engineering* 38. 5: 1062-1072.
- Shamshirband, Shahaboddin, et al. 2013. An appraisal and design of a multi-agent system based cooperative wireless intrusion detection computational intelligence technique. *Engineering Applications of Artificial Intelligence* 26. 9: 2105-2127.
- Huang, Nen-Fu, et al. "A GPU-based multiple-pattern matching algorithm for network intrusion detection systems. " *Advanced Information Networking and Applications-Workshops*, 2008. AINAW 2008. 22nd International Conference on. IEEE, 2008.
- Vasiliadis, Giorgos, et al. "Regular expression matching on graphics hardware for intrusion detection. " *Recent Advances in Intrusion Detection*. Springer Berlin Heidelberg, 2009.
- Vokorokos, Liberios, Anton Baláž, and Branislav Madoš. "Intrusion detection architecture utilizing graphics processors. " *Acta Informatica Pragensia* 1. 1 (2013): 50-59.

- Jamshed, Muhammad Asim, et al. "Kargus: a highly-scalable software-based intrusion detection system." Proceedings of the 2012 ACM conference on Computer and communications security. ACM, 2012.

Computer Science

Index Terms

Security

Keywords

Intrusion detection; Parallelized ACO; Clustering; Cluster Head Selection; Agent based IDS