A body of work focuses on improving the scalability of IDSes by parallelizing IDSes with multi-thread [7], multi-core [14, 18] processing and cluster architecture [15]. Those existing work improves the capacity of the IDSes by employing more execution instances/threads. A another body of work focuses on improving the processing speed of a single IDS instance leveraging special hardware such as GPU [10, 16, 17]. Unlike our approach, which improves the capacity of IDSes by reducing the overall resource consumption of the whole system (thus with the same amount of resources, our approach gains greater capacity), those approaches enable greater capacity by exploiting more resources.

The work closest to our discussion is [8], which reduces the resource consumption by predicting the traffic patterns and selectively loading detection polices for IDSes. However, that work is limited to a single IDS instance and is not specific for high performance networks like the Science DMZs. We can employ the approach presented by this work to each of our IDS instances.

SciPass [4] presents an approach to secure the Science DMZ using OpenFlow and Bro. The authors employ an array of IDS instances to handle all flows. In contrast, our work filters out known valid flows with a lightweight detection system, reducing the number of flows being sent to the IDS instances. Our goal is to significantly reduce the resource consumption of the IDS instances.

5 CONCLUSION AND FUTURE WORK

We proposed a new approach to efficiently monitoring the traffic of Science DMZ based on side-channel features of flows. Our approach employs a lightweight detection system as a traffic filter, which significantly reduces the volume of traffic being processed by the IDS instances. We have designed and implemented a lightweight detection system based on the inter-packet timing feature. Our preliminary evaluation results demonstrated that our approach can achieve greater efficiency in CPU usage than traditional approaches.

As our future work, we will formalize the resource usage of our approach and conduct more comprehensive evaluations based on the formulas. In addition, we will include more side-channel features in the lightweight detection and employ more advanced machine learning techniques to achieve better detection accuracy, while ensuring sufficient efficiency.

ACKNOWLEDGMENTS

This work was partially supported by grants from National Science Foundation (NSF-OAC-1642143, NSF-CNS-1700499, and NSF-DGE-1723663).

REFERENCES

[1] 2015. CloudLab. http://www.cloudlab.us/. (2015).
[2] 2018. Snort. https://www.snort.org/. (2018).
[3] 2018. The Bro Network Security Monitor. https://www.bro.org/. (2018).
[4] Edward Balas and A Ragusa. 2014. SciPass: a 100Gbps capable secure Science DMZ using OpenFlow and Bro. In *Supercomputing 2014 conference (SC14)*.
[5] Prasad Calyam, Alex Berryman, Erik Saule, Hari Subramoni, Paul Schopis, Gordon Springer, Umit Catalyurek, and Dhabaleswar K Panda. 2014. Wide-area overlay networking to manage science DMZ accelerated flows. In *Computing, Networking and Communications (ICNC), 2014 International Conference on*. IEEE, 269–275.
[6] Eli Dart, Lauren Rotman, Brian Tierney, Mary Hester, and Jason Zurawski. 2014. The science dmz: A network design pattern for data-intensive science. *Scientific Programming* 22, 2 (2014), 173–185.
[7] Lorenzo De Carli, Robin Sommer, and Somesh Jha. 2014. Beyond pattern matching: A concurrency model for stateful deep packet inspection. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 1378–1390.
[8] Holger Dreger, Anja Feldmann, Vern Paxson, and Robin Sommer. 2008. Predicting the resource consumption of network intrusion detection systems. In *International Workshop on Recent Advances in Intrusion Detection*. Springer, 135–154.
[9] Aaron Gember-Jacobson, Raajay Viswanathan, Chaithan Prakash, Robert Grandl, Junaid Khalid, Sourav Das, and Aditya Akella. 2014. OpenNF: Enabling innovation in network function control. In *ACM SIGCOMM Computer Communication Review*, Vol. 44. ACM, 163–174.
[10] Muhammad Asim Jamshed, Jihyung Lee, Sangwoo Moon, Insu Yun, Deokjin Kim, Sungryoul Lee, Yung Yi, and KyoungSoo Park. 2012. Kargus: a highly-scalable software-based intrusion detection system. In *Proceedings of the 2012 ACM conference on Computer and communications security*. ACM, 317–328.
[11] George Khalil. 2015. Open Source IDS High Performance Shootout. https://www.sans.org/reading-room/whitepapers/intrusion/open-source-ids-high-performance-shootout-35772. (2015).
[12] C. Lu, J. M. Schwier, R. M. Craven, L. Yu, R. R. Brooks, and C. Griffin. 2013. A Normalized Statistical Metric Space for Hidden Markov Models. *IEEE Transactions on Cybernetics* 43, 3 (June 2013), 806–819. https://doi.org/10.1109/TSMCB.2012.2216872
[13] Shriram Rajagopalan, Dan Williams, Hani Jamjoom, and Andrew Warfield. 2013. Split/Merge: System Support for Elastic Execution in Virtual Middleboxes.. In *NSDI*, Vol. 13. 227–240.
[14] Robin Sommer, Vern Paxson, and Nicholas Weaver. 2009. An architecture for exploiting multi-core processors to parallelize network intrusion prevention. *Concurrency and Computation: Practice and Experience* 21, 10 (2009), 1255–1279.
[15] Matthias Vallentin, Robin Sommer, Jason Lee, Craig Leres, Vern Paxson, and Brian Tierney. 2007. The NIDS cluster: Scalable, stateful network intrusion detection on commodity hardware. In *International Workshop on Recent Advances in Intrusion Detection*. Springer, 107–126.
[16] Giorgos Vasiliadis, Spiros Antonatos, Michalis Polychronakis, Evangelos P Markatos, and Sotiris Ioannidis. 2008. Gnort: High performance network intrusion detection using graphics processors. In *International Workshop on Recent Advances in Intrusion Detection*. Springer, 116–134.
[17] Giorgos Vasiliadis, Michalis Polychronakis, and Sotiris Ioannidis. 2011. MIDeA: a multi-parallel intrusion detection architecture. In *Proceedings of the 18th ACM conference on Computer and communications security*. ACM, 297–308.
[18] Benjamin Wun, Patrick Crowley, and Arun Raghunth. 2009. Parallelization of Snort on a multi-core platform. In *Proceedings of the 5th ACM/IEEE Symposium on Architectures for Networking and Communications Systems*. ACM, 173–174.
[19] L. Yu, J. M. Schwier, R. M. Craven, R. R. Brooks, and C. Griffin. 2013. Inferring Statistically Significant Hidden Markov Models. *IEEE Transactions on Knowledge and Data Engineering* 25, 7 (July 2013), 1548–1558. https://doi.org/10.1109/TKDE.2012.93
[20] Nuyun Zhang, Hongda Li, Hongxin Hu, and Younghee Park. 2017. Towards Effective Virtualization of Intrusion Detection Systems. In *Proceedings of the ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization*. ACM, 47–50.
[21] X. Zhong, A. Ahmadi, R. Brooks, G. K. Venayagamoorthy, L. Yu, and Y. Fu. 2015. Side channel analysis of multiple PMU data in electric power systems. In *2015 Clemson University Power Systems Conference (PSC)*. 1–6. https://doi.org/10.1109/PSC.2015.7101704