Josh Hatfield

INFO-I 433 (Section 8027)

Professor Xing

2 May 2023

Efficient Detection and Comparative Performance of Machine Learning Intrusion Detection Systems

Section I: Introduction

Although machine learning, especially in relation to mechanisms like taint analysis for various library dependencies and the more recently pervasive use of anomaly-based intrusion detection, has had substantial research and implementation to better coalesce flexibility between network processes and applications' execution environments, more emphasis on efficient as well as comparative performance between machine learning algorithms may help us be able to offer better unification compared to the considerably differentiating intrusion detection systems (IDS) that exist today. If we can better propagate detection across the dependencies, networks, and servers that serve as imperative integrations for much of our world's multi-industry commerce, then we may be better equipped to do so through the fluidity and affordances of machine learning that may be lacking with signature and anomaly-based IDS. Ultimately, this will remain an interesting issue within the cybersecurity space since attackers are utilizing increasingly unconventional tools like artificial intelligence and IP spoofing, so having the means to address the parameters of machine learning for intrusion detection may help individuals, governments, and entities to be able to find a sufficient balance between runtime efficiency and mitigation efforts wherein time exists as a valuable asset within itself.

Section II: Approach

Due to the wide-ranging techniques elucidated within machine learning as a whole, the following sections enumerate important aspects of this technicality in relation to intrusion detection. Within Section III, I highlight three specific techniques and prior research for

addressing machine learning in the scope of efficient detection and comparative performance across multiple algorithms. Then, in Section IV, I provide three overarching suggestions for future work based on my interpretation and explication of the three existing solutions utilizing various sources. Lastly, in Section V, I offer some final insights regarding the philosophical ruminations of both the research and suggestions as they stand currently.

Section III: Existing Techniques / Solutions

Data Preprocessing and Feature Classification for Low Latency

While machine learning has generally become more proficient based on our understanding across the range of algorithms and less taxing computations in training data processing software to compare outcomes based on tuning for input functions, many anomaly-based IDS are lacking in their ability to detect intrusions within sensitive execution environments where applications need to be able to serve clientele quickly. Therefore, as described by Ahmad et al. (2022) within their journal article titled "Low-Latency Intrusion Detection Using a Deep Neural Network," given the scope of machine learning (and deep learning as a more granular subset of machine learning)—particularly with classifiers like Random Forest for tabulating importance scores of various training set indicators as parsed by the machine learning model—the concept of data preprocessing can eliminate the model's need to likewise parse through every byte of information passed from either the local execution environment or more commonly across the network when interacting across network packets.

Once the feature classification is tuned in correspondence to the most satisfactory comparisons for detection rate and false alarm rate, as with any IDS, the machine learning model applies the features to future models for more accurately predicting previous exploitations, regardless of the exact contingency of usage based on the feature classification (Ahmad et al., 2022). In the case of Ahmad et al.'s (2022) model, they not only achieved a variance of only 0.62% from the initial training accuracy of 98.88% to the testing accuracy (after validation testing has occurred) of 98.26% but did so while analyzing over 22,500 network

packets in less than 500 ms. Ultimately, we can see how a combination of data preprocessing and sensitive tuning of the activation and loss functions within different types of machine learning models can delineate both highly accurate and precise intrusion detection while doing so with a greater emphasis on low latency performance.

Dimensionality and Usage between Machine Learning Algorithms

Although this subsidiary existing solution perhaps does not apply to a specific process like the first existing solution above, understanding the dimensionality of when and where to implement one machine learning algorithm over another can significantly improve how the machine learning model performs based on the sensitive parameters that generally affect the input or activation functions of that model. Therefore, when understanding machine learning retrospectively in terms of how a model learns over time (we would assume a realm of learning with some form of guidance for the sake of cybersecurity), the model likely first needs to utilize a training set to parse through the data for learning based on the algorithms. As illustrated by Buczak and Guven (2016) in their own journal article titled "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection," Random Forest classifiers may benefit when the training set is scarce, which requires more contemplation on the spectrum of model iterations since many of the open-source datasets are based on common yet ubiquitously applied attack patterns; this creates a lack of compartmentalizations between the types of information being passed based on the function of the system in place.

Otherwise, "if the attack signature capture is important, decision trees, evolutionary computation, and association rules can be useful," which is generated from Buczak and Guven's (2016) in-depth criteria and comparisons when viewing many of the algorithms' different functions under the umbrella of intrusion detection. While it would seem that this added variability lessens the intention of unification between the other types of IDS, machine learning as a whole mitigates obfuscation by providing much more interchangeability and refinement based on which algorithms can be implemented for which aspects of the system, which is done

so in a way that addresses proceeding data that may be more prone to human errors. Lastly, due to the inherently dimensionality of machine learning based on training sets, we have the capacity to communicate other types of information, like kernel-level data with network data, to better understand the probabilistic outcomes of our models (Buczak and Guven, 2016). Overall, our progressive understanding of the dimensionality of machine learning intrusion detection for large training sets in addition to the comparative performance of each type of algorithm allows us to more holistically compare which types of machine learning could be employed for each system.

Recursive Network Isolation and Learnable Attack Patterns

In the aforementioned scope of intrusion detection, attackers are utilizing increasingly network-reliant attacks since they can better masquerade themselves with prevalent mechanisms like IP spoofing or network node mobilization. In turn, the intention of machine learning is to understand low-level translations of visual representations regarding these attack patterns so that the model can also predict similar future attackers based on the behavior of the nodes on the overall network. For example, black hole attacks create an optimized path to the attacker's node, which is then dropped, thereby causing legitimate streams of packets to be lost or disrupted while the rerouting continues to the attacker's node ("What is blackhole routing?" n.d.). Rath and Mishra (2020), in their journal article titled "Advanced-Level Security in Network and Real-Time Applications Using Machine Learning Approaches," further exacerbate our recognition of these patterns by providing some visual diagrams of attacks ranging from blackhole to collaborative to wormhole attacks, all of which recursively localize the attacker(s) to respective nodes since we can visually map attack paths that occur between the legitimate and malicious nodes on a network. If nodes acting as servers are located on an out-of-band channel when a wormhole attack occurs, for instance, we can measure where the packets are routed whenever a threshold for receiving packets is not met for the server nodes, therein ascertaining malicious nodes that may alter the temporal synchronization between clients and servers (Rath

and Mishra, 2020).

Finally, understanding the attack patterns in correspondence to strong datasets like KDD-99 certainly helps us to strengthen these machine learning models since they provide dozens of concentrated yet diversified types of attacks based on our recognition of how the attacks transgress, and more training data should always improve the efficacy of the model if the correct tuning and algorithms have been adjusted; as Ahmad et al. (2022) mention, "[The KDD Cup] consists of packets with 24 types of attacks, which are categorized under the following four classes, i.e., DOS, probe, remote to local, and user to root attacks and consists of more than 25,000 samples. Each network connection sample consists of 41 features." We can intrinsically visualize from these datasets that we have the initial tools to create proficient machine learning models while employing efficient performance, and correct use of data preprocessing or algorithm selection can create effective machine learning IDS, as was the case of Ahmad et al. (2022).

Section IV: Suggestions

Now that we have a better understanding of where machine learning resides in relation to its efficacy for intrusion detection, I have considered the following recommendations for future work, which may not be comprehensive in the technical sense yet highlight various avenues that I felt were lacking after conducting my research. Firstly, even though machine learning can be categorized based on its overarching intention to learn based on algorithms that parse through data, machine learning within itself encapsulates multiple subsets like deep learning and neural networks, which may contain different parameters such as the use of hidden neurons or input versus activation functions. As a result, future work could better compare the efficacy of these subsets with the same training sets and perhaps focus on similar algorithms so that the comparisons have less of a focus on mutually exclusive algorithms in relation to the more important effects on computational efficiency. Secondly, I would research models' differences based on the type of training data used; for example, customer relationship management (CRM)

versus medical records have different methods for storing data, and even though datasets like KDD-99 have been effective for all-encompassing machine learning models, there has not been sufficient research into data sensitivities and interactions across different types of datasets for machine learning models. Lastly, as somewhat elucidated by Ahmad et al. (2022), more work with machine learning models that learn from the interoperability between network and kernel-level data may benefit; for example, most of my research focused on network intrusion detection rather than host-based intrusion detection, and while some of the other research I found focused exclusively on host-based studies, there was little unification between the two components that interact with each other when transmitting data. Since the kernel needs to be efficient when computing certain types of information, it may be helpful to observe where attack vectors could occur based on incongruities between the fast communication of the kernel and the latent communication of the network.

Section V: Conclusions

To reiterate my findings throughout this research process, I first wanted to view machine learning in relation to performance capacity since we tend to intrinsically think of slower response times with many current anomaly-based systems. Facets like data preprocessing, depending on the type of machine learning algorithm used, can minimize the latency for viewing future datasets by tabulating a set of features that are most important based on previous attack vectors. Next, I wanted to comprehend how the interchangeability and dimensionality of machine learning may affect a model's efficacy given different attributes like kernel access and training set size. Lastly, I intuitively knew how previous attack patterns and datasets could help improve machine learning models but sought existing solutions in regard to both how we understand attack patterns on networks as well as what affordances we have for better visualization of attack patterns. These pieces of information lead to suggestions for future work on machine learning subset comparisons, different training set comparisons, and research into greater interoperability between network and kernel intrusion detection.

Overall, it is evident that we have beneficial IDS in place that can often mitigate the range of attack vectors within applications and other mediums like library dependencies, but more synchronicity, flexibility, and performance capacity need to be considered if we want to overcome human errors when viewing potentially new attacks. As technologies become ever more prominent across personal engagement and industry commerce, attackers have more tools to commit malicious attacks and only need to find one vulnerability, while the defenses within a system need to consider the increasing potential attack channels. Having a model that can learn over time and unify the best aspects of current IDS may be the answer to comprehensively addressing these attack channels. With time becoming a crucial asset in today's and tomorrow’s world, machine learning intrusion detection may very well be the solution to protecting this time so that we can continue to employ more technologies that benefit others.

References

Ahmad, U. B., Akram M. A., & Mian, A. N. (2022). Low-Latency Intrusion Detection Using a Deep Neural Network. IEEE Computer Society, 24(3), 67-72. https://doi.org/10.1109/MITP.2022.3154234

Buczak A. L. & Guven E. (2016). A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. IEEE Communications Surveys & Tutorials, 18(2), 1153-1176. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7307098

Rath, M. & Mishra, S. (2020). Advanced-Level Security in Network and Real-Time Applications Using Machine Learning Approaches. M. Khan (Ed.), Machine Learning and Cognitive Science Applications in Cyber Security (pp. 84-104). IGI Global. https://doi.org/10.4018/978-1-5225-8100-0.ch003

What is blackhole routing? CloudFare. (n.d.). Retrieved May 2, 2023, from https://www.cloudflare.com/learning/ddos/glossary/ddos-blackhole-routing/