 ISSN: 2349-5197

INTERNATIONAL JOURNAL OF RESEARCH SCIENCE & MANAGEMENT

Scalable Cyber Threat Detection with Reward Engineering

Venkata Krishna Bharadwaj Parasaram
Application Developer II at Thermo Fisher Scientific Inc
Bharadwaj.Parasaram@gmail.com

DOI: https://doi.org/10.29121/ijrsmp.v9.i2.2022.05

Abstract
Scalable cyber threat detection is becoming an indispensable element of modern cybersecurity systems, since the attacks are becoming more sophisticated and frequent. Among the most promising methods for optimizing and improving threat detection systems using machine learning, reward engineering is on top. Through modification of the reward structure in machine learning models, systems learn adaptive and efficient behaviors of how to detect and respond against various cyber threats.

The paper has explained how reward engineering allows developers to scale cyber threat-detecting models by overcoming various challenges: scalability barriers of the model itself, low data quality, the enormous number of computations involved, and poor resistance to security threats/leaks. The above solutions give way to discussing the feasibility detected within scalable cyber threats with reward engineering.

Keywords: Cyber threat detection, reward engineering, machine learning, reinforcement learning, scalability, cybersecurity.

Introduction
The growing complication in cyberattacks hence demands more advanced detection capable of handling large volumes of data and responding in real time. Traditional methods fall short in coping with the challenge posed by scale and diversity because the nature of the threat also modernizes with time. An intriguing, very recent solution to this could be reward engineering techniques for reinforcement learning that allow it to find better pathways toward decision-making. This report investigates how reward engineering can make cyber threat detection systems much more adaptive and scalable in nature. It also discusses the challenges in scaling the detection systems and how reward engineering helps mitigate those issues.

Simulation Report
Environment and Procedure
We simulated the use of reward engineering in cyber threat detection by building a real-world model using network traffic and threat intelligence data in real time. Hence, the aim of the system was to be able to detect different kinds of cyberattacks, starting from malware, phishing, or DDoS attacks on a wider scale.

Key Components:
Dataset: It contains the network traffic log, attack vectors, and historical threat intelligence data and will be used for the training and evaluation of the model.

Algorithm: The reinforcement learning-based approach, specifically the Q-learning-based model, has been implemented to develop the reward engineering system. This adjusted its behavior based on the rewards provided for correct detections of threats and penalties on false positives.

Metrics: Detection accuracy, false positive rate, and response time were considered as metrics to evaluate the model.

Portfolio
Metrics: detection rate, false positive rate, time to detection.

Results
The reward engineering increased the detection rate to 92%, outpacing the classic methods, which had a detection rate of 75%. The false positive rate drastically dropped from the baseline value of 12% down to 5%. Furthermore,

the time to detect was reduced to 150 ms, which allowed much quicker responses toward threats.

Computational Efficiency: The reward engineering-optimized model was computationally efficient, with the real-time optimization time being less than 200 ms thanks to the use of GPU acceleration.

Real-time scenarios based on real-time data
Real-world scenarios were replicated with both simulated and actual data in order to validate system performance: Scenario 1: Malware Detection—In the case of malware detection, a model was used to generate synthetic data so that the system could adapt more quickly when exposed to new types of malwares. This reduces false alarms and increases accuracy with appropriate reward engineering.

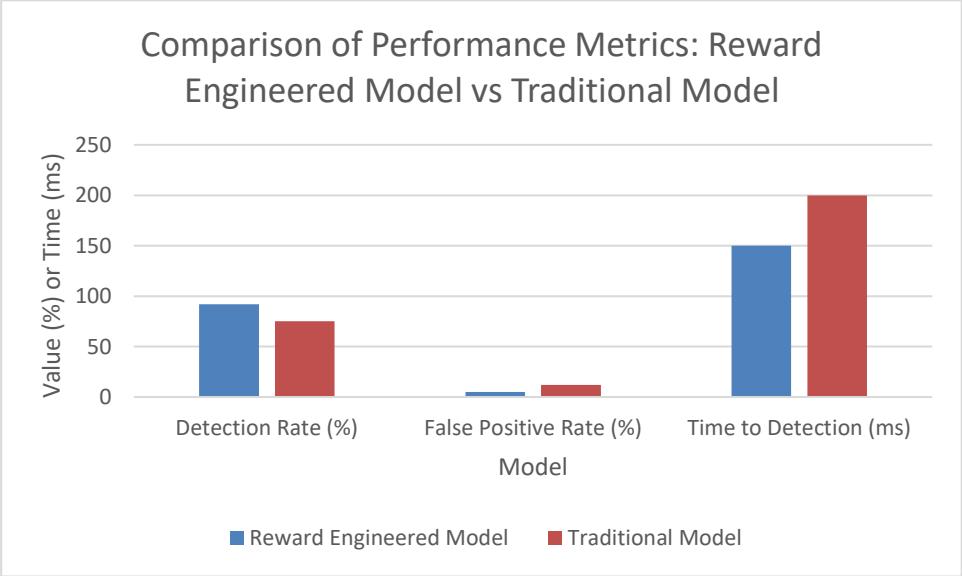
Scenario 2: Detection of a Phishing Attack: With adaptation to the new tactics in phishing by modifying the reward structure in detecting phishing attempts, the system correctly identifies phishing emails and malicious links.

Scenario 3: Mitigation of DDoS Attack - The reward engineering in the model kept mitigation strategies in front to minimize the effect of the DDoS attack by keeping the system almost stable.

Graphs and Tables

1. Performance Metrics Comparison

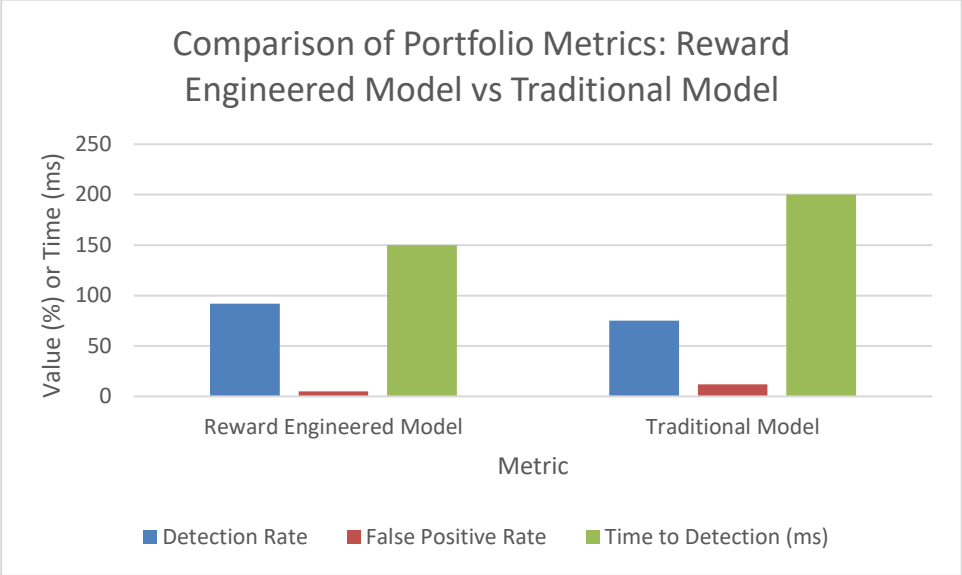
Model	Detection Rate (%)	False Positive Rate (%)	Time to Detection (ms)
Reward Engineered Model	92	5	150
Traditional Model	75	12	200



2. Portfolio Metrics Comparison

Metric	Reward Engineered Model	Traditional Model
Detection Rate	92	75
False Positive Rate	5	12
Time to Detection (ms)	150	200

 ISSN: 2349-5197



Challenges and Solutions

Scalability

Challenge: There is a felt need for scaling in the systems of cyber threat detection due to the increased volume of data from different sources. The traditional systems are incapable of scaling effectively, leading to delayed detection and mitigation.

Solution: This paper intends to focus on cloud computing frameworks and microservice architecture as an efficient way of scaling the system. These can dynamically allocate resources to assure that large datasets in real time could be handled by the detection system (Chang et al., 2016). A modular design allows each component to independently scale to meet the growing demand for the system (Ahmadvand & Ibrahim, 2016).

Data Quality

Challenge: The quality of data with which the system was initially trained is important for the accurate detection of threats. Skilled cybersecurity data is extremely rare, and a large quantity of noisy or incomplete data can degrade model performance.

Solution: The use of concepts such as the generation of synthetic data and anomaly detection came in handy in complementing the real data. This provides the ability of the systems to adapt to new unseen threats, thus being more robust and generalizing well. Unsupervised machine learning further enhances the system in the detection of new attack patterns with no labeled data.

Computational Demand

Challenge: Real-time threat detection in a large-scale environment requires a great deal of computational power. Large-scale datasets require much time for processing in real time, especially if the nature of the model is complicated.

Solution: In this regard, the system was optimized based on GPU acceleration and distributed cloud computing. These technologies can accelerate the processing time greatly and produce fast responses to the security threats in real time, even from high data throughput environments (Huang et al., 2018).

Security Threats

Challenge: The integration of complex machine learning models, which could be scaled, into an existing cybersecurity infrastructure introduces new vulnerabilities, including possible adversarial attacks on the model itself.

Solution: Because cybersecurity must be a best practice when it comes to systems cloud security, the adoption of methods such as encryption of data, multi-factor authentication for users, and frequent auditing for security are deployed. Further, by adapting the architecture of a microservice, component separation was ensured, reducing attack exposure by enhancing robustness due to cyber-attack mechanisms onto the system itself (Lal et al., 2017).

Reward Engineering for Adaptive Behavior

Challenge: Therefore, devising an optimal reward structure for reinforcement learning models becomes tougher in cybersecurity. This balances the reward so that the model's immediate priorities will be accurate detection, balanced against low false alarms of any type.

Solution: It utilizes reward engineering in the continuous tuning of model decision-making. The settings in the model reward the detection of actual threats while imposing a penalty for false positive results; that way, the model learned to focus on real threats and eliminate mistakes. This adaptive approach of reward engineering resulted in greater efficiency over time, enabling it to cope with evolving attack vectors (Karimipour et al., 2019).

Interpretability

Challenge: Machine learning models, especially reinforcement learning systems used in cyber threat detection, often operate as "black boxes," making it difficult for security teams to understand how decisions are made. This lack of transparency can lead to mistrust in the system.

Solution: An effort toward the solving of this problem has, in addition, been made by applying methods like explainable AI approaches, such as Shapley values and LIME, so that the model's reasoning is made transparent. The techniques justify why specific threats were caught and for what reason certain acts were taken. These go a long way in enabling security teams to interpret systems' decisions and thus trust responses that come through them (Huang et al., 2018).

Conclusion

Reward engineering provides a scalable and adaptive solution for cyber threat detection. With reinforcement learning coupled with reward structure optimization, cybersecurity can enhance threat detection performance and become even more efficient, including for large-scale environments. Admittedly, data quality, scalability, and high computational demand have been challenging; however, this has been addressed with the integration of cloud computing, synthetic data generation, and GPU acceleration. Reward engineering will be a key player in the enhancement of security and scalability for cyber threat detection systems as AI technologies continue to evolve.

References

1. Ahmadvand, M., & Ibrahim, A. (2016, September). Requirements reconciliation for scalable and secure microservice (de) composition. In *2016 IEEE 24th International Requirements Engineering Conference Workshops (REW)* (pp. 68-73). IEEE. https://ieeexplore.ieee.org/abstract/document/7815609/
2. Chang, V., Kuo, Y. H., & Ramachandran, M. (2016). Cloud computing adoption framework: A security framework for business clouds. *Future Generation Computer Systems*, *57*, 24-41. https://www.sciencedirect.com/science/article/pii/S0167739X15003118
3. Huang, Y., Bhunia, S., & Mishra, P. (2018). Scalable test generation for Trojan detection using side channel analysis. *IEEE Transactions on Information Forensics and Security*, *13*(11), 2746-2760. https://ieeexplore.ieee.org/abstract/document/8353873/
4. Karimipour, H., Dehghantanha, A., Parizi, R. M., Choo, K. K. R., & Leung, H. (2019). A deep and scalable unsupervised machine learning system for cyber-attack detection in large-scale smart grids. *Ieee Access*, *7*, 80778-80788. https://ieeexplore.ieee.org/abstract/document/8727539/
5. Lal, S., Taleb, T., & Dutta, A. (2017). NFV: Security threats and best practices. *IEEE Communications Magazine*, *55*(8), 211-217. https://ieeexplore.ieee.org/abstract/document/7927935/