International Journal of Scientific Research in Science and Technology
Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com)
doi : https://doi.org/10.32628/IJSRST

Dynamic Cybersecurity Risk Assessment: Temporal Graph Neural Networks and Reinforcement Learning for Proactive Threat Management

Ashish Reddy Kumbham
Independent Researcher, USA

Abstract – The cyber threat necessitates rapid paradigm shifts in cyber security strategies. The traditional approach to threat/risk management is becoming increasingly ineffective in dealing with the dynamic nature of modern threats. Therefore, this paper provides a dynamic cyber security risk assessment framework that combines temporal graph neural networks and reinforcement learning (RL). This would allow threat management TGNNs to make proactive decisions to help evolve relationships within networking environments. On the other hand, RL optimizes its defensive technique by learning from previous threats and predicting potential vulnerabilities. The evaluation would require demonstrable efficacy in reducing response time while improving threat detection accuracy and risk mitigation in real-world scenarios.

Keywords: Reinforcement Learning, Risk Assessment, Threat Management, General Purpose Unit, Temporal Graph Neural Network

Introduction

As the evolving cyber threat spreads throughout the digital ecosystem, a dynamic, interconnected nature is required to deal with it. This is due to an increase in the complexity of network infrastructure, which is fueled by the proliferation of sophisticated cyberattacks. As a result, an innovative solution for quick and proactive threat management must be implemented.

Furthermore, cyber-attacks have a common feature in the image of recognition: roughly 99 percent of new attacks are lightweight and mutated (1). This change can be seen in their pixels, indicating that signatures and patterns are automatically learned.

To identify threats, computations, and management states in the programming model must now be built. This tensor flow model would allow programmers to demonstrate an experimental parallelization scheme by offloading computation to servers (2). This would hold the shared states accountable for ensuring there is a reduction in network traffic. The tensor flow phase would consist of two distinct stages: first, identifying the neural network that needs to be constructed and modifying rules, and second, optimizing and executing global computation, such as achieving high GPU utilization via graph dependency structure.

Simulation Report

Datasets

The proposal framework consists of two core components: temporal graph neural network and reinforcement learning.

Temporal Graph Neural Network

The TGNNs provide time-based analysis and graph representations of network interactions such as patterned communication and anomaly propagation. TGNN captures the mutual effects on user items and

item-to-item relationships (3). As a result, to learn temporal information, heterogeneous relations and nodes must be considered from various perspectives while also encoding neighborhood information. The cross-view learning strategy would be better suited for examining the extensive relationships over time.

Scenario 1: Temporal Graph Neural Network

The data below comes from "the Canadian Institute for Cybersecurity Intrusion Detection System (CICIDS) along with the University of New South Wales (UNSW), founded by the Australian Centre for Cyber Security."

Dataset	Precision %	Recall %	F1 scor%
CICIDS	92	93	92.5
UNSW-NB15	89	90	89.5

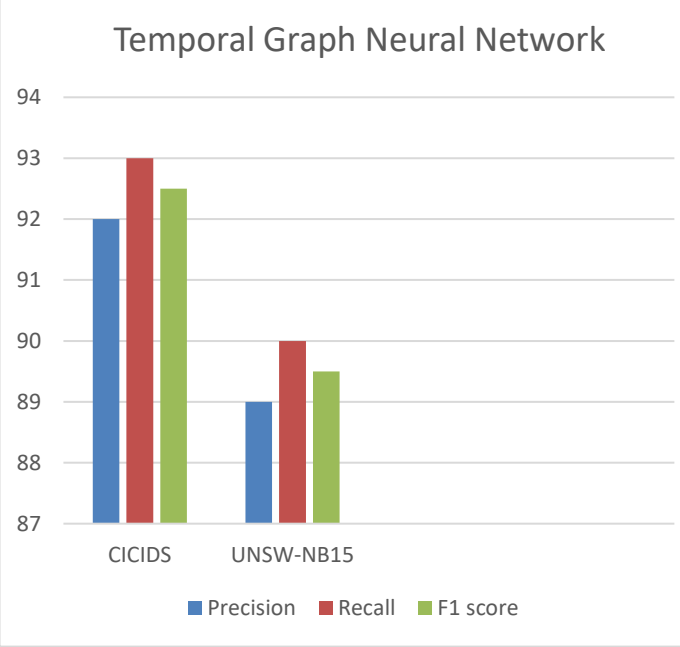

Fig1: temporal graph neural network

Scenario 2 : Reinforcement Learning

The goal of RL is to take the best possible action to mitigate a threat. The environment model network and RL provide an agent policy that reduces risk by interacting with the environment. In RL simulation, agents must acquire more effective ways to optimize network behavior, such as winning as many games (threats) as possible (4). As a result, adversarial reinforcement learning is required to establish an algorithmic war in cyber attacks. This is because the defender and attacker tend to observe states and incomplete information when simulating an adversarial game. Monte Carlo's e-greedy strategies can only be addressed if a reinforcement learning plan is implemented.

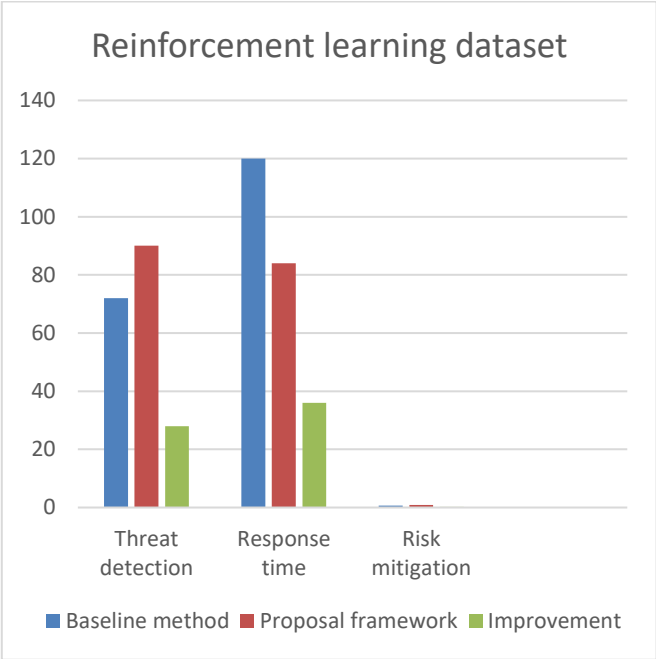

Fig 2 : reinforcement learning model

Challenges and Solution

Challenges

Although there is a shift toward focusing on cyber security threats, many companies do not consider other significant exposures to company risks, such as credit obligations or excessive claims. Too much emphasis is on combining machine learning across various dynamic cyber security assessment tasks. Machine learning has only been used to solve traditional quantitative problems, such as forecasting risk models and optimizing portfolio construction (5). As a result, the algorithm used here is under-labeled training, making it simple to predict for unlabeled examples. The risk assessment can monitor learning tasks only related to classification, regression, and ranking problems.

Solutions

The concept of computing infrastructure must be continually targeted for cyber attacks to acquire access to sensitive information like data. Risk assessment requires resilience to be developed through cybersecurity monitoring, intuition prevention, and secure configuration (6). That is, the network attack has to incorporate both passive and active attacks. The passive attack would provide a silent gain of information about the target while not altering the data on the target's end. On the other hand, an active attack would attempt to change the target's cyber security status or introduce new strategies. This will result in a monitoring anomaly if the activities represent behavior different from standard or expected threats.

Conclusion

A dynamic assessment of cyber security risks determines the potential of TGNN and RL integration. This can be demonstrated by modeling a temporal relationship and implementing an optimal defense strategy. The new and proposed framework should proactively approach threats and management. This would further guide future work, focusing on scaling a more muscular system in the case of more extensive networks or incorporating advancements to RL techniques to improve efficacy.

REFERENCES

[1]. He, Y., Meng, G., Chen, K., Hu, X., & He, J. (2020). Towards security threats of deep learning systems: A survey. IEEE Transactions on Software Engineering, 48(5), 1743-1770.

[2]. Abadi, M., Barham, P., Chen, J., Chen, Z., Davis, A., Dean, J., ... & Zheng, X. (2016). {TensorFlow}: a system for {Large-Scale} machine learning. In 12th USENIX symposium on operating systems design and implementation (OSDI 16) (pp. 265-283).

[3]. Bai, T., Zhang, Y., Wu, B., & Nie, J. Y. (2020, December). Temporal graph neural networks for social recommendation. In 2020 IEEE International Conference on Big Data (Big Data) (pp. 898-903). IEEE.

[4]. Elderman, R., Pater, L. J., Thie, A. S., Drugan, M. M., & Wiering, M. A. (2017, January). Adversarial reinforcement learning in a cyber security simulation. In 9th International Conference on Agents and Artificial Intelligence (ICAART 2017) (pp. 559-566). SciTePress Digital Library.

[5]. Mashrur, A., Luo, W., Zaidi, N. A., & Robles-Kelly, A. (2020). Machine learning for financial risk management: a survey. Ieee Access, 8, 203203-203223.

[6]. Nguyen, G., Dlugolinsky, S., Tran, V., & Garcia, A. L. (2020). Deep learning for proactive network monitoring and security protection. Ieee Access, 8, 19696-19716.

[7]. Sukender Reddy Mallreddy(2020).Cloud Data Security: Identifying Challenges and Implementing Solutions.JournalforEducators,TeachersandTrainers,Vol.11(1).96 -102.