Crimson Publishers
Wings to the Research

Opinion

Towards an Automatic Self-Learning Intrusion Detection System

Quang Vinh Dang*

Industrial University of Ho Chi Minh City, Ho Chi Minh city, Vietnam

ISSN: 2694-4391

***Corresponding author:** Quang Vinh Dang, Industrial University of Ho Chi Minh City, Ho Chi Minh city, Vietnam

Submission: 📅 March 15, 2023
Published: 📅 March 24, 2023

Volume 3 - Issue 3

How to cite this article: Quang Vinh Dang. Towards an Automatic Self-Learning Intrusion Detection System. Int J Conf Proc. 3(3). ICP. 000562. 2023.
DOI: 10.31031/ICP.2023.03.000562

Abstract

Intrusion detection systems (IDS) are essential in safeguarding computer networks against malicious attacks. Machine learning (ML) has been widely applied to IDS to enable the systems to identify and respond to threats effectively. One challenge in ML-based IDS is the need for frequent model updates to account for new attack patterns and tactics. A self-update machine learning system (SUMS) is a solution that can help IDS maintain optimal performance by continuously adapting to new threats. In this paper, we will discuss the concept of a SUMS for IDS and explore its benefits and challenges.

Introduction

Machine learning algorithms are powerful tools for detecting intrusion attempts in network traffic. Traditional signature-based intrusion detection systems work by comparing network traffic to a database of known attack signatures. However, this method has its limitations. Attackers can easily modify their attack signatures to bypass detection, rendering signature-based IDS ineffective. Machine learning IDS, on the other hand, can learn to detect new attack patterns and tactics without the need for explicit signature updates. However, ML-based IDS requires regular model updates to keep up with the ever-evolving threat landscape. This is a tedious and resource-intensive process, and even a small delay in updating the model can expose the network to significant security risks. This is where a self-update machine learning system (SUMS) comes in. A SUMS automates the process of updating the model, making it more efficient and less prone to human error.

Benefits of a SUMS for IDS

The main benefit of a SUMS for IDS is the ability to maintain optimal performance even in the face of new threats. When the model is not updated regularly, it becomes less effective in detecting new attacks, resulting in a higher false-negative rate. This, in turn, increases the likelihood of successful attacks on the network. A SUMS automates the process of model updates, ensuring that the model is always up-to-date and able to detect new threats effectively. Another benefit of a SUMS is the reduction in the workload for security analysts. Updating the model manually is a time-consuming and laborious process. With a SUMS in place, security analysts can focus on other critical tasks, such as investigating alerts and responding to incidents.

Challenges of a SUMS for IDS

Despite its benefits, implementing a SUMS for IDS poses some challenges. One major challenge is the potential for model drift. Model drift occurs when the distribution of data used to train the model changes over time. This can happen as attackers change their tactics or as the network undergoes changes. As a result, the model may become less accurate in detecting new attacks. To address this challenge, the SUMS must be designed to detect and correct model drift automatically. Another challenge is the risk of model poisoning. Model poisoning is a type of attack where an attacker introduces malicious data into the training dataset to manipulate the model's behavior. A SUMS must be designed to detect and prevent model poisoning attacks to ensure the integrity of the model.

Approaches to implementing a SUMS for IDS

There are several approaches to implementing a SUMS for IDS. One approach is to use an ensemble of models. An ensemble is a group of models that work together to make decisions. Each model in the ensemble is trained on a different subset of the data. This approach can help mitigate the risk of model drift and model poisoning by ensuring that the overall system is robust to attacks. Another approach is to use online learning. Online learning is a type of machine learning that updates the model in real-time as new data arrives. This approach can help address the challenge of model drift by allowing the model to adapt to changes in the data distribution as they occur.

Conclusion

In conclusion, a self-update machine learning system (SUMS) can help maintain optimal performance for intrusion detection systems (IDS) by continuously updating the model to account for new attack patterns and tactics. A SUMS automates the process of updating the model, making it more efficient and less prone to human error. The benefits of a SUMS include improved detection rates, reduced workload for security analysts, and enhanced security posture for the network. However, implementing a SUMS for IDS poses some challenges, including model drift and model poisoning. To address these challenges, the SUMS must be designed to detect and correct model drift automatically and prevent model poisoning attacks. Approaches to implementing a SUMS for IDS include using an ensemble of models and online learning. In summary, a SUMS is a promising solution to the challenge of keeping IDS up-to-date with the ever-evolving threat landscape. As the threat landscape continues to evolve, it is essential to explore new and innovative ways of improving the effectiveness and efficiency of IDS. A SUMS is one such solution that holds great potential in the fight against cyber threats [1-3].

References

1. Dang QV (2023) Learning to transfer knowledge between datasets to enhance intrusion detection systems. Computational Intelligence pp. 39-46.
2. Dang QV (2022) Detecting intrusion using multiple datasets in software-defined networks. Future Data and Security Engineering. Big Data, Security and Privacy, Smart City and Industry 4.0 Applications: 9th International Conference, FDSE 2022, Ho Chi Minh City, Vietnam, pp. 739-746.
3. Dang QV (2022) Machine learning for intrusion detection systems: Recent developments and future challenges. Real-Time Applications of Machine Learning in Cyber-Physical Systems, pp. 93-118.