RADemics

Bayesian Deep Learning for Probabilistic Risk Assessment and Attack Surface Reduction in CyberPhysical Systems

Er. Ram Prasad Pokhrel, B. Dineshkumar, Kayalvizhi K R
CHANDIGARH UNIVERSITY, VELALAR COLLEGE OF ENGINEERING AND TECHNOLOGY, ST. JOSEPH'S COLLEGE OF ENGINEERING.

1. Bayesian Deep Learning for Probabilistic Risk Assessment and Attack Surface Reduction in Cyber Physical Systems

[1]Er. Ram Prasad Pokhrel, Independent Research Scholar, ECE department, Chandigarh University, Punjab. rmprsdpokhrel06@gmail.com

[2]B. Dineshkumar, Assistant professor, Electronics and Communication Engineering, Velalar College of Engineering and Technology, Thindal, Erode-12, Dineshappliedelectronics@gmail.com

[3]Kayalvizhi K R, AP –ECE,St. Joseph’s college of Engineering ,OMR, Chennai 600119 , kayalvizhikr@stjosephs.ac.in

Abstract

CyberPhysical Systems (CPS) are increasingly targeted by sophisticated cyber threats, necessitating advanced Intrusion Detection Systems (IDS) capable of probabilistic risk assessment and adaptive defense mechanisms. Traditional deep learningbased IDS models, while effective in pattern recognition, lack uncertainty quantification, leading to unreliable classifications in dynamic attack environments. Bayesian Deep Learning (BDL)offers a principled approach to addressing this challenge by integrating probabilistic inference for enhanced threat detection and risk estimation. This book chapter explores the role of Bayesian Neural Networks (BNNs) in IDS, emphasizing their ability to model epistemic and aleatoric uncertainties, thereby improving detection accuracy and decision confidence. the chapter presents Bayesian Hyperparameter Optimization (BHO) as a scalable solution to optimize IDS model parameters, ensuring efficient and adaptive learning against evolving attack patterns. The integration of Bayesian techniques in both anomaly based and signature based IDS frameworks is examined, highlighting their potential in reducing false positives and mitigating adversarial attacks. , case studies and empirical evaluations are provided to demonstrate the real world applicability of BDL driven IDS in securing industrial control systems, smart grids, and IoT networks. The findings underscore the importance of uncertaintya ware AI driven cybersecurity frameworks for robust and resilient CPS protection.

Keywords: Bayesian Deep Learning, Intrusion Detection System, Cyber Physical Systems, Uncertainty Quantification, Probabilistic Risk Assessment, Adversarial Robustness..

Introduction

Cyber Physical Systems (CPS) represent a critical component of modern infrastructure, integrating computational intelligence with physical processes across various domains, including industrial control systems, autonomous vehicles, smart grids, and healthcare systems. The increasing interconnectivity and reliance on real time data exchange expose these systems to a wide range of cyber threats, including malware, denialofservice (DoS) attacks, insider threats, and adversarial manipulations. Traditional security mechanisms, such as firewalls and rulebased Intrusion Detection Systems (IDS), struggle to address the complexity and evolving nature of these threats. Deep learningbased IDS models have emerged as a promising approach for detecting sophisticated cyberattacks; however, their deterministic nature limits their ability to quantify uncertainty, leading to potential misclassifications. A more resilient approach is required to ensure robust and adaptive threat detection in CPS environments.

Bayesian Deep Learning (BDL) offers a powerful framework for enhancing IDS by incorporating probabilistic reasoning and uncertainty estimation. Unlike conventional deep learning models, which provide fixed predictions, Bayesian Neural Networks (BNNs) generate probability distributions over possible outcomes, enabling confidenceaware decisionmaking. This capability is particularly crucial in cybersecurity, where a lack of uncertainty quantification can result in false alarms or undetected intrusions. By capturing both epistemic uncertainty (uncertainty in the model) and aleatoric uncertainty (uncertainty in the data), BDL allows IDS to assess threats more accurately, even in adversarial scenarios. The ability to model uncertainty enhances IDS resilience, making it more effective in detecting zeroday attacksand novel threat patterns that have not been previously observed in training data.

In addition to uncertainty quantification, Bayesian Hyperparameter Optimization (BHO)plays a crucial role in improving the efficiency and adaptability of IDS models. Deep learning models require extensive tuning of hyperparameters such as learning rate, dropout rate, activation functions, and model architecture to achieve optimal performance. Traditional hyperparameter tuning techniques, including grid search and random search, are computationally expensive and inefficient in highdimensional spaces. BHO addresses this challenge by employing probabilistic models, such as Gaussian Processes (GPs) and Treestructured Parzen Estimators (TPE), to intelligently explore the hyperparameter space. This optimization technique ensures that IDS models are trained with the most effective configurations, enhancing their ability to generalize across diverse cyberattack scenarios.