


Chapter 7

A Survey on Network Intrusion Detection Using Deep Generative Networks for Cyber–Physical Systems

Srikanth Yadav M.

 <https://orcid.org/0000-0003-2796-7978>

VFSTR University, India

Kalpana R.

Pondicherry Engineering College, India

ABSTRACT

In the present computing world, network intrusion detection systems are playing a vital part in detecting malicious activities, and enormous attention has been given to deep learning from several years. During the past few years, cyber-physical systems (CPSs) have become ubiquitous in modern critical infrastructure and industrial applications. Safety is therefore a primary concern. Because of the success of deep learning (DL) in several domains, DL-based CPS security applications have been developed in the last few years. However, despite the wide range of efforts to use DL to ensure safety for CPSs. The major challenges in front of the research community are developing an efficient and reliable ID that is capable of handling a large amount of data, in analyzing the changing behavioral patterns of attacks in real-time. The work presented in this manuscript reviews the various deep learning generative methodologies and their performance in detecting anomalies in CPSs. The metrics accuracy, precision, recall, and F1-score are used to measure the performance.

DOI: 10.4018/978-1-7998-5101-1.ch007

INTRODUCTION

In the present computing world, the volume of the data or information is increased rapidly, and the role of computers in managing and maintaining the integrity of the networks is quickly expanded in domains such as social networks, e-commerce, and health care. More human activities are also grown in these domains; this leads to the occurrence of more internal intrusion within the network. The role of the Intrusion Detection System (IDS) is to protect networks from vulnerable attacks from both external and internal intruders. An IDS (P Anderson, 1980) is either a software or hardware used to monitor the activities of computer networks. The IDS protects the network from the threats by analyzing patterns of captured data packets. These threats can be overwhelming; for example, Denial of service (DoS) attacks prevent genuine user's resources by generating unwanted traffic (Mitchell & Chen, 2014). In contrast, Malware or Trojans are the hidden programs installed by the attackers to interrupt network systems (Kettani & Cannistra, 2018). Many IDS exist in the contemporary digital era, but most of the IDS services have experienced the difficulty of a high false alarm rate. This is also one of the challenges to be handled in designing efficient IDS. One more significant issue to be resolved is to reduce the load on the administrator and useful classification of assigning class labels to the unlabelled records. Another difficulty of some existing IDS is their incapability to recognize unknown attacks. These IDS depends on the signatures of acknowledged attacks.

An active IDS can be designed by using various machine learning techniques. The machine learning classification schemes are used to separate regular traffic from abnormal traffic. The machine learning model is developed by training on an NSL-KDD (Farahnakian & Heikkonen, 2018) dataset to forecast an attack using classification schemes. Many machine learning approaches have been productively implemented as classifiers on IDS. But these approaches have several flaws such as high false alarm rate (FAR) and low throughput.

Cyber-physical systems (CPS) can be referred to as modern systems with assimilated computational and physical capabilities that can communicate with humans in new ways. Such technologies have an immense effect on several sectors, such as environmental management, smart transport, manufacturing, smart grid, smart house, smart infrastructure, and smart healthcare. Both of these domains are network-dependent because they involve remote data transmission to transmit data from sensors to actuators through the control center. Contact in a large network renders the device fragile and creates a humongous space for adversaries to attack.

The Internet of Things (IoT), one of the core sub-domains of CPS, has introduced major technical developments to a whole new stage where data is the driving power. In tandem with actuators, motors, cameras, applications, and networking, IoT has opened up a new layer to facilitate communication, processing, and data sharing. While generally acknowledged, almost 85 percent of IoT systems remain susceptible to a large variety of cyberattacks. These are vulnerable to different forms of threats, such as man-in-the-center, data and identity stealing, distributed denial of service (DDoS), computer hijacking, etc. To secure protection vital structures from intruders, rigorous monitoring procedures to identify all types of intruders must be taken into consideration.

The IDS is responsible for monitoring network activity and device data for unauthorized behaviors and for providing warnings, which are the first and foremost component of the security policy in the CPS environment. Getting clear awareness of the precise place and period at which particular anomalies produce hazards in the environment tends to minimize impacts by taking suitable measures, and therefore,

21 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/a-survey-on-network-intrusion-detection-using-deep-generative-networks-for-cyber-physical-systems/266137

Related Content

Cancer Diagnosis Using Artificial Intelligence (AI) and Internet of Things (IoT)

Samiksha Garse, Khadija Shahab Turabi, Jyotirmoi Aich, Amit Ranjan, Shuchi Nagar, Soumya Basuand Shine Devarajan (2023). *Revolutionizing Healthcare Through Artificial Intelligence and Internet of Things Applications* (pp. 50-71).

www.irma-international.org/chapter/cancer-diagnosis-using-artificial-intelligence-ai-and-internet-of-things-iot/324935

Modelling Software-Defined Wireless Sensor Network Architectures for Smart Grid Neighborhood Area Networks

Nazmus S. Nafi, Khandakar Ahmedand Mark A. Gregory (2017). *Security Solutions and Applied Cryptography in Smart Grid Communications* (pp. 267-286).

www.irma-international.org/chapter/modelling-software-defined-wireless-sensor-network-architectures-for-smart-grid-neighborhood-area-networks/172684

Artificial Intelligence-Based Billing System: Fingerprint Mechanism

Kathirvel A., Sabarinathan C., Saravanan N., Ramesh S., Meera S., Karnavel K.and Sudha D. (2022). *Methods, Implementation, and Application of Cyber Security Intelligence and Analytics* (pp. 151-164).

www.irma-international.org/chapter/artificial-intelligence-based-billing-system/306864

Possibility Interval-Valued Vague Soft Expert Sets and Its Similarity Measure

Ganeshsree Selvachandranand Sunil Jacob John (2017). *International Journal of Fuzzy System Applications* (pp. 108-121).

www.irma-international.org/article/possibility-interval-valued-vague-soft-expert-sets-and-its-similarity-measure/171655

A Key Management Scheme for Secure Communications Based on Smart Grid Requirements (KMS-CL-SG)

Bashar Alohal, Kashif Kifayat, Qi Shiand William Hurst (2017). *Security Solutions and Applied Cryptography in Smart Grid Communications* (pp. 242-265).

www.irma-international.org/chapter/a-key-management-scheme-for-secure-communications-based-on-smart-grid-requirements-kms-cl-sg/172682