Physics-Informed Intrusion Detection using Deep Learning

Professor Souvik Chakraborty
Department of Applied Mechanics
IIT Delhi
https://www.csccm.in/our-team#h.4tungbrwmhpe

Research Interests: Uncertainity Quantification, Multiscale Dynamic Systems,Reliability analysis Physics informed Neural Networks

Professor Vireshwar Kumar
Department of Computer Science
IIT Delhi
https://www.cse.iitd.ac.in/~viresh/

Research Interests: System Security User Privacy, Cryptography,ML

Neha Arora
Research Scholar
SIRe, IIT Delhi

In emerging applications, e.g., smart farming and precision agriculture, a large number of robotic devices (RDs) are getting closely integrated with the existing computer infrastructure to form the Internet-of-Things (IoT).While this connectivity facilitates real-time feedback and remote control of an RD, it makes the RD vulnerable to cyber threats. In a typical attack, the adversary poisons the RD's sensor values to realize the desired anomalous behavior. It is very challenging to detect such data poisoning because of three major reasons. Firstly, each RD is equipped with a large number of sensors which report continuous streams of data leading to a bigdata analysis problem. Secondly, even a minor anomalous change in the RD's operation may result into a grave impact in critical applications. Lastly, the real impact of the anomaly can only be observed over a long duration of time which could be months in some cases, e.g., an attack affecting the yield. Hence, the conventional intrusion detection systems (IDSs) have low attack detection rate because they fail to detect small anomalies while processing the bigdata. Moreover, they analyze the reported values from each sensor individually, and hence they fail to identify a stealthy attack that poisons multiple sensor values concurrently.

PROPOSED SOLUTION

To address these challenges, we propose to develop a novel intrusion detection system that employs deep learning tools to first learn the governing physics from the sensor data, and then utilize the same for anomaly detection. Physically invariants correlation between multiple sensors will be exploited to track and uncover concurrent anomalies. To detect small anomalies, we propose to utilize the concepts of nonlinear transformation and manifold learning. The outcome of this project will be a comprehensive framework for designing a deep learning-based and physics-informed intrusion detection system that reliably and robustly detects a wide array of cyber threats.