PURDUE INNOVATES | Office of Technology Commercialization

LIDAR: Lifelong-learning-based Intelligent, Diverse, Agile and Robust Architecture for Network Attacks Detection

LIDAR is an adaptable, robust intrusion detection system that uses lifelong learning to identify known and unknown zero-day attacks in diverse settings, including wireless networks.

Researchers at Purdue University have developed LIDAR, an adaptable intrusion detection system suitable for diverse settings, including wireless networks. This technology can detect a wide range of diverse attacks and allows the intrusion detection system to learn how to best identify the already known attacks as well as recognize unknown/zero-day attacks and capture their behavior for future identification. The robustness of the technology is ensured by using lifelong learning updates, input pre-processing components that are designed to be resilient to adversarial attacks, and a cross-layer feature extraction mechanism for networks with a wireless communication medium. Furthermore, this technology is able to adapt to the environment through lifelong learning, and relies on very little assumptions for the attacker behavior.

Advantages:

-Adaptable

-Explore generic zero day attack behavior

-Suitable for diverse settings

-Robust

Potential Applications:

-Intrusion detection system

TRL: 5

Intellectual Property:

Technology ID
2019-GHAF-68713

Category
Artificial Intelligence & Machine Learning/Reinforcement & Federated Learning

Authors
Aly El Gamal
Ali Elghariani
Arif Ghafoor

Further information
Matt Halladay
MRHalladay@prf.org

Erinn Frank
EEFrank@prf.org

View online

Provisional-Patent, 2020-02-03, United States

Utility Patent, 2020-11-25, United States

Keywords: LIDAR intrusion detection, zero-day attack detection, adaptable intrusion detection system, lifelong learning security, wireless network intrusion detection, cross-layer feature extraction, adversarial attack resilience, Purdue University cybersecurity, autonomous agents for intrusion detection, behavior-based monitoring, Computer Technology, Cybersecurity, Electrical Engineering, Intrusion Detection, Machine Learning, Network Attacks, Network Security, Wireless Network Security