1. Illustration of non-ML based and ML -based diagram

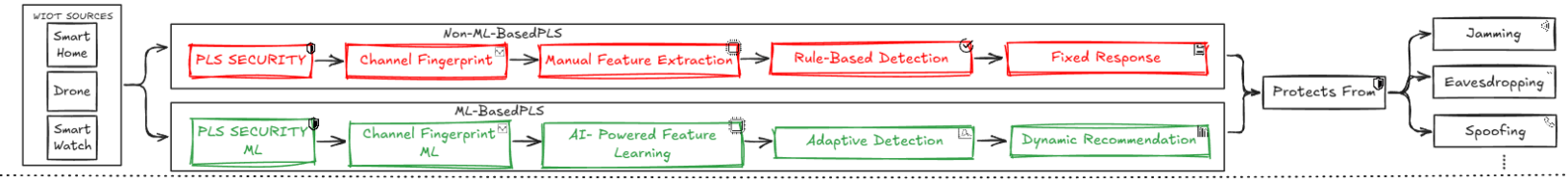

Figure1. Physical-Layer Security in WIoT Systems with non-ml and ml based PLS

In this diagram we explain the difference between using ML-based and non- ML -based in protecting Physical layer Security. The diagram consists of two different approaches:

- **Non-ML-Based PLS:**

  The diagram provides a detailed comparison between traditional non-ML-based (PLS) techniques and more advanced, An Enhanced AI methods that provide ML and DL that focus on features and extract the patterns of the signals. On the left side of the diagram, WIoT sources as “Smart Home, Drones, etc.”[1] The rectangles marked with red are known as **Non-ML-Based PLS** that include four sequential steps: **channel fingerprints, manual feature extraction, rule-based identity, and fixed response**. These phases are based on classic signal processing techniques, where the security network depends on predefined features derived from the wireless channel and is a stable set of rules for detecting and responding to security threats. Although this approach has been fundamental to securing wireless networks, it suffers from boundaries when it comes to adaptability and scalability, especially in a dynamic and strange environment such as WIoT.[2]

- **ML-Based PLS:**

  Enhanced PLS techniques highlight green more dynamic and flexible security solutions. The first step, AI-Powered feature learning, identifies and is automatically identified on learning from wireless signals, appoints machine learning algorithms, eliminates the need for manual extraction and enables the system to adapt to the environment in the network. This is followed by adaptive detection, which uses a machine learning model to continuously monitor and adjust the safety mechanisms based on real time data and offers more accurate threats than the static methods used in the traditional approach[3]. Finally, the dynamic recommendation phase benefits from advanced AI techniques to generate individual safety strategies based on the landscape of the developed danger and unique properties of the WIoT. This ability to suggest security measures dynamic strengthens the flexibility of the system against several types of attacks, making it more effective in the scenarios where conditions change rapidly.[4]

The main contribution depends on the integration of these AI-operated techniques that are PLS for WIoT. Unlike prior studies that focus on the rule-based or manual recovery approach, your work includes machine learning models that can develop over time. This allows for more intelligent and adaptive security measures that especially fit the dynamic nature of the wireless IoT environment. Changes in static, predetermined reactions to data-driven models represent a significant advance, so that the security system can learn and be suitable for new types of threats. In addition, not only exists literature, but also presents practical analysis and future approach to this integration and places your work as a bridge between the future of current research and intelligent to achieve adaptive security. This is a comprehensive approach, a combination of theoretical exploration, experimental verification, and forward-looking insight, and separates the paper from existing studies, which provides a comprehensive and practical map to apply machine learning techniques in the PLS for the WIoT network.

2. Illustration of non-DL based and DL-based diagram

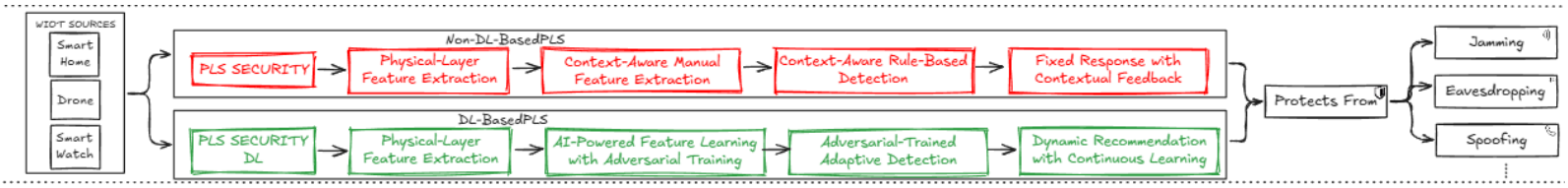

Figure 2. Physical-Layer Security in WIoT Systems with non-DL and DL based PLS.

In this diagram we explain the difference between DL-based and non- DL -based in protecting Physical layer Security. The diagram consists of two different approaches:

- **Non-DL-based PLS:**

  PLS Security begins with certainty, followed by physical layer feature extraction. This phase involves extracting key features from the physical layer of the network, which is manually selected based on predetermined criteria. Thereafter, reference - context manual function extraction is used, which includes relevant information to further refine the feature set. However, this approach is stable and limited in its ability to adapt to changes over time[5]. Thereafter, the reference Context -Aware-Rule -Based Detection step introduces rule -based methods that define fixed detection limits, which are defined using the features and relevant data extracted. Finally, the fixed response responds with the relevant response phase to potential threats based on predetermined rules without adaptive learning, leading to less flexible safety measures[6]

- **DL-based PLS:**
  DL-based PLS approach, defined in green, introduces more sophisticated and dynamic security mechanisms through intensive learning integration. After the first PLS security step, the system uses physical layer feature extraction but moves toward learning AI-powered feature learning with hostility training. Here, deep learning models, including unfavorable training techniques, are used to learn the relevant features of physical layer data automatically, end the need for manual feature extraction and improve the system's ability to manage complex network conditions[7]. The next phase is known as Adversarial-Trained Adaptive Detection, which improves the accuracy of the detection of the training model to identify and optimize the dangers by means of adversarial examples, which improves the strength of the detection system. Finally, dynamic recommendations with constant learning provide real -time, data -driven safety recommendations that develop based on continuous learning from new data and ensure that the systems adapt to the dangers of the environment.[8]

  We can compromise the two techniques from protecting WIoT systems from the perspective of attack vectors including Jamming, Eavesdropping, and Spoofing but the DL-Based solution provides significant enhancements and advantages over the static non-DL-Based solution. The contribution by using DL in dynamic WIoT system moving from traditional to reach out the power of these techniques and evolving the range of security challenges.

References

[1] Z. Rehman, N. Tariq, S. A. Moqurrab, J. Yoo, and G. Srivastava, “Machine learning and internet of things applications in enterprise architectures: Solutions, challenges, and open issues,” *Expert Syst*, vol. 41, no. 1, Jan. 2024, doi: 10.1111/exsy.13467.

[2] H. Hellström *et al.*, “Wireless for Machine Learning: A Survey,” *Foundations and Trends® in Signal Processing*, vol. 15, no. 4, pp. 290–399, 2022, doi: 10.1561/2000000114.

[3] O. Aouedi *et al.*, “A Survey on Intelligent Internet of Things: Applications, Security, Privacy, and Future Directions,” Jun. 2024.

[4] J. Jagannath, N. Polosky, A. Jagannath, F. Restuccia, and T. Melodia, “Machine learning for wireless communications in the Internet of Things: A comprehensive survey,” *Ad Hoc Networks*, vol. 93, p. 101913, Oct. 2019, doi: 10.1016/j.adhoc.2019.101913.

[5] N. Wang, P. Wang, A. Alipour-Fanid, L. Jiao, and K. Zeng, “Physical-Layer Security of 5G Wireless Networks for IoT: Challenges and Opportunities,” *IEEE Internet Things J*, vol. 6, no. 5, pp. 8169–8181, Oct. 2019, doi: 10.1109/JIOT.2019.2927379.

[6] W. Shi *et al.*, “Physical Layer Security Techniques for Future Wireless Networks,” Dec. 2021.

[7] Y. E. Sagduyu, Y. Shi, and T. Erpek, “IoT Network Security from the Perspective of Adversarial Deep Learning,” May 2019.

[8] A. Uprety and D. B. Rawat, “Reinforcement Learning for IoT Security: A Comprehensive Survey,” Feb. 2021, doi: 10.1109/JIOT.2020.3040957.