Avinashilingam Institute for Home Science and Higher Education for Women,

Deemed to be University, Estd. u/s 3 of UGC Act 1956, Category A by MHRD
Re-accredited with 'A++' Grade by NAAC. CGPA 3.65/4, Category I by UGC,
Coimbatore – 641 043, Tamil Nadu India.

Department of Physics and Information Technology

01. Title : **Energy Efficient Intrusion Detection System for Zigbee based Wireless Sensor Networks using Machine Learning Techniques**

[Project Reference No:No. AIHS@HE/R/2022/10204
Project File No. Avinuty/Seed/SPSCS-2021-22/002; Dated: 25.03.2022]

02. PI, details : **Dr. V.Sasirekha**
Assistant Professor (SS), Department of Physics,
Avinashilingam Institute for Home Science and Higher Education
for Women, Coimbatore – 641 043, Tamil Nadu, India
Email ID: sasirekha_phy@avinuty.ac.in

Co PI : **Dr.D.Shanmugapriya**
Dr.D.Nethra Pingala Suthishni
Assistant Professor, Department of Information Technology,,
Avinashilingam Institute for Home Science and Higher Education
for Women, Coimbatore – 641 043, Tamil Nadu, India
Email ID: shanmugapriya_it@avinuty.ac.in, nethra_it@avinuty.ac.in

03. Source of funding : **AIHSHEW, IQAC, Seed Money Project Grants , 2022 – 2023**

04. Abstract :

ABSTRACT

ZigBee-based WSNs are now widely employed in a variety of real-world applications, including sustainable control, military applications, healthcare, logistics, habitat monitoring, and home security networks. Apart from consumer and industry adoption, one of the primary problems of ZigBee-based WSNs is security. Despite the fact that the ZigBee communication protocol has many appealing features such as low cost, low power consumption, and low complexity, ZigBee-based WSN networks are vulnerable to a variety of security attacks due to the open nature of the wireless communication channels and the deployment of nodes in hostile environments. As a result, security is a prerequisite for these networks. Although security solutions like as authentication, cryptography, or key management approaches improve the security of ZigBee-based WSNs, they are not appropriate for resource-constrained networks, and they also require more energy for attack detection. Because standard cryptography-based security measures are ineffective against such attacks, a practical security defence technique called Intrusion Detection System is required to strengthen the security of ZigBee-based WSNs. As a

result, a unique and lightweight energy efficient IDS for resource restricted ZigBee-based WSN is needed. Machine learning algorithms can be employed in this project to classify intrusions and to enhance the security features in the sensor network. A robust and energy efficient Intrusion Detection System that can identify the probe and Denial of Sevice (DoS) attacks is proposed for protection of zigbee based wireless sensor networks.

05. Outcome of the project :

- A software for "Energy Efficient Intrusion Detection System for Zigbee based Wireless Sensor Networks using Machine Learning Techniques"
- Minimum Two Publications in Scopus/WoS indexed Journals/Conference Proceedings

06. Societal Impact:

The understanding regarding the traffic dynamics within WSNs provide a basis for further works on network optimization and anomaly detection for WSNs. As WSNs uses sensor nodes to collect data from a smart grid environment, smart grids have become popular intrusion targets. These data are transported to the cloud, which is a vast network of supercomputers that delivers a variety of services to smart infrastructures including smart homes and buildings. These can provide attackers a lot of room to launch damaging cyberattacks. The construction of a strong framework system for detecting intrusions based on the machine learning techniques is a novel aspect of this suggested research. When a WSN is assaulted by a probe attack, the attacker attempts to map out the network by gathering information about the target machine or network. And, Denial-of-Service (DoS) attack tends to be the fundamental threat to the functioning of wireless sensor network. When a sensor network is attacked by these two attacks, it gradually degrades the network's functionality and overall performance. Common security architecture with an intrusion detection system (IDS), which offers visibility into system's actions and allows for prompt detection and reaction to any undesirable events, becomes significant.

	20/9/22	20/9/22	20/9/22
PI	**Co-PI**	**HOD**	**Dean**