# Abstract

*Wireless Sensor Networks* (WSNs), in recent times, have become one of the most promising network solutions with a wide range of applications in agriculture, health and military environments. Despite these promising applications, sensor *nodes* in WSN are vulnerable to security attacks, one of which is *virtual jamming*. The goal of this report is to develop a system that can protect data from *virtual jamming* attacks using *neural networks technology*. To evaluate the performance of the proposed system, *the confusion matrix* is used as the main evaluation tool. *The confusion matrix* will make it possible to measure the extent to which the system is able to distinguish between normal conditions and *virtual jamming attacks*. Evaluation of the level of detection accuracy, precision, *recall*, and F1 value is carried out to provide an in-depth understanding of the effectiveness of the system.

**Keywords**: *wireless sensor networks, virtual jamming, neural networks, confusion matrix.*