Abstract

The use of wireless networks is expanding in Internet of Things technology, especially in the healthcare sector. It is projected that the Wireless Sensor Network industry in the healthcare sector will reach 10.34 million by 2025. However, WSNs are vulnerable to cyber attacks, including jamming attacks which can be classified into physical and virtual jamming. Denial of Service (DoS) attacks take advantage of network resource limitations by constantly sending excessive data to attack the network. Jamming attacks on WSNs are dangerous because they do not require specialized software or hardware. Common jamming attacks on WSNs include constant, reactive, deceptive, and random attacks. Random jamming attacks, as part of reactive jamming attacks, use transmitters to block wireless transmissions or disrupt important messages. Random jamming causes network performance degradation and blocks packet delivery. The attacker provides interference by sending radio wave signals or blocking messages from reaching the destination. Decision Tree is an effective classification and prediction method, often used in data mining. This method is suitable for detecting jamming attacks because it can transform large data into an easy-to-understand decision tree. The limitations of this research include protection against virtual jamming using the DT method and analysis of jamming attacks based on network data. From the results of the DT method, the accuracy of using this method is 96.92%, which means that the rate of detecting jamming attacks is very accurate.