Resumen

Las redes inalámbricas Wifi hoy en día son las redes que más abundan debido a los beneficios que estas presentan, como son el de movilidad. Sin embargo, a pesar de que el estándar que define su funcionamiento, el estándar 802.11, se desarrolló hace muchos años, este todavía cuenta con falencias y vulnerabilidades que no han sido corregidas hasta el día de hoy. Hoy en día existen diferentes ataques a redes inalámbricas Wifi que comprometen uno de los aspectos claves que toda red debe poseer: disponibilidad. Ataques de denegación de servicio comprometen y entorpecen la comunicación entre los dispositivos que pertenecen a la red inalámbrica Wifi. Además de estos ataques de denegación de servicio, existen otros tipos de ataques que intentan apropiarse de los datos sensibles de los mismos, usando técnicas y métodos que engañan a los usuarios y hacen que estos se conecten a redes falsas creadas por atacantes. El presente proyecto tiene como objetivo diseñar e implementar un sistema de detección de intrusiones para detectar ataques a redes inalámbricas Wifi. Para la implementación del sistema se utilizó herramientas de Big Data como son: Apache Spark, Kafka y Elasticsearch. El sistema usa el modelo de machine learning, Random Forest, para clasificar todo el tráfico de la red y diferenciar tramas normales de las tramas maliciosas creadas por un atacante. Los resultados se analizan y visualizan en un Dashboard creado en Kibana.

Palabras Clave:

- **BIG DATA**
- **MACHINE LEARNING**
- **SISTEMA DE DETECCIÓN DE INTRUSIONES**

Abstract

Wi-Fi wireless networks are nowadays the most abundant networks due to the benefits they offer, such as mobility. However, even though the standard that defines their operation, the 802.11 standard, was developed many years ago, it still has flaws and vulnerabilities that have not been corrected to date. Today there are several attacks on wireless Wi-Fi networks that compromise one of the key aspects that every network must have: availability. Denial-of-service attacks compromise and hinder communication between devices belonging to the wireless Wi-Fi network. In addition to these denial-of-service attacks, there are other types of attacks that attempt to appropriate sensitive data from them, using techniques and methods that deceive users and make them connect to fake networks created by attackers. The present project aims to design and implement an intrusion detection system to detect attacks on wireless Wi-Fi networks. For the implementation of the system Big Data tools were used such as: Apache Spark, Kafka and Elasticsearch. The system uses the machine learning model, Random Forest, to classify all network traffic and differentiate normal frames from malicious frames created by an attacker. The results are analyzed and visualized in a Dashboard created in Kibana.

Keywords:

- **BIG DATA**
- **MACHINE LEARNING**
- **INTRUSION DETECTION SYSTEM**