ABSTRACT

Critical infrastructure, such as communication systems and networks, is an important component in maintaining the stability and security of a country or organization. However, with the development of technology, threats to critical infrastructure are also increasingly complex. One threat that often appears is the FakeBTS (Base Transceiver Station) attack which aims to disrupt and steal data from telecommunication networks.

In this research, the implementation of Independent Station was carried out as a solution to detect the presence of FakeBTS in critical infrastructure areas. Independent Station is a system that uses independent transmitting stations installed around critical infrastructure areas, such as government facilities, airports or military installations. This system aims to monitor existing telecommunications networks and detect any suspicious activity that can be associated with the presence of FakeBTS.Independent Station implementation involves the use of specially developed hardware and software. The hardware consists of independent transmitting stations capable of collecting data from the surrounding telecommunications network. The software is designed to analyze collected data and use sophisticated detection algorithms to identify abnormal behavior patterns that may indicate the presence of FakeBTS.The experimental results show that the implementation of Independent Station can produce a reliable detection of the existence of FakeBTS.

This system is capable of identifying suspicious network patterns, such as changing bitrates and RSRP. By using this fakeBTS detection machine, it is expected to help reduce more serious attacks from fakeBTS abuse. This research has important implications in the field of critical infrastructure security. Furthermore, the findings of this research can also be used as a basis for developing more advanced and effective detection systems to address the evolving threats in critical infrastructure security.

Keywords: FakeBTS, Critical Infrastructure, Security.