ABSTRACT

Along with the times, telecommunications is one of the vital aspects in human life. Thus making the demands for an increase from 4G technology services to 5G technology even greater. All developments in 5G technology are expected to be combined to make 5G services more effective by enabling more people to deliver things faster and more conveniently than previous technologies. In line with its development, there are many open sources that provide 5G core network services to be able to help agencies, researchers create and simulate their own 5G networks privately. However, for the construction of a private cellular network using open source, further consideration needs to be given regarding its functionality and non-functionality.

In this study, the author will conduct a simulation using the open source *Free*5GC and test and analyze the security side of the open source 5G core. Testing is done using Distributed Denial of Service (DDoS) attacks. This attack is intended to *flood* the 5G service core network using high traffic. So, by using the attack concept, we can measure the effect of attacks on security parameters on the availability side of 5G network security.

From the test results, it is found that the network that has been built and run when it gets a DDoS attack has an impact on the quality of service such as the bandwidth flowed by *Free*5GC decreases and has an impact on CPU usage and increased network traffic due to incoming DDoS attacks. Then, the core network function (AMF) components that are in 5G service experience errors or crashes after getting a DDoS attack with a large packet delivery. Thus, users cannot use the service because if an error occurs in the core network function (AMF), the connection to the NAM and UE will also be lost.

Keywords: 5G Network, *Telco Cloud*, Network Security, Private Cellular.