

## ***ABSTRACT***

*In the current era, Wireless Sensor Network (WSN) has started being implemented in various areas of life, such as health, environment, etc. And one of the applicative form of WSN that currently being applied at this time is for monitoring, such as environmental control to monitor the state of an environment. WSN is formed from multiple sensor device, or called sensor nodes, that are connected via a wireless network (wireless) and can exchange data in real-time. The sensor node is small sized, so it has a limited resources to do the computation process, especially in ensuring the security aspects such as confidentiality, integrity and authenticity. That's why it takes a security protocol that not only can guarantee the security aspects but also can minimize the overhead of the sensor device. To ensure the security aspects in WSN, a securing method like Cipher Block Chaining (CBC) and Message Authentication Code (MAC) are used. This research will use two security protocols, TinySec and Link-Layer Security Protocol (LLSP). Those two protocols will be tested against each other's through a simulation using NS-3 simulator. Then it will show the performance level of each protocol and compare them. The performance parameters that will be used are energy consumption, confidentiality, integrity and authentication. Based on system testing, we can draw a conclusion that LLSP can reduce energy consumption up to 15% compared to TinySec. It's caused by a differences in byte length for overhead communication.*

**Keywords:** *Wireless sensor network (WSN), Security protocol, TinySec, Link-Layer Security Protocol (LLSP).*