ABSTRACT

The IEEE 802.15.4 standard is a protocol development standard that is applied for most of industrial wireless sensor network technology. Data security elements in industrial wireless sensor networks shall be considered due to the impact of the disruption that arises will be able to give a directly impact on the safety of workers, equipment and environment. Encryption method is a general method used in data protection on a wireless sensor network system.

Physical layer encryption using Rabbit stream cipher algorithm will be proposed as an alternative method of data protection in industrial wireless sensor network application systems which commonly apply a block cipher encryption methods in the upper layer as protection method. The Rabbit algorithm will be compared with the RC4 algorithm that has been previously studied to measure the security assurance level, resource utilization and industrial standard compliance.

From the simulation results, Rabbit algorithm with a shorter number of keys and fewer cipher text can provide better results for the value of avalanche effect, entropy and CPU usage compared to the RC4 algorithm. Although obtaining varied results on memory usage and end to end delay, Rabbit algorithm on a certain number of nodes can still meet industry requirements for oil and gas sector applications.

Keywords: *IEEE 802.15.4, Physical Layer Encryption, Rabbit Algorithm, Industrial WSN, Oil and Gas Sector*.

ABSTRAK

Standar IEEE 802.15.4 merupakan standar acuan pengembangan protokol yang diterapkan untuk teknologi *industrial wireless sensor network* pada saat ini. Unsur keamanan data dalam *industrial wireless sensor network* perlu untuk diperhatikan karena dampak gangguan yang timbul akan dapat berpengaruh secara langsung pada proses industri yang sedang beroperasi dan berdampak pada keselamatan pekerja, peralatan dan lingkungan serta keekonomian. Metode enkripsi adalah metode umum yang dipergunakan dalam perlindungan data pada sistem *wireless sensor network.*

Metode enkripsi pada *layer physical* dengan menggunakan algoritma *stream cipher Rabbit* dipergunakan sebagai metode alternatif perlindungan data pada sistem aplikasi *industrial wireless sensor network* yang mana pada umumnya menggunakan metode enkripsi *block cipher* pada lapisan *upper layer*. Algoritma Rabbit akan dibandingkan dengan algoritma RC4 yang telah diteliti sebelumnya.

Dari hasil simulasi, algoritma Rabbit dengan jumlah kunci yang lebih pendek dan *cipher text* yang lebih sedikit dapat memberikan hasil yang lebih baik untuk nilai *avalanche effect*, *entrophy* dan penggunaan CPU dibandingkan dengan algoritma RC4. Meskipun mendapatkan hasil yang bervariasi pada penggunaan memori dan *end to end delay*, algoritma Rabbit pada jumlah node tertentu masih dapat memenuhi standar kebutuhan industri untuk aplikasi sektor migas.

Kata Kunci: *IEEE 802.15.4, Physical Layer Encryption, Algoritma Rabbit, Industrial WSN, Sektor migas.*