Analisa Enkripsi pada Protokol IEEE 802.15.4 dengan Algoritma Rabbit untuk Aplikasi Industri Sektor Migas

R. Benny Gandara
Teknik Elektro, Universitas Mercu Buana, Jakarta
Bennygandara.bg@gmail.com

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.

***Keywords**: IEEE 802.15.4, Physical Layer Encryption, Algoritma Rabbit, Industrial WSN, Sektor migas*

1. PENDAHULUAN

Teknologi *Wireless Sensor Network* (WSN) menawarkan beberapa keunggulan dibandingkan dengan penggunaan teknologi sensor kabel yang umumnya dipergunakan pada saat ini, terutama dalam penerapannya disektor industri sebagai alat pendukung dalam sistem proses sistem otomasi. Beberapa keunggulan yang ditawarkan dalam teknologi *Industrial Wireless Sensor Network* (IWSN) ini antara lain adalah: fleksibilitas, skalabilitas dan nilai keekonomian yang lebih kompetitif. Namun selain dari sisi keunggulan yang ditawarkannya, beberapa keterbatasan WSN seperti yang terkait dengan : sumber daya komputasi, sumber daya energi, jarak jangkau, kapasitas transfer data yang terbatas dan ancaman keamanan yang

menyertainya yang perlu untuk dipertimbangkan [1] nantinya.

Ketentuan standar yang diterapkan pada teknologi WSN pada sektor industri memiliki aturan dan pertimbangan yang berbeda, dibandingkan dengan teknologi WSN yang lain karena dampak gangguan yang timbul dari gangguan keamanan dan kehandalan pada IWSN akan dapat berpengaruh secara langsung terhadap fungsi operasional dan keselamatan pekerja, serta lingkungan disekitarnya [2]. Standar metode pengamanan yang dilakukan pada WSN seperti pada penelitian [2][3] menjelaskan bahwa sebagian besar menggunakan metode enkripsi dan prosesnya dilakukan pada struktur lapisan bagian atas (*upper layer*) setelah lapisan fisik (*physical* layer) WSN seperti pada penjelasan Tabel 1.

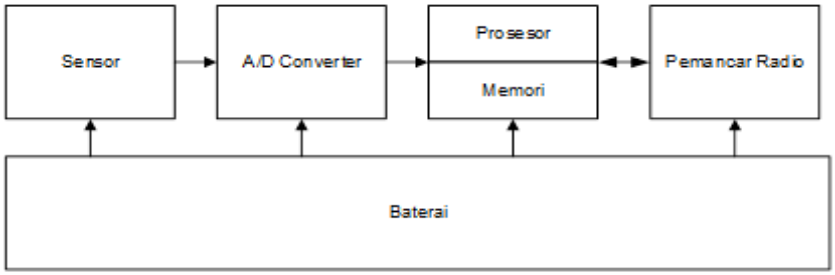
Tabel 1 Informasi Perbandingan Lapisan Layanan Keamanan IWSN [3]

No	Protokol Lapisan Keamanan	Protokol
1	Network Layer	Zigbee
2	Application support Layer	
3	Data Link	WirelessHART
4	Network Layer	
5	Link Layer	ISA 100.11a
6	Transport Layer	
7	Link Layer	WIA-PIA
8	Application support Layer	

Namun metode enkripsi pada lapisan diatas (*upper layer*) ini masih memiliki kelemahan ancaman keamanan berupa: *Denial of Service* (DoS), pemborosan energi, *analysis traffic* dan serangan *network flood* menurut penelitian [2][4]. Oleh karena itu belakangan ini banyak muncul penelitian yang dilakukan untuk dapat mengatasi masalah tersebut, yang antara lain diantaranya dengan menggunakan metode pengamanan layer fisik (*Physical Layer Security*, *PLS*) dan metode pengamanan enkripsi pada lapisan fisik (*Physical Layer Encryption*, *PLE*) seperti pada pembahasan penelitian [4]. Dan metode enkripsi *stream cipher* dengan menggunakan algoritma Rabbit pada layer fisik akan diajukan pada penelitian ini, sebagai salah satu alternatif bentuk perlindungan keamanan data pada perangkat IWSN.

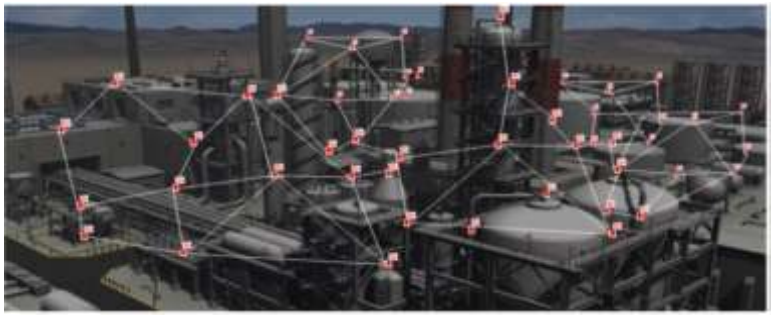
2. TEKNOLOGI *WIRELESS SENSOR NETWORK*

Wireless Sensor Network (WSN) adalah jenis jaringan nirkabel yang dilengkapi perangkat sensor otonom (*node*) yang didistribusikan secara spasial dan bekerja secara kolaboratif dengan sistem lain untuk dipergunakan dalam berbagai sistm aplikasi. Sebuah *node* dalam WSN akan terdiri beberapa unit subsistem seperti pada penjelasan Gambar 1, yang terdiri dari: sensor, prosesor, baterai, dan unit komunikasi radio.



Gambar 1 Sistem Arsitektur *node* WSN

Sifat kolaboratif pada teknologi WSN memungkinkan penggunaan yang fleksibel untuk dilakukannya penambahan *node* baru ke dalam jaringan dan dapat dioperasikan dengan berbagai jenis topologi jaringan yang berbeda-beda. *Industrial Wireless Sensor Network* (IWSN) adalah merupakan salah satu bagian dari teknologi WSN yang secara khusus ditujukan untuk aplikasi industri [1]. Penerapan IWSN dalam sektor industri pada saat ini sudah diimplementasikan dalam untuk beberapa sistem yang terkait dengan: sistem pengawasan (*monitoring*), kendali proses dengan sistem *open-loop* dan *close loop* serta sistem tanggap darurat (*emergency respond system*). Secara umum topologi IWSN yang di pergunakan pada saat ini adalah dengan tipe *star*, *mesh*, dan *tree* [1].



Gambar 2 Contoh jaringan IWSN

2.1 Standar Protokol WSN dan Protokol IEEE 802.15.4

Struktur lapisan standar komunikasi data pada WSN terdiri dari beberapa bagian yaitu : *physical, data link, network, transport* dan *application layer* ,yang tugas dari masing-masing lapisan akan dijelaskan seperti pada Tabel 2 [5].

Tabel 2 Standar Struktur lapisan komunikasi data WSN [5]

APPLICATION LAYER	Data aggregation, interactions with the end user
TRANSPORT LAYER	Reliable transport of data
NETWORK LAYER	Routing, networking, topology management
DATA LINK LAYER	Medium access and error control, data frame detection, multiplexing
PHYSICAL LAYER	Modulation, frequency and channel selection, signal processing

Keterkaitan antara struktur lapisan komunikasi data pada WSN dan penerapan protokol IEEE 802.15.4 pada sistem tersebut dapat dijelaskan seperti pada tabel 3 yang mengacu pada penelitian [5].

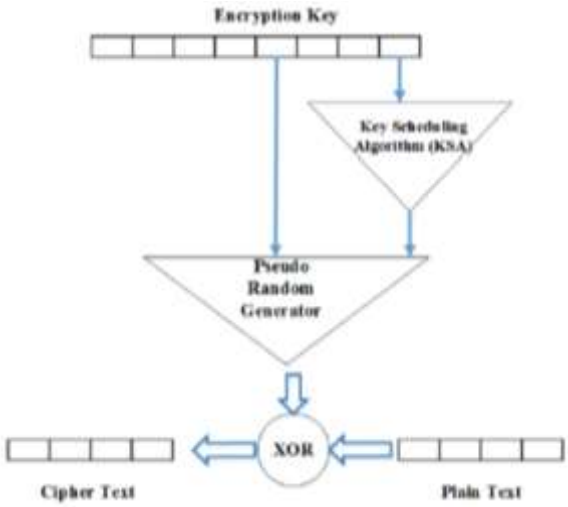
Tabel 3 Alokasi protokol IEEE 802.15.4 pada WSN

Layers	Protocols
Transport/Application	CoAP
Network/Routing	RPL, BCP, CTP
Adaptation	6LoWPAN
MAC	IEEE 802.15.4.e, B-MAC
Physical	IEEE 802.15.4

IEEE 802.15.4 adalah standar protokol yang ditetapkan oleh kelompok kerja IEEE 802.15.4 untuk perangkat komunikasi data yang beroperasi pada jaringan komunikasi nirkabel jarak pendek dengan kapasitas data transfer yang rendah (*Low Rate Wireless Private Network*), yang memiliki jarak maksimum sampai dengan 300 meter [1]. Dalam standar ini didefinisikan, bentuk susunan lapisan protokol terdiri dari dua tingkat lapisan, yaitu lapisan *physical* dan *Medium Access Control* (MAC). Dimana pada spesifikasi lapisan fisik (*physical layer*) mengatur tentang: persyaratan alokasi frekuensi, skema modulasi, penyebaran parameter (*spreading parameter*), pengaturan daya transmisi, rincian saluran dan penugasan saluran [1]. Sedangkan lapisan MAC berfungsi sebagai pengatur akses protokol ke media fisik jaringan , mengatur komunikasi antar *node*, manajemen *beacon,* pengaturan CSMA/CA dan dukungan keamanan pada perangkat [1].

2.2 Enkripsi Simetris RC4

Enkripsi RC4 adalah salah satu jenis enkripsi *stream cipher* dengan algoritma kunci simetris, dirancang oleh Ron Rivest pada tahun 1987. Secara teori algoritma enkirpsi RC4 dapat menggunakan ukuran panjang kunci sebesar 2048 bit ,namun berdasarkan standar uji *test vector* oleh *Internet Engineering Task Force* (IETF) hanya direkomendasikan sampai dengan ukuran 256 bit. Dua proses utama dalam proses algoritma RC4 terdiri dari: *Key Scheduling Algorithm* (KSA) dan *Pseudo Random Generation Algorithm* (PRGA). Pada proses KSA ini, pembentukan tabel S-Box “S “(tabel array S) dan Kunci (tabel array [K]) akan di permutasi sebanyak 256 iterasi. Dan selanjutnya tabel array KSA ini kemudian digunakan pada (PRGA) untuk dapat menghasilkan *key stream* yang jumlahnya sama dengan jumlah banyaknya karakter *plaintext,* dan kemudian akan di-XORkan dengan *plaintext.* Byte K akan di-XOR-kan dengan *plaintext* untuk menghasilkan *ciphertext* atau akan di-XOR-kan dengan *ciphertext* untuk menghasilkan *plain text.* Dengan algoritma PRGA seperti pada penelitian [6]. Gambaran algoritma RC4 secara umum adalah mengacu pada Gambar 3[7].



Gambar 3 Algortima Enkripsi RC4 [7]

2.3 Kriptografi

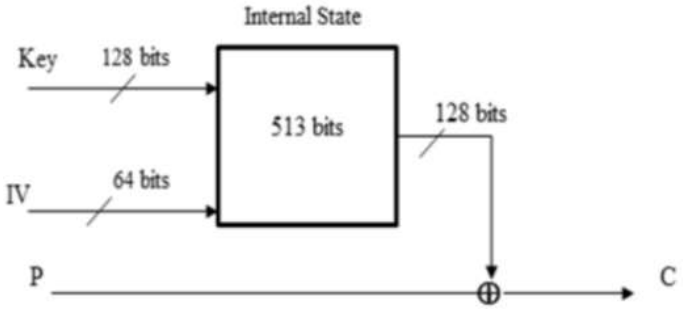
Kriptografi adalah teknik yang dipergunakan untuk merubah informasi yang tidak terlindungi untuk dirubah menjadi sebuah informasi yang tidak terbaca dan hanya dapat dibaca oleh pihak yang berhak. Keamanan pada kriptografi akan bergantung pada panjang kunci kriptografi yang dipergunakan selama dalam proses enkripsi [8] berlangsung. Tujuan mendasar dari penggunaan kriptografi adalah untuk menjaga kerahasiaan data, integritas data, autentikasi dan pencegahan penyangkalan. Istilah-istilah yang umum digunakan dalam kriptografi:

a. *Plain text* adalah informasi atau data asli yang akan dikirimkan dan dijadikan sebagai masukan dari sebuah proses kriptografi.
b. *Cipher text* adalah pesan yang telah rubah atau dikodekan dan siap untuk ditransmisikan.
c. *Cipher* adalah algoritma matematik yang dipergunakan untuk mengolah *plain text* menjadi *cipher text.*
d. Enkripsi adalah proses perubahan dari sebuah *plain text* menjadi *cipher text* dengan menggunakan metode atau algoritma tertentu.
e. Dekripsi adalah proses perubahan dari sebuah *cipher text* menjadi *plain text* dengan menggunakan metode tertentu.
f. *Stream Cipher* adalah metode enkripsi di mana aliran digit *cipher pseudorandom* dikombinasikan dengan digit teks biasa. Aliran digit *cipher pseudorandom* ini diterapkan ke setiap digit biner, satu bit pada satuan waktu yang sama.
g. *Entropy* adalah ukuran ketidakpastian yang terkait dengan variabel acak, sehingga semakin besar nilai *entropy* semakin baik kualitas algoritma yang dipergunakan [9].
h. *Avalanche effect* adalah ukuran yang dipergunakan untuk mengukur seberapa baik atau tidaknya sebuah algoritma enkripsi, dengan nilai minimum yang inginkan adalah lebih besar dari 50%. Rumus yang dipergunakan untuk perhitungan avalanche effect adalah seperti rumus 1 [9].

$$\textit{Avalanche Effect} = \frac{\Sigma \text{ bit\_berubah}}{\Sigma \text{bit\_total}} \times 100 \quad (1)$$

2.4 Enkripsi Simetris Rabbit

Algoritma Rabbit adalah salah salah algoritma keamanan *stream cipher* yang sudah distandarisasi oleh badan internasional ISO/ IEC, dengan kode ISO/IEC 18033-4. Algoritma ini menggunakan kunci rahasia 128 bit dan 64 bit untuk *initialization vector* (IV). Kunci rahasia dan IV dipergunakan untuk membangkitkan 128 bit blok *pseudo random*. Kemudian proses enkripsi dan dekripsinya lakukan dengan cara menggunakan logika XOR dengan input data dari data *pseudo random* dan *plaintext* ataupun *cipher text*. Ukuran dari status internal adalah 513 bit dibagi menjadi 8 variabel status dengan ukuran 32 bit, kedelapan variabel status di-update dengan 8 buah fungsi non-linear [10], dimana memiliki proses parameter seperti *Key* sebagai kunci, IV sebagai *initialization vector* , P sebagai *plain text* dan C sebagai *cipher text*,seperti informasi pada Gambar 4.



Gambar 4 Algoritma Enkripsi Rabbit [10]

2.5 Standar Industri WSN

Standar Industri aplikasi WSN telah diatur oleh badan standarisasi internasional seperti *International Society of Automation* (ISA), yang diklasifikasikan berdasarkan dari fungsi penggunaan alat, waktu proses yang dibutuhkan dan tingkat keamanan yang dibutuhkan, tabel informasi yang diperoleh dari penelitian [1].

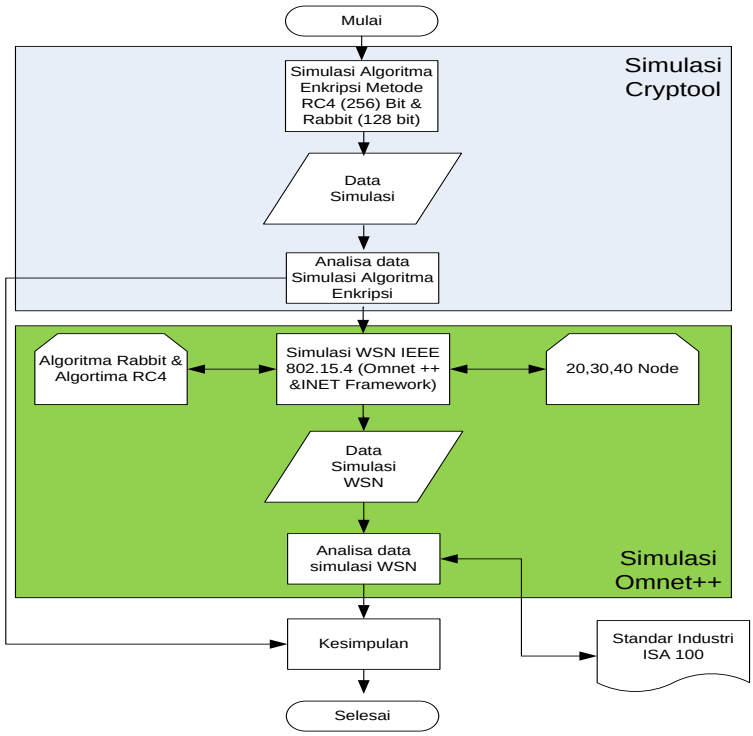
Tabel 4 Standar Industri WSN [1]

Sensor Network Application	Security Requirement	Update Frequency
Monitoring and Supervision		
Vibration Sensor	Low	Sec-days
Pressure Sensor	Low	1 Sec
Temperature Sensor	Low	5 Sec
Gas Detector	Low	1 Sec
Data Acquisition	Low	> 100 ms
Maintenance diagnosis	Low	Sec-days
Close Loop Control		
Control Valve	Medium to High	10-500 ms
Pressure Sensor	Medium to High	10-500 ms
Temperature Sensor	Medium to High	10-500 ms
Torque Sensor	Medium to High	10-500 ms
Variable Speed Drive	Medium to High	10-500 ms
Motion Control	Medium to High	10-500 ms
Control Machine Tools	High	1 -10 ms
Interlocking and Control		
Proximity Sensor	Medium to High	10-250 ms
Motor	Medium to High	10-250 ms
Valve	Medium to High	10-250 ms
Protection Relays	Medium to High	10-250 ms
Machinary and Tools	Medium to High	10-250 ms
Motion Control	Medium to High	10-250 ms

3. METODE SIMULASI KRIPTOGRAFI IWSN

3.1 Simulasi Algoritma Enkripsi IWSN

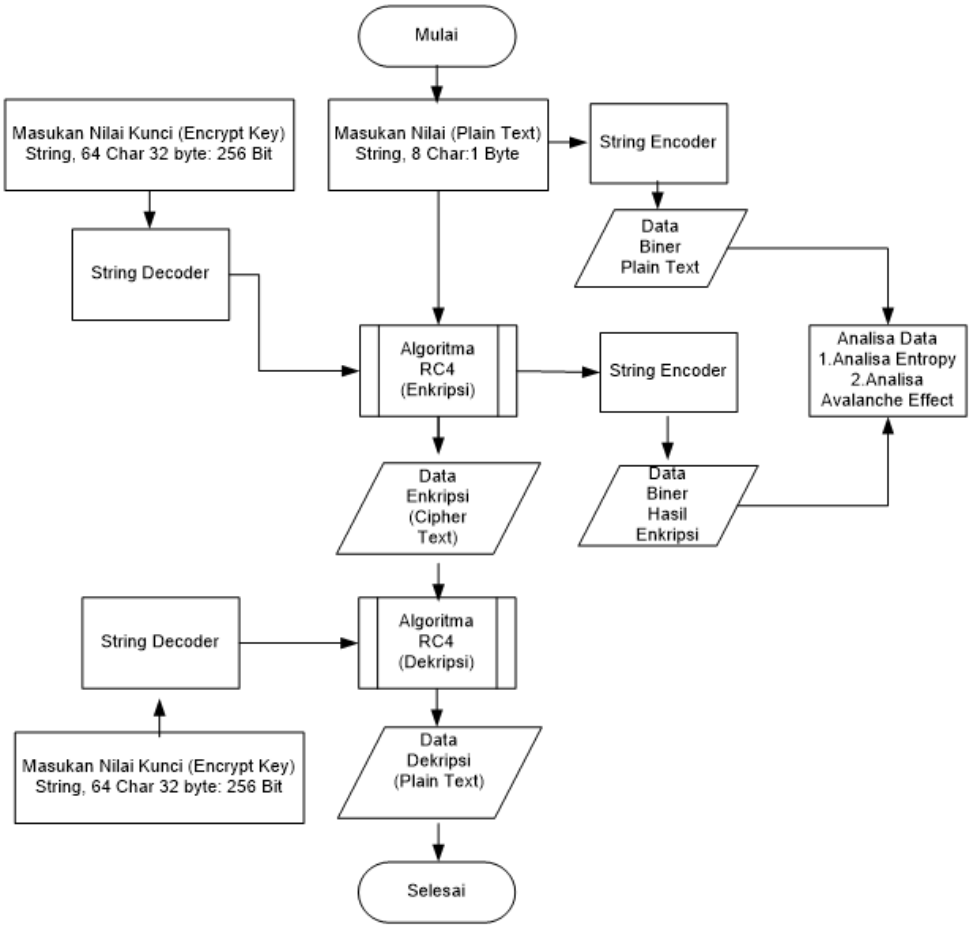
Dua metode algoritma akan dibandingkan dalam penelitian ini, yaitu metode enkripsi dengan menggunakan algoritma RC4 dan algoritma Rabbit.



Gambar 5 Diagram Alur Simulasi Algoritma dan IWSN

3.2 Simulasi Algoritma Enkripsi RC4

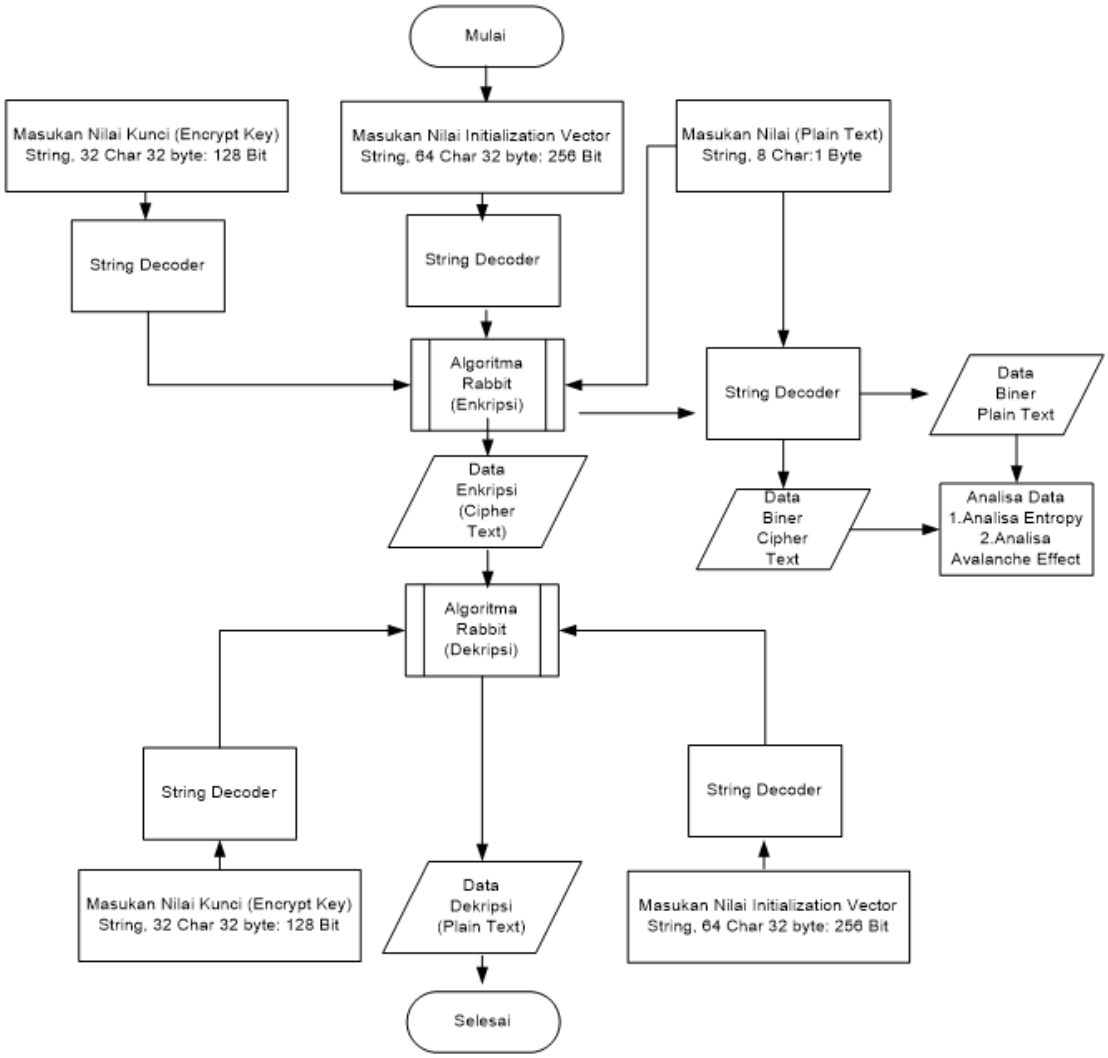
Simulasi enkripsi RC4 ini lakukan dengan Cryptool 2.1.73 dengan melakukan modifikasi *template library* algoritma RC4 yang telah tersedia pada program ini. *Template library* algoritma RC4 ini akan dipergunakan sebagai bagian sebuah proses yang kemudian perlu dirangkai dengan menambahkan beberapa fungsi tambahan *library* seperti : *text input, string encoder*, *string decoder* dan *text output*, untuk mendapatkan simulasi proses algoritma yang memiliki unsur : masukan, proses dan hasil. Dalam simulasi ini akan masukan nilai acak dengan tipe *string* sepanjang 8 karakter sebagai nilai *plain text*. Dan masukan panjang kunci dengan karakter acak hexadesimal dengan panjang ukuran 256 bit untuk diproses selanjutnya dalam blok algoritma RC4. Untuk keperluan pengambilan data pada penelitian, maka nilai dari *plain text* dan *cipher text* dikonversikan kedalam nilai biner untuk diambil dan analisa datanya. Hasil data adalah ukuran panjang data sebelum dan setelah dienkripsi serta perubahan nilai bitnya. Setelah uji simulasi dengan menggunakan versi 2.17.73 selesai dilakukan maka kemudian data dari hasil enkripsinya akan simulasikan dengan menggunakan versi 1.14.40 untuk pengujian nilai entropy enkripsi. Bentuk rancangan diagram alur untuk simulasi ini diilustrasikan seperti pada Gambar 6.



Gambar 6 Rancangan Diagram Alur Simulasi Algoritma RC4

3.3 Simulasi Algoritma Enkripsi Rabbit

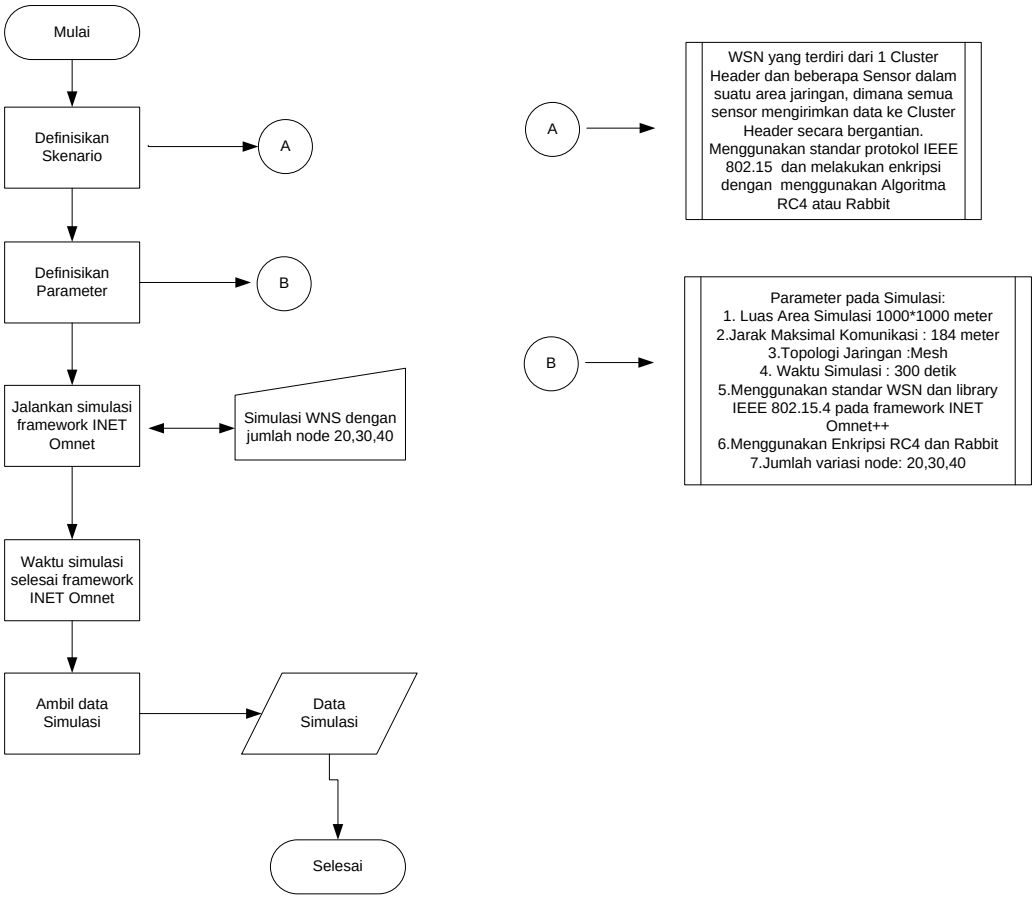
Simulasi enkripsi Rabbit ini dilakukan menggunakan perangkat Cryptool 2.1.73 dengan cara melakukan modifikasi *template library* algoritma Rabbit yang telah tersedia pada program ini. *Template library* algoritma Rabbit ini akan dipergunakan sebagai bagian sebuah proses, yang kemudian modifikasi dengan menambahkan beberapa fungsi tambahan *library* seperti : *text input, string encoder, string decoder* dan *text output*, untuk mendapatkan simulasi proses algoritma yang memiliki: nilai masukan, proses dan hasil keluaran. Dalam simulasi ini akan masukan nilai acak dengan tipe string sepanjang 8 karakter sebagai nilai *plain text*. Dan masukan panjang kunci dengan karakter acak hexadesimal dengan panjang ukuran 128 bit, serta masukan *initialization vector* sebesar 64 bit untuk diproses selanjutnya dalam blok algoritma Rabbit. Untuk keperluan pengambilan data pada penelitian, maka nilai dari *plain text* dan *cipher text* akan dikonversikan ke dalam nilai biner untuk diambil dan analisa datanya. Hasil data yang akan dipergunakan dari simulasi ini adalah ukuran panjang data setelah sebelum dan setelah dienkripsi serta perubahan nilai bitnya. Setelah uji simulasi dengan menggunakan versi 2.17.73 selesai dilakukan maka kemudian data dari hasil enkripsinya akan analisa dengan menggunakan Cryptool versi 1.14.40 untuk pengujian nilai *entropy* enkripsi. Dimana untuk ilustrasi mengenai diagram alur untuk simulasi ini terdapat pada Gambar 7.



Gambar 7 Rancangan Diagram Alur Simulasi Algoritma Rabbit

3.4 Enkripsi WSN Protokol IEEE 802.15.4

Skenario simulasi WSN pada penelitian ini akan menggunakan satu unit perangkat *Cluster Header* (CH) dan beberapa unit node sensor, dimana aliran data akan dikirimkan dari node sensor menuju CH akan dienkripsikan dengan menggunakan algoritma RC4 dan algoritma Rabbit. Sedangkan untuk pengaturan parameternya akan menggunakan luasan area simulasi sebesar 1000 meter persegi, penyebaran secara acak untuk penempatan node dengan menggunakan topologi *mesh* dan batasan jarak maksimal komunikasi sejauh 184 meter untuk jarak antar nodenya. Jumlah node sendiri akan divariasikan dengan 20 , 30 dan 40 jumlah unit node sensor untuk tujuan pengujian skalabilitas jaringan. Sedangkan untuk pengaturan parameter protokol IEEE 802.15.4 pada simulasi akan mengacu pada standar *library* INET, yang nantinya akan dimodifikasi sesuai dengan kebutuhan penelitian. Untuk ilustrasi rancangan alur simulasinya dapat dilihat pada Gambar 8. dan tabel parameter simulasi pada Tabel 5.



Gambar 7 Rancangan Alur Simulasi IWSN

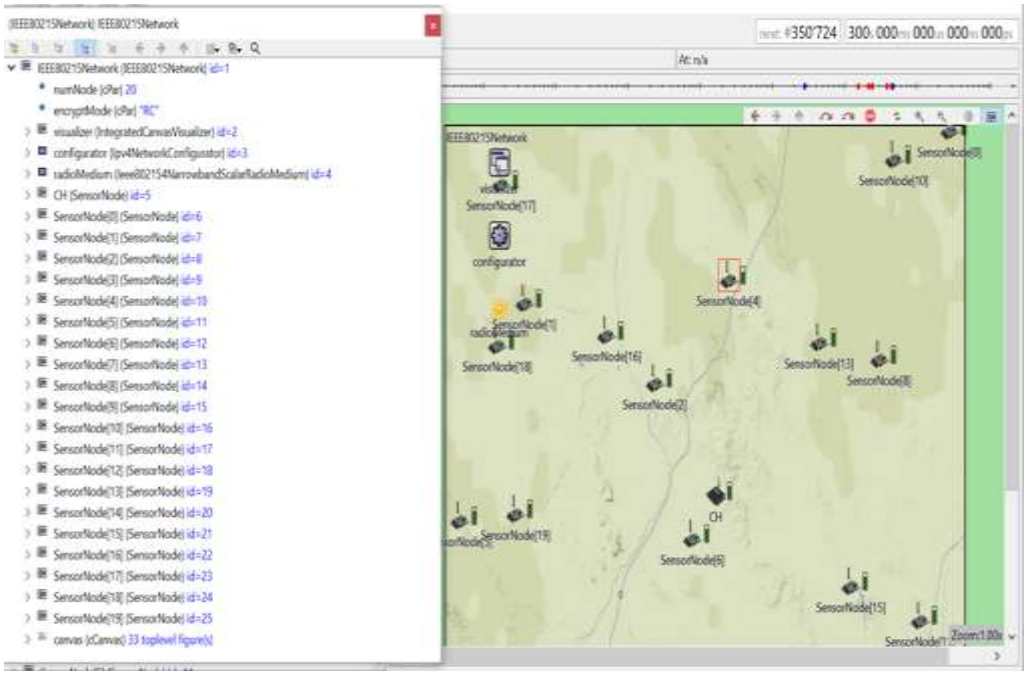
Tabel 5 Parameter Simulasi Enkripsi IWSN

No	Deskripsi	Nilai/Informasi
1	Luas Area Simulasi	1000 x 1000 Meter
2	Jarak Maksimal Komunikasi Jaringan	184 Meter
3	Topologi Jaringan	Mesh
4	Waktu Simulasi	300 Detik
5	Physical Layer	Library Omnet 802.15.4
6	Algoritma Enkripsi (1)	Stream Cipher RC-256 Bit
7	Algoritma Enkripsi (2)	Stream Cipher Rabbit
8	Jumlah Variasi Sensor Node	20,30,40

Modul *physical layer* IEEE 802.15.4 pada penelitian ini disimulasikan dengan menggunakan fungsi modul Ieee802154*NarrowBandScalarRadio*, dan fungsi modul IpV4*NetworkConfigurator* untuk pengaturan pengalamatan Internet *Protocol* (IP) pada perangkat dan pengaturan *routing table* statis dalam jaringan. Parameter lapisan *physical layer* pada modul ini akan mengacu pada standar IEEE 802.15.4 yang memiliki kriteria : frekuensi 2450 MHz DSSS, *symbol rate* 62,5, *bit rate* 250 Kbps, modulasi OQPSK dan *chiprate* 2000. Pengaturan nilai-nilai parameter pada simulasi dalam penelitian ini, sebagian besar masih menggunakan nilai standar yang telah tersedia dan ditetapkan oleh fungsi modul *library* INET. Modul *library* yang dipergunakan dalam simulasi ini dapat lihat pada Tabel 6 dan bentuk hasilnya pada Gambar 8.

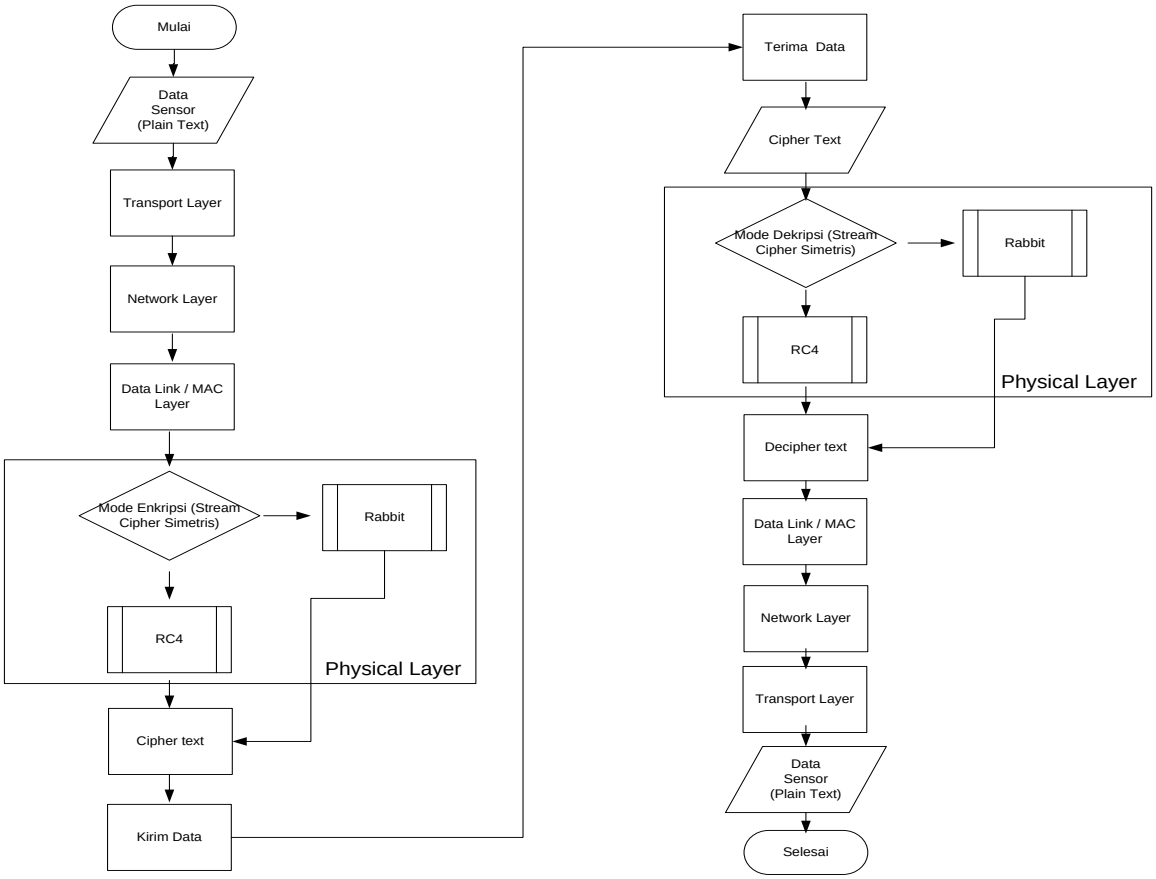
Tabel 6 Library INET Protokol IEEE 802.15.4

No	Perangkat Simulasi	Paket Library INET (Source code & Parameter)
1	IEEE80215Network.Configurator	
1.1	IpV4Network Configurator	src/inet/networklayer/configurator/ipv4/Ipv4NetworkConfigurator.ned
2	IEEE80215Radio.Medium	
2.1	Ieee802154NarrowBandScalarRadio	src/inet/physicallayer/ieee802154/packetlevel/Ieee802154NarrowbandScalarRadio.ned
3	ClusterHeader	
3.1	ClusterHeader (UdpSink)	src/inet/applications/udpapp/UdpSink.ned
4	SensorNode	
4.1	SensorNode (UdpBasicApp)	src/inet/applications/udpapp/UdpBasicApp.ned



Gambar 8 Simulasi Omnet IWSN

Bentuk rancangan diagram transformasi data dalam WSN dan metode enkripsi yang akan dibuat untuk simulasi penerapan algoritma RC4 dan algortima Rabbit dalam jaringan WSN pada lapisan fisik, dapat dilihat pada Gambar 9.



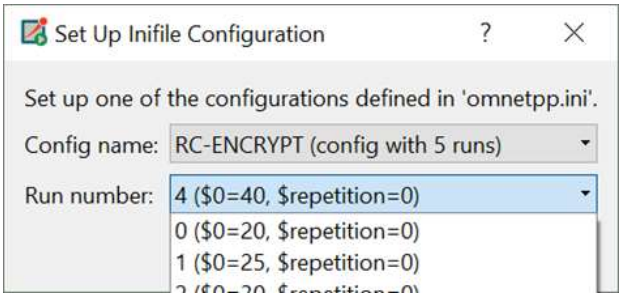
Gambar 9 Transformasi dan Enkripsi Data Simulasi IWSN

Dan ringkasan parameter simulasinya dapat dilihat dari Tabel 7, dimana untuk penjelasannya akan disimulasikan aliran data *plain text node* sensor yang akan ditransformasikan dari lapisan *layer application* dengan menggunakan modul Udp*BasicApp* akan dikirimkan kelapisan *transport layer* dan menggunakan modul Udp *transport layer* untuk berkomunikasi sampai dengan *layer physical,* kemudian menggunakan modul TCP *transport layer* untuk berkomunikasi dengan *layer network.* Selanjutnya pada *layer network* akan digunakan modul IpV4*NetwokLayer* yang didalamnya terdiri dari beberapa modul seperti : modul Ipv4N*odeConfigurator* yang berfungsi seperti jembatan untuk menghubungkan antara node dan modul konfigurator global jaringan, modul IpvRoutingTable untuk menyimpan tabel routing statis, modul IGMP (*Internet Group Management Protocol*) yang bekerja pada untuk menginformasikan router-router IP tentang keberadaan group-group jaringan multicast, modul ICMP (*Internet Control Message Protocol*) untuk keperluan analisa jaringan, modul ARP (*Address Resolution Protocol*) untuk fungsi pemetaan alamat IP menjadi alamat MAC dan modul IP untuk pengalamatan perangkat. Kemudian pada lapisan berikutnya, *link layer* dengan modul Ieee802154NarrowbandMac yang berfungsi sebagai protokol *Media Access Control* (MAC) yang mengatur lalu lintas jaringan dengan metode *Carrier Sense Multiple Access* (CSMA) untuk menghindari proses tabrakan dalam lalu lintas data. Terakhir pada tingkat *physical layer* dengan menggunakan modul Ieee802154NarrowbandScalarRadio yang memiliki sub modul untuk perangkat fisik terkait antenna dengan modul IAntenna, transmitter dengan modul ITransmitter, dan receiver dengan modul Ireceiver.

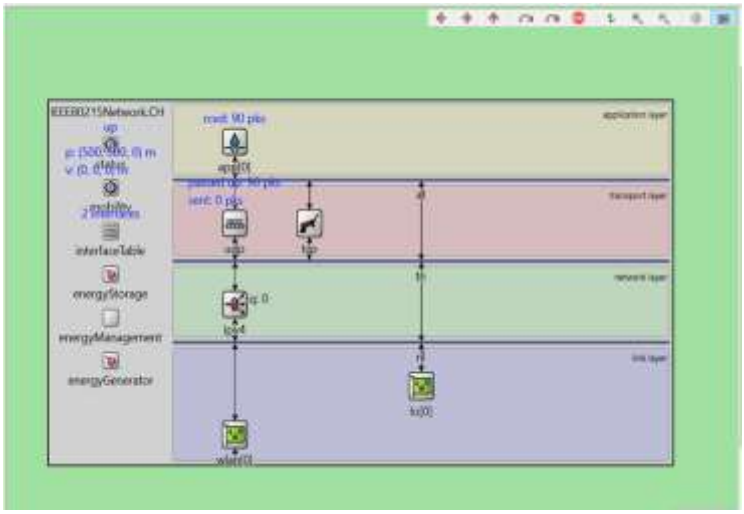
Tabel 7 Ringkasan Setting Parameter IWSN

NO	Model INET Framework 802.15.4	Paket Library INET (Source code & Parameter)	Model Layer
1	**Physical Layer**		Link Layer
1.1	Ieee802154NarrowBandScalarRadio	src/inet/physicallayer/ieee802154/packetlevel/Ieee802154NarrowbandScalarRadio.ned	
1.1.1	Antenna	src/inet/physicallayer/contract/packetlevel/IAntenna.ned	
1.1.2	Transmitter	src/inet/physicallayer/contract/packetlevel/ITransmitter.ned	
1.1.3	Receiver	src/inet/physicallayer/contract/packetlevel/IReceiver.ned	
1.1.4	Energy consumer	src/inet/power/contract/IEnergyConsumer.ned	
2	**MAC Protocol**	src/inet/linklayer/ieee802154/Ieee802154NarrowbandMac.ned	
3	**Network Interface**		Network Layer
3.1	Ieee802154NarrowBandInterface	src/inet/linklayer/ieee802154/Ieee802154NarrowbandInterface.ned	
4	**Network Layer**		
4.1	IpV4NetworkLayer	src/inet/networklayer/ipv4/Ipv4NetworkLayer.ned	
4.1.1	IpV4NodeConfigurator	src/inet/networklayer/configurator/ipv4/Ipv4NodeConfigurator.ned	
4.1.2	IpV4RoutingTable	src/inet/networklayer/ipv4/Ipv4RoutingTable.ned	
4.1.3	arp	src/inet/networklayer/contract/IArp.ned	
4.1.4	ip	src/inet/networklayer/ipv4/Ipv4.ned	
4.1.5	icmp	src/inet/networklayer/ipv4/Icmp.ned	
4.1.6	igmp	src/inet/networklayer/ipv4/Igmp.ned	
5	**Transport Layer**		Transport Layer
5.1	udp	src/inet/transportlayer/udp/Udp.ned	
5.2	tcp	src/inet/transportlayer/tcp/Tcp.ned	
6	**Application Layer**		Application layer
6.1	ClusterHeader (UdpSink)	src/inet/applications/udpapp/UdpSink.ned	

Dan untuk prosesnya enkripsi proses transformasi dan komunikasi data ini dilakukan pada *physical layer.* Algoritma enkripsi yang dipergunakan adalah algoritma RC4 dan algoritma Rabbit yang dalam proses pengujiannya simulasi akan dilakukan beberapa kali dengan format algoritma tertentu dan jumlah node tertentu seperti Gambar 10 dan Gambar 11, dimana aliran transformasi data bergerak dari lapisan *link layer* sampai dengan *physical layer* dengan menggunakan fungsi modul *loopback interface* dari *layer physical* sampai dengan *network layer* yang bertujuan untuk mengidentifikasi perangkat komunikasi, informasi routing dan melakukan *packet filtering*.



Gambar 10 Setup Konfigurasi Simulasi IWSN



Gambar 11 Transformasi dan Enkripsi Data Simulasi Omnet IWSN

4. DATA SIMULASI

Dari hasil percobaan dengan dua perangkat simulasi Cryptools dan OMNET ++ dihasilkan dua kelompok data simulasi terkait dengan pengukuran kualitas algoritma dan penerapannya pada protocol IEEE 802.15.4 dengan uji skalabilitas tertentu.

4.1 Data Enkripsi Algoritma RC4 dan Algoritma Rabbit

Dengan mengacu pada desain rancangan diagram alur simulasi algoritma RC4 seperti pada Gambar 6 dan menggunakan peralatan simulasi Cryptool, maka percobaan dilakukan dengan menggunakan parameter algoritma enkripsi RC4 diperoleh hasil seperti pada Tabel 8.

Tabel 8 Data Simulasi Algoritma RC4

No	Metode	Plain text	Tipe Data String	Plain String Encoder (Binary)	Jumlah Bit Plain text	Kunci	Panjang Kunci
1	RC4	12345678	8 Char	00110001 00110010 00110011 00110100 00110101 00110110 00110111 00111000	71	0F62B5085BAE0154A7FA4DA0F34699EC0F62B5085BAE0154A7FA4DA0F34699EC	256 Bit
No	Metode	Plain text	Tipe Data String	Cipher String Encoder (Binary)	Jumlah Bit Cipher text	Kunci	Panjang Kunci
2	RC4	12345678	8 Char	01111100 10110011 10000100 01000000 01010101 10100000 10111100 00000000	71	0F62B5085BAE0154A7FA4DA0F34699EC0F62B5085BAE0154A7FA4DA0F34699EC	256 Bit

Pada simulasi algoritma Rabbit, data masukan *plain text* dengan type *string* terdiri dari 8 karakter yang dikonversikan menjadi 71 bit dalam bentuk biner seperti pada kolom *plain string encoder* seperti pada Tabel 9, akan dienkripsi dengan algoritma Rabbit menggunakan kunci enkripsi 128 bit dan tambahan *initialization vector* sebesar 64 bit. Dan menghasilkan sebuah *cipher text* yang panjang ukuran bitnya 50% lebih pendek dari ukuran panjang *bit plain text*nya .

Tabel 9 Data Simulasi Algoritma RC4

No	Metode	Plain text	Tipe Data String	Plain String Encoder (Binary)	Jumlah Bit Plain text	Kunci	Panjang Kunci	Initialization Vector (IV)	Panjang Initialization Vector
1	Rabbit	12345678	8 Char	00110001 00110010 00110011 00110100 00110101 00110110 00110111 00111000	71	0F62B5085BAE0154A7FA4DA0F346999EC	128 Bit	288FF65DC42B92F9	64 Bit
No	Metode	Plain text	Tipe Data String	Cipher String Encoder (Binary)	Jumlah Bit Cipher text	Kunci	Panjang Kunci	Initialization Vector (IV)	Panjang Initialization Vector
2	Rabbit	12345678	8 Char	01110011 00001000 11100110 11000010	35	0F62B5085BAE0154A7FA4DA0F346999EC	128 Bit	288FF65DC42B92F9	64 Bit

4.2 Data Analisa Nilai Entropy, *Avalanche Effect* Algortima RC4 dan Rabbit

Dari simulasi Cryptool diperoleh hasil *cipher text* yang dipergunakan selanjutnya untuk analisa *entropy* dan *avalanche effect* dan mengukur tingkat kualitas keamanan algoritma seperti pada penjelasan Tabel 10,11 dan 12.

Tabel 10 Perbandingan Hasil *Cipher Text* RC4 dan Rabbit

No	Algoritma	Plain text	Tipe Data String	Cipher String Encoder (Bin)	Jumlah Bit Cipher text	Kunci	Panjang Kunci
1	RC4	12345678	8 Char	01111100 10110011 10000100 01000000 01010101 10100000 10111100 00000000	71	0F62B5085BAE0154A7FA4DA0F34699EC0F62B5085BAE0154A7FA4DA0F34699EC	256 Bit
2	Rabbit	12345678	8 Char	01110011 00001000 11100110 11000010	35	0F62B5085BAE0154A7FA4DA0F34699EC	128 Bit

Tabel 11 Nilai Entropy Enkripsi Algoritma RC4 dan Rabbit

No	Algoritma	Ukuran File Plain text	Ukuran Panjang Kunci	Hasil Cipher Text(Hex)	Nilai Maksimum Probabilitas Entropy	Hasil Entropy
1	RC4	8 Char (String)	256 Bit	94 23 90 8D 41 ED 03 49	4.7	0.91
2	Rabbit	8 Char (String)	128 Bit	73 08 E6 C2	4.7	1

Tabel 12 Nilai *Avalanche Effect* Enkripsi RC4 dan Rabbit

No	Algoritma	Nilai Masukan Plain text	Hasil Cipher Text	Avalance Effect (%)
1	RC4	00110001 00110010 00110011 00110100 00110101 00110110 00110111 00111000	10010100 00100011 10010000 10001101 01000001 11101101 00000011 01001001	50
2	Rabbit	00110001 00110010 00110011 00110100 00110101 00110110 00110111 00111000	01110011 00001000 11100110 11000010	76.5625

Dan selanjutnya melakukan uji penerapan algoritma algoritma enkripsi RC4 dan algoritma Rabbit pada lapisan fisik jaringan protokol IEE 802.15.4 sehinga diperoleh data seperti pada Tabel 12,13 dan 14.

Tabel 13 Data Analisa Penggunaan CPU Algoritma RC4 dan Rabbit

Percobaan	Jumlah Node	CPU (Clock Prosessor,Hz)		Analisa % CPU Rabbit terhadap RC
		RC4	Rabbit	
1	20	166848	86176	48.35059455
2	30	271616	138554	48.9890139
3	40	514528	307072	40.31967162

Tabel 14 Data Analisa Penggunaan Memori Algoritma RC4 dan Rabbit

Percobaan	Jumlah Node	Memori (kB)		Analisa % Memori RC4 terhadap Rabbit
		RC4	Rabbit	
1	20	675	426	36.88888889
2	30	772	711	7.901554404
3	40	4288	5616	-30.97014925

Tabel 15 Data Analisa Simulasi *End to End Delay* Algoritma RC4 dan Rabbit.

Percobaan	Jumlah Node	End to End Delay (s)		Selisih Waktu RC4 dan Rabbit
		RC4	Rabbit	
1	20	0.049	0.034	0.015
2	30	0.035	0.034	0.001
3	40	0.035	0.038	-0.003

5. KESIMPULAN

Meskipun algoritma Rabbit memiliki panjang kunci yang lebih pendek 50% dibandingkan dengan algoritma RC4 namun, algoritma Rabbit memiliki tingkat kualitas keamanan algoritma lebih baik 9% untuk nilai entropy dan 25.56% nilai *avalanche effect*nya. Dan dari penggunaan sumber daya , algoritma Rabbit memiliki keunggulan yang lebih baik 45% untuk sumber daya prosesor. Serta hasil yang bervariasi untuk uji skalabilitas penggunaan memori dan waktu pemrosesan namun masih dapat memenuhi kriteria standar pemenuhan waktu proses industri dibawah 100 milidetik untuk keperluan aplikasi aplikasi open loop, monitoring dan data logging yang umumnya dipergunakan dalam sektor industri migas untuk penggunaan teknologi *wireless sensor network* .

REFERENCES

[1] M. Raza, N. Aslam, H. Le-Minh, S. Hussain, Y. Cao, and N. M. Khan, "A Critical Analysis of Research Potential, Challenges and Future Directives in Industrial Wireless Sensor Networks," *IEEE Commun. Surv. Tutorials*, no. October, pp. 1–1, 2017.

[2] J. Zhu, Y. Zou, and B. Zheng, "Physical-Layer Security and Reliability Challenges for Industrial Wireless Sensor Networks," *IEEE Access*, vol. 5, pp. 5313–5320, 2017.

[3] Q. Wang, J. Jiang, and S. Member, "Comparative Examination on Architecture and Protocol of Industrial Wireless Sensor Network Standards," vol. 18, no. 3, pp. 2197–2219, 2016.

[4] A. K. Nain, J. Bandaru, M. A. Zubair, and R. Pachamuthu, "A Secure Phase-Encrypted IEEE 802.15.4 Transceiver Design," *IEEE Trans. Comput.*, vol. 66, no. 8, pp. 1421–1427, 2017.

[5] I. Tomic and J. A. McCann, "A Survey of Potential Security Issues in Existing Wireless Sensor Network Protocols," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1910–1923, Dec. 2017.

[6] S. Sen Gupta, A. Chattopadhyay, K. Sinha, S. Maitra, and B. P. Sinha, "High-performance hardware implementation for RC4 stream cipher," *IEEE Trans. Comput.*, vol. 62, no. 4, pp. 730–743, 2013.

[7] C. S. Narayanan and S. A. Durai, "A Critical Study on Encryption Based Compression Techniques," *J. Comput.*, vol.

11, no. 5, pp. 380–399, 2016.

[8] D. Costa, S. Figuerêdo, and G. Oliveira, "Cryptography in Wireless Multimedia Sensor Networks: A Survey and Research Directions," *Cryptography*, vol. 1, no. 1, p. 4, 2017.

[9] P. Patil, P. Narayankar, D. G. Narayan, and S. M. Meena, "A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish," *Procedia Comput. Sci.*, vol. 78, no. December 2015, pp. 617–624, 2016.

[10] J. A. P. Marpaung, B. Ndibanje, and H. J. Lee, "Higher-Order Countermeasures against Side-Channel Cryptanalysis on Rabbit Stream Cipher," *J. Inf. Commun. Converg. Eng.*, vol. 12, no. 4, pp. 237–245, Dec. 2014.

[11] J. Choi, "Channel-Aware Randomized Encryption and Channel Estimation Attack," *IEEE Access*, vol. 5, pp. 25046–25054, 2017.

[12] J. Zhang, T. Duong, R. Woods, and A. Marshall, "Securing Wireless Communications of the Internet of Things from the Physical Layer, An Overview," *Entropy*, vol. 19, no. 8, p. 420, Aug. 2017.

[13] G. Leroy, *Designing User Studies in Informatics*. London: Springer London, 2011.

[14] J. Strombergson and S. Josefsson, "Test Vectors for the Stream Cipher RC4," May 2011.

[15] X. Zhang, H. M. Heys, and C. Li, "Energy efficiency of symmetric key cryptographic algorithms in wireless sensor networks," in *2010 25th Biennial Symposium on Communications*, 2010, pp. 168–172.

[16] S. Petersen and S. Carlsen, "Wireless Instrumentation in the Oil & Gas Industry - From Monitoring to Control and Safety Applications," in *SPE Intelligent Energy International*, 2012.

[17] A. Nechibvute and C. Mudzingwa, "Wireless Sensor Networks for SCADA and Industrial Control Systems," *Int. J. Eng. Technol.*, vol. 3, no. 12, pp. 1025–1035, 2013.