Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer e-ISSN: 2548-964X
Vol. 5, No. 10, Oktober 2021, hlm. 4689-4697 http://j-ptiik.ub.ac.id

Implementasi Algoritma Enkripsi Snow-V pada Wireless Sensor Network (WSN)

Yulius Adi Pratama[1], Agung Setia Budi[2], Ari Kusyanti[3]

Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Brawijaya
Email: [1]yuliuspratama9e@gmail.com, [2]agungsetiabudi@ub.ac.id, [3]ari.kusyanti@ub.ac.id

Abstrak

Wireless sensor network (WSN) merupakan teknologi yang terdiri dari kumpulan node-node yang tersebar dalam ruang lingkup sistem yang dapat digunakan untuk monitoring, pelacakan dan kontrol alat. Setiap node pada WSN menggunakan jaringan nirkabel dalam pertukaran data sehingga memungkinkan data dapat dilihat dan dikumpulkan oleh pihak lain dengan cara menguping jalur pertukaran data antar node. Data yang dilihat dan dikumpulkan pihak lain mungkin mengandung informasi sensitif seperti identitas, lokasi, dll. Dalam penelitian ini penulis menggunakan metode streamciper dalam mengamankan data dengan algoritma Snow-v. Streamciper dipilih karena kesederhanaannya dalam mengamankan data dan kecepatannya. Algoritma Snow-v merupakan algoritma baru yang menawarkan kecepatan dan ringan dalam menjalankan algoritmanya. Algoritma Snow-v juga menjadi usulan dalam enkripsi perimitif dalam sistem 5G. Dalam penelitian ini algoritma snow-v digunakan sebagai pembuat keystream dalam streamciper. Penelitian ini memanfaatkan nRF24L01 sebagai modul komunikasi pertukaran data antar node yang menggunakan media frekuesi radio dan arduino uno sebagai alat yang digunakan sebagai media untuk menjalankan metode Streamciper dan algoritma Snow-v. Dari hasil penelitian yang dibuat data tidak dapat di baca oleh pilak lain yang sedang menguping pertukaran data antar node. Dalam penelitian ini waktu yang dibutuhkan node dalam enkripsi rata-rata 241 ms dan waktu yang dibutuhkan untuk mengdekripsi data adalah 185 ms.

Kata kunci: *WSN, snow-v, streamciper*

Abstract

Wireless sensor network (WSN) is a technology consisting of a collection of nodes that are spread out within the scope of the system that can be used for monitoring, tracking and controlling equipment. Each node on the WSN uses a wireless network in exchanging data so that it allows data to be seen and collected by other parties by eavesdropping on the data exchange path between nodes. The data seen and collected by other parties may contain sensitive information such as identity, location, etc. In this study the author uses the streamciper method in securing data with the Snow-v algorithm. Streamciper was chosen because of its simplicity in securing data and its speed. The Snow-v algorithm is a new algorithm that offers speed and lightness in running the algorithm. The Snow-v algorithm is also a proposal in the encryption of perimits in 5G systems. In this study, the snow-v algorithm is used as a keystream generator in the streamciper. In this study, using nRF24L01 as a communication module for data exchange between nodes using radio frequency media and Arduino Uno as a tool used as a medium to run the Streamciper method and the Snow-v algorithm. From the research results, the data cannot be read by other pilaks who are eavesdropping on the exchange of data between nodes. In this study, the average time required for the node to encrypt is 241 ms and the time required to decrypt the data is 185 ms.

Keywords: *WSN, snow-v, streamciper*

1. PENDAHULUAN

Teknologi pada era revolusi industri keempat sekarang ini berkembang begitu cepat pada bidang komunikasi. semakin berkembangnya teknologi komunikasi ini

membuat hubungan antar perangkat elektronik semakin banyak. Untuk mengimbangi luasnya perangkat elektronik yang terhubung membutuhkan model komunikasi yang efisien. Salah satu yang sedang berkembang saat ini model komunikasi nirkabel

komunikasi nirkabel dikembangkan menjadi Wireless Sensor Network(WSN). Semacam teknologi tergabung dari banyak node yang tersebar dalam lingkup sistemyang menerapkan jaringan nirkabel. Pengaplikasian teknologi ini untuk pelacakan, monitoring dan kontol alat, kemudian bertukar data melalui jaringan nirkable dengan node-node yang saling terhubung. WSN memiliki keterbatasan sumber daya energi oleh karena itu manggunakan nRF24L01 sebagai media jaringan nirkabel denagn sifatnya yang Ultra Low Power (ULP).

Dalam WSN, komunikasi antar node di lakukan secara nirkabel sehingga data dikirmkan menggunakan media gelombang elektromagnetik, sehingga menyebabkan data yang dikirmkan antar node dapat dilihat pihak luar sistem. Metode untuk melihat data yang sedang di kirimkan dengan cara Sniffing. Sniffing adalah serangan pasif dengan cara menguping pertukaran data antar node.

Data yang dikumpulkan oleh sensor mungkin mengandung informasi sensitif dan tidak boleh bocor ke perangkat yang tidak sah. Lebih lanjut, kunci enkripsi dan informasi tentang sensor itu sendiri (mis., Identitas, lokasi, dll.) Harus dilindungi untuk mencegah penyadapan dan serangan berdasarkan analisis trafik (Dargie & Poellabauer , 2010)..

Ada bebrapa solusi dalam mengamankan suatu informasi dalam sistem jaringan WSN ada enkripsi dan protokol keamanan. enkripsi merupakan suatu cara dalam mengamankan data dengan mengacak data sebelum di kirimkan. Sehingga apabila jaringan tersebut disadap maka data yang telah diacak yang akan di terima oleh penyadap. Streamciper digunakan sering pada perangkat keras karena kecepatan dan kesederhanaan.

Snow-v merupakan algoritma enkripsi berkecepatan sangat tinggi dalam lingkungan virtual, lebih cepat daripada AES-256 dengan tingkat keamanan yang hampir sama dengan AES-256. Algoritma ini juga merupakan salah satu usulan dalam pengemankan jaringan 5G sehingga peneliti memilih algoritma ini dalam mengamankan komunikasi data didalam WSN.

Berdasarkan masalah yang tersebut, diperlukan suatu algoritma yang dapat mengamankan data yang terkirim antar node. Karena hal tersebut pada penelitian ini akan di implementasikan metode keamanan streamciper dengan algoritma enkripsi SNOW-V dan modul nRF24L01 sebagai akusisi data antar node

Penggunaan algoritma enkripsi ini, memungkinkan dalam mengamankan komunikasi antara dua node yang menggunakan media radio. Dengan cara menenkripsi data sebelum dikirimkan sehingga sniffer memungkinkan untuk tidak bisa mambaca data asli. penelitian ini memasikan solusi dengan enkripisi data asli sebelum dikirimkan. Sehingga dapat dijalankan dan dikembangkan untuk mengamankan data didalam WSN.

2. DASAR TEORI

2.1 Wireless Sensor Network (WSN)

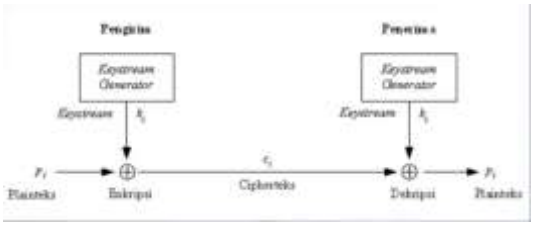
Node sensor yang berkumpul pada suatu tempat untuk melakukan pendataan dengan parametaer terukur dan akan dikirimkan ke node sentral yang menjadi node pengumpulan data (Firdaus, 2014) Node disebar dalam cakupan sistem sesuai dengan kebutuhan yang ingin diketahui besarannya dalam meter ukur (Ilyas. M., Mahgoub. I., 2005)

2.2 Stream Ciper

Stream Ciper adalah metode enkripsi data dengan mengenkripsi plainteks menjadi ciperteks byte per byte dengan kunci keystream. Diperkenalkan oleh Vernam dengan algoritma yang mempuyai nama Vernam Ciper. Konsep Stream ciper terdapat didalam gambar 1

2.3 SNOW-V

SNOW-V merupakan Algoritma Keystream



Gambar 1 Skema Streamciper

generator dari keluarga SNOW. SNOW pertama kali di kemukakan dalam pers proyek NESSIE dengan lisensi terbuka (Open Source).

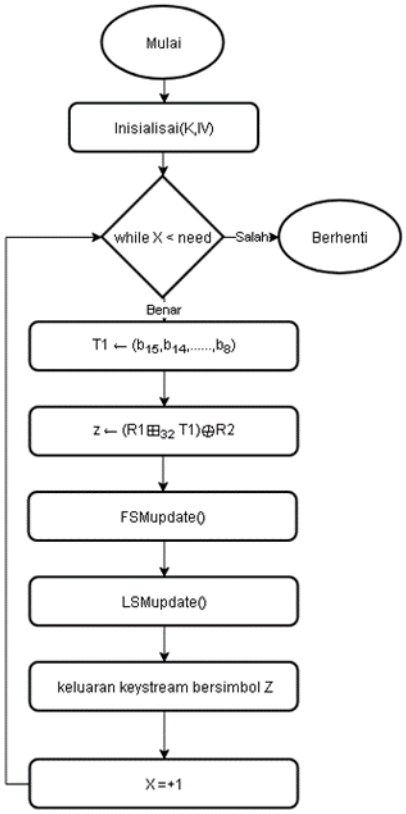
2.4 *Sniffing*

Sniffing merupakan salah satu serangan

pasif yang untuk mencuri dengar proses komunikasi yang di lakukan pada suatu sistem, tanpa mengubah atau menggangu komunikasi sistem tersebut. Sniffing dilakukan untuk mencari titik lemah sistem dan mencari informasi yang terkait yang bisa dilakukan dalam serangan aktif pada sistem. Pada penelitian ini, Sniffing dilakukan sebagai pengujian resistensi serangan. Metode ini digunakan untuk menguji data yang sedang dikirimkan.

3. PERANCANGAN DAN IMPLEMENTASI

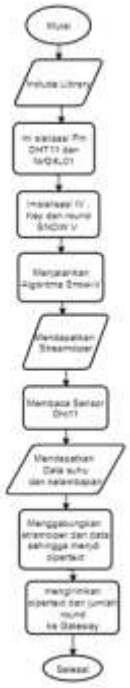
3.1. Perancangan Algoritma SNOW-V



Gambar 2 Flowchart SNOW-V

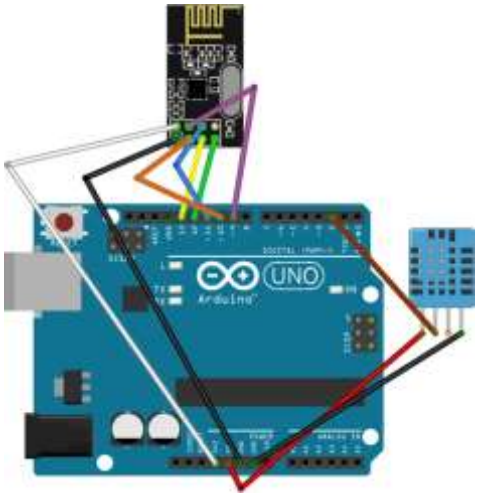
Seperti dalam gambar 2 flowchart Algoritma Snow-V pada Gambar 5.9 nilai K dan IV di masukkan terlebih dahulu sebagai inisialisasi setelah itu nilai dari round ditetapkan. Setelah itu memasukkan b15 sampai b8 sebagai T1. R1 di addition modulo dengan T1 dan hasil nya akan di-Xor-kan dengan R2 dan keluarannya menjadi di masukkan ke dalam variabel z. Nilai di dalam variabel z ini yang akan di-xor-kan dengan data suhu sehingga menjadi streamciper. Setelah itu akan mengeksekusi FSMupdate untuk memperbarui nilai di dalam FSM. Apabila FSM telah perbarui dilanjutkan dengan mengeksekusi LSMupdate untuk memperbarui nilai dari LSM. Setelah itu nilai dari X akan ditambahkan 1 karena telah menyelesaikan alur algoritma. Apabila nilai X masih belum sesuai dengan round maka program akan kembali di eksekusi sampai syarat nilai round terpenuhi. Variabel z menjadi keystream untuk mengenkripsi data maupun mendekripsi data. Algoritma SNOW-V diimplemantasikan kedalam node enkripsi dan dekripsi

3.2 Perancangan Dan Implementasi Node Enkripsi



Gambar 3 Flowchart Node Enkripsi

Seperti di gambar 3 dimulai dari inisialisasi pin sensor Dht11 dan modul komunikasi nRF24L01 di sesuaikan dengan perancangan perangkat keras node enkripsi. Dilanjut dengan inisialisasi IV, Key dan round untuk algoritma Snow-v selatah itu algoritma dijalankan untuk mendapat keystream setelah itu menunggu 1 detik untuk membaca data sensor Dht11 apabila data sensor telah didapatkan maka data akan di-Xor-kan dengan keystream untuk medapatkan streamciper yang akan di kirimkan ke node selanjutnya bersama round pada algoritma snow-v.



Gambar 4 Skematik Node Enkripsi

Skematik dalam gambar 4 sensor Dht11 bersama modul komunikasi nRF24L01 terhubung dengan Arduino Uno. Sensor Dht11 vcc terhubung dengan 5v dalam pin ardunio , pin GND Dht11 menyambung dengan pin GND arduino uno sedangkan pin data Dht11 tersambung dengan pin 2 pada arduino uno.tabel konfigurasi antar pin terdapat dalam tabel 1

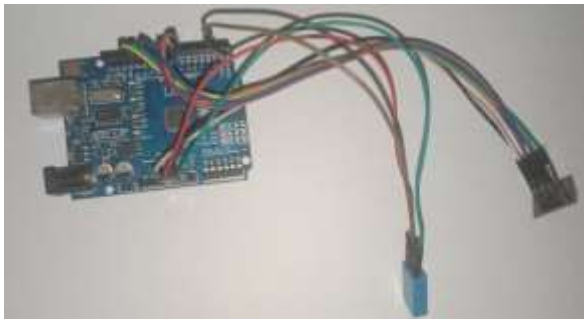
Tabel 1 Keterangan Pin Dht11

No	DHT11	Arduino Uno
1	VCC	5V
2	GND	GND
3	Data	Pin 2

Pin VCC NRF24L01 dengan Arduino Uno di pin 3.3 v saling terhubung, Pin GND NRF24L01 tersambung Arduino uno di Pin GND , Pin CE tersambung ardunio uno di pin 10 untuk mengirim dan menerima data dan Pin SCN tersambung Arduino Uno di pin 9i untuk mengaktifkan chip SPI sedangkan pin SCK , MISO dan MOSI yeang secara berurutan terhubung ke pin 13, 12 dan 11 Arduino Uno untuk menerima dan mengirim data ke modul lain. Konfigurasi pin dapat di lihat pada tabel 5.2, Pin-Pin yang terhubung di dalam skematik di rangkum dalam tabel berikut:

Tabel 2 Keterangan Pin nRF24L01

Pin pada Arduino	Pin Pada nRF24L01
3.3v	VCC
GND	GND
10	CE
9	SCN
13	SCK
11	MOSI
12	MISO

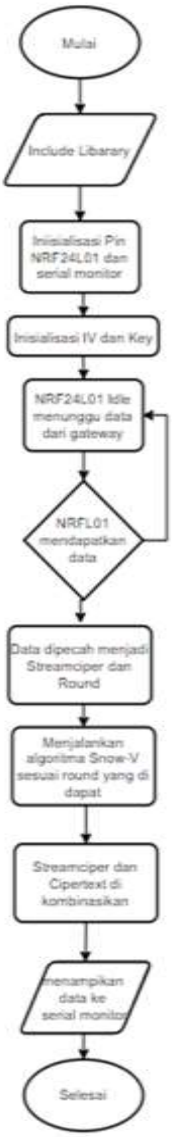


Gambar 5 Implementasi Node Enkripsi

Gambar 5 Implementasi node enkripsi membuat Perancangan node enkripsi menjadi alat. Mengikuti sketsa didalam perancngan node enkripsi dengan modul komunikasi nRF24L01 dengan sensor DHT11 yang dihubungkan dengan arduino uno.

3.3 Perancangan dan Implementasi Node Dekripsi

Node dekriptor menggunakan modul komunikasi nRF24L01, maka library RF24 di masukkan di awal kode program untuk memudah kan dalam mengatur modul komunikasi nRF24L01. Untuk flowchart kode program dapat dilihat pada gambar 6



Gambar 6 Flowchart Dekripsi

Inisialisasi pin disesuaikan dengan perancangan perangkat kerasnode dekriptor dan inisialisasi serial monitor dilanjut dengan inisialisasi IV dan key pada algoritma snow-v. Modul komunikasi nrf24L01 menunggu data yang datang dari node gateway untuk mendapat data. Apabila data telah diterima akan di pecah menjadi 2 bagian yaitu streamciper dan round. round akan digunakan untuk menjalankan algoritma snow-v untuk medapat streamkey yang akan di-Xor-kan dengan streamciper yang di dapat sehingga menjadi data asli dari sensor

Gambar 7 Skematik Node Dekriptor

Modul komunikasi nRF24L01 terhubung dengan arduino seperti skematik pada gambar 7 dengan konfigurasi pin yang sama dengan node pengirim. Pada Modul komunikasi Pin VCC NRF24L01 terhubung dengan Arduino Uno di pin 3.3 v, Pin GND NRF24L01 tersambung Arduino uno di Pin GND , Pin CE tersambung ardunio uno di pin 10 untuk mengirim dan menerima data dan Pin SCN tersambung Arduino Uno di pin 9i untuk mengaktifkan chip SPI sedangkan pin SCK , MISO dan MOSI yeang secara berurutan terhubung ke pin 13, 12 dan 11 Arduino Uno untuk menerima dan mengirim data ke modul lain. Konfigurasi pin dapat di lihat tabel 5.3, Pin-Pin dalam skematik saling terhubung dan di rangkum dalam tabel berikut

Tabel 3 Konfigurasi Pin nRF24L01

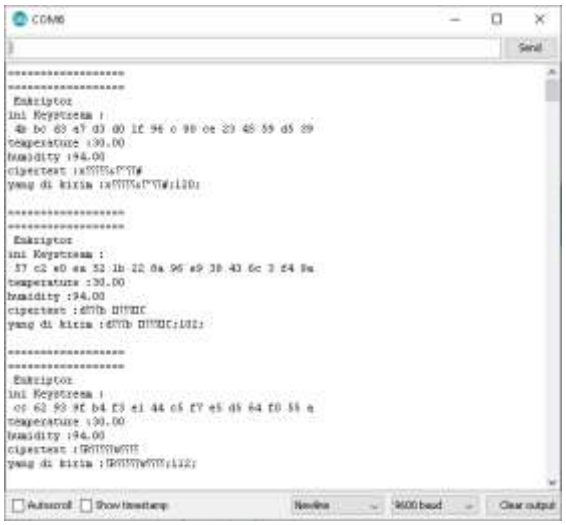
Pin pada Arduino	Pin Pada nRF24L01
3.3v	VCC
GND	GND
10	CE
9	SCN
13	SCK
11	MOSI
12	MISO

4. PENGUJIAN

4.1 Node Enkripsi

Node enkripsi akan diuji dalam mengambil data dari sensor suhu dan mngenkripsi data tersebut dengan metode streamciper dengan algoritma Snow-v. Untuk

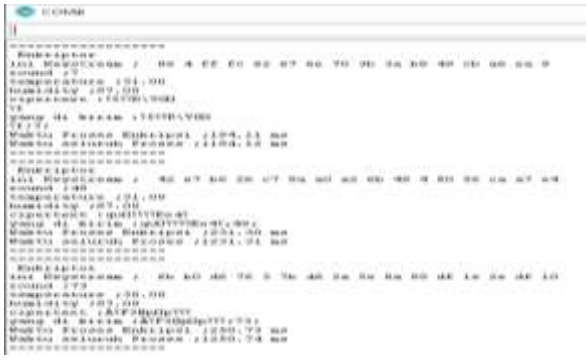
mengetahui bahwa node enkripsi dapat berjalan dengan baik dan dapat mengenkripsi data dengan hasil yang dinginkan. Sketsa pengujian node enkripsi akan tersambung dengan sumber daya dan sensor suhu dan data suhu akan di tampilkan di serial monitor bersama data yang telah di enkripsi



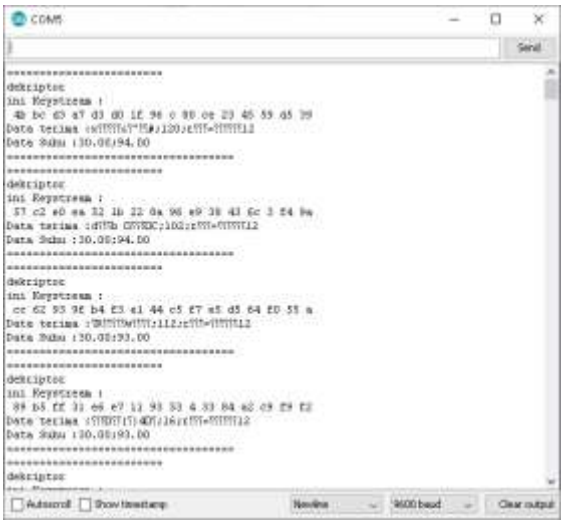
Gambar 7 Tampilan Serial Monitor

Tampilan dalam serial monitor dalam Gambar 7 ada keystream sebagai keluaran dari algoritma snow-v. Temperature dan hummidity adalah data yang diambil dari sensor suhu dalam, cipertext merupakan data sensor suhu yang telah di-xor-kan dengan keystream. yang di kirim merupakan gabungan dari cipertext dan round yang akan di kirimkan ke node gateway.

4.2 Node Dekriptor



Node Dekriptor akan diuji dalam menerima data dari gateway dan dapat mengubah data yang telah diterima menjadi data semula sebelum terjadi proses enkripsi. Tujuan dari pengujian untuk mengetahui node dekriptor dapat berjalan dengan baik dan mengetahui kemampuan node dekriptor dalam melakukan penerimaan data dan di ubah menjadi data sebelum dilakukan proses enkripsi kembali. Seketsa pengujian yang di lakukan node dekriptor akan terhubung dengan sumber daya dan Modul komunikasi, node dekriptor menunggu data yang masuk dan mengubahnya kembali menjadi data sebelum di enkripsi untuk ditampilkan ke serial monitor



Gambar 8 Tampilan serial Monitor

Node dekriptor menampilkan hasil dalam Gambar 8 “keystream” merupakan hasil dari algoritma snow-v, dalam “data terima” merupakan data yang diterima dari node gateway dan diproses sehingga menampilkan “data suhu” yang merupakan data asli dari sensor suhu.

4.3 Waktu Proses

Node dekriptor dan enkripsi akan diuji dalam lamanya waktu untuk memproses data, tujuan pengujian ini untuk mengetahui waktu yang dibutuhkan dalam memproses data. Seketsa pengujian kedua node akan berjalan sesuai sistem yaitu node enkripsi akan mengirimkan data ke node dekriptor. Dan masing-masing node akan menampilakan waktu program berjalan dalam serial monitor.

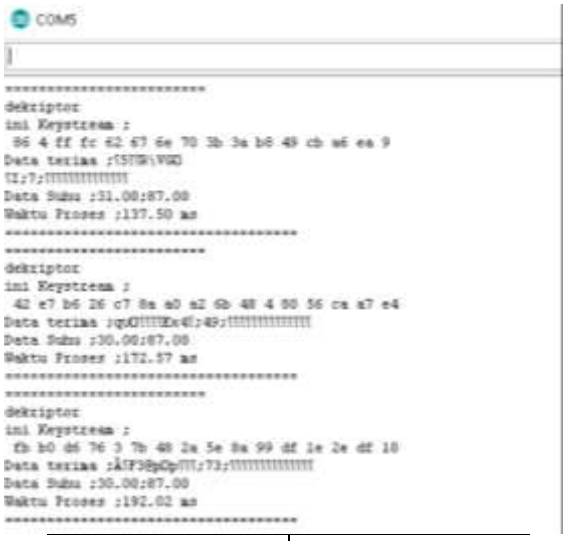
Gambar 9 Tampilan lama waktu Proses Node Enkripsi

Node enkripsi gambar 9 menampilkan waktu proses enkripsi. Diketahui dari hasil output lama proses waktu enkripsi berbeda-beda pada setiap roundnya

Gambar 10 Tampilan Lama Waktu Proses Node Dekriptor

Node dekriptor gambar 10 menampilkan waktu proses enkripsi. Diketahui dari hasil output lama proses waktu enkripsi berbeda-beda pada setiap roundnya. Lama waktu proses yang didapat dapat dilihat pada tabel 1

Tabel 1 Waktu Proses Node



Node Enkriptor	Node dekriptor
194 ms	137 ms
231 ms	172 ms
250 ms	192 ms
238 ms	179 ms
280 ms	238 ms
250 ms	191 ms
299 ms	249 ms

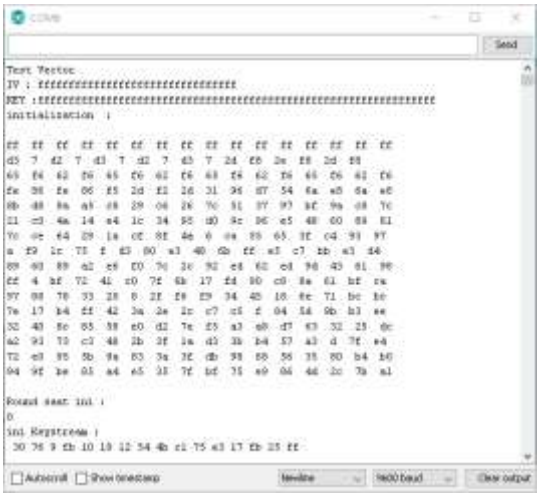
Didalam tabel 1 ditunjukkan waktu enkripsi dan dekripsi pada node , node enkripsi rata – rata waktu proses 241 ms dan node dekriptor 185 ms

4.4 Test Vektor

Algoritma snow-v yang akan di tanamkan ke dua node akan diuji test vektor terlebih dahulu. Dengan tujuan untuk mengetahui bahwa algoritma yang terpasang didalam node mempuyai hasil yang sama dengan jurnal yang digunakan sebagai dasar teori. Skema pengujian arduino akan ditanamkan algoritma snow-v dengan hasil yang ditampilkan ke dalam serial monitor.

Tampilan hasil di tunjukan pada gambar 11 di dalam serial monitor.

Tabel 2 Test Vektor didalam jurnal



Gambar 11 Tampilan Hasil Test Vector

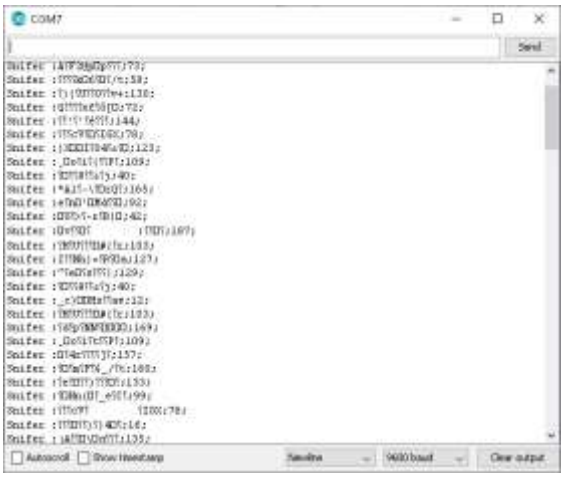
ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
d3 07 d2 07 d3 07 d2 07 d3 07 2d f8 2e f8 2d f8
65 f6 62 f6 65 f6 62 f6 65 f6 62 f6 65 f6 62 f6
Fe 86 fe 86 f5 2d f2 2d 31 96 d7 54 6a e8 6a e8
8b d8 8a a5 c8 29 c6 26 7c 51 37 97 bf 9a c8 7c
21 c0 4a 14 e4 1c 34 95 d0 9c 96 e5 48 60 89 81
7c ce 64 29 1a cf 8f 4a 06 ca 55 65 3f c4 93 97
0a f9 1c 75 0f d3 80 e3 48 6b ff e5 c7 bb e3 d4

Jika dibandingkan dengan tabel 2 yang merupakan test vektor jurnal dengan gambar 11 maka terjadi pebedaan dengan hilang nya angka nol yang ditampilkan didalam serial monitor karena memang nilai nol yang berada didepan tidak dapat ditampilkan.

4.5 Serangan Sniffing

Data yang dikirimkan dari node enkripsi ke node dekriptor akan dipantau node sniffer dan melihat data yang berjalan di jalur tersebut. Tujuan pengujian ini untuk mengetahui data yang diambil baca node sniffer merupakan data

yang telah terenkripsi sehingga tidak dapat terbaca. Sketsa pengujian kedua node akan berjalan sesuai sistem dan node sniffer akan menyusup kejalur komunikasi dengan hasil snifiing yang ditampilkan ke serial monitor.



Gambar 12 Tampilan hasil sniffing

Data yang terbaca oleh node sniffer akan ditampikan dalam Gambar 12 dengan hasil data yang teracak.

5. KESIMPULAN

Dengan melakukan pengujian dan implementasi maka berikut kesimpulan yang dapat di buat :

1. Algoritma SNOW-V dapat bekerja dengan baik didalam mengenkripsi data didalam node enkripsi. Dimulai dari node enkripsi yang dapat membaca suhu dengan sensor suhu, mengenkripsi data suhu yang telah didapatkan menjadi cipertext serta mengirimkan cipertext ke node selanjutnya. Didalam node dekriptor algoritma SNOW-V juga berjalan dengan baik dalam mendekripsi data. Dimulai dari node dekriptor dalam menerima data dari node sebelumnya dan mendekripsi data tersebut menjadi data suhu kembali
2. Dalam waktu komputasi algoritma SNOW-V pada wsn untuk enkripsi data rata-rata membutuhkan waktu 241 ms dan dekripsi data membutuhkan waktu rata-rata 185 ms
3. Dalam serangan sniffing dengan menyerang jakur dari node enkripsi ke node gateway. Data yang diterima sniffer merupakan data acak yang tidak dapat dibaca.

6. DAFTAR PUSTAKA

Ekdahl, P., Johansson, T., Maximov, A., & Yang, J. (2018). A new SNOW stream cipher calledEkdahl, P., Johansson, T., Maximov, A., & Yang, J. (2018). A new SNOW stream cipher called SNOW-V. International Association for Cryptologic Research. Sweden.

Zhao, Z., Huangfu, W., & Sun, L. (27 September 2012). NSSN: A network monitoring and packet sniffing tool for wireless sensor networks. International Wireless Communications and Mobile Computing Conference, IWCMC (hal. 4). Limassol,Cyprus: IEEE.

Caforio, A., Balli, F., & Banik, S. (17 November 2020). Melting SNOW-V: improved lightweight architectures. Journal of Cryptographic Engineering.

Dargie , W., & Poellabauer , C. (2010). Fundamentals of Wireless Sensor Networks: Theory and Practice. Wiley.

Dener, M. (2014). Security Analysis in Wireless Sensor Networks. International Journal of Distributed Sensor Networks 2014(Hindawi Publishing Corporation), 9.

Dhanda, S. S., Singh, B., & Jinda, P. (2020). Lightweight Cryptography: A Solution to Secure IoT. Springer (hal. 34). India: National Institute of Technology Kurukshetra.

Firdaus. (2014). Wireless Sensor Network. Yogyakarta: Grha Ilmu.

Hidayat, R. F., Akbar, S. R., & kusyanti, A. (2018). Implementasi dan Analisa Performansi Protokol Keamanan TinySec pada Wireless Sensor Network dengan Media Pengiriman Data NRF24L01 melalui Frekuensi Radio. Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer, 2858-2865.

Ilyas. M., M. I. (2005). Handbook of Sensor Networks : Compact Wireless and Wired Sensing Systems. Washington D.C: CRC Press.

Minglin, Y., & Junshuang, M. (2011). Stream Ciphers on Wireless Sensor Networks. International Conference on Measuring Technology and Mechatronics

Automation, ICMTMA (hal. 358-361). Shanghai, China: IEEE. SNOW-V. *International Association for Cryptologic Research.* Sweden.

Dargie , W., & Poellabauer , C. (2010). *Fundamentals of Wireless Sensor Networks: Theory and Practice.* Wiley.

Dener, M. (2014). Security Analysis in Wireless Sensor Networks. *International Journal of Distributed Sensor Networks 2014*(Hindawi Publishing Corporation), 9.

Dhanda, S. S., Singh, B., & Jinda, P. (2020). Lightweight Cryptography: A Solution to Secure IoT. *Springer* (p. 34). India: National Institute of Technology Kurukshetra.

Hidayat, R. F., Akbar, S. R., & kusyanti, A. (2018). Implementasi dan Analisa Performansi Protokol Keamanan TinySec pada Wireless Sensor Network dengan Media Pengiriman Data NRF24L01 melalui Frekuensi Radio. *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, 2858-2865.