1. Pendahuluan

Latar Belakang

Pada masa kini, *Internet of things* (IoT) sudah semakin maju dan berkembang. Hampir semua orang menggunankannya untuk kepentingan yang berbeda-beda. Jaringan sensor nirkabel (JSN) merupakan salah satu pengaplikasian IoT yang sudah banyak digunakan. JSN sudah banyak dimanfaatkan dalam berbagai bidang seperti, mengatur lampu lalu lintas pada bidang transportasi, mengecek perubahan struktur jembatan pada bidang konstruksi, mendeteksi kondisi tubuh pasien dalam bidang Kesehatan, dan lain-lain [2][3][4][5][6][7]. JSN adalah sebuah kumpulan node yang dapat berupa sensor yang akan melakukan pengambilan data pada parameter ukur dan kemudian dikirimkan pada sebuah node sentral atau sebuah server untuk dilakukan pengolahan data [8]. Setiap node yang ada dalam JSN memiliki memori, komputasi, dan sumber daya yang terbatas. Ketika data-data dikirimkan dari node yang satu ke node yang lainnya, pada proses tersebut terdapat kerentanan data diakusisi oleh penyerang.

Autentikasi *broadcast* merupakan suatu layanan keamanan dalam JSN. Pada makalah [9] mempresentasikan skema autentikasi *broadcast* untuk bertahan dari serangan *Denial of Service* (DoS). Salah satu cara mengatasinya dapat menggunakan skema *puzzle* dengan memanfaatkan kunci sesi [1]. Hasil dari evaluasi yang dikerjakan, skema tersebut menunjukkan keamanan dan efisiensi yang lebih baik dibandingkan skema yang sudah ada sebelumnya. Selain dari skema *puzzle* ada juga contoh skema lain yang memanfaatkan kunci sesi seperti pada makalah [10].

Dalam pemanfaatan JSN di dunia nyata, terdapat kerentanan data yang dikirim oleh masing-masing node untuk diketahui, diubah, ataupun dirusak oleh penyerang. Untuk mengamankan data tersebut bisa menggunakan autentikasi *broadcast*. Mengacu pada makalah [9] yang menjelaskan komunikasi pada autentikasi *broadcast* menggunakan *digital signature* dan skema *puzzle* untuk menghadapi serangan *denial of service* (DoS). Akan tetapi, pesan dan kunci sesi dikirim dalam bentuk aslinya sehingga memungkinkan penyerang untuk memecahkan isi *puzzle* tersebut. Karena belum adanya aspek *confidentiality* pada makalah acuan maka pada tugas akhir ini membuat penambahan aspek *confidentiality*.

Topik dan Batasannya

Pada Tugas Akhir ini, akan memodifikasi skema yang sudah ada sebelumnya dengan mengenkripsi kunci sesi yang sudah dibuat sebelum didistribusikan kepada node-node lain. Kunci sesi merupakan kunci yang digunakan untuk mengamankan *puzzle* dan bisa juga digunakan untuk mengenkripsi dan mendekripsi pesan dalam satu sesi komunikasi. kemudian, untuk membuat kunci sesinya akan menggunkan *backward key chain*. *Backward key chain* memiliki kelebihan penggunaan memori yang cukup kecil karena kunci yang dibangun terbatas dan penyerang tidak akan bisa mengetahui kunci selanjutnya. Lalu mengenkripsi kunci tersebut dengan metode *hill cipher* yang sudah dimodifikasi pada makalah [11]. Modifikasi yang dibangun tersebut dapat mengenkripsi semua jenis pesan tidak hanya abjad dan menghilangkan data redundan yang terjadi dalam pola teks biasa, dengan itu kompleksitas *hill cipher* meningkat.

Batasan masalah dari pengerjaan Tugas Akhir ini adalah :

1. Tugas Akhir ini fokus pada aspek *confidentiality*, maka penggunaan *puzzle* dan tanda tangan digital (*digital signature*) diabaikan.
2. Tugas akhir ini hanya dijalankan secara simulasi menggunakan bahasa pemrograman python.
3. Pengiriman dan penerimaan data disimulasikan satu sesi dalam sehari.
4. Simulasi fokus untuk mengukur performansi dengan penambahan aspek *confidentiality* kunci sesi sebanyak 30 sesi pengiriman dan penerimaan data.

Tujuan

Tujuan dari Tugas Akhir ini adalah memodifikasi skema yang sudah ada untuk mengamankan data pada autentikasi *broadcast* dalam JSN dengan menggunakan memori dan sumber daya yang sedikit serta komputasi yang sederhana. Makalah ini terfokus pada mengamankan kunci sesi yang digunakan untuk mengenkripsi pesan. Karena kunci tersebut juga ikut dikirim dengan pesan, maka kunci sesi itu diamankan dengan dienkripsi agar penyerang tidak bisa mengetahui atau merusak pesan walaupun penyerang mengetahui kunci untuk mengetahui pesan tersebut. Proses enkripsi dan dekripsi pesan disimulasikan untuk mendapatkan performansi dari skema yang dimodifikasi tersebut. Nilai performansi yang didapatkan dari simulasi tersebut menjadi hasil akhir dari tujuan jurnal Tugas Akhir ini.