SEMINAR NASIONAL INOVASI DAN APLIKASI
TEKNOLOGI DI INDUSTRI (SENIATI) 2016
ISSN : 2085-4218

A Secure Scheme for Fixed Topology In Wireless Sensor Network

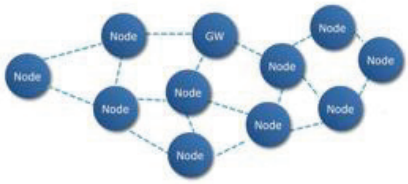
Arya Sony[1,*], **Selo Sulistyo**[1]
1 Universitas Gadjah Mada Jl.Grafika No.2 Yogyakarta-Indonesia
* E-mail : aryasny@gmail.com,selo@ugm.ac.id

Abstrak. Penelitian tentang keamanan WSN selalu fokus pada bagaimana gateway dapat mengirimkan data ke pengguna dengan aman, keamanan di tingkat node tidak terlalu diperhatikan karena data yang melewatinya tidak sesensitif dan sebanyak dibandingkan interaksi antara gateway ke pengguna. Namun terdapat kasus tertentu dimana data yang dihasilkan oleh sensor node perlu untuk diamankan.

Penelitian ini memanfaatkan banyaknya node sebagai lompatan/hop yang akan digunakan untuk memperumit proses enkripsi. Setiap node memiliki identitas dan kunci spesifik yang hanya diketahui oleh gateway. Semakin banyak node yang dilalui akan semakin sulit bagi penyerang untuk menysusup. Selain enkripsi berlapis penelitian ini juga menerapkan keamanan integritas berlapis menggunakan konsep yang sama, sehingga selain menjamin keamanan data, gateway dapat mengetahui pada node manakah penyusupan oleh penyerang terjadi.

Kata Kunci: Fixed Topology, Novel Security Scheme

1. Pendahuluan



Gambar 1. Node dan Gateway pada jaringan WSN

Teknologi Wireless Sensor Network (WSN) memiliki pembagian taksonomi dilihat dari mobilitas node sensornya[1]. Perbedaan ini mengarah pada penggunaan protokol yang berbeda, secara singkat menurut penelitian[1] topologi WSN dapat digolongkan menjadi fixed dan mobile node. Topologi mobile node banyak terdapat pada protokol MANET (Mobile Adhoc Network) dan IoT (Internet Of Things), sedangkan fixed node implementasinya lebih mengarah ke monitoring data dan Early Warning System.

Data yang sudah dikumpulkan oleh sensor tentu digunakan untu keperluan pengguna, teknologi 6lowpan menjanjikan hasil yang menggiurkan, mulai dari kemudahan koneksi internet sampai pada level pengamanan data, namun dengan menggunakan teknologi tersebut artinya memasang modul internet pada node yang notabene low power, hal ini tidak realistis dilakukan dimana WSN adalah perangkat dengan sumber energi yang sangat terbatas. Perkembangan metode pada WSN mengerucut pada penggunaan hop/lompatan, hop memanfaatkan node sebagai router/relay lalu membebankan tanggung jawab transmisi data internet ke pengguna pada gateway yang memiliki sumber tenaga melimpah, skema umum metode WSN untuk fixed topology dapat dilihat pada gambar 1.

Data yang terkumpul di gateway kemudian dianalisis yang kemudian menghasilkan informasi, informasi dikirimkan ke pengguna menggunakan teknologi 6lowpan yang sudah banyak berkembang dan relatif stabil. Hal ini sangat berbanding terbalik dengan keadaan transimisi data antar node yang belum mendapat perhatian pada sisi keamanannya karena data yang ditransmsikan per node bukan data sensitif, data-data tersebut menjadi berharga setelah terkumpul dengan data pada node lainnya dan kemudian dianalsis.

ISSN : 2085-4218

2. Permasalahan dan Asumsi

2.1 Permasalahan

Masalah muncul saat data yang dikirimkan tiap sensor node adalah data sensitif, sehingga perlu untuk diamankan perjalanannya dari node ke node menuju gateway.

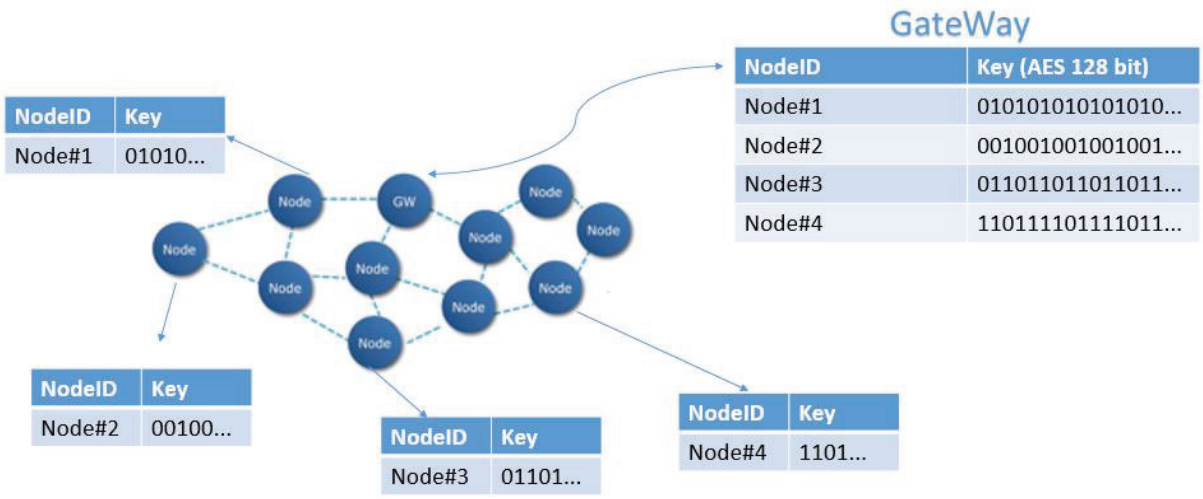
2.2 Asumsi

Asumsi diperlukan untuk memperjelas cakupan dan menyamakan persepsi, asumsi juga dapat digunakan layaknya studi kasus, berikut asumsi yang digunakan

- Node Sensor diletakkan pada area yang sulit dijangkau oleh sumber energi listrik
- Jumlah node tidak terlalu banyak, dan diatur oleh [2][3] untuk mendapatkan skema optimal peletakan node sensor sebagai relay/router guna memenuhi cakupan area yang akan dimonitor

3. Skema Umum

Secara umum lingkup penelitian sudah kami bahas pada latar belakang, disana kami paparkan keadaan yang mewakili mengapa harus ada skema ini, tentu rancangan ini tidak akan dapat menyelesaikan semua permasalahan, implementasi pada perkotaan menggunakan Smart City misalnya akan sangat berbeda protokol yang digunakan dengan implementasi pada hutan atau pegunungan untuk sistem Early Warning Disaster, masing-masing implementasi harus memperhatikan parameter apa yang paling ingin ditonjolkan, apakah itu keadaan geografis, keadaan sumber tenaga, lingkup daerah yang dimonitor, keamanan dsb.



Gambar 2. Persebaran Kunci pada Jaringan Shared Key Infrastructure

4. Metode

Paper ini membahas dua skema besar yang pada paper lain umumnya dipisah karena terlalu luas pembahasannya, kami gabungkan dalam satu paper karena keduanya bukan hanya saling berkaitan namun juga saling membutuhkan, jadi jika boleh dikatakan inti dari penelitian ini adalah memanfaatkan skema routing untuk memperkompleks proses pengamanan data, dimana kompleks selalu berbanding lurus dengan keamanan.

Mekanisme authentikasi kami tidak sertakan tata cara seperti perkenalan yang rumit pada pertukaran kunci di PKI (public key infrastructure) atau menjadikan node sebagai agen verifikasi VCA (virtual certificate authority) [4]. Kami beranggapan penggunaan public key infrastructure hanya akan melemahkan keamanan sistem secara keseluruhan, dimana shared key infrastrucute yang notabene lebih simple justru menawarkan keamanan maksimum tentu hal ini hanya berlaku pada kasus-kasus tertentu diantaranya saat kasus tersebut memenuhi asumsi yang kami berikan, pemilihan shared key memiliki kelebihan dan kekurangan, mekanisme ini dapat dilihat pada gambar 2. Kelebihan dari

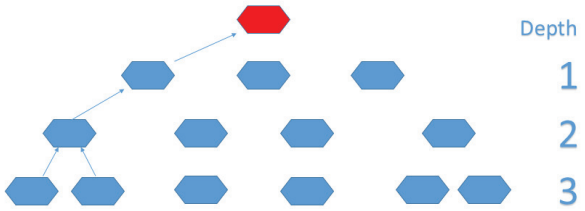
ISSN : 2085-4218

metode shared key infrastructure adalah sistem sangat aman dari gangguan luar, karena yang mengetahui kunci dari masing-masing node adalah node itu sendiri dan gateway, dengan skema seperti ini ditambah dengan mekanisme routing yang acak, penyerang akan kesulitan untuk mendapatkan data asli yang sudah dienkripsi, karena kunci yang digunakan untuk dekripsi pesan adalah kunci berlapis sesuai banyaknya hop. Kekurangan penggunaan shared key infrastructure adalah operasional yang cukup rumit pada awal pemasangan antara node dengan gateway. Sekali lagi, kerumitan berbanding lurus dengan keamanan, itulah harga yang harus dibayar.

4.1. Pseudorandom Routing Protocol (PRP)

Routing adalah proses bagaimana paket data dikirimkan dari sumber data (node) menuju ke tujuan (gateway) melalui beberapa router. Routing pada protokol PRP mengurangi kompleksitas yang ada pada protokol-protokol sejenis, contohnya pada protocol shortest path[5] saat node ingin mengirimkan data, terlebih dahulu harus berkomunikasi dengan beberapa node yang bertetanggaan dengannya, padahal komputasi yang dilakukan untuk "say hello" pada tetangga memakan jumlah energi yang sama dengan pengiriman data standar[6].

PRP adalah protokol yang dikembangkan dari protokol routing terdahulu yang bernama Random Walk Routing (RWR) [6], antara PRP dan RWR sebenarnya memiliki tujuan yang sama yaitu menggunakan algoritma acak untuk menentukan node mana yang akan dipilih dalam pengiriman paket, improvisasi PRP ada pada penambahan variabel "Depth" dimana variabel ini berisi angka kedalaman dari suatu node dalam topologi, angka dimulai dari 0 dan bergerak positif, angka 0 mereferensi ke gateway, angka 1 mereferensi node yang terhubung langsung ke gateway, angka 2 mereferensi node yang terhubung langsung ke node dengan nilai depth 1 dan begitu seterusnya. Berikut gambaran umum dari skema PRP dengan penambahan variabel depth.



Gambar 3. Skema protokol PRP

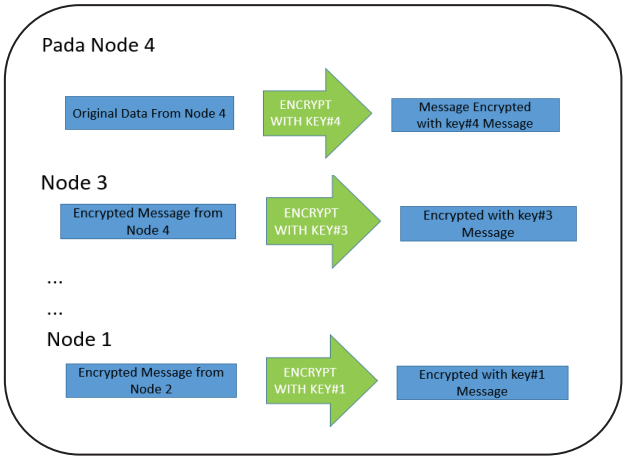
Aturan routing dari PRP,

- Node bebas untuk mengrimkan data pada node manapun yang berada dalam radius transmisinya.
- Arah transmisi data harus menuju ke node dengan *depth* yang lebih rendah dengan kata lain menuju ke gateway
- Node bertanggung jawab pada transmisi data sampai data tersebut sukses disalurkan pada node yang berada pada depth 2 tingkat dibawahnya
- Jika tidak lagi ada node yang lebih rendah depthnya maka transmisi boleh dilakukan ke node yang memiliki depth dengan nilai sama, artinya paket data sudah berada pada puncak node namun tidak ada akses langsung ke gateway

4.2 Multilevel Enkripsi dan Penandatanganan Data

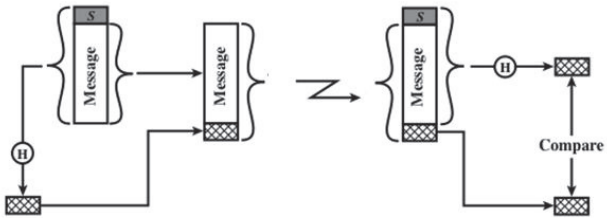
Enkripsi dan penandatanganan data secara multilevel ini hanya dapat dilakukan bersamaan dengan diimplementasikannya routing PRP pada jaringan WSN. Cara kerja dari metode ini adalah data dienkripsi dan diberi tanda tangan digital pada setiap node, menggunakan cara ini semakin banyak lompatan/hop yang dilakukan oleh satu paket maka data yang dibawanya akan semakin aman. Jika tidak dapat dikatakan terlalu aman maka metode ini akan mustahil untuk membuka pintunya tanpa mengetahui banyak kunci sekaligus yang tersebar pada node-node. Gambar dibawah mendeskripsikan bagaimana pesan dienkripsi secara multilevel, data berasal dari node 4 ingin menuju ke gateway pada node 1.

ISSN : 2085-4218



Gambar 4. Multilevel Data Enkripsi

Dengan cara yang sama, tanda tangan digital berfungsi sebagai metode untuk mendeteksi dimanakah terjadinya penyusupan oleh penyerang. Karena data yang sampai ke gateway saat dekripsi akan terlihat melewati node mana saja kah paket tersebut sebelum sampai gateway. Berikut adalah gambar bagaimana tanda tangan digital dilakukan.



Gambar 5. Multilevel Data Integrity

Metode ini memanfaatkan fungsi Hash untuk menandai paket yang disalurkan menggunakan spesifik kunci milik masing-masing node. Dengan skema ini hanya gateway yang dapat memastikan apakah pesan ini masih terjaga integritasnya atau sudah terdapat pengubahan isi. Cara deteksi adalah dengan dekripsi secara multilevel, gateway memiliki semua kunci node yang berada pada jaringannya, oleh karena itu dialah satu-satunya dalam topologi jaringan WSN yang dapat memnentukan data tersebut apakah masih asli atau sudah disusupi pesan oleh node yang tidak terdaftar dan juga dengan metode ini, gateway dapat menentukan pada node manakah terjadi penyerangan atau penyusupan.

5. Kesimpulan dan Saran

Penelitian ini bertujuan untuk memberikan skema baru dalam mengamankan data dengan memanfaatkan lompatan. Banyak hal dianggap ideal untuk membatasi lingkup penelitian. Titik paling rawan dari metode ini ada pada gateway, segala sumber daya untuk mengamankannya baik secara fisik maupun logik perlu dimaksimalkan pada titik ini. Oleh karena itu perlu peneltian lebih lanjut mekanisme untuk menghilangkan identitas diri (id&kunci) secara otomatis saat penyerangan fisik terdeteksi.

ISSN : 2085-4218

6. Daftar Referensi

[1] T. Sameer, B.Nael, H.Wendi, A Taxonomy of Wireless Micro-Sensor Network Models
[2] J. Biagoni , E.S. Sasaki, G, Wireless Sensor Placement For Reliable and Efficient Data Collection, 2003
[3] H.Tian, Shen.H, Matsuzawa.T, Developing Energy Efficient Topologi of Routing of Wireless Sensor Network, 2005
[4] Flaure.R.P, Shakre, A.V, Efficient in Node Authentication in WSN Using Virtual Certivicate Authority, 2014
[5] M.A. Youssef, M.F. Younis, K.A. Arisha, A Constrained Shorthest Path Energy Aware Routing Algorithm for Wireless Security Network, 2002
[6] Tian. H, shen. H, Matsuzawa. T, Random Walk Routing for WSN, 2005