MANAJEMEN KESALAHAN DALAM JARINGAN SENSOR NIRKABEL MENGGUNAKAN ROUTING PROTOCOL FOR LOW-POWER AND LOSSY NETWORK (RPL)

Muhammad Hafiz Reza Syaputra

Jurusan Sistem Komputer, Universitas Sriwijaya Palembang
Jl. Masjid Al Ghazali, Bukit Lama, Kec. Ilir Barat. I, Kota Palembang, Sumatera Selatan 30128, Indonesia

Email : hapiisreza@gmail.com

Abstrak

Jaringan sensor nirkabel (WSN) secara bertahap muncul sebagai salah satu area pertumbuhan utama untuk komputasi luas, Kemajuan terbaru dari teknologi WSN telah memungkinkan pengembangan pemantauan nirkabel baru dan aplikasi pengendalian lingkungan. Salah satu tantangan penelitian utama mengenai Wireless Sensor Networks (WSN) adalah manajemen kesalahan dan kegagalan. Itu jaringan harus dapat mendeteksi kesalahan dan bereaksi lebih cepat terhadap anomali ini dan memastikan kelangsungan pemantauan layanan. Di sisi lain, dengan RPL (IPv6 Routing Protocol untuk Low Power dan Lossy Network, RPL pada awalnya dirancang untuk jaringan statis, tanpa dukungan untuk mobilitas. Namun, menangani mekanisme perbaikan untuk RPL dengan mobile node adalah nyata tantangan. Dengan menggunakan metode protokol RPL (MFM-RPL yang efektif untuk Manajemen Kesalahan dengan di WSN.

Kata kunci : Wireless Sensor Networks, Fault Management, RPL protocol, FCAPS, Mobile node

Abstract

Wireless sensor networks (WSN) are gradually emerging as one of the main growth areas for broad computing, the latest advances in WSN technology have enabled the development of new wireless monitoring and environmental control applications. One of the main research challenges regarding Wireless Sensor Networks (WSN) is error and failure management. The network must be able to detect errors and react more quickly to these anomalies and ensure continuity of service monitoring. On the other hand, with RPL (IPv6 Routing Protocol for Low Power and Lossy Network, RPL was originally designed for static networks, without support for mobility. However, addressing the repair mechanism for RPL with mobile nodes is a real challenge. Using the RPL protocol method (Effective MFM-RPL for Error Management with on WSN.

Keyword : Wireless Sensor Networks, Fault Management, RPL protocol, FCAPS, Mobile node

I. PENDAHULUAN

Manajemen kesalahan secara luas dianggap sebagai bagian penting dari manajemen jaringan saat ini. Pesatnya pertumbuhan baru-baru ini dalam jaringan sensor nirkabel (WSN) telah semakin memperkuat pentingnya manajemen kesalahan, karena memainkan peran penting dalam penggunaannya yang efektif[1]. Wireless Sensor Networks (WSN) juga disebut Low power and Lossy Networks (LLNs), semakin muncul sebagai area yang menjanjikan dan menarik untuk berbagai aplikasi dalam kehidupan kita sehari-hari, karena mereka menawarkan banyak solusi untuk deteksi dan pemantauan di lingkungan kita. Pada saat yang sama WSN menghadirkan tantangan yang terkait dengan optimasi energi, menghormati kendala waktu nyata dan metode manajemen kesalahan untuk layanan komunikasi.

Namun keandalan dan kontinuitas pemantauan layanan tidak selalu dijamin di WSNs. Untuk memastikan kontinuitas layanan untuk menangkap, mengumpulkan dan memproses data, perlu untuk menerapkan strategi kontrol yang memenuhi persyaratan mereka sambil meminimalkan konsumsi energi. Di sisi lain kegagalan tidak dapat dihindari dalam LLNs, ini dapat menyebabkan konektivitas dan kehilangan data. Oleh karena itu, perlu bahwa kegagalan jaringan terdeteksi terlebih dahulu, cari node sensor yang salah dan langkah-langkah yang tepat diambil untuk melanjutkan operasi jaringan. Dalam konteks ini, manajemen dan metode perbaikan adalah fitur utama untuk setiap protokol routing dan merujuk pada kemampuan untuk memperbaiki topologi routing ketika kegagalan terjadi[2].

II. WIRELESS SENSOR NETWORK (WSN)

Jaringan sensor nirkabel (WSN) adalah teknologi signifikan yang menarik minat banyak penelitian. Kemajuan terbaru dalam komunikasi nirkabel dan elektronik telah memungkinkan pengembangan sensor berbiaya rendah, berdaya rendah, dan multi-fungsional yang berukuran kecil dan berkomunikasi dalam jarak pendek. Sensor murah dan cerdas, yang terhubung melalui jaringan nirkabel dan digunakan dalam jumlah besar, memberikan peluang yang belum pernah ada sebelumnya untuk memantau dan mengendalikan rumah, kota, dan lingkungan. Fungsi utama dari WSN adalah mengumpulkan data tersebar melalui jaringan sensor yang kemudian dikirimkan dengan jaringan wireless menuju Base Station (BS) untuk diolah lebih lanjut. Salah satu masalah yang sering muncul dalam implementasi WSN yaitu tingkat konsumsi energi dan masa hidup dari jaringan tersebut[3].

Selain itu, sensor jaringan memiliki spektrum aplikasi yang luas di area pertahanan, menghasilkan kemampuan baru untuk pengintaian dan pengawasan serta aplikasi taktis lainnya[4]. WSN biasanya memiliki sedikit atau tidak ada infrastruktur. Ini terdiri dari sejumlah node sensor (beberapa puluh hingga ribuan) yang bekerja bersama untuk memantau suatu wilayah untuk mendapatkan data tentang lingkungan[5].

Pada prinsipnya pembacaan kondisi oleh sensor ini akan diinformasikan secara realtime dan keamanan data yang terjamin hingga diterima oleh pengolah data. Beberapa karaketeristik dari wireless sensor ini diantaranya[6]:

- Dapat digunakan pada daya yang terbatas
- Dapat ditempatkan pada kondisi lingkungan yang keras
- Dapat digunakan untuk kondisi dan pemprosesan data secara mobile
- Mempunyai topologi jaringan yang dinamis, dengan sistem mode yang heterogen
- Dapat dikembangkan untuk skala besar

III. ROUTING PROTOCOL FOR LOW-POWER AND LOSSY NETWORK (RPL)

RPL adalah protokol routing standar de-facto yang sepenuhnya ditentukan untuk IPv6 WSNs. Karena WSN biasanya tidak memiliki topologi yang telah ditentukan, misalnya mereka yang menggunakan kabel point-topoint, RPL harus menemukan tautan untuk membentuk topologi pada awalnya. RPL membangun dan memelihara jaringan sebagai grafik asiklik terarah (DAG), yang dapat dibagi menjadi beberapa DAGs Berorientasi Tujuan (DODAG). Selain itu, dapat dianggap sebagai topologi routing logis melalui jaringan fisik[7]. Dalam beberapa kasus, jaringan harus dioptimalkan untuk skenario dan penyebaran aplikasi yang berbeda. Misalnya, DODAG dapat dibangun dengan cara di mana Jumlah Transmisi yang Diharapkan (ETX) atau di mana jumlah daya baterai saat ini dari sebuah node dipertimbangkan[8].

Spesifikasi RPL mendefinisikan empat jenis pesan kontrol untuk pemeliharaan topologi dan pertukaran informasi. Yang pertama disebut DODAG Information Object (DIO) dan merupakan sumber utama informasi kontrol routing. Ini dapat menyimpan informasi seperti Peringkat node saat ini, Mesin Virtual RPL saat ini, alamat IPv6 dari root, dll. Yang kedua disebut Tujuan Iklan Obyek (DAO). Ini memungkinkan dukungan jalur bawah dan digunakan untuk menyebarkan informasi tujuan ke atas di

sepanjang DODAG. Yang ketiga bernama DODAG Information Solicitation (DIS) dan memungkinkan sebuah simpul untuk meminta pesan DIO dari tetangga yang dapat dijangkau. Keempat tipe adalah DAO-ACK dan dikirim oleh penerima DAO sebagai respons terhadap pesan DAO.

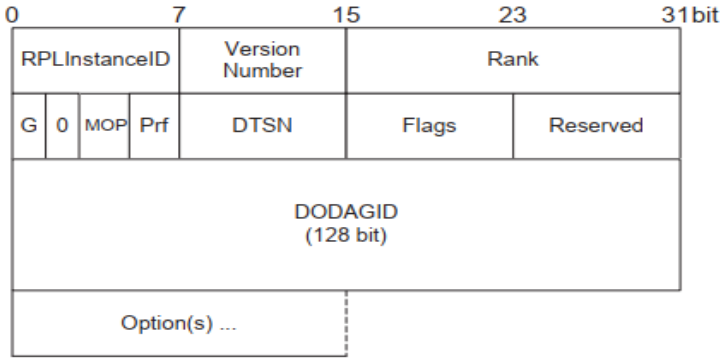
IV. STRUKTUR PROSES PEMBANGUNAN DODAG

Proses pembuatan grafik dimulai pada root , Konstruksi DODAG didasarkan pada proses Neighbor Discovery (ND), yang terdiri dari dua operasi utama[2]:

- Transmisi pesan kontrol DIO (Obyek Informasi DODAG) dituntut oleh root DODAG untuk membangun rute ke arah bawah dari root ke node
- Siaran pesan kontrol DAO yang dikeluarkan oleh node dan dikirim ke root DODAG untuk membangun rute ke arah atas. Untuk membangun DODAG baru, dua paket kontrol digunakan, disebut DIO dan DODAG Information Solicitation (DIS) untuk menyampaikan informasi DODAG.

DIO Message Structure

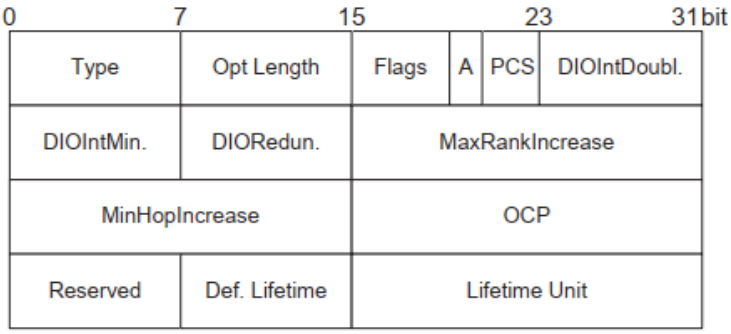
Seperti disebutkan sebelumnya, pesan DIO adalah sumber utama informasi yang diperlukan selama konstruksi topologi. Gambar 1 mewakili struktur pesan.



Gambar 1: Struktur Pesan DIO[8].

DIO pertama memungkinkan node untuk menemukan Mesin Virtual RPL dengan menyimpan yang sesuai di bidang data pertama. Kolom kedua dan ketiga termasuk Versi DODAG dan Pangkat pengirim pesan. Jika tidak disetel, DODAG dikatakan mengambang. Ini dapat terjadi ketika DODAG terputus dari sisa jaringan dan hanya mendukung konektivitas ke node-nya. Bidang MOP (ukuran 3 bit) diatur oleh root DODAG dan menentukan mode operasi yang digunakan untuk perutean ke bawah. Bidang Prf (ukuran 3 bit) mendefinisikan bagaimana simpul akar lebih disukai dibandingkan dengan simpul akar lainnya. Node seperti itu diidentifikasi oleh bidang DODAGID[8].

Pesan DIO dapat diperpanjang dengan menggunakan opsi. Dalam makalah ini, hanya opsi Konfigurasi DODAG yang dibahas, karena ini memainkan peran penting untuk pertukaran parameter. Gambar 2 menguraikan strukturnya.



Gambar 2: Opsi Konfigurasi DODAG[8].

Dua byte pertama selalu menyertakan jenis (0x04) dan panjang opsi (14 byte). Byte berikutnya termasuk bendera 'A', bidang Bendera dan bidang PCS. Dua byte berikutnya menentukan nilai timer maksimum *T*max dan nilai timer minimum *T*min diperlukan untuk pengaturan timer tetesan.

V. METODE UNTUK MANAJEMEN KESALAHAN DENGAN RPL (MFM-RPL)

Untuk menerapkan strategi kontrol yang memenuhi persyaratan WSN dengan mendeteksi kegagalan node sensor dan merespons lebih cepat dengan metode MFM-RPL memproses tiga kasus untuk kegagalan node di WSN dengan mengusulkan teknik perbaikan lokal baru dengan protokol RPL, menggunakan mobilitas node induk dengan prosedur pilihan berdasarkan pada:

1) kasus dari kegagalan simpul daun dalam topologi jaringan
2) kasus simpul selain kegagalan simpul daun seperti jumlah pendahulu dan / atau penerus kegagalan simpul lebih besar dari nol dan,
3) kasus simpul seperti pendahulunya adalah "root".

Algoritme yang diusulkan dalam makalah ini memungkinkan pada pertama kalinya, dengan mekanisme pendeteksian RPL dari kegagalan node dalam jaringan pada langkah kedua, solusinya adalah fokus untuk mengganti sumber kegagalan sensor oleh mobile node lain untuk ketiga kasus. Algoritma MFM-RPL menggabungkan tiga aturan baru, pertama kali untuk mendeteksi kegagalan simpul (didefinisikan oleh S seperti ditunjukkan pada tabel 1) untuk dua kasus dalam jaringan (leaf leaf, parent node). Pada langkah kedua solusinya adalah mengganti kegagalan node dengan mobilitas node pendahulunya (didefinisikan oleh Pred (S) seperti yang ditunjukkan pada tabel 1) untuk kemampuan pengumpulan dan perutean data. Ini ditentukan sebelumnya oleh aturan 1, 2 dan 3 yang didefinisikan lebih lanjut di bawah ini.

VI. ANALISIS HASIL SIMULASI

Contoh Untuk percobaan menggunakan simulasi Cooja, Keunggulan utama dari simulator Cooja adalah dapat mensimulasikan sensor node berdasarkan karakter yang sebenarnya, karena simulator Cooja memanfaatkan Java Native Interface (JNI) untuk mengeksekusi kode program ContikiOS dan TinyOS[9]. Parameter simulasi yang digunakan dalam simulasi ini ditunjukkan pada Tabel 1. Kami memvariasikan nilai DIO ke (2, 3, 4-16) dalam iterasi simulasi dan menempatkan rasio RX hingga 70%[2].

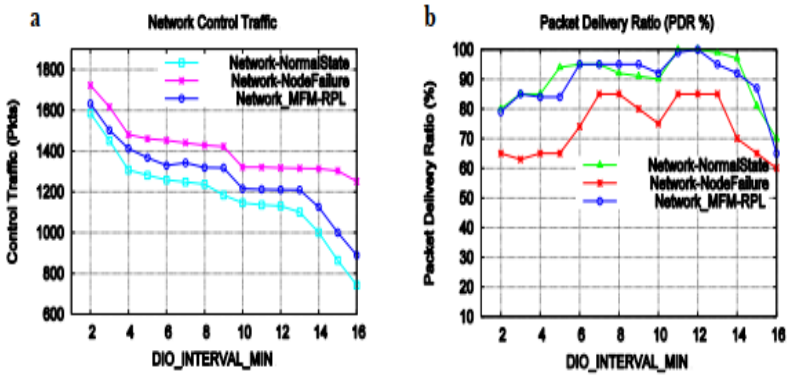
Parameters	Values
Network simulator	COOJA under contiki OS (2.6)
Area of Deployment	200 * 200 m²
Radio Environment	DGRM (Directed Graph Radio Medium)
Simulation time	1 hours
Client Nodes	100 and 1 sink
Mote Type	Tmote Sky
Duty Cycle	ContikiMAC
PYH and MAC Layer, Network Layer	IEEE 802.15.4, uIPv6
Objective Function	ETX
RX Ratio	30, 40, 50, 60, 70, 80, 90, 100
Max Packets	32583
DIO Min	2,3,4,5,6,7,8,9,10,11,12,13,14, 15,16

Table 1. Parameter Simulasi Umum[2].

Hasil simulasi digambarkan dalam Gambar (3a,b) dan (4a,b) untuk metrik kinerja hingga metrik yang dipelajari. Hasil dalam gbr. (3a) menunjukkan perbandingan antara tiga keadaan jaringan:

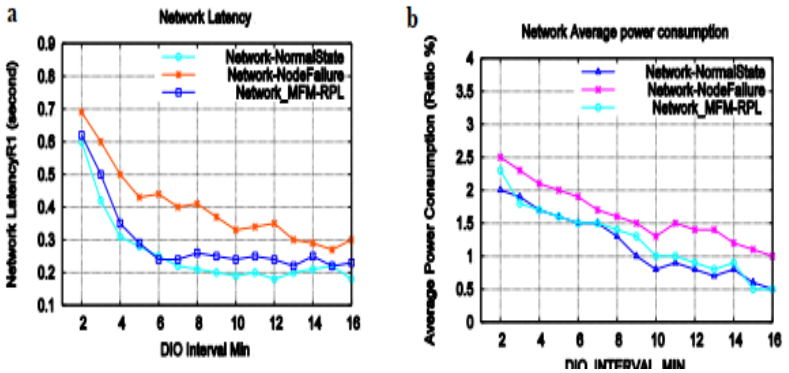
1) keadaan normal,
2) keadaan kegagalan simpul,
3) keadaan MFM-RPL dengan aturan1, aturan2 dan aturan3 seperti yang disajikan di bagian 4.

Selain itu, overhead kontrol untuk keadaan normal dan MFM-RPL luar biasa untuk nilai perkiraan selama konstruksi DAG dan transmisi data. Ini berbeda dengan nilai-nilai yang meningkat dalam keadaan kegagalan node. Hal ini terkait dengan kegagalan dan tidak adanya simpul di jaringan, yang mentransmisikan paket kontrol ICMPv6 (pesan DIO) oleh setiap node meningkat, sehingga node merespons untuk bergabung dengan dag dan membangun transmisi tersebut[2].



Gambar 3: Network control traffic dan Packet delivery ratio[2].

Dari gambar (3b), yang mewakili PDR (%) menunjukkan penurunan kinerja Jaringan untuk DIO Mini antara 2 dan 6 dan 13-16 untuk keadaan kegagalan simpul dalam jaringan, PDR di bawah 75%, itu berarti karena simpul kegagalan dan ketidakhadiran dalam kasus yang berbeda dan overhead kontrol yang lebih tinggi dikunyah dalam gambar (3a).



Gambar 4: Network latency dan Network average power consumption[2].

Pada Gambar (4a), DIO Min rendah (2 hingga 6) menurun perlahan dengan nilai minimum untuk metrik kinerja latensi, dan kira-kira sama untuk keadaan jaringan normal dan status MFM-RPL. Ini dapat dijelaskan dengan meningkatnya DIO min dan rasio Pengiriman Paket yang baik (lebih dari 95%) dan yang terendah dari overhead lalu lintas kontrol. Gambar (4b) menunjukkan bahwa konsumsi total energi penting ketika rendahnya interval DIO min (2, 3), jaringan mengkonsumsi banyak energi sekitar 2,3% rasio waktu untuk MFM-RPL, 2% untuk Jaringan RPL dalam keadaan normal dan 2,55 untuk kondisi kegagalan simpul[2].

VII. KESIMPULAN

Tujuan dari contoh simulasi ini adalah untuk mengevaluasi kinerja teknik baru yang diusulkan untuk protokol perbaikan RPL lokal dalam jaringan yang dikenal sebagai metode MFM-RPL. Evaluasi kinerja percobaan kami dilakukan pada simulator Cooja. Latensi Jaringan, kontrol lalu lintas, energi konsumsi,. Kesimpulan utama dari proposisi penelitian ini adalah bahwa MFMRPL memiliki beberapa manfaat untuk RPL di jaringan LLN dalam hal teknik proposisi baru untuk perbaikan lokal di RPL. Dibandingkan dengan perbaikan lokal saat ini yang menawarkan protokol RPL. Teknik ini bereaksi cepat untuk mengganti kegagalan node oleh pendahulu node mereka dengan mobilitas. Hasil eksperimen yang diperoleh telah membuktikan efektivitas metode manajemen kesalahan untuk memastikan kelangsungan layanan yang dijamin dalam jaringan.

VIII. DAFTAR PUSTAKA

[1] M. Y. U. Engjie, H. A. L. A. M. Okhtar, M. A. M. Erabti, dan J. O. H. N. M. O. U. Niversity, "F Ault M Anagement in W Ireless S Ensor N Etworks," *System*, no. December, hal. 13–19, 2007.

[2] D. Bendouda, L. Mokdad, dan H. Haffaf, "Method for Fault Management with RPL Protocol in WSNs," *Procedia Comput. Sci.*, vol. 73, no. Awict, hal. 395–402, 2015.

[3] W. Cahyadi, M. A. Wahyudi, dan C. S. Sarwono, "Analisis Perbandingan Konsumsi Energi dan Masa Hidup Jaringan pada Protokol LEACH, HEED, dan PEGASIS di Wireless Sensor Network," *J. Rekayasa Elektr.*, vol. 14, no. 2, 2018.

[4] G. Mao, B. Fidan, dan B. D. O. Anderson, "Wireless sensor network localization techniques," *Comput. Networks*, vol. 51, no. 10, hal. 2529–2553, 2007.

[5] J. Yick, B. Mukherjee, dan D. Ghosal, "Wireless sensor network survey," *Comput. Networks*, vol. 52, no. 12, hal. 2292–2330, 2008.

[6] T. Hidayat, "Sistem Pendeteksi Dini Longsor Menggunakan Teknologi Wireless Sensor Network (WSN)," *J. Tek. Elektro ITP*, vol. 6, no. 1, hal. 87–92, 2017.

[7] Q. Le, T. Ngo-Quynh, dan T. Magedanz, "RPL-based multipath Routing Protocols for Internet of Things on Wireless Sensor Networks," *Int. Conf. Adv. Technol. Commun.*, vol. 2015-February,

hal. 424–429, 2015.
[8] andreas Heider, "Einführung in Sensornetze - Abhängigkeiten zwischen Protokolldesign und verwendeter Hardware," *Work Progress), http//tools. ietf. org/html/draft-ietf-roll-rpl-19*, no. July, hal. 1–164, 2011.
[9] I. N. R. Hendrawan, "Analisis Kinerja Protokol Routing RPL pada Simulator," *J. Sist. dan Inform.*, vol. 12, no. 2, hal. 9–18, 2018.