Cyberspace: Jurnal Pendidikan Teknologi Informasi
Volume 5, Nomor 1, Maret 2021, 44-58

SAFE ROUTING MODEL AND BALANCED LOAD MODEL FOR WIRELESS SENSOR NETWORK

Julianto Agus Prabowo[1], Harry Dhika[2]

Program Studi Informatika, Fakultas Teknik Ilmu Komputer, Universitas Indraprasta PGRI
E-mail: juliantoagusp@gmail.com, dhikatr@yahoo.com

Abstract

Wireless Sensor Networks (WSNs) play a very important role in providing realtime data access for Big Data and Internet. However, the open deployment, energy constraint, and lack of centralized administration make WSNs very vulnerable to various kinds of malicious attacks. In WSNs identifying malicious sensor devices and eliminating their sensed information plays a very important role for mission critical applications. Standard cryptography and authentication schemes cannot be directly used in WSNs because of the resource constraint nature of sensor devices. Thus, energy efficient and low latency methodology is required for minimizing the impact of malicious sensor devices. This paper presents a Secure and Load Balanced Routing (SLBR) scheme for heterogeneous clustered based WSNs. SLBR presents a better trust-based security metric that overcomes the problem when sensors keep oscillating from good to bad state and vice versa, and also SLBR balances load among CH. Thus, aids in achieving better security, packet transmission, and energy efficiency performance. Experiments are conducted to evaluate the performance of proposed SLBR model over existing trust-based routing model namely Exponential Cat Swarm Optimization (ECSO). The result attained shows SLBR model attains better performance than ECSO in terms of energy efficiency (i.e., network lifetime considering first sensor device death and total sensor device death), communication overhead, throughput, packet processing latency, malicious sensor device misclassification rate and identification.

Keywords: *Energy efficiency, External and Internal attacks, Heterogeneous Wireless Sensor Networks, Load balancing, Multi-objective trust computation, Trust management mechanism, Secure routing, Reputation evaluation system.*

Abstrak

Wireless Sensor Networks (WSNs) memainkan peran yang sangat penting dalam menyediakan waktu akses data untuk aplikasi Big Data dan Internet. Namun, terbuka penyebaran, kendala energi, dan kurangnya administrasi terpusat membuat WSN sangat rentan terhadap berbagai macam serangan berbahaya. Di WSN mengidentifikasi sensor berbahaya perangkat dan menghilangkan informasi yang dirasakan memainkan peran yang sangat penting untuk misi aplikasi kritis. Kriptografi standar dan skema otentikasi tidak bisa langsung digunakan di WSN karena sifat kendala sumber daya perangkat

sensor. Jadi, energi metodologi yang efisien dan latensi rendah diperlukan untuk meminimalkan dampak berbahaya perangkat sensor. Makalah ini menyajikan skema Secure and Load Balanced Routing (SLBR) untuk WSN berbasis cluster yang heterogen. SLBR menyajikan metrik keamanan berbasis kepercayaan yang lebih baik yang mengatasi masalah saat sensor terus berosilasi dari kondisi baik ke buruk dan sebaliknya Sebaliknya, dan SLBR menyeimbangkan beban antara CH. Dengan demikian, membantu mencapai keamanan yang lebih baik, transmisi paket, dan kinerja efisiensi energi. Eksperimen dilakukan untuk mengevaluasi kinerja model SLBR yang diusulkan di atas model perutean berbasis kepercayaan yang ada yaitu Eksponensial Cat Swarm Optimization (ECSO). Hasil yang dicapai menunjukkan SLBR model mencapai kinerja yang lebih baik daripada ECSO dalam hal efisiensi energi (yaitu, jaringan seumur hidup mempertimbangkan kematian perangkat sensor pertama dan kematian perangkat sensor total), komunikasi overhead, throughput, latensi pemrosesan paket, kesalahan klasifikasi perangkat sensor berbahaya tingkat dan identifikasi.

Kata kunci: *Efisiensi energi, Serangan Eksternal dan Internal, Nirkabel Heterogen Jaringan Sensor, Load balancing, Perhitungan kepercayaan multi-tujuan, Manajemen kepercayaan mekanisme, Perutean aman, Sistem evaluasi reputasi.*

1. Pendahuluan

Jaringan Sensor Nirkabel telah menjadi salah satu aspek penting dari Internet of Things (IoT) aplikasi [1] dan memainkan peran yang sangat penting dalam menyediakan berbagai aplikasi IoT menggunakan node sensor nirkabel seperti pemantauan lingkungan, pertanian, keamanan negara, penanggulangan bencana dll [21], [22], [23], dan [24]. WSN didefinisikan sebagai jaringan perangkat fisik dan peralatan lain yang tertanam dengan koneksi internet dan sensor [1], WSN memberikan fleksibilitas pada objek yang saling berhubungan untuk merasakan dan mengontrol kerangka kerja dan ini mengarah ke integrasi langsung dari model komputasi dan dunia fisik. Selanjutnya interkoneksi antara objek tersebut memiliki kemampuan untuk mentransfer data dengan interaksi manusia yang minimal. Disebabkan oleh Fitur inheren WSN, dapat dengan mudah digunakan di lingkungan manapun (terutama bermusuhan), tetapi rentan terhadap berbagai ancaman [2], [3], [25] yang dapat menyebabkan penularan yang tidak dapat diandalkan.

Mari kita ambil misalnya, penjahat dunia maya mencoba mengeksploitasi terminal yang dikonfigurasi dengan buruk untuk merusak data atau mencuri data melalui penempatan hotspot yang tidak sah dan menyesatkan pengguna akhir. Karenanya, dalam Untuk memberikan keamanan yang lebih baik, model keamanan yang efisien perlu dirancang. Metode berbasis kriptografi adalah metode konvensional untuk mengamankan jaringan [9], [10]. Metode kriptografi membahas sejumlah masalah yang berkaitan dengan otentikasi, kebenaran, kerahasiaan, dan sertifikasi. Namun karena sifat WSN yang beragam, pendekatan tradisional gagal total. Kerugian utama dari teknik kriptografi adalah komputasi yang rumit membuat strategi kriptografi tidak sesuai untuk jaringan sensor nirkabel, dan hal itu diamati strategi ini memiliki overhead energi yang lebih tinggi [3], [4]. Karenanya, untuk mengatasi masalah seperti itu, Intrusion Detection System (IDS) telah digunakan untuk menyediakan mekanisme keamanan [5], [47]. Intrusion Detection System bertujuan untuk mendeteksi perilaku perangkat sensor atau fitur unggulan terkait ke perangkat sensor. Model IDS berbasis kepercayaan telah mendapatkan popularitas dan telah menunjukkan signifikansi peningkatan dalam mencapai keamanan yang efektif terhadap serangan internal [4], [5], [33], [34], [35], [36] di jaringan Peer-to-Peer (P2P) dan WSN juga.

IDS memiliki beberapa aplikasi di WSN; perutean keamanan adalah salah satunya, di mana algoritme yang dirancang memilih berdasarkan jalur yang paling aman pada evaluasi

kepercayaan perangkat sensor yang berdekatan [6]. Selain itu, [7] memperkenalkan model kepercayaan pertama untuk WSN, kerangka kerja menggunakan reputasi terdistribusi [11] dan diuraikan dalam [7] di mana dalam model mendeteksi perangkat sensor yang rusak sesuai dengan data transaksional antar tetangga perangkat sensor. Node menghitung reputasi sensor mitranya dengan membangun peringkat itu menunjukkan "kooperatif" [7] perangkat sensor mitra dalam menyampaikan data atau kualitas kemampuan node untuk menyampaikan informasi secara akurat di jaringan sensor. Dalam [7] rekomendasi kepercayaan tidak dipertimbangkan, karena itu gagal mendeteksi sejumlah serangan internal. Selanjutnya, [8] menerapkan IDS menggunakan kepercayaan QoS dan kepercayaan sosial yang membantu menginformasikan metrik kepercayaan, bagaimanapun, evaluasi keakraban nilai-nilai hanya bergantung pada terjadinya interaksi maksimum di antara node ini. Fenomena ini dapat dengan mudah disesatkan oleh perangkat sensor yang tidak jujur melewati batas interaksi normal. Selanjutnya, dengan pertumbuhan Internet, volume yang sangat besar data sedang dibuat yang mengarah ke berbagai ancaman dan masalah keamanan. Secara umum, mengadopsi IDS yang ada akan menyebabkan jumlah paket yang lebih tinggi yang dijatuhkan karena berat skenario beban lalu lintas. IDS kemudian menjadi lebih kompleks mengingat kasus-kasus seperti itu di Big Data lingkungan Hidup. Dengan demikian, evaluasi kepercayaan hanya menggunakan informasi status berbasis paket standar ketika data yang sangat besar menjadi sangat menantang karena keefektifan komputasi kepercayaan bisa jadi berkurang secara signifikan. Untuk menghindari degradasi ini, diperlukan penghitungan kepercayaan yang efektif model yang membawa pengorbanan yang baik untuk melakukan serangan orang dalam dengan mempertimbangkan lingkungan Big Data.
Tantangan utama untuk membangun model perutean yang aman dan efisien untuk WSN adalah sebagai berikut:

a. Menyeimbangkan tradeoff antara kinerja dan keamanan, prasyarat untuk heterogen
b. WSN [26].
c. Untuk mendeteksi perangkat berosilasi yang bergoyang dari kondisi baik ke buruk dan sebaliknya dan mengevaluasi kredibilitas umpan balik yang diberikan oleh perangkat sensor.
d. Penyeimbangan beban di antara perangkat kepala kluster cukup menantang karena model perutean yang ada selalu merutekan paket ke node dengan parameter kepercayaan tertinggi yang menyebabkan overhead di antara kepala cluster.

Hipotesis penelitian adalah banyaknya model routing berbasis multipath dan kepercayaan model berbasis yang dimodelkan bertujuan untuk menyeimbangkan pengorbanan antara pengurangan latensi, efisiensi energi dan mengurangi overhead dalam penyediaan keamanan untuk WSN. Namun, kepercayaan yang ada model perutean berbasis gagal untuk membedakan perangkat WSN yang berosilasi dan menyebabkan overhead energi di antara perangkat WSN berperilaku baik. Makalah ini berhipotesis bahwa, routing paket melalui yang terkecil overhead energi dengan perangkat parameter kepercayaan tertinggi akan membantu dalam mencapai tingkat keamanan yang optimal dan persyaratan kinerja seumur hidup jaringan dari jaringan sensor nirkabel heterogen. Untuk mengatasi tantangan penelitian, pekerjaan ini menyajikan Secure Load Balanced Routing (SLBR) model untuk WSN heterogen berbasis cluster. Model SLBR menggunakan Latensi Rendah Teknik perutean Multipath Berbasis Kluster Hemat Energi (LLEECMP) [19]. LLEECMP memilih CH dengan kategori energi yang berbeda (yaitu, rendah ke tinggi). Teknik LLEECMP menetapkan dua multipath yang berbeda untuk mentransmisikan paket real-time dan non-real-time di mana paket dirutekan melalui jalur terpendek (yaitu, untuk mengurangi latensi). Selanjutnya, SLBR mempekerjakan a teknik keamanan berbasis kepercayaan yang dimodelkan dalam bagian III dan dimasukkan ke dalam LLEECMP. Itu Metrik kepercayaan SLBR dimodelkan untuk secara akurat membangun kredibilitas umpan balik, mengidentifikasi berosilasi perangkat dari kondisi baik ke buruk dan sebaliknya, dan masa depan bobot keamanan perangkat sensor. Selanjutnya, untuk mengurangi overhead di antara CH dalam model SLBR, metrik perutean dengan beban seimbang adalah disajikan. Model SLBR akan membantu mencapai keamanan yang lebih baik dengan transmisi paket dan kinerja efisiensi energi.

Sisa kertas diatur sebagai berikut. Pada bagian II, penelitian survei aman yang ada metode perutean untuk WSN dibahas. Pada bagian III, perutean berbasis kepercayaan efisien yang diusulkan metode untuk WSN heterogen berbasis cluster disajikan. Dalam percobaan bagian kedua dari belakang studi dilakukan. Kesimpulan dan pekerjaan masa depan dijelaskan di bagian terakhir.

2. Survei Literatur

Bagian ini menyajikan survei ekstensif tentang berbagai skema perutean aman yang ada jaringan sensor nirkabel. Baru-baru ini, sejumlah model berbasis kepercayaan telah diperkenalkan menangani persyaratan Quality of Service (QoS) dan keamanan untuk aplikasi Big Data. Untuk menangani masalah yang disebutkan di atas dalam [12] menyajikan model komputasi kepercayaan berbasis Bayesian untuk WSN perutean hierarkis. Kepercayaan dihitung menggunakan informasi status paket dan perangkat sensor berbahaya diidentifikasi menggunakan parameter thresholding kepercayaan. Dalam [13] disajikan Skema Evaluasi Kepercayaan dan Reputasi Berbasis Eksponensial (ETRES) untuk keamanan penyediaan untuk jaringan sensor nirkabel. Untuk mengukur Direct Trust (DT) digunakan metode entropi. Selanjutnya, untuk memperkuat komunikasi dan menghadirkan lebih banyak keandalan, Kepercayaan Tidak Langsung (IDT) digunakan. Model dapat secara dinamis menyesuaikan bobot kepercayaan untuk mengurangi dampak yang ditimbulkan ke perangkat sensor yang disusupi.

Dalam [14] disajikan desain perutean sadar kepercayaan berbasis multi-atribut untuk WSNs. Perutean selesai berdasarkan perangkat sensor dengan rekomendasi, energi, dan parameter komunikasi yang lebih baik menggunakan jendela geser yang ditingkatkan. Model jendela geser mempertimbangkan frekuensi serangan untuk mengidentifikasi sifat jahat penyusup. Dalam [15] menunjukkan bahwa kebutuhan aplikasi IoT modern transmisi paket yang andal di bawah tautan yang tidak dapat diandalkan dan tidak stabil. Akibatnya, terkadang paket kegagalan mungkin timbul karena saluran yang buruk dan tidak dapat diandalkan. Jadi, model reputasi seharusnya tidak menghilangkan perangkat sensor tersebut sebagai perangkat berbahaya. Untuk mengatasi masalah seperti itu di [16], menunjukkan yang ada metode menggunakan mekanisme Geographic Opportunistic Routing (GOR) [28], [29], [30], [31] dengan beberapa perangkat sensor penerusan candidatur. Namun, mekanisme GOR mengalami Denial of Serangan Service (DoS) [27]. Ini karena beberapa perangkat berbahaya sengaja mengirim secara berlebihan paket tidak valid ke perangkat sensor penerima yang mempengaruhi fungsi normal sensor nirkabel jaringan. Untuk mengatasi serangan DOS dan memodelkan protokol yang andal [16] disajikan Entropy Berdasarkan metode GOR berbasis Autentikasi Selektif di mana kepercayaan dihitung menggunakan tautan nirkabel informasi status statistik. Model mereka mampu meminimalkan serangan DoS dengan minimal biaya komputasi. Namun, memeriksa setiap perangkat sensor untuk memvalidasi tanda tangan menginduksi penundaan yang signifikan.

Dalam [37] disajikan model beta yang ditingkatkan untuk mendeteksi perangkat sensor berbahaya. Yang berdekatan perangkat dipilih berdasarkan informasi kepercayaan selama fase komunikasi. Status file perangkat sensor yang berdekatan diperbarui secara berkala. Model ini meningkatkan efisiensi energi WSN. Namun, batasan energi dan memori tidak dipertimbangkan dalam model kepercayaan. Dalam [38] menangani masalah fluktuasi kepercayaan. Kepercayaan dihitung menggunakan kepercayaan langsung dan tidak langsung.

Namun, kredibilitas kepercayaan model tidak dipertimbangkan. Dalam [17], beberapa metodologi yang ada pertimbangkan sumber daya dan keamanan secara terpisah [39], [40], [41], [42]. Mereka juga menunjukkan seleksi yang buruk node hop akan menyebabkan kehilangan data atau paket perlu dikirim ulang sehingga menghasilkan sumber daya yang lebih tinggi konsumsi. Untuk pemilihan hop yang lebih baik, mereka menyajikan desain perutean berbasis

kepercayaan yang adaptif. Itu model menggunakan DT, IDT, dan Witness Trust (WT) dengan beberapa atribut untuk evaluasi kepercayaan. Model ini membantu membawa keseimbangan yang baik antara disipasi energi dan meningkatkan masa pakai WSN. Namun, ini menyebabkan latensi transmisi paket. Untuk meningkatkan kinerja transmisi paket dalam [18] disajikan desain routing multipath untuk WSN menggunakan teknik Exponential Cat Swarm Optimization (ECSO). Teknik ECSO adalah dirancang dengan menggabungkan Cat Swarm Optimization dengan Exponential Weighted Moving Average teknik. Pada ECSO, CH dipilih menggunakan penguin fuzzy dengan metode optimasi koloni semut [32]. Setelah pemilihan CH, multipath dibuat menggunakan Exponential Cat Swarm Optimization teknik. Path yang ideal diperoleh untuk mengkomunikasikan paket dengan mempertimbangkan berbagai QoS parameter seperti ketersediaan tautan, jarak, penundaan, kepadatan beban, energi, dan kepercayaan. Di sini cluster head dengan parameter QoS maksimal digunakan untuk pemanfaatan komunikasi data multipath Teknik ECSO. Meskipun model ECSO mencapai kinerja transmisi paket yang lebih baik dengan penyediaan keamanan itu masih menyebabkan overhead di antara CH karena paket-paket dirutekan ke sensor perangkat dengan parameter QoS maksimal. Untuk mengatasi masalah penelitian dalam membawa pengorbanan antara keamanan dan kinerja, prasyarat untuk WSN heterogen (LLEECMP [19] model) dirancang dan selanjutnya sebagai prasyarat, makalah ini menggunakan model keamanan berbasis kepercayaan untuk jaringan sensor nirkabel yang heterogen

3. Model routing berbasis kepercayaan yang efisien untuk heterogen berbasis cluster jaringan sensor nirkabel

Bagian ini menyajikan model Secure Load Balanced Routing untuk sensor nirkabel heterogen jaringan. Layanan aplikasi heterogen berbasis sensor nirkabel modern memerlukan latensi rendah pemberian layanan dengan penggunaan energi minimal dan mekanisme keamanan yang baik. Untuk memenuhi ini persyaratan metode pengelompokan yang efisien yaitu LLEECMP [19] untuk WSN heterogen adalah diimplementasikan. Pekerjaan ini memasukkan pemilihan kepala klaster LLEECMP ke dalam SLBR karena itu mencapai kinerja seumur hidup jaringan yang sangat baik jika dibandingkan dengan evolusioner algoritma komputasi seperti Swarm Optimization dan pemilihan Fuzzy Based Cluster Head metode. Selanjutnya, LLEECMP membawa pertukaran yang baik antara mengurangi latensi dan meningkatkan seumur hidup jaringan. Signifikansi utama adalah LLEECMP CH berdasarkan energi yang berbeda level / kategori, dua jenis jalur dipilih untuk routing paket real-time dan non-real-time dan paket dirutekan melalui jalur terpendek menuju stasiun pangkalan. Namun, model LLEECMP tidak menyediakan perutean yang aman. Baru-baru ini, sejumlah metode keamanan telah disajikan untuk WSN. Secara umum, skema keamanan digunakan untuk otentikasi node dan perlindungan data. Pekerjaan ini terutama berfokus pada membangun metode otentikasi node yang efisien untuk LLEECMP di clustered berbasis WSN heterogen. Skema otentikasi berbasis kepercayaan adalah salah satu metode yang efektif digunakan di WSN. Namun, skema keamanan berbasis kepercayaan yang ada tidak efisien sebagai umpan balik kredibilitas tidak akurat. Lebih lanjut, model keamanan berbasis kepercayaan yang ada tidak dapat mendeteksi perangkat jahat perangkat sensor saat berosilasi dari kondisi baik ke buruk atau sebaliknya. Seiring dengan, yang ada model menginduksi overhead perutean di antara perangkat sensor dengan parameter kepercayaan tertinggi. Ini adalah karena dalam skema perutean berbasis kepercayaan yang ada, paket diarahkan ke perangkat sensor dengan parameter kepercayaan tertinggi. Untuk mengatasi masalah penelitian, pekerjaan ini menyajikan kepercayaan model routing berbasis (yaitu, Secure Load Balanced Routing Model) untuk cluster berbasis heterogen jaringan sensor nirkabel.

a) *Model Jaringan dan Model Energi:*

Untuk mengevaluasi kinerja perutean model yang diusulkan, pengaturan berikut adalah dipertimbangkan. Perangkat sensor tidak bersifat seluler. Kepala cluster menerima dan mentransmisikan data. Stasiun pangkalan sudah diperbaiki dan ditempatkan jauh dari area penginderaan. Paket masuk jaringan berukuran sama. Transmisi paket rentan terhadap latensi dan kehilangan. Setiap sensor perangkat memiliki energi yang berbeda satu sama lain. Konsumsi energi perangkat sensor untuk WSN yang heterogen bergantung pada model komunikasi radio yang diadopsi. Dalam energi kerja ini disipasi penginderaan, komunikasi radio dan unit pemrosesan dipertimbangkan dalam pemodelan konsumsi energi. Unit penginderaan merasakan paket dan kemudian mentransmisikan ke unit pemrosesan. Kemudian, unit pemrosesan memproses paket-paket ini dan mengontrol unit komunikasi. Radio unit komunikasi melakukan komunikasi nirkabel di antara perangkat sensor. Unit utamanya adalah pemancar dan penerima antena dan komponen amplifikasi. Energi yang terakumulasi disipasi oleh ketiga unit ini adalah disipasi energi kumulatif oleh masing-masing unit. Oleh karena itu, disipasi energi kumulatif diperoleh sebagai berikut

$C_{\mathbb{E}} = K_{\mathbb{E}} + L_{\mathbb{E}} + D_{\mathbb{E}}$

di mana, , $L_{\mathbb{E}}$ $K_{\mathbb{E}}$ dan $D_{\mathbb{E}}$ adalah disipasi energi unit pemrosesan, penginderaan dan komunikasi, masing-masing. Model energi yang diterapkan memberikan distribusi energi yang lebih idealis di jaringan sensor nirkabel heterogen [19].

b) *Umpan balik dan evaluasi model kredibilitas:*

Bagian ini menyajikan umpan balik dan model evaluasi kredibilitas untuk WSN berbasis cluster. Pertama, pekerjaan ini menghitung Tingkat Kepercayaan (TL) yang dimiliki perangkat sensor tentang Perangkat Sensor masing-masing (SD) / Kepala Klaster (CH). Artinya, perangkat sensor menyimpan informasi tingkat kepercayaan keseluruhan

interaksi yang dibuat SD dengan SD lainnya. Untuk mengurangi overhead penyimpanan di antara perangkat sensor dan menetapkan bobot khusus sesi untuk interaksi, pekerjaan ini menggunakan pembaruan rata-rata eksponensial operasi untuk menyimpan hasil tingkat kepercayaan. Membiarkan $Sec_{u\ o}(x,y)$ menggambarkan tingkat kepercayaan keseluruhan itu

(,) Perangkat sensor memiliki perangkat sensor dengan mempertimbangkan jenis layanan tertentu dengan interaksi di periode sesi. Operasi pemutakhiran tingkat kepercayaan dapat dihitung menggunakan berikut ini $_h$ persamaan,

$Sec_{u\ o}(x,y) = \gamma * Sec_{rec}(x,y) + (1 - \gamma) * Sec_{u\ o-1}(x,y).(1)$

Dengan Sec_{rec} yang menggambarkan parameter tingkat Kepercayaan dari transaksi terbaru. Bersamaan dengan ini Work menyajikan model keamanan berbasis umpan balik di mana perangkat sensor memberikan umpan balik tentang kualitas pengalaman dengan perangkat sensor lain menggunakan persamaan berikut,

$$Sec_{rec} = \begin{cases} 0, if \text{ interaksi tidak dapat dipercaya}, 1, if \text{ interaksi dapat dipercaya}, \in (0,1), \text{sebaliknya.} \end{cases} (2)$$

Dalam Persamaan. (1), dioptimalkan menurut Collected Variance (CV) $\beta_{u\ o}\ (x,y)$ yang mana dihitung menggunakan persamaan berikut,

$$\gamma = W + d * \mu u\ o(x,y) \quad 1 + \beta u\ o(x,y) \quad (3)$$

Simpangan kumulatif dihitung menggunakan persamaan berikut

$\beta_{u\ o}(x,y) = d * \mu_{u\ o}(x,y) + (1 - d) * \beta_{u\ o-1}(x,y).$ (4)

Dimana d adalah parameter konstan yang menggambarkan bagaimana sistem berperilaku sehubungan dengan kegagalan baru-baru ini. Itu dapat dihitung menggunakan persamaan berikut

$\mu_{u\ o}(x,y) = \left|Sec_{u\ o\backslash -\ 1}(x,y) - Sec_{rec}\right|$. (5)

Dengan demikian, model tersebut memberikan reputasi yang kurang untuk varian terkini daripada varian yang dikumpulkan dan sebaliknya jika kita menurun. Lebih jauh, itu terlihat $\mu_{u\ o}(x,y)$ meningkat begitu juga. Ini menunjukkan lebih dari itu signifikansi (yaitu, ambang batas yang lebih tinggi) diberikan untuk umpan balik terbaru. Juga, menggambarkan reputasi bobot (yaitu, ambang) yang membantu mencegah menjadi parameter tetap.

$\mathbb{V}_{u\ o}(x,y) = \Sigma_{p \in \mathcal{H}}\left(Sec_{u\ o}(x,p) - Sec_{u\ o}(y,p)\right)2|\mathcal{H}(x,y)|$ (6)

di mana p mewakili perangkat sensor umum,menggambarkan perangkat sensor umum dengan siapa $\mathcal{H}$ (x,y) perangkat sensor dan telah berinteraksi.

Selanjutnya, untuk membangun hubungan antara perangkat sensor dan, perangkat sensor ($\mathbb{R}$ (x,y)) pertama membandingkan dengan variasi asosiasi. Kemudian perbarui asosiasi menggunakan berikut (,) $\mathcal{I}$ persamaan

$\mathbb{R}_{u\ o}$

$$(x,y) = \begin{cases} \mathbb{R}_{u\ o-\ 1}(x,y) + 1 - \mathbb{R}_{u\ o-\ 1}(x,y)X, & if\ \mathbb{V}_{u\ o}(x,y) < \mathcal{H}, \\ \mathbb{R}_{u\ o-\ 1}(x,y) - 1 - \mathbb{R}_{u\ o-\ 1}(x,y)Y, & else, \end{cases} \quad (7)$$

Dengan demikian, model tersebut memberikan reputasi yang kurang untuk varian terkini daripada varian yang dikumpulkan dan sebaliknya jika kita menurun. Lebih jauh, itu terlihat meningkat begitu juga. Ini menunjukkan lebih banyak ($\mu_{u\ o}(x,y)$)signifikansi (yaitu, ambang batas yang lebih tinggi) diberikan untuk umpan balik terbaru. Juga, menggambarkan reputasibobot (yaitu, ambang) yang membantu mencegah menjadi parameter tetap.

Variasi Personalisasi (PV) dalam umpan balik yang dapat dipercaya di antara perangkat sensor dan diperolehdengan berinteraksi dengan perangkat sensor umum dan menggunakan persamaan berikut.

$\mathbb{V}_{u\ o}(x,y) = \Sigma_{p \in \mathcal{H}}\left(Sec_{u\ o}(x,p) - Sec_{u\ o}(y,p)\right)2|\mathcal{H}(x,y)|$(6)

di mana mewakili perangkat sensor umum, menggambarkan perangkat sensor umum dengan siapa$\mathcal{H}$ (x,y) perangkat sensor dan telah berinteraksi.

Selanjutnya, untuk membangun hubungan antara perangkat sensor dan, perangkat sensor($\mathbb{R}$(x,y)) pertama membandingkan dengan variasi asosiasi. Kemudian perbarui asosiasi menggunakan berikut $\mathbb{V}_{u\ o}(x,y)$ $\mathcal{I}$persamaan

$\mathbb{R}_{u\ o}$

$$(x,y) = \begin{cases} \mathbb{R}_{u\ o-1}(x,y) + 1 - \mathbb{R}_{u\ o-1}(x,y)X, & if\ \mathbb{V}_{u\ o}(x,y) < \mathcal{H}, \\ \mathbb{R}_{u\ o-1}(x,y) - 1 - \mathbb{R}_{u\ o-1}(x,y)Y, & else, \end{cases} \quad (7)$$

di mana menggambarkan parameter hadiah dan menggambarkan parameter penalti, dan kedua parameter tersebut bisa dimodifikasi secara dinamis berdasarkan kebutuhan keamanan sistem.

c) *Evaluasi kredibilitas umpan balik:*

Pekerjaan ini mengevaluasi kredibilitas informasi umpan balik. Dalam keamanan berbasis kepercayaan yang ada model untuk jaringan sensor nirkabel, informasi kepercayaan yang diberikan oleh perangkat sensor yang baik adalahdianggap benar dan umpan balik yang diberikan oleh perangkat sensor berbahaya adalah salah. Namun, secara nyata waktu lingkungan WSN pertimbangan ini mungkin tidak selalu benar karena perangkat sensor yang baik mungkin memberikan informasi kepercayaan negatif dan perangkat sensor berbahaya secara berkala dapat memberikan informasi positif mempercayai informasi untuk menyembunyikan perilakunya yang berbahaya. Dengan demikian, penting untuk membangun yang efisien Metode evaluasi kredibilitas umpan balik. Untuk menghitung tingkat kepercayaan, umpan balik diberikan oleh sensor perangkat dengan keandalan yang baik dapat dipercaya dan aman. Dengan demikian, bobot tinggi diberikan pada sensor tersebut perangkat jika dibandingkan dengan perangkat sensor keandalan rendah. Membiarkan mendefinisikan Umpan Balik (,) Kredibilitas (FC) perangkat sensor dari sudut pandang perangkat sensor. Itu bisa diperkirakan ′menggunakan persamaan berikut

$\mathbb{F}_{u\ o}$

$$(x,y) = \begin{cases} 1 - \log\left(Sec_{u\ o}(x,y)\right) \log\theta, & if\ \mathbb{R}_{u\ o}(x,y) > \theta, \\ 0, & else \end{cases} \quad (8)$$

dimana log 0 menggambarkan parameter kesamaan yang paling tidak dapat ditoleransi.

d) *Evaluasi Kepercayaan Langsung:*

Bagian ini menyajikan evaluasi Direct Trust komunikasi intra cluster (yaitu, di antara Sensor Perangkat (SD) dan Cluster Head (CH)) dan komunikasi antar cluster (yaitu, antara Cluster Head ke Cluster Head dan Cluster Head ke Base Station). Membiarkan mewakili nilai langsung yang dapat dipercaya $\mathbb{L}_{u\ o}(x,y)$ perangkat sensor itu memiliki perangkat sensor dengan setidaknya interaksi dalam contoh sesi. $_h$ Menggunakan metrik yang dapat dipercaya, Kepercayaan Langsung dihitung menggunakan persamaan berikut

$$\mathbb{L}_{u\ o}(x,y) = Sec_{u\ o}(x,y). \quad (9)$$

Jadi, menggunakan Persamaan. (9) jika perangkat sensor memberikan kinerja transmisi yang lebih baik, maka sensor perangkat akan memberikan parameter terpercaya yang ideal. Ini membantu perangkat sensor untuk lebih dipercaya parameter dari sudut pandang perangkat sensor.

e) *Evaluasi Kepercayaan Tidak Langsung:*

Bagian ini menyajikan evaluasi Indirect Trust komunikasi intra cluster dan antar cluster komunikasi berdasarkan pengalaman dari perangkat sensor lain. Untuk mencapai aman komunikasi, perangkat sensor meminta sensor lain untuk memberikan informasi umpan balik dari sensor perangkat yang beroperasi dengan perangkat sensor tertentu. Perangkat sensor mengumpulkan umpan balik dari yang lain perangkat sensor untuk komputasi Indirect Trust menggunakan persamaan berikut

$$\mathbb{G}u\ o(x,y) = \begin{cases} \Sigma p \in Z - \{x\}\mathbb{F}u\ o(x,p) * \mathbb{L}u\ o(x,y)\Sigma p \in Z - \{x\}\mathbb{F}u\ o(x,p), 0, if\ |Z - \{x\}| > 0, \\ if\ |Z - \{x\}| = 0.\ if\ |Z - \{x\}| > 0, \end{cases} \quad (10)\ if\ |Z - \{x\}| = 0.(10)$$

dimana, $Z = \mathbb{S}(y)$ menggambarkan set perangkat sensor, yang berinteraksi dengan perangkat sensor.

f) *Evaluasi Kepercayaan terbaru:*

Bagian ini menyajikan evaluasi Trust Terkini untuk komunikasi intra cluster dan antar cluster komunikasi di bawah WSN yang heterogen. Parameter tepercaya terbaru dapat dihitung menggunakan metrik kepercayaan Langsung dan Tidak Langsung. Disini Direct Trust diberikan kepercayaan yang lebih tinggi sebagai perangkat sensor komputasi melakukan lebih banyak interaksi dengan perangkat sensor target. Biarkan $\mathbb{C}uo(x,y)$menjelaskan parameter tepercaya saat ini yang dimiliki perangkat sensor pada perangkat sensor.

$$\mathbb{C}u\ o(x,y) = \delta * \mathbb{L}u\ o(x,y) + (1 - \delta) * \mathbb{G}u\ o(x,y)\ (11)$$

dimana δ menggambarkan bobot parameter yang dapat dipercaya yang dapat dievaluasi menggunakan persamaan berikut

$$\delta = \mathbb{T}u(x,y)\mathbb{T}u(x,y) + \mathbb{T}u(x,y)(12)$$

$\mathbb{T}u(x,y)$ perangkat dalam contoh sesi. Kemudian, menggambarkan ukuran interaksi rata-rata yang lain $\mathbb{T}u(x,y)$ perangkat sensor telah dilakukan sehubungan dengan perangkat sensor dan dibuat dengan menggunakan berikut persamaan

$$\mathbb{T}u(x,y) = \Sigma p \in Z - \{x\}\mathbb{F}u\ o(x,p) * \mathbb{T}u(p,y)|Z - \{x\}|(13)$$

g) *Evaluasi Kepercayaan Historis:*

Bagian ini menyajikan Evaluasi Kepercayaan Historis komunikasi intra cluster dan inters komunikasi cluster di bawah WSN heterogen. Seiring berjalannya waktu, parameter tepercaya terbaru akan menjadi parameter historis yang dapat dipercaya. Mirip dengan komputasi parameter yang dapat dipercaya, file parameter kepercayaan historis dihitung dengan operasi pembaruan rata-rata secara eksponensial. Membiarkan $\mathbb{L}u\ o(x,y)$ menjelaskan parameter Historical Trust yang dimiliki perangkat sensor pada perangkat sensor.

$$\mathbb{L}u\ o(x,y) = \varphi * \mathbb{L}u\ o-1(x,y) + \mathbb{C}u\ o-1(x,y)2,(14)$$

Dimana $\varphi(0 \leq \varphi \leq 1)$ adalah parameter reward dan. Dengan menggunakan Historical Trust $\mathbb{L}_{00}(x,y) = 0$ parameter, perangkat sensor berbahaya saat ini yang berinteraksi dengan perangkat sensor tertentu tidak bisacepat berperilaku ideal dengan mengabaikan perilaku sebelumnya. Untuk perangkat sensor yang akan dianggap sebagai ideal, seseorang harus berinteraksi secara kooperatif untuk sejumlah besar interaksi sehingga parameter tepercaya terbarunya dapat diganti dengan parameter Kepercayaan Historisnya.

4. Hasil Simulasi Dan Analisis

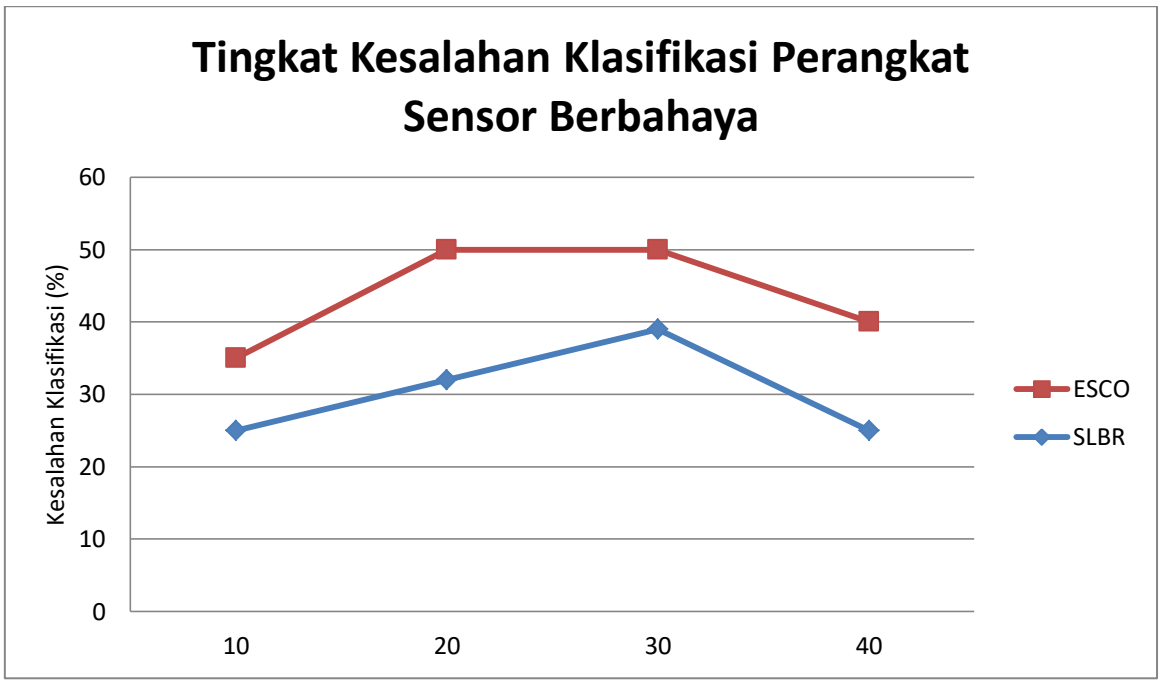
Bagian ini melakukan evaluasi kinerja model SLBR yang diusulkan pada ECSO yang ada
model perutean [18]. Simulator SENSORIA [20] dipertimbangkan untuk studi eksperimental. Itu kinerja skema perutean aman yang diusulkan dan yang ada dievaluasi dalam istilah berbahaya tingkat kesalahan klasifikasi perangkat sensor, identifikasi perangkat sensor berbahaya, throughput sistem, dan efisiensi energi (yaitu, umur jaringan). Untuk mengevaluasi kinerja 1000 perangkat sensor ditempatkan di area penginderaan 100m × 100m yang terdiri dari persentase tertentu yang berbahaya perangkat sensor. Pekerjaan ini masing-masing dianggap 10%, 20%, 30%, dan 40%. Simulasi pengaturan parameter untuk analisis eksperimental ditabulasikan pada Tabel I.

TABEL I. SIMULASI PARAMETER YANG DIPERTIMBANGKAN

Parameter Jaringan	**Nilai**
Area Jaringan / Simulasi	100m x100m
Jumlah stasiun pangkalan / Sink	1
Jumlah perangkat sensor	500 sampai 1000
Jumlah perangkat sensor berbahaya	10, 20, 30, dan 40 (%)
Protokol MAC	IEEE 802.11b dengan 1 Mbps
Propagasi radio / Jangkauan transmisi masing-masing sensor alat	6 meter
Rentang penginderaan setiap perangkat	3 meter
Energi awal setiap perangkat sensor	0,05-0,2 Joule (j)
Disipasi energi radio	50 nj / bit
Kontrol panjang paket	248 bit
Panjang paket data	2000 bit
Kecepatan transmisi data	100 bit / dtk
Bandwidth	10.000 bit / dtk
Merasakan waktu acara	0,1 dtk
Jenis perangkat sensor	Suhu
Konsumsi energi menganggur (Eelec)	50 nj / bit
Energi amplifikasi (Emp)	100 pJ / bit / m2

a) *Evaluasi kinerja tingkat kesalahan klasifikasi perangkat sensor berbahaya mempertimbangkan bervariasi*

persentase node berbahaya: Bagian ini menyajikan evaluasi kinerja tingkat kesalahan klasifikasi perangkat sensor berbahaya SLBR yang diusulkan melalui model perutean ECSO yang ada di bawah WSN berbasis cluster yang heterogen. Itu kinerja tingkat kesalahan klasifikasi perangkat sensor berbahaya yang dicapai oleh SLBR dan ECSO Mengingat ukuran perangkat sensor berbahaya yang berbeda ditunjukkan pada Gambar. 1. Dari hasil yang diperoleh itu dapat dilihat bahwa SLBR mengurangi tingkat kesalahan klasifikasi sebesar 28,57%, 34,0%, 22,0%, dan 35,135% melebihi ECSO saat perangkat sensor berbahaya masing-masing adalah 10%, 20%, 30%, dan 40%. Dari Hasil keseluruhan yang dicapai terlihat SLBR jauh lebih efisien daripada model ECSO yang ada mempertimbangkan perangkat sensor berbahaya yang berbeda untuk kesalahan klasifikasi perangkat sensor berbahaya di jaringan sensor nirkabel.



Evaluasi kinerja tingkat identifikasi perangkat sensor berbahaya mempertimbangkan bervariasi perangkat sensor berbahaya.

5. Kesimpulan

Meminimalkan disipasi energi dengan penyediaan keamanan yang lebih baik sangat diinginkan di Big modern Aplikasi data dan IoT. Selanjutnya, untuk memenuhi aplikasi ini,

penting untuk mengurangi latensi dengan hasil yang lebih baik dan overhead komunikasi yang minimal. Jadi, untuk memberikan yang efisien mekanisme keamanan dengan kebutuhan energi WSN, metode yang ada menggunakan trust- metode keamanan berbasis. Namun, model ini tidak efisien jika perangkat sensor tetap menyala berosilasi dari perilaku berbahaya ke normal dan sebaliknya. Selanjutnya, komunikasi multipathdigunakan oleh beberapa metode yang ada untuk mengurangi latensi komunikasi. Namun, ini pendekatan menginduksi overhead energi di antara CH sebagai perangkat dengan parameter kepercayaan maksimal dipilih untuk paket perutean. Untuk mengatasi masalah penelitian, pekerjaan ini menyajikan beban yang aman model perutean yang seimbang. Eksperimen dilakukan untuk mengevaluasi kinerja model SLBR di atas model ECSO. Tingkat kesalahan klasifikasi perangkat sensor berbahaya rata-rata sebesar 29,92% adalah dicapai oleh SLBR dibandingkan model ECSO. Kemudian identifikasi perangkat sensor berbahaya rata-rata peningkatan sebesar 18,46% dicapai oleh SLBR dibandingkan model ECSO. Throughput rata-rata peningkatan sebesar 21,45% dicapai oleh SLBR dibandingkan ECSO. Overhead komunikasi rata-rata dan pengurangan latensi pemrosesan paket sebesar 69,95% dan 21,13% dicapai oleh SLBR melalui ECSO model, masing-masing. Peningkatan kinerja seumur hidup jaringan sebesar 45,86% dan 61,45% dicapai oleh SLBR atas ECSO dengan mempertimbangkan kematian perangkat sensor pertama dan kematian perangkat sensor total, masing-masing. Hasil signifikan yang dicapai adalah karena penggunaan metrik kepercayaan bersih dan beban yang lebih baik model balancing. Pengurangan latensi rata-rata 67,5% dan 42,23% dicapai oleh SLBR selama [16] dan [17], masing-masing. Hasil keseluruhan yang dicapai menunjukkan efisiensi model SLBR terhadap status model seni [16], [17], dan [18]. Signifikansi pekerjaan penelitian dijelaskan sebagai berikut. Metode perutean dengan beban seimbang yang aman disajikan. Model ini mengurangi overhead CH yang membantu peningkatan seumur hidup CH. Jalur terpendek dengan beban paket paling sedikit, parameter kepercayaan maksimum, dan parameter energi yang lebih baik digunakan untuk paket routing di WSN heterogen berbasis cluster. Itu Model SLBR mencapai kinerja masa pakai yang lebih baik daripada ECSO baik dalam hal kematian node pertama maupun total kematian node. Dengan demikian, membantu meningkatkan konektivitas jaringan WSN. Model SLBR mencapai throughput yang lebih baik, mengurangi kesalahan klasifikasi, meningkatkan identifikasi node berbahaya dengan latensi dan overhead komunikasi yang lebih sedikit jika dibandingkan dengan ECSO [18], dan teknologi canggih lainnya metode perutean aman [16], [17]. Pekerjaan masa depan akan mempertimbangkan evaluasi kinerja mempertimbangkan parameter jaringan lainnya dan juga mempertimbangkan menganalisis paket untuk mendeteksi yang berbeda jenis serangan.

Referensi

[1] T. M Behera, SK Mohapatra, UC Samal, MS Khan, M. Dansoman, & AH Gangdom,
"Pemilihan cluster-head berbasis energi sisa di WSN untuk aplikasi IoT," IEEE Internet of
Things Journal, 6 (3), 5132-5139, 2019.

[2] K. Kalkan, "SUNTEC: SDN Memanfaatkan Pengelompokan Aman berbasis Kepercayaan di IoT," Komputer Jaringan, 178. 107328. 10.1016 / j.comnet.2020.107328, 2020.

[3] Xueqiang Yin, dan Shining Li. "Model evaluasi kepercayaan dengan pembobotan berbasis entropi untuk deteksi node berbahaya dalam jaringan sensor nirkabel, "EURASIP Journal on Wireless Komunikasi dan Jaringan, (2019) 2019: 198.

[4] BD Narayan, P. Vineetha, dan BKR Alluri, “Peningkatan pemilihan kepala klaster berbasis kepercayaan dalam jaringan sensor nirkabel, "Dalam Inovasi dalam ilmu komputer dan teknik (hlm. 263-
275). Springer, Singapura, 2019.
[5] Danyang Qin, Songxiang Yang, Shuang Jia, Yan Zhang, Jingya Ma, dan Qun Ding, "Penelitian tentang Mekanisme Perutean Aman Berbasis Kepercayaan untuk Jaringan Sensor Nirkabel, "di IEEE
Access, vol. 5, hlm. 9599-9609, DOI: 10.1109 / ACCESS.2017.2706973, 2017.
[6] Osama AlFarraj, Ahmad AlZubi, Amr Tolba, “Pemilihan tetangga berbasis kepercayaan menggunakan aktivasi berfungsi untuk perutean yang aman dalam jaringan sensor nirkabel, "Journal of Ambient Intelligence dan Komputasi Manusiawi, https://doi.org/10.1007/s12652-018-0885-1, 2018.
[7] Shuzie Nie, “Model kepercayaan baru dari pengoptimalan dinamis berdasarkan metode entropi dalam nirkabel jaringan sensor, ”Komputasi Cluster 22 (7): 1–10, DOI: 10.1007 / s10586-017-1337-y, 2017.
[8] Raja Waseem Anwar, Anazida Zainal, Fatma Outay, Ansar Yasar, Saleem Iqbal “BTEM:
Mekanisme evaluasi kepercayaan berbasis kepercayaan untuk Jaringan Sensor Nirkabel ”, Generasi Mendatang Sistem Komputer, Volume 96, DOI: 10.1016/j.future.2019.02.004,2019.
[9] S. Agrawal, ML Das dan J. Lopez, "Deteksi Serangan Penangkap Node di Sensor Nirkabel Networks, "dalam IEEE Systems Journal, vol. 13, no. 1, pp. 238-247, March 2019.
[10] AA Fröhlich, RM Scheffel, D. Kozhaya dan PE Veríssimo, "Byzantine Resilient Protocol for the IoT, "dalam IEEE Internet of Things Journal, vol. 6, no. 2, pp. 2506-2517, April 2019.
[11] AW Al-Dabbagh, Y. Li dan T. Chen, "Sistem Deteksi Intrusi untuk Serangan Cyber di Sistem Kontrol Jaringan Nirkabel, "dalam Transaksi IEEE di Sirkuit dan Sistem II: Express Briefs, vol. 65, tidak. 8, hlm.1049-1053, Agustus 2018.
[12] W. Meng, W. Li, C. Su, J. Zhou dan R. Lu, "Meningkatkan Manajemen Kepercayaan untuk Nirkabel Deteksi Intrusi melalui Pengambilan Sampel Lalu Lintas di Era Big Data, "dalam IEEE Access, vol. 6, hlm. 7234-7243, 2018.
[13] J. Zhao, J. Huang dan N. Xiong, "Kepercayaan dan Reputasi Berbasis Eksponensial yang Efektif Evaluation System in Wireless Sensor Networks, "dalam IEEE Access, vol. 7, pp. 33859-33869,2019.
[14] B. Sun dan D. Li, "Protokol Perutean Sadar Tepercaya Dengan Multi-Atribut untuk WSNs, "dalam IEEE Access, vol. 6, pp. 4725-4741, 2018.
[15] H. Sedjelmaci, SM Senouci dan T. Taleb, "Game Keamanan Akurat untuk Sumber Daya Rendah Perangkat IoT, "dalam IEEE Transactions on Vehicular Technology, vol. 66, no. 10, pp. 9381-9393, Oktober 2017.
[16] C. Lyu, X. Zhang, Z. Liu dan C. Chi, "Geografis Berbasis Otentikasi Selektif Routing Oportunistik dalam Jaringan Sensor Nirkabel untuk Internet of Things Against DoS Attacks, "dalam IEEE Access, vol. 7, pp. 31068-31082, 2019.
[17] NA Khalid, Q. Bai dan A. Al-Anbuky, "Adaptive Trust-Based Routing Protocol for Large Scale WSNs, "dalam IEEE Access, vol. 7, pp. 143539-143549, 2019.
[18] PKH Kulkarni dan P. Malathi Jesudason, "Transmisi data multipath di WSN menggunakan eksponensial cat swarm dan optimasi fuzzy, "dalam IET Communications, vol. 13, no. 11, hlm.1685-1695, 16 7 2019.

[19] Gousia Thahniyath, M. Jayaprasad, “Teknik Perutean Latensi Rendah dan Hemat Energi
untuk Jaringan Sensor Nirkabel Hetrogeneous berbasis Cluster, dalam Journal of Advanced Research dalam Dynamical and Control Systems, vol.2, pp.977-985, 2018.
[20] JN Al-Karaki dan GA Al-Mashaqbeh, "SENSORIA: Platform Simulasi Baru untuk Jaringan Sensor Nirkabel, "Konferensi Internasional 2007 tentang Teknologi Sensor dan Aplikasi (SENSORCOMM 2007), Valencia, hlm.424-429, 2007.
[21] I. Butun, SD Morgera, dan R. Sankar, "Sebuah survei sistem deteksi intrusi di nirkabel
jaringan sensor, ”IEEE Communications Surveys & Tutorials, vol. 16, tidak. 1, hlm. 266–282,2014.
[22] A. Abduvaliyev, ASK Pathan, Jianying Zhou, R. Roman, dan Wai-Choong Wong, “Di area penting dari sistem deteksi intrusi dalam jaringan sensor nirkabel, ”IEEE Communications Survei & Tutorial, vol. 15, tidak. 3, hlm. 1223–1237, 2013.
[23] BB Zarpelão, RS Miani, CT Kawakani, dan SC de Alvarenga, “Survei intrusi deteksi di Internet of Things, ”Jurnal Aplikasi Jaringan dan Komputer, vol. 84, hal.25–37, 2017.
[24] A. Ghosal dan S. Halder, “Sebuah survei tentang deteksi intrusi hemat energi pada sensor nirkabel jaringan, ”Journal of Ambient Intelligence dan Smart Environments, vol. 9, tidak. 2, hlm. 239– 261, 2017.
[25] Z. Ruirui, X. Xin, “Deteksi Intrusi di Jaringan Sensor Nirkabel dengan Peningkatan NSA Berdasarkan Divisi Luar Angkasa ”, Jurnal sensor, SN - 1687-725X UR https://doi.org/10.1155/2019/5451263, 2019.
[26] F. Gianluigi, Z. Mengjia, H. Xu, Z. Bo, F. Xiangxiang, "Nirkabel Energi Heterogen
Protokol Pengelompokan Jaringan Sensor ", Komunikasi Nirkabel dan Komputasi Seluler, vol. 1530-8669, https://doi.org/10.1155/2019/7367281, 2019.
[27] DR Raymond dan SF Midkiff, “Denial-of-service dalam jaringan sensor nirkabel: Serangan dan pertahanan, "IEEE Pervasive Computing, no.1, hlm 74-81, 2008.
[28] R. Sanchez-Iborra dan M. Cano, “JOKER: Protokol perutean oportunistik baru,", "IEEE Journal on Selected Area in Communications, vol. 34, tidak. 5, hlm. 1690-1703, Mei 2016.
[29] J. Luo, J. Hu, D.Wu, dan R. Li, "Algoritme perutean oportunistik untuk pemilihan node relai di jaringan sensor nirkabel, "IEEE Trans. Ind. Informat., vol. 11, no. 1, pp. 112-121, Feb. 2015.
[30] J. So dan H. Byun, “Perutean oportunistik yang seimbang untuk sensor nirkabel duty-cycled jaringan, "IEEE Transactions on Mobile Computing, vol. 16, no. 7, pp. 1940-1955, Jul. 2017
[31] L. Cheng, J. Niu, J. Cao, SK Das, dan Y. Gu, "QoS sadar perutean oportunistik geografis
dalam jaringan sensor nirkabel, "IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 7, pp. 1864-1875, Juli 2014.
[32] PKH Kulkarni, P. Malathi, "PFuzzyACO: Pendekatan Pengoptimalan Berbasis Fuzzy untuk Energi- sadar Cluster Head Selection di WSN, "Journal of Internet Technology, vol. 20, no. 6, pp.
1787-1800, November 2019.

[33] Y. Liu et al., `` QTSAC: Sebuah protokol MAC hemat energi untuk meminimalkan penundaan dalam nirkabel jaringan sensor, " IEEE Access, vol. 6, hlm.8273-8291, 2018.
[34] J. Tang, A. Liu, J. Zhang, NN Xiong, Z. Zeng, dan T. Wang, ``A perutean aman berbasis kepercayaan skema menggunakan pendekatan traceback untuk jaringan sensor nirkabel penghasil energi Sensor, vol. 18, tidak. 3, hlm.751, 2018.
[35] M. Huang et al., `` Skema caching berbasis perutean layanan untuk CRN yang dibantu cloud, " IEEE Access, vol. 6, hlm.15787-15805, 2018.
[36] T. Qiu, Y. Zhang, D. Qiao, X. Zhang, ML Wymore, dan AK Sangaiah, `` Waktu yang tepat skema sinkronisasi untuk Internet of Things industri, " IEEE Trans. Ind. Informat., Vol. 14, tidak. 8, hlm.3570-3580, Agustus 2018.
[37] V. Umarani, KS Sundaram, dan D. Jayashree, ``Enhanced beta trust model in wireless sensor jaringan, " dalam Proc. Int. Conf. Inf. Komun. Menanamkan. Syst., Februari 2016, hlm. 1-5.
[38] N. Labraoui, `` Sebuah skema manajemen kepercayaan handal dalam jaringan sensor nirkabel, " di Proc. IEEE Int. Symp. Program. Syst. (ISPS), April 2015, hlm. 1-6.
[39] G. Han, J. Jiang, L. Shu, J. Niu, dan H.-C. Chao,`` Manajemen dan penerapan kepercayaan pada jaringan sensor nirkabel: Sebuah survei, " J.Comput. Syst. Sci., Vol. 80, tidak. 3, hlm. 602-617, 2014.
[40] J. Jiang, G. Han, F.Wang, L. Shu, dan M. Guizani, `` Model kepercayaan terdistribusi yang efisien untuk jaringan sensor nirkabel, " IEEE Trans. Distribusi Paralel. Syst., Vol. 26, tidak. 5, hlm. 1228-1237, 2015.
[41] A. Ahmed, KA Bakar, MI Channa, K. Haseeb, dan AW Khan, `` TERP: A trust and energy protokol perutean sadar untuk jaringan sensor nirkabel, " IEEE Sensors J., vol. 15, tidak. 12, hlm. 6962- 6972, 2015.
[42] NA Khalid, `` Pengambilan keputusan routing berbasis kepercayaan terdistribusi untuk WSN, " Ph.D. disertasi, School Eng., Comput. Matematika. Sci., Universitas Auckland Technol., Auckland, Selandia Baru, 2019.