SMARTICS Journal, Vol.10 No. 1 2024. p 21-26
ISSN online: 2476-9754, ISSN print: 2623-0429
DOI : https://doi.org/10.21067/smartics.v10i1.9186

Sistem Keamanan *Data Privacy* Pada Jaringan Sensor Nirkabel Menggunakan Teknik *Routing*

Yeni Yanti[a*], Taufik Hidayat[a], Dicky Wahyudi[a]
[a] Prodi Teknik Komputer, Fakultas Teknik, Universitas Serambi Mekkah, Banda Aceh, Indonesia
*e-mail *Corresponding Author: yeniyanti@serambimekkah.ac.id*

***Abstract*— Wireless Sensor Networks (WSN) have attracted the attention of researchers in recent years. WSN , is increasingly using it in various fields. Even though the use of WSNs is becoming more widespread, they are often vulnerable to security attacks. Therefore, it is important to have a strong security system that can provide users with a sense of security and comfort in sending data via WSN. Sending data via WSN also carries significant security risks, especially when the data sent is related to the sender's location. Therefore, this research aims to analyze the scalability of the security system in sending data via WSN using the LSP routing technique. The main focus of this research is protecting data source location information in the context of WSN using LSP Routing techniques. In the tests carried out in this research, a sinkhole attack was used which aims to detect nodes. The research results show that the data transmission rate from the node to the CH increases by 50%, 75%, and 90% in each cycle when the security system is implemented. However, only around 25% and 50% of node attacks in the data transmission process are successfully detected by the sinkhole. The impact of such attacks is felt on the nodes operating in the network, with approximately 95% of nodes eventually going down at the end of the cycle when no security systems are in place. However, when a security system is implemented, only about 60% of nodes fail to send data to their destination.**

***Index Terms*— Wireless Sensor Networks, Data Security , Sinkhole Attack, LSP Routing techniques**
.

***Abstrak*—- Jaringan Sensor Nirkabel (JSN) telah menarik perhatian para peneliti dalam beberapa tahun terakhir. JSN, yang secara real-time mengirimkan pesan yang telah diimplementasikan menggunakan jaringan komputer, semakin meningkatkan jumlah penggunaannya dalam berbagai bidang. Meskipun penggunaan JSN semakin meluas, JSN sering kali rentan terhadap serangan keamanan. Hal ini terutama disebabkan oleh keterbatasan daya komputasi dan daya baterai yang dimiliki oleh sensor-sensor dalam jaringan ini. Oleh karena itu, penting untuk memiliki sistem keamanan yang kuat yang dapat memberikan rasa aman dan kenyamanan pengguna dalam mengirimkan data melalui JSN. Pengiriman data melalui JSN juga membawa risiko keamanan yang signifikan, terutama ketika data yang dikirimkan terkait dengan lokasi pengirim. Oleh karena itu, penelitian ini bertujuan untuk menganalisis skalabilitas sistem keamanan dalam pengiriman data melalui JSN dengan menggunakan teknik routing LSP. Fokus utama dari penelitian ini adalah melindungi informasi lokasi sumber data dalam konteks jaringan sensor nirkabel yang menggunakan teknik Routing LSP. Dalam pengujian yang dilakukan dalam penelitian ini, digunakan serangan sinkhole yang bertujuan untuk mendeteksi node dalam JSN. Hasil penelitian menunjukkan bahwa tingkat transmisi data dari node ke CH mengalami peningkatan sebesar 50%, 75%, dan 90% dalam setiap siklus ketika sistem keamanan diterapkan. Namun, hanya sekitar 25% dan 50% dari serangan node dalam proses pengiriman data yang berhasil dideteksi oleh sinkhole. Dampak dari serangan tersebut terasa pada node yang beroperasi dalam jaringan, dengan sekitar 95% node yang akhirnya mati pada akhir siklus ketika tidak ada sistem keamanan yang diterapkan. Namun, ketika sistem keamanan diterapkan, hanya sekitar 60% node yang gagal dalam mengirimkan data ke tujuan**

***Kata Kunci*— Jaringan Sensor Nirkabel ,Keamanan Data,Serangan Sinkhole,Teknik Perutean**

I. PENDAHULUAN

Jaringan Sensor Nirkabel (JSN) telah menjadi pusat perhatian bagi peneliti dalam beberapa tahun terakhir ini dan teknologi komunikasi nirkabel yang berkembang dan menjanjikan digunakan didunia ini. WSN yang secara *real time* dalam melakukan proses pengiriman pesan disetiap aplikasi yang telah diterapkan menggunakan jaringan komputer [1]. Meningkatnya penggunaan jaringan sensor nirkabel (JSN) dalam berbagai aplikasi di berbagai bidang, seperti pemantauan lingkungan, pertanian, kesehatan, dan keamanan Penggunaan JSNmemberikan kemudahan dan efisiensi dalam mengumpulkan data dari sensor

Received October 03, 2023; Revised August, 2024; Accepted August 30, 2024

yang tersebar di area yang luas. JSN juga memiliki beberapa permasalahan, salah satunya adalah keamanan data yang dikirim melalui jaringan sensor [3].

Jaringan Sensor Nirkabel sering kali rentan terhadap serangan keamanan, terutama karena sensor yang digunakan dalam jaringan ini biasanya memiliki keterbatasan daya komputasi dan daya baterai [4]. Selain itu, informasi yang dikirimkan oleh sensor seringkali bersifat rahasia, seperti informasi medis pada aplikasi kesehatan atau informasi industri pada aplikasi manufaktur. Salah satu teknik yang digunakan untuk meningkatkan keamanan data pada JSN adalah teknik enkripsi. Teknologi blockchain untuk meningkatkan keamanan dan privasi data pada jaringan sensor network. Metode ini memungkinkan data yang dikirimkan oleh sensor dienkripsi dan disimpan secara aman pada blockchain, sehingga data tersebut tidak dapat dimanipulasi atau diubah oleh pihak yang tidak berwenang [5]. Kemudian oleh penelitian yang sama [6] ditahun 2021 melakukan penelitian dengan menggunakanteknik deteksi intrusi untuk mendeteksi serangan pada jaringan sensor network. Metode ini memanfaatkan teknik pembelajaran mesin untuk mengidentifikasi pola yang mencurigakan pada data sensor dan memperingatkan pengguna jika terdapat serangan yang terdeteksi [7]. Pada Tahun 2022 penelitian [8] menggunakan teknik pengenkripsian data untuk melindungi keamanan data pada jaringan sensor network. Metode ini memanfaatkan algoritma kriptografi untuk mengenkripsi data sebelum dikirimkan pada jaringan, sehingga data tersebut tidak dapat diakses oleh pihak yang tidak berwenang. Begitu juga penelitian oleh [9] menggunakan teknik kriptografi ringan untuk melindungi privasi data pada jaringan sensor network. Metode ini memanfaatkan algoritma kriptografi yang lebih ringan dan efisien dalam melindungi data pada jaringan sensor network. Namun, teknik enkripsi dapat meningkatkan konsumsi energi dan memperpendek umur baterai pada sensor [10]. Oleh karena itu, diperlukan pendekatan baru untuk meningkatkan keamanan pada JSN tanpa mengorbankan konsumsi energi dan umur baterai. Karena ketika JSN tersebut diterapkan dalam lingkungan area cakupan yang luas tanpa adanya pengawasan dan saluran nirkabel yang terbuka dengan sumber daya energi yang hanya di suplay oleh baterai mengakibatkan menjadi sangat rentan terhadap berbagai serangan yang berbahaya seperti pengungkapan Location Source Privacy [11]. Untuk melindungi privasi lokasi pengiriman data dari serangan yang digunakan oleh penyerang dengan memberikan keamanan terhadap lokasi dan membuat penyerang tidak dapat mengetahui lokasi sumber [11].

Deteksi intrusi telah menjadi topik penelitian aktif untuk jaringan nirkabel, khususnya jaringan ad hoc nirkabel [12]. Namun jaringan sensor berbeda dengan jaringan ad hoc. *Node* yang terlibat dalam WSN sebagian besar identik dalam hal perangkat keras dan dirancang dengan harga yang sangat murah untuk penerapan dalam jumlah besar [13]. *Node* ini biasanya memiliki sumber daya yang lebih terbatas dibandingkan kebanyakan *node ad hoc*, dengan memori dan daya komputasi yang lebih sedikit untuk mengurangi biaya dan memperpanjang masa pakai baterai. Untuk jaringan sensor, beberapa protokol aman atau perutean geografis yang ada tahan terhadap serangan *sinkhole* yang melakukan routing hanya informasi dan interaksi lokal tanpa inisialisasi dari base station. Namun, banyak protokol perutean yang ada, terutama yang berbasis pada pesan rute, sangat rentan terhadap serangan *wormhole*[13].

Mengingat lawan yang lebih kuat, Wang dkk. Protokol Perlindungan Privasi Lokasi Sumber (PRLA) berbasis Angular, di mana konsep area visibilitas pertama kali diusulkan dan mendefinisikan jalur melalui area tampilan selama perutean virtual, yang dikenal sebagai jalur kesalahan dan RAPFPR keduanya menjamin privasi lokasi sumber, namun tidak memperhitungkan pengaruh wilayah yang terlihat. PRLA Protokol menghitung probabilitas maju berdasarkan sudut defleksi node sensor untuk mengurangi kemungkinan perutean melalui wilayah yang terlihat. Karena kekurangan program PRLA memberikan dua algoritma yang menggunakan node virtual untuk melindungi lokasi sumber [14]. Keamanan dengan menggunakan overflow terbatas, node yang jauh dari sumber dipilih sebagai node virtual, sehingga meningkatkan lokalisasi secara signifikan. Keragaman node virtual dalam protokol melindungi privasi lokasi sumber di jaringan sensor nirkabel menggunakan overflow terbatas berbasis sumber (PUSBRF).Dibandingkan dengan protokol PUUSBRF, EPUSBRF menghindari area yang terlihat selama perutean dan memperpanjang waktu keamanan jaringan. Penelitian oleh Kong Xiangxue dkk. mengusulkan protokol perutean yang menjaga privasi lokasi sumber berdasarkan Random Virtual Loop (PRVR), yang memperluas jalur routing ke rentang virtual node sumber, sehingga menyulitkan musuh untuk melakukan

backtracking yang efektif. Berbeda dengan Serangan aktif hingga lawan tipe ini hanya dapat melancarkan serangan pasif lokal[15].

Penelitian akan dilakukan analisis skabilitas sistem keamana data menggunakan jaringan sensor nirkabel menggunakan metode LSP. *State Of The Art* dalam penelitian ini adalah jaringan sensor *network* menjadi sangat penting untuk mengumpulkan dan mentransmisikan data dari lingkungan sekitar, namun keamanan data menjadi masalah besar pada jaringan sensor *network*. Beberapa teknik telah dikembangkan untuk meningkatkan keamanan jaringan sensor, namun kebanyakan teknik tersebut tidak mampu melindungi lokasi pengirim data, yang dapat memberikan informasi penting tentang lokasi sumber data

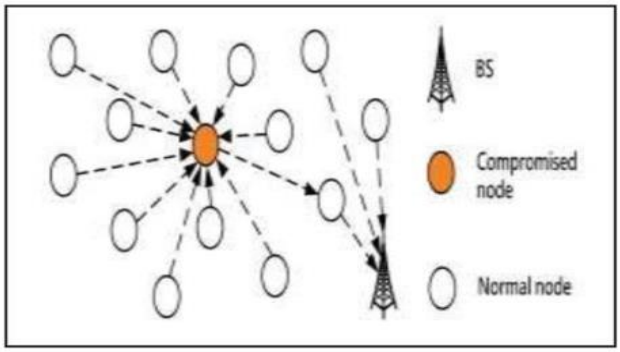
II. METODE PENELITIAN

A. Model Jaringan

Model jaringan dalam penelitian ini mengasumsikan bahwa banyak node dikerahkan secara acak untuk melacak lokasi target. Setiap node mampu melakukan komunikasi, komputasi, dan penginderaan. Semua node dalam jaringan bertenaga baterai dan beroperasi tanpa pengawasan [2]. Oleh karena itu, efisiensi energi merupakan pertimbangan desain yang paling penting baik untuk perangkat lunak maupun perangkat keras. Pada WSN hanya terdapat satu base station sebagai pintu gerbang ke jaringan eksternal. Semua node di WSN bekerja secara terkoordinasi untuk mendeteksi keberadaan target. Metode pelacakan yang dapat digunakan untuk mendeteksi target, asalkan menghemat energi. Ketika target terdeteksi, node sumber mengirimkan paket ke stasiun pangkalan untuk melaporkan informasi target. Node sumber melapor ke stasiun pangkalan untuk jangka waktu tertentu hingga target bergerak di luar radius deteksi. Node lain di WSN akan tertidur kecuali diinstruksikan untuk meneruskan paket dari node sumber ke stasiun pangkalan.

B. Model Serangan

Model Serangan dalam penelitian ini diasumsikan jaringan sensor yang terdiri dari satu BS. Node jaringan tersebar secara acak di area tertentu. Lokasi node bersifat statis, artinya tidak berubah setelah penerapan dan semua node diidentifikasi secara unik. Node sensor terus mengumpulkan dan mengirim data ke stasiun pangkalan dengan meneruskan paket dari node ke BS. Node tidak mengandung perangkat keras anti kerusakan sehingga dapat disusupi. Stasiun pangkalan menyimpan catatan semua ID node. Jika sebuah node diganti atau didistribusikan ulang yang akan diperbarui. Penyerang melakukan serangan sinkhole dengan menyusup ke satu atau lebih node sah yang menyediakan rute berkualitas tinggi ke stasiun pangkalan. Hanya stasiun pangkalan yang mempertahankan pandangan global lokasi node melalui mekanisme lokalisasi [12]. Otentikasi berkala untuk semua node di jaringan. Hal ini mencegah node mengidentifikasi stasiun pangkalan secara salah.



Gambar 1. Sistem Serangan Sinkhole

C. Model Location Source Privacy

Teknik perutean lebar sama: Teknik ini diasumsikan paket akan diteruskan ke node tetangga ini memiliki ke lebar perutean jarak yang samake BS. Dapat dikakatan bahwa ada hanya mungkin dalam kasus implementasi node jarang, tetangga ini mungkin tidak tersedia. Dan memiliki jaringan padat. Oleh karena

itu, setiap node memiliki jumlah yang cukup ke tetangga di setiap memiliki jarak perutean yang sama. Paket mungkin memakan waktu searah jarum jam atau berlawanan arah jarum jam dan pindah ke sudut b (dalam derajat) atau hop by hop arah yang dipilih, ketika jumlah hop menjadi 0 ke node tertentu, lalu paket diteruskan ke BS. SN dapat mengatur minimum bernilai 0 untuk privasi lebih. Selanjutanya menggunakan sequence number dalam jaringan.

$$\text{Threshold} = \frac{1}{N} \sum_{k-1}^{N} X_k$$

Persamaan tersebut cara untuk menghitung rata-rata sequence number dalam jaringan dimana N adalah banyaknya node dalam jaringan, dan X_k adalah jumlah dari sequence number dalam jaringan (Salve et al., 2015).

III. HASIL DAN PEMBAHASAN

A. Sistem Pengujian

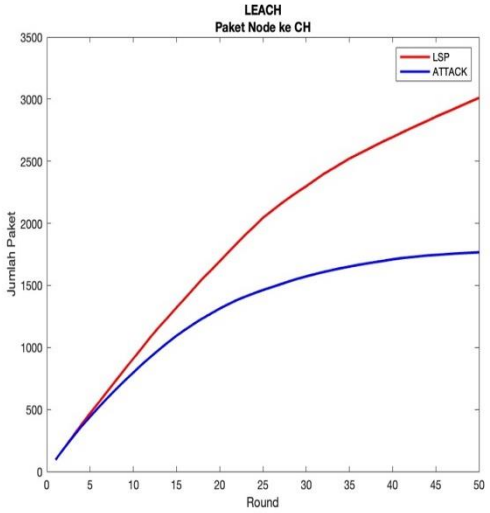
Pada pengujian ini, dilakukan variasi jumlah sensing dalam satu siklus untuk setiap node padajaringan sehingga diperoleh jumlah sensing optimal untuk menghasilkan waktu hidup jaringan yang optimal. Pengujian dilakukan pada sistem jaringan sensor nirkabel yang terdiri dari 100 node, 6 Cluster (C), dan Setiap node memiliki Energi awal 2 Joule/bit, paket 4000 kb. Pengujian algoritme LEACH dilakukan dengan menjalankan sistem jaringan sensor nirkabel, Membentuk Cluster Head (CH), penentuan BS, area yang digunaka 150 x 100 meter, Setiap Node akan mengirimkan pesan ke cluster head kemudian akan dilanjutkan proses pengiriman ke Bs, Namun akan ada proses serangan sinkhole mendeteksi rute proses transmisi pake dari lokasi node sumber ke Base Statiun. Teknik perutean yang memiliki lebar jarak yang sama dengan jarak perutean tetangga node, akan melakukan proses sistem keamanan dengan menggunakan batas ambang yang berbeda ketika dilakukan proses tersebut. Pengujian dilakukan pada satu ruangan dengan jarak setiap sensor node ke sink node sekitar 1meter dan jarak antar node dalam satu klaster sekitar 0,2 meter. Penggunaan jarak antar node dibuat cukup dekat agar data yang ditransmisikan pada jaringan selalu sampai ke node tujuan. Penggunaan jarak antar node yang terlalu jauh dapat menyebabkan adanya data yang tidak sampai ke node tujuan sehingga menyebabkan sistem berhenti.

B. Skalibilitas Sistem Keamanan Data

Analisis skalabilitas dalam konteks jaringan sensor nirkabel adalah proses evaluasi kemampuan jaringan untuk tetap efektif dan efisien saat jumlah node sensor atau kompleksitas jaringan meningkat. Penelitian ini membatasi analisis skalabilitas JSN pada Performa Jaringan: Bagaimana kinerja jaringan berubah seiring dengan peningkatan jumlah node sensor atau tingkat lalu lintas data?

- **Transmisi Paket Node Ke CH**

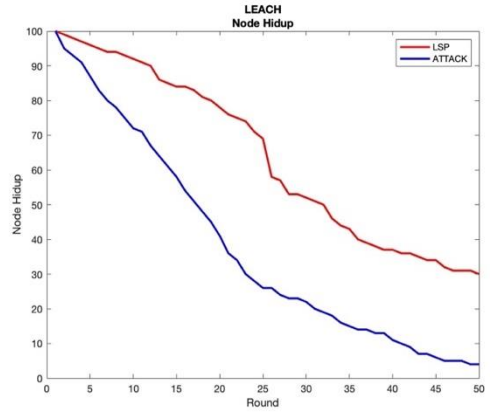
Dalam penelitian ini proses transmisi Paket Node ke CH pada jaringan sensor nirkabel, Protokol LEACH (Low-Energy Adaptive Clustering Hierarchy) yang dapat menghemat energi dalam jaringan sensor nirkabel. Node sensor mengumpulkan data dari lingkungan atau sensorannya sendiri. Node sensor memilih atau ditentukan untuk menjadi anggota kluster tertentu dengan memilih CH. lalu Node sensor yang ingin mengirimkan paket mengirimkannya ke CH dalam kluster yang sesuai dalam putaran jaringan namun ada masalah yang terjadi terjadi peningkatan paket data yang dikumpulkan oleh node- node sensor ke CH sehingga akan menguras membutuhkan suatu energy yang meningkat dan tidak tersampai pengiriman pake ke CH dengan benar, terlihat pada Gambar 3. Setiap putaran jaringan node 100 di setiap putaran 1 s/d 50 putaran terjadi sebesar bernilai 25%,dan sebesar bernilai 50% yang mempunyai peluang tidak sukses sampai ke CH. Akan tetapi, ketika diberikan sistem keamanan menggunakan Teknik perutean dengan jarak yang sama ketika Energy awal node $\geq$ 2 joule yang telah ditetapkan dan batas ambang sebesar 2, terdeteksi bahwa node tersebut melebihi energy dan batas ambang maka node tersebut akan di hentikan dan node lain akan di transmisikan ke node tetangga dengan perutean jarak yang sama, agar pengiriman node ke CH terjalin dengan sukses terlihat pada gambar 3. Terjadi peningkatan ketika diberikan keamanan dalam setiap putaran pengiriman terjadi peningkatan sebesar 50%, 75% dan 95% paket sukses terkirim ke CH.



Gambar 2. Hasil Transmisi Paket Node Ke CH

- **Analisis Node Hidup**

Node-node dalam jaringan sensor nirkabel bertugas untuk melakukan proses sensor dalam membentuk suatu kelompok (cluster) dan node membentuk cluster head yang bertugas mengumpulkan semua paket lalu mentransmisikan ke node tujuan disetiap bidang aplikasi salah satunya monitoring dalam bidang militer. Namun node adalah sasaran dalam setiap serangan baik serangan lokal, serangal pasif, serangan global. Penelitian ini berfokus pada serangan sinkhole. Serangan Sinkhole mendeteksi, memantau aktivitas node dalam jaringan sensor Nirkabel. Dalam semua simulasi Algoritma pendeteksi serangan sinkhole memiliki rate yang lebih tinggi. tingkat kelebihan rute, hal ini disebabkan oleh sifat algoritma pendeteksian yang dipaksa untuk mengulangi penemuan rute ketika paket respons terdeteksi sebagai paket berbahaya. Hal ini menyebabkan sumber mengirimkan ulang RREQ dan melakukan penemuan rute awal, sehingga lebih banyak siaran yang dikirim, yang pada gilirannya meningkatkan beban perutean pada jaringan terlihat Gambar 4. Hasil node hidup dalam jaringan ketika terjadinya serangan dalam setiap putaran sebanyak 50 putaran peningkatan sangat besar menunjuh 95% diakhir putaran ke 50 sudah hampir mendekati node semuanya mati sehingga tidak sampai ketujuan proses pengirimannya. Namun ketika diberikan keamanan menggunakan Teknik perutean jarak yang sama terjadi node yang hidup 60% menunjuh ke putaran 50 node yang mati atau node yang dikirimkan ketujuan.



Gambar 3. Node Hidup pada Jaringan Sensor Network.

IV. KESIMPULAN

Dari hasil analisi skalibilitas sistem keamanan data pada jaringan sensor nirkabel menggunakan sequence number yang berbeda pada routing protokol LEACH dan location source privacy dengan

menggunakan Teknik perutean jarak yang sama. Mengimplementasikan algoritma deteksi serangan *sinkhole* dengan memodifikasi routing protokol LEACH untuk mendeteksi paket berbahaya ketika pemrosesan transmisi data node ke CH dan menganalisi lifetime jaringan dilihat dari segi node hidup dalam jaringan. Proses pengujian tersebut berhasil dilakukan. Terdapat tingkat transmisi data node ke CH ketika diberikan keamanan naik peningkatan 50%, 75% dan 90% dalam setiap putaran. Hanya 25% dan 50 % terjadi serangan node proses pengiriman data terdekteksi oleh sinkhole. Sehingga berdampak pada node yang hidup di dalam jaringan sebesar 95 % diakhir putaran 50 node menujuh node mati semuanya, namun ketika diberikan sistem keamanan hanya 60% menujuh node gagal mengirimkan ke tujuan. Namun di sisi lain, algoritma deteksi ini memiliki efek samping berupa peningkatan beban routing dalam jaringan.

UCAPAN TERIMA KASIH

Ucapan Terima Kasih Terima kasih kepada Ristek Dikti yang telah memberikan pendanaan sehingga penelitian ini berjalan dengan
lancar

DAFTAR RUJUKAN

[1] Mohamed RE, Saleh AI, Abdelrazzak M, Samra AS. Survey on Wireless Sensor Network Applications and Energy Efficient Routing Protocols. Wirel. Pers. Commun. 2018;101(2):1019–55. doi: 10.1007/s11277-018-5747-9.
[2] Boubiche A, Benferhat S, Drias H. Location source privacy in wireless sensor networks: A survey. J Ambient Intell Humaniz Comput. 2020;11(2):757-776. doi: 10.1007/s12652-019-01301-4.
[3] Wang Y, Shu L, Zhang Z, Mao J. Research on wireless sensor network security technology based on layered architecture. J Phys Conf Ser. 2019;1174(1):012018. doi: 10.1088/1742-6596/1174/1/012018.
[4] Zhang H, Zhang J, Chen H. A Traffic Observation-Based Method for Denial-of- Service Attacks Detection in Wireless Sensor Networks. IEEE Access. 2019;7:75992-76000. doi: 10.1109/ACCESS.2019.2927562.
[5] Yang J, Zhu H, Sun Z, Zhang Y. Secure and privacy-preserving data transmission in wireless sensor networks based on blockchain. IEEE Internet of Things J. 2020;7(11):11156-11167. doi: 10.1109/JIOT.2020.3014331.
[6] Li X, Wang D, Li Y. An intrusion detection system for wireless sensor networks based on machine learning. IEEE Access. 2021;9:28134-28144. doi: 10.1109/ACCESS.2021.3060231.
[7] Wang Y, Chen X, Li L, Wu Y. Lightweight cryptography-based secure data transmission in wireless sensor networks. Sensors. 2021;21(5):1729. doi: 10.3390/s21051729.
[8] C, Wang J, Chen J. Data encryption for secure data transmission in wireless sensor networks. Int J Distrib Sensor Netw. 2022;18(1):15501447211007999. doi: 10.1177/15501447211007999.
[9] Arjunan S, Pothula S. A survey on unequal clustering protocols in wireless sensor networks. Journal of King Saud University-Computer and Information Sciences. 2019 Jul 1;31(3):304-17.
[10] Manjula R, Datta R. A novel source location privacy preservation technique to achieve enhanced privacy and network lifetime in WSNs. Pervasive and Mobile Computing. 2018 Feb 1;44:58-73.
[11] Wang WP, Chen L, Wang JX. A source-location privacy protocol in WSN based on locational angle. In: International Conference on Communications. IEEE; 2008:1630-1634.
[12] Lu Z,Wen Y. Credit routing for source-location privacy protection in wireless sensor networks. In: International Conference onMobile Ad-Hoc and Sensor Systems (MASS 2012). 9th ed. IEEE; 2012:164-172.
[13] Zhao Z, Liu Y, Zhang F, Zhou J, Zhang P. Reseach on source location privacy routing based on angle and probability in wireless sensor networks.
[14] *Chen J, Fang B, Yin L, Su S. Source location privacy protection protocol based on limited ooding of source nodes in sensor networks. Chin J Comput. 2010(9):1736-1747*
[15] *Kong X, Yuan S, Chen M. Source location privacy protection routing protocol based on virtual ring. SensMicrosyst. 2018(1):66-69.*