An Assessment of Data Transmission Reliability in Mobile Wireless Sensor Networks

[1]J Xin Ge and [2]Yuan Xue
[1,2]School of Chemistry and Chemical Engineering, Nanjing University, Jiangsu, China, 210093.
[1]ktxin@nju.edu.cn, [2]yuanxuenu93@gmail.com

Correspondence should be addressed to J Xin Ge : ktxin@nju.edu.cn

Article Info
Journal of Computing and Natural Science (http://anapub.co.ke/journals/jcns/jcns.html)
Doi: https://doi.org/10.53759/181X/JCNS202303013
Received 10 September 2022; Revised from 15 November 2022; Accepted 25 January 2023.
Available online 05 July 2023.

Published by AnaPub Publications

Abstract – Despite the significant improvements made to the internet in recent years, fewer individuals are utilizing it on a regular basis. Although there are many avenues via which people may share and gather information online, online social networks have quickly risen to prominence as a primary means of dissemination. Many of the previous researches have issues, such as clumsy computing processes and poor efficiency, while the sheer volume of nodes and interactions in social networks provide significant challenges for privacy protection. In this article, we use the dynamic setting of Social Networking Sites (SNS) as a study context, zeroing in on the critical concerns of mobile Wireless Sensor Networks (WSNs) dependability in terms of scalability, information simplicity, and delay tolerance. Various issues of dependability are discussed, including but not limited to: topological reliability evaluation techniques in engineering field applications, the implications of mobile maximization of cellular WSNs on the efficiency of data collection and reliability of network, dependable information transmission reliant of the approaches of smart learning, data fusion, and the bionic optimization of swarm intelligence.

Keywords – Wireless Sensor Networks (WSNs)**,** Social Networking Sites (SNS), Social Network Optimization (SNO).

I. INTRODUCTION

The primary use of sensors is to initiate real-time surveillance of complex regions, with the goal of understanding data attributes of the regions. Sensors are crucial in many different areas, including the environment, food production, and manufacturing. Wireless Sensor Networks (WSNs) nodes have several desirable features, including a big number, a vast range, low energy requirements, a complicated environment, and network stability. These features make sensors vulnerable to noise and interference from their surroundings, as well as from network issues and failed nodes. The inaccuracy of sensor data may have devastating effects on engineering projects and military operations. For this reason, investigating the robustness and flexibility of data collected by sensor nodes under perturbation circumstances is of paramount importance.

Several researchers have proposed various solutions to the issue of WSN data dependability. A novel distributed and adaptive trust assessment approach for Mobile Adhoc Network (MANET) was developed by [1] based on an examination of sensor failures. Inter-node communications, energy, and recommended algorithms are used to directly compute trust. Furthermore, the indirect trust degree is computed by taking into account the distances of propagation relate to the trust degree, which significantly enhances the capacity to differentiate malicious nodes. In order to evaluate WSNs dependability evaluation from exterior intrusion, and interior defects, [2] offered an applicable evaluation methodology that depended on the modular BRB (Belief Bule Base); [3]suggested a method for detecting different series of data on the sensor node, which have the capacity to evaluate the different dimension between typical intervals and computed test dataset in order to determine the causal agent of the faults; Using the aforementioned technique, we may examine several

factors related to the identification of rogue nodes and sensor failures. When data undergoes dramatic change, these techniques perform better in terms of analysis. Nevertheless, good findings are not attainable for minor data variations.

Energy-balanced routing based on advanced perception variables was introduced by [4] with the goal of increasing the trustworthiness of data transmission. The transmissions node is chosen by this technique by taking into account both the path's relative importance and the forward power density. It is simple to introduce issues of poor network throughput and dependability by investigating the way of picking cluster heads in conventional clustering methods. Introducing a novel passive multi-hop clustering technique, Bazar, Sharma, and the Department of Electronics and Communication [5] posited. By examining the benefits of compressed sensing technologies in WSNs information aggregation, [6] suggested a useful data clustering approach based on compressed sensing. In order to address the problem of data loss and abnormalities, [7] introduced a novel approach of tensile heterogeneous data loss assimilation and estimation based on the fuzzy neural network. In order to prevent data packet loss in the network, [8] suggested a dependable transmission scheme with congestion management system called cache-aware RT-CaCC. The impact and interplay of node variability on routing choices was studied by [9]. These made WSN more trustworthy in several use cases. The technique enhances the sensor's dependability by addressing issues like maximizing the efficiency of data transfer. Data transmission errors and distortions are also mitigated by these techniques. The outcome is not satisfactory, however, when looking at the impact on sensor data.

In this article, we propose to investigate mobile WSNs reliability concerns and undertake a systematic and deep research in cellular WSNs stability evaluation and modification by employing smart optimization methodologies and swarm intelligent regenerative optimization approaches, to effectively address cellular WSNs node technologies and networking failures forecast methodologies, network dependability assessment approaches for forest, mesh, and other topologies. The rest of the paper is arranged as follows: Section II provides a background analysis of the research. Section III provides a detailed analysis of previous literature sources. Section IV focuses on data reliability research of WSN for SNO, where details of data reliability study of WSNs and data transfer reliability assessment of wireless sensors, are provided. More details regarding this research are provided in Section V. Lastly, Section VI provides a summary of the discussion presented in this paper.

II. BACKGROUND ANALYSIS

The increased advancement of the Internet and computing power has led to the emergence of social networks, which have altered the conventional means by which humans interact with one another. Today, many people rely on social media for everything from their primary source of news and information to their primary source of entertainment, commerce, and education. In-depth messaging, content sharing, and other forms of interaction with friends are all made possible through social networks. In the conditions of rapidly developing network technology, social networks have spread across people's personal and professional life due to their widespread availability and ease of use. At the same time, as the network expands rapidly, people are starting to worry about their privacy online. With a wide variety of sensor nodes deployed across the monitored region, Wireless Sensor Networks (WSNs) are intelligent networks capable of transmitting information as a proximity multi-hop cooperation, collaboration, and self-organization among different nodes.

The network integrates data sensing, embedded computing, wireless communications, and distributed data processing; node pre-processing the needed information and data before transferring it to the aggregation node in a type of multi-hop self-management; the aggregation node then transfers the gathered data to the surveillance station, where it is subjected to the required processing action before being integrated to the makers of decisions and sent. During the assessment phase, the physical capacities, and connections are recorded to traffic pathways, providing a simple reflection of the network's performance deterioration. For assessing the system performance dependability, the likelihood that the data accessed from the source gets to the destination points within the desired timeframe is applied as a timely dependability of this system. To measure network congestion, we look at the rate at which the routing buffer fills up; we may also gauge the network's overall dependability by contrasting the different packets obtained with the number sent, or by looking at the ratio between the two.

Users' identities, login details, lists of friends, material posted on the social networking platform, and the spread of data all fall under the umbrella of privacy information in social networking systems. When people’s private information is shared across social media platforms without their knowledge or consent, there is a potential for data leakage and for users without appropriate permissions or malevolent intent to access the information published by data owners. Today's social networking services have a significant issue in figuring out how to balance data publication with privacy-preserving mechanisms and stop the leaking of sensitive user information. WSNs may be broken down into subcategories depending on their dependability, which is a key metric for gauging overall network efficacy. Reliability evaluation may be broken down in a number of ways: according to the methodologies used for analysis and computation, into connectivity-based dependability, and coverage-based reliability; from the basis of applications requirement into conditional probabilities, block diagram approach, Markov chain, binary decision diagram, Monte Carlo simulation approach, fault tree evaluation, etc.

In this article, we propose to investigate mobile WSNs reliability issues and undertakea critical and systematic review in cellular WSNs dependability evaluation and optimization by employing swarm intelligent bionic optimization approach, and smart optimization algorithms, in order to address the hardware in cellular WSNs nodes and networking failure forecasting approaches, network dependability evaluation approaches for tree, mesh and different topologies.

III. LITERATURE REVIEW

Kim and Choi [10] examined how sensor nodes perform in a chaotic setting. The degree to which sensor nodes can adjust to a variety of disturbance settings varies. In other words, if the impact of interruption on the input is too severe, the sensor networks often cannot operate in this setting. Also, sensor data integrity is compromised. As a result, modifications must be made to other aspects of WSN. To assess sensor node adaptation to disturbance environment, the formula is $S[(\Delta z(t)] = \gamma[y(t), \Delta z(t) Y(t)]$ where $S[(\Delta z(t)]$signifies the factor of disturbance of the indicator dataset at the moment stimulated by the $\Delta z(t)$variable of disturbance. It could be utilized to assess and measure the WSN node adaptability within a distributed ecosystem. The entire assessment process is illustrated in **Fig 1**.

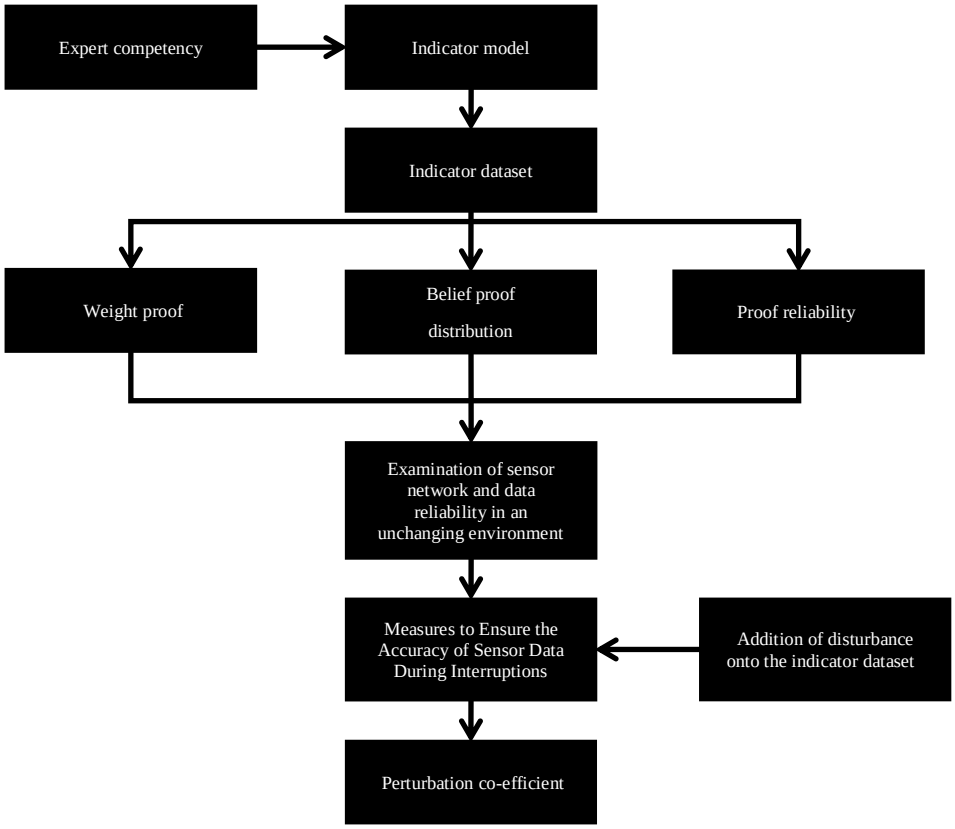

Fig 1. Perturbation-Based Data Reliability Evaluation at Sensor Nodes

To create an online community of individuals who have same interests, histories, and activities, one might make use of a Social Networking Sites (SNS). Those who utilize a social networking service may meet new people and broaden their social horizons. One of the most important aspects of an SNS is the ability for its users to share information about themselves, such as their likes, dislikes, activities, and so on. Social Networking Sites (SNS) like Twitter and Facebook have risen in popularity in recent years to become preferred means of communication for billions of internet users worldwide. These platforms allow users to keep in touch with their loved ones and coworkers by combining a social networking profile with a messaging system. The popularity of these platforms stems from the ease with which members can manage their accounts, communicate with one another, and peruse the information of other members. SNSs have the potential to greatly improve users' lives by lowering financial and geographic barriers.

Moreover, they may be used to accomplish objectives in the areas of employment exploration, leisure, and learning. The widespread usage of SNSs, however, exposes users to substantial danger. SNSs are attractive to cybercriminals due to the wealth of personally identifiable information (PII) that their users voluntarily provide. Spam, malware, social bots, and identity theft are just some of the assaults that may be carried out with the help of an SNS once the attackers have obtained access to users' private information. Attackers may also perform online crimes like bank fraud by analyzing the user's personal data, which includes sensitive information like bank account information. Gunderson et al. [11] examine the spectrum of SNS assaults and finds that anything from account takeovers and fraud to impersonation attacks and virus dissemination is possible. The company's networks are vulnerable to sophisticated attacks. **Fig 1** depicts the basic idea behind an SNS.

SNSs like Facebook and others are increasingly emphasizing the production and sharing of video, music, and other forms of audiovisual material. According to data compiled by ZDM (Zephoria Digital Marketing), 136,000 novel images are transferred to Facebook in each minute. As per the statistics compiled by SocialMediaToday, the average number of times a video is seen and shared on Facebook is on the rise. Facebook now has over 8 billion daily video views, which is

double the amount observed in 2015. An increase in worries about Facebook's safety has corresponded with the site's meteoric surge in audiovisual material. Intentionally harmful content may be posted to a social networking site in the form of multimedia files. It also makes it easy for an attacker to learn sensitive information about the user, such as the user's identity and location.

Users' security and confidentiality concerns in virtual communities have real-world consequences. Recent years have seen an uptick in research on privacy measures for social networks, while this work lags behind that of industrial networks. Node failure and energy consumption are two of the main topics of study when it comes to WSN reliability. The nodes' random failure is visualized in the research on distributed WSNs for the purpose of determining the WSN's viability. In order to evaluate the reliability of WSNs, Zhang and Y. Li [12] takes into account a network topology in which there is a sensor nodes and Sink nodes. Lu et al. [13] introduce the concept of common cause failure and present a Monte Carlo simulation-oriented technique to analyse the dependability aspect of WSNs. In [14], the Markov model is initially considered as a means of gauging the sensor node dependability. A binary decision graphical method is recommendedfor handling with WSN dependability in common cause failure ecosystem. Prior WSN reliability evaluations make the assumption that sensor nodes are not reliant on one another and do not put into consideration the fundamental correlations of sensor networks; in that case, this assessment is incomplete.

According to Kumar and Wagatsuma [15], the binary decision diagram is changed into a well-ordered bipartite network, which takes into account common causes of failure in a network. In [16], it was proposed that a survey questionnaire be used to tally many metrics, with respondents selected on the basis of their expected differences in privacy-protecting behaviors. They compare survey metrics to two standard privacy safeguards and draw connections between the two sets of metrics. They contend that the metrics are a useful tool for managing the web and might be used to the investigation of privacy indicators on the internet. Avellina, Brankovic, and Piroddi [17] describe how the ALNS heuristic was modified to include an adaptive random selection approach and an algorithm for temporal adjustment to resolve the transportation pathway and enhance the privacy of the transport pathway. By integrating the pathway category, the pathway traffic effect elements prevailing in the real pathway network. Matrenin [18] employ an enhanced ant colony approachto find the best route that suits the demands of passengers. To lessen consumers' wait times and more fairly divide traffic burdens across social network members and the customers they seek, a strategy based on a reverse ant colony approach with an algorithm known as boosted pheromone update is presented by Cheng, Wang, Wei, Liang, and Song [19].

For the situation of combining multiple characteristics and types of characteristics such as uncertainty and deterministic in complex multi-attributes, the subjective and objective weights in each form of attribute of the route are produced using a methodology known as data entropy and subjective allotment, and the dual weights are then examined expansively to compute the path's reach capability, TOP-K pathway query, and optimum pathway selection. It has been suggested by Siddiqi, Shiraishi, and Sait [20] that a generic strategy may be utilized to handle multi-constrained route inquiries in networks by first limiting the non-linear cost functionality to visualize whether the recognized pathway is viable and them reducing the major cost functionality to effectively determine in case there are any other, effective pathways while maintaining Quality of Service (QoS). Difference-based route multiplex selection algorithms (CMT-DPS) are developed in the literature to improve throughput and reduce transmission time. If there is a big enough difference between the routes, the ones with the lower quality won't be chosen to send the data. Path selection algorithms for software-defined networks (SDNs) have been proposed by Nsafoa-Yeboah et al. [21]; these algorithms use dual effect factors oriented on the real Quality of Experience (QoE) to guarantee load balancing and connection quality through real-time acquisition of the state, and dynamic weight adjustment, and they also utilize the ant colony technique to boost the transmission rates.

IV. DATA DEPENDABILITY RESEARCH OF WSN FOR SNO

Data Reliability Study of WSNs

The "single" and "dual" factions of product reliability and quality work refer to the task reliability and basic reliability of wireless connectivity, correspondingly. "Single" indicates that the product design itself serves as a major application of task reliability. "Dual sides" indicates that the product design also acts as the main implementation of basic reliability. According to their respective definitions, the difference between fundamental dependability and task reliability may be broken down as follows: This is because (1) people have various conceptions of time. The task profiling cycle determines the "defined time" included in the idea of mission dependability. General life cycle profiling, which often comprises of many job profiles, establishes the "defined time" in the idea of fundamental dependability. (2) There is a difference in the range of success and failure statistics. As they are not a part of the concept of dependability, failure, which not impact "completion of the work" is ignored in reliability evaluations.

However, when comparing the two, it is crucial to remember that the range of failures within basic reliability dataset is more compared the failures in mission reliability. (3) There are different final impacts on the consumption of products. Fundamental reliability ability has an impact on both the costs of coverage maintainability and the availability of equipment. Mission dependability impacts how well the network's mission-based applications run and is a crucial determinant of whether the product can effectively carry out its mission. The Weibull distribution is also highly popular because its continuous nature closely resembles other distributions and its range of shape parameter values well captures the features of product failure [22].

Mission reliability initially creates mission profiles based on mission descriptions in order to construct separate calculation models. Depending on the range of missions supported by a system, there may be several mission profiles. In contrast, for evaluating a system's minimal minimum dependability, there is only one reliability calculation methodology that is relevant. The theoretical foundations on which the vast majority of earlier studies of network reliability assessment have been built include mathematical analysis techniques grounded in probability theory and graph theory, simulation approaches, which model randomized occurrences, and field experiment approaches based on real-life cases. Connectivity reliability, which classifies networks into passive and active classes oriented on the absence or reliability of particular source nodes, is the first recommended metric for network dependability [23].

The conventional analytical techniques used to determine network connection dependability integrate state enumerations, the subtraction principle, disjoint summation, graph delimitation, and transformation, and factorization. The approaches typically utilize the assumption that there are only two possible states for connections: normal and fault, and those failure probabilities of system's individual connections are not reliant of one another. Factors such as network administrators, resilience design, information management, connection and node dependability, confidentiality, annihilation resistance, and others must be taken into account when developing a reliable network. The likelihood of effectively transferring the needed capacity between two different ends of the connection once maximum capacity for every link has been determined is referred to as capacity reliability [24].

Based on this concept, a variety of computational methods have been proposed. A model oriented on identified conditions, e.g., link and node reliability data (such as dependability), link and node capacitance data, transmission capacity, and network topology requirements, is employed to mitigate the issue of probability that a connectivity path exists for some set of nodes that satisfies particular capacity requests. The synchronous reliability of a network is defined as the likelihood that data transported from the source networks gets to the destination networks within the allotted period. Methods such as calculating the likelihood of route buffer overflows are used to gauge congestion in the network, and the ratio of obtained packets at the receiver end to those sent from the senders' end may be used to demonstrate the network's overall reliability. The three forms of network dependability evaluation illustrated above (capacity reliability, performance reliability, and connectivity reliability) [25] can reflect different requirement of functionalities, network performance and metric ranges, but it is still problematic to determine the complete capacity of the system whereas it is undertaking a specific task.

In reliability engineering, a number of discrete and continuous lifetime distributions are used. The most frequent discrete distributions are binomially, geometrically, and Poisson distributions, whereas the most frequent continuous distributions are exponential, log-normal, Weibull, and normal. The exponential distribution of continual form is by far the most typical and extensively used distribution type for characterizing the dependability of electronic tool. The failure rate is constant throughout time for an exponential distribution. From theonset of reliability evaluations, an exponential distribution has often been the most employed because of its numerous advantages, such as its ease of computation, ease of parameter estimate, and failure rateadditivity. Similar to this, if a system's component failures conform to the exponential distribution, then the system as a whole conforms to the exponential distribution. It is also often used because the continuous Weibull distribution is more comparable to other distributions and because the shape parameter of the Weibull distribution has a range of values that correspond to the product's failure characteristics. Weibull and the exponential distributions, which are often used to describe sensor lifetimes, are the two continuous distributions that we concentrate on in this work.

A star network design creates two-way communications between the Sink (base station), and the sensor nodes, but there is no communication linkage provided between different nodes, making it perfect for researching WSN reliability. Also, the sensor nodes may transmit data directly it its base stations, hence failures may have an instantaneous effect on the WSN's normal operation. All of these advantages are critical for evaluating the level of WSNs dependability. The research on WSNs dependability fruits of start network designs has reference significance for future investigation of different network topologies. As a result of this, WSN dependability research in this research uses star network architecture. While creating a dependable network, several different factors must be taken into consideration, including fault prevention, redundancy design, link trustworthiness, data management, resistance security and destruction.

The following are some essential considerations: This design is redun stylish (1). It necessitates planning the communication lines and backup systems first. Several major devices integrated in the same domain are employed to re-distribute loads, and different routing protocols and many transmission channels are used in the transmission technique. (2) The second one is network security measures. Common network security methods include hot backup standards, dependable routing, proactive security switching modalities, and route binding modalities. Failure-tolerant design (3) or, to put it another way, the network is solidly constructed to go on even if there are errors or malfunctions, although with reduced functionality.

The probability of people's pathways overheating, their likelihood of having numerous shared nodes, the equalization of the system's consumption of energy, the rate of success of data transmissions, and the network's lifetime can all be improved by taking into account the remaining energies of the nearest nodes, the distances of information transfer mission, and load balancing of networks. Fault shielding, fault detection, retry methods, rearrangement, fault diagnosis, reconfiguration, and recovery other tactics are important ones. The fourth is controlling traffic flow. An effective congestion management approach may be put into place by evaluating or performing a dependability simulation test to

identify the network traffic "bottleneck", which may increase network resources and lower user demand. (5) Online maintenance guarantee design ensures that network uptime is maintained and protected with little disruption. Two strategies that are often used are live software updates and hot-plugging hardware. Using simulation enables the supplemental analysis and design of a network's completeness, resistance to destruction, availability, and dependability.

Data Transfer Reliability Assessment of Wireless Sensors Networks for SNO

When it comes to managing and expanding a company's messaging and online presence, Social Network Optimization (SNO) is the way to go. Digital marketing strategies like SNO may be used to reach more consumers, spread the word about new offerings, and even counteract the effects of negative press. In the early days of the Internet, Search Engine Optimization (SEO) was the gold standard of online advertising. Search Engine Optimization (SEO) refers to a process of enhancing the quantity and quality of traffic to a website by making webpages increasingly visible to its users of a specific search engine, especially Google. SNO also aims to provide traffic and enhance awareness of the corporate's website. In recent years, social media marketing has risen to prominence, merging with and even supplanting SEO as the preferred method of boosting a company's online presence, brand awareness, lead generation, and audience engagement. Facebook, Twitter,Snapchat,Instagram, Pinterest, YouTube, and TikTok are just few of the social media sites that may be used for digital advertising.

As a result of SNO, users are typically redirected from the respective sites to the main corporate website. A social media campaign promoting a new car, for instance, can link consumers interested in learning more about the vehicle and scheduling a test drive to the manufacturer's website. If your company uses more than one social media network, there are online tools you may utilize to streamline content creation and distribution. An employee responsible for social media content creation may use these technologies to simultaneously publish to several channels, monitor comments and messages, and connect with the audience. Loomly, PromoRepublic, Agorapulse, Buffer, Hootsuite, and Sprout Social are just a few of the most well-known platforms for social media management.

Data Owners (DOs), Servers for Data Owners (DOs) and Attribute Management Servers (AMSs), Users Gaining Access (UAs), and Social Networking Platforms (SNPs) all make up the PPSSN Model. The DO serves is obliged to encrypt the buddy list of DO, store it, and then questions the list whenever individuals want to gain access to the data, all while maintaining the confidentiality of the information. The AMS transfers a request to the data owner (DO) for a buddy relationship, uses the information given by the DO to identify the buddy relationship, and then gives the private key to the user making the request. Data is sent to users using the social network service platform SNP. V, a user of the social networking site, must acquire the proper permissions before seeing the data on the SNP made available by the DO. Access to the SNP data is granted only once the visitor has successfully authenticated with both DO and AMS and received private keys. Non-DO friends can only see the most recently released data on SNP, and unpermitted individuals are flagged by AMS as the social networking sites are denied access to any data from DO publications.

Multiconstraint route pattern matching, or the process of locating data graph matches that also satisfy pattern graph constraints, is presented in accordance with the diversified complex network framework of social networks. In order to successfully create feedbacks that satisfy the needs of the queries supplied by users, the multi-constraint edge pairing technique is used to each edge in the sequence graph once the individual's query has been processed. To improve connection performance and computational efficiency, it is suggested to use a probability-oriented sampling estimate technique to speed up the implementation of the path matching methodology and to give directions that allow the mapping of search data connection technique. The algorithm might be used for pattern matching in things like social networks based on location, geographical crowdsourcing, and recommendation engines. Forecasts of sequence frequencies using a model of time series are erroneous owing to the juxtaposition of seamless and chaotic sequencing that constitute the cellular connections quality profile as indicated by the signal-to-noise ratio.

In this research, we propose an LSTM-based prediction algorithm for secure and private internal communication based on the principle of trust. This is achieved by incorporating various characteristics of the S/N pattern of wireless connections with the intricate energy grid environment. In this work, we establish a metric for comparing the degree to which two individuals share common attributes by checking to see whether the values of those attributes are same. The result of verifying that these nine qualities are consistent is shown as a 9D (Nine-Dimensional) vector, where the element representing the date of birth matches only the residence and the calendar year, and the birthplace attribute matches the city. For each pair of attributes in this vector, 1 is assigned to the element if the two attributes' contents are same, and 0 otherwise. Taking into consideration a user's name and avatar helps determine the likelihood that two accounts belong to the same person or are associated in some way. This is especially true when the names and avatars of the accounts are extremely similar or identical. Because of the compact nature of avatar files, this research employs the perceptual hashing technique to check for similarities between them.

The most fundamental method used in present research on characteristic inference, link inference, and user identity connection is based on the concept of homogeneity, which states that users' information is similar to that of their surrounding friends, and that the degree of similarity increases with the proximity of friends. The first suggested network reliability index, connectivity reliability, classifies networks as either "active" or "passive" reliant on the absence or existence of particular source points within the networking system. State enumerations, the exclusion rule, disjoint product

summation, graph transformations, factorization and delimitation technique are examples of traditional analytical procedures used to calculate network connection dependability. Links are often assumed to have just two possible states in these algorithms: fault and normal and individual link failure probability are treated as if they were independent. The easiest and most accurate approach to do this is to establish a comparison between the individual's profile attribute data. Using these premises, this paper argues that a malicious intruder could infer target individual's data according to the attribute data of the greatest number of similar users or friends, even if the target individual himself does not reveal this data. Like trustworthiness, intimacy between two people may be self-reflective, asymmetrical, dynamic, complicated, and transferable (not to be elaborated here).

As proximity is determined by the participants' interaction behavior, it is not subjective and is instead objective, and can be evaluated using data mining methods. It is also deteriorating, with the decay rate increasing with the journey length. The following search procedure should be carried out while taking into account the participants' geographical links and social identities: In order to locate the nodes, which fulfill the locations and text data, we must first traverse all of the nodes in the network. Then, we must determine which pathways in the system match the multiple constraints based on various constraints distributed by the users, utilizing one of the nodes as source nodes, and the other one as the destination nodes. However, as the number of nodes increases, the first phase becomes more challenging, rendering the method given above insufficient for addressing the optimum route selection issue for different constraints according to geographical locality and requiring the reduction of the search space according to geographical location and textual data for mitigating the optimum route selection problem for distinct constraints reliant on the social constraints and geographical constraints.

The creation of geographical text indexes for social network users is necessary to facilitate the rapid filtering of geo-location data and text data. The spatial indexing of text may be categorized as text indexing, spatial indexing, or a combination of the two. Text-first and spatial-first classifications are possible because of the relative importance of spatial and text indices.

V. DISCUSSION

There are a total of 2626 records in the dataset utilized for this article, each of which includes the user's pattern number, key textual data and nick name obtained from the tweet, and geographical geographic position information (latitude and longitude). Using a small-world approach, the WS algorithm generates random values for each participant's trust, proximity, and reputation constraints. What exactly happens during the making of anything is as follows: (1) There are N nodes in the network (N is chosen at random; values include 1050, 750, 600, 450, 300, and 150) and m edges (m is chosen at random; values include 1 to 8) connecting each node to its closest m neighbors; (2) When the probability of pr is satisfied, a connection is established between two seemingly unrelated nodes (pr is chosen at random; values include 0.1 to 0.8); and (3) there is a maximum of 1 edge connecting any two nodes. Twenty-four different sub-datasets were synthesized by repeating the steps outlined above. The source users exhibited the bound trustworthiness, accessibility, and notoriety of f 0:05, f 0:001, and f0:3g for the numerical simulations, essentially copying the proximity decay inside social networks.

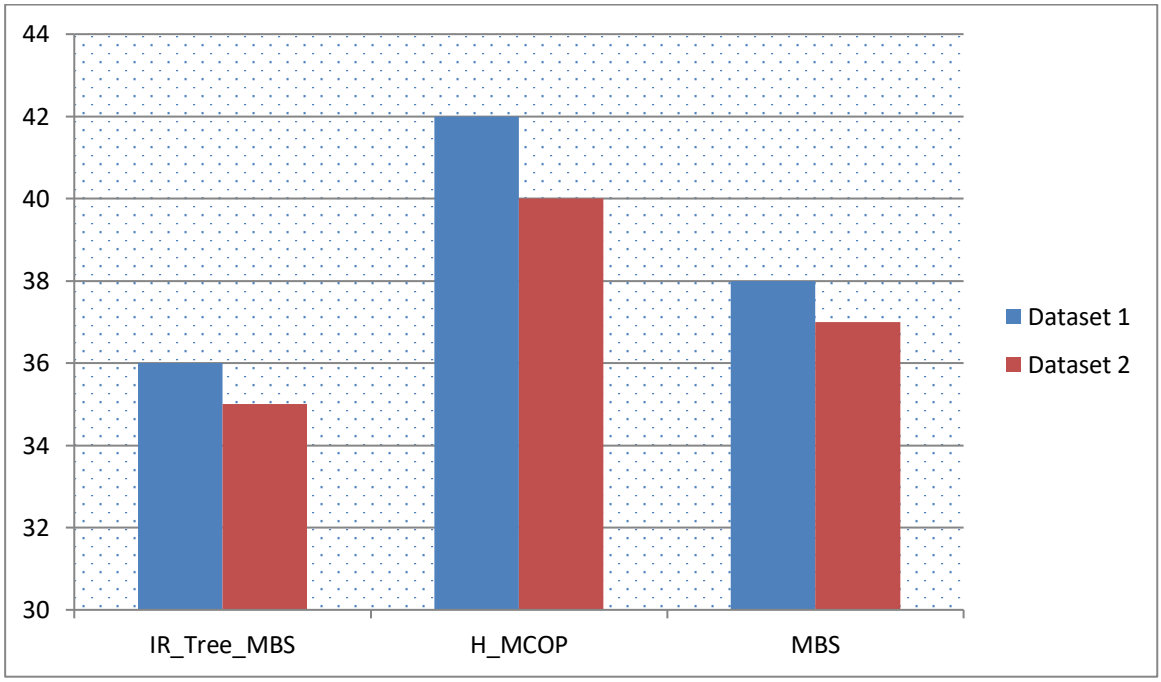

Fig 2. Contrast of route quality results and the results of Various Algorithms on Distinct Datasets

Identity information, login data, friend data, content provided on social media networking, and data distribution are the key categories of private information in social networks. The goal of this parameter setting is to broaden the range of solutions that may be found by satisfying the restrictions. The route quality function assigns values of 0:25, 0:25, and 0:5g to trust, intimacy, and reputation, respectively, emphasizing the significance of reputation in determining the level of trust. There are comparisons made between the H_MCOP and MBS, and IR Tree-MBS approaches. In each of the 24 randomly created sub-datasets, all three algorithms run the identical route query condition three times to get an average. **Fig 2** displays the results of a comparison of the algorithms' route quality and the efficiency of their respective path queries. Since they share a same lookup technique and goal function, the MBS algorithms and R-Tree-MBS provide similarly high-quality path lookups. Due to the fact that the MBS algorithm, the H_MCOP and IR-Tree-MBS algorithms all regard the route identified as optimum whenever it has maximal quality of routes and is a viable solution, all three approaches achieve comparable path-finding quality (e.g., on 9 and 15 datasets illustrated in **Fig 2**).

When a maximum path quality exists but no practical solution can be found, the H MCOP method switches to looking for the minimal objective $g\lambda\eth p\text{Þ} < 1$ function. The IR-Tree-MBS and the MBS algorithms are able to locate near-optimal solutions, but the H_MCOP method is unable to do so. This leads to the paradox that even when a workable solution exists, H_MCOP will produce an invalid result. **Fig 3** shows that whenever the size of the network is minimal and the topology of the system is modest, the MBS and H-MCOP algorithms have effective execution effectiveness compared to the IR-Tree and MBS algorithms. This is due to the fact that whenever the Tree-MBS- IR algorithms is performed, it first has to construct IR-Tree indexes of the networking node, which takes roughly 1-5 seconds. The three most common types of discrete distribution are the geometric distribution, Poisson distribution, and the binomial distribution.

The most common types of discrete distributions are the exponential, log-normal, and Weibull, normal distributions. However, the H_MCOP and MBS algorithms for more direct inquiry have a better performance whenever the size of the systemis modest. The efficacy of the H_MCOP and MBS algorithms steadily diminishes with increasing network complexity and size of network construction, but the IR-Tree-MBS approach is rather stable. You may break it down into two categories of causes: First, unlike the H_MCOP, MBS, and IR-Tree MBS approaches makes use of the IR-Tree structure by performing keyword pruning and distance pruning before querying the route, therefore reducing the search space to some extent; second, the IR-Tree_MBSalgorithms do not integrate the attributes of H_MCOPto determine $gp >$ 1in the process of forward searches.

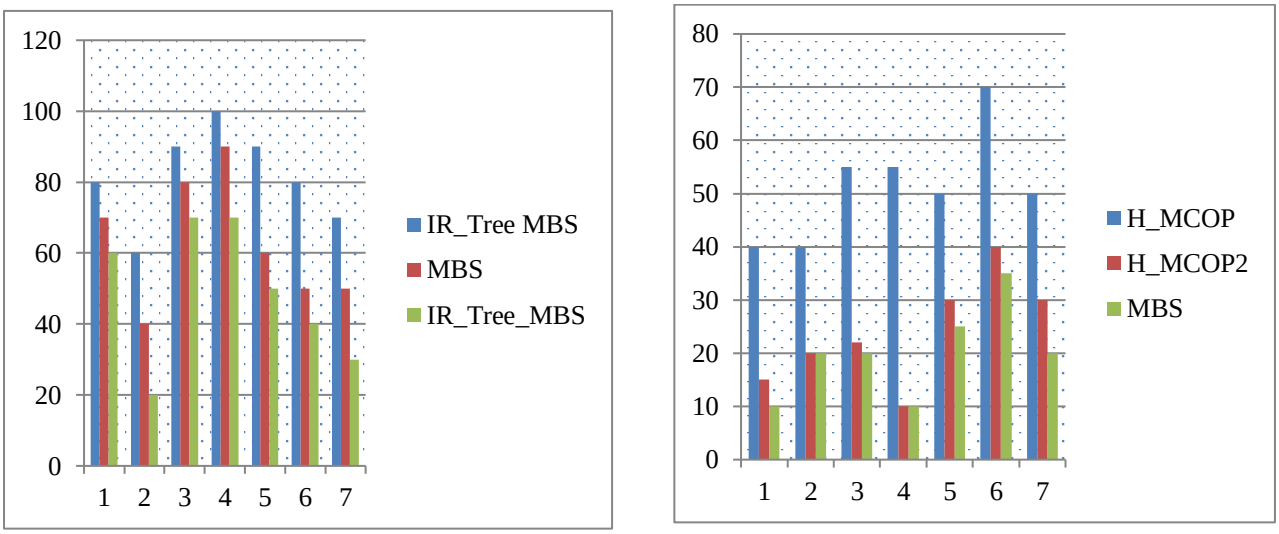

Fig 3(a). Dataset 1 **Fig 3(b).** Dataset 2

Fig 3. Execution effectiveness of Distinct Algorithms on Various Datasets

Fig 4 demonstrates that whether a network contains 100 or even 200 nodes, the overall amount of energy needed by the network grows as the number of polls sent out increases. Rising energy consumption is seen most by the AODV-SMS protocol for path recover, then by the PSO (AODV-SMS) protocol, and finally but the ABC-PSO (AODV-SMS) protocol, which uses the least power. The number of sensing nodes tends to enhance in parallel with the networking density, the route recovery (AODV-SMS) technique only uses sensing nodes, and one transmission route that fail the fastest during source-to-destination transmissions are typically found within the typical node, alongside the channel of transmission whereby the typical node is situated, or not far from the destination node Sink. Nevertheless, when the sensing node density enhances, data transmission and data loss connection stoppage become more likely due to the common node's high energy consumption, which makes it vulnerable to early "death" events.

In order to find a path for packet forwarding that reduces the likelihood of piecewise overheating, reduces the likelihood of considering multiple shared endpoints, evens the endpoints within the subnet, evens the usage of system

energy, and increases the transmission rate, the ABC-PSO (AODV-SMS) multipath routing recovery method presented here takes into consideration a detergent residue of the nearest endpoints, network bandwidth balancing, and downlink distance. **Fig 5** shows that, in comparison to AODV-SMS protocol of routing, the method presented in this study requires much more energy to run. This is because the original data transmission line is disrupted when the Sink moves, a new transmission path is sought out that is close to the initial route, and network power consumption equalization is considered. While thinking about the participants' locations and social groups, it's crucial to do the following search: First, the whole network must be re-traversed to detect nodes, which fulfill both the textual and location data; then, from among different nodes, one is employed as the endpoint node and the other as the nodes at the source to effectively identify the pathways within the network, which meet distinct constraints.

Whilst the swarm intelligent optimization method ABC-PSO (AODV-SMS) uses some energy in order to effectively optimize the path for data transmission, in consideration to the residual energy of the neighborhood nodes, the detachment of transmission, and t, the recommended multi-path transmission path recovery approach could make full usage of data supplied by the initial path to swiftly recover a reliable and efficient transmission route, providing prompt worldwide convergence. The end-to-end transmission delays enhance while employing the protocol of AODV-SMS protocols with a minimal nodes number (100 nodes). The ABC-PSO and AODV-SMS's multi-route recovery methods are more comprehensive. Since data transmission congestion is unlikely to be severe when dealing with a minor node number, and the variation of transmission delay between thePSO (AODV-SMS) and the ABC-PSO (AODV-SMS)multipath transmission path recovery approaches is negligible, the suggested algorithm attains a minimal end-to-end delay compared to the AODV-SMS method

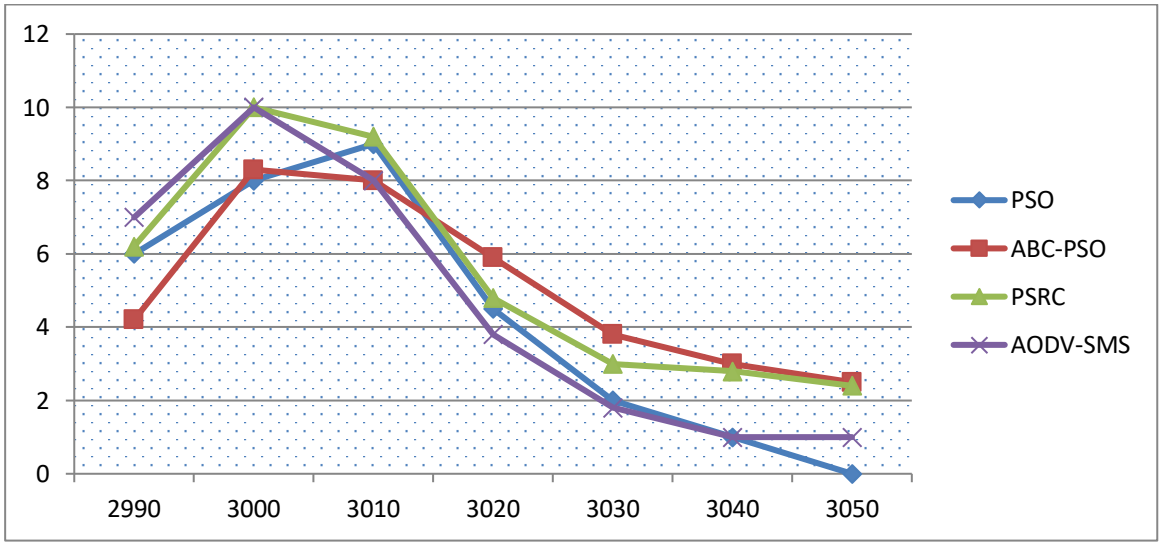

Fig 4. A comparison of the Consumption of Network Energy

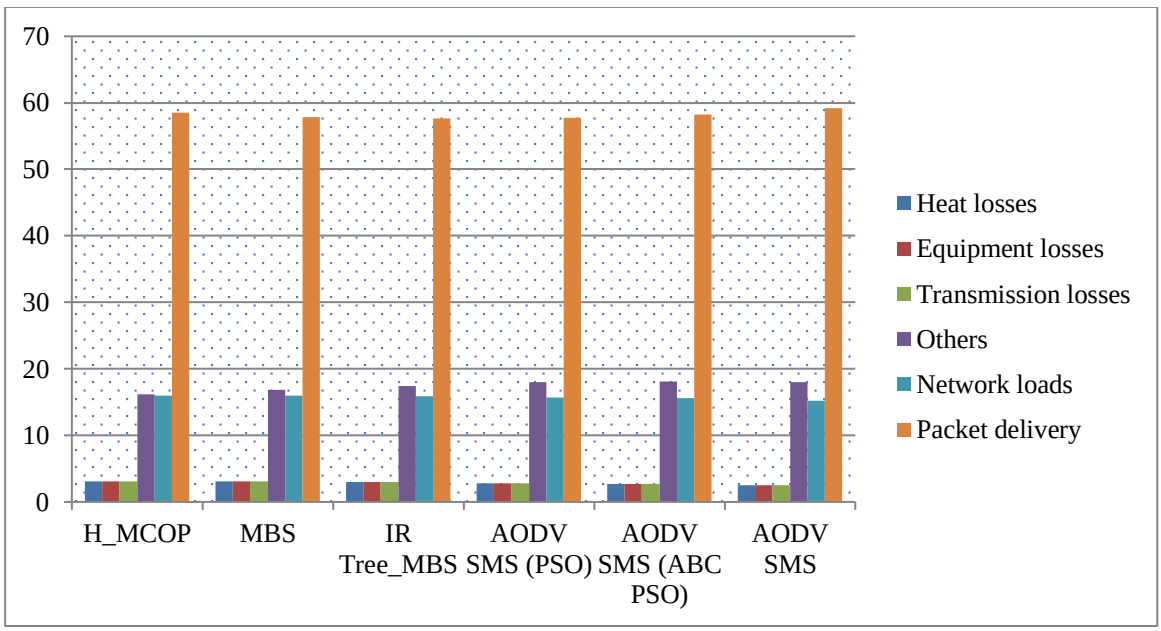

Fig 5. Algorithmic Energy Usage

The multi-path recovery approach of the PSOand the ABC-PSO algorithms is considered to diversify the overall number of transmission channels onto the destination nodes as sensing nodes number rises, with the additional transmission paths being designed with careful transmission consideration ABC-PSO (AODV-SMS) path recovery factors illustrating an enhanced delay timeframe of packet transmission compared to the rest of the path recovery techniques. The time it takes for a packet to be sent decreases with time, while the gap between them widens. As a result, the multipath path recovery approach discussed in this research contribution is capable of considering the remaining power to the nodes nearest of the transmission connections, the network bandwidth balance, and the communication distance, selecting more appropriate communication nodes to effectively structure an improved route. This is especially true when the network size increases, as the transmitter and delay route dimension employed by the nodes at the source to effectively communicate to the destination point also increase.

VI. CONCLUSION

The expansion of contemporary digital communication technologies has led to the development of social networking sites (SNSs). As the infrastructure for the Internet has matured, the widespread use of social networks has become an integral part of many people's daily lives and careers. Nevertheless, people's worries about their privacy when using social media have been growing in recent years. As the data owner's sensitive data is accessible over the social networking site without the data owner's direct and immediate administration, data leakage may occur, allowing the users who were not granted access to all the information or data by the proprietor or who misappropriated the data to see the material. Here, we take a fresh approach to the research of network reliability by analyzing performance metrics in ways that go beyond the standard research of dependability content (fault repair, fault identification, and network failure rates, etc.) and network connectivity, load balancing, and network energy consumption among others.

In this research contribution, we provide smart optimization and artificial intelligence techniques to mitigate the issue of reliability including fundamental research on mobile WSNs network reliability and fault prediction evaluation techniques, the influence of cellular path optimization on the efficiency of information access, and system reliability, dependable transfer of data-based data fusion approach, the smart fault tolerance techniques for multi-path routing to minimize the issue of fault interference. Distributions such as binomial, Poisson and geometric distributions fall under the umbrella of "discrete." Distributions like the exponential, Weibull, log-normal and normal are all examples of discrete distributions. To lessen the burden on the data owner and prevent collusion intrusions between unauthorized users, and attribute management servers, the issue of keys for attribute encryption is a collaborative effort between the server and the owner of the data. Access control for various users with varying rights is achieved by user classification and design to strike a balance between the practicality of data dissemination and the privacy of data security. Moreover, the decryption cost may be decreased by optimizations made to the original system and a caching mechanism for the buddy data. This architecture is advantageous because it increases query performance, decreases system overhead, and strengthens privacy protections.

Data Availability

No data was used to support this study.

Conflicts of Interests

The author(s) declare(s) that they have no conflicts of interest.

Funding

No funding was received to assist with the preparation of this manuscript.

Ethics Approval and Consent to Participate

The research has consent for Ethical Approval and Consent to participate.

Competing Interests

There are no competing interests.

References

[1]. K. Sindhanaiselvan, J. M. Mannan, and S. K. Aruna, “Designing a dynamic topology (DHT) for cluster head selection in mobile adhoc network,” Mob. Netw. Appl., vol. 25, no. 2, pp. 576–584, 2020.

[2]. A. Kilic and F. Iscioglu, “An algorithmic reliability evaluation approach for a multi-state k-out-of-n:G system with nonidentical and large number of components,” Proc. Inst. Mech. Eng. O. J. Risk Reliab., vol. 237, no. 1, pp. 58–68, 2023.

[3]. S. Bhandari, N. Bergmann, R. Jurdak, and B. Kusy, “Time series analysis for spatial node selection in environment monitoring sensor networks,” Sensors (Basel), vol. 18, no. 2, p. 11, 2017.

[4]. J. Xu, H. Huang, J. Kan, and R. Wang, “Energy-balanced routing protocol based on data priority for lung terahertz nanosensor networks,” in 2022 IEEE 95th Vehicular Technology Conference: (VTC2022-Spring), 2022.

[5]. K. Bazar, Department of Engineer, Central Government, New Delhi, India, D. K. Sharma, and Assistant Professor, Department of Electronics and Communication, National Institute of Technical Teachers Training and Research (NITTTR), Chandigarh, India, “Energy Efficient Multi-

Hop Multipath Sub Clustering Routing Protocol for wireless sensor network," International Journal of Recent Technology and Engineering (IJRTE), vol. 11, no. 6, pp. 1–12, 2023.

[6]. A. Jasinska-Piadlo et al., "Data-driven versus a domain-led approach to k-means clustering on an open heart failure dataset," Int. J. Data Sci. Anal., vol. 15, no. 1, pp. 49–66, 2023.

[7]. C. Krause, W. Huang, D. B. Mechem, E. S. Van Vleck, and M. Zhang, "A metric tensor approach to data assimilation with adaptive moving meshes," J. Comput. Phys., vol. 466, no. 111407, p. 111407, 2022.

[8]. M. I. Alipio and N. M. C. Tiglao, "RT-CaCC: A reliable transport with cache-aware congestion control protocol in wireless sensor networks," IEEE Trans. Wirel. Commun., vol. 17, no. 7, pp. 4607–4619, 2018.

[9]. Y.-J. Hu, L.-J. Bao, C.-L. Huang, S.-M. Li, P. Liu, and E. Y. Zeng, "Assessment of airborne polycyclic aromatic hydrocarbons in a megacity of South China: Spatiotemporal variability, indoor-outdoor interplay and potential human health risk," Environ. Pollut., vol. 238, pp. 431–439, 2018.

[10]. S. Kim and J. Choi, "Optimal deployment of sensor nodes based on performance surface of underwater acoustic communication," Sensors (Basel), vol. 17, no. 10, p. 2389, 2017.

[11]. J. Gunderson et al., "Social and non-social sensory responsivity in toddlers at high-risk for autism spectrum disorder," Autism Res., vol. 14, no. 10, pp. 2143–2155, 2021.

[12]. Y. Zhang and Y. Li, "High-gain omnidirectional dual-polarized antenna for sink nodes in wireless sensor networks," Sensors (Basel), vol. 22, no. 3, p. 788, 2022.

[13]. W. Lu et al., "Monte Carlo simulation for performance evaluation of detector model with a monolithic LaBr3(Ce) crystal and SiPM array for γ radiation imaging," Nucl. Sci. Tech., vol. 33, no. 8, 2022.

[14]. A. N. Kislyakov and Vladimir branch of the Russian Academy of National Economy and Public Administration under the President of the Russian Federation, "The algorithm for binary classification on graph-based decision-making in the tasks of credit scoring," Models, Systems, Networks In Economics, Engineering, Nature And Society, no. 1, 2021.

[15]. A. Kumar and H. Wagatsuma, "A Kamm's circle-based potential risk estimation scheme in the local dynamic map computation enhanced by binary decision diagrams," Sensors (Basel), vol. 22, no. 19, 2022.

[16]. Y. Feng and W. Xie, "Teens' concern for privacy when using social networking sites: An analysis of socialization agents and relationships with privacy-protecting behaviors," Comput. Human Behav., vol. 33, pp. 153–162, 2014.

[17]. M. Avellina, A. Brankovic, and L. Piroddi, "Distributed randomized model structure selection for NARX models: Distributed randomized model structure selection for NARX models," Int. J. Adapt. Control Signal Process., vol. 31, no. 12, pp. 1853–1870, 2017.

[18]. P. V. Matrenin, "Improvement of ant colony algorithm performance for the job-shop scheduling problem using evolutionary adaptation and software realization heuristics," Algorithms, vol. 16, no. 1, p. 15, 2022.

[19]. L. Cheng, K. Wang, L. Wei, Y. Liang, and P. Song, "A novel automatic voltage control strategy based on adaptive pheromone update improved ant colony algorithm," in 2022 2nd International Conference on Electrical Engineering and Mechatronics Technology (ICEEMT), 2022.

[20]. U. F. Siddiqi, Y. Shiraishi, and S. M. Sait, "Multi-constrained route optimization for Electric Vehicles (EVs) using Particle Swarm Optimization (PSO)," in 2011 11th International Conference on Intelligent Systems Design and Applications, 2011.

[21]. K. Nsafoa-Yeboah et al., "Software-defined networks for optical networks using flexible orchestration: Advances, challenges, and opportunities," J. Comput. Netw. Commun., vol. 2022, pp. 1–40, 2022.

[22]. H.A, A. R and S. M, "Cognitive Radio Communication and Applications for Urban Spaces," Computing and Communication Systems in Urban Development, pp. 161–183, 2019. doi:10.1007/978-3-030-26013-2_8

[23]. H.A, A. R and S. M. (2019). Machine Learning and Big Data for Smart Generation. Computing and Communication Systems in Urban Development, 185–203. doi:10.1007/978-3-030-26013-2_9.

[24]. H.A, A. R and S. M, "Smart Sensor Networking and Green Technologies in Urban Areas," Computing and Communication Systems in Urban Development, pp. 205–224, 2019. doi:10.1007/978-3-030-26013-2_10

[25]. S.-C. Lin, "Hydromechanics, Aerodynamics and Thermodynamics: Critical Numerical Analysis of Aerodynamics of BLE Turbine Blade," Journal of Machine and Computing, pp. 20–28, Jan. 2021.