Computers, Materials & Continua

Tech Science Press

Doi:10.32604/cmc.2025.065660

ARTICLE

AI-Driven Sentiment-Enhanced Secure IoT Communication Model Using Resilience Behavior Analysis

Menwa Alshammeri[1], Mamoona Humayun[2,*], Khalid Haseeb[3] and Ghadah Naif Alwakid[1]

[1]Department of Computer Science, College of Computer and Information Sciences, Jouf University, Sakaka, 72388, Saudi Arabia
[2]Department of Computing, School of Arts Humanities and Social Sciences, University of Roehampton, London, SW15 5PH, UK
[3]Department of Computer Science, Islamia College Peshawar, Peshawar, 25120, Pakistan

*Corresponding Author: Mamoona Humayun. Email: mamoona.humayun@roehampton.ac.uk

Received: 19 March 2025; Accepted: 28 April 2025; Published: 09 June 2025

ABSTRACT: Wireless technologies and the Internet of Things (IoT) are being extensively utilized for advanced development in traditional communication systems. This evolution lowers the cost of the extensive use of sensors, changing the way devices interact and communicate in dynamic and uncertain situations. Such a constantly evolving environment presents enormous challenges to preserving a secure and lightweight IoT system. Therefore, it leads to the design of effective and trusted routing to support sustainable smart cities. This research study proposed a Genetic Algorithm sentiment-enhanced secured optimization model, which combines big data analytics and analysis rules to evaluate user feedback. The sentiment analysis is utilized to assess the perception of network performance, allowing the classification of device behavior as positive, neutral, or negative. By integrating sentiment-driven insights, the IoT network adjusts the system configurations to enhance the performance using network behaviour in terms of latency, reliability, fault tolerance, and sentiment score. Accordingly to the analysis, the proposed model categorizes the behavior of devices as positive, neutral, or negative, facilitating real-time monitoring for crucial applications. Experimental results revealed a significant improvement in the proposed model for threat prevention and network efficiency, demonstrating its resilience for real-time IoT applications.

KEYWORDS: Internet of things; sentiment analysis; smart cities; big data; resilience communication

1 Introduction

IoT is a cutting-edge technology, interconnected with various electronic equipment that supports real-time observation and big data analytics for critical applications [1,2]. Using the developed system, network devices and end users gathered data from the deployed IoT sensors to improve the sustainability of the sensing field [3,4]. Due to the high speed and low implementation costs, web-based network infrastructure is utilized frequently for critical analysis of big data in smart applications [5,6]. The extensive use of digital devices has accumulated massive data repositories; therefore, proposing intelligent solutions for effective communication along with security is a significant area of research [7,8]. Due to the massive amount of data, constrained devices cannot interpret network requests intelligently. Numerous artificial intelligence and machine learning techniques have been investigated for optimization and system sustainability [9,10]. Future technologies are interconnected with electric equipment to significantly develop next-generation communication services, effectively addressing evolving critical user demands [11,12]. Constrained devices cannot interpret network requests intelligently due to the timely processing of big data. To address these

issues, many learning techniques have been explored for optimization in developing emerging services by exploring network conditions [13,14]. Alternatively, sentiment analysis offers critical services for smart applications with the support of IoT security by evaluating the user response and device feedback based on real-time insights. It provides the early detection of communication threats and network anomalies, thus reducing the probability of data breaches and providing a timely response in the event of fault detection [15,16]. It enhances the decision-making process for trusted and secure algorithms by exploring authentic and access control strategies. The continuous monitoring of user behavior and system activities using sentiment analysis copes with malicious activities and reduces unauthorized access on IoT networks. Accordingly, we need a predictive innovative system for sustainable development growth by exploring user demands and system feedback. This research aims to present an Artificial Intelligence-driven (AI-driven), sentiment-based adaptive model for smart cities to guarantee the efficient allocation of network resources and increase trust in coping with network anomalies by exploring system feedback. The objectives of our proposed model focus on enhancing the efficiency of IoT routing using sentiment analysis by determining the device's behavior. It combines big data analytics and the status of the network environment to ensure quality of service and improve decision-making in the management of resources. Moreover, based on the device's response, time detection of threats against various anomalies is carried out, increasing the trustworthiness of the intelligent communication systems. In addition, decision-making strategies are dynamic and updated using continuous evaluation of sentiment-driven insights, providing resilience with the intelligent computing environment. The following are the main research contributions of our proposed model.

i. By exploring the sentiment analysis with fitness evaluation, the proposed model leverages big data and improves the efficiency of routing based on various real-time parameters and user feedback.
ii. The incorporation of network behavior for sentiment analysis, the proposed model offers in-depth involvement in ensuring the quality of service and generates dynamic decision-making policies for efficient management of big data.
iii. Leveraging the user feedback allows for the early detection of network anomalies and malicious threats, thus improving the security framework of smart systems.

The following subsections organize this research. Section 2 presents related work. Section 3 provides a discussion of the proposed model. Section 4 presents the results and discussion. At the end, a conclusion is provided in Section 5.

2 Related Work

Wireless networks utilize adaptive computing and integrate artificial intelligence techniques to elevate the processing and dynamic strength of distributed systems. This combination not only affects the sustainability level of the network but on the other side also enables timely prediction for emerging IoT applications [17,18]. In addition, the advancements in sentiment analysis and future technologies are reshaping the decision-making process in real-time and dynamic networks [19,20]. In smart cities, sentiment-enhanced network infrastructure contributes to system and user response and enables the communication system to adjust adaptively based on the network conditions [21,22]. The combination of user response, system feedback, and sentiment-driven IoT networks enables smart systems to adapt to latency, reliability, and security needs for big data analytics. It enhances the network performance optimization, responsiveness, and threat detection over the unpredictable environment [23]. The integration of blockchain technology for smart communication with the combination of AI-driven approaches fosters a more sustainable environment against threats and guarantees an efficient digital world [24,25]. Smart cities face significant research in real-time systems, particularly in optimizing IoT systems with scalability and the least computational cost. Moreover, ensuring security with trust and reliable communication between IoT users is a crucial factor

for the development of sustainable solutions [26,27]. Therefore, integrating sentiment analysis into smart systems can enhance adaptability for the processing of big data by assessing system and user feedback. It reduces traffic distribution and reduces network congestion on constrained electronic devices and sensing systems [28,29]. In [30], an Energy-Efficient Multilevel Secure Routing (EEMSR) protocol is proposed for IoT networks. Because the clustering technique efficiently manages energy resources, a cluster-based, multi-hop routing protocol reduces the high communication overhead in IoT networks. In particular, a more reasonable analytic hierarchy process and genetic algorithms are used to assign precise weights and optimize intercluster routing in heterogeneous IoT systems that support numerous network services. By computing the trust factor on the data and routing, including data perception trust, data fusion trust, and communication trust, multiple clustering levels are adopted to defend against the various attacks. However, it faces research challenges in terms of scalability for a high number of IoT devices and imposing additional computational overheads. In addition, to cope with real-time threat detection, the proposed approach is very limited in controlling the dynamic network infrastructure. To optimize the efficiency of authentication, the authors [31] proposed a lightweight blockchain-based authentication mechanism for IoT networks. It stores only a few credentials of ordinary sensors to reduce the computational overhead for IoT networks. Furthermore, a genetic algorithm-based SDN controller is explored to increase the network lifetime for route calculation and on-demand routing, as a result, the proposed solution optimizes energy consumption. Furthermore, to detect malicious devices, a route correctness mechanism is introduced, and a list of malicious devices is in the form of a blockchain. However, it is observed that the proposed scheme only copes with energy resources and the detection of malicious activities, but overlooks the scalability problem for a wide range of IoT devices and coverage areas. In such cases, it reduces the timely response to crucial services and decreases the reliability level of the deployed system. In [32], the main aim of the proposed work is to propose an Enhanced Multi-Attribute-Based Attack Resistance (EMBTR) algorithm that securely performs data routing based on trusted values of nodes. The proposed algorithm explored Quality of Service (QoS) characteristics, including Stability rate (SR), Reliability rate (RR), and elapsed time (ET), to improve network performance and prevent trust-related attacks. It may introduce the complexity and communication overheads for IoT devices due to the multi-attributed routing scheme. In terms of network scalability, latency may vary due to the inconsistent selection of forwarders. In mobile edge computing networks, authors [33] proposed an adaptive routing protocol for the effective control of energy usage among end-user devices. Firstly, a link quality prediction method is utilized to split the objects of the network into different clusters. Secondly, the data is routed toward the destination by considering an account of the object's movement. However, the ARPMEC protocol incurs the research problem in coping with network scalability issues while the IoT environment is densely deployed. Moreover, under the adaptive network scenario, the proposed approach can degrade the performance of mobile devices and cause unnecessary network disruption. The authors [34] proposed a data aggregation back pressure routing (DABPR) method to aggregate overlapping routes for effective data transmission while extending the network's lifetime. Event data is transferred from the event regions to the sink nodes during each of the five phases of the DABPR routing algorithm. These include the phases of route selection with multiple attributes, such as decision-making metrics, data aggregation, scheduling, maximizing event detection reliability, and cluster-head selection. The proposed algorithm performs data aggregation on redundant data at relay nodes to reduce message size, exchange rate, communication overhead, and energy consumption. However, the DABPR approach may introduce research challenges to establish the trusted forwarding connections among devices and make it harder to cope with communication breaches in the event of malicious activities. Moreover, the DABPR may incur network congestion and disruption under emergency and more responsive applications when the devices have mobility patterns. As per the analysis of existing studies, IoT applications are broadly utilized in the growth of smart wireless systems. They interact with many mobile devices to sense the real-time environment and communicate

with central processing stations for onward data processing. However, the rapid growth in unpredictable IoT devices and wireless networks imposes significant challenges to optimizing the network resources with efficient energy consumption and intelligent decisions for crucial conditions. In addition, most existing approaches lack scalability and adaptive network traffic management when IoT devices communicate in a large-scale target field.

3 Proposed Model

This section describes the AI-Driven Sentiment Analysis Secure Communication (AI-SASC) model for IoT networks. Initially, it connects the sensors with cutting-edge wireless technologies to collect data from the unpredictable environment and process it using lightweight computing power. Sentiment rules are integrated to attain fault-tolerant routes while transmitting sensitive data. The routes are kept secure with user and device feedback. It strengthens the IoT system in processing the collected data and increases the stability of the network. The AI-SASC model intends to optimize the allocation of resources for smart systems with the combination of sentiment analysis. Unlike traditional metrics, it also utilizes user sentiment, which reflects feedback and system satisfaction. Fig. 1 shows the proposed model's architecture, highlighting the designed states' interaction. Initially, the population of routes is identified as P, defined in Eq. (1), and each route r_i is the random sample for transmitting IoT data.

$$P = \{r_1, r_2, \ldots, r_n\} \tag{1}$$

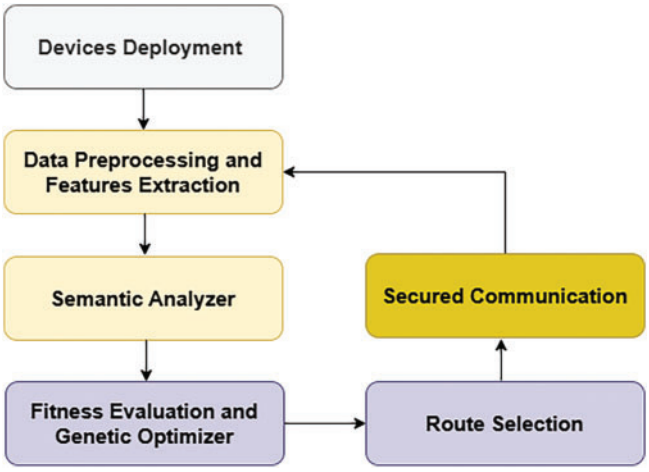


Figure 1: Sequential architectural flow of the proposed AI-SASC model

Each route r_i determines its fitness function $F(r)$ formulated using latency lt, reliability rel, and fault tolerance ft parameters. Also, the semantic score Sc based on the user feedback is incorporated into the decision-making process, given in Eq. (2).

$$F(r) = w_1 * lt(r_i) + w_2 * rel(r_i) + w_3 * ft(r_i) + w_4 * Sc(r_i) \tag{2}$$

where w_i (for $i = 1, 2, 3, 4$) are weighted contributions. The latency of a route is determined using Eq. (3) and derived from the time taken to transmit the IoT data toward the destination. Moreover, distance d_r is also considered for all the hops k in the route r_i.

$$lt(r) = \sum_{i=1}^{k} t_i + d_r \tag{3}$$

Reliability for a particular route $rel(r_i)$ performs a significant role in evaluating network optimization, as it reflects the consistency and trust of the devices. It is based on the average reliability $RL(j)$ over hops k on a particular route, as given in Eq. (4).

$$rel(r_i) = \frac{1}{k} \sum_{j=1}^{k} RL(j) \tag{4}$$

ft is used to evaluate the combined effect of failure probability $Prob_f$ and security level $Rt(s)$ at state s, as given in Eq. (5). It ensures the system's availability while transmission of IoT data on most reliable and trustworthiness links.

$$ft(r_i) = 1 - (Prob_f).Rt(s) \tag{5}$$

where $Rt(s)$ is defined as a weighted sum of the encryption En and authenticity $authen$ of the selected route r_i, along with weighted factors α and β as shown in Eq. (6).

$$Rt(s) = \alpha \cdot En(r_i) + \beta \cdot auhen(r_i) \tag{6}$$

The proposed AI-SASC model utilizes some rules to derive the sentiment scores and explore them for the computation of the fitness function. The rules are based on positive and negative feedback from users n that reflects the semantic score, as given in Eq. (7). Also, if user feedback is higher than a certain threshold T, a priority is assigned to a particular route r_i, defined in Eq. (8).

$$Sc = \frac{1}{n} \sum_{i=1}^{n} r_i \tag{7}$$

$$Priority = \begin{cases} Assigned, & if\ Sc > T \\ Not\ Assigned, & otherwise \end{cases} \tag{8}$$

A mutation is performed on the new route $r_{new}(r)$ to introduce some variations, and as a result, a mutated route $r_{mutated}$ is given in Eq. (9). The fitness of the newly established route r is re-evaluated based on the multi-facet attributes and sementic score, defined in Eq. (10).

$$r_{\text{mutated}}(r) = \text{Mutation}(r_{\text{new}}(r)) \tag{9}$$

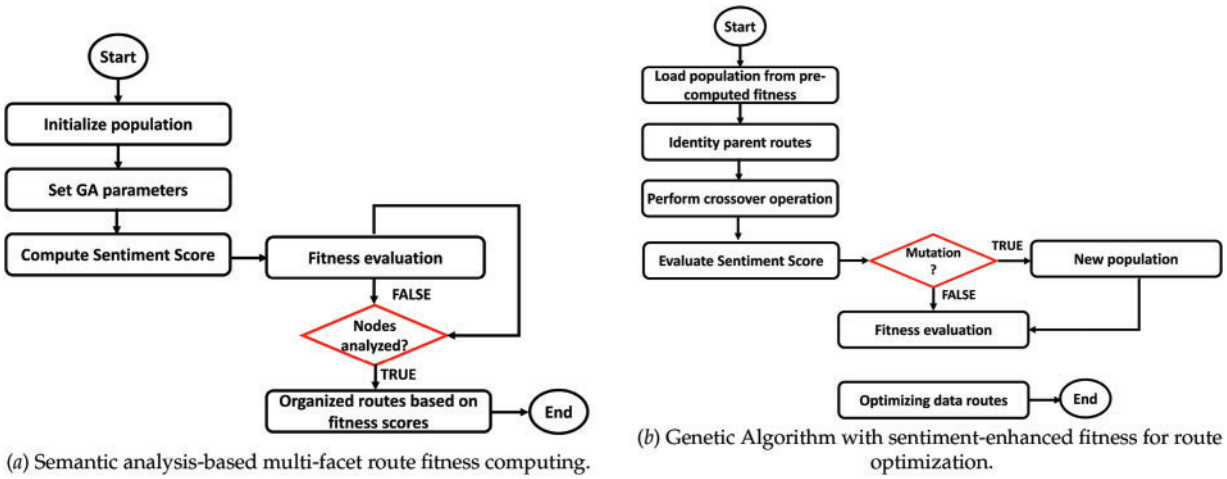
$$F_{\text{new}}(r) = w_1 \cdot lt(r) + w_2 \cdot rel(r) + w_3 \cdot ft(r) + w_4 \cdot Sc(r) \tag{10}$$

In the end, fitness values F'_{new} of route r is normalized in the standard range of $[0, 1]$ using Eq. (11), where F_{min} and F_{max} denotes minimum and maximum fitness values.

$$F'_{\text{new}}(r) = \frac{F_{\text{new}}(r) - F_{\text{min}}}{F_{\text{max}} - F_{\text{min}}} \tag{11}$$

Fig. 2a,b depicts the AI-SASC model flowchart for sentiment score evaluation. It explores the genetic algorithm inspired by Charles Darwin's theory of natural selection to optimize complex problems [35]. The proposed mode integrates the sentiment scores to identify the multi-facet attributed routes. The sentiment analysis evaluates the network based on user feedback and route experience. A genetic algorithm explores

the fitness function to identify the set of routes. Using sentiment analysis, it performs some crossover and mutation operations to determine the alternate and most reliable route. Later, the AI-SASC model performs recursive strategies to compute the fitness, and the sentiment score continues until optimal routing performance is achieved. It leads to learning from the network behavior and efficient utilization of resources and their consumption.



(*a*) Semantic analysis-based multi-facet route fitness computing.

(*b*) Genetic Algorithm with sentiment-enhanced fitness for route optimization.

Figure 2: Flowchart of the AI-SASC model: (**a**) Semantic analysis-based multi-facet route fitness. (**b**) Genetic Algorithm with sentiment-enhanced fitness for route optimization

Algorithm 1 illustrates the pseudocode of sentiment score computing and Genetic Algorithm Sentiment-Enhanced Fitness evaluation for Route Optimization. In the beginning, it initializes the evaluation of the fitness function for the populated routes using latency, reliability, fault tolerance, and sentiment scores from user feedback. The sentiment score is derived for each route; otherwise, the default value is retrieved. In the proposed model, weighted factors are explored to compute the fitness values using multiple parameters. Moreover, to guarantee reliability and consistency, the computed fitness values are normalized. In the end, the algorithm returns all the determined computed values of the routes, and optimizing decision-making is made for routing the smart application. Unlike most of the existing solutions, the proposed algorithm combines the users' feedback and response in the decision-making process of IoT routing, ultimately enhancing the sustainability and adaptability of network infrastructure.

Algorithm 1: Route fitness using sentiment score evaluation

Input: Population of routes P
Output: Initial fitness values for population P
1 **for** *each route* $r \in P$ **do**
2 Evaluate sentiment score *Sc(r)* from user feedback;
3 **if** *Sc(r) is unavailable* **then**
4 Assign default *Sc(r)*;
5 **end**
6 Compute fitness: $F(r) = w_1 lt(r) + w_2 rel(r) + w_3 ft(r) + w_4 Sc(r)$;

(Continued)

Algorithm 1 (continued)

```
    if Normalization required then
        F'(r) = (F(r) − F_min) / (F_max − F_min);
    end
end
return Initial fitness values for population P
```

Algorithm 2 shows the genetic algorithm driven sentiment-enhanced fitness for route optimization, aims to present the evolutionary methods and principles to improve further the process of route selection with the computation of multiple generations. The parent routes are selected using the derived fitness values of populated routes in Algorithm 1. Later, genetic operations, crossover, and mutation, are applied to generate offspring routes, and all new routes undergo a recomputation of sentiment-based fitness based on user response and device feedback. Accordingly, the most reliable and optimized routes are selected to transmit IoT data and ensure the continuous enhancement of the decision-making process using an AI-driven approach.

Algorithm 2: Genetic algorithm with sentiment-enhanced fitness for route optimization

Input: Population P with pre-evaluated fitness scores
Output: Best route from final population P_G

```
for generation g = 1 to G do
    Select parents r_i, r_j based on fitness;
    Generate offspring r' = Crossover(r_i, r_j);
    for each r' do
        Mutate if condition met; Recompute fitness using Eq. (2);
    end
    Update population P_g with selected parents and offspring;
    Retain top N best routes for next generation;
    If No fitness improvement over threshold generations then
        Terminate;
    end
end
return Best route from P_G
```

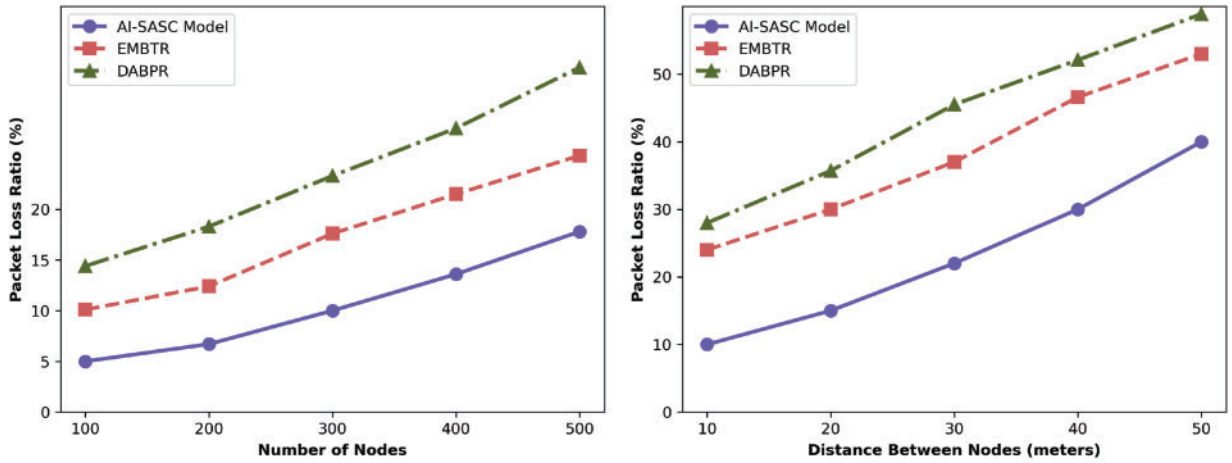
4 Simulations and Results

We evaluate the performance of the AI-SASC model through simulations using Network Simulator 3 (NS-3) compared to existing studies. The experiments are done against two different scenarios. One is a varying number of nodes, and the second is a varying distance among nodes. The simulated data was stored in log files, and later, scripting files were explored to get the computed results for statistical analysis. The AI-SASC model simulates the observing environment that comprises mobile sensors and gateways. The network field is fixed to 4000 m × 4000 m, populated by 100 to 500 sensors, with 5J of initial energy level. Three sink nodes are deployed to support data collection. Sensors are equipped with GPS with a 5 m transmission radius. The simulation parameters are depicted in Table 1.

Table 1: Simulation parameters

Parameter	Value
Simulation area	4000 m × 4000 m
Number of sensors	100 to 500
Number of edges	10
Initial energy	5J
Malicious devices	20
Simulations run	60
Packet size	512 bytes
Evaluation scenarios	Varying distances and number of nodes

Fig. 3a,b illustrates the evaluation of packet loss for the AI-SASC model and related schemes for varying distances and IoT nodes. The performance results show that the AI-SASC model remarkably decreased the packet loss ratio by an average of 33.6% and 38% over EMBTR and DABPR, respectively. It is the combination of a Genetic Algorithm, network conditions, and sentiment analysis that leads to optimizing the data routes and offers a more intelligent decision-making system for constraint innovative applications. The AI-SASC model employs a fitness computing function that uses multi-facet attributes and explores latency, reliability, fault tolerance, and user sentiment feedback. Moreover, it produces the load-balancing routes with effective traffic management on the communication links. Using optimized forwarders in the proposed model further strengthens crucial data transmission using trusted data collectors and attains sustainable applications.



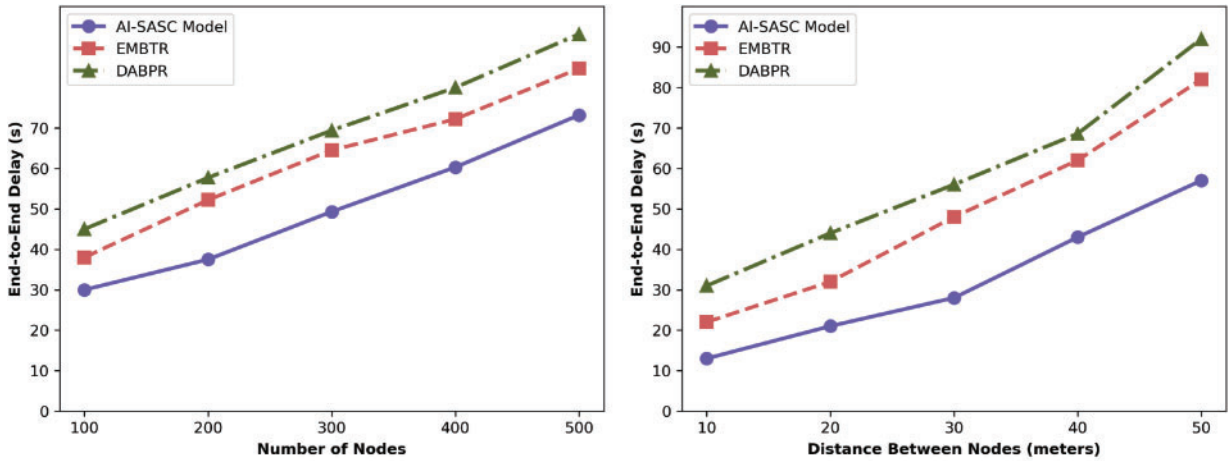
(*a*) Packet loss ratio vs. number of nodes.

(*b*) Packet loss ratio vs. distance between nodes.

Figure 3: Comparison of AI-SASC, EMBTR, and DABPR for packet drop ratio under varying nodes and distances

The experimental results presented in Fig. 4a,b show the performance results of the AI-SASC model and existing solutions in terms of end-to-end delay. Based on the statistical analysis, the AI-SASC model significantly improves the ratio of end-to-end delay by an average of 49.6% and 55.8% under varying distances and numbers of nodes, as compared to EMBTR and DABPR, respectively. The proposed model explored the genetic algorithm combined with semantic analysis and evaluated the network status to attain fault tolerance and system reliability. Moreover, the user's semantic feedback provides a more dynamic IoT

system with intelligent monitoring of data aggregation and processing services for constrained devices. It reevaluates the decision-making with the collaborative and system-level metrics to ensure a long-term and stable communication channel for efficient big data management. In addition, the AI-SASC model reduces the overloaded data flow on the bounded links with robust and adaptive routing policies. Ultimately, it offers crucial data on time from source to destination and is appropriate for realistic smart applications.

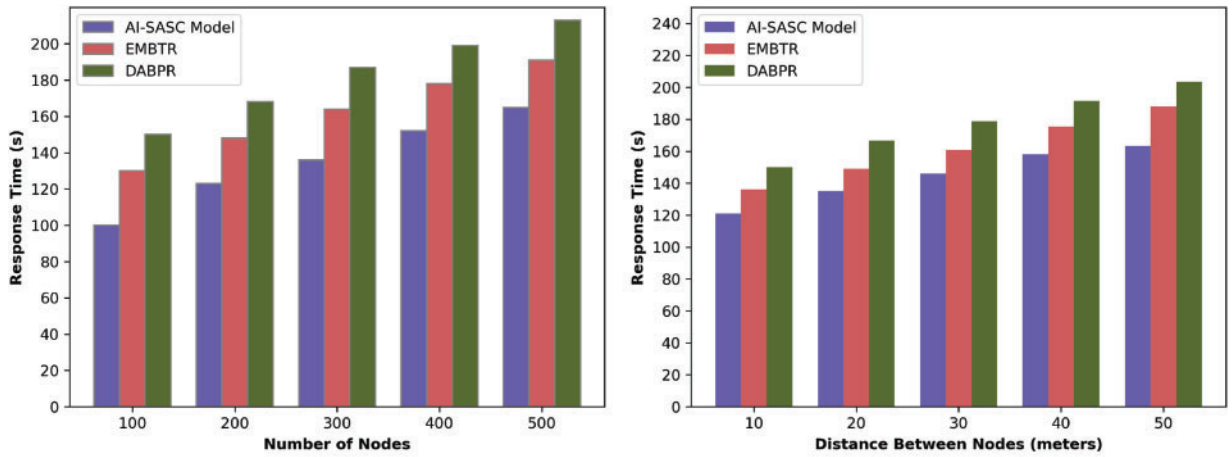


(*a*) end-to-end delay vs. number of nodes. (*b*) end-to-end delay vs. distance between nodes.

Figure 4: Comparison of AI-SASC, EMBTR, and DABPR for end-to-end delay under varying nodes and distances

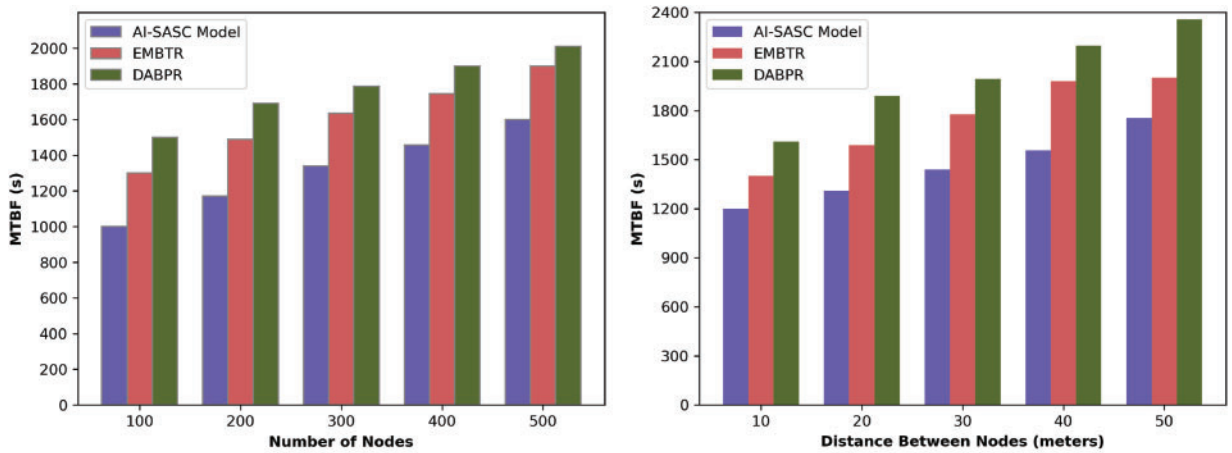
In comparison to the existing solutions, the AI-SASC model enhances the performance of response time for varying distances and numbers of nodes by an average of 43% and 52%, as illustrated in Fig. 5a,b. This is because forwarding routes are re-evaluated based on the system behavior and semantic analysis at the device level. The devices frequently update their tables to keep the most reliable forwarders and select the optimal ones among them. In case any device in the route is malicious or inefficient, the AI-SASC model announces the formulation of the new alternative routes using crossover and mutation operations of the Genetic Algorithm. In addition, based on the sentiment score, the AI-SASC model can prioritize routes based on user feedback and satisfaction. The routes with positive feedback gain more priority for the selection and lead to network optimization for real-time IoT applications. Such strategies offer rapid and reliable routing systems, and devices dynamically adjust the routes by exploring network demands.

In Fig. 6a,b, the performance evaluation of the AI-SASC model is compared with existing solutions in terms of mean time between failures. It was improved for varying distances and number of nodes an average of 38% and 47.9% by utilizing a more reliable fault detection mechanism. By exploring sentiment scores and user feedback for system performance, unpredictable events and issues can be identified before they cause a system to fail. Using assigned priority values, the AI-SASC model can identify the data routes or IoT devices at risk of failure at a particular time. In this case, the allocation of resources dynamically manages the failure chances of the routes and provides optimized solutions with the least interruption or communication delays. Thus, the AI-SASC model intelligently manages the network resources and improves the quality of service across the network devices.



(*a*) Response time vs. number of nodes. (*b*) Response time vs. distance between nodes.

Figure 5: Comparison of AI-SASC, EMBTR, and DABPR for end-to-end delay under varying nodes and distances



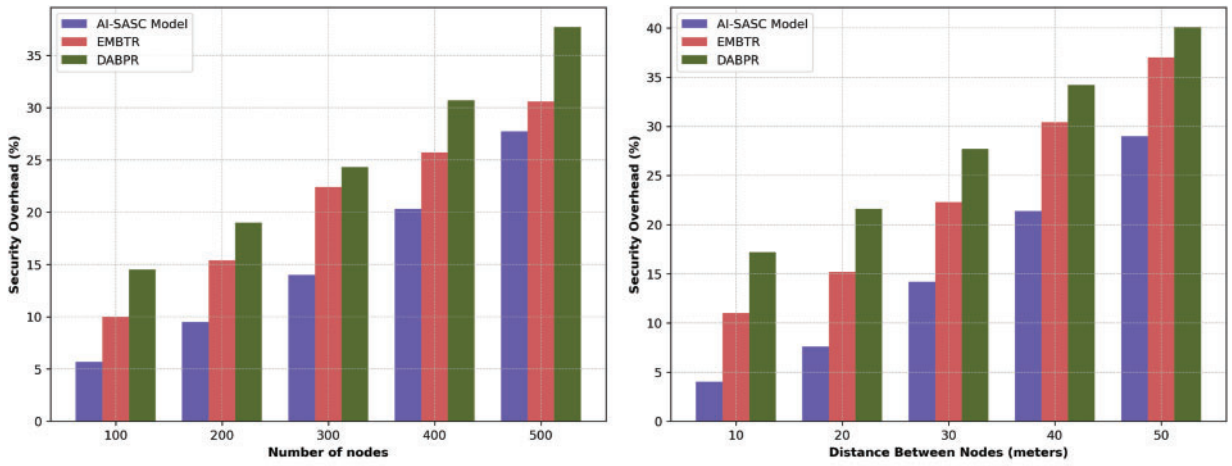
(*a*) MTBF vs. number of nodes. (*b*) MTBF vs. distance between nodes.

Figure 6: MTBF comparison of AI-SASC, EMBTR, and DABPR under varying nodes and distances

In Fig. 7a,b, the AI-SASC model is assessed for security overhead in the comparison of related studies. It is revealed that the AI-SASC model remarkably improved the overheads of the constraint IoT devices by an average of 37.3% and 42% compared to other solutions due to the lightweight computing rules applied in decision-making processes. In addition, the faults are detected at the beginning of communication and marked as faulty communication associations with the help of the system log and appropriate network conditions. The proposed AI-SASC model utilizes the user and device feedback in assigning priorities to network resources with trusted links, decreasing the congestion on the IoT systems and attaining smooth, reliable route maintenance for achieving optimized smart services.

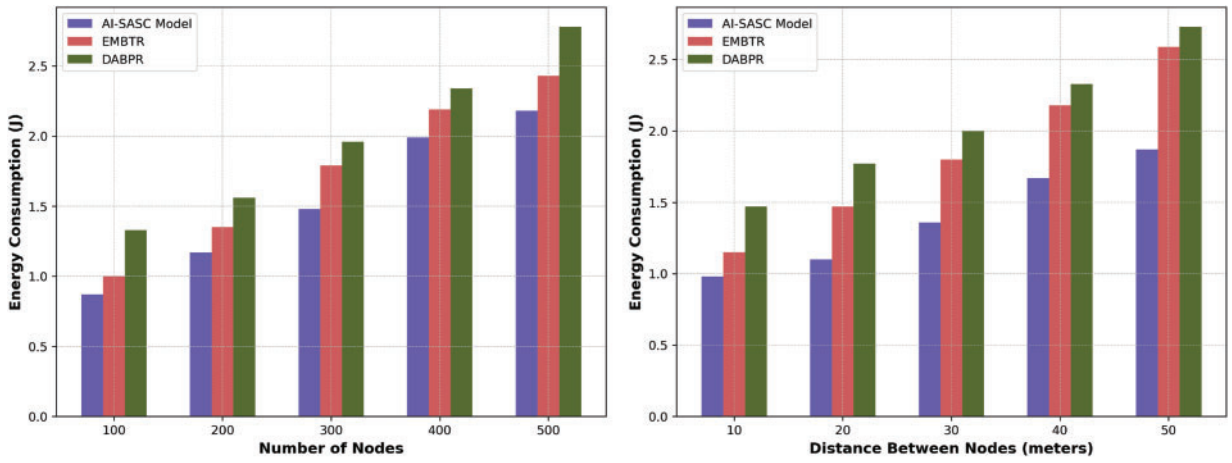
In Fig. 8a,b, the AI-SASC model exhibits improved energy consumption against varying numbers of nodes and varying distances as compared to existing solutions by an average of 29.6% and 36.7%. This is due to the selection and exploration of the most intelligent forwarding schemes while transmitting the routing data. The mult-attributed computation of fitness evaluation ensures the reliable channels based on the

sentiment score. Moreover, the energy efficiency of the proposed AI-SASC model is significantly improved by selecting optimal routing paths based on multi-attribute fitness, which includes latency, reliability, fault tolerance, and user sentiment. The intelligence of the genetic algorithm decreases the network disruption in routing the IoT data and effectively tackles the energy resource of the constraint devices. The device responses play an additional role in preventing the energy hole near the source nodes and ultimately enhance the stability of the management of big data in real-time applications.



(*a*) Security Overhead vs. number of nodes. (*b*) Security Overhead vs. distance between nodes.

Figure 7: Comparison of AI-SASC, EMBTR, and DABPR for security overhead under varying nodes and distances



(*a*) Energy Consumption vs. number of nodes. (*b*) Energy Consumption vs. distance between nodes.

Figure 8: Comparison of AI-SASC, EMBTR, and DABPR for energy consumption under varying nodes and distances

5 Conclusion

Smart cities are increasingly incorporating the technology of IoT and future networks for the growth of smart communication systems. However, many existing approaches often struggle to overcome the research challenges of optimization and allocation of resources for constrained applications. With the integration of

sentiment analysis, the proposed model contributes to real-world smart city infrastructures by improving the way users understand their experiences and promoting more responsiveness with reliable schemes. Advanced data analysis, processing techniques, and strengthened security architecture enable prompt response in decision-making capabilities. In addition, it provides proactive threat mitigation and offers a trusted smart system. Moreover, utilizing a genetic algorithm, our proposed model enhances semantic analysis to attain fault tolerance, service reliability, and smart traffic management by observing the network behavior and device feedback. However, as the number of mobile devices increases, the proposed model may raise the issues of scalability while analyzing big data. Furthermore, leveraging advanced machine learning techniques with sentiment analysis can lead to growth in the development of more resilient and efficient smart systems.

Acknowledgement: This work was funded by the Deanship of Graduate Studies and Scientific Research at Jouf University under Grant No. DGSSR-2024-02-01011.

Funding Statement: This research was supported by the Deanship of Graduate Studies and Scientific Research at Jouf University under Grant No. DGSSR-2024-02-01011.

Author Contributions: The authors confirm contributions to the paper as follows: Conceptualization: Menwa Alshammeri, Mamoona Humayun; methodology: Menwa Alshammeri, Mamoona Humayun, Khalid Haseeb; software: Ghadah Naif Alwakid, Khalid Haseeb; validation: Ghadah Naif Alwakid, Mamoona Humayun; formal analysis: Menwa Alshammeri, Ghadah Naif Alwakid; investigation: Mamoona Humayun, Ghadah Naif Alwakid; resources: Menwa Alshammeri; data curation, Mamoona Humayun, Khalid Haseeb; writing—original draft preparation: Menwa Alshammeri, Mamoona Humayun; writing—review and editing: Ghadah Naif Alwakid, Khalid Haseeb; visualization: Khalid Haseeb, Ghadah Naif Alwakid; supervision: Mamoona Humayun, Menwa Alshammeri; project administration: Menwa Alshammeri, Ghadah Naif Alwakid; funding acquisition: Menwa Alshammeri, Mamoona Humayun. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: Not applicable.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

References

1. Ahmad T, Zhang D. Using the internet of things in smart energy systems and networks. Sustain Cities Soc. 2021;68(1):102783. doi:10.1016/j.scs.2021.102783.
2. Pandurangan P, Rakshi AD, Sundar MSA, Samrat AV, Meenambiga S, Vedanarayanan V, et al. Integrating cutting-edge technologies: aI, IoT, blockchain and nanotechnology for enhanced diagnosis and treatment of colorectal cancer—a review. J Drug Deliv Sci Tech. 2024;91(1–2):105197. doi:10.1016/j.jddst.2023.105197.
3. Ahmed K, Dubey MK, Kumar A, Dubey S. Artificial intelligence and IoT driven system architecture for municipality waste management in smart cities: a review. Measurement: Sensors. 2024;36(12):101395. doi:10.1016/j.measen.2024.101395.
4. Jabbar WA, Tiew LY, Shah NYA. Internet of things enabled parking management system using long range wide area network for smart city. Int Things Cyber-Phys Syst. 2024;4(4):82–98. doi:10.1016/j.iotcps.2023.09.001.
5. Xu QA, Chang V, Jayne C. A systematic review of social media-based sentiment analysis: emerging trends and challenges. Decision Analyt J. 2022;3(2):100073. doi:10.1016/j.dajour.2022.100073.
6. Soubraylu S, Rajalakshmi R. Hybrid convolutional bidirectional recurrent neural network based sentiment analysis on movie reviews. Computat Intellig. 2021;37(2):735–57. doi:10.1111/coin.12400.
7. Li X, Liu H, Wang W, Zheng Y, Lv H, Lv Z. Big data analysis of the internet of things in the digital twins of smart city based on deep learning. Future Generat Comput Syst. 2022;128(10):167–77. doi:10.1016/j.future.2021.10.006.

8. Ahmed I, Zhang Y, Jeon G, Lin W, Khosravi MR, Qi L. A blockchain- and artificial intelligence-enabled smart IoT framework for sustainable city. Int J Intell Syst. 2022;37(9):6493–507. doi:10.1002/int.22852.
9. Sarker IH, Khan AI, Abushark YB, Alsolami F. Internet of things (IoT) security intelligence: a comprehensive overview, machine learning solutions and research directions. Mob Netw Appl. 2023;28(1):296–312. doi:10.1007/s11036-022-01937-3.
10. Azevedo BF, Rocha AMA, Pereira AI. Hybrid approaches to optimization and machine learning methods: a systematic literature review. Mach Learn. 2024;113(7):4055–97. doi:10.1007/s10994-023-06467-x.
11. Zhang S, Lim WYB, Ng WC, Xiong Z, Niyato D, Shen XS, et al. Toward green metaverse networking: technologies, advancements, and future directions. IEEE Network. 2023;37(5):223–32. doi:10.1109/mnet.130.2200510.
12. Rajagopalan A, Swaminathan D, Bajaj M, Damaj I, Rathore RS, Singh AR, et al. Empowering power distribution: unleashing the synergy of IoT and cloud computing for sustainable and efficient energy systems. Resu Eng. 2024;21(15):101949. doi:10.1016/j.rineng.2024.101949.
13. Deng M, Lyu Y, Yang C, Xu F, Ahmed M, Yang N, et al. Lightweight trust management scheme based on blockchain in resource-constrained intelligent IoT systems. IEEE Internet Things J. 2024;11(15):25706–19. doi:10.1109/jiot.2024.3380850.
14. Oliveira F, Costa DG, Assis F, Silva I. Internet of Intelligent Things: a convergence of embedded systems, edge computing and machine learning. Int Things. 2024;26(9):101153. doi:10.1016/j.iot.2024.101153.
15. Liu T, Liu Q, Chen T. Security management method of public sentiment analysis based on blockchain and edge computing. IEEE Transact Cybern. 2024;54(11):6397–409. doi:10.1109/tcyb.2024.3403923.
16. Karthik M, Soni K, Lokchandar C, Radhamani V. Empowering secure transactions: blockchain-enabled payments with AI sentiment analysis. In: 2024 10th International Conference on Communication and Signal Processing (ICCSP); 2024 Apr 12–14; Melmaruvathur, India. p. 277–82.
17. Luo G, Yuan Q, Li J, Wang S, Yang F. Artificial intelligence powered mobile networks: from cognition to decision. IEEE Network. 2022;36(3):136–44. doi:10.1109/mnet.013.2100087.
18. Panahi U, Bayılmış C. Enabling secure data transmission for wireless sensor networks based IoT applications. Ain Shams Eng J. 2023;14(2):101866. doi:10.1016/j.asej.2022.101866.
19. Gandhi A, Adhvaryu K, Poria S, Cambria E, Hussain A. Multimodal sentiment analysis: a systematic review of history, datasets, multimodal fusion methods, applications, challenges and future directions. Inform Fus. 2023;91(3):424–44. doi:10.1016/j.inffus.2022.09.025.
20. Angamuthu S, Trojovskỳ P. Integrating multi-criteria decision-making with hybrid deep learning for sentiment analysis in recommender systems. PeerJ Comput Sci. 2023;9(4):e1497. doi:10.7717/peerj-cs.1497.
21. Raghunathan N, Saravanakumar K. Challenges and issues in sentiment analysis: a comprehensive survey. IEEE Access. 2023;11:69626–42. doi:10.1109/access.2023.3293041.
22. Zhang P, Xu W, Liu Y, Qin X, Niu K, Cui S, et al. Intellicise wireless networks from semantic communications: a survey, research issues, and challenges. IEEE Commun Surv Tut. 2024 Aug. doi:10.1109/COMST.2024.3443193.
23. Sengan S, Subramaniyaswamy V, Nair SK, Indragandhi V, Manikandan J, Ravi L. Enhancing cyber-physical systems with hybrid smart city cyber security architecture for secure public data-smart network. Future Generat Comput Syst. 2020;112(10):724–37. doi:10.1016/j.future.2020.06.028.
24. Ressi D, Romanello R, Piazza C, Rossi S. AI-enhanced blockchain technology: a review of advancements and opportunities. J Netw Comput Appl. 2024;255(21):103858. doi:10.1016/j.jnca.2024.103858.
25. Kuznetsov O, Sernani P, Romeo L, Frontoni E, Mancini A. On the integration of artificial intelligence and blockchain technology: a perspective about security. IEEE Access. 2024;12:3881–97. doi:10.1109/access.2023.3349019.
26. Bibri SE, Alexandre A, Sharifi A, Krogstie J. Environmentally sustainable smart cities and their converging AI, IoT, and big data technologies and solutions: an integrated approach to an extensive literature review. Energy Informatics. 2023;6(1):9. doi:10.1186/s42162-023-00259-2.
27. Serrano W. CyberAIBot: artificial Intelligence in an intrusion detection system for CyberSecurity in the IoT. Future Gener Comput Syst. 2025;166:107543. doi:10.1016/j.future.2024.107543.

28. Jain DK, Boyapati P, Venkatesh J, Prakash M. An intelligent cognitive-inspired computing with big data analytics framework for sentiment analysis and classification. Inform Process Manag. 2022;59(1):102758. doi:10.1016/j.ipm.2021.102758.
29. Birjali M, Kasri M, Beni-Hssane A. A comprehensive survey on sentiment analysis: approaches, challenges and trends. Knowl Based Syst. 2021;226:107134. doi:10.1016/j.knosys.2021.107134.
30. Zhang Y, Ren Q, Song K, Liu Y, Zhang T, Qian Y. An energy-efficient multilevel secure routing protocol in IoT networks. IEEE Int Things J. 2021;9(13):10539–53. doi:10.1109/jiot.2021.3121529.
31. Abbas S, Javaid N, Almogren A, Gulfam SM, Ahmed A, Radwan A. Securing genetic algorithm enabled SDN routing for blockchain based Internet of Things. IEEE Access. 2021;9:139739–54. doi:10.1109/access.2021.3118948.
32. Khan AF, Hannah Lalitha R, Kalpana Devi S, Rajalakshmi C. A multi-attribute based trusted routing for embedded devices in MANET-IoT. Microprocess Microsyst. 2022;89(1):104446. doi:10.1016/j.micpro.2022.104446.
33. Foko Sindjoung ML, Velempini M, Kengne Tchendji V. ARPMEC: an adaptive mobile edge computing-based routing protocol for IoT networks. Cluster Comput. 2024;27(7):9435–50. doi:10.1007/s10586-024-04450-2.
34. Amiri IS, Prakash J, Balasaraswathi M, Sivasankaran V, Sundararajan T, Hindia MN, et al. DABPR: a large-scale internet of things-based data aggregation back pressure routing for disaster management. Wireless Netw. 2020;26(4):2353–74. doi:10.1007/s11276-019-02122-3.
35. Katoch S, Chauhan SS, Kumar V. A review on genetic algorithm: past, present, and future. Multimed Tools Appl. 2021;80(5):8091–126. doi:10.1007/s11042-020-10139-6.