Received: 13 August 2019 | Revised: 5 October 2019 | Accepted: 8 November 2019

DOI: 10.1002/dac.4272

WILEY

RESEARCH ARTICLE

Performance analysis of wireless sensor networks assisted by on-demand-based cloud infrastructure

Umamaheswari S.

Department of Electronics and Communication Engineering, Kumaraguru College of Technology, Coimbatore, India

Correspondence
Umamaheswari S, Department of Electronics and Communication Engineering, Kumaraguru College of Technology, Coimbatore, India.
Email: umamaheswari.s.ece@kct.ac.in

Summary

The wireless sensor networks composed of tiny sensor with the capability of monitoring the tangible changes for a wide range of applications are limited with the capabilities on processing and storage. Their limited capabilities make them seek the help of the cloud that provides the rented service of processing and storage. The dense deployment of the wireless sensor and their vulnerability to the unknown attacks, alterations make them incur difficulties in the process of the conveyance causing the modifications or the loss of the content. So, the paper proposes an optimized localization of the nodes along with the identification of the trusted nodes and minimum distance path to the cloud, allowing the target to have anytime and anywhere access of the content. The performance of the cloud infrastructure-supported wireless sensor network is analyzed using the network simulator 2 on the terms of the forwarding latency, packet loss rate, route failure, storage, reliability, and the network longevity to ensure the capacities of the cloud infrastructure-supported wireless sensor networks.

KEYWORDS

cloud, infrastructure as service, localization of nodes, performance enhancements, trusted nodes, wireless sensor networks

1 | INTRODUCTION

The tremendous developments of the wireless sensor networks (WSNs) have paved way for its utilization in wider and larger applications that involve the accumulation and tracking of a huge amount of data,[1] and the usage and adopting of the cloud computing are becoming progressively important, making the cloud an essential component of the future internetwork.[2] The WSN composed of tiny sensors deployed in a random manner are very popular in gathering the information related to an object, its physical changes, its position, attributes, etc. The monitoring capabilities of these wireless sensors has made it a prominent component in gathering information for a wide range of applications[3] and also in the areas that are beyond reach. Their low cost and easy installation make them progressively attract the users in employing the WSNs in application that range from the small scale to the large scale. Despite their capabilities, the WSNs are built with the low processing, battery, and storage capacities; this brings them difficulties in processing and storing of the huge amount of content gathered in case of the applications that produce large amount of information. The big data gathered based on the tangible environmental changes from the industries or any other application needs an alternative with the substantial storage and the processing capabilities. So, the WSNs in most of the large-scale application prefer the on-demand cloud

infrastructures that help in the storing, computing, and conveying of the information, eg, in health-care service,[4] in intelligent road transportation,[5] in water quality monitoring,[1] in the industries of hydraulic fracturing,[6] agriculture,[7] real-time continuous monitoring[8] of humidity, air pressure, pollution, temperature, natural, and manmade disasters, the WSNs concentrate only on the monitoring and conveys the content gathered to the cloud infrastructure service providers. The cloud service providers who enable a rented service on the software, platform, and the infrastructure are capable of storing an enormous amount of information by the transparent and the ubiquitous sharing of the infrastructure.[5] So, the WSN could extend its network longevity and reduce the energy consumption by directing the processing of the content and their storage towards the cloud that is quite well at providing the infrastructure as service on pay per use. Apart from the challenges due to the processing and the storing capacities, the WSNs incur challenges in the coverage and the routing due to their nature of deployment and loss of data during the information conveyance due to the attacks, like black hole, Sybil attack, warm hole attack, modification, and selective forwarding, resulting in the alteration of the information, route failures, and delay in the conveyance and forwarding of the data increasing the packet losses. The information gathered from the WSNs become altered or lost due to the above-mentioned reasons before reaching the cloud storage. So, there is a necessity for storage expansion and the data analysis for the WSNs to limit its energy usage along with the protection against vulnerabilities and better coverage in the routing of the information.

So, the paper proposes an optimized deployment of the WSN that helps in improving the network coverage of the wireless sensors along with the protected routing enumerating the trust of nodes and finding the shortest path to the cloud storage, reducing the energy consumption of the nodes that are involved in the storing and the processing, allowing an anytime access of the information from anywhere by the target.

The paper details the related works in Section 2, the proposed work on finding the optimal solution for the deploying of the nodes along with the identification of the trusted nodes and the shortest routing path in Section 3, the analysis of the performance of the cloud infrastructure supported WSNs in Section 4, and the conclusion in Section 5

1.1 | Problem formulation

The WSNs that are capable of monitoring the changes in the physical environment lack in storage due to the low storage capacities. This paves way for a storage requisition to the cloud that rents the storage as the service. So, the wireless sensors take only the responsibility of the monitoring and forwarding of the monitored content to the cloud so that the contents can be viewed at any time they have been requested for. The sensors' dense deployment and the susceptibility of being attacked or altered causes damages to the monitored content from reaching the cloud. Moreover, the energy availability of the nodes also takes an important part in the process of the routing. So, the paper addresses the deployment of the nodes considering the distance of the nodes (D_{nodes}) to the cloud providing a maximum coverage of the network and further proceeds with the routing identifying the nodes based on the trust (T_r) and the energy availability (Er_n) and enumerating the shortest path enumerating the data points (nodes) close to the cloud storage. So, the objectives of the paper is for the following:

1. Localize the nodes enumerating the minimum distance to the targets.
2. Identify the trust of the nodes.
3. Proceed with the routing evaluating the shortest path (evaluating the distance from the node to the destination and the energy availability).

Accordingly, the node arrangement and the routing difficulties are formulated as a G (V, E), where "V" is the set of nodes $\{i_1,i_2,\ldots\ldots . i_n\}$ and E are the edges for the vertices. The two nodes existing are said to be linked if their distance is enumerated to be lesser than the maximum coverage (Max_C) such that (i_1,i_2) are linked when the $D_{nodes}(i_1, i_2) < Max_C$ and the linked nodes are described to be the neighbors. The trust (T_r) of the nodes are evaluated, gathering the certain constraints such as the probability rate of the successful transmission (ST_{Prob}) and the probability of the failure rate (FT_{prob}), the rate of the received content (R_R), and the consistency and inconsistency of the transmitted and the received packets (C_p) and (IC_p), and further, the routing is proceeded identifying the (D_{nodes}) and the available energy (Er_n) of the nodes and evaluating the shortest distance between the nodes.

2 | RELATED WORKS

Botta et al[2] present the survey on the integration of the cloud and the internetwork of things, with the up-to-date information of the cloud and Internet of Things (IoT) integration along with the challenges and the future scope for

the same. Stergiou et al[9] present the survey on the integration of the cloud and the IoT along with the secure connection extension between them by surveying the possible security challenges and presenting the remedies for them. In Doshi et al,[1] the WSNs in the real-time data monitoring is proffered in this paper to reduce the delay in tracking by extending the network capability of the data point, causing a continuous monitoring. In Akyildiz et al,[10] the WSN that is the combination of the MEMS, wireless-communication, and the digital electronics is surveyed based on its tasks, applications, communication architectures, and network protocols along with the discussion for the realization of the sensor networks. In Elhoseny et al,[4] the paper proposes the processing of the large amount of information flow through the IoT to the cloud by employing virtual machines and selection of the proper virtual machines based on the GA, PSO, and PPSO to reduce the waiting time and improve the processing speed for the health care industry. In Aznoli et al,[11] the paper presents the survey on the deployment strategies of the cloud along with the challenges incurred in it and the guidelines for the future study. In Bitam et al,[5] the paper details the employment of the cloud services for the intelligent transport system to avoid the unnecessary, fatalities, and disasters on the road side to enhance safety on the road transportation by developing of the cloud for the vehicular network. In Ojha et al,[7] the paper gives comprehensive reviews of the application of the WSN over the agriculture and the farming application and presents the complete case study in exploring the prevailing solutions from the literature under various categories. In Butun et al,[3] the paper presents the survey on the intrusion detection techniques for the WSNs and the MANETs along with merits, demerits, and the information of the IDS that could be applied in the WSNs. In Saleh et al,[12] the paper address the energy problem of the WSNs using the NN-SRAM method to reduce the total amount of energy in the transmission and the storage. In Van et al,[6] the paper presents the cloud-based services for detecting, localizing, and quantifying the leaks in the methane in the natural gas. In Wang et al,[13] the paper engages the private cloud in the process of the streaming data analytics for fault detection and tracking of the large-scale information gathered by continuous monitoring using the WSN for the IoT. In Guanochanga et al,[8] the secure low-cost pollution monitoring of the air is implemented using the three-layer architecture that consists of raspberry pie, Arduino, and the MQTTP for the processing of the data and transmitting, respectively. Wang et al[14] proffer a fog-based hierarchical structure that employs the WSN in monitoring and performing the data analytics in the fog layer, preventing the energy consumption and detection of the malicious nodes and recovering the misjudged nodes within an acceptable delay. In Rath et al,[15] the paper presents the web-based application software that relies on the cloud server and the data centers for the monitoring of the available resources and allocation of the resources for the wireless mobile network that are subjected to dynamic changes. In Satyanarayanan et al,[16] the symbiotic exploration of the relationship between the edge and the augmented cognition for the low latency access to the powerful infrastructure access by the light weight wearable resources. In Bao et al,[17] the paper proffers a highly trust-based hierarchical routing protocol to deal with the selfish and the malicious sensor nodes. The trust information derived from the communication and the social network-based is used in evaluating the trust of the nodes. In Wang et al,[18] the cloud storage based on the fog computing is presented in the paper to ensure the integrity, availability, and the reliability of the personal data stored in the cloud to ensure the safety of the data by retrieving from both the cloud and the fog eluding the malicious alteration of the data and the cyber threats. In Wang et al,[19] the wireless sensors that are deployed in the nature being prone to a direct attack mislead the information to the unauthorized targets, so the paper reviews the literature available on the secured localization of the nodes along with the problems involved in it. In Savas et al,[20] the paper details the integration of the cloud with the WSNs to extend the capacities of the WSNs and further surveys the trust management of the service addressing the security challenges and enhancing the security of the system. In Chen et al,[21] the paper presents the trust evaluation of the nodes in the MANET to improve the security provision with minimum energy consumption.

3 | PROPOSED WORK

The paper proposes the optimal localization to enhance the network coverage, by enumerating the nodes with the minimum distance from the destination, and proceeds with the identification of the trust of the nodes and estimation of the shortest path using the proactive routing protocols. The localization of the nodes enables in having the shortest route at ease as the localization is done using the distance between the nodes. The flow chart below explains the process in the proposed work. Figure 1 below gives the steps involved in the phases of the proposed work. The information stored in the cloud are reserved permanently allowing an anytime access by the users.

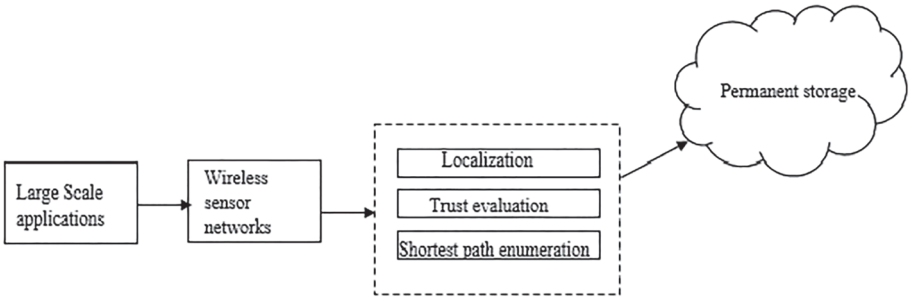

FIGURE 1 Flow of the proposed work

3.1 | Localization of the nodes for enhanced coverage

The coverage, connection, and the accuracy of the network depends on the effective localization of the nodes, as the dense deployment often show inadequacy in achieving the above-mentioned connectivity, accuracy, and coverage due to the distancing between the nodes and the destination or their unavailability within the communication circle of the destination. So, the localization of the nodes become essential. Localization is being a difficult task, as it is to enumerate the prevailing and the picture the future positioning of the sensors; at present, in this paper, we localize the prevailing position of the nodes to locate the nodes nearby the destination to have maximum coverage. Here, the paper employs the ant colony optimization in the localization of the nodes using the foraging behavior of the ant. The ant estimating the shortest route based on the random walk to its food source from the nest is used in the section to identify the nodes within the circle of the target.

The area to be covered is expected to be a two-dimensional plane, with the total area divided into a smaller grids of area 1*1, the area possess a dense deployment of "n" number of nodes, with the coordinates defined for each node and the smaller grid as (x,y) and (x_x, y_x), respectively. A middle point of each grid is picked to represent the whole grid. The space distancing ($dist_{SD}$) the middle point and the node is given as shown in equation (1).

$$dist_{SD} = \sqrt{(x-x_x)^2 + (y-y_x)^2}. \tag{1}$$

In order to reduce the serious problem of the localization and extend a better understanding, the paper utilizes the circular model to detail the coverage for the area to be sensed. The network coverage of the data points (nodes) to the grid is perceived to be in a circular form. Considering the sensor node as the midpoint of the circular area, the points of the grid that lie within the circle is assumed to be under the coverage area, and in the closest position along with the neighbor or the destination and those that lie outside are considered to be out of the coverage range, equation (2) is framed in this regard shows the probability (P_{cov}) of the grid under the coverage

$$P_{Cov} = \begin{cases} 1 & for\ dist_{SD} < radius\ of\ the\ circular\ area \\ 0 & other\ wise \end{cases}. \tag{2}$$

Now, the total ratio of the network coverage (N_c) could be given as the ratio of the covered area (Cov_a) to the area tracked ($trac_a$) that is given as shown in equation (3)

$$N_c = {Cov_a}/{trac_a} \tag{3}$$

To address the problem of the localization and attain an optimal location for the data point, the foraging behavior of the ant is used such that a maximum ratio of the area could be covered Max (N_c).

3.1.1 | Ant colony optimization for optimal localization

The foraging behavior of the ant is utilized to identify the optimal location of the data point that are within the coverage area from the destination. The process starts by the ants with the initial aim of the identification of food, so the ant starts taking the random walk as its initial step in the identification of the food and deposits a fluid called pheromone

in each path it takes so that the other ants could follow the path towards the food without any difficulties. Pheromone deposited on each trail evaporates in due time. The shorter the path it takes, the longer will be the time of evaporation as more will be the density of the pheromone as the path is more frequently used. The steps in the ant colony optimization are as follows:

Step 1.. Initialize a random walk, based on the attractiveness and the pheromone deposit, with the probability ($Prob_{ants}$) given, where ά and ń are the control parameters influencing the τ and ή, respectively, $Prob_{ants} = \frac{[\tau_{AB}]^{\acute{\alpha}} * [\acute{\eta}_{AB}]^n}{\sum_{lc\ X} [\tau_{AB}]^{\acute{\alpha}} * [\acute{\eta}_{AB}]^n}$.

Step 2.. Update pheromone, based on the vaporization coefficient and the deposition amount of the pheromone as $\tau_{AB} = \Delta\tau_{AB} + (1 - p)\tau_{AB}$, p is the vaporization coefficient, and $\Delta\tau_{AB}$ is the deposition amount of the pheromone.

Step 3.. Based on the density of the pheromone updation, the near location of the food that is within the coverage area from the anthill is identified.

Considering the anthill to be the destination, the ants to be the nodes, and the position of the food to be coordinates of the nodes, the ant colony optimization is applied to the localization problem of the data-points helps in arriving at a global optimum for the localization problem, allowing to have a maximum area coverage. The localization of the nodes is very much essential, as the information gathered would become insignificant without the proper localization of the senor nodes.

3.2 | Trust evaluation for the nodes and shortest path routing

The next objective is to evaluate the trust nodes and ensure the safety of the information being transmitted, the sensor deployed in the freely without any control access are liable of being attacked by any modifications and unauthorized devices, so to avoid this the paper employs the nodes evaluated with their trust values for the safe conveyance of the information. The data point within the network coverage is subjected to the trust evaluation based on Chen et al[21] evaluating the direct, indirect, and the combined trust, where Tr_n gives the trust value for the nodes and the NTr_n gives the nontrust values of the nodes. The direct trust of the node is based on the information got from its immediate neighboring nodes that are directly linked, based on the successful (S_{con}) and unsuccessful conveyance, (US_{con}) the rate of the reception (Rep_{rate}) along with the stableness (st_p), and the instability ($InSt_P$) of the data-packets, collected from the node and the neighboring node. Probability of $Direct_{Tr_n}$ information to be gathered from the neighboring nodes is shown in equation (4).

$$Direct_{Tr_n} = \begin{cases} Tr_n = \sum S_{con} + Rep_{rate} + st_p \\ NTr_n = \sum US_{con} + Rep_{rate} + InSt_P, \\ (Tr_n, NTr_n) = 1 - (Tr_n + NTr_n) \end{cases} \tag{4}$$

whereas the indirect trust based on the ITr_n and $INTr_n$ is calculated for two nodes beyond the reach is estimated using an intermediated node, based on the successful (S_{con}) and unsuccessful conveyance, (US_{con}) the rate of the reception (Rep_{rate}) along with the stableness (st_p), and the instability ($InSt_P$) of the data-packets, gathered from the node itself, its immediate neighbor and the indirect neighbor, and the combination trust incorporates both the direct and the indirect trust for the nodes. Equations (5) and (6) give the probability of the trust evaluation for the indirect and the combination trust (Cob_{tr}).

$$InDirect_{Tr_n} = \begin{cases} ITr_n = \sum S_{con} + Rep_{rate} + st_p \\ INTr_n = \sum US_{con} + Rep_{rate} + InSt_P, \\ (ITr_n, INTr_n) = 1 - (Tr_n + NTr_n) \end{cases} \tag{5}$$

$$Cob_{tr} = \left(\sum S_{con} + Rep_{rate} + st_p\right) * Direct_{Tr_n} + \left(\sum US_{con} + Rep_{rate} + InSt_P\right) * InDirect_{Tr_n}. \quad (6)$$

The average trust value (avg_{Tr}) over a number of sensors involved is given as in equation (7).

$$avg_{Tr} = \sum_{nodes=1}^{n} estimated_{trust} \frac{(t)}{n}, \quad (7)$$

where the $estimated_{trust}$ is given by equation (8).

$$estimated_{trust} = M_{Tr} + \left({}^{Prob_{Tr}}/_{Prob_{Tr}} + Prob_{Ntr}\right) * M_{(Tr,NTr)}. \quad (8)$$

Once the trust of the nodes are evaluated, the information conveyance begins identifying the shortest path through in a proactive manner, dissipating the routing request from the destination to identify the nodes at the shortest distance to the destination and the higher distance to the source and gathering the information of the trust of the nodes along with the residual energy availability of the nodes. From the routing reply, the information carrying the details of the nodes regarding the trust, distance, and the residual energy are gathered. The nodes with the maximum of the energy availability and trust along with the minimum distance are gathered and proceeded with the route discovery identifying the shortest path such that the distance to the destination is less and the energy consumption of the transmission is also low.

So, the routing process starts with the initial identification of the path dispatching the request for the routing from the base station (*BS*) towards all the neighboring nodes, the forwarding node (*FN*) in between updates, and the details of the next neighboring node (*NN*) only if the distance of the next neighboring node satisfies equation (9) that enumerates the nodes with the shortest distance from the base station.

$$D(FN, Source) < D(NN, source) \text{ And } D(FN, BS) > D(NN, BS). \quad (9)$$

Further, the routing also takes care of the energy consumption of the transmission, energy required for the transmission between the nodes. *FN* to *NN* are given as the *E*(*FN*, *NN*) and the energy available are given as the *e*(*FN*) and *e*(*NN*), respectively, for the forwarding and the neighboring nodes. The nodes with the minimum energy consumption and the maximum energy availability are identified for the transmission process eliminating the nodes consuming the higher energy consumption. The information gathered are updated in the table with the routing information to proceed with the information conveyance whenever there is a need. The algorithm given below in Figure 2 explains the routing process.

So, the information gathered can be transmitted in a reliable, energy efficient, and the shortest path using the routing method. The information are transmitted to the cloud for the permanent storage using the above-mentioned method. The routing update is done periodically to note down the energy availability and the distance of the nodes to the base station (cloud) as the WSNs are mobile; the new information gathered regarding the nodes are updated to the table for further conveyance.

3.3 | WSN assisted by cloud infrastructure

The information gathered by the WSNs employed for large-scale applications cannot be retained in them due to their low storage capabilities and requires a safer place to store with whenever the need arises. So, the WSNs seek the on demand storage services of the cloud to store the data permanently so that the data can be accessed any time and from anywhere. This helps the WSN to be employed in any large-scale application that has a huge amount of data to be sensed and stored; deploying too many senors for the purpose of storage also would not be economical. So, wireless sensors adapting to the cloud would be a more preferable and economical. The information from the senor being conveyed through the routing path evaluating the trusted nodes and the energy consumption and the shortest distance are transmitted in a safer way to the cloud without any modifications and illegal uses. The flow chart in Figure 3 below explains the information gathered and the steps involved in routing the sensed information to the cloud storage.

FIGURE 2 Proposed Routing Process

Input: All Neighbor Nodes
Output: Updated Routing Table
Start
Initialize neighbor table
Dissipate Request
IF acknowledged
Receive Reply
For all NN
Gather NN-Tr_n
Gather NN-D_{nodes}
Gather NN-Er_n
Enumerate Energy consumption of the path E_p =$[\sum e(NN) - E(FN, NN)]$
Selected NN = (Max (Tr_n)) ∪ (Min (D_{nodes})) ∪ (Max (Er)) ∪ (Min (E_p))
Update Routing Table = Selected NN
Next NN
End
Choose Optimal Route
Convey content with the selected path
Stop

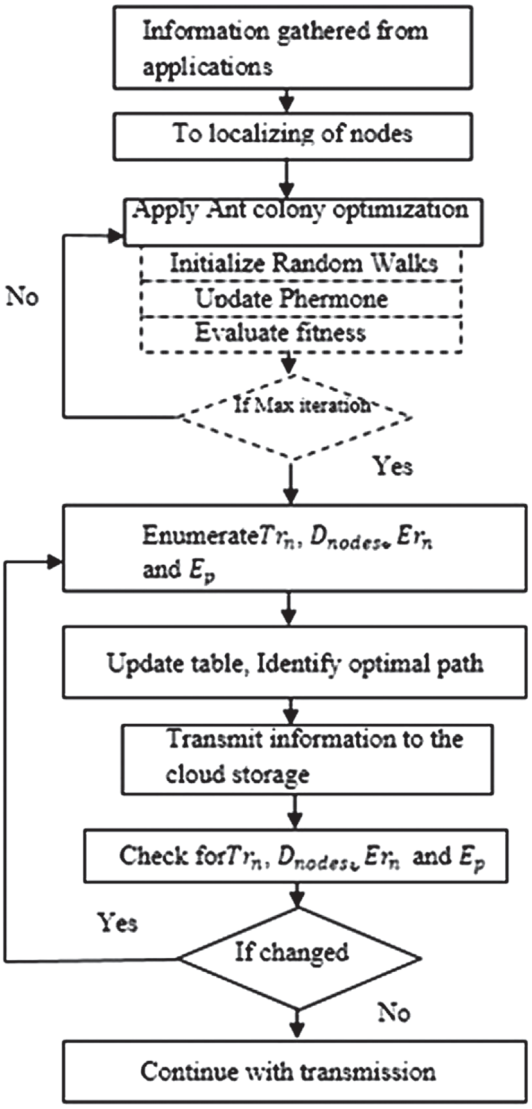

FIGURE 3 Routing of information to cloud

TABLE 1 Simulation parameters

Parameters	Value
Total number of nNodes	500
Simulation time	100 seconds
Simulation aArea	1000*1000 Sq. units^2
Packet sSize	1024 bytes
Packet dData rRate	1 packet per second
Initial eEnergy	100 Joules

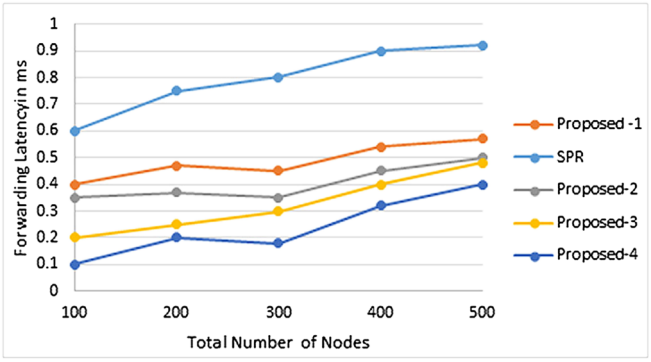

FIGURE 4 Forwarding latency

So, Figure 3 shows the possible information gathered and the transmission to the cloud based on the trustworthy, energy efficient, and the shortest distance routing protocol that enables the safer transmission of the sensed data to the cloud storage for any time access. So, the storage problem in the WSN is addressed by transmitting the information to the cloud and the problem based on the security threats and the during the transmission is addressed using the highly secured trust-based and energy-aware routing method enumerating the shortest distance; the next section presents the result validation of the routing method of the WSN in the transmitting the sensed data to the cloud.

4 | PERFORMANCE ANALYSIS

The proposed routing method that helps in the secure transmission of the information from the WSNs to the cloud storage for the permanent storage is evaluated using network simulator 2 to analyze the performance of the proffered methods with the varying number of nodes ranging from the 100 to 500, with the simulation time 100 seconsds in an allotted area of 1000*1000 m^2 with the packet size of 1024 bytes and transmitting one packet per second and compared with the simple proactive routing that lacks the localization and the trust evaluation. Table 1 below shows the simulation parameters used in the analysis.

The proposed method achieves an optimum localization employing the ant colony optimization, enhances the network coverage and the node arrangement reducing the latency in the process of transmission. This improved coverage of the network enables the base station to identify the nodes with minimum distance and limited energy easily, thus reducing the time consumption in the identification of the nodes and more over the proactive routing method used holding the complete information of all the route available makes easy the conveyance process without any delay.

Figure 4 shows the simulation results of the forwarding delay of the proffered method and its comparison with the other methods involving the simple proactive routing without the aid of the localization and the trust. The results ensure that the proposed method has a reduced forwarding delay compared with the other methods; the simulation on varying number of nodes and multiple iterations shows proficiency of the proposed method in terms of the forwarding latency. Moreover, the trust evaluation enables the information to be to secure, increasing the reliableness in the transmission of the information to the cloud. Employing the trusted nodes enables the transmission to be safe from hacking, unnecessary alterations, and attacks, improving the reliability and security of the data transmission.

Figure 5 shows the simulation results of the reliableness of the proposed method and its comparison with the prevailing method for varying number of nodes. The results for the reliability of the system show that the proposed method

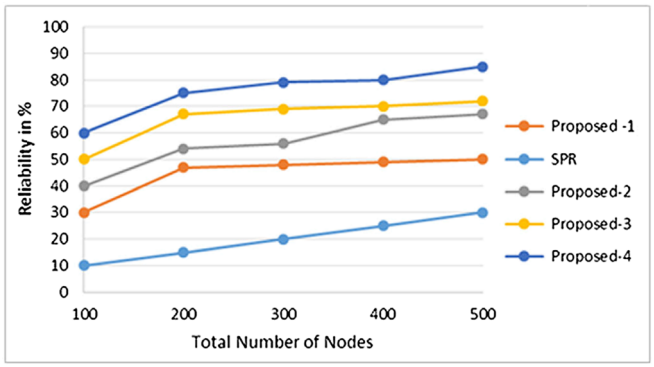

FIGURE 5 Reliability

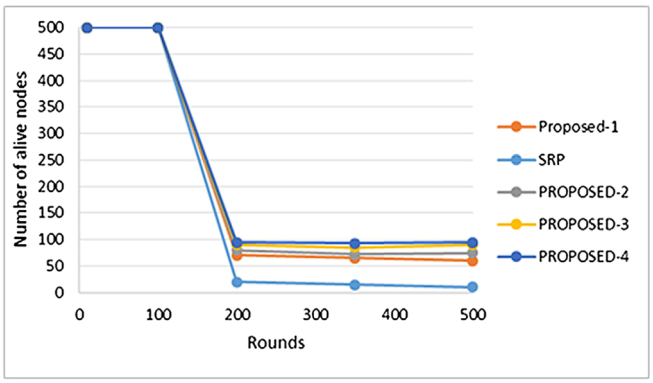

FIGURE 6 Network longevity

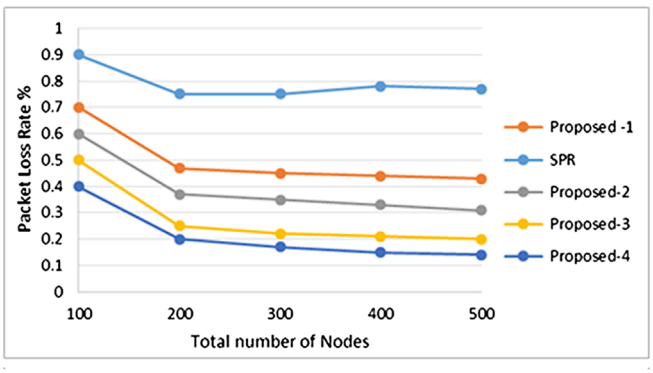

FIGURE 7 Packet loss rate

shows improvement against the security threats and the unknown attacks causing alterations. So, this enables the information stored in the cloud to be reliable, as only trusted nodes eluding the malicious nodes are employed in the routing process. The enhanced network coverage by localization enables in reducing the delay and the path for the conveyance with minimum distance and the minimum energy consumption, enables to have an extended network longevity, reduced route failures, and packet loss rate. Improvement in the network longevity would enable the continuous transmission, thus reducing the route failures. The reliableness of the proposed method and the reduced route failure enables in having a negligible packet losses compared with the prevailing methods.

The simulation result in Figure 6 shows the network longevity of the proffered method along with the comparison of the prevailing method. The obtained results show the network longevity for the varying number of nodes over multiple iterations show that the proposed method enumerating the shortest distance with the path enriched minimum energy consumption nodes, reduces the energy consumption of the network improving the longevity of the network.

Figure 7 gives the simulation result for the packet loss rate. The network routing path enriched with the trusted nodes eluding the malicious unknown attacks, and the routing process with the limited energy utilization extending

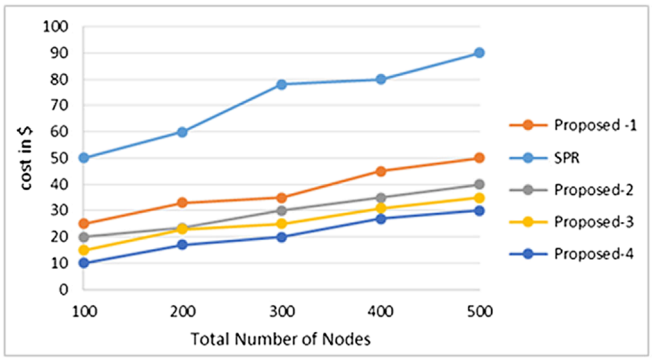

FIGURE 8 Cost of routing

the network longevity limits the packet loss rate. Further, the reduction in the forwarding delay due to the shortest distance path and proper localization of the nodes paves way for the timely delivery of packets without any losses and alterations.

Figure 8 with the analysis on the cost for the proposed method of routing and the other method, and the cost percentage of the proposed method shows considerable improvement than the other method as it does not employ a separate cryptography method but provides a reliable transmission by enumerating the trust of the nodes. The cost of the proposed method over varying number of nodes shows 35% improvement than the prevailing method that employs simple proactive routing without localization and evaluation of the trust.

The proposed method using the rented cloud storage services enables the information to have a permanent storage, making sure the anytime and anywhere access of the information by the user. This causes the WSN to have a continuous monitoring of the content in the large-scale application that has a huge flow of data so the cloud storage becomes essential for the WSN. The extended storage services of the cloud enables the WSNs to be equipped with the additional storage from the cloud. Though using the rented service might result with the additional cost, it would be more preferable as the information finds a permanent storage and could be accessed anytime and anywhere.

5 | CONCLUSION

The WSNs of limited storage uses the rented storage facilities of the cloud to have a permanent storage for the access of information from any place at any time. The information that moved from the WSN to the cloud get affected due to the issues that arise due to the improper coverage, failure of nodes, and the unknown attacks. So, the paper has addressed the issue of coverage by improving the localization of the nodes using the any colony optimization, identifying the trust of the nodes to enhance the protection against the attacks, and the short path with the minimum distance nodes to the destination along with the minimum energy consumption to elude the failure of the nodes due to the lack of battery power and extending the network longevity. The further performance analysis of the WSN routing process using the network simulator 2 shows the efficiency of the proposed method on the grounds of forwarding latency, reliability, network longevity, packet loss rate, and cost of the routing process for the WSN. Future direction of the paper would be lead with the secure retrieval of the information from the cloud storage for further use.

ORCID

Umamaheswari S. https://orcid.org/0000-0002-6151-9602

REFERENCES

1. Doshi S, Dube S. Wireless sensor network to monitor river water impurity. In: *International Conference on Computer Networks and Communication Technologies*. Singapore: Springer; 2019:809-817.
2. Botta A, De Donato W, Persico V, Pescapé A. Integration of cloud computing and internet of things: a survey. *Future generation computer systems*. 2016;56:684-700.
3. Butun I, Morgera SD, Sankar R. A survey of intrusion detection systems in wireless sensor networks. *IEEE communications surveys & tutorials*. 2013;16(1):266-282.

4. Elhoseny M, Abdelaziz A, Salama AS, Riad AM, Muhammad K, Sangaiah AK. A hybrid model of internet of things and cloud computing to manage big data in health services applications. *Future generation computer systems*. 2018;86:1383-1394.
5. Bitam S, Mellouk A, Zeadally S. VANET-cloud: a generic cloud computing model for vehicular ad hoc networks. *IEEE Wireless Communications*. 2015;22(1):96-102.
6. van Kessel TG, Ramachandran M, Klein LJ, et al. Methane leak detection and localization using wireless sensor networks for remote oil and gas operations. In: *2018 IEEE SENSORS*. IEEE; 2018:1-4.
7. Ojha T, Misra S, Raghuwanshi NS. Wireless sensor networks for agriculture: the state-of-the-art in practice and future challenges. *Computers and Electronics in Agriculture*. 2015;118:66-84.
8. Guanochanga B, Cachipuendo R, Fuertes W, et al. Real-time air pollution monitoring systems using wireless sensor networks connected in a cloud-computing, wrapped up web services. In: *Proceedings of the Future Technologies Conference*. Cham: Springer; 2018:171-184.
9. Stergiou C, Psannis KE, Kim B-G, Gupta B. Secure integration of IoT and cloud computing. *Future Generation Computer Systems*. 2018; 78:964-975.
10. Akyildiz IF, Weilian S, Sankarasubramaniam Y, Cayirci E. Wireless sensor networks: a survey. *Computer networks*. 2002;38(4):393-422.
11. Aznoli F, Navimipour NJ. Deployment strategies in the wireless sensor networks: systematic literature review, classification, and current trends. *Wireless Personal Communications*. 2017;95(2):819-846.
12. Saleh N, Kassem A, Haidar AM. Energy-efficient architecture for wireless sensor networks in healthcare applications. *IEEE Access*. 2018; 6:6478-6486.
13. Wang G, Nixon M, Boudreaux M. Toward cloud-assisted industrial IoT platform for large-scale continuous condition monitoring. *Proceedings of the IEEE*. 2019;107(6):1193-1205.
14. Tian W, Zhang G, MD Bhuiyan ZA, Liu A, Jia W, Xie M. A novel trust mechanism based on fog computing in sensor–cloud system. *Future Generation Computer Systems* (2018).
15. Rath M. Resource provision and QoS support with added security for client side applications in cloud computing. *International Journal of Information Technology*. 2019;11(2):357-364.
16. Satyanarayanan M, Davies N. Augmenting cognition through edge computing. *Computer*. 2019;52(7):37-46.
17. Bao F, Chen R, Chang MJ, Cho J-H. Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection. *IEEE transactions on network and service management*. 2012;9(2):169-183.
18. Wang T, Zhou J, Minzhe H, et al. Fog-based storage technology to fight with cyber threat. *Future Generation Computer Systems*. 2018;83: 208-218.
19. Wang H, Wen Y, Lu Y, Zhao D, Ji C. Secure localization algorithms in wireless sensor networks: a review. In: *Advances in Computer Communication and Computational Sciences*. Singapore: Springer; 2019:543-553.
20. Savas O, Jin G, Deng J. Trust management in cloud-integrated wireless sensor networks. In: *2013 International Conference on Collaboration Technologies and Systems (CTS)*. IEEE; 2013:334-341.
21. Chen Y, Lin M, Zheng M, Kai Y. A trust routing protocol based on DS evidence theory in mobile ad hoc network. In: *2014 IEEE/CIC International Conference on Communications in China (ICCC)*. IEEE; 2014:786-790.

How to cite this article: S. U. Performance analysis of wireless sensor networks assisted by on-demand-based cloud infrastructure. *Int J Commun Syst*. 2020;33:e4272. https://doi.org/10.1002/dac.4272