Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 5431413, 9 pages
https://doi.org/10.1155/2022/5431413

*Research Article*

# Routing Path Selection and Data Transmission in Industry-Based Mobile Communications Using Optimization Technique

**Rajendra Kumar Bharti,[1] V. Bhoopathy,[2] Parul Bhanarkar,[3] Kanahaiya Lal Ambashtha,[4] K. Priya,[5] C. Anand Deva Durai,[6] Manam Vamsi Krishna,[7] P. Joel Josephson,[8] and Kibebe Sahile[9]**

[1] *Department of CSE, B. T. Kumaon Institute of Technology, Dwarahat, Almora, Uttarakhand, India*
[2] *Department of Computer Science and Engineering, Malla Reddy College of Engineering, Hyderabad, Telangana, India*
[3] *Department of Computer Science and Engineering, Jhulelal Institute of Technology, Nagpur, Maharashtra, India*
[4] *Faculty of Information Technology, Gopal Narayan Singh University, Sasaram, Bihar, India*
[5] *Department of Computer Science, Marudhar Kesari Jain College for Women, Vaniyambadi, Tamil Nadu, India*
[6] *College of Computer Science, King Khalid University, Abha, Saudi Arabia*
[7] *Computer Science and Engineering, Malla Reddy Institute of Technology, Maisammaguda, Kompally, Hyderabad, Telangana, India*
[8] *Department of ECE, St. Martin's Engineering College, Secunderabad, Telangana, India*
[9] *Department of Chemical Engineering,*
*College of Biological and Chemical Engineering Addis Ababa Science and Technology University, Ethiopia*

Correspondence should be addressed to Rajendra Kumar Bharti; rajendramail1980@gmail.com
and Kibebe Sahile; kibebe.sahele@aastu.edu.et

Received 11 May 2022; Revised 27 June 2022; Accepted 30 June 2022; Published 21 July 2022

Academic Editor: Kalidoss Rajakani

In a mobile network, nodes are share data packets; sometimes, that packets are totally flooding. The packet dropping node does not easily detect for routing time instance. The node trust level is minimum causing the packet loss; it affects the entire network performance, and it reduces throughput and increases communication overhead. Proposed exhaustive routing path allocation (ERP) technique is applied to select the legitimate node for broadcasting the data packets completely. The attacker nodes of that flooding packets are detected by using the legitimate detector which are present in network environment. The node credence level evaluation algorithm is planned to estimating each and every node authority range, whether the nodes have higher credence level basis efficient packet transmission in wireless nodes; otherwise, nodes have lesser credence level basis in effective packet broadcasting. These higher credence level nodes are assigned for communication process in movable network. It improves the throughput and minimizes the communication overhead. The performance metrics of the parameters are delay, communication overhead, throughput, network lifetime, energy consumption, and packet loss.

## 1. Introduction

A mobile ad hoc network is a self-processing dynamic network, comprise of mobile nodes, where all the participating nodes are freely broadcasting data packets from starting point to ending point in wireless network and considered as energetic with various velocity in a random way along the network environment [1]. Therefore, it is extremely not easy to make certain long-term definite route from one node to the various nodes in path. Normally, the mobile network is employed for urgent situation such as service operation, observing the detail of network environment changes, where there is a requirement for packet sharing network instantly subsequent with a few major process, else a few short-term needs such as discussion or class at a novel position where no former network communications are carried, and an optional result is essential [2].

The real-time uses and the widespread use of wireless network mobile nodes have to create the needs to suggest the superiority of service maintained in wireless and mobile networking structure. This is also a vital one to decide the superiority of service of the network environment that is primarily based on the network appearance. In mobile network, there are various metrics which in authority for improving the superiority of service of the network like a transmission rate, packet latency, and packet success ratio [3]. The above-mentioned metrics are enhanced by changing the schemes and techniques.

Characteristically, superiority of service indicates to the ability of a network to provide better service to selected network traffic against a variety of primary methods. Superiority of service routing needs detecting not only for a routing path from a source to a target node but also a path which assures the latency for superiority of service need. Superiority of service is extracomplicated to the assurance in mobile networks than in most various kinds of network structures [4], since the network transmission rate is shared through the neighbouring nodes and the network topology alters owing to the nodes travelling. Therefore, sequentially, to obtain the superiority of service in mobile network, the widespread collaboration among the nodes is necessary to launch the path and to protect the network energy level. Principally, superiority of service can be obtained as overload controlling [5]. The best-effort scheme basically enhanced the residual energy. Otherwise, overloading managing tries to use energy as well to make the network superiority of service aware that includes extra service module.

Superiority of service provisioning improves the latency routine in maximum traffic occurrence in network environment throughout superiority of service aware communication, admission control, resource reservation, overload measurement, and process allocation [6]. The main aim of superiority of service is to obtain the more deterministic network characteristics, anywhere, in turn, the details are carried by the network shared successfully, and network resources are used, though there still residue to a major difficulty to obtain the superiority of service results and continue packet latency for superiority of service with node velocity [7]. The superiority of service provisioning should guide to improve in computational and packet transmission rate. The superiority of service provisioning methods are divided into two groups: inflexible superiority of service and flexible superiority of service methods. Whether superiority of service needs of a link connectivity is assured for the entire process time, the superiority of service method is expressed as inflexible superiority of service method [8].

The mobile network is very difficult to obtain the hard superiority of service certification to use. In flexible superiority of service, the superiority of service needs is not assured for the whole process. There are various difficulties which are in details though offering superiority of service in mobile network such as secreted incurable difficulty, lack of central organization, unconfident intermediate, restricted energy presence, energetically changing network scheme, error-prone combined radio path, and inaccurate state of details [9]. In mobile ad hoc network, one of the most vital mechanisms of a network for superiority of service provisioning is to calculate the condition of the network energy and in that way choose the uses of data for processing. This evaluates the obtainable transmission rate in a seriously overloaded wireless network which is a nontrivial charge considered to the above-mentioned aspect of wireless network environment [10].

The rest of the paper is constructed as follows. Part II provides related works. Part III presents the information of proposed exhaustive routing path allocation (ERP) technique to obtain legitimate node routing along the network path. The node credence level evaluation algorithm is constructed to select the node as higher credence node to provide a route from source to destination node. Part IV provides simulated performance result analysis obtained under various metrics. At last, part V concludes the paper with future work.

## 2. Related Works

Sreevatsan and Thomas [11] present the resource availability-based grouping estimation which takes into account various factors, velocity, energy level, transmission rate, and separation to neighbor nodes for data packet sharing process. After assigning the route between any two nodes comprising a target node of the groups in the routing path, this leads to continuous routes between any two nodes. In the affiliation also, separation of hub nodes to and from assigning the dependability of the system designs and subsequently reconstructing and reestablishing of the network structure is frequently acceptable. Notwithstanding, it is critical to maintain the topology steady as far as it might be efficient. The grouping estimation can collaborate with directing evaluation to find link connection between two nodes. This work primarily comprises three sectors. The primary part comprises purifying the arrangement, which incorporates distinguishing the malicious nodes. The second part comprises the weighted bunching of the network that consolidates another again grouping scheme known as security factor. The third part comprises a fluffy technique to obtain the best route among the routes accessible for steering in view of the lingering vitality and versatility of the hub nodes in the routes.

According to Sharma and Kumar [12], allocation is a route by which numerous strings and procedures get access to network energy. Allocation is the calculation for enhancing the quality by assignment of packets in a waiting state. The communication is forwarding data packets and data along the network from sender to target node. Along these paths, the principle objective is to evaluate the improved path from source node to aim for sending information. The utilized swarm insight locates the optimized route for information forwarding. The packet forwarding path is estimated with the support of resource availability of network.

Hershey et al. [13] present a multilayered progressive movable specially appointed network. This UAS supported to arrange also the given packet forwarding through maximum distance path and high reliability and accomplish higher throughput. Despite the fact that MANET can possibly offer different areas for each given source and target node match, it is critical for each network nodes which need to choose a suitable interchanged packet in path that can fulfill the process necessities and propose an agent-based data transfer capacity reservation method, known as real-time correspondence resource allocator. This scheme tends to the course choice issue by giving a process and design and estimating to allocate the packet transmission speed to an assignment in network and, right now, accessible energy assigned to start communication process.

Abirami and Ramesh [14] present that trust is a social idea executed to provide solution to the directing issue which is an accumulation of recommendations by neighboring nodes about a node before dropping a data. Dependability is a mix of direct trust level estimated by the immediate collaborations and processing the confided computation based on coordinate connections and additionally the assessment about the target by neighbor node. Investigating node trust level is based communication network. It has been thought about against four regular network metrics to be specific throughput and packet blockage. Productivity of those procedures is demonstrated by means of investigation of result.

Kulkarni and Yuvaraju [15] propose a trust-based grouping scheme where the trust level is assessed for each versatile gadget in the network structure, and the gadgets with slightest trust esteem are disposed of as intruder nodes. The nodes are added to the companion list and calculate the trust level. The companions having a most noteworthy trust level are qualified to target nodes. The nodes having slightest trust esteems are considered as noxious and are expelled from the companion list. The calculation represents the accompanying stages: challenge your neighbors, rate your neighbors, and share neighbors and route through neighbor nodes.

Patil and Chandre [16] present credence and neighbor scope-based convention which can enable nodes to rebroadcast the request data just if their combined trust and remaining vitality fall over certain edge. The rebroadcast arrangement is shaped by reliability factor range to limit communication overload. The dependability factor is indicated based on combined credence, remaining vitality, and neighbors secured. A vitality is effective, and most secure route is chosen still within the sight of low vitality, else malicious nodes.

Mukherjee et al. [17] proposed an average processing rate as one of the trust metrics with the aim of "encounter." This is a trust-based communication method named AER-AODV convention which assesses coordinate trust with normal experience rate and effective collaboration recurrence. Roundabout trust is assessed utilizing the modified D-S prove hypothesis. Reenactment comes about demonstrating that AER-AODV should disconnect the malicious nodes adequately when building the routing path. Moreover, it accomplishes preferred execution through the AODV and TAODV as far as tarnsmission rate and packet success rate.

Biswas et al. [18] present a result for distinguishing and removing attack from network and guaranteeing secure packet transmission through the side proficient energy consumption of movable node in the meantime. As indicated by network proposition, assessment of protection of each node in the network structure is based on metrics, such as steadiness of a node characterized by its flexible and waiting time and remaining battery for controlling. This is trust of a node that premised of option of the most dependable course for transmission. The recreation comes about demonstrating that our answer gives great execution as far as throughput, secure directing, and proficient resource utilization.

Xia et al. [19] show the procedure of node trust appraisal depending on node previous characteristic information. At that point, using the protected information succession, weighted Markov stochastic tie measure observes node credence for future basic target node. Test comes about having been guided to assess the adequacy of the present security, as a vital security uses, in view of the standard On-Demand Multicast Routing Protocol, to make four noteworthy upgrades which take the issue of trust into thought and propose a novel trust-based communication method called the On-Demand Trust-Based Multicast Routing method.

Seo et al. [20] show a packet flow estimation linked to the GlobalTrust conspire called as cluster-based global secure to place the packet collected to restrict the execution time, which comprises trust data computational time and intricacy, while satisfying the put stock in steady quality availability. The model number of group is gotten from restricting the purpose of the estimation of many-sided quality resources. Reproduction comes about displaying that the computational time and many-sided quality of credence are controllable and can be utilized adequately in time basic system tasks that require resources for process.

## 3. Overview of Proposed Scheme

The MANET nodes do not share data packets continuously, because nodes make the flooding attacker node. The flooding attack node is not directly found and removed from network structure. Intruder node should obtain that the node trust level is minimum causing the packet loss, it affects the entire network performance, and it minimizes the throughput and improves the communication overhead.

The proposed exhaustive routing path allocation (ERP) technique is used to choose the legitimate node for forwarding data packets perfectly. The flooding nodes are found by using the legitimate detector available in network environment. The node credence level evaluation algorithm is implemented to calculate each node credence level; if node has higher credence level, then it causes efficient packet transmission. If node has lesser credence level, then it causes inefficient packet transmission. These higher credence level nodes are allocated for routing. This enhances the throughput and reduces the communication overhead.

Figure 1 shows the proposed exhaustive routing path allocation (ERP) method. The nodes are ready to perform communication process along the network environment. The packet is flooding during the malicious node activity. Exhaustive routing path allocation is used to assign legitimate node for broadcasting the data packets. Node credence level evaluation algorithm is designed to achieve higher credence level node for path. This technique increases the throughput and reduces communication overhead.

*3.1. Nodes in Routing Path Perform Communication Process.* While a node go into the communication limit based on a particular node resource availability, this should launch recent

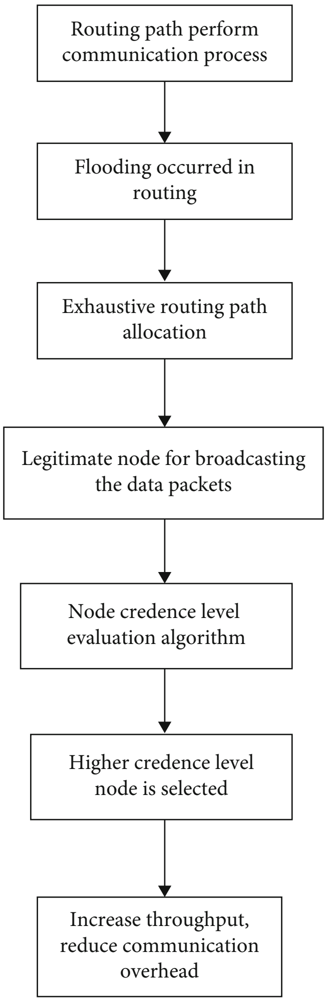

Routing path perform communication process
Flooding occurred in routing
Exhaustive routing path allocation
Legitimate node for broadcasting the data packets
Node credence level evaluation algorithm
Higher credence level node is selected
Increase throughput, reduce communication overhead

Figure 1: Block diagram of exhaustive routing path allocation (ERP) technique.

present paths to a target node which was accessible by a longer path, else earlier in accessible path. The alert packets are transmitted by each node which offer details considering the accessibility of a node as a subsequently hop node, while a node leaves the communication limit of a specified node, and the attacker node is disconnected from the communication table. The probability in the communication table of the node are altered as pursue. For the node is considered as next neighbor hop node, the possibility is made low for every target node from sender node. For the remaining nodes, the possibility distribution is standardized in perfect manner which is the total of the probability higher level. At each node, define two planes of precedence. Each range, connect a backlog at initial time instance of the plan, to use the backlog with maximum precedence for data packets sharing. The data packet sharing depends on the probability at every relay node received by a neighbor node; the packet is again forwarded to the next neighbor node, whether the probability of node is the maximum of all the earlier neighboring nodes, where Rp is the routing path, Lp is the legitimate path, and CN is the credence node

$$\mathrm{Rp} = \mathrm{Lp} + \mathrm{CN}. \tag{1}$$

Transmission rate of node is a difficult problem in mobile network, and they are surveyed by using different techniques; this easily estimates the transmission rate for each node in ad hoc networks. Considering the implementation of every mobile node in the network is constructed with the similar wireless nodes, consequently, every node in the network contains the similar higher transmission rate. Sequence to perform process, for a condition, an uncomplicated scheme depends on measuring the time taken to node observing an inactive route. Different way also to measure amount of time is taken to perform communication process; this is presenting to broadcast the new packets through the link connectivity. At every node, the detail regarding the amount of time taken for the transmission medium is staying full of active. A node need to forward data packet, simply throughout time instance, while neither its direct neighbor nodes nor former nodes in its intrusion limit are broadcasting. Emax is the energy higher, Emin is the energy lower, and CT is continous transmission of packet.

$$\begin{gathered} \mathrm{Lp} = E\max * \mathrm{CT}, \\ E\max = E - E\min. \end{gathered} \tag{2}$$

To calculate the characteristics of the devise scheme using network simulator with different techniques, the routing operates in a way therefore with the source node need to share a surveying data packet next to the lesser node count route to the planned target node to verify its possibility. For the condition of assenting reaction, the target node needs to share a reply packet to sender node, whether not the relaying node transmission rate bound is wrong to forward a unhelpful packet to sender node. Packet delivery rate of its characteristic parameters is calculated, that is, definite as a whole count of communication link requirements explicit to the whole amount of requests; every request packet needs a permanent transmission rate. In simulation, all the calculated techniques were run frequently with recent random request packets on various frequently formed charts. Simulation output indicates that the packet delivery ratio is considered to every of the simulated techniques which improves with respite of the transmission rate restriction to discover also that the presentation of the quality of service routing scheme should be significant one. The data packet loss by occurrence of flooding attacks along the routing path. $R(u)$ is the resource utilization.

$$\begin{gathered} \mathrm{CT} = R(u), \\ \mathrm{Lp} = (E - E\min) * R(u), \end{gathered} \tag{3}$$

While a recent traffic is inwards at a node $n$, at regular intervals, the node $n$ creates a familiar discovery of data packet called familiar routing. This is a transmitted data packet instructed to finding the path between sender node and target node. Every transmitting agent packet has the following fields such as source node IP address, destination node IP address, next hop IP address, load of forwarding route, and count of node. Whether the entry of the present target node does not exist while the broadcasting agent is formed, a communication table access is instantaneously formed.

*3.2. Exhaustive Routing Path Allocation Technique.* Optimization depending on node count can guide to the minimum distance route and also does not provide a successful efficient routing path for wireless network. This offers the usual amount of control packet broadcasting counting again broadcasting to forward sequence of data packets. This routing is biased with parameter performance as a resource of measuring the packet drop rate. Related to the hop count parameter, characteristics also supports to choose the route with lesser rate of packet success. Request packet relaying and reply packet relaying are distinct to appear at the estimation of routing that represent the traffic on the connectivity among node in terms of traffic managing data packets among the alert packets. As every node transmits the alert packet to identify its straight neighbor nodes, request and reply packet can be processed depending on the part of packet drop, thus the possibility of a successful symmetric communication. Display the worth of connection in the way from a sender node to intermediate node. Correspondingly, estimate the amount of well-organized connection in the way from the source node to the intermediate nodes in the path. $Eu(R(u)$ is the energy used for total process.

$$\begin{gathered}\mathrm{Lp} = ER(u) - E \min R(u), \\ ER(u) - E \min R(u) = Eu(R(u). \end{gathered} \tag{4}$$

The link does not dispose to calculate the transmission rate of the connection quality. Simply at the credible network success ratio, every packet broadcasting is performed, and usual data packet transmission is maximum than the probability is used. This denotes a lesser range since it neither differentiates connectivity with various transmission rates except minding the size of data packet. To perform communication process over this issue, the whole time instance required for a data packet relaying providentially to all intermediate node is expressed as process. This varies the packet size to ensemble various physical connection for packet success rate with size of data packet.

Sequence to choose a suitable routing path to assemble the task needs, the task assigner decide the objectives and its qualified precedence for every mission with both the premission and planning parts. Then, the planers analyze the task aims and decide the resource usage, and the required and lesser transmission rate needs to achieve these aims before the process initiates. When the packet sharing route from the sender node to the target node is chosen, every node in the route must convince the task resource needs. To achieve this aim, two procedures are needed: initially, choose a route which should convince the restriction; metrics are packet delay and transmission rate of every node link connectivity. Since each process can contain its individual distinctive needs, this is possible that, given the similar sender node and target node group, for overload to alter the various paths, the legitimate nodes are used to construct the routing path.

$$\mathrm{Lp} = Eu(R(u). \tag{5}$$

The basic problem with the previous communication techniques is that simply for path cost estimated and stored in routing table, and then, the data packet transmitting decision is completed depending to this routing table lacking for entity overload requirements. An new path chosen techniques which having the overload features in the path chosen scheme has already presented to concentrate on this problem. The aim of this investigation is to focal point to control the energy consumption is direct to convince the task needs and energetically alter the transmission rate assigned when the connection breakdown, else transmission rate reduction.

*3.3. Node Credence Level Evaluation Algorithm.* The credence value of routing node is verified before initiating the communication process. The higher level of credence nodes are selected, and remaining nodes are rejected from routing path construction. A routing node becomes a qualified node whether it can arrive at the target node straight else not directly and assure the constraint and transmission rate needs of the task. Classify the accessible rate to be the transmission rate; therefore, all the qualified nodes in the path should differ for this communication process. Primarily, the obtainable transmission rate is fixed to be the required communication range. The changing path was chosen procedure. While accepting a resource maintaining process, this verifies initially whether it is straightlinked to the target node.

$$\begin{gathered}\mathrm{CN} = \mathrm{HCN}, \\ \mathrm{Rp} = Eu(R(u) -+ \mathrm{HCN}. \end{gathered} \tag{6}$$

This observes the transmission rate with lesser energy consumptions and senses connection superiority altering the predefined entrance or connection breakdown. The process for this identification and relay is mentioned. Communication carried out in that network bandwidth reorganization process relates only to the task that contains the previously finished resource condition. Since communication details are verification of the resource limitation and transmission rate needs of a task, subsequent to the reconsideration, this can decide whether it can carry on to maintain the task, else does not depend on the current network conditions and mission's resource needs. Missions without the preceding resource condition contributes to the residual available transmission rate of network based on node credence level.

Node credence level evaluation algorithm is easy to choose the higher credence node for communication process. It improves the attack throughput and reduce communication overhead.

*3.3.1. Packet ID.* Packet ID contains each and every mobile node information. It also has the location of intermediate nodes.

In Table 1, the proposed ERP packet format is shown. Here, the source and destination node ID field occupy 2 bytes. The third one is routing path perform communication process that takes 3 bytes; this nodes are ready to initiate the communication process. The fourth field occupies 2 bytes.

```
Step 1: the nodes are placed in path which are ready for process
Step 2: for each node discover neighboring node
Step3: sender node forward data packet continuously
Step 4: if{ Path == Efficient}
Step 5: legitimate nodes are used
Step 6: that provide the continuous communication
Step 7: else if{Path == breakdown}
Step 9: flooding attack occurred
Step 10: that does not provide continuous communication
Step 11: end if
```

Algorithm 1: For exhaustive routing path allocation.

```
Step 1: estimate the credence level of routing nodes
Step 2: for each node route to destination node
Step 3: if {credence level = high}
Step 4: these nodes are chosen for communication
Step 5: else if {credence level = low}
Step 6: these nodes are does not chosen for communication.
Step 7: end if
Step 8: improve throughput
Step 9: end for.
```

Algorithm 2: Node credence level evaluation algorithm.

Table 1: Proposed ERP packet format.

| Source ID | Destination ID | Routing path perform communication process | Flooding occurred in routing | Exhaustive routing path allocation | Node credence level evaluation algorithm |
|---|---|---|---|---|---|
| 2 | 2 | 3 | 2 | 4 | 3 |

Flooding occurred in routing; the malicious nodes in path should loss or flood the data packets. The fifth occupies 4 bytes; exhaustive routing path allocation is used to choose the legitimate node for routing. The last field is node credence level evaluation algorithm; this selects the higher credence value node to improve throughput, and it occupies 3 bytes.

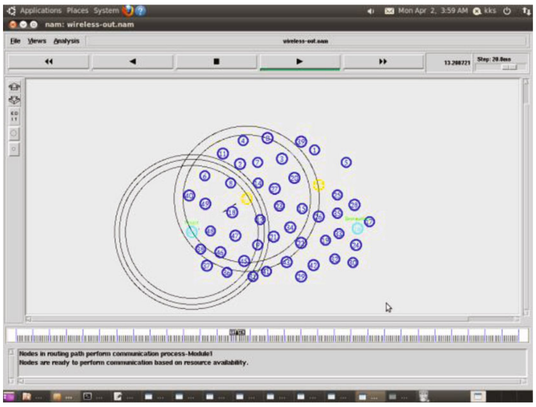
## 4. Performance Evaluation

*4.1. Simulation Model and Parameters.* The proposed ERP is simulated with network simulator tool (NS 2.34). In our simulation, 100 mobile nodes move in an 840-meter × 640-meter-square region for 33-millisecond simulation time. Each mobile node goes random manner among the network in different speed. All nodes have the same transmission range of 250 meters. CBR (constant bit rate) provides a constant speed of packet transmission in the network to limit the traffic rate. AODV (ad hoc on demand distance vector) routing protocol is used to provide maximum network lifetime in mobile network and used node credence level evaluation algorithm to select higher credence value node for routing in path. Table 2 shows simulation setup estimation.

Table 2: Simulation setup.

| | |
|---|---|
| No. of nodes | 100 |
| Area size | 840 × 640 |
| Mac | 802.11 g |
| Radio range | 250 m |
| Simulation time | 33 ms |
| Traffic source | CBR |
| Packet size | 512 bytes |
| Mobility model | Random way point |
| Protocol | AODV |

*4.1.1. Simulation Result.* Figure 2 shows that the proposed exhaustive routing path allocation (ERP) scheme is used to provide legitimate node communication along path compared with existing NLT [19] and RTC [20]. ERP method observes the entire network resource availability and then assign the routing process. Node credence level evaluation algorithm selects the higher credence value node. It reduces communication overhead and increases throughput.



Nodes in routing path perform communication process-Module1
Nodes are ready to perform communication based on resource availability.

Figure 2: Proposed ERP result.

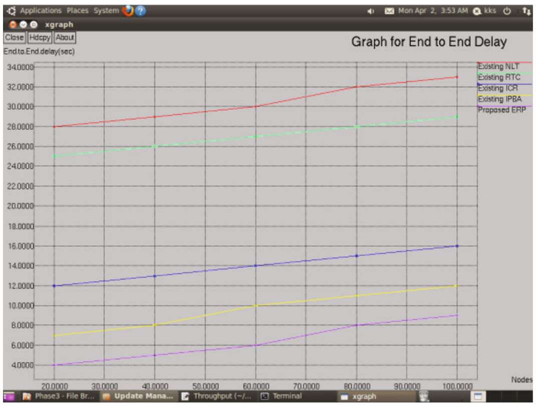


Figure 3: Graph for nodes vs. end-to-end delay.

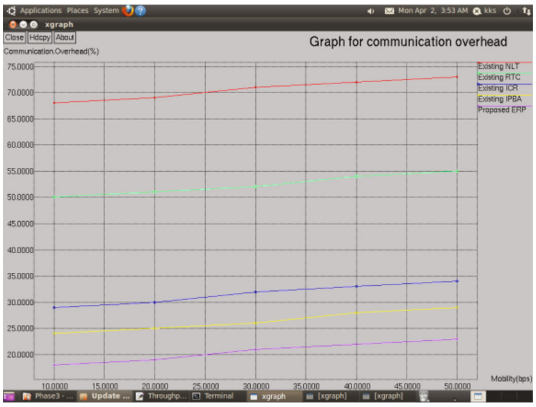


Figure 4: Graph for mobility vs. communication overhead.

*4.2. Performance Analysis.* Simulation analyzes the following performance metrics using X graph in ns2.34.

*4.2.1. End-to-End Delay.* Figure 3 shows end-to-end delay estimated by the amount of time used for packet transmission from the source node to destination node; each node detail is maintained in the routing table. In the proposed ERP method end-to-end, the delay is reduced compared to existing methods NLT, RTC, PBT, and IPBA.

$$\text{EndtoEndDelay} = \text{EndTime} - \text{StartTime}. \quad (7)$$

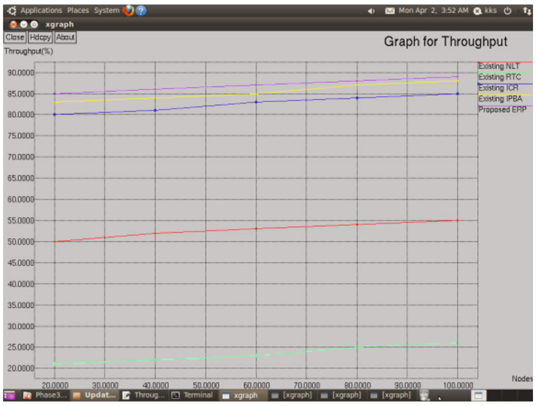


Figure 5: Graph for nodes vs. throughput.

*4.2.2. Communication Overhead.* Figure 4 shows that communication overhead is minimized in which sender transmits the packet to the receiver node; exhaustive routing path allocation (ERP) scheme is used to offer legitimate node communication along path among sender to receiver node. In the proposed ERP method, communication overhead is decreased compared to existing methods NLT, RTC, PBT, and IPBA.

$$\text{Communicationoverhead} = \left(\frac{\text{NumberofPacketLosses}}{\text{Received}}\right) * 100. \quad (8)$$

*4.2.3. Throughput.* Figure 5 shows that throughput is measured by no. of received from no. of a packet sent in particular speed. Node velocity is not constant; simulation mobility is fixed at 100 (bps). Exhaustive routing path allocation (ERP) scheme is used to a chosen intrusion free communication route. In the proposed IPBA method, throughput rate is increased compared to existing methods NLT, RTC, PBT, and IPBA.

$$\text{Throughput} = \left(\frac{\text{Numberofpacketreceived}}{\text{Sent}}\right) * \text{speed}. \quad (9)$$

*4.2.4. Network Lifetime.* Figure 6 shows that lifetime of the network is measured by node process time taken to utilize network from overall network ability. In the proposed ERP method, link connectivity is established, so network lifetime is improved compared to existing methods NLT, RTC, PBT, and IPBA.

$$\text{NetworkLifetime} = \frac{\text{timetakentoutilizenetwork}}{\text{overallability}}. \quad (10)$$

*4.2.5. Energy Consumption.* Figure 7 shows energy consumption, how extended energy spends for communication, that means estimate energy consumption starting energy level to ending energy level. In the proposed ERP method attack free routing inmovable network environment, energy consumption is minimized compared to existing methods NLT, RTC, PBT, and IPBA.

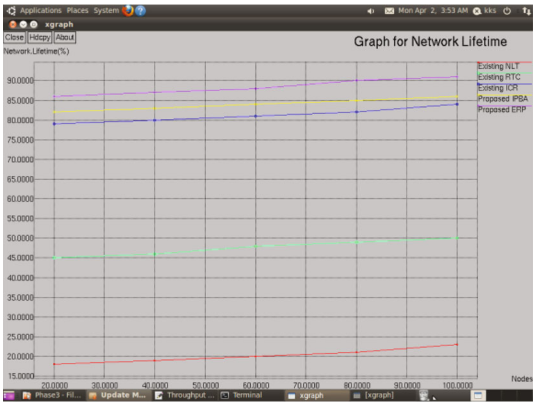


Figure 6: Graph for nodes vs. network lifetime.

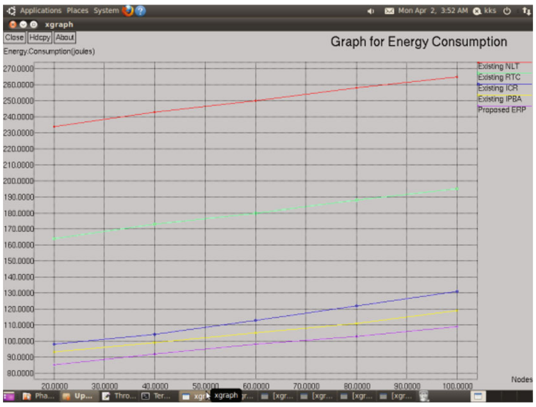


Figure 7: Graph for nodes vs. energy consumption.

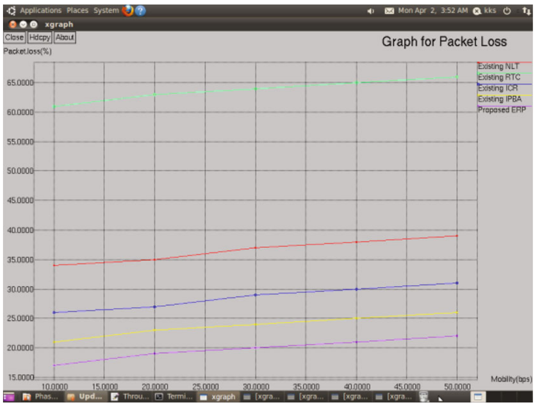


Figure 8: Graph for mobility vs. packet loss.

$$\text{EnergyConsumption} = \text{InitialEnergy} - \text{FinalEnergy}. \tag{11}$$

*4.2.6. Packet Loss.* Figure 8 shows that packet loss of particular communication in the network is calculated by node loss packet with weak connectivity to obtain traffic free communication; the coupling node selection algorithm is designed to select the coupled similar energy node for communication. In the proposed ERP method, packet loss is minimized compared to existing methods NLT, RTC, PBT, and IPBA.

$$\text{Packetloss} = \left(\text{Numberofpacket}\frac{\text{dropped}}{\text{Sent}}\right) * 100. \tag{12}$$

## 5. Conclusion

In general mobile network, nodes are inflexible to nature, since its characteristics are changed every time, causing the data packet flooding during the communication period. The protection level of routing path is varied at a very time. This increases communication overhead and reduces throughput; the proposed exhaustive routing path allocation (ERP) technique is used to select the legitimate node for broadcasting the data packets perfectly. The flooding nodes are identified by using the legitimate detector available in network environment. The node credence level evaluation algorithm is designed to calculate each and every node credence level, if higher credence level nodes are chosen, and remaining nodes are rejected. It improves the throughput and minimizes the communication overhead. In future enhancement, this work can be improved with optimization scheme for efficient routing and unpredictable resource weight age-based path selection in mobile network, to measure various parameters.

## Data Availability

The datasets used and/or analyzed during the current study are available from the corresponding author on reasonable request.

## Conflicts of Interest

The authors declare that they have no conflicts of interest.

## References

[1] Z. Movahedi, Z. Hosseini, F. Bayan, and G. Pujolle, “Trust-distortion resistant trust management frameworks on mobile ad hoc networks: a survey,” *IEEE Communication Surveys and Tutorials*, vol. 18, no. 2, pp. 1287–1309, 2016.

[2] X. Chen, J. Li, J. Weng, J. Ma, and W. Lou, “Verifiable computation over large database with incremental updates,” *IEEE Transactions on Computers*, vol. 65, no. 10, pp. 3184–3195, 2016.

[3] X. Chen, J. Li, J. Ma, Q. Tang, and W. Lou, “New algorithms for secure outsourcing of modular exponentiations,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 9, pp. 2386–2396, 2014.

[4] W. Li, J. Parker, and A. Joshi, “Security through collaboration and trust in MANETs,” *Mobile Networks & Applications*, vol. 17, no. 3, pp. 342–352, 2012.

[5] N. Marchang and R. Datta, “Light-weight trust-based routing protocol for mobile ad hoc networks,” *IET Information Security*, vol. 6, no. 2, pp. 77–83, 2012.

[6] H. Xia, Z. Jia, X. Li, L. Ju, and E. Sha, “Trust prediction and trust-based source routing in mobile ad hoc networks,” *Ad Hoc Networks*, vol. 11, no. 7, pp. 2096–2114, 2013.

[7] R. Khatoun, Y. Begriche, J. Dromard, L. Khoukhi, and A. Serhrouchni, “A statistical trust system in wireless mesh

networks," *Annals of Telecommunications*, vol. 70, no. 4, pp. 29–41, 2015.

[8] A. Elgohary, T. S. Sobh, S. A. Nouh, and M. Zaki, "An efficient and dependable protocol for critical MANETs," *Journal of HighSpeed Networks*, vol. 20, no. 3, pp. 153–168, 2014.

[9] B. Wang, X. Chen, and W. Chang, "A light-weight trust-based QoS routing algorithm for ad hoc networks," *Pervasive and MobileComputing*, vol. 13, pp. 164–180, 2014.

[10] N. B. Truong, T.-W. Um, and G. M. Lee, "A reputation and knowledge based trust service platform for trustworthy social Internet of Things," in *Proc. 19th International ICIN Conference- Innovations in Clouds, Internet and Networks*, pp. 104–111, China, 2016.

[11] A. P. Sreevatsan and D. Thomas, "An optimal weighted cluster based routing protocol for MANET. In data mining and advanced computing (SAPIENCE)," in *2016 International Conference on Data Mining and Advanced Computing (SAPIENCE)*, pp. 310–316, Ernakulam, India, 2016.

[12] P. Sharma and R. Kumar, "Enhanced swarm intelligence-based scheduler to improve QoS for MANETs," in *2014 5th International Conference - Confluence The Next Generation Information Technology Summit (Confluence)*, pp. 340–346, Noida, India, 2014.

[13] P. C. Hershey, S. A. Davidson, and M. C. Wang, "Real-time communications resource allocation process, architecture, and algorithm," *MILCOM 2013 - 2013 IEEE Military Communications Conference*, 2013, pp. 1482–1487, San Diego, CA, USA, 2013.

[14] G. Abirami and S. Ramesh, "An illustrative disquisition on trust based routing techniques in MANET," in *2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)*, pp. 1–4, Coimbatore, India, 2017.

[15] S. B. Kulkarni and B. N. Yuvaraju, "Rating and friend sharing algorithm of trust based clustered routing algorithm in MANETS," in *2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES)*, pp. 843–846, Paralakhemundi, India, 2016.

[16] S. P. Patil and P. R. Chandre, "Trust and neighbor coverage based protocol to improve reliability of routing in MANET," *2016 International Conference on Computing Communication Control and automation (ICCUBEA)*, 2016, pp. 1–5, Pune, India, 2016.

[17] S. Mukherjee, M. Chattopadhyay, and S. Chattopadhyay, "A novel encounter based trust evaluation for AODV routing in MANET," in *2015 Applications and Innovations in Mobile Computing (AIMoC)*, pp. 141–145, Kolkata, India, 2015.

[18] S. Biswas, T. Nag, and S. Neogy, "Trust based energy efficient detection and avoidance of black hole attack to ensure secure routing in MANET," in *2014 Applications and Innovations in Mobile Computing (AIMoC)*, pp. 157–164, Kolkata, India, 2014.

[19] H. Xia, X. Cheng, Y. Zheng, and A. Liu, "A novel light-weight subjective trust inference framework in MANETs," *IEEE Transactions on Sustainable Computing*, vol. 5, no. 2, pp. 236–248, 2020.

[20] S. Seo, J. W. Kim, J. D. Kim, and J. M. Chung, "Reconfiguration time and complexity minimized trust-based clustering scheme for MANETs," *EURASIP Journal on Wireless Communications and Networking*, vol. 2017, no. 1, Article ID 155, 2017.