Indonesian Journal of Electrical Engineering and Computer Science
Vol. 40, No. 1, October 2025, pp. 225~235
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v40.i1.pp225-235

A multi-path routing protocol for IoT-based sensor networks

Udaya Suriya Rajkumar Dhamodharan[1], Krishna Prasad Karani[2], Saranya Pichandi[3], Kavitha Palani[4], Sathiyaraj Rajendran[5]
[1]Department of Computer Science and Engineering, Srinivas University, Mangalore, India
[2]Department of Cyber Security and Cyber Forensics, Institute of Engineering and Technology, Srinivas University, Mangalore, India
[3]School of Computing, Sathyabama Institute of Science and Technology, Chennai, India
[4]Department of ISE, CMR Institute of Technology, Bengaluru, India
[5]Manipal Institute of Technology, MAHE Bengaluru Campus, Karnataka, India

Article Info

Article history:

Received Sep 19, 2024
Revised Apr 18, 2025
Accepted Jul 3, 2025

Keywords:

Internet of things
Multi-path routing protocol
Optimal path
Particle swarm optimization
Shortest path

ABSTRACT

Internet of things (IoT) based sensors are to link a big number of low-cost and power-integrated devices in a reliable manner. Numerous military and adventurous applications are regulated by communication among IoT sensors. The multi-path routing protocol (MRP) approach presented in this research to enhance secure routing in IoT sensors is significant. This technique makes use of data transfer routing and the relationships between network components. It finds the most efficient route between the nodes that minimizes communication overhead and is both reliable and economical in terms of shortest duration. The particle swarm optimization (PSO) technique is used to find the shortest path that is most cost-effective. To reach the target node, end-to-end data transmission must transit via intermediary nodes, which are provided by the routing path node history. The optimal path is chosen by MRP from PSO, and it traces the path to identify the intermediate nodes. In the unlikely event of a crisis, MRP offers the most affordable backup route for data transfer. When compared to earlier techniques, the outcomes of these current approaches enhance network efficiency, balance energy consumption among nodes, and routing attacks.

Corresponding Author:

Udaya Suriya Rajkumar Dhamodharan
Department of Computer Science and Engineering, Srinivas University
Mukka-574146, Mangalore, Karnataka, India
Email: raisingun82@gmail.com

1. INTRODUCTION

The IoT comprises one of the newest technologies in the smart communication space, and because of its benefits, more and more institutions and companies are embracing it on a daily basis [1]. The capacity to accommodate a larger number of devices than those in use today is one of the main features of the introduction of IoT. Imagined potential uses for the internet of things (IoT) include managing communication among billions of connected sensors and radio devices [2]. Numerous applications evaluate and utilize the data that IoT gathers from connected devices over time. However, we haven't typically used IoT data to enhance the network's proficiency and flexibility [3]. This many devices will require a communication platform, which poses new security risks. Attack targets, for example, might not be able to use their smartphones, motor vehicles, or household equipment within such a network. As a result, many studies have offered ways to ensure security and routing in these networks [4]. The variety of linked devices and apps has sharply increased thanks to IoT, providing attackers with more avenues for attack [5]. This study addresses the requirement for a coordinated and effective approach to secure routing and concurrent IoT detection of

attacks. The key objective of this study has been to come up with a complete and useful way to set up secure routing that can spot IoT attacks and fix the problems with older methods of protecting against attacks.

The main contribution of this paper is to provide a protocol for routing that is suitable for IoT based sensor networks, which can address a variety of difficulty in IoT. The current approach can be divided into three categories: single path, low overhead, and flat protocols for routing. The basic goal of the current protocol is to maintain routes as cheaply as possible while lowering routing overhead and improving efficiency. Due to its reactive design, the existing routing protocol has a low propensity for control traffic creation. Many factors need to be taken into account while creating multipath routing algorithms, such as path length and energy usage. One may classify the optimization of network parameters for IoT-based WSN routing operations as a combinatorial optimization challenge. The effectiveness of particle spam optimization (PSO) in resolving the issue is advantageous to our suggested method. The method known as PSO is well-suited for searching routing in contemporary networks of communication because to its features, which include distributed computing, self organization, and positive feedback. For reactive IoT-based WSN, this study suggests a multi-path routing protocol (MRP) based on PSO. Our work's primary goal is to extend the lifespan of networks while preventing routing attacks.

This section examines a few current studies in this area that deal with secure routing on IoT. Routing protocol for low power networks [6] covers a wide range of applications, including linked homes, building automation, industrial monitoring, health care, and transportation. The SRAIOT method, described in [7] article, enhances assured routing in the IoT. The authors of [8] suggest using adversarial confidence perturbation to conceal a variety of confidence distributions in response to various queries, hence protecting against model stealing attacks (also known as APMSA) [9]. Using three methods, this system makes it possible to identify rank distortion assaults in routing. The three types of rank distortion attacks described in this article are decline, increase, and inconsistency of the rank. Within [10], this study aims to build low latency, low-energy consumption, and extremely secure path in the IoT. As a result, the regular rider optimization algorithm (ROA) and the bacterial foraging optimization algorithm (BFO) are combined to create a new method known as the rider foraging optimization algorithm (RFO), which produces an optimal solution—that is, the best route for information transmission.

Gali and Nidumolu [11] proposed a safe routing technique for the IoTs that was based on the deft use of a meta-heuristic strategy to ascertain device authenticity. The CBBMO algorithm (chaotic bumble bees mating optimization) is used in this work to provide safe transmission of data. The BBMO algorithm was enhanced, and for faster convergence, the ideas of chaos theory were incorporated into the CBBMO method. In Kore and Patil [12], a secure routing method for IoT-based smart health networks is presented. It relies on cryptography. Deep learning methods are applied in [13] to protect routing in the IoT-based 5G network.

SDN and blockchain technologies have been utilized in [14] to offer routing safety for the IoT. Using this approach, the network framework is split up into a number of domains, with a controller keeping an eye on each subdomain. A reliable routing technique for the IoTs was developed by research in [15], which depends on the skillful application of a meta-heuristic strategy to determine the legitimacy of components. A node intimacy and credit criterion-based opportunistic and safe routing system for the IoTs was introduced in [16]. This approach aims to address the issue of uneven transmission security and efficiency during the process of delivering messages. The multilevel security routing protocol for IoT that's mentioned in [17] is a different protocol that takes cues from nature. This approach computes the credit of objects and ascertains the data aggregation pattern through the use of the node behavior detection method. The approach described in [18] is likewise a credit-based, safe routing algorithm for the IoTs, with the primary examination of mitigating signal processing assaults.

Hayajneh [19] proposed EECRP-SID method consists of three major steps are cluster formation, optimal path selection, and intrusion detection. utilizing a hybrid heuristic approach, we offer in [20] this research an optimal cluster-based (COOC) algorithm for IoT networks that is conscious of communication overhead. Within [21], in order to provide a concise overview of current energy optimization strategies in WSN, this study evaluates all of the previous energy optimization techniques, classifies and broadly discusses their advantages and disadvantages. There is variation in the available bandwidth between the nodes, ranging from 10 Mbps to 10 Kbps or lower [22]. The routing techniques ought to operate effectively based on the network's available bandwidth. Numerous routing protocols have been developed over time to deal with such issues and challenges [23], [24]. The author proposes a quantum PSO strategy to tackle the QoS broadcast routing methods, which involves first transforming the issue into an integer programming issue, which QPSO is used to solve [25].

2. METHOD

In IoTbased sensor networks, the proposed technique solves issues regards energy, throughput, delay and packet drop. While MRP is an extension and modification of LOARP, it also includes route tracing, maintenance, and repair; it also uses the PSO algorithm to determine the best path among several options. MRP's primary goal is to prolong the life of a network by resolving issues with unidirectional routing. Figure 1 depicts the MRP system method and the general features of the MRP. The information about the source, intermediate, and destination nodes in the optimal path is stacked by MRP. PSO chooses the best route, and the routing table stores the path data. In order to validate the route, MRP transmits the data via the chosen path and tracks the routing information. MRP qualifies the route using RERR messages. The next best path is selected from the PSO routing table as a backup route for route repair if the route is deemed ineligible. Additionally, this path item is deleted from the PSO routing table and the prior path is declared an irreversible failure in the current cycle of data transfer operations. The state automata for MRP includes several states, are route discovery, route-tracing, route-maintenance and data transmission. Each state associates with actions called REQ and RES and ERR. For simplification, state was identified as q0, q1, …, qn.

Let the finite state automata N= $(Q, \Sigma, \Gamma, q_0, q_3)$. Where Q gives set of states, Σ gives set of all input symbols, Γ gives the transition function. $Q = \{q_0, q_1, q_2, q_3\} \Sigma = \{0, 1, \varepsilon\}. \Gamma = Q \, X \, \Sigma, q_0 =$ $startstateofautomata q_3 = finalstateofautomata$. Here input symbol 0 represents RREQ, 1 represents RREP and ε represents RERR. If error message has been traced by any state will directly go to final state and control is handover to the MRP algorithm. The stage-wise functionality of the MRP algorithm is depicted in Figure 2. MRP functionality starts with route discovery, where the route is the best route selected by PSO algorithm.

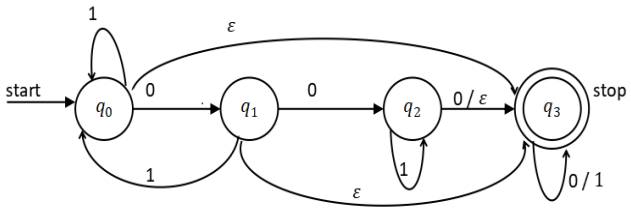

Figure 1. Finite state machine for MRP

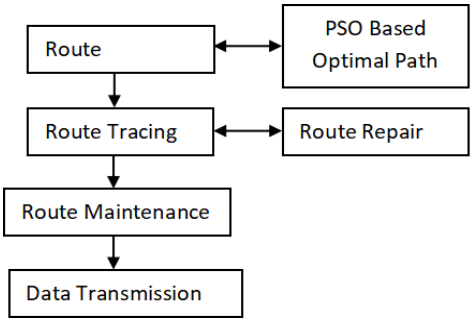

Figure 2. MRP system model

2.1. Route discovery using PSO

One stochastic optimization technique for studying the social dynamics of bird flocks is particle swarm optimization. It is a population-based search strategy in which every person is seen as a particle. A swarm of particles is formed, which stands in for a potential fix for the optimization issue [20]. Every particle travel in a multi-dimensional space, and as a result of their interactions with other particles, they all modify their positions within the searching space. Depending on where their neighboring particles are in relation to the ideal solution, each particle can sit in a better position on its own. location adjustments made repeatedly in an attempt to find the best location may result in the best solution while the search is still in progress. By contrasting the present value with the predetermined fitness value, the best ideal value is found. Since PSO is both more straightforward and sophisticated than GA, it is used in this work to determine the best route. In this paper, PSO is utilized for path discovery, and the information about the created paths is kept in a table known as the PSO table for future verification. Here is the PSO algorithm in Algorithm 1:

Algorithm 1. PSO algorithm
Input: AlltheNodesandlinksbetweenthenodesare representedintheformofadirectedacyclicgroup.
Output: Best, shortestpath
Step-1: Initializethesystem
Step 2: Calculate all the possible paths from Source node to destination node.
Step-3: ForI = 1 toN
Step-4: Generateparticles
Step-5: Applyfitnessfunction
Step-6: Forallparticlesinthesystem

Step-7: Update the position and distance among various nearest neighbour local and global best values
Step-8: Obtain new particles from existing particlesbasedonpersonalbestandglobalbestvalues.
Step-9: EndFor
Step-10: End

The source and destination nodes include all possible intermediate nodes selected as neighbor nodes. Once the nodes and the links between the nodes are initialized into a graph all the possible paths are chosen under various conditions such as less distance, less cost, less travelling time and high energy. The nodes are chosen using depth first search (DFS) iteratively and this path information is stored in PSO table.

2.2. Particles generation

A better path is chosen from the PSO table, from the source to the destination node, and a tree will be formed to constitute a particle. The total number of particles decides the size of the input. The initial fitness function is applied as $F(x) = w_1/tbw * (w_2 * tdel + w_3 * tdel_{jit} + w_4 * tp_{loss})$ for $bestpath_{mindist}$. Where w_1, w_2, w_3, w_4 are constants, tdel is the overall delay, $tdel_{jit}$ is the overall delay jitter, tp_{loss} is the overall loss of the packet and $bestpath_{mindist}$ is the minimum distance path obtained. The fitness method is applied as a minimization function. The parameters used in every tree represent the network model described. The function for fitness then uses these values of parameters as an alternative. Updating the personal best and global best values of each particle within a network has a unique best value associated with it; this number signifies the fitness function value that the particle obtains when measured against the current pbest value. The given formula can be used to determine Pbest amount as (1).

$$\rho_i = \frac{2(n+c)}{2} \forall i = 0, 1, 2, \ldots \quad (1)$$

Where c is a constant factor assumed as 0. n varies from 0 to N (finite natural number). Initially ρ_i value is compared with ρ_{i+1} always to fetch the best value and the gbest is calculated as (2).

$$gbest = \max(\rho_i) \forall i = 0, 1, 2, \ldots \quad (2)$$

Every particle's personal greatest is contrasted with the result that the fitness function returns. The particle's personal greatest is set to the fitness value if the result of the fitness function is smaller than that. The global best value is updated as the sum of all the personal best values once every particle's personal best value has been calculated.

2.3. Obtaining new particle

Old particles to new particles can be acquire and generated according to the pbest andgbest values of the particles. Every particle has a velocity value, which may be computed as (3).

$$V_{new} = w * V_{old} + c_1 * rand( ) * (p_{best} - curr) + c_2 * rand( ) * (g_{best} - curr) \quad (3)$$

Where w, c_1, c_2 $are\ constants$, V_{old} $is\ old\ value\ of\ velocity$, $Rand( )$ $generates\ random\ values$, p_{best} is personal best value of a particle, g_{best} is global best value of a particle, $Curr$ is current particle value and new particle is computed as (4).

$$X_{new} = X_{old} + V_{new} \quad (4)$$

We next apply the preceding procedure to these newly created particles. Gbest value is regarded as the minimal number of supports. This process continues till every particle converge towards the global optimal value. The best possible network among the specified source and destination is represented by this tree.

2.4. Route tracing

If a node is sending data to another node, it may pass via a number of intermediary nodes before selecting the most suitable, shortest path via PSO in the network. The distance that exists among a node and another node determines how many nodes in between are needed. In (5) can be used to retrieve the node's intermediate data that is saved in a routing table during data transmission.

$$\overrightarrow{Sdata} \sum_{i=1}^{f} N_i \overrightarrow{dataD} \quad (5)$$

$\forall i = 1, 2, .. f, fisthenumberofintermediatenodes$, if data travels from source node S to destination node D via intermediary nodes (f). For example: the Node-13 sending a packet of data to Node-23 through Node-16, Node-19 and Node-21. A diagram of the path tracing is shown in Figure 3.

The target node is Node-23, and the packet of data is sent from Node-13 to Node-16, which is the current intermediate node. Additionally, at 10:39, data were received by the intermediate node-16 at 10:42, it passed. For future reference, the aforementioned data is kept in the routing Table 1.

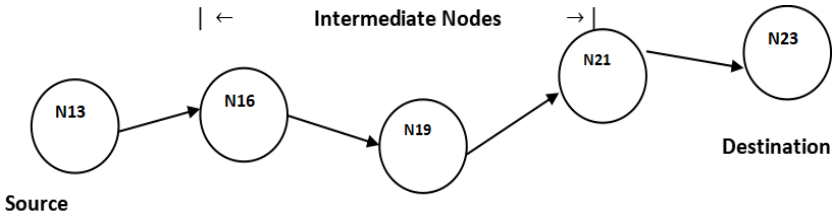

Figure 3. Route tracing

Table 1. Routing table

REC-ID	NODE-ID	REC-TM	SND-TM	DES-ID
Start	13	10:39	10:39	N16
N13	16	10:42	10:42	N19
N16	19	10:45	10:45	N21
N21	23	10:49	Nil	N23/Stop

2.5. Route maintenance

Both the source and the destination nodes might be found anytime on the network and are dynamic. Once multiple paths have been found, the better optimal path is chosen. A routing table is kept up to date with the different routes that have been found as well as the route data for future use. Figure 4 depicts the data transmission among the source and destination nodes.

Theorem-1: $\exists |S| \xrightarrow{DataTx} N_i(f) \rightarrow \exists |D|$// sends a data packet to the destination from each source node. via in between nodes. Let 'S' be a sensor node, then there exists an intermediate node N_i^0 such that for any data transmission, in S such that |S| is pass through N_i to reach 'D'. SolutionS(G) = S(G) – {ε} where, 'G' has number of nodes, it can be rewrite as:S(G) = S – {ε}. Data transmission obtained in 'n' path whose best path of length 'm' since 'G' has m variables. Here longest path has the length $2^{m-1} = n/2$. So, according to a theorem the path $Z(n_i)$ has atleast length of m+1. From the below tree, 'w' is a path that yield, **S → n_2→ n_5→ n_7→ D**. using Top-Down approach and there is no unreachable path. Since S(G) = S – {ε}. Hence it is clear that for all i≥ 0, the source node 'S' included in S(G) which can be parsed through the explored nodes in the path to reach D. The request and response communication among the nodes in a path is defined as Figure 4.

2.6. Route-repair

In order to build a path, each node has the ability to transmit an RREQ message and receive an RREP message. In the event that the route is incorrect or fails, an RERR message is also sent. By having the path automatically repaired, this can be prevented. A link among any two nodes in the network is confirmed by RREQ, RREP.A route failure is conformed by RREQ and RERR. The nodes that are intermediates transmit the RREQ signals in order to fix the issue or discover a different route to the destination since they more closely spaced from the source node to the destination node. Assume that there are K nodes accessible in a path connecting S and D, where S and D are the source and target nodes, respective. You may obtain the path maintenance by:

$$S \xrightarrow{RREQ} N_i^1 \longrightarrow N_{i+1}^2 \xrightarrow{RREQ} \ldots\ldots\ldots\ldots\ldots \xrightarrow{RREQ} D \quad (6)$$

$$S \xleftarrow{RREP} N_i^1 \longrightarrow N_{i+1}^2 \xleftarrow{RREP} \ldots\ldots\ldots\ldots\ldots \xleftarrow{RREP} D \quad (7)$$

$$\left\{Next\ neighbor = N_i^1\ if\ RREQ \leftrightarrow RRES\ is\ valid\ next\ neighbor = N_i^2\ if\ RREQ \leftrightarrow RERR\right\} \quad (8)$$

where, N_i^1, indicates the adjacent in the first level, and N_i^2 represents the alternate neighbor in the second level. Additionally, the following in (5) can be used to determine the distance between two nodes:

$$dist(N_i, N_j) = \sqrt{(x_j - x_i)^2 + (y_j - y_i)^2} \quad (9)$$

In (9) calculates the distance between $N_i$and N_j, where (x_i, y_i) represents the Cartesian coordinate of the node N_i and (x_j, y_j) represents the Cartesian coordinate of the node N_j. In (8) illustrates the RERR message that is produced along a path if the RREQ and RRES are not accurate or on time. With in (6) and (7), a different path can be found at the moment of RERR.

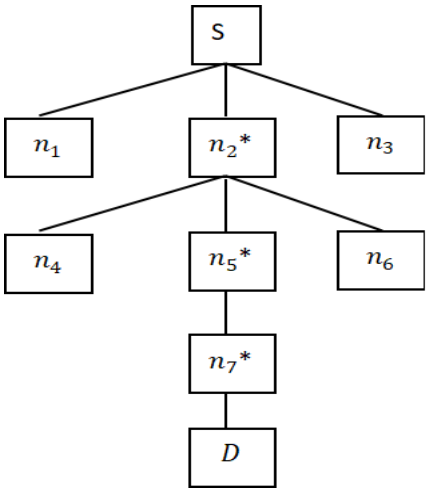

Figure 4. Path tree S(G)

2.7. Energy computation

This suggested framework adopts a well used energy dissipation model. In our model $E_{tx,ij} = \rho + \varepsilon d_{ij}^1$ indicated the joules of energy required to send one bit of data $E_{rx} = \rho$. Also ρ convey the dispersed energy in e, an electronic circuit ε indicates the transmitters' efficiency, ∝indicates the route loss, and d_{ij}, is the distance between N_i (the source node) and N_i (the destination node).

The entire flow, including network building, route discovery, repair, maintenance, data transfer, and energy calculation for a route, is represented by the MRP pseudo code (Algorithm 2). When the energy falls significantly below a threshold, the node state is referred to as dead. The PSO employed in this work finds a path where the nodes have the most energy and the path's length is at its lowest.

Algorithm 2. Algorithm for MRP
Step 1: Start
Step 2: Network$G = (V, E)$, where$V = \{N_1, N_2, \ldots, N_N\}$ // network
Step 3: Location $(N)_i = (rand_x, rand_y)$ // random location
Step 4: $S = rand(N_i)$ and $D = rand(N_j)$ where $i \neq j$ // choose source node and destination node
Step 5: For $I = 1toN$ // node deployment
Step 6: For $x = 1$ to max(X) and For $y = 1$ to max(Y)// X, Y are the width and height of the network area
Step 7: $Node_i.ID = i$
Step 8: $Node_i.X = rand(x)$ and $Node_i.Y = rand(y)$;
Step 9: End X, Y
Step 10: Begin I
Step 11: For $I = 1toN$
Step 12: PSO_dist(Ni, Ni+1)
Step 13: If dist(Ni, Ni+1) <dist // shortest path routing
Step 14: Dist = dist(Ni, Ni+1)
Step 15: $Route_i.SD = add(Node, Node_i)$

Step 16: $\text{Node} \xrightarrow{\text{Link}} \text{Node}_i$
Step 17: $\text{routingTable} = \text{append}(S, \text{route}_i.\text{SD})$
Step 18: Endif
Step 19: End i
Step 20: $\text{RoutingTable} = \text{append}(\text{routingTable}, D);$
Step 21: $\text{ForI} = 1\text{toNIf}\ (\text{routingTable}_i \xrightarrow{\text{link}} \text{routingTable}_{i+1})\ \text{Valid} = \text{true})$ then $\text{Data}.S \rightarrow \text{routingTable}_i$
Step 22: If(message-type == RERR) then
Step 23: RouteRepair(S, D)
Step 24: Endif
Step 25: Step 18: Endfor
Step 26: $E_{init} = 100\text{joules}$
Step 27: $\text{ForI} = 1\text{toN}$
Step 28: $\text{Etx}(k, d) = \text{Etx} - \text{elec}(k) + \text{Etx} - \text{amp}(k, d)$ // energy computation
Step 29: $E_{Tx}(k, d) = E_{elec} * k + E_{amp} * k * d^2$
Step 30: $\text{ForI} = 1\text{toN}$
Step 31: $\text{Update}(\text{Node}_i.\text{Energy})$
Step 32: For I = 1 to N
Step 33: $\text{If}(\text{Node}_i.\text{energy} \leq \varepsilon)\ \text{then}\text{Node}_i.\text{state} = '\ \text{dead}';$
Step 34: $\text{MainNode} = \{\text{mainNode}, \text{deadNode}\}$ // eliminating dead node
Step 35: Else
Step 36: $\text{ForI} = 1\text{tolength}(\text{mainNode})$
Step 37: $\text{MainNode}.\text{energy} = 100\text{Joules};$ // recharging the dead node
Step 38: EndI
Step 39: End

3. RESULTS AND DISCUSSION

The path selection mechanism is first implemented, and then PSO is used to retrieve the optimal path selection. This study investigates the proposed routing protocol MRP, which is an extension of AODV, using the NS2.34. A mobility scenario based on CBR and TCP was created, involving 100 to 500 nodes in a 1500 × 1500 simulation area with 2.0 Mbps and a maximum speed of 120 seconds. The comparison between PSO-based wireless sensor networks for optimal path determination is presented in Figure 5. It shows that fewer iterations were used to find the PSO-WSN's optimal path than the standard WSN.

Figure 6 shows a average packet delivery ratio of 94% and 90% out of 100 nodes, MRP has a PDR of over 99%. On the other hand, for 500 nodes, the PDR is 93% in the suggested approach, 84% in LOARP, and 79% in AODV in the current method. Here X axis shows the number of nodes and Y axis shows the % of the packet delivery ratio. Since it is expected that the nodes are based on mobility, more thought should be given to route discovery and the connections between the nodes because of how frequently they change. PDR calculates the ratio of successfully obtained packets to all packets sent. PDR describes the application's quality in terms of managing congestion.

The throughput based on end-to-end, packet overhead, PDR, and other measures are used to assess MRP efficiency. Throughput is the number of bytes that are effectively received at the destination every second. Figure 7 shows the network's throughput charted, and the quantity of nodes in the network can be changed from 100 to 500 to change the network's size. In the instance of 500 nodes, the throughput in the proposed MRP technique is 93%, whereas in the existing approach, LOARP is 84% and AODV is 81%. Similarly, for 100 nodes, the throughput ratio in the suggested MRP method is 99%, whereas in the existing method, LOARP is 94% and AODV is 93%. The greater throughput as compared to the current method demonstrates the effectiveness of the suggested approach.

The network's end to end delay is plotted in Figure 6 and its size is adjusted by differing the number of nodes in the network from 100 to 500. In the instance of 500 nodes, the end-to-end delay in the proposed MRP technique is 3%, whereas in the existing approach, LOARP is 4% and AODV is 5%. Similarly, for 100 nodes, the end-to-end delay in the recommended MRP method is 12%, whereas in the existing method, LOARP is 18% and AODV is 20%. The lesser end to end delay as compared to the current method demonstrates the effectiveness of the suggested approach. Figure 8 and Table 2, the detection of harmful nodes is presented for 100 to 500 nodes. Compared to other approaches the finding of malicious nodes was high. Figure 9 illustrates the consumption of energy. There are 100 nodes in the network. The average energy consumption rate is illustrated in Figure 10. In contrast to the current method, which uses 5% for AODV and 4% for LOARP, the suggested method uses 2% energy. In a similar vein, the proposed MRP method's energy

consumption for 500 nodes is 7%, while the current method's LOARP is 11% and AODV is 15%. It demonstrates the execution of the proposed technique.

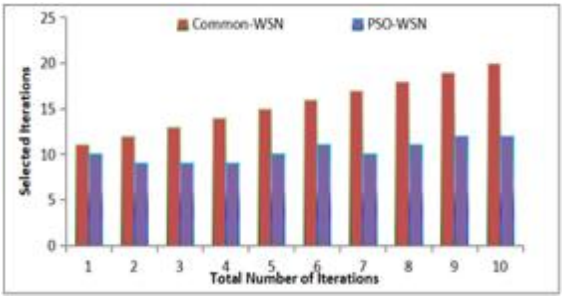

Figure 5. Evaluation of fitness value incur from PSO for WSN and WSN

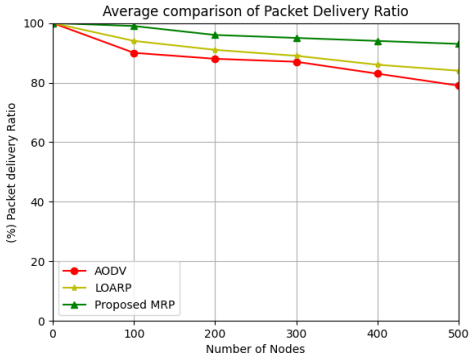

Figure 6. Average packet delivery ratio

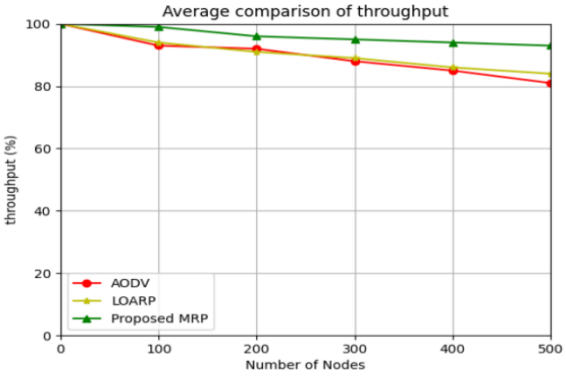

Figure 7. Comparison of throughput

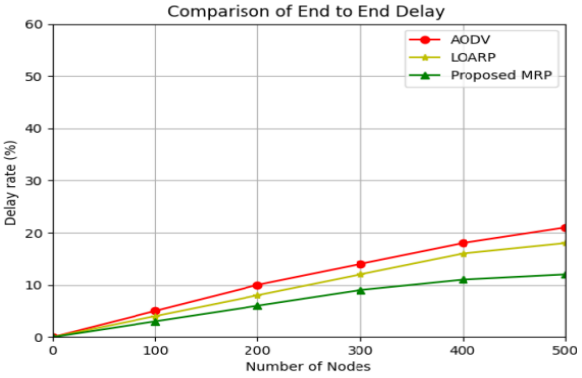

Figure 8. Comparison of end-to-end delay

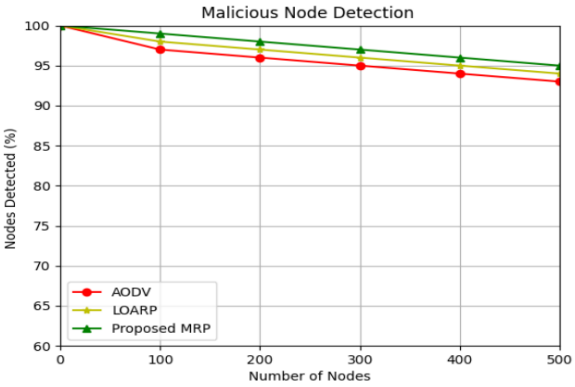

Figure 9. Malicious node detection

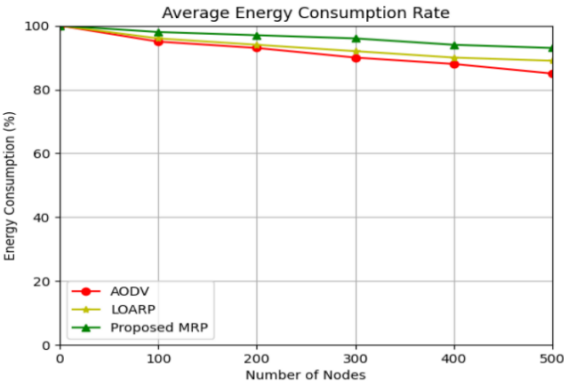

Figure 10. Average energy consumption rate

Table 2. Shows the overall metics available based on the proposed method

Over ALL performance metrics OF proposed multi-PATH routing protocol					
Number OF nodes	% OF energy	% OF delay	% OF throughput	% OF packet delivery ratio	% OF malicious node detection rate
100	98	3	99	99	100
200	97	6	96	98	99
300	96	9	95	98	98
400	94	11	94	97	97
5000	93	12	93	96	96

4. CONCLUSION AND FUTURE WORK

We propose a PSO-based MRP for an IoT-enabled WSN. The protocol is essential for increasing the energy efficiency, robustness, and dependability of communication between nodes. Multi-path routing is useful for real-time data delivery, which is necessary for load balancing and network lifetime extension. For the purpose to identify and route assaults and determine the most effective and suboptimal routes among nodes for dynamically choosing one data transmission path. Optimizing these protocols for diverse IoT contexts still presents difficulties. Future studies should concentrate on developing protocols that can easily scale with the growing number of IoT-based sensors, investigating novel approaches like machine learning for dynamic path selection, and refining protocol design to meet these challenges.

FUNDING INFORMATION

Authors state no funding involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Udaya Suriya Rajkumar Dhamodharan	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓		✓	✓
Krishna Prasad Karani		✓	✓	✓		✓	✓	✓	✓	✓	✓	✓		✓
Saranya Pichandi	✓			✓	✓		✓			✓	✓	✓	✓	
Kavitha Palani	✓	✓	✓		✓			✓	✓				✓	
Sathiyaraj Rajendran	✓		✓	✓	✓	✓	✓			✓	✓		✓	

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

DATA AVAILABILITY

- The data that support the findings of this study are available from the corresponding author, USRD, upon reasonable request.

REFERENCES

[1] Y. Li, X. Su, A. Y. Ding, A. Lindgren and X. Liu, "Enhancing the internet of things with knowledge-driven software-defined networking technology, future perspectives," *Sensors*, vol. 20, no. 12, 2020, 1-20, doi: 10.3390/s20123459.
[2] A. Ahad, M. Tahir, M. A. Sheikh, K. I. Ahmed, and A. Mughees, "Technologies trend towards 5G network for smart health-care using IoT: a review," *Sensors*, vol. 20, no. 14, 2020, pp. 1-22, doi: 10.3390/s20144047.
[3] A. Khanna and S. Kaur," Internet of things (IoT), applications and challenges: A comprehensive review," *Wireless Personal Communication*, vol. 114, no. 2, 2020, pp. 1687–1762, doi: 10.1007/s11277-020-07446-4.
[4] M. El-Hajj, A. Fadlallah, M. Chamoun, and A. Serhrouchni, "A survey of internet of things (IoT) authentication schemes," *Sensors*, vol. 19, no. 5, 2019, pp. 1-43, doi: 10.3390/s19051141.
[5] Z. Shah, A. Levula, K. Khurshid, J. Ahmed, and I. Ullah, "Routing protocols for mobile internet of things (IoT): a survey on challenges and solutions," *Electronics*, vol. 10, no. 19, 2020, pp. 1-29, doi: 10.3390/electronics10192320.
[6] S. Kim, C. Kim, Hyunchong, and K. Jung," A hierarchical routing graph for supporting mobile devices in industrial wireless sensor networks," *Sensors*, vol. 21, no. 2, 2021, pp 1-24, doi: 10.3390/s21020458.
[7] K. Rui and H. Pan, and S. Shu, "Secure routing in the internet of things (IoT) with intrusion detection capability based on software define networking (SDN), and machine learning techniques," *Scientific Reports*, vol. 13, no. 18003, 2023, pp. 1-18, doi: 10.1038/s41598-023-44764-6.
[8] J. Zhang, S. Peng, Y. Gao, Z. Zhang, and Q. Hong, "APMSA: Adversarial perturbation against model stealing attacks," *IEEE Transaction on Information Forensics and Security*, vol. 18, 2023, pp. 1667–1669, doi: 10.1109/TIFS.2023.3246766.

[9] R. Stephen, A. C. Donald, A. D. V. Kumar, B. J. Shanthan, and L. Arockiam, "AROSTEV: A unified framework to enhance secure routing in IoT environment," *Advances in Computational Intelligence and Communication Technology*, vol. 399, 2022, pp. 251–261, doi: 10.1007/978-981-16-9756-2_25.
[10] A. V, Kore and M. R. Mishra, "Trust-based secure routing in IoT network based on rider foraging optimization algorithm," *Journal of High Speed Networks*, vol. 28, no. 1, 2022, pp. 75–94, doi: 10.3233/JHS-2206.
[11] S. Gali and V. Nidumolu, "An intelligent trust sensing scheme with metaheuristic based secure routing protocol for Internet of Things," *Cluster Computing*, vol. 25, no. 3, 2022, 1779–1789, doi: 10.1007/s10586-021-03473-3.
[12] A. Kore and S. Patil, "Cross layered cryptography based secure routing for IoT-enabled smart healthcare system," *Wireless Networks*, 2022, vol. 28, no. 1, pp. 287–301, doi: 10.1007/s11276-021-02850-5.
[13] S. Rajasoundaran *et al.*, "Secure routing with multi-watchdog construction using deep particle convolutional model for IoT-based 5G wireless sensor networks," *Computer Communications*, vol. 187, 2022, pp. 71–82, doi: 10.1016/j.comcom.2022.02.004.
[14] Z. Zeng, X. Zhang, and Z. Xia, "Intelligent blockchain-based secure routing for multidomain SDN-enabled IoT networks," *Wireless Communication and Mobile. Computing*, vol.1 0, no. 1155, 2022, pp. 1-10, doi: 10.1155/2022/5693962.
[15] S. Gali and V. Nidumolu, "An intelligent trust sensing scheme with metaheuristic-based secure routing protocol for Internet of Things," *Cluster Computing*, vol. 25, no. 3, 2022, pp. 1779–1789, doi: 10.1007/s10586-021-03473-3.
[16] L. Yu, G. Xu, Z. Wang, N. Zhang, and F. Wei, "A hybrid opportunistic IoT secure routing strategy based on node intimacy and trust value," *Security and Communication Networks*, vol. 10, no. 1155, 2022, pp. 1-12, doi: 10.1155/2022/6343764.
[17] N. Chandnani and C. N. Khairnar, "Bio-inspired multilevel security protocol for data aggregation and routing in IoT WSNs," *Mobile Networ kand Application*, vol. 27, no. 3, 2022, pp. 1030–1049, doi: 10.1007/s11036-021-01859-6.
[18] G. K. Ragesh and A. Kumar, "Trust-based secure routing and message delivery protocol for signal processing attacks in IoT applications," *Journal of Supercomputing*, vol. 79, no. 3, 2022, pp. 2882–2909, doi: 10.1007/s11227-022-04766-z.
[19] A. Al Hayajneh, M. Z. A. Bhuiyan, and I. McAndrew, "Improving internet of things (IoT) security with software-defined networking (SDN)," *Computers*, vol. 9, no. 1, 2020, pp. 1-14, doi: 10.3390/computers9010008.
[20] S. Alkhliwi, "Energy efficient cluster-based routing protocol with secure IDS for IoT assisted heterogeneous WSN," *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 11, 2020, pp. 405-502, doi: 10.14569/IJACSA.2020.0111162
[21] M. Srinivasulu and G. S. Murthy, "Routing overhead aware optimal cluster-based routing algorithm for IoT network using heuristic technique," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 2, 2023, pp.55-64.
[22] A. P. Kavya and D. J. Ravi, "Snapshot of energy optimization techniques to leverage life of wireless sensor network," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 7, 2021, pp. 122-133, doi: 10.14569/IJACSA.2021.0120714.
[23] U. S. D Rajkumar, P. Shanmugaraja, K. Arunkumar, R. Sathiyaraj and P. Manivannan, "A HSEERP-Hierarchical secured energy efficient routing protocol for wireless sensor networks," *Peer-to-Peer Networking and Applications*, vol. 17, no. 1, 2023, pp. 163-175, doi: 10.1007/s12083-023-01575-w.
[24] U. S. Rajkumar, R. Anand, and Sathiyaraj, "A centralized mechanism for preventing DDOS attack in wireless sensor network," *Wireless Personal Communication*, vol. 10, no. 1007, 2021, pp. 1191-1208, doi: 10.1007/s11277-021-09401-3.
[25] D. Rajkumar, S. Gavaskar, A. F. Al Turjman, R. Sathiyaraj, and B. Balusamy, "Artifcial bee colony method for identifying eaves dropper in terrestrial cellular networks," *Transaction Emerging on Telecommunication Technology*, vol. 10, no. 1002, 2019, pp. 1–17, doi: 10.1002/ett.3941

BIOGRAPHIES OF AUTHORS

Udaya Suriya Rajkumar Dhamodharan is post-doctoral fellow, in Department of Computer Science and Engineering, Srinivas University, Mukka, Mangalore, Karnataka, India. He completed his doctorate degree in Computer Science and Engineering at Sathyabama University. He is having more the 15 years of teaching experience from various reputed institute. He can be contacted at email: raisingun82@gmail.com.

Krishna Prasad Karani currently working as a professor and HOD in the Department of Cyber Security and Cyber Forensics Institute of Engineering and Technology, Srinivas University, Mukka, Mangalore, Karnataka, India. His research interests include fingerprint hash code generation methods and multifactor authentication models. He can be contacted at email: krishnaprasadkcci@srinivasuniversity.edu.in.

Saranya Pichandi is currently working as a assistant professor in the department of computing at Sathyabama institute of Science and Technology. She completed her master degree in Vellore institure of Technology. He attended many national and international conference. Here area of interest in networks, IoT, and machine learning. She can be contacted at email: pramilasaran96@gmail.com.

Kavitha Palani is currently working as a assistant professor in the Department of ISE at CMR institute of Technology. She completed her master degree in Anna University Chennai. He attended many national and international conferences. Here area of interest in IoT, machine learning, and deep learning. She can be contacted at email: kavithapalani.n@cmrit.ac.in.

Sathiyaraj Rajendran is currently working as an associate professor in the Manipal Institute of Technology, Manipal Academy of Higher Education, Bangalore Campus. He received his Ph.D. from Anna University Chennai. His research interests lie in the area of big data analytics, AI, and IoT. He has collaborated actively with researchers in several other disciplines of computer science, particularly traffic prediction systems and intelligent systems. He authored more than 25 publications and filed 5 patents. He can be contacted at email: rsr026@gmail.com.