International Journal of Computer and Engineering Optimization (IJCEO)
Volume 02, Issue 03, May – June (2024)

RESEARCH ARTICLE

DARE-RPL DEEP SEQUENTIAL NEURAL NETWORK BASED AUTHENTICATED ROUTING IN RPL

S.V. Thilagan[1, *]

[1]Assistant professor, Department of Electronics and Communication Engineering, University College of engineering pattukottai, Marudangavayal, Tamil Nadu, 614701, India.

[*]*Corresponding e-mail: go2thilagan@gmail.com*

Abstract – The Internet of Things has been heralded as the most important technical development in recent years due to its low-cost and low-power sensor technology. The IoT makes everyday tasks easier, including smart transportation, smart housing, and smart healthcare, which uses Bluetooth and other low-power wireless technologies in low power lossy network (LLN). The LLN has low throughput and substantial delay due to its traffic patterns, to communicate with resource-constrained sensor devices. To fix this issue RPL is used to solve complicated problems. Routing Protocol for Low-Power and Lossy Networks (RPL) is still working through issues with energy use, scalability, security, and dependability, to name just a few. However, managing all of these challenges in the RPL-IoT network is essential since the RPL contains heterogeneous traffic. In this paper, a novel approach on Deep Sequential Neural Network (DSNN) based Authenticated Routing Enforced RPL (DARE-RPL) is introduced to overcome complex issues in routing and secure transmission of packet. The border router for the LLN network additionally connects the roots to the internet. It has been suggested to use a secure RPL with a congestion avoidance approach to lessen traffic and offer a secure environment. DSNN is the congestion detection method used to avoid congestion in the network during the transmission. The MATLAB simulator is use to evaluate the DARE-RPL technique. The load balancing capacities of the RPI-IOT and MADM current systems are lower for the same set of malicious nodes, at 69% and 58%, respectively, compared to the 93% load balancing capacity achieved by our proposed DARE-RPL.

Keywords *– Routing Protocol for Low-Power and Lossy Networks, Deep Sequential Neural Network, Congestion, Internet of Things.*

1. INTRODUCTION

The IoT has been heralded as the most important technical development in recent years due to its low-cost and low-power sensor technologies [1]. The Internet of Things facilitates everyday tasks including smart transportation, smart housing, and smart healthcare [2]. In order to connect with resource-constrained sensor devices, low-power wireless technologies like Bluetooth are utilized, which have low throughput and significant latency because of their traffic patterns [3]. The International Engineering Task Force (IETF) created a special RPL to address these issues [4]. Due to its restricted resources, it is a crucial routing mechanism for the Internet of Things [5]. RPL is constructed using child nodes and root nodes. ETX is frequently used by RPL as the OF to ensure accurate parent selection. RPL is still working through issues with energy use, scalability, security, and dependability, to name just a few.

The improvement of RPL networks has recently been the target of numerous research projects [6]. However, provenance-based path tracing technology is also used to focus on secure data transmission [7]. Blackholes, sinkholes, wormhole assaults, vampire assaults, hello flooding, Clone ID, Distributed Denial of Service (DDoS), Sybil, and ranking assaults are some of the major attacks that pose a threat to the network environment. future research will concentrate on trickle timer evaluation [8-10]. Following the traditional RPL trickle timer either worsens DODAG stability or increases floods. Therefore, using the best trickle timer is essential for getting better results. The fuzzy method is applied to many metrics, including ETX and energy consumption, for adaptive trickle timers. Many research studies in the field of security provision consider trust evaluation RPL removes rogue nodes from the network using direct and indirect trust values. The comprehensive trust model is constructed using a variety of measures that are based on trust. Rate limiting and isolation are recommended following the mitigating strategies for replay and DIS flooding attacks. For secure and congestion avoidance in routing transmission a novel approach DARE-RPL is developed in this paper using DSNN algorithm for congestion detection in routing.

- The paper's goal is to enhance congestion detection in routing, by implementing Deep Sequential Neural Network (DSNN) techniques.
- The number of resources used and traffic overhead are frequently increased when unauthorised nodes are permitted in construction, as result RPL node authentication technique is used.

- The DSNN has been utilized to investigate for congestion reduction for transmission and to provide an efficient routing protocol.
- Therefore, the routing is enhanced for secure and congestion reduction in DARE-RPL method

The sections that follow are arranged as follows: section 2 represents the literature review, section 3 represent the proposed methodology, section 4 represent the results and discussion, section 5 represent the conclusion.

2. LITERATURE REVIEW

In 2020, Narayan et al, [11] proposed an energy-efficient two-tier cluster-based protocol that partitions the WSN into various levels, which increases the remaining energy of the node and CH. Multiple-level clusters are formed based on variable nodes and the size of the network. The model consists of two phases, network, and protocol. The network is divided into C regions and sub-regions. Based on the distance to the cluster member, one CH is selected at each sub-region, called the Local Cluster Head (LCH). A set of LCHs then selects a Main Cluster Head (MCH). Then MCH transmits data to the sink depending on the bandwidth of the nodes. The results show that as number of nodes deployed is increased, it does not maximize the network's lifetime.

In 2020, Verma et al. [12] proposed a delivered Security breaches are the main issue with the IoT. Routing attacks primarily disrupt IoT networks by modifying and stealing data from them. The bulk of these attempts are discovered by Intrusion Detection Systems (IDS), which take several factors into account. As features, time, flow, and fundamentals are considered. The flow feature comprises the packet type, id, control packet type, transmitter, source, receiver ids, and destination. The basic and time operations also contain a variety of IDS components. The RPL-IoT network's fundamental idea is the trickling timer. As it manages and modifies the network's routing protocol.

In 2020, Solapure et al. [13] developed an objective function that could manage a variety of routing metrics and the traffic from RPL IoT. The function of the energy, content, and ETX variables is used in this study to calculate a composite measure. The ideal parent node in RPL is then chosen using this composite measure. To improve performance, a more effective trickle-timer algorithm is also recommended. The K value in the enhanced trickling timer is calculated using the transmission time, consistency counter, trickle interval, difference between two transmission timings, and redundancy factor. Only a few applications, not sensitive or large-scale data applications, are suitable for this work.

In 2020, Kumar et al. [14] proposed a discussed spam DIS attack mitigation in an RPL context. To prevent malicious nodes, all the data is saved here using both private and public keys. This study reveals the rogue node's MAC address, which was generated arbitrarily. For valid nodes to join the network, this research also generates new piggybacked identities using the trickling process A spam DIS attack is described as an overabundance of DIS and DIO message creation that results in resource waste.

In 2020, Sharma et al. [15] proposed a shortlisting of CHs, based on a fuzzy decision-making method. For CH selection, a fuzzy based Multiple Attribute Decision-Making (MADM) method is used, which is based on three criteria: the number of neighbours, the size of the community, the size of the neighbourhood, the amount of energy remaining, and the distance from the sink to the nodes. MADM compares and ranks alternatives, ranked by the desirability of their characteristics. As the nodes start to die, the number of alive nodes also starts to decrease with cycles, which causes a decrease in information as there are only a few nodes left.

In 2020, Pu et al. [16] proposed a dual context-based route for RPL IoT. Multiple grids are created from the entire network, and each grid's best grid head is chosen using a random walk ranking method. The data must be scheduled by the grid nodes in such a way that congestion is prevented. A variety of factors are taken into account by the adaptive trickle timer, including the volume of incoming DIS, the likelihood of duplicate packets, the number of neighbours, and the distance from the sender node or root node.

In 2021, Alghamdi et al [17]. proposed a clustering model with optimal CH based on four major criteria: which is delay, energy, security, and distance. The optimal CH is chosen here using the Firefly Algorithm Position Update in Dragonfly Algorithm (FPU-DA) model, a new hybrid classifier that manages to combine the ideas of firefly and dragonfly methodologies. The DA algorithm has certain disadvantages like minimum internal memory and low convergence, and firefly also has a constricted convergence rate, so both concepts are combined to solve the optimization problem.

3. PROPOSED METHOD

In this section, a novel approach on DSNN based Authenticated Routing Enforced RPL (DARE-RPL) is introduced to overcome complex issues in routing and secure transmission of packet. The border router for the low power lossy network (LLN) network additionally connects the roots to the internet. It has been suggested to use a secure Routing Protocol for Low-Power and Lossy Networks (RPL) with a congestion avoidance approach to lessen traffic and offer a secure environment. Deep Sequential Neural Network (DSNN) is the congestion detection method used to avoid congestion in the network during the transmission. Figure 1 represents the architecture of proposed DARE-RPL.

3.1. RPL Node Authentication

The first action that our research triggers is node authentication. The number of resources used and traffic overhead are frequently increased when unauthorised nodes are permitted in construction. As a result, we suggest a brand-new Rank-based PUF Validation (R-PUF) method. Physically Unclonable Function (PUF) is an important form of authentication for Internet of Things nodes. The RPL network's central element is rank, which functions similarly. Every node must first register its PUF, MAC address, IP address, ID, and rank in the corresponding sink node to apply PUF and Rank validation in the authentication step. The sink then uses the rank value and sink node ID as inputs to the blowfish technique to generate a secret key for that node.

Energy consumption is decreased by minimising unwanted traffic when assaults are prevented. Only nodes that can be validated using the network's secret key will be considered authentic. The suggested approach generates the highest prime integer as a key, which is impervious to manipulation and increases security. The range from one to n was employed in the proposed blowfish algorithm. The key value is created for this integer.

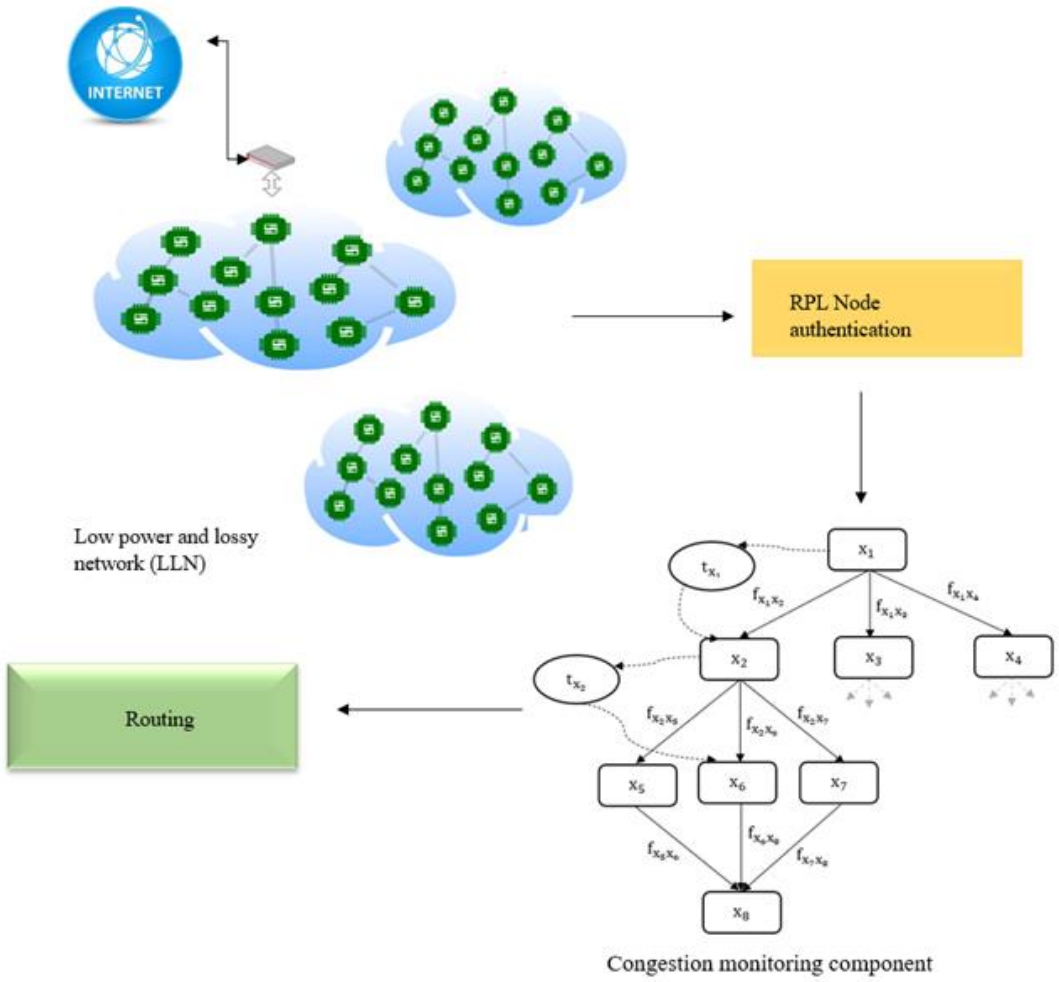

Figure 1. Architecture of proposed DARE-RPL

3.2. Congestion Detection

3.2.1. Deep Sequential Neural Network (DSNN)

Assume that the input space is $Z = \mathbb{R}^z$, and the output space is $W = \mathbb{R}^W$. The dimensions of the input and output spaces are Z and W, respectively. We designate the collection of labelled training instances as $\{(z_1, w_1), \ldots, (z_i, w_i)\}$, where $z_j \epsilon U$ and $w_j \epsilon W$. $\{(z_{i+1}, w_{i+1}), \ldots, (z_S, w_S)\}$ will denote the set of testing examples. The DSNN model has a directed acyclic graph (DAG)-structure defined as follow:

Each node u is in $\{u_1, \ldots, u_N\}$ where N is the total number of nodes of the DAG. The root node is u_1, u does not have any parent node. $d_{u,k}$ corresponds to the k-th child of node u and #u is the number of children of u so, in that case, j is a value be between 1 and #u. leaf(u) is true if node u is a leaf of the DAG - i.e. a node without children.

Each node is linked to a space representation space, denoted as $\mathbb{R}^{dim(u)}$ with dim(u) serving as the corresponding dimension. In conventional neural networks, nodes and layers have the same function. $dim(u_1) = X$, meaning that the root node's equals the model's input dimension. If leaf(x) = true, meaning that the output space dimension of the leaf nodes, then $dim(u) = W$ for any node u.

Mapping functions $f_{u,u'}$ are examined. Functions related to edge (u, u') are $f_{u,u'}: \mathbb{R}^{dim(u)} \rightarrow \mathbb{R}^{dim(u')}$. $Given\ the$ representation x in node u, u' computes a new representation of the input u in node u'. A series of f-transformations applied to the input, much like in a neural network, is the output generated by the model.

Furthermore, every node is linked to a selection function called $t_u: \mathbb{R}^{dim(u)} \rightarrow \mathbb{R}^{\#u}$, which may be used to calculate a score for every child of node x given an input $\mathbb{R}^{dim(u)}$. This function uses the softmax transformation to generate a probability distribution over the children nodes of u, such as, given a vector $y \epsilon \mathbb{R}^{dim(u)}$. The goal of selection functions is to choose a path in the DAG from the root node to a leaf node in order to determine which f-functions to use.

Algorithm
Procedure INFERENCE(x), u is the input vector

$y^{(1)} \leftarrow z$
$u^{(1)} \leftarrow u_1$
q← 1
while not leaf($u^{(q)}$) do
$c^{(q)} \sim t_u(q)(k^{(q)})$
$u^{(q+1)} \leftarrow d_{u^{(q)},c^{(q)}}$
$y^{q+1} \leftarrow f_{u^q,u^{q+1}}(y^q)$
q← $q + 1$
end while
return $y^{(q)}$
end procedure

4. RESULT AND DISCUSSION

This section summarizes the simulation findings and assesses the suggested DARE-RPL using performance indicators. To assess the effectiveness of the suggested DARE-RPL, simulations are run. This part includes two subsections, such as "Simulation setup" and "Comparison study." This section provides a research summary of the proposed DARE-RPL.

Simulation setup:

The network simulator simulates the proposed DARE-RPL model. Table 1 presents network parameters. IoT gadgets, a server, router, and a sink node are all included in the proposed DARE-RPL ecosystem. Congestion mitigation using the suggested DARE-RPL model is tested in a 500×600m simulation setting. Network Parameters is shown in Table 1. Average Energy consumption is shown in Figure 2.

Table 1. Network Parameters

Parameters	Value
Router	1
area	500*600
Simulation time	50s
Simulation rounds	2000
Initial energy	100J
Packet period	15s
No. of packets	10-100 per sec
Initial energy	100J
Sink node	1
Time for encryption	6.928(ns)

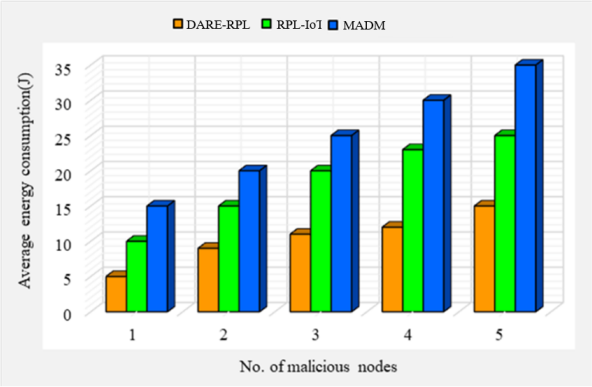

Figure 2. Average Energy consumption

In Figure 2, the RPL-IOT, MADM and the proposed DARE-RPL approaches are compared. The average energy usage increases as more malicious nodes are present. The results show that the suggested method requires less energy than other methods currently in use. When choosing a parent, RPL nodes frequently expend a lot of energy. Energy consumption is decreased by employing the DSNN algorithm, which rapidly chooses the ideal parent and has a high convergence rate. comparison of Delay is shown in Figure 3.

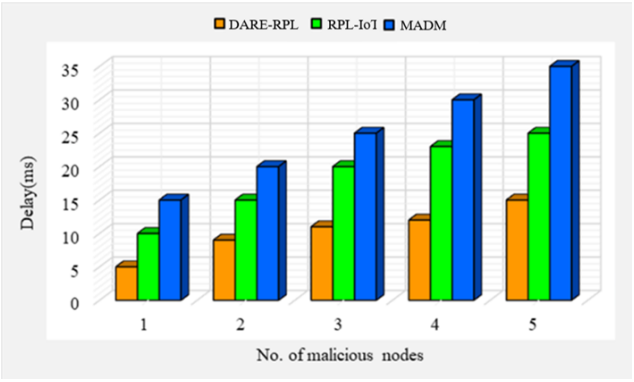

Figure 3. comparison of Delay

The proposed and actual system delays in response to network growth are compared in Figure 3. The comparison results demonstrate that, even with a 100-capacity network, the Sec-RPL method lowers delay by 7 ms. For the same network capacity, the current works, RPL-IOT and MADM, produce significant delays of 13 and 18 milliseconds, respectively. The suggested DARE-RPL reduces the delay by 6 to 9 milliseconds when compared to the current works. Comparison of load balancing capacity with network size is shown in Figure 4.

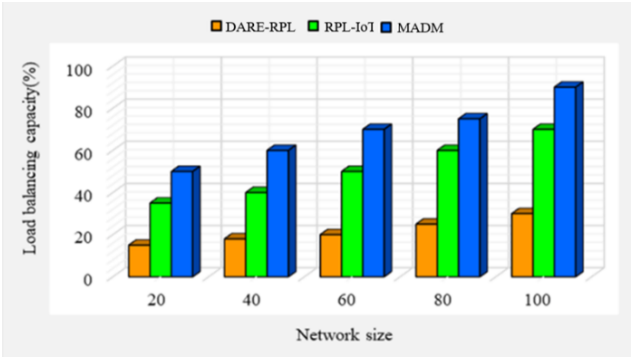

Figure 4. Comparison of load balancing capacity with network size

The load balancing capacities of the RPI-IOT and MADM current systems are lower for the same set of malicious nodes, at 69% and 58%, respectively, compared to the 93% load balancing capacity achieved by our proposed DARE-RPL when there are 5 malicious nodes, as shown by the numerical data in Figure 4. The evaluation reveals that the suggested work performs 35% to 25% better overall than present efforts. The current works, RPI-IOT and MADM only manage 70 and 60 percent load balancing capacity.

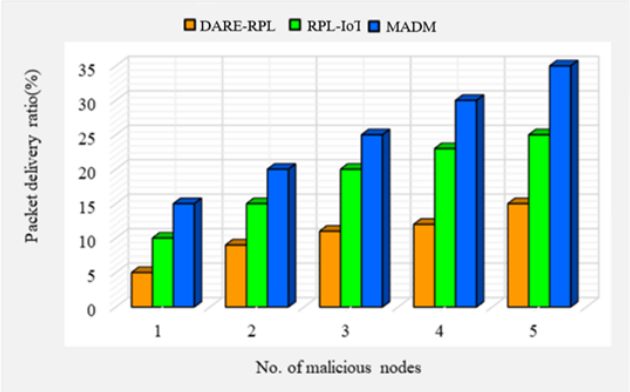

Figure 5. Comparison of packet delivery ratio with network size

The suggested work outperforms the existing works by 24% to 34%, according to the overall measurement. Figure 5 compares the packet delivery ratio to network size, like Figure 5. As the network size increases, the PDR increases. As seen in the figure, the suggested DARE-RPL obtains a high PDR of 90%. The prior works' maximum network sizes were 72% and 70%, respectively, with a lower packet delivery ratio. The suggested effort produces 18%–20% less as compared to earlier programs.

5. CONCLUSION

In this section, a novel approach on DSNN based Authenticated Routing Enforced RPL (DARE-RPL) is introduced to overcome complex issues in routing and secure transmission of packet. The border router for the low power lossy network (LLN) network additionally connects the roots to the internet. It has been suggested to use a secure Routing Protocol for Low-Power and Lossy Networks (RPL) with a congestion avoidance approach to lessen traffic and offer a secure environment. Deep Sequential Neural Network (DSNN) is the congestion detection method used to avoid congestion in the network during the transmission. A DSNN algorithm that takes environmental states like generation status, loss status, and buffer status into account is described for maintaining minimal congestion. The experimental data from this chapter shows that the DARE-RPL achieves high packet delivery ratios of 90%, lower packet loss rates of 15%, load balancing capacities of 91%, lower delays of 7ms, lower energy consumption of 60J, and lower control traffic overhead of 30kb when compared to other methods. For future, routing protocol can be enhanced by using various deep learning algorithm and accuracy can improved.

CONFLICTS OF INTEREST

This paper has no conflict of interest for publishing.

FUNDING STATEMENT

Not applicable.

ACKNOWLEDGEMENTS

The author would like to express his heartfelt gratitude to the supervisor for his guidance and unwavering support during this research for his guidance and support.

REFERENCES

[1] C. J. PuBrown, and L. Carpenter, "Atheil index-Based countermeasure against advanced vampire attack in the internet of things", *IEEE 21st International Conference on High-Performance Switching and Routing (HPSR), INSPEC Accession Number: 19634829*. 2020. [CrossRef] [Google Scholar] [Publisher Link]

[2] M. J. Pushpa, M. K. Sandhya, and K. Murugan, "RPR: Reliable path routing protocol to mitigate congestion in critical IoT applications", *Wireless Networks*, vol. 27, no. 8, pp. 5229-5243. 2021. [CrossRef] [Google Scholar] [Publisher Link]

[3] K. N. Qureshi, S. S. Rana, A. Ahmed, and G. Jeon, "A novel and secure attacks detection framework for smart cities industrial internet of things", *Sustainable Cities and Society*, vol. 61, pp. 102343, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[4] H. Pereira, G. L. Moritz, R. Souza, A. Munaretto, and M. Fonseca, "Increased network lifetime and load balancing based on network interface average power metric for RPL", *IEEE Access*, vol. 8, pp. 48686-48696, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[5] P. Rajpoot, S. Harsh Singh, R. Verma, K. Dubey, S. Kumar Pandey, and S. Verma, "Multi-factor-based energy-efficient clustering and routing algorithm for WSN", *Soft Computing: Theories and Applications*, pp. 571-581, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[6] R. S. Rathore, S. Sangwan, S. Prakash, K. Adhikari, and R. Kharel, "Hybrid WGWO: Whale Grey Wolf Optimization-Based novel energy- efficient clustering for EH-WSNs", *EURASIP Journal on Wireless Communications and Networking*, vol. 101, pp. 1-28, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[7] B. M. Sahoo, H. M. Pandey, and T. Amgothc, "GAPSO-H: A hybrid approach towards optimizing the cluster-based routing in wireless sensor network", *Swarm and Evolutionary Computation*, vol. 60, pp. 100772, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[8] A. Saleem, M. K. Afzal, M. Ateeq, S. W. Kim, and Y. B. Zikria, "Intelligent learning Automata-Based objective function in RPL for IoT", *Sustainable Cities and Society*, vol. 59, pp. 102234, 2020, [CrossRef] [Google Scholar] [Publisher Link]

[9] J. B. Madavarapu, H. Islam, A. Appathurai, G. A. Safdar, N. Muthukumaran, and J. Gnanamalar, "Heterogeneous Energy Harvesting Techniques for Smart Home IOT Acceleration", *IEEE Access*, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[10] B. Muthu Kumar, S. Ramamoorthi, S. Rajakumar, and A. Ahilan, "D2D Self Organization in IOT via Triple Modular Redundancy Based MDS Code", *IETE Journal of Research*, pp. 1-13, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[11] V. Narayan, A. K. Daniel, and A. K. Rai, "Energy efficient two-tier cluster-based protocol for wireless sensor network", *International Conference on Electrical and Electronics Engineering, INSPEC Accession*, vol. 19728627, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[12] A. Verma, and V. Ranga, "Mitigation of DIS flooding attacks in RPL-based 6LoWPAN networks", *Transactions on Emerging Telecommunications Technologies*, vol. 31, no. 2. 2020. [CrossRef] [Google Scholar] [Publisher Link]

[13] S. S. Solapure, and H. H. Kenchannavar, "Design and analysis of RPL objective functions using variant routing metrics for IoT applications", *Wireless Networks*, vol. 26, pp. 4637-4656, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[14] A. Kumar, and N. Hariharan, "DCRL-RPL: Dual context-based routing and load balancing in RPL for IoT networks", *IET Communication*, vol. 14, pp. 1869-1882, 2020.[CrossRef] [Google Scholar] [Publisher Link]

[15] R. Sharma, V. Vashisht, and U. Singh, "eeTMFO/GA: A secure and energy efficient cluster head selection in wireless sensor networks", Telecommunication Systems, vol. 74, no. 6, pp. 253-268, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[16] C. Pu, "Sybil attack in RPL-Based internet of things: Analysis and defenses", *IEEE Internet of Things Journal*, vol. 7, no. 6, pp. 4937-4949. 2020. [CrossRef] [Google Scholar] [Publisher Link]

[17] T. A. Alghamdi, "Parametric analysis on optimized energy-efficient protocol in wireless sensor network", *Soft Computing*, vol. 25, pp. 4409-4421, 2021. [CrossRef] [Google Scholar] [Publisher Link]

AUTHORS

S.V. Thilagan is an assistant professor is currently working in the university college of engineering.

Arrived: 10.05.2024
Accepted: 12.06.2024