Evolutions of Low Power and Lossy Networks Protocols in the Internet of Things: A Review

Poorana Senthil Kumar S and Subramani B

1 Department of Computer Science, SNMV College of Arts and Science, and Computer Applications, Dr. N.G.P. Arts and Science College, Coimbatore, India
2 Principal, SNMV College of Arts and Science, Coimbatore, India
Email: pooranasenthilkumar@drnagpasc.ac.in

ABSTRACT

Routing protocols render significant issues in the Internet of Things (IoT) real-time network scenarios because they are the authoritative responsibility for discovering, constructing paths, and transmitting packets between network nodes. The IoT delegates more improvements in sensors node, RFID, and Internet technologies in this development of routing protocols are playing a vital role in IoT networks. IoT application requires the reliability of data communication, limited latency, and considerable power consumption for network operations. The evolutions of these protocols are maximizing the Quality of Service (QoS), minimizing energy utilization, and increasing the node's lifetime is the most considerable part of all enhanced protocols in Low power Lossy Networks (LLNs). This article analyzes the Internet Protocol version 6 (IPv6) features enabled routing protocols for Low-Power and Lossy Networks (RPL) and Lightweight On-demand Ad hoc Distance-vector routing protocol - next generation (LOADng) protocols in IoT networks routing operation. The gradual progress of routing protocol evolutions in LLNs/IoT with satisfactions and limitations in recent years highlights the traffic pattern's contribution. These approaches are entirely new solutions influenced by routing protocols in the route discovery process. In this context, this analysis summarizes the most recently approached routing protocols of the merits and demerits in LLNs/IoT.

Keywords: IoT; LLNs; routing protocols; RPL; LOADng;

1. INTRODUCTION

An IoT network connecting smart constrained low-energy devices in real-time through Internet, such as sensor nodes or IoT objects, often functioning devices, are required highly variable link quality with low energy and constrained components called LLNs. This network has high-level challenges, including low power capacity devices and limited memory, highly inconstant link quality, uncertain link outage, and mobility of nodes or devices. The deployments of the smart environment, such as home automation, smart industrial operations, and environment monitoring system, center control equipped network systems [1], [2]. The IoT network operations frequently require topology updates, and the existing methods of conventional distance vector routing (DVR) protocols in the Internet network, such as Enhanced Interior Gateway Routing Protocol (EIGRP) and Ad Hoc On-Demand Distance Vector (AODV), failed in quick and frequent updates. Therefore, most of the researchers and industrialists are focusing on the challenging task of routing protocols for providing optimized path discovery and forwarding data packets across the connected node in IoT networks with constrained manners of limited computational energy, packet loss, limited throughput, and latency of data transmission [3]. On the other hand, researchers are developing more proposals for exchanging information with external objects with or without Internet service using the general protocol terms of proactive and reactive manner.

The functionality of IoT applications is the heterogeneity of real-time objects and worldwide gadgets that can transmit required information in a local context with or without the Internet. In 2025, these objects will be present in humans' daily life cycle in the manifestation of smart home appliances, smart industries, smart transport, etc. Humans will remotely control objects and monitor them objects [4]–[6]. Therefore, day to day rapidly, the IoT network becomes pervasive. At the same time, the vast number of multidisciplinary domains will face the technical challenges of combining more than one technology in their domain. The Wireless Sensor Network (WSN) devices are essential for data collections interface in IoT because they can collect several data in real-time environments (e.g., humidity, healthcare systems, and manufacturing) [7]. Several research papers proposed additional structures to provide interoperability and a relationship between WSN and the Internet's IP communication infrastructure. To address this complication issue in October 2004, the Internet Engineering Task Force (IETF) Working Group (WG) proposed and adhering to the principles of IPv4 and developed an IPv6 over Low-power Wireless Personal Area Network (6LoWPAN) inclusion of IP stack layer adaptation between the network layer for host-to-host and data link layer for node-to-node transmission. In packet framing, fragmentation and defragmentation follow and permits the IEEE 802.15.4 standard [8], [9].

The continued existence of IoT applications and the tiny smart devices to use the IP-based network contribution initiated by the 6LoWPAN WG based on emerging LLNs. The 6LoWPAN WG specifies the Internet connection to LLNs standards at various protocol stack layers [10]. From February 2008 to February 2012, the Routing over Low-power and Lossy networks Working Group (RoLL-WG) at the initial stage defined different protocols for routing like smart home appliance LLN, industry LLN, urban LLN, and transport automation. At the same time, the Roll working group initiated and studied IETF standard routing and identified the need for
LLN protocols [11]. The RoLL working group standard protocol of LLNs defined the IPv6 features enabled protocol for LLNs RPL in March 2012 and presented it in the RFC [6550][12]. The IoT networks consider RPL proactive standardization and tree-based routing protocol that forms a Directed Acyclic Graph(DAG) between network instance nodes since RPL has several downsides. New enhanced solutions have been emerging to overcome the drawbacks in future application requirements [13].

On the other end, researchers have contributed to reactive protocols for Internet service-enabled networks, and they are considering IoT core components limitations (e.g., memory, computation, energy, performance) based on AODV and adaptation of LLNs. Depending on AODV, the Internet-Draft of Lightweight On-Demand Ad-hoc Distance-vector Routing Protocol-next generation (LOADng) was presented to the IETF in October 2011. They proposed new protocols to improve LLNs performance and find solutions to problems based on observations and classification of existing solutions. The requirements of mobile-based adaptation in IoT with LLNs using RPL or LOADng are further improved depending on AODV. The classical AODV algorithm facilitates dynamic, multi-hop routing between mobile nodes. The routing is obtained quickly based on a loop-free manner in dynamic network topology [14].

The rest of this article is structured as follows: Section 2 presents LLNs/IoT routing methods and functionality in applications, and RPL and LOADng protocol evolutions are discussed in section 3. Section 4 describes the discussion and consideration of the new protocol design, and Section 5 concludes this review study with future enhancements.

2. ROUTING METHOD IN LLNs/IOT APPLICATIONS

Routing functionalities include path discovery and selecting paths between network devices for message transmission, and they securely transfer messages from source to destination. IoT applications are varied and in different fields. IoT application devices are generally designed with strong restrictions on computation, memory, energy utilization, and information exchange with other devices. The routing in IoT is a broad concept without the requirement of human intervention. Hereafter, the IoT devices are referred to as nodes. IoT applications’ objective nodes can have different hardware capacities based on real-time implementation.

In some cases, routing can be performed based on the local context, with or without an Internet connection. Based on route creation principles for constrained IoT networks, the routing protocols (set of rules for communications) can be labeled as proactive and reactive [15]. The proactive protocol has been widely adopted, with each node maintaining a separate one or more tables to represent the overall network topology structure. These tables are maintained with regular updates to maintain routing information from node to node. For this reason, proactive routing protocols are widely used for periodical data collection applications in LLNs [16].

On the other hand, routes will always be available based on request. Reactive protocols always construct routes only when nodes have intended to send a packet to its desired destination in the network instance; the goal of reactive protocols is to react based on demand. The source node wishes to send a message to a network instance destination where no route exists. It broadcasts request information for route creation in a network. Other nodes also receive this broadcast information from the source node, but other nodes only maintain the next hop address in the routing table [17], [18]. Hence, uneven interval traffic IoT applications, where any instance node can send a message to any available node in the topology instance. Therefore, the most current LLNs reactive protocol in the IoT is LOADng for improving network energy and QoS [19].

2.1 RPL-Functionality

The RoLL working group created the RPL tree-based protocol. The IETF defines the RPL to support the LLNs in the network, which creates a topology in the form of Destination-Oriented Graphs (DAG) tree for routing as the mode of DVR proactive routing protocol technique. The RPL network topology is organized into DAG, which forms one or more Destination-Oriented Directed Acyclic Graphs (DODAG), where the root nodes are represented in the DODAG routing tree. Based on a user specification, the Objective Functions (OFs) facilitate routing metrics and constraints to calculate the optimized route among the number of nodes. According to OFs, the RPL creates a routing structure in logical topology to build on a physical topology[20]. Figure 1 shows the DODAG formation and RPL topology and structure. The sub-network is considered a DODAG instance.

In the RPL process, to begin with, network nodes construct the DODAG. The second step is that the node initiates the operation of building the DODAG root node and sending a DODAG Information Object (DIO) control message to its instance neighbours. Even though this message is not a single component, it carries various relevant data like OF, metrics, node rank, node-ID, mode of operation, and timer. According to the OFs operation specification, DIO messages should be received by each node and processed before deciding whether or not to join the DODAG. RPL permits routes from the node to its root (upward stream) and from the root node to the leaf/child (downward stream) routes. In which the upward stream routes are automatically created during the initial operation of DIO message sending time, it does not require any other additional process. On the opposite side, it requires Destination Advertisement Object (DAO) control message.
handling for downward stream DIO message sending. The RPL downward specifies two types of modes for a downward traffic flow; "storing mode/deeper down," where all routers store all destinations in their sub-DODAG, and "non-storing mode," where only the DODAG root node has the route information to destinations in the LLNs [21], [22].

Based on the traffic pattern, RPL permits Multipoint-to-Point (MP2P), Point-to-Multipoint (P2MP), and Point-to-Point (P2P). Figure 2(a) shows the MP2P, and an upward flow sends data messages to the root. Figure 2(b) shows the P2MP downward flow of data messages from the root to other instance nodes. Figure 2(c) represents P2P; a node sends messages to other nodes both upward and downward, as required for non-root constraint [23]. The solid arrow line indicates the directions of traffic patterns, and the dotted lines represent the topology links.

The entire process of routing construction DODAG in RPL depends on OFs metrics consideration. The optimized path selection operation is directly linked to the network instance. Depending upon the metrics and constraints, the optimized path selection between a node and a root has the possibility of increasing or decreasing the network performance. For example, some IoT applications require minimum latency and maximum reliability. On the other end, they require low energy utilization and node mobile state. For example, wild animals, health care, and environmental monitoring systems.

Figure 2 (a): MP2P traffic flow

Figure 2 (b): P2MP traffic flow

The entire process of routing construction DODAG in RPL depends on OFs metrics consideration. The optimized path selection operation is directly linked to the network instance. Depending upon the metrics and constraints, the optimized path selection between a node and a root has the possibility of increasing or decreasing the network performance. For example, some IoT applications require minimum latency and maximum reliability. On the other end, they require low energy utilization and node mobile state. For example, wild animals, health care, and environmental monitoring systems.

Figure 2 (c): P2P traffic flow

These LLNs/IoT real-time applications accomplish the applications' requirements and can require different OFs [24]. In this part of network construction, the OFs metrics information node calculates the weight of the available path to the root node rank hierarchy and selects the transmission path on the network instance.

2.2 LOADng - Functionality

The LOADng routing protocol, with a base concept inherited from the AODV standard [RFC3561], is enhanced to node mobility, and its working manner is reactive. In October 2011, this protocol was presented as an Internet-Draft to the IETF with specifications. Since then, LOADng has had several extended updates; the updated last version was released in July-2016. The foremost operation of LOADng is gearing the Route Requests (RREQs) message by the originator called the LOADng router; while forming a route to a destination until it reaches the destination LOADng router forwards RREQs in the network. While reaching their destination, RREPs are initiated by the destination node and unicast forwarding RREPs messages hop-by-hop to reach the originator [15].

During the route discovery process, the network instance of each node should have a piece of information about available network nodes. This routing information set, pending acknowledgement information, failure states, and blacklisted neighbour information is maintained by each node. The routing set is the same process as the routing table, and entries of the routing information set are created during route discovery and maintain the information to reach the destination node, which includes node information, next hop address, and the number of hops. The pending acknowledge information set maintains the RREP acknowledgement reply if a node cannot reply. The RREP that the node address requires the reply information and is maintained by the blacklisted neighbour set.

The route discovery function sends the data message from source to destination and should be verified in the routing set's existing entry. If the path exists in this routing set, the data message can be sent from the origin node to the target. Otherwise, the current sender node starts a new route discovery process if no more route is available. During the route discovery phase, the sender node creates an RREQ(originator) message and the address of the desired destination information with a unique seq-sum for defining the other message fields. Finally,
the RREQ(originator) broadcasts to the neighbour nodes to construct a path from the sender to the destination node.

Each RREQ-received node executes a verification process that validates the address length and other details, and the nodes should update the routing set's fields. At the same stage, its destination node or the current node creates an RREP control message. In case of failure in this process, forward the RREQ control message to the next node in the route path until it meets the destination node in the network topology. Route Reply Acknowledgment (RREP_ACK) is generated for the signal message to its neighbour node that transmitted the RREP signal message that the reply message was successfully received. Receipt of an RREP_ACK indicates the high link quality between these two adjacent neighbours and sought bidirectional flow. An RREP_ACK message is unicast to the neighbour node from which the RREP message has arrived. Figure 3(a) represents the process of RREQ message transmission in the network nodes, and Figure 3(b) shows the process of RREP_ACK transmission.

3. RPL and LOADng

The IoT/LLN routing protocol solutions are proposed for the better improvement of existent; more protocols were discussed and proposed by researchers. However, the recent years most approaches are focusing on the RPL and LOADng according to the researcher's proposal and motivation.

3.1 Evolution of RPL

In IoT/LLN scenarios, implementing P2P traffic patterns in IETF-introduced RPL is costly in some applications. Around April 2010, RoLL-WG started a new proposal for enriching the P2P traffic flow in RPL [25]–[27]. In August 2013, the IETF standard in the RFC [6697] allowed the creation of P2P routes on demand in the Reactive Discovery of Point-to-Point Routes in Low-Power and Lossy Networks (P2P-RPL) supporting of reactive protocol principle [28].

The source node starts a route discovery movement and creates a temporary routing tree for sending P2P data messages. The temporary DODAG root is the sender node across the network request sent by the Point-to-Point Route Discovery Option (P2P-RDO) to the destination node. It is forwarded the packets up to it reaches the destination or the total number of hops in the network. While P2P-RDO reaches the destination, P2P Discovery Reply Object (P2P-DRO) replies back to the source node from the destination. The intermediate nodes maintain the reverse routing flow information to supply the P2P-DRO for message forwarding. After receiving P2P-DRO source-to-destination, the data message transmission starts with the P2P traffic pattern. The strength is the alternative number of P2P routes to accomplish the routing requirements, and forwarding P2P messages avoids using a permanent root node. The weakness is flooding, increasing the energy consumption of each node and overhead.

In [29] proposed Energy-efficient Region-based Routing Protocol (ER-RPL) presents the hybrid model approach of a combination of proactive and reactive methods in RPL. Proposed P2P communication with low energy consumption and improved network reliability. The concept of this protocol is to consider different partitions using Reference Nodes (RNs) and compute the distance between nodes. Therefore, it requires location-aware nodes are formed with Global Positioning System (GPS) in the entire network. According to the region, select the path, and a binary Region Code (RC) indicates each segment, this protocol's initial stage, RNs flood the control message with Region Formation Object (RFO) message to the entire network. In the communication part, the default route of RPL sent a P2P route request done using a Message Request Object (MRO) control message. If the destination node receives, MRO should verify path cost is satisfactory. If the path is satisfied, the source node receives confirmation from the destination through the formed reverse path flow, and the source node starts sending data messages in the selected path. The merit of this approach is reducing energy consumption by eliminating the flooding process in the entire network. Demerit requires additional control messages to default RPL, and location-aware nodes are required.

During the path discovery process, IoT applications emerging improvement of symmetric and asymmetric links in P2P is proposed [30]. This Ad hoc On-demand Distance Vector routing-based RPL (AODV-RPL) is an on-demand principle. No desired paths exist, and the preferred current path is not satisfied. The source node starts the route construction process to the purpose of reach the destination node. The source node starts to send DIO and a Route Request content (DIO-RREQ) message to generate an RREQ-instance(originator) and find the
route to the destination node. DIO-RREQ fields carry an additional state field of S, indicating that the route is a symmetric or asymmetric state and is updated by each node. The state of S is symmetric notification then the destination node unicasts a DIO and Route Reply content (DIO-RREP) to the DIO-RREQ sender. Otherwise, the destination node multicasting process starts with DIO-RREP to the neighbour node. The main interest of this protocol is at the time of the route discovery phase to minimize the control message size and consider the solid bidirectional link conditions. The disadvantage is not yet evaluated the performance result (theory representation only) and is still under draft form.

In IoT environments, most applications require mobility in urban and industrial scenarios, which have always been challenging deployment tasks. The common standard RPL was designed for static networks. Originally the Corona architecture was proposed in [31]; the main objective of this architecture used to extend the network lifetime and focus on QoS. This proposal has been extended for static and mobile wireless sensor networks. In real-time applications, constant changes in mobility nodes of network topologies are at risk of high link failure cases, frequently affecting the result of PDR parameters. In [32], the comparison between standard RPL and the Corona mechanism (Co-RPL) aims to improve the PDR, end-to-end delay, and average energy consumption. Co-RPL proposes the standard RPL control messages with some added message fields to achieve the QoS in the LLNs instance. All the network nodes information table maintains a piece of information about a neighbour (node ID, corona ID, DAG, and link quality). If the receiver node gets a DIO control message, the node defines the lowest corona ID and best parent node selection and calculates the rank based on the OF. In the new path recovery mechanism proposed in Co-RPL, the node is not able to reach the destination, and the highest corona ID sends a DIS message to the data packet. This finding process occurs till the router node identifies a new root; this node can't be able to deliver the packet data to any available neighbor of the high corona IDs and sends pause information to the preceding hop to the data packets for pausing the data packets sending process. The advantages of this proposal are mobility support, a new concept of path recovery, and a reduced packet delivery ratio with average energy consumption. The disadvantages are the manipulation required in the default RPL message and the routing table size increase.

In addition, [33] proposed simple, effective, and backward compatibility with the native RPL protocol for mobility support nodes and named mRPL. In real-time and reliable mobility, data collection scenarios incorporate a proactive hand-off system (smart-HOP) within RPL. As part of this proposal, nodes are considered Mobile-Nodes (MN) and Access-Points (AP). The working principle also considers two phases the name of data transmission and discovery phase. The sequence of DIS beacons is received by AP from MN for calculating the Average Received Signal Strength Indicator (ARSSI) and sends the calculated values to MN. If the received value of ARSSI is smaller than the defined threshold in MN, the second phase of discovery starts. In this phase, DIS messages are sent based on intervals from MN to AP until a reply is received from AP nodes with an ARSSI value greater than the specified threshold. Once the condition is satisfied in the threshold parameter, MN moves to the next phase of data transmission with the new root. In the failure to serve AP sending DIO messages, the MN begins in the discovery phase. These two phases are detached from regular RPL data packets and control messages. Hence, mRPL nodes are synchronized in the same network as the standard RPL process.

The dynamic strategy handling mechanism in LLN network traffic proposed in [34]. Backpressure RPL (BRPL) is the routing protocol combined with the LLN and RPL. The basic idea is to provide various throughput adaptability and mobility nodes data transmission, allowing dynamic multiple logical topologies (Multiple DAGs) to create different OFs. Each DAG buffered BRPL nodes maintain a packets queue. The RPL rank and queue length information are exchanged by using DIO messages. DIO message should be received by each node and update the packet sender information in the neighbour table. Based on rank value and queue length, each neighbour link weight is computed at the part of packet forwarding.

Moreover, the packet loss minimized achieved by using \( \Theta \) (theta) parameter for operating the link cost computation using QuickTheta algorithm. It defines the \( \Theta \) values between 0 and 1 consistent with the mobility of the nodes. The congestion level measurement is acquired by the ratio between the queue capacity and the number of available queues. In the BRPL routing switching strategy defined by \( \Theta \), the consistency of different traffic loads and changes in topology values are automatically adjusted by mobility. In the next process, QuickBeta calculated the mobility node changes in the neighbour table defined as \( \beta \). If \( \Theta = 1 \), then BRPL understood the packet forwarding is concluded to use the OFs of RPL; else \( \Theta = 0 \) or nearest to 0, BRPL concluded to perform the proposed backpressure routing concept for packet transmission.
<table>
<thead>
<tr>
<th>Routing protocols</th>
<th>Issues</th>
<th>Merit</th>
<th>Demerit</th>
<th>Applications Area</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>P2P-RPL</strong></td>
<td>● Alternative for P2P in RPL.</td>
<td>● Routing requirements fulfilled alternative P2P routes.</td>
<td>● Flooding increases energy consumption.</td>
<td>P2P Traffic pattern</td>
</tr>
<tr>
<td></td>
<td>● Improving support of RPL.</td>
<td>● Avoid the use of permanent root nodes.</td>
<td>● Overhead increases</td>
<td></td>
</tr>
<tr>
<td><strong>ER-RPL</strong></td>
<td>● Low energy consumption.</td>
<td>● Reducing energy consumption. Eliminating the flooding process in the entire network</td>
<td>● Additional control message Location-aware nodes are required.</td>
<td>P2P Traffic pattern</td>
</tr>
<tr>
<td></td>
<td>● Improving network reliability.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>AODV-RPL</strong></td>
<td>● On-demand principle implementation.</td>
<td>● Reduced the control message size.</td>
<td>● The draft mode only.</td>
<td>P2P Traffic pattern</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● Solid bidirectional link.</td>
<td>● The performance results are not evaluated.</td>
<td></td>
</tr>
<tr>
<td><strong>Co-RPL</strong></td>
<td>● Mobility</td>
<td>● Alternative path recovery from RPL.</td>
<td>● Manipulation is required in the default RPL message.</td>
<td>Mobility wireless applications</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● Reduced packet delivery ratio with average energy consumption.</td>
<td>● Routing table size.</td>
<td></td>
</tr>
<tr>
<td><strong>mRPL</strong></td>
<td>● Mobility support nodes.</td>
<td>● Collision and loop-free.</td>
<td>● Control message size.</td>
<td>Healthcare monitoring applications</td>
</tr>
<tr>
<td></td>
<td>● Provide fast, continuous, and reliable</td>
<td>● Low packet loss and delay</td>
<td>● Exchanged control message.</td>
<td></td>
</tr>
<tr>
<td><strong>BRPL</strong></td>
<td>● Various throughput adaptability.</td>
<td>● Level of congestion is acquired</td>
<td>● High end–to–end delay</td>
<td>Mobile node applications</td>
</tr>
<tr>
<td></td>
<td>● Mobility node's data transmission</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>EMA-RPL</strong></td>
<td>● Energy-efficient Mobility</td>
<td>● Reduced energy consumption.</td>
<td>● High overload and affecting the network performance.</td>
<td>Healthcare applications</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● Other resources Computational</td>
<td>● Interoperability in standard RPL</td>
<td></td>
</tr>
<tr>
<td><strong>CLRPL</strong></td>
<td>● Different data traffic pattern</td>
<td>● Reduced packet delivery ratio.</td>
<td>● Require additional memory</td>
<td>Dynamic traffic pattern</td>
</tr>
<tr>
<td></td>
<td>● Improved packet delivery ratio.</td>
<td>● Select a parent with less number of nodes</td>
<td>● Increase end–to–end delay</td>
<td></td>
</tr>
<tr>
<td>Routing protocols</td>
<td>Issues</td>
<td>Merit</td>
<td>Demerit</td>
<td>Applications Area</td>
</tr>
<tr>
<td>-------------------</td>
<td>--------</td>
<td>-------</td>
<td>---------</td>
<td>-------------------</td>
</tr>
</tbody>
</table>
| LOADng-CTP        | ● Efficient data acquisition  
                   ● Supports upward traffic flow from child to root in bidirectional flow | ● considerable reduction of routing overhead | ● End-to-End delay and additional memory usage | Smart grid in suburban |
| LOADng + NDM      | ● Avoiding local failures.  
                   ● Global knowledge of neighbours' information | ● The packet delivery ratio is tolerable. | ● Complexity in the protocol.  
                   ● High latency and throughput | Not Defined |
| LOADng-SmartRREQ  | ● Constrained environment.  
                   ● Unicast reply from the destination | ● Improved processing complexity and loop-free | ● Same data delivery ratio with AODV | MP2P |
| LOADng-ExpRing    | ● Region-based flooding.  
                   ● To avoid flooding in the entire network | ● Reduced control message and overheads.  
                   ● Collisions get good | ● A digital signature cannot cover it from the originator.  
                   ● The average delay is high. | MP2P |
| LOADng-IoT        | ● Routing by Internet connected nodes autonomously  
                   ● Not maintaining the previous definition of gateways | ● significant in QoS, reliability, and energy efficiency | ● Unstable performance considers collision Interference | Healthcare systems  
                   Smart home appliances, smart cities, and Industrial automation |
| LOADng-IoT-Mob    | ● Mobility node, dynamic topology  
                   ● Avoid sending messages in failure routes due to the mobility of the nodes.  
                   ● Low latency, Data delivery reliability, low control overhead | ● High memory usage | IoT - mobile devices |

forwarding. In this scenario, end-to-end delays become increased.

Energy-efficient and Mobility-Aware routing (EMA) based RPL is proposed in [35] for mobility nodes avoiding broken routes, improved energy consumption, and network performance in low-density networks. Composed of static and MNs, in standard RPL, the MNs are called leaf nodes. In this case, MNs avoid routing data packets received from other nodes. Through the MNs, static node data messages can be sent and received; in this proposal, MNs are named Associated-Node (AN); these AN nodes take responsibility for the monitor, notifying the movements, and identifying and defining a new AN to the MNs. This protocol functionality is represented into three stages: mobility disclosure, reaction and prediction and forecast notification. In stage one, AN monitors and identifies the movements of MN nodes in the network nodes according to RSSI measured method data message values are received from AN. Suppose the measured RSSI value is lesser than a specified threshold value. In that case, the second stage of the reaction and prediction process is activated, and then control messages are sent by AN for searching a new static node to form a new AN from MNs. In this stage, if a new AN founds, the third phase of notification triggers and informs the MN. Thus, the old AN informs changes of the current status MN by using a control message. After this received message, MN should conform to the received messages and update the new AN details on the routing information table. Energy consumption is achieved by this method of reducing MN unwanted sending control messages, monitoring and forecasting its movements.
However, the network density increases with a high range of mobility scenarios that have high overload and affect the network performance. Therefore, this proposal requires more changes in the control message part, and interoperability is difficult in standard RPL.

An LLNs/IoT real-time applications require various data traffic patterns during data exchange between nodes, such as P2P, MP2P, and P2MP ( multicasting) communications; for this scenario, Context-aware and Load-balancing RPL (CLRPL) proposed in [36]. The objectives of this protocol design focused on improving the packet delivery ratio, supporting heavy throughput and different traffic, and increasing the network lifetime in LLN. CLRPL process has segregated into three phases, and phase one introduced Context-Aware Object Function (CAOF) for calculating and defining the rank of each node, node Excepted Transmission Count (ETX), parent residual energy, and parent node rank. The DIO messages work with a piggyback mechanism, and the receiver node stores the DIO in an array to calculate the DIO sender's rank. The CAOF calculates the rank from best to worst using an algorithm of sorting. Avoiding the thundering herd phenomenon is broadcasting DIO with the best rank. The next phase used Context-Aware Routing Metric (CARF). The information maintains the path's queue chain details, the node's rank, the status of the node, and an index value of network traffic for obtaining values to select the parent. The CARF is carried in DIO and interface layer between this protocol's first and third phases. The parent selection technique is the third phase of this proposal; CARF has selected the parent based on the lower value CARF computed; if more than one CARF has the same value, this phase selects the root node with the minimum number of child nodes. These phases are directly related to each other; it reduces the node energy consumption and improves the packet loss ratio by considering the workload of the path. This routing solution supports different traffic parents. A comparison summary of the routing solution of RPL-based routing is presented in Table 1.

3.2. Evolution of LOADng

In recent years, research people [37] proposed an alternative routing protocol for IoT network interactive approach derived from AODV. This protocol interoperability to LLNs requirement is named as LOADng. The LOADng packet forwarding routing process operates only on demand behaviour to a given destination. Around 2007, the LOAD 6LoWPAN working group suspended further development because of RPL pending results from ROLL working group experiences. The LLNs have opened a new interest in AODV implementation to the IoT network with a constrained device environment. The LOADng operation concepts removed many elements from AODV and introduced two new concepts, RREQ and RREP [38].

An extension of LOADng, in [39] proposed LOADng-Collection Tree Protocol (CTP), has been approached by ETX for improving the energy consumption in a new method, extending the network's lifetime in constrained computation and memory. Hence, no changes in packet format and two base operations of route discovery and route maintenance of standard LOADng operation. The foremost operation of route discovery floods the RREQ messages to the network generated by the source node (originator). The destination desired node only replies to RREP, and all other intermediated nodes do not make any replies to the source node. An actively used route fails, the second operation of the route maintenance process, the source receives RERR(Route Error), and the source node starts to find a new route discovery from source to destination. LOADng-CTP added two REQ flags in the existing RREQ message, RREQ COLLECTION_TREE_TRIGGER, which discovers a bidirectional link of neighbours and RREQ COLLECTION_TREE_BUILD to construct a route to the root and enable data traffic transmission from root to all other bidirectional nodes. Due to lossy or topology changes, network failure could occur. This scenario will rebuild the existing tree instead of building a new one. This approach, LOADng-CTP, achieved low overhead, a higher data delivery ratio, and improved delay time.

The link failure scenario to utilizing multipath selection methodology for optimally selected alternative path selected from the backup path is proposed in [40] and implemented on the top of LOADng. Therefore, this proposal termed LOADng+NDM (Neighbour-Disjoint-Multipath), implementation of the NDM algorithm is compared IPv6 standard RPL and LOADng with basic metrics of PDR, overhead, end-to-end latency, and average route table size. The same existing LOADng path construction of RREQ and RREP technique for primary path, shortest route selection used Dijkstra's algorithm with a modification of RELAX procedure, and the new backup path is utilized as an alternative approach for route selection. The primary and backup path employed by RREQ and RREP for message exchanges in distributed NDM, there are no changes in the route discovery phase of the RREQ process method, same as broadcasting from source to destination on the other end, the destination creates two different messages in RREP. Unicast RREP (RREPv) and broadcast RREP(RREPb), if the source receives RREPv, it is considered the same operation of standard LOADng protocol. It follows the primary path for further process in case the source has received RREPb from the source node and is validated if it is inside the main path in the network instance or updates the correlation and hop-count metric. If these two metrics of correlation parameter and hop count are improved with equal or less than the primary path, the further process will begin else RREPb is dropped. Whether the path is primary or backup is set up by RREP. LOADng+NDM could need further performance improvement in terms of latency and throughput.

In standard LOADng intermediate nodes, RREPs are avoided for reducing the control message size and free from loop operation. In a constrained environment, the proposal [41] introduced the alternative to the intermediate/gratuitous SmartRREQ simple mechanism to enable intermediate RREPs from AODV to reduce large control messages and improve processing complexity. In this approach, they consider the following two schemes; If RREQ and RREP solicit only unicast from source to destination according to their existing routing table, RREP should be unicast. In the second scheme of next node link failure or not available in routing table fashion, RREQ solicits broadcast in the MP2P traffic pattern. It obtains the same data delivery ratios as AODV.
The smartRREQ cannot improve the traffic control overhead of LOADng. [42] proposed an extension of LOADng to perform the route discovery operation using Expand-Ring (LOADng-ExpRing) applied to flood control messages on rings. The Expanding Ring flooding mechanism derived from AODV does not flood the RREQ into the entire network. Instead of only a limited distance flooding without intermediate RREP result, the floods employed with Time-To-Live (TTL) concept. If an intermediate route has a well-founded route to the destination, the TTL does compute the least distance among the source and destination nodes. Therefore, the IP header is eliminated in LOADng-ExpRing. This process can be achieved by using the alternative 8-bit field in the name Maximum Number of Broadcasts (MNB), and it does an equal operation as an IP header field of the TTL field. The route discovery in LOADng protocol enabled with ExpRing flooding to set timeout parameters for receiving an RREP. If the time out expires without receiving RREP, then the new RREQ is broadcasting starts from the originator and MNB filed increments by one up to MAX_HOP_COUNT in the MNB field. By this proposal, the ring tires reduce the number of routes impact, control messages, and overheads.

Simple node and Internet capability nodes connected and forms network operations are proposed in [43] with three improvements in IoT scenario, dynamically find the Internet-connected nodes, reduce the control message overhead, and decrease data message loss. This proposal is termed LOADng-IoT, the network formed with regular nodes and Internet-connected nodes (INs). These INs devices are highly equipped and then potentially follows IEEE 802.15.4 standard, have direct Internet connections, these INs can directly send Internet message, and networks simple nodes perform operations generating Internet messages, find INs for forwarding their message, hence INs work as a gateway of the network. This work obtains network QoS and reliability, improves the end-to-end latency by increasing the PDR parameter, adopts unrelated hardware capability nodes, and reduces energy while building the path and routing. This proposal does not require previous definitions of nodes and can detect the appropriate Internet node to forward messages. In this part, the author introduced the iot-flag and Internet Route Cache mechanism that previously removed Internet nodes from the routing table.

A novel solution for enhancing LOADng in mobile IoT (LOADng-IoT-Mob) routing is proposed in [44]. Avoid packet transmission in network failure nodes in the mobility topology. Introduced the new concept of a short periodical control message for managing the routing table, low control message frequency adopted in dynamic network changes, and tracking the nodes' location of its mobile network. This proposal added three sub-fields, smart_rreq, mnb_value, and iot, to the SmartRREQ message. Expanding Ring flooding and LOADng-IoT introduced a new field in the routing set termed R_next_hop_valid_time for recording the valid time of the next-hop. They implemented two kinds of route discovery mechanisms, using the ExpRing flooding technique to create paths in local data packet transmission with normal nodes, known as simple route discovery. A node that wants to send data packets to Internet nodes following the proposal of existing LOADng-IoT is called Internet route discovery. Each node received control messages, and the next hop was refreshed according to duration and executed the shortest path in self-adopted topologies.

An improved method of this LOADng-IoT-Mob is designed to provide self-adaptation to the topology updates and maintain the data about the next hop path of the source to the destination. Able to obtain a preferable data delivery ratio, low latency, and lower control overhead. Table 2 presents a comparison summary of routing solutions for the LOADng protocols.

4. DISCUSSION AND CONSIDERATION

The reviewed protocols of RPL and LOADng routing solutions are limited, showing that proposed solutions are employed in PDR and energy consumption. Currently, more IoT applications are required in different fields with different traffic patterns. The current and future LLNs/IoT applications will require mobility applications [45]. In this scenario, the upcoming proposal is advised to acknowledge the network topology changes, node movements, energy, end-to-end delay, self-adaptation, and network density changes in the traffic pattern. The MP2P traffic is the minimum support of RPL and LOADng base protocol.

This review discussed valuable routing solutions in LLNs/IoT and identified the main intention satisfied at a certain level. The complexity of algorithms, message length size, and overhead are constrained in current solutions. However, studied solutions are implemented in simulation computation in most approaches. Also, the results are not represented in real-time scenarios, leading to higher traffic variation while networking density increases in real-time and environment adaptation. These considerations are not mandatory and represent the right direction to enhance routing solutions for fulfilling the LLNs/IoT requirements in real-time traffic patterns.

The following statements of a few open issues and suggestions for a new approach

- **Nature of application:** More real-time applications in various work courses in the 6LoWPAN routing protocol. Based on the application's requirements, few applications are implemented with energy constraints. Other applications are considered computation of efficiency and load balancing, leading to end-to-end delay.

- **Global standardization:** The part of the network protocol solution is highly complicated because the same applications have different hardware components. The existing solutions are designed considering only a few applications, and IoT applications interoperability among more heterogeneous devices varies from one device to another.

- **Base protocol heritage:** Significant changes should be avoided from the base protocol framework for implementing new protocols. Usually, existing most of the implementations of the protocols are followed the RPL and AODV structure as the base. This
approach is easily adopted into existing network protocols and interoperability into IoT devices.

- **Public availability**: Make all the proposals open-source, which is easy to bring the protocols into reproducible, the many of the required matters like flow charts, algorithms, equations, and structures are not available. Because of this, more protocol proposals cannot be improved and reconstructed.

- **Follow IETF’s standard**: The IETF’s working group does not consider the specific application protocol. The IETF always considers allowing the proposal should follow the high acceptability and common standardized solution for all applications. However, IETF’s specification is also avoidable; several proposals demand different types of IoT/6LoWPAN applications.

5. CONCLUSION

IoT applications are good solutions for real-time applications without human interaction. This analysis has presented the summary of an extension of RPL and LOADng to proactive and reactive routing, another aspect of working principles of proposed evolution and supporting different traffic patterns as per the real-time application scenario requirements; each evolution requires enhancements for obtaining efficient network routing operations in IoT. This analysis and discussion studied current LLN routing strategies to identify improvements in RPL and LOADng base protocol. All these proposed works could not solve for LLNs in the different traffic patterns. However, the devices’ heterogeneity and routing in the constrained environment could not fulfill the mobile node in the high-density network. Furthermore, this analysis shows that the proposed solutions cannot satisfy the IoT routing requirements because of some limitations. End-to-end delay, memory, node lifetime, energy utilization, overhead, and packet delivery are essential in the context of IoT network routing protocol. In future IoT, efficient routing protocols are required in real-time to extend the network lifetime, optimized routing, and mobility applications to accomplish the different traffic patterns.

REFERENCES


AUTHOR PROFILES

Mr. Poorana Senthilkumar S received B.Sc (Computer Science) from Bharathiar University, Coimbatore, in year 2004 and Master of Computer Applications from Anna University, Chennai, in year 2008. He is currently pursuing Ph.D. in Bharathiar University and currently working as an Assistant Professor in Department of Computer Applications at Dr. N.G.P. Arts and Science College, Coimbatore. He is a life time member of IAENG. He has published more than 5 research articles in National/ International journals. His research interests on Internet of Things, LLNs, RPL, VANET, Cloud Computing, and WSN Networks. He has 12 year of teaching experience and 4 years of Research Experience.

Dr. B. Subramani received M.Sc Mathematics from Bharathiar, Coimbatore and Master of Computer Applications from Madras University, Chennai. He received Ph.D from Bharathiar University, Coimbatore. He is currently working as a Principal in SNMV College of Arts and Science. He is a recognized Research Supervisor at Bharathiar University, Coimbatore and currently he has guided more than 5 scholars Ph.D scholars. He is a life time member in Computer Society of India and vice-president of Bharathiar University self-finance colleges Principal’s Association. He published more than 25 research articles in National and International journals. He is acting as a BOS member in more than 4 Universities in Tamilnadu. He has around 28 years of experience in teaching. His research interests are Computer Networks, Information Security, Machine Learning, Internet of Things, WSN, and Big Data Analysis.