A Review of RPL Protocol Using Contiki Operating System

S.N.Vikram Simha
School of Electronics and Communication Engineering
REVA University
Bengaluru, India
vikramsimha943@gmail.com

Reema Mathew
Centre for Artificial Intelligence and Robotics
DRDO
Bengaluru, India
reema@cair.drdo.in

Shubhashisa Sahoo
Centre for Artificial Intelligence and Robotics
DRDO
Bengaluru, India
sahoo@ieee.org

Rajashekhar C. Biradar
School of Electronics and Communication Engineering
REVA University
Bengaluru, India
dir.ece@reva.edu.in

Abstract— **Growth of Internet of Things (IoT), in leaps and bounds has diverted major attention towards wireless sensor networks and its associated routing protocols. Use of a routing protocol which is not suitable for a particular scenario may result in a loss of packets. This in turn will lead to retransmissions which has an obvious impact on bandwidth, the amount of power being consumed among various other parameters. These issues are to be considered since IoT involves Low Power and Lossy Networks (LLNs) formed using low power devices. Hence for IoT applications, Routing Protocol for LLNs (RPL) is custom designed. The objective of this study is to describe the RPL protocol and the operating system contiki which paves the way for its reliable implementation. Also, a collective information regarding RPL implementation is provided for better comparison.**

Keywords—IoT; RPL; Contiki; Cooja; Low Power and Lossy Networks

I. Introduction

With the evolution of technology, the concept of Internet of Things (IoT) has gained utmost importance. IoT has devices with computing capabilities, living beings, other digital machines that can perform data exchange. Specifically, in IoT, the “things” part mainly focuses on intelligent or smart devices, that can connect to the internet and proceed with communication process [1]. IoT offers vast range of applications ranging from simple home applications to industrial applications. For instance, smart health is one IoT application, where sensors measure patient’s parameters like temperature, heart rate and communicate this over internet with the aid of a smart phone. IoT involves Low Power and Lossy Networks (LLNs) with devices constrained in terms of power, storage capacity and other resources required for operating. The interconnecting links in LLNs are not stable, and also have high loss rate along with low data rates.

Wireless Sensor Networks (WSNs) that use sensors to sense changes which occur in its surrounding environment are an example for LLNs [2]. WSNs are inclusive of sensor nodes or devices that are connected in a wireless fashion in order to perform a desired task. In certain environments where it is not possible to set up a traditional wired communication, WSNs are preferred. In comparison to traditional networks, wireless sensor networks are different in few aspects. Majority of the sensors work on batteries as a result of which power consumption is a matter of concern. The sensor nodes are smaller in size which implies that their computation capabilities might be constrained [3]. Due to compact size of the nodes, the energy storage capacity is also limited. Hence energy is one major constraint of these networks. So, using a routing protocol that works by considering these constraints is a prime aspect that has to be taken care of [4].

IoT constitutes wireless sensor networks, whose deployment is remote in nature [5]. Sensors can be deployed in areas that are hard to reach. WSNs have a prime role in making IoT work appropriately. Hence the routing protocol chosen for such networks must consider the low power requirements of sensor nodes and also the lossy nature of the communication links. Internet Engineering Task Force-Routing Over Low power and Lossy networks (IETF-ROLL) is the working group that was formed with a task to develop a routing protocol that suits the needs of LLNs like wireless sensor networks. This particular group provided the specifications of IPv6 Routing Protocol for LLNs (RPL) which has been tailor made for LLNs used in IoT [6]. RPL works by constructing a Destination Oriented Directed Acyclic Graph (DODAG) and facilitates point to point, multi-point to point as well as point to multi-point communication.

RPL surpasses the other protocols through its ability to be used in LLNs. Of late, the implementation of RPL protocol in applications like that of smart grid has increased. Also, test beds of WSNs are being used for RPL practical implementations. RPL is included in different operating systems to facilitate increase in its usage. The significance of this proposed work is that it provides the information necessary

978-1-7281-5518-0/20/$31.00 ©2020 IEEE

for understanding the RPL protocol and the operating system to be used for implementing it, in a concise manner.

Though there are other platforms like Network simulator, TinyOS that allow the implementation of RPL, Contiki Operating System (OS) is selected as it provides greater flexibility for exploring and implementing RPL protocol effectively.

The rest of the paper is organised as follows: Section II provides information about RPL protocol and its working. Section III provides a brief insight into the contiki operating system for RPL implementation. Section IV highlights few of the works related to RPL. The paper is concluded in section V.

II. RPL Protocol

RPL is an IPv6 routing protocol which is based upon the distance vector concept. It helps in reduction of complexity in routing, memory used, control messages sent [7].

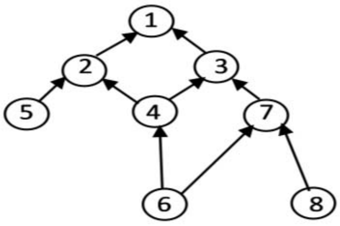

Fig. 1. Destination Oriented Directed Acyclic Graph

RPL works by constructing an infrastructure of its own which is called as DODAG [8]. A DODAG contains three types of nodes. The first one is the sink node which is also called as the root node that leads to DODAG formation. The second type is the router nodes which have the ability to generate the traffic along with collecting and forwarding the traffic. The nodes that just generate the data traffic but cannot forward it on other node's behalf are the third type of nodes called as leaf nodes. They simply join a DODAG under existence, as end nodes [9]. Figure 1 shows a DODAG with node 1 being the sink, nodes 2,3,4,7 being router nodes and nodes 5, 6, 8 are the leaf nodes.

In a DODAG these nodes are arranged in a tree structure with paths between the sender and the sink nodes. Every node will have its preferred parent node and its corresponding route to reach the sink node [10]. A neighbour node with the least rank is selected as preferred parent when forwarding any packet [11]. Rank of a node is defined as the distance between the sender and the root or sink nodes [12]. Rank of a particular node helps in avoiding formation of loops. RPL also includes a concept called objective function which will have its respective path metric by which a best possible path can be obtained to reach the sink node [13]. The value of rank of a node is found relative to this objective function used in the RPL protocol [14].

A. Formation of a DODAG

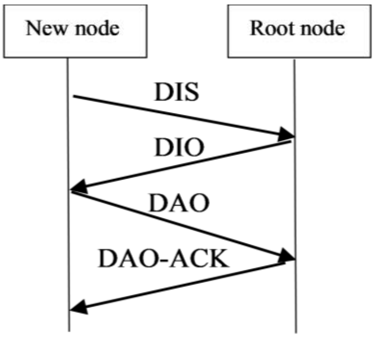

Fig. 2. Exchange of control messages in Routing Protocol for LLNs

The root or the sink node is responsible to begin the formation of a DODAG. Three types of control messages are involved in the construction of a DODAG namely, DODAG Information Solicitation (DIS), DODAG Information Object (DIO) and Destination Advertisement Object (DAO) [15].

1) DODAG Information Solicitation: DIS will help the new node in soliciting a DIO from one of its neighbouring nodes [16]. Receiving this control message from new nodes is perceived as a request in order to join the DODAG.

2) DODAG Information Object: A root node is responsible for sending this control message. The nodes that receive this control message from the root directly, become its neighbouring nodes. These neighbour nodes rebroadcast DIOs to their neighbouring nodes. DIO will include the rank of a node, objective function used and also the routing metric. If a node receives this control message, it can then join the DODAG by choosing a parent node of its choice [17]. Figure 2 shows the control message exchange between the root and new nodes. DIO's are sent on a periodic basis in order to maintain the consistent routing information [18]. The rate at which this particular control message is sent is governed by the trickle timer. This timer makes sure that DIOs are sent in case of an addition of a new node or when there are any inconsistencies in the network [19]. This will help in reducing the number of control messages sent as long as the network is in a stable condition.

3) Destination Advertisement Object: DAO will allow the child nodes to become a part of the DODAG. It will also help in recording the information regarding the nodes that are visited along the path towards the sink node [20]. Apart from the above-mentioned control messages, Destination Advertisement Object Acknowledgment (DAO-ACK) will be sent after receiving the DAO in order to acknowledge its reception [21].

There are two different modes in which RPL can function namely storing mode and non-storing mode [22]. In storing mode, child nodes send DAO messages to their respective parent nodes. The nodes that receive this DAO will then store details like sender's address along with the hop that has to be taken next to reach the root [23]. For nodes that are limited in terms of capacity of storage, non-storing mode is suitable. In non-storing mode, nodes unicast the DAO to the root node directly [24]. The root node alone has the information of the entire DODAG topology. The data will have to go through the root node before it reaches its intended destination.

B. *Objective Function*

In a DODAG formation, objective function helps in choosing a desired parent node and it is also used while routing the messages. Further, objective functions use a routing metric to find a path through a parent node to the root node [25]. Along with this, the way in which these metrics get converted to a rank is also defined by the objective function [26]. The mechanism of selecting a path is optimised as the objective function selects a best path to reach the root node.

Minimum Rank with Hysteresis Objective Function (MRHOF) and Objective Function zero (OF0) are two objective functions included as a part of RPL [27]. OF0 works by taking minimum hop count as the criterion, whereas MRHOF has Expected Transmission Count (ETX) as its default routing metric [28]. It means that OF0, finds a path towards the root node such that number of hops are kept to a minimum value. ETX in the case of MRHOF is the number of retransmissions required for sending a packet to the root node [29]. MRHOF hence tries to select nodes as preferred parent only if the nodes have a minimum value of ETX.

III. Contiki OS for RPL implementation

Contiki Operating System is designed particularly for Wireless Sensor Networks [30]. It makes use of C programming to implement various simulations [31]. Contiki's RPL is one of the early real time implementations of RPL which also is reliable. Hence contiki is commonly preferred for analysing the RPL protocol. It is well suited for micro controllers with memory constraints. It makes use of certain techniques for memory management so as to allow its usage in devices with less memory. One such technique is dynamic allocation [32]. Also, devices that work on batteries can be used adequately as it has the feature where no event leads to a sleep mode in the system. The nodes can check the channel on a periodic basis for radio signals. Real time systems implementation is possible with the rtimer library of contiki.

Contiki mainly is event driven and it also supports multi-threading [33]. Protothreads based model is used for programming in contiki. The advantage in using protothreads is that overhead of memory is very minimal. ContikiMAC is the mechanism that is responsible for allowing the radio to operate at low power. Nodes have the ability of receiving and transmitting messages even at these low power levels [34].

In order to make the communication possible, contiki offers microIP (uIP) stack and also rime stack. Micro IP is a TCP/IP related implementation which supports both IPv4 as well as IPv6 networking [35]. It can very well be used for 8-bit micro controllers. Rime stack is meant to be used for radio communications using low power. It supports unicast and roadcast communication with single hop. Apart from this, communication using multiple hops is also possible [36].

Contiki has an RPL directory in its core folder with files required for RPL's implementation. This RPL directory has RPL functions which modify the routing entries and functions necessary for the construction of DODAG. Objective function can be changed from MRHOF to OF0 and vice versa from this core folder.

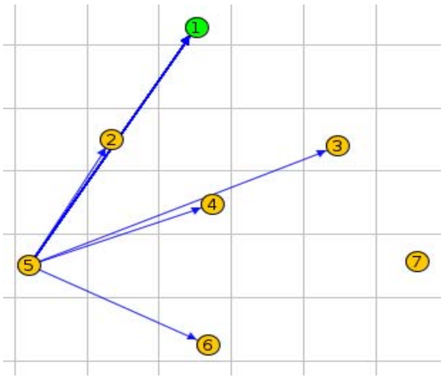

Fig. 3. Destination Oriented Directed Acyclic Graph visualisation in cooja

Cooja simulator is used to simulate the sensor networks in contiki operating system. The main target of this simulator is to support the low power devices that are used as a part of IoT [37]. Cooja is based on Java and it also works with sensor nodes being written in C.

Cooja provides the feature of using different kinds of hardware platforms like TelosB, Z1, Tmote Sky, MicaZ. Figure 3 depicts how a DODAG appears for the RPL protocol in cooja simulator. Here, node 1 is the sink node and nodes 2,3,4,5,6,7 are the sender nodes. The DODAG is shown at some random instant of time and node 7 is yet to begin the communication.

IV. Related Works

The authors in [7] performed a comparison between the cooja simulations and physical real-world implementation in order to understand and also analyse RPL protocol. The operating system used for this purpose is contiki-3.0 with cooja simulator making use of four Z1 motes. This paper considered overhead of control messages, the energy being consumed which is measured using the Energest tool and the rate at which packets are delivered as metrics to evaluate RPL.

In [17], a system that can be used for monitoring the light is proposed by the authors. Latency and the delivery ratio of packets are considered for analysis. The proposed work has photo diodes connected to street lights which sense the intensity of light and send this information to a border router. Further actions can be taken by observing this data which is uploaded to a server. RPL is involved in transmission of data. In [24], multiple sink nodes are used and then the RPL protocol is evaluated. The number of sink nodes are increased from 1, 5 and to 10. Sender nodes are kept to a constant value of 35. Summarization of the data that is surveyed is in table I.

In [25], the aim of the authors is to identify which objective function has to be chosen based on the scenario. Cooja simulator in Contiki-2.7 version of operating system was used

to collect information of different parameters like average

TABLE I: SURVEY DATA

Serial number	Author/Year	Technique	Advantages	Limitations	Noteworthy Results
1	M.S.Aman et al. [7]/ 2017	Nodes were deployed in an open field as well as a lobby. Data obtained is compared with cooja simulation data.	Performing physical implementation provided an edge to understand how RPL behaves in real time scenarios.	The number of nodes were limited to four.	The energy being consumed in the real experimental setup is more than that of cooja. The ratio at which packets are delivered is found to be less in real time.
2	P.T.V.Bhuvaneswari et al. [17] /2018	Using Linear topology, deployment in random order RPL parameters are found.	Along with the usually measured parameters like delay, delivery ratio of packets, the light intensity, temperature are also measured.	Complete practical set up of the work proposed is not clearly mentioned. Scalability aspect is not included.	The efficiency of random topology is better when participation of nodes other than root is considered.
3	I.Zaatouri et al. [24] /2017	Random topology with number of sink nodes increased for each simulation.	Proves that increasing the number of sink nodes, gives a decreased number of lost packets.	Limited only to cooja simulation.	More the sinks, better is the performance.
4	N.Pradeska et al. [25]/ 2016	Grid topology, random deployment of nodes is used and data is obtained using the feature sensor data collect. The collection of data is done for both the objective functions and then compared.	How RPL behaves when nodes are not stationary is observed.	Not used the latest version of contiki to perform the simulation.	The network convergence time is less for OF0 than for MRHOF. In terms of reliability MRHOF is better.
5	W.Mardini et al. [29] /2018	The period value is changed from 60 seconds to 2,5,10,15,30 seconds.	More insight of OF performance is provided	Only cooja simulation is done	The packet transmitting rate can be increased by increasing the interval of sending.
6	S.Umamaheswari et al. [30] / 2017	Random deployment of nodes, then data is analyzed. Control messages were observed by increasing the number of nodes in order to see how scalable RPL is.	Performed the simulation in an application-oriented manner.	Latest version of contiki is not used. Limited the simulation only to OF0.	As the network size grows larger, the rate at which the control messages increase is less.
7	M.D.Shirbhate et al. [37] /2018	Correlated data is routed together	Reduction in energy usage and also congestion of traffic.	Only 10 nodes are used for the simulation.	Less power is used for transmission.
8	B.Ghaleb et al. [38] /2018	If the child node's number of forwarded DAOs exceed a predetermined threshold, then they are discarded.	A counter is used with respect to child node which is reset between two DIOs to maintain consistent information.	Number of DAOs forwarded is slightly more in the proposed system than that of reference RPL model.	The consumed power amount and also the delay values are less in the proposed system when compared with the RPL under attack.
9	P.Perazzo et al. [39] /2017	The victim node is put under the impression that the information related to routing that it is sending is already sent by other nodes many times.	Better than jamming attack in terms of power consumption.	Hello flood and DIO suppression's effect is not evaluated together.	An experimental proof that the attack degrades the performance of network is provided.
10	A.Le et al. [40] /2013	The attacking node works without considering the basic rule set up for rank.	Higher security can be set by correlating between the location of attack and its impact.	Real test bed is not used.	Attack will have a higher impact in areas that have larger load of forwarding.

value of ETX and hops, delivery ratio of packets for both static and mobile nodes, average latency, time taken for the DODAG to form among few other parameters. In [29], objective function's behaviour is observed by changing the intervals at which packets are sent. The nodes are varied from 20 to 40 in number.

The authors in [30] considered a smart health system to see how RPL performs. Such a system will involve initial collection of data followed by its storage in a database and finally to take an appropriate action on analysing the data. The simulation is done for a period of one hour on cooja using contiki-2.7. The value of power consumed, delay and the ratio of packet delivery were few parameters considered. The authors in [37], used routing based on content to improve the current RPL. Routing is done by seeing what type the packet is rather than the destination. Sky motes are used and the simulation is done for a period of 20 minutes.

In [38], a solution is proposed by the authors for the DAO insider attack. SecRPL is the mechanism proposed to reduce the number of DAOs that a parent node forwards. The restriction method used is to restrict the DAOs based on the destination. Fifty nodes are used with three malicious nodes to simulate the attack. Performance is then evaluated by considering the ratio of packets delivered, delay, DAOs forwarded number.

In [39], an attack that will suppress DIO, in order to observe how RPL protocol behaves, is conducted. This will lead to formation of routes of degraded quality. A set of consistent DIOs is sent by the adversary. Nodes that receive this will then not send their DIOs. A network of 31 nodes with 5 malicious nodes is used. In [40], an attack based on rank is generated such that nodes do not choose a best parent node. A grid topology is considered with 100 nodes. A pseudo code is included in this paper to generate this attack.

V. Conclusion

For any communication system, as routing is of paramount importance, this paper includes an insight of the routing protocol RPL which suits the IoT applications. The key aspects covered in this paper are:

- RPL is explained clearly by including the DODAG formation.
- The features of Contiki OS and its associated simulator Cooja that makes it suitable for implementing RPL are mentioned.
- Works related to the respective field of concern, RPL are discussed.

Changing the objective functions and analyzing various parameters so as to see the suitability of the objective function in a scenario like that of monitoring an environment, forms the future scope.

References

[1] G. Ma, X. Li, Q. Pei, and Z. Li, “A security routing protocol for Internet of Things based on RPL,” In *Proc. 2017 International Conference on Networking and Network Applications (NaNA)*, 2017, pp. 209-213.

[2] D. Gadde and M.S. Chaudhari, “Survey on routing protocol for low-power and lossy networks,” In *Proc. 2015 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC)*, 2015, pp. 1-5.

[3] L. Li, Z. Xi, Y. Zhu, and S. Wang, “Improvement and implementation of RPL routing protocol in wireless sensor networks,” In *Proc. 11th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM 2015)*, 2015, pp.1-4.

[4] K. Heurtefeux and H. Menouar, “Experimental evaluation of a routing protocol for wireless sensor networks: RPL under study,” In *Proc. 6th Joint IFIP Wireless and Mobile Networking Conference (WMNC)*, 2013, pp. 1-4.

[5] Y. Pant and H. S. Bhadauria, “Performance study of routing protocols in wireless sensor network,” In *Proc. 2016 8th International Conference on Computational Intelligence and Communication Networks (CICN)*, 2016, pp. 134-138.

[6] A. Hassan, S. Alshomrani, A. Altalhi, and S. Ahsan, “Improved routing metrics for energy constrained interconnected devices in low-power and lossy networks,” *Journal of Communications and Networks*, vol.18, no.3, pp. 327-332, 2016.

[7] M.S. Aman, K. Yelamarthi, and A. Abdelgawad, “A comparative analysis of simulation and experimental results on RPL performance,” In *Proc. 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON),* 2017, pp. 483-487.

[8] L. Gao, Z. Zheng, and M. Huo, “Improvement of RPL protocol algorithm for smart grid,” In *Proc. 2018 IEEE 18th International Conference on Communication Technology (ICCT)*, 2018, pp. 927-930.

[9] W. Alayed, L. Mackenzie, and D. Pezaros, “Analytical hierarchy process multi-metric objective function for RPL,” *In Proc. 2018 IEEE 17th International Symposium on Network Computing and Applications (NCA)*, 2018, pp. 1-5.

[10] H. Tran, M.T. Vo, and L. Mai, “A comparative performance study of RPL with different topologies and MAC protocols,” In *Proc. 2018 International Conference on Advanced Technologies for Communications (ATC)*, 2018, pp. 242-247.

[11] E. Ancillotti, R. Bruno, and M. Conti, “Reliable data delivery with the IETF routing protocol for low-power and lossy networks,” *IEEE Transactions on Industrial Informatics*, vol. 10, no. 3. pp. 1864-1877, 2014.

[12] H.S. Kim, J. Ko, D. E. Culler, and J. Paek, “Challenging the IPv6 routing protocol for low-power and lossy networks (RPL): A survey,” *IEEE Communications Surveys & Tutorials*, vol.19, no.4, pp. 2502-2525, 2017.

[13] P. Janani,V. C. Diniesh, and M.J.A. Jude, “Impact of path metrics on RPL's performance in low power and lossy networks,” In *Proc. 2018 International Conference on Communication and Signal Processing (ICCSP)*, 2018, pp. 0835-0839.

[14] D. Airehrour, J. Gutierrez, and S.K. Ray, “A testbed implementation of a trust-aware RPL routing protocol,” In *Proc. 2017 27th International Telecommunication Networks and Applications Conference (ITNAC)*, 2017, pp. 1-6.

[15] S. Goyal, and T. Chand, “Improved trickle algorithm for routing protocol for low power and lossy networks,” *IEEE Sensors Journal*, vol.18 , no.5, pp. 2178-2183, 2017.

[16] I. Kechiche, I. Bousnina, and A. Samet, “A comparative study of RPL objective functions,” In *Proc. 2017 Sixth International Conference on Communications and Networking (ComNet)*, 2017, pp. 1-6.

[17] P.T.V. Bhuvaneswari, V. Gokilapriya, and J. Mahalakshmi, “Ambient light monitoring system for low power and lossy networks using RPL routing protocol,” In *Proc. 2018 8th International Conference on Communication Systems and Network Technologies (CSNT)*, 2018, pp. 84-88.

[18] M. Banh et al., “Performance evaluation of multiple RPL routing tree instances for Internet of Things applications,” In *Proc. 2015 International Conference on Advanced Technologies for Communications (ATC)*, 2015, pp. 206-211.

[19] M.O. Farooq, C.J. Sreenan, K.N. Brown, and T. Kunz, “RPL-based routing protocols for multi-sink wireless sensor networks,” In *Proc. 2015 IEEE 11th International Conference on Wireless and Mobile*

Computing, Networking and Communications (WiMob), 2015, pp. 452-459.

[20] C. Pu, and S. Hajjar, "Mitigating forwarding misbehaviors in RPL-based low power and lossy networks," In *Proc. 2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, 2018, pp. 1-6.

[21] S. Mishra, P. Singh, D. Arora, and K.K. Agrawal, "Analyzing and evaluating the performance of 6L0WPAN and RPL using CONTIKI," In *Proc. 2017 International Conference on Intelligent Sustainable Systems (ICISS)*, 2017, pp. 1100-1105.

[22] V. Gokilapriya and P.T.V. Bhuvaneswari , "Analysis of RPL routing protocol on topology control mechanism", In *Proc. 2017 4th International Conference on Signal Processing, Communications and Networking (ICSCN)*, 2017, pp. 1-5.

[23] A.N. Abbou, Y. Baddi, and A. Hasbi, "Routing over low power and lossy networks protocol: Overview and performance evaluation," In *Proc. 2019 International Conference of Computer Science and Renewable Energies (ICCSRE)*, 2019, pp. 1-6.

[24] I. Zaatouri, N. Alyaoui, A. B. Guiloufi, and A. Kachouri, "Performance evaluation of RPL objective functions for multi-sink," In *Proc. 2017 18th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA)*, 2017, pp. 661-665.

[25] N. Pradeska, Widyawan, W. Najib and S.S. Kusumawardani, "Performance analysis of objective function MRHOF and OF0 in routing protocol RPL IPV6 over low power wireless personal area networks (6LoWPAN)," In *Proc. 2016 8th International Conference on Information Technology and Electrical Engineering (ICITEE)*, 2016, pp. 1-6.

[26] I. Kechiche, I. Bousnina, and A. Samet, "An overview on RPL objective function enhancement approaches," In *Proc. 2018 Seventh International Conference on Communications and Networking (ComNet)*, 2018, pp. 1-4.

[27] M. Qasem, H. Altawssi, M. B. Yassien and A. Al-Dubai, "Performance evaluation of RPL objective functions," In *Proc. 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing* , 2015, pp. 1606-1613.

[28] H. Lamaazi, and N. Benamar, "RPL enhancement using a new objective function based on combined metrics," In *Proc. 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC)*, 2017, pp. 1459-1464.

[29] W. Mardini, S. Aljawarneh, A. Al Abdi, and H. Taamneh, "Performance evaluation of RPL objective functions for different sending intervals," In *Proc. 2018 6th International Symposium on Digital Forensic and Security (ISDFS)*, 2018, pp. 1-6.

[30] S. Umamaheswari, and A. Negi, "Internet of Things and RPL routing protocol: A study and evaluation," In *Proc. 2017 International Conference on Computer Communication and Informatics (ICCCI)*, 2017, pp. 1-7.

[31] Kamaldeep, M. Malik, and M. Dutta, "Contiki-based mitigation of UDP flooding attacks in the Internet of things," In *Proc. 2017 International Conference on Computing, Communication and Automation (ICCCA)*, 2017, pp. 1296-1300.

[32] N. Al-Taleb, and N. Min-Allah, "A study on Internet of Things operating systems," In *Proc. 2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT)*, 2019, pp. 1-7.

[33] P. Gaur and M. P. Tahiliani, "Operating systems for IoT devices: A critical survey," In *Proc. 2015 IEEE Region 10 Symposium*, 2015, pp. 33-36.

[34] C. Sabri, L. Kriaa, and S.L. Azzouz, "Comparison of IoT constrained devices operating systems: A survey," In. *Proc. 2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA)*, 2018, pp. 369-375.

[35] F. Javed, M.K. Afzal, M. Sharif, and B.S. Kim, "Internet of Things (IoT) operating systems support, networking technologies, applications, and challenges: A comparative review," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 3, pp. 2062-2100, 2018.

[36] A. Musaddiq et al., "A survey on resource management in IoT operating systems," *IEEE Access*, vol. 6, pp. 8459-8482, 2018.

[37] M.D. Shirbhate and S.S. Solapure, "Improving existing 6LoWPAN RPL for content based routing," In *Proc. 2018 Second International Conference on Computing Methodologies and Communication (ICCMC)*, 2018, pp. 632-635.

[38] B. Ghaleb et al., "Addressing the DAO insider attack in RPL's Internet of Things networks,"*IEEE Communications Letters*, vol. 23,no.1,pp.68-71, 2018.

[39] P. Perazzo, C. Vallati, G. Anastasi and G. Dini, "DIO suppression attack against routing in the Internet of Things," *IEEE Communications Letters*,vol.21, no.11, pp. 2524-2527, 2017.

[40] A. Le et al., "The Impact of rank attack on network topology of routing protocol for low-power and lossy networks," *IEEE Sensors Journal*, vol.13, no.10, pp. 3685-3692, 2013.