Performance Analysis of Routing Protocol for Low Power and Lossy Networks (RPL) in Large Scale Networks

Xiyuan Liu, Zhengguo Sheng, Changchuan Yin, *Senior Member, IEEE,* Falah Ali, *Senior Member, IEEE,* and Daniel Roggen

Abstract—With growing needs to better understand our environments, the Internet-of-Things (IoT) is gaining importance among information and communication technologies. IoT will enable billions of intelligent devices and networks, such as wireless sensor networks (WSNs), to be connected and integrated with computer networks. In order to support large scale networks, IETF has defined the Routing Protocol for Low power and Lossy Networks (RPL) to facilitate the multi-hop connectivity. In this paper, we provide an in-depth review of current research activities. Specifically, the large scale simulation development and performance evaluation under various objective functions and routing metrics are pioneering works in RPL study. The results are expected to serve as a reference for evaluating the effectiveness of routing solutions in large scale IoT use cases.

Index Terms—RPL, WSN, Large Scale Network, Performance Analysis

I. INTRODUCTION

THE Internet-of-Things (IoT) has become a new focus for both industry and academia involving information and communication technologies (ICTs), and it is predicted that there would be almost 50 billion devices connected with each other through IoT by 2020 [1]. The concept of IoT can be traced back to the pioneering work done by Kevin Ashton in 1999 and it is initially linked to the new idea of using radio frequency identification in supply chains. Soon after, this term became popular and is well known as a new ICT where the Internet is connected to the physical world via ubiquitous wireless sensor networks (WSNs) [2].

With the development of WSN technologies, a wide range of intelligent and tiny wireless sensing devices will be deployed in a variety of application environments. Generally, these sensing devices are constrained by limited energy resources

X. Liu and C. Yin are with Beijing Laboratory of Advanced Information Networks and Beijing Key Laboratory of Network System Architecture and Convergence, Beijing University of Posts and Telecommunications, Beijing, (Email: {lxy, ccyin}@bupt.edu.cn).

Z. Sheng, F. Ali and D. Roggen are with Department of Engineering and Design, University of Sussex, UK (Email: {z.sheng, F.H.Ali, D.Roggen}@sussex.ac.uk.)

(battery power), processing and storage capability, radio communication range and reliability, etc., and yet their deployment must cover a wide range of areas. In order to cope with those challenges, a number of breakthrough solutions have been developed, for example, efficient channel hopping in IEEE 802.15.4e TSCH [3], emerging IPv6 protocol stack for connected devices [4] and improved bandwidth of mobile transmission.

Routing, particular in large scale networks, is always challenging for resource constrained sensor devices. The IETF Routing Over Low-power and Lossy networks (ROLL) working group has been focusing on routing protocol design and is committed to standardize the IPv6 routing protocol for Low-power and Lossy Networks (LLN). RFC6550 [5], first proposed by ROLL group of IETF in the form of draft to define Routing Protocol over Low Power and Lossy Networks (RPL), serves as a milestone in solving routing problems in LLNs. Due to the limitation of short-range radio in personal area network (PAN) and local area network (LAN), multi-hop transmission is necessary in large scale networks. RPL is designated to provide such a viable solution to maintain connectivity and efficiency in a cost effective way. However, there is a lack of existing literature in evaluating the RPL performance in large scale networks.

In this paper, we focus on the comprehensive review of RPL protocol and its performance in large scale networks. Our contribution can be summarized as follows:

- We make a deep analysis of objective functions and metrics in RPL under varied scenarios, with references to the latest literature and studies, which can fundamentally contribute to the understanding of RPL performance and provide inspiration to raise more viable methods to further improve the network performance. An extended discussion of security issue and future challenges are also included.
- We make the first attempt to build a large scale network using RPL and provide analytical results under different objective functions. A more practical scenario incorporating UDP, IPv6 and 6LowPAN has also be considered in the analysis.
- We make an investigation on network simulation tools and select OMNeT++ as the ideal one for a large scale RPL simulation. We have fully implemented the RPL protocol according to IETF specifications in OMNeT++ and discussed its performance. The source code is also

supplemented online to support further study by the research community.

The rest of the paper is organized as follows. Section II gives an overview of RPL definition. Section III discusses the current Objective Functions and routing metrics in RPL. Section IV introduces simulation platforms and our practice in developing RPL as well as its performance analysis. Section V provides further discussions on the applications of RPL in reality. Based on the research findings in previous sections, a future prospect and challenges are raised in Section VI. The conclusion is then given in Section VII.

II. INTRODUCTION OF RPL

LLNs are resource constrained networks in terms of memory, energy and processing power. IETF ROLL Working Group mainly focuses on the routing in LLNs and has proposed RPL in RFC6550 [5]. RFC6550 was firstly released in March 2012 and then a number of supplementary and supportive RFCs and Internet drafts have been progressed. For instance, RFC6997 [6] is aimed at clarifying the specified route discovery mechanism, while RFC7416 [7] is with the purpose of strengthening the security issues in RPL.

With the development of IoT, RPL is entitled to new chance for the development of wireless sensor networks in a large scale. It is able to meet the specific routing requirements of application areas including urban networks (RFC 5548) [8], building automation (RFC 5867) [9], industrial automation (RFC 5673) [10], and home automation (RFC 5826) [11]. Among those mechanisms standardized in RPL, routing and message control are two important mechanisms in establishing and maintaining an effective and reliable network, which will be highlighted in details as follows.

A. Routing Mechanism of RPL

RPL is a distance vector routing protocol. It does not have predefined topology but will be generated through the construction of Destination-Oriented Directed Acyclic Graphs (DODAGs). Directed Acyclic Graphs (DAGs) describe tree shaped structures. However, a DAG is not a traditional tree structure in which one node is allowed to have multiple parent nodes. The DODAG, with sink node or the node providing default routing to the Internet as the root node, is a direction-oriented graph.

The construction of network topology is controlled by three types of control message - DODAG Information Object (DIO), DODAG Information Solicitation (DIS) and Destination Advertisement Object (DAO) messages. They all belong to RPL control message, which is an Internet Control Message Protocol (ICMP) information message type with type value 155. DIO message is used for upward routing construction, which is essential for establishing communication from non-sink nodes (or multiple points) to the sink node (one point). Such Multipoint-to-point (MP2P) mode is dominating the RPL applications. The construction of upward route of RPL is realized by DIOs. The sink node will first broadcast DIOs, the nodes receiving the DIO directly from the sink node become its neighbours. By setting the sink node as their parent nodes,
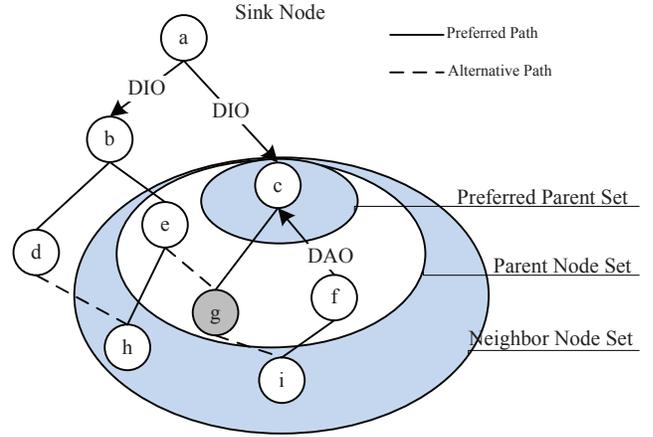

Fig. 1. An example of DODAG and node set relationships.

those neighbour nodes will re-broadcast DIOs to further nodes. The similar step will repeat in such way that the DODAG topology is constructed through handling DIOs and building parent sets. DIS message is used for soliciting the sending of DIO in order to make immediate response to network inconsistency. The structure of DIO message is presented in the following subsection.

DAO message is used for downward routing construction (Point-to-Point and Point-to-multipoint). There are two modes of downward routing - storing and non-storing modes, which indicate that the routing table information is stored in intermediate nodes (non-root and non-leaf nodes) and root node, respectively.

An Objective Function (OF) defines the rule of selecting neighbours and parent nodes by rank computation. Routing metrics related to link or node characteristics (RFC6551 [12]) can be used by OF to make routing determination. One of the widely used OF0 is defined in RFC6552 with hop count as the routing metrics. OF determines Neighbour Set, Parent Set and Preferred Parents according to specified routing metrics and constraints. The node set selection is involved in the route discovery process and indicates the best path computation. The rank of a node must be larger than that of its parent node, in order to avoid routing loops.

It is worth noting that in order to construct a valid RPL routing, firstly, candidate neighbour node set must be the subset of nodes that can be reached through link local multicast. Secondly, parent set is the subset of candidate neighbour set which satisfies specific limitation conditions. Thirdly, preferred parents are those with optimal path characteristics. If there exist a group of nodes with equivalent rank and preferred extent regarding the metrics calculation, there can be more than one preferred parent nodes. Fig. 1 illustrates logical relationships of candidate neighbour node set, parent node set, and preferred parent node of the node.

B. Message Structure of DIO

DIO message is the most fundamental control message in RPL's topology construction process. Fig. 2 outlines its structure.
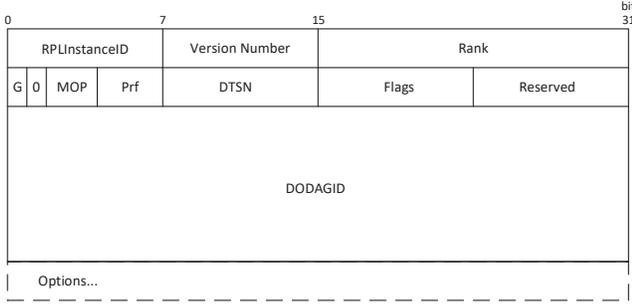
0			7		15		bit 31
RPLInstanceID			Version Number		Rank		
G	0	MOP	Prf	DTSN	Flags		Reserved
DODAGID							
Options...							

Fig. 2. DIO format.

0	7	bit 13
Type = 0x02	Option Length	Metric Data

Fig. 3. DAG Metric Container.

0	7	15			bit 31
Type = 0x04	Opt Length = 14	Flags	A	PCS	DIOIntDoubl.
DIOIntMin.	DIORedun.	MaxRankIncrease			
MaxHopRankIncrease		OCP			
Reserved	Def. Lifetime	Lifetime Unit			

Fig. 4. DODAG Configuration Option.

Fig. 5. Structure of DIO message in our simulation

DIO carries information that allows a node to discover a RPL Instance, learn its configuration parameters, select a DODAG parent set, and maintain the DODAG [5]. The main fields of DIO message include Version Number, DODAGID and RPLInstanceID. Version Number is used within a DODAG, DODAGID is used within a RPL Instance. The 'G' flag indicates whether the DODAG is grounded or floating. DODAGPreference is used when there exist multiple DODAG and defines the preferable root. Rank indicates the DODAG rank of the node when sending the DIO. Mode of Operation (MOP) and Destination Advertisement Trigger Sequence (DTSN) are used in maintaining the downward routes. In our simulations, we have defined the DIO in an independent structure as shown in Fig. 5. The basic fields of DIO format are included in the DIO structure definition. Some fields, such as Flags and Reserved, are not included in our definition since they are not used in our simulation, which can be added if necessary. According to the requirements in RFC6550 [5], the DODAGID is 128-bit length defined by the DODAG root to uniquely identify a DODAG. In our simulations, we set the DODAGID field in the form of a unique 128-bit IPv6 address.

As can be seen in Fig. 2, DIO message can be extended with the use of options, which include the DAG Metric Container Option in Fig.3 and configuration option in Fig. 4. The DAG Metric Container Option exists not only in DIO, but also in DAO. It can carry multiple chosen metrics and constraints, which are in the form of Routing Metric/Constraint object. The Routing Metric/Constraint object can present in any order in Metric Data in DAG Metric Container [12]. The routing metric data is also declared in the DIO structure in our simulation. If there exist multiple routing metrics in the DODAG, for example, the RSSI-ETX Objective Function discussed in Section IV is composed of Received Signal Strength Index (RSSI) and ETX, we will declare all of them in DIO as shown in Fig. 5.

The DODAG Configuration Option is an important option in DIO structure. It is used to report the configuration information through the DODAG. Therefore, It contains the trickle timer config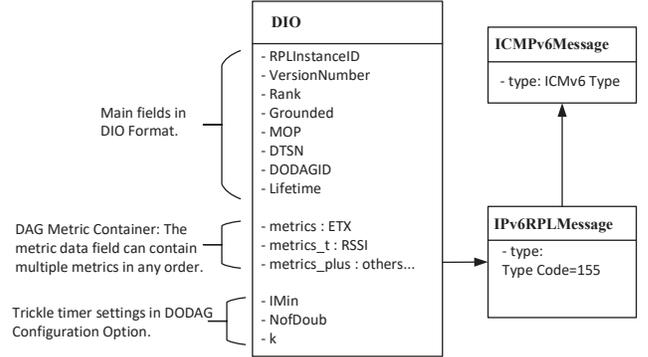uration parameters of message mechanism, including DIOIntMin (I_{min}), DIOIntDoubl (I_{max}) and DIORedun (k), which will be further explained in the following subsection. The rank calculation parameters, including *MaxRankIncrease* and *MinHopIncrease*, are also contained in this option. Generally, this option is usually configured and only allowed to be modified by DODAG root. Unlike the main fields in DIO format and DAG Metric container, which can be changed in the simulation, DODAG Configuration Option is kept unchanged through the simulation and therefore is defined in the configuration file of the simulation as shown in table IV in section IV.

C. Message Control Mechanism of RPL

It is obvious that any routing mechanism involves significant control overhead in a large-scale network. Particularly in a multi-hop network, an effective message control mechanism is significantly important in reducing network overhead and balancing limited network resources.

Trickle timer mechanism [13], which is mainly used by DIO, has been emphasized as an important part of message control mechanism. A Trickle timer is implemented based on trickle algorithm and is able to detect and respond to network inconsistency and instability. Particularly, the inconsistency of RPL is occurred in the following circumstances: detection of routing loops, first time joining a DODAG and rank change of a node. The fundamental mechanism of trickle timer is shown in Fig. 6. It is worth noting that the frequency of sending messages which is decided by the trickle timer can be dynamically adjusted to stabilize the network and govern the network status as well as improve the energy efficiency.

In the trickle timer process, let t denote the time for sending message, C the counter indicates whether the network is
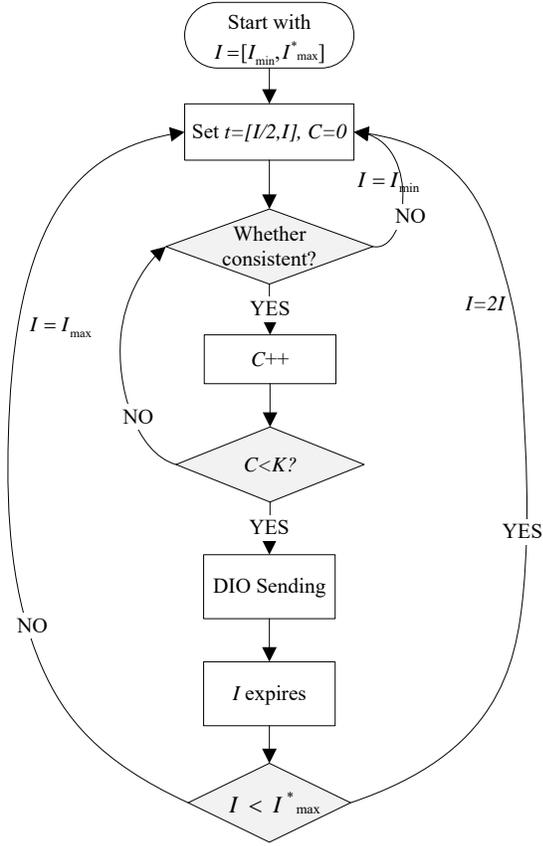
Fig. 6. Trickle timer process.

	RPL	LOAD-ng
Routing Mode	Active	Reactive
Delay	Shorter	Longer
Storage Requirement	Less	More
Complexity	More	Less
Control Overhead	More	Less

known routing protocols, such as Open Shortest Path First (OSPF) and Intermediate System to Intermediate System (IS-IS), are not suitable for the LLNs because they will lead to excessive control traffic in constrained environment. Moreover, the large volume of routing traffic can also pose a threat to lossy links and rapid-in-change networks.

The comparison between RPL, LOAD, and Geographical routing [15], in the case of advanced metering infrastructure (AMI), shows that LOAD fails to satisfy the requirements of LLNs regarding control overload, end-to-end delay and reliability. The next generation alternative, LOAD-ng, which is also raised by IETF working group, is the representative of reactive routing while RPL is active routing. Under two cases of MP2P and P2MP traffic flows, in which the downward routing considers both storing and non-storing modes [16], both of the two protocols perform closed in link quality and delay. RPL also suffers from instability in control overload, which is similar for LOAD-ng in the multicast situation. However, the reactive routing requires a larger cache. A brief comparison between RPL and LOAD-ng is shown in table I.

Compared with LOAD-ng and other routings in IoT, RPL is much more complex. The complicated types and options in control messages not only increase complexity in practice, but also elevate the hardware requirements in storage when it comes to the practical deployment.

consistent or not; predefined parameters include redundancy constant k, minimum time unit I_{min}, and maximum time unit I_{max}. I_{max}^* denotes the maximum time period specified by the time units. Time consumption to transmit k packets is represented by t_K. Typically, we have

$$I_{max}^* = I_{min} \cdot 2^{I_{max}} \qquad (1)$$

$$I_{min} = (2 \sim 3) \cdot t_K \qquad (2)$$

Configuring the trickle timer with appropriate parameters is vital since it will influence the network reliability and stability [14], especially in large-scale networks. The redundancy constant k for each node should be carefully chosen in order to avoid mismatching values among all nodes in the network or being infinity which can lead to uneven load of traffic flow, depletion of energy or congestion in dense networks [13]. I_{min} also needs to be set accordingly to avoid congestion and high packet loss. In our study, we find out that the appropriate value of I_{min} falls into a fixed time period, which may be different in other simulators or settings. Particularly, with an inappropriate value of I_{min}, the packet delivery rate will be decreased.

D. RPL and Its Counterparts

The development of wireless sensor networks has contributed to proposals of a variety of routing protocols. LLNs have their specific requirements on routing. The commonly

III. OBJECTIVE FUNCTIONS AND METRICS OF RPL

The topology of RPL is constructed according to specific OFs, which are configured according to metrics and constraints. OFs are responsible for constructing routing and providing optimal routing choice by determining DODAG topology and rank of each node. In the following, we summarize several typical OFs used in RPL.

1) Hop Count: It is one of the two well defined Objective Functions and also used as routing metrics. Hop count is the most commonly used routing metrics and it is deployed in the network routing calculation with the Hop Count OF.

2) ETX: Expected Transmission Count defined in RFC6551 [12] can also be used as routing metrics for OF in LLNs. The ETX metric is the number of transmissions a node is expected to a destination in order to successfully deliver a packet. With a higher value of ETX, the link quality may be worse. It is an addictive metrics since it will add the ETX of each link along the path to the destination.

3) Per-Hop ETX: The combination and optimization of classic metrics can also bring better performance. Xiao

et al. in [17] integrated the two traditional metrics - hop count and ETX into per-hop ETX. The new proposed metric is based on the addictive nature of ETX. It is demonstrated that calculating link metrics by dividing the aggregated ETX through the path using hop counts can improve packet delivery rate, delay and energy cost.

4) Stability Based OF: Iova *et al.* [18] offered an overview and outlook against RPL from aspects of reliability, end-to-end packet delivery rate, end-to-end delay and energy cost. Through comparisons and observations of OFs with metrics including hop count, ETX and link quality index (LQI), it reveals the tradeoff between network stability which is mainly reflected by switching frequency of parent nodes, and the routing reliability. A deeper understanding of the issue regarding stability can be found in [19]. By taking numbers and frequency of control messages into consideration, the authors proposed a solution that combines DIO, DAO and DIS with given relative weights into one measurement for a specific node. Through this method, the packet delivery rate can be significantly improved, the control plane overload is largely deducted and the network stability is enhanced with reduced parent nodes switching times.

5) Energy Based OF: It is also interesting to consider energy based OF given that energy efficiency is highly required in large scale sensor networks. Actually, the power-supply of nodes is quite complex, therefore, in the structure of routing metrics, there is a field indicating the power-supply type [12]. The power-supply sources include powered, battery and scavenger. Regarding different power-supply means, how to accommodate with various energy characters is a thought-provoking issue. Patrick *et al.* brought minimum path loss [20] into the definition of metrics, which is defined as the minimum node energy level that captures the energy-based path weight. It keeps the principle that parent nodes with maximum remaining energy is preferable and demonstrates satisfactory performance in network longevity and overload balance compared with ETX metrics. Existing literature also proposed to integrate node energy with other metrics. Capone *et al.* [21] combined node energy with ETX. By referring to the exponent of a ratio of transmission power and remaining energy and incorporating it with ETX, the method can gain improvement in network longevity and node energy.

Other solutions such as in RFC6551 [12], a series of metrics and constrains related to node and link attributes in RPL are proposed. Table II summarizes classic and recently proposed OFs of RPL with metrics used, key observation parameters and performance of the metrics.

One unique feature of the tree-based topology in RPL is that a node can possibly have multiple parent nodes. As described in RFC6550 [5], each node only chooses one preferred parent node to forward data packets to sink node, even though the node may store multiple parent nodes information in the parent set. RPL does not implement the parent switching mechanism, thus a node with a large number of child nodes will run

TABLE II
OBJECTIVE FUNCTIONS COMPARISON.

Routing Metrics Used	Observation Parameters	Key Features
Hop count [12]	Hop count between two nodes	Small end-to-end delay in sacrificing packet delivery rate
ETX [12]	Expected transmission count of data packet between two nodes	Packet Delivery Rate (PDR) is higher, increased delay
LQI [18]	Link quality data from the wireless chip after receiving data packets	End-to-end delay increases with an increase of PDR
Per-Hop ETX [17]	Expected transmission count of data packet per hop between two nodes	Delay and PDR are improved to some extent, the energy requirement is less in large scale networks
Stability Index [19]	Numbers of DIO, DIS and DAO in the network	PDR is improved a lot while the number of control message is largely reduced
Path loss metrics [20]	Remaining energy of nodes	Increased Network longevity and evenly distributed energy consumption
ETX and energy composite metrics [21]	Energy parameter of nodes and ETX	Increased network longevity, given the same overall degree of network reliability
Expected Longevity [22]	Energy of nodes and ETX, forwarding according to specific probablity	Increased network longevity

out of energy easily. To increase the stability of network and make full use of the candidate parent nodes to better balance the network overload, multi-parents selection is considered by some existing works.

The non-uniform flow distribution is likely to deplete some extensively selected nodes, which will be the bottlenecks and have significant impact on the longevity of the whole network. Additionally, nodes closed to the sink or with lower rank, tend to be more congested and with high energy cost. Capone *et al.* [21] proposed the expected longevity based metrics that considers both energy and ETX. The essence of the idea is that the network flow should be balanced when data packets are forwarded to different parent nodes according to certain probability, which will help improve the network longevity.

ROLL group proposed an alternative approach by dividing RPL into clusters [23] within which nodes form to determine their parent nodes and construct the sub-topology. The RPL-based clustering scheme takes into account the remaining energy of cluster head based on the hierarchy of RPL topology as a sub-optimal parent for cluster member nodes. Therefore, the multi-parents issue can be transformed into clusters problem in RPL [24]. The proposed solution with opportunistic packet forwarding and priority mechanism, has been shown to obtain reduced delay and retransmission times compared with traditional RPL.

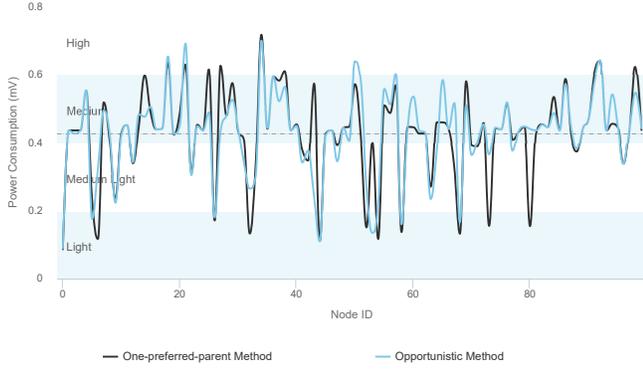As shown in Fig. 7, the data is obtained from OMNeT++

Fig. 7. Energy consumption of 100 nodes with one-preferred-parent method and opportunistic method [24].

simulation platform with basic settings in Section IV. We run the simulation with a duration of 100s during which the topology construction and packet forwarding have been finished and assume that nodes with zero energy will quit the topology immediately. According to the average energy consumption of 100 nodes using the two methods, the opportunistic forwarding method has a lower standard deviation (12.235) than the one-preferred-parent method (13.485) while the total consumption of the both are closed, which indicates that more balanced energy consumption can be achieved in the opportunistic method.

IV. LARGE-SCALE RPL SIMULATION USING OMNET++

A. Simulation Platforms

So far there are a number of software tools [25], [26], [27] that can be used for evaluating RPL performance. However, this is not always the case for a large-scale simulation. Table III summarizes the key features and large-scale simulation capacity of major simulation platforms.

In our study, we consider to use OMNeT++[1], which is event triggered, time discrete open source network simulator, and based on module construction and realization. It is capable of implementing RPL simulation at a larger scale as well as with advantages at other aspects, such as ease access of OMNeT++ frameworks for different network scenarios, functional output API to obtain a series of targeted data.

B. Framework Integration for OMNeT++

The RPL simulation is developed based on the integration of INET 2.2.0[2] with MiXiM 2.3[3]. The latest version INET 2.3 has already incorporated several functions from MiXiM. Both of them are the most prevalent frameworks in OMNeT++.

INET is a simulation framework with comparatively mature network layer realization. Its IPv6 network layer has been realized with diversified sub-modules, taking into account neighbour discovery functions and its message mechanism, including Neighbor Advertisement (NA), Neighbor Solicitation (NS), Router Advertisement (RA), and Router Solicitation

[1]https://omnetpp.org
[2]https://inet.omnetpp.org
[3]http://mixim.sourceforge.net

(RS) handlings. Here we incorporate the IPv6 mechanism to construct RPL related functions. The routing table can store parents information, which is necessary in RPL DODAG construction.

MiXiM framework is well known for its realization of MAC and physical layers, especially IEEE 802.15.4. In our study, the CC2420 radio model is used for IEEE 802.15.4 MAC and PHY. Moreover, its battery module has been developed with a liner model which is more reliable in battery consumption observation. Here we deploy SimpleBattery module in MiXiM to model the energy consumption of networks and will mainly focus on the realistic results of Tx power consumption [35].

Moreover, INET framework provides several mobility models that can be easily utilized in the simulation, such as the mobility model in which the node randomness is controlled by the linear model, the Gauss-Markov model, etc. We only consider the stationary scenarios, therefore the StationaryMobility model is used as shown in table IV.

With the integration of the above frameworks, we are able to run experiments with flexible parameters to observe the performance of large scale RPL under various circumstances. Specifically, the integration offers an experimental basis to construct networks with specified functions, such as implementing new OFs, Metrics, Constraints, etc.

C. Configuration Details

We build our network layer based on IPv6 module in INET, the IEEE 802.15.4 MAC and PHY layer in MiXiM through 6LoWPAN adaptation. The upward routing has been realised with DIO and DIS messages mechanism. The DIO messages are implemented with trickle timer. The parent and routing selections are decided by an extra class corresponding to the OFs we defined. The basic parameters of layers are defined in a .ini configuration file and the topology can also be preconfigured, which can be either randomly set or according to certain patterns. The source code is made available[4] for further reference. With the node structure implemented above, the RPL mechanism can be implemented in the following three aspects.

1) The RPL message mechanism is defined and achieved in **IPv6NeighborDiscovery** module. It replaces the default RA and RS message functions. The module is deployed with DIO and DIS messages handling and responsible fpr undertaking the update of preferred parents and path selection.
2) **RoutingTable** module plays a valid role of recording related routing information and making routing choice when forwarding packets. It mainly serves as a storing module that records the routing information and completes parent node selection.
3) The DODAG construction and rank computation obeys certain Objective Function, which exists as an independent class completely performing the minimum cost routing path selection. This paper mainly focuses on metrics analysis, therefore multiple OFs with different

[4]https://github.com/qqbzg/rpl_omnet

TABLE III
SIMULATOR COMPARISONS FOR SUPPORTING RPL.

Simulator	Support for RPL	Support for Large-scale Simulations	Supported Platforms and Programming Languages
JSim [28]	• Supports multiple protocols while the only MAC protocol can be used is IEEE 802.11, which is a limitation in supporting RPL in JSim • Inactive since 2006	• Able to support simulation scale around 500 nodes while the execution takes longer time • Complicated to use and less efficient	• Linux, Mac, and Windows • Java and tcl script language
Cooja [29]	• Fully support of RPL • Part of contiki OS • No specific energy consumption model	• Relatively low efficiency • Limited simulation scale with 200-500 nodes • Long processing time	• Linux, Mac, and Windows • Standard C
TOSSIM [30], [31]	• TinyRPL supports MP2P, P2P, P2MP traffic in RPL • However, TinyRPL is not supported on the TOSSIM simulator which requires a micaz binary. Therefore, it is not fully support RPL simulation	• Able to support thousands of nodes	• TOSSIM is designed specifically for TinyOS applications to be run on MICA Motes • C++ and python
Ns-2 [32]	• Object-oriented design which allows for straightforward creation and use of new protocols • Extensible for general WSN simulation • Fail to simulate problems of the bandwidth, power consumption or energy saving in WSN	• Only support less than 100 nodes • Rather complex and time-consuming • Only slightly maintained now	• General simulator and compatible with Linux, Mac, and Windows • C++ and OTcl
Ns-3 [33]	• Not backward compatible with Ns-2 • Modelling of Internet protocols and networks work • Weak in MAC and PHY layer development support	• Support of large scale but more nodes beyond 400+ may lead to unrealistic results.	• General simulator and compatible with Linux, Mac, and Windows • C++ and python scripts
OMNeT++ [34]	• Offers various frameworks to deploy the network with RPL while the integration of available modules may introduce compatible problems • Extensible for general WSN simulation • Support energy consumption and mobility models	• Scale-free simulator	• General simulator and compatible with Linux, Mac, and Windows • C++ and NED language

metrics need to be deployed separately. We deploy **OF** as a single class file in the simulation, such that hard codes can be avoided and it is easy to be replaced and updated accordingly, which provides enough flexibility and extensibility. Fig. 8 summarizes the simulation architecture that combines the frameworks, node structure, and fundamental mechanisms.

We consider the messages that have been defined in RFCs - DIO and DIS for upward routing, which are the triggers for DODAG construction. We have defined the main fields of the

control messages, which have been discussed in the Message Structure of DIO part in section II. In our simulation. the content of DIO and DIS messages is included in the *.msg* file. The essential key options for routing selection are contained in messages. For example, Fig. 9 shows the handling procedures across layers when a message uses received signal strength index (RSSI) as the key option. The RSSI information needs to be transmitted across layers and finally be utilized for path selection in **IPv6NeighborDiscovey** module. It is worth noting that Fig. 9 deploys RSSI based handling. Other key
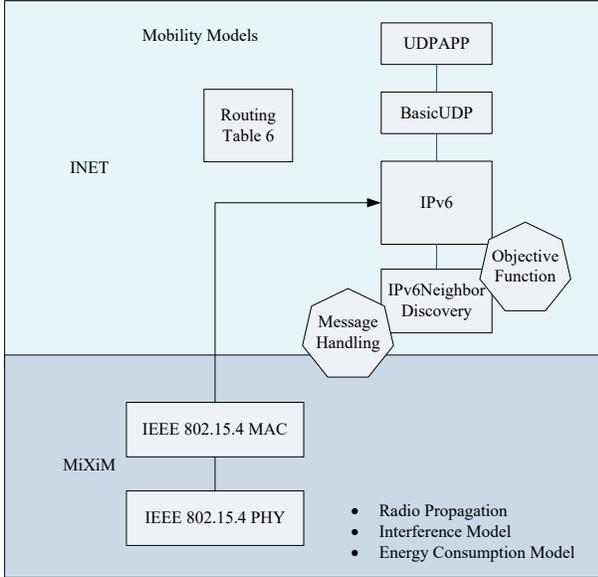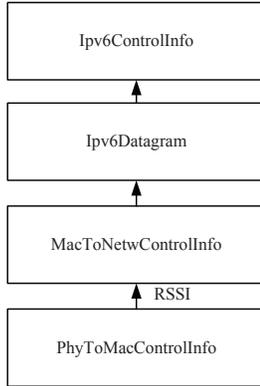
Fig. 8. Simulation construction structure.

Fig. 9. Message handling procedure cross layers for RSSI based handling.

TABLE IV
PARAMETERS OF RPL SIMULATION IN OMNET++.

	MAC Layer	
	macTransPower	1 mW
	macMinBE	1
	macMaxBE	6
	macMaxCSMABackoffs	20
	rxSetupTime	0.1 s
MiXiM	macAckWaitDuration	0.000864 s
	Phy Layer	
	phySensitivity	-100 dBm
	phyMaxTXPower	1.1 mW
	AnalogueModel	LogNormalShadowing
	Connection Manager	
	carrierFrequancy	2.4e9 Hz
	pMax	60 mW
	AttenuationThres	-84 dBm
	Trickle Timer	
	DIOIntMin (I_{min})	0.75 s
	DIORedun (t_K)	10
	DIOInetDoubl (I_{max})	8
	Topology Formation	
INET	Start Time	0 s
	Simulation End Time	300 s
	UDPApp (Packet Generation)	
	Size of Packet Payload	60~1000 Bytes
	StartTime (from)	60 s
	EndTime (stop at)	60.19 s
	Interval	0.02 s
	Destination Node Id	0
	Source Node Id	All nodes except 0
	Mobility	
	Mobility Type	StationaryMobility
	Playground Size	480 m×480 m

options may only involve the top two layers if there is nothing to do with the PHY or MAC layers. Table IV shows the parameter configuration in our simulation. The parameters in PHY and MAC are set according to the CC2420 datasheet. The trickle timer parameters have been explained in Section II. Fig. 10 depicts an example of random topology generated by OMNeT++ with 100 and 500 nodes, respectively.

D. Cross-layer Issues

RPL is compatible with a variety of MAC and physical protocols, especially IEEE 802.15.4. Since MAC and physical layer parameters have direct impacts on the link reliability as well as energy consumption, taking a cross-layer approach to incorporate low layer elements into metrics design may offer extra benefits for routing.
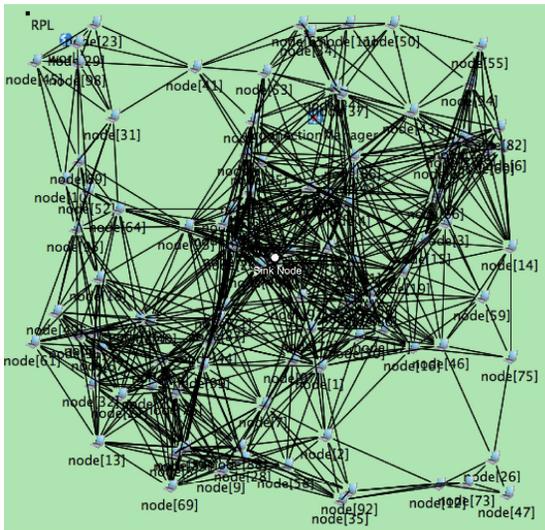
Sheng *et al.* in [36] proposed a novel method combining multipath topology with duty cycle ratio in MAC layer. It proves the sustainable network performance with the dynamic duty cycling adjustment. Marco *et al.* [37] proposed a re-liability metric based on the Markov analysis model [38]

and designed an algorithm with backwards and retransmission times of forward flow in IEEE 802.15.4. The forward flow contains flow generated by the node itself and relayed flow from child nodes. Compared with ETX, it takes the packet loss into account. Besides, in order to better balance the flow in the whole network, an optimized metric is also proposed to integrate itself flow and relayed flow with sending and receiving power, respectively. Sajan *et al.* [39] proposed a cognitive radio network (CRN) based RPL protocol by utilizing six frequency channels between nodes to represent the channel availability obtained through efficient spectrum sensing algorithm. The main contribution lies in the routing repair functions regarding different channels with trickle timer of RPL.

To illustrate the cross-layer impact on the network performance, we develop a simulation experiment using OMNeT++. Particularly, under the same simulation settings, the OFs are compared among hop count, ETX and a tailored ETX with a correction factor - RSSI (RSSI-ETX), which is incorporated into the classic ETX to further rectify the deviation of link quality. RSSI is calculated as the maximum received signal strength in a time period from its last packet reception to

(a) 100 nodes
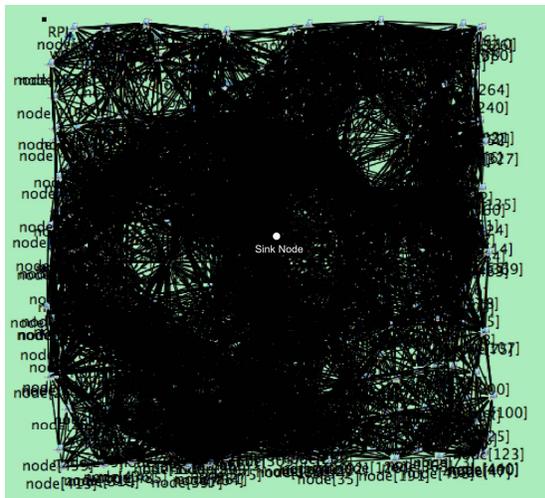
(b) 500 nodes

Fig. 10. A random topology with 100 and 500 nodes developed by OM-NeT++.
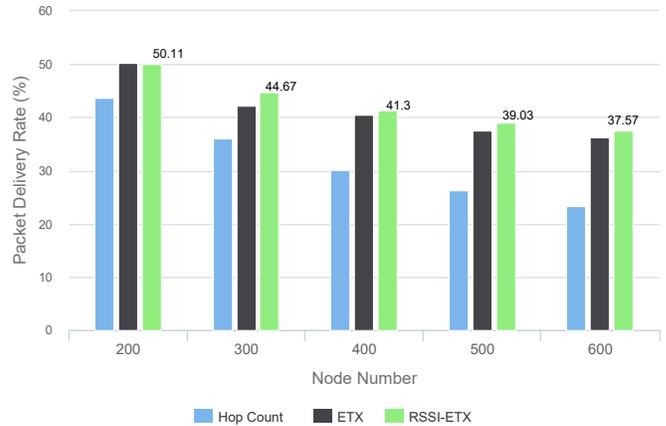

Fig. 11. Packet delivery rate versus network scale under different Objective Functions.
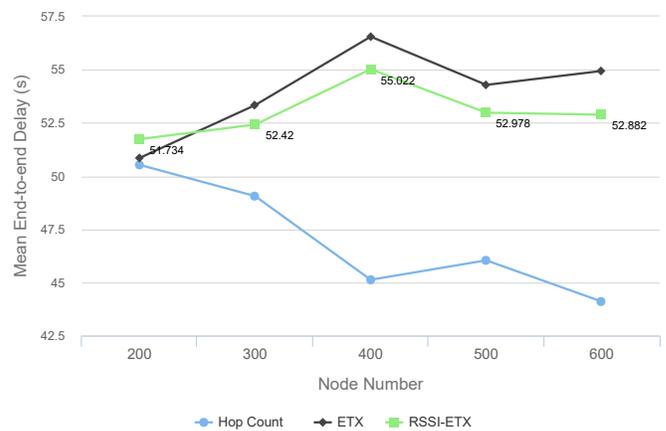

Fig. 12. Mean end-to-end delay versus network scale under different Objective Functions.
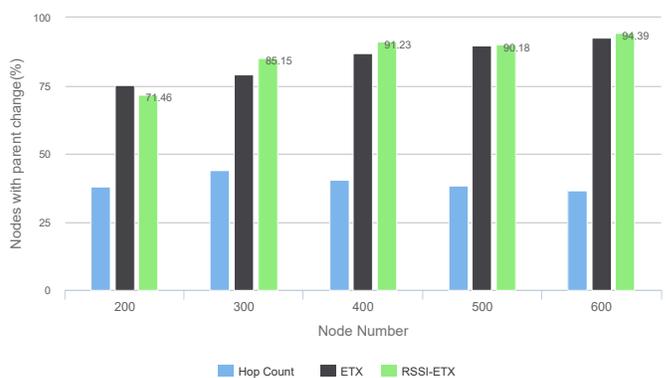
Fig. 13. Percentage of nodes with parent change under different Objective Functions.

the current reception. It will be logarithmically recorded and then combined with ETX. The role it plays is as a deviation controller to the ETX.

We consider the simulation with the network size from 200 nodes to 600 nodes connected by log-normal shadowing channel for a period of 300 s with a fixed UDPApp payload size of 60 bytes. The time schedule of data packet transmitting is shown in UDPApp parameters in Table IV. The data packets generation is initiated from 60 s when a comparatively stable topology can be formed from the beginning of the simulation (0 s). The simulation result is averaged over 5 dependent trials with different random seeds[5]. As depicted in Figs. 11 and 12, packet delivery rate and mean end-to-end delay are shown, respectively. The maximum number of hops in the simulation is 12. It is worth noting that the general packet delivery rate in

[5]Random seeds are generated with Mersenne Twister as a random sequence. The random seed can be set differently for each module. For example, the random seed will determine the random time unit generated in the trickle timer at network layer.

Fig. 11 is lower compared with the simulation results in [40] because of the high packet loss in multi-hop networks and burst transmissions simultaneously in the same time frame, which causes significant congestion and interference. In Fig. 12, we only consider the time delay of successful packet delivery. The retransmission and buffering have not been taken

into account in our study. The increase of network size will lead to more hops when a node undertakes the parent selection process and therefore causes a longer delay. However, for the hop-based approach, the increasing density of nodes can lead to a better selection of path with minimum hops, hence its mean end-to-end delay presents decreasing trend. When RSSI element is considered, the rectified OF performs better in a comprehensive view in packet delivery rate and mean end-to-end delay. Fig. 13 shows the percentage of nodes with parent change which reflects the extent of dynamic adjustment in the network during the simulation. A higher change rate indicates a more dynamic network topology and prompt response to link quality. However, we should admit that the overhead imposed by dynamic change will be a bottleneck for large scale deployment. In essence, the benefits by reflecting physical communication channels and signal behaviours on upper layers do play a vital role in routing communications, however, the performance trade-off between packet delivery rate, delay and maintenance overhead should be well considered in large scale network design.

V. RPL APPLICATIONS

RPL provides routing solutions for a wide scope of application areas including urban networks, building automation, industrial automation, and home automation. In different use cases, adaptation of RPL need to be considered to ensure optimized network performance.

1) Smart Grid (SG): It has attracted much attention in both academia and industry. By monitoring energy usage and feedback responses automatically, SG is able to balance the energy distribution based on the power necessity. Countries including China, Japan, South Korea and Australia have invested extensive funding in the next-generation grid technology. The European Union set a target to deploy smart meters for more than 80% of customers by 2020. For Africa/Latin America, countries are directly investing smart grid or indirectly utilizing renewable energy, which will ultimately require more advanced SG techonology [41].

   There is no denying that RPL plays a prominent role in Smart Grid deployment and is expected to be the standard routing protocol in AMI[6] applications. The methods of rank computation as well as failures handling have been considered in AMI [42]. Ancillotti et al. [43] made a comprehensive elaboration and evaluation of RPL in AMI. They investigated the packet loss distribution of nodes in the network and pointed out that the scale of network and density of flows have significant impact on the network performance under AMI infrastructure applications. Ancillotti et al. in [44] made another research on RPL in AMI and proposed optimal methods for protocol deployment considering the presence of duty cycling with different RPL prototypes based on Contiki simulation platform.

---

[6]AMI (Advanced Metering Infrastructure) is an important part of Smart Grid. AMI can be considered as an advanced version of Automated Meter Reading (AMR), which is capable of setup two way communications with meter devices.

SG is composed by power system and smart grid communication network (SGCN). The latter can be partitioned into home area network, industrial area network and neighbour area network. Regarding smart grid under neighbour area network that involves devices at premises and utility monitors, Ho et al. [45] added positive parents switching functions in the RPL design which requires nodes to change their parent nodes proactively when packets are not received until certain number of trials. The packets will be disposed if the switching times equal the number of candidate parent nodes. The proposed solution would definitely result in topology changes by providing dynamic updates.

2) Machine-to-Machine (M2M): It is able to realize autonomous communication and require no outer assistance to closed systems in a variety of fields. Aijaz et al. [46] summarized routing protocols design for M2M and proposed to modify RPL to adapt to cognitive radio. They also acknowledged the role of RPL as a standard routing protocol in the future M2M development.

3) Agriculture Greenhouse: Quynh et al. [47] proposed a multi-path RPL protocol for the greenhouse environment monitoring system. According to the real-life greenhouse deployment and scale of the network, the proposed method can improve RPL with better energy balance and faster local repair, compared with the traditional hop count based RPL. The authors verified that RPL satisfies the requirements in greenhouse circumstances and can achieve better performance in packet delivery rate, time delay and packet error at the base station with multi-path improvements. The greenhouse scenarios provide decent results of RPL performance with consideration of hop count and residual energy.

4) Medical Applications: Gara et al. [48] considered such a use case with dynamic and hybrid topology and implemented a modified RPL in which the mobile nodes are implemented as leaf nodes and only send DIS to request parent without broadcasting DIO. The modified RPL shows better performance compared with native RPL in supporting low mobility nodes, which is indispensable in healthcare and medical applications.

In essence, the deployment of RPL should be adapted to real application scenarios, and further investigations of the diversified RPL deployments, especially those related with smart devices, are necessary in promoting the future development and applications of RPL. Table V summarizes the major RPL applications with topology features and metrics characteristics.

VI. CHALLENGES AND FUTURE WORK

So far we have discussed RPL from different aspects. Although it is emerging as a comprehensive routing solution to general wireless sensor networks, there are still challenges as follows.

A. Transmission Mode

Currently, the prominent transmission traffic type in RPL is MP2P, that is, the upward routing implemented by DIO, which

TABLE V
RPL APPLICATIONS AND METRICS.

Application Scenarios	Topology Features	Metric/Objective Function Characteristics
Smart Grid [44], [45]	Large-scale and dense distribution	• Parents switching autonomously • Appropriate duty cycling
M2M (General Scope) [46]	Heterogeneous sensor system and involves a large number of devices	• Multiple next hops • Best forward selection
Agriculture Greenhouse [47]	Heterogeneous information system	• Multipath • Hop count and residual Energy
Medical Applications [48]	Mobile nodes; Dynamic and hybrid topology	• Mobile nodes work as leaf node without broadcasting DIO

is well defined in the standard. However, for the downward routing, the P2P and P2MP traffic modes that are mainly implemented by DAO are not precisely defined in literature. A complementary IETF standard protocol [6] has been proposed to solve the congestion and latency issues exposed by P2P traffic mode while the multicast protocol [49] has been taken into account for the MP2P mode. More efforts need to be done in DAO scheduling to relieve the congestion and buffer requirements.

Furthermore, storage limitation is still a big challenge for large scale routing. Considering the non-storing and storing modes in downward routing, with the network size increases, storing mode will lead to large memory consumption while the non-storing mode will introduces large communication overhead [50]. The challenge is to find a balanced solution by effectively integrating both models to reduce the memory overhead risk and improve the utilization of node capacity.

B. Diversification of OFs

Existing literature investigated diversified influential elements in routing construction, including the control overhead, link quality, remaining energy, and etc.

Due to the nature of WSN and IoT applications, the network performance is not only limited to the packet delivery and time delay, but also energy efficiency and long term stability required by LLN. It has been verified that the combination of the influential elements can result in trade-off in routing performance. For example, node's remaining energy and link quality can be considered jointly to create an optimal metrics in delivering long lifetime and reliable WSN. Kamgueu et al. [51] put forward a new perspective regarding the OF design, which introduced the fuzzy inference system (FIS) that is mainly defined for an uncertain system. The FIS is able to merge several metrics into one in a reasonable way. The qualitative approach is promising for RPL OF design.

Additionally, the possibility of multi-parents in high dense networks can be further explored. Balancing the traffic load with multicast traffic or introducing parent switching in traffic routing can relief the network load and prolong the network longevity.

In an emerging new IoT application domain, mobile nodes are allowed to connect to the static routing topology and thus the routing protocol to cope with node mobility is extremely challenging. Mobile RPL tends to lead to dynamic changes of topology and link failures. The technical question is how to react to a rapid change of preferred parent which has a significant impact on the reliability and stability of the network. The mobility influence should be considered in the OF for mobile based routing protocols. Hayes et al. [52] proposed a solution for mobile wireless sensor networks taking into account multiple paths utilisation and blind forwarding technique, which is evaluated to be highly adaptable and robust. Mechanisms in the proposed routing protocol can be brought in by RPL and better support mobile RPL.

In essence, an effective routing protocol design should consider application environment. Thus, OFs need to be adjusted specifically to satisfy the characteristics of application scenarios.

C. Energy Issue

The energy consumption is always a concern in LLNs. Because of the differences of relative distances from the current node to the sink node in the network, energy consumption among nodes may be distinct and can lead to scenarios with emerging bottlenecks, which will affect the network reliability. Current studies make effort to take nodes' energy depletion rate into the metrics and make predictions about the path that will consume energy at the lowest rate. An alternative method is to introduce backup node to take place of the dead nodes with minimum network cost. However, the bottleneck nodes can be unavoidable to some extent, thus the critical questions on how to balance the energy of nodes effectively is what need to be looked into in the future.

In LLNs, especially in a large scale, equalizing the energy consumption is much more important than saving the energy in the network. Nurmio et al. [53] considered the energy of all parent nodes along the path towards the sink node, which resulted in an equalized energy consumption rate among nodes in the network.

Besides the scalability, the diversity of networks and distinction among nodes also have impacts on the energy consumption. Thus different Quality of Services requirements and power-supply types of nodes should also be considered in the future work.

D. Cross-layer Issue

The cross-layer issue existing here is mainly related to the discrepancy between the payload in network layer and MAC layer. MTU of IPv6 network is 1280 bytes while that of IEEE 802.15.4 MAC is 127 bytes, thus an adaptive layer - 6LoWPAN is indispensable to handle fragmentation and reassembly of data packets as well as head compression.
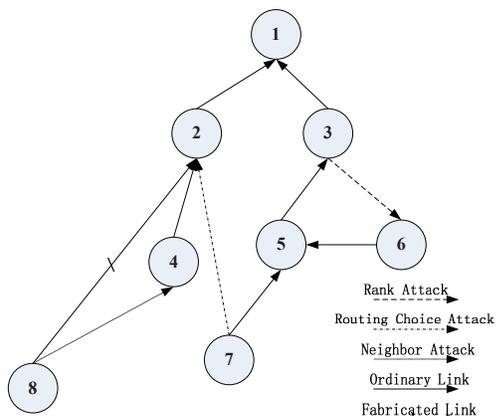
Fig. 14. An illustration of attacks in RPL.

TABLE VI
CATEGORY OF ATTACKS IN RPL.

Attack Type	Feature	Impact
Rank Attack [55], [57]	Choose non-preferred parent as parent node	Destroy routing or format loops
Local Repair Attack [55], [57]	Send local repair information untimely	Destroy routing, waste routing resources
Neighbor Attack [57]	Manipulate control information to deceive neighbour nodes	Forge and destroy routing, waste network resources
Routing Choice Attack [56]	Choose non-optimal routing path	Destroy routing, waste routing resources
Sinkhole Attack [58]	Route traffic to the node pretending to be a valid sink	Destroy routing and topology
Distance Spoofing Attack[58]	Route traffic to a node near the sink	Destroy routing and waste computation resources

Gardasevic *et al.* [54] has proved that with the increase of UDP payload, the routing performance including delay and PDR will be worsen in both unicast and multicast scenarios.

The increasing size of the packet payload will impact the routing performance on consuming much more energy, decreasing packets delivery and increasing network latency. The challenge of how the strategy of routing should be adjusted according to the packet payload need to be further explored.

E. Security Issues in RPL

Security poses a serious challenge to RPL implementation. There are issues related to energy and link quality specified by LLNs [42]. LLNs require stable links maintenance and lower energy consumption beyond the common network circumstances and their limitation tends to have high impact on the effective design of security solutions. Especially in large scale networks, security should be well considered in order to avoid large scale contamination or information leakage.

Threats and attacks over RPL can lead to failures in authentication, maintenance of routing information and attacks on integrity or availability of the network operations [7]. Once an attacker captures a node, it is able to obtain the encrypted information and inject evil code to disturb the routing, which is quite difficult to be detected particularly when innocent nodes fail to know the attacks. Table VI depicts the attack types in RPL.

As depicted in Fig. 14, the attacks can lead to a non-optimal routing or even result in a worse situation such as routing loops or unreachable neighbours. For example, when node 3 chooses node 6 as its preferred parent, which has a larger rank, a rank attack happens with a formed loop of 3-6-5. Routing choice attack happens when node 7 detaches node 5 and chooses node 2 as its parent node. As for neighbour attack, node 4 can replicate messages from node 2 and deceives node 8 to choose node 2 as its parent, which is totally out range for node 8.

To solve the above issues, an Intrusion Detection System (IDS) that is capable of analysing activities or processes in a network or in a node is proposed. The IDS normally deploys monitor nodes in finite state machine mode, every node in a network should be monitored under at least one of them. Such a method works well to efficiently detect rank attacks and local attacks [55]. Other IDS based methods, such as the one mainly focusing on the inner intrusion [56], can successfully solve routing choice attack by avoiding the optimal routing path failure caused by tampering options of DIOs. [57] made a comprehensive analysis of rank attack, local repair attack, neighbour attack and DIS attack, and suggested that the handling models of the attacks can be developed through training of data.

Besides the intrusion detection based methods, the encryption of information in RPL is another option. Clark *et al.* [58] proposed a node-to-node encrypted authentication method by exchanging encryption key. Seeber *et al.* [59] deployed a Trust Platform Model (TPM), which is able to provide cryptographic operations and node authentication, to avoid evil routing information through related trust construction and key exchange mechanism.

As shown above, anti-attacks can be a challenging task for LLNs. ROLL WG analyzed the security threats and attacks including authentication, access control, confidentiality, integrity and availability in [7]. Considering the different categories of threats and attacks, possible solutions have been offered, which mainly focus on establishing session keys, encapsulation during encryption and access control. It also points out that the sensor network limitations including energy, physical locations, directional traffic and etc, combining with use case requirements including urban networks [8], building automation[9], industrial automation[10] and home automation[11], can be the new motivation to design more effective RPL in real scenarios.

VII. CONCLUSION

We mainly focused on the performance analysis of RPL in multi-hop networks with large scale. We first provided an overview of RPL's key features, metrics and objective functions. Then we performed an exhaustive analysis on RPL performance using OMNeT++ in large scale. Application

deployment and security issues posed by RPL have also been discussed. Based on analysis of literature and our simulation, we have raised the future challenges for RPL. The results obtained in the paper will be a useful reference for network engineers to develop more effective routing solutions for IoT use cases.

REFERENCES

[1] D. Evans, "The internet of things: How the next evolution of the internet is changing everything," *CISCO white paper*, vol. 1, pp. 1–11, Accessed on Sep. 2017.

[2] C. Alcaraz, P. Najera, J. Lopez, and R. Roman, "Wireless sensor networks and the internet of things: Do we need a complete integration?" in *Proc. Intl. Workshop on the Security of the Internet of Things (SecIoT'10)*, Tokyo, Nov 2010.

[3] A. Paventhan, D. D. B, H. Krishna, N. Pahuja, M. F. Khan, and A. Jain, "Experimental evaluation of ietf 6tisch in the context of smart grid," in *Proc. IEEE 2nd World Forum on Internet of Things (WF-IoT)*, Milan, Dec 2015, pp. 530–535.

[4] G. Montenegro, C. Schumacher, and N. Kushalnagar, "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals," RFC 4919, Accessed on Sep. 2017. [Online]. Available: https://rfc-editor.org/rfc/rfc4919.txt

[5] T. Winter, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks," RFC 6550, Accessed on Sep. 2017. [Online]. Available: https://rfc-editor.org/rfc/rfc6550.txt

[6] M. Goyal, M. Philipp, A. Brandt, and E. Baccelli, "Reactive Discovery of Point-to-Point Routes in Low-Power and Lossy Networks," RFC 6997, Accessed on Sep. 2017. [Online]. Available: https://rfc-editor.org/rfc/rfc6997.txt

[7] T. Tsao, R. Alexander, M. Dohler, V. Daza, A. Lozano, and M. Richardson, "A Security Threat Analysis for the Routing Protocol for Low-Power and Lossy Networks (RPLs)," RFC 7416, Accessed on Sep. 2017. [Online]. Available: https://rfc-editor.org/rfc/rfc7416.txt

[8] M. Dohler, T. Watteyne, T. Winter, and D. Barthel, "Routing Requirements for Urban Low-Power and Lossy Networks," RFC 5548, Accessed on Sep. 2017. [Online]. Available: https://rfc-editor.org/rfc/rfc5548.txt

[9] J. Martocci, P. D. Mil, N. Riou, and W. Vermeylen, "Building Automation Routing Requirements in Low-Power and Lossy Networks," RFC 5867, Accessed on Sep. 2017. [Online]. Available: https://rfc-editor.org/rfc/rfc5867.txt

[10] K. Pister, P. Thubert, S. Dwars, and T. Phinney, "Industrial Routing Requirements in Low-Power and Lossy Networks," RFC 5673, Accessed on Sep. 2017. [Online]. Available: https://rfc-editor.org/rfc/rfc5673.txt

[11] A. Brandt and G. Porcu, "Home Automation Routing Requirements in Low-Power and Lossy Networks," RFC 5826, Accessed on Sep. 2017. [Online]. Available: https://rfc-editor.org/rfc/rfc5826.txt

[12] D. Barthel, J. Vasseur, K. Pister, M. Kim, and N. Dejean, "Routing Metrics Used for Path Calculation in Low-Power and Lossy Networks," RFC 6551, Accessed on Sep. 2017. [Online]. Available: https://rfc-editor.org/rfc/rfc6551.txt

[13] P. Levis, T. Clausen, J. Hui, O. Gnawali, and J. Ko, "The Trickle Algorithm," RFC 6206, Accessed on Sep. 2017. [Online]. Available: https://rfc-editor.org/rfc/rfc6206.txt

[14] J.-P. Vasseur and A. Dunkels, *Interconnecting smart objects with ip: The next internet*. Morgan Kaufmann, 2010.

[15] G. Iyer, P. Agrawal, and R. S. Cardozo, "Performance comparison of routing protocols over smart utility networks: A simulation study," in *Proc. IEEE GLOBECOM Workshops*, Atlanta, GA, Dec 2013, pp. 969–973.

[16] T. Clausen, A. C. de Verdiere, J. Yi, A. Niktash, Y. Igarashi, H. Satoh, U. Herberg, C. Lavenu, T. Lys, C. Perkins *et al.*, "The lightweight on-demand ad hoc distance-vector routing protocol-next generation (loadng)," *draft-clausen-lln-loadng-15*, Accessed on Sep. 2017. [Online]. Available: https://tools.ietf.org/html/draft-clausen-lln-loadng-15

[17] W. Xiao, J. Liu, N. Jiang, and H. Shi, "An optimization of the object function for routing protocol of low-power and lossy networks," in *Proc. Intl. conf. Systems and Informatics (ICSAI)*, Shanghai, Nov 2014, pp. 515–519.

[18] O. Iova, F. Theoleyre, and T. Noel, "Stability and efficiency of rpl under realistic conditions in wireless sensor networks," in *Proc. IEEE Intl. Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, London, Sept 2013, pp. 2098–2102.

[19] X. Yang, J. Guo, P. Orlik, K. Parsons, and K. Ishibashi, "Stability metric based routing protocol for low-power and lossy networks," in *Proc. IEEE Intl. Conf. on Communications (ICC)*, Sydney, NSW, June 2014, pp. 3688–3693.

[20] P. O. Kamgueu, E. Nataf, T. D. Ndié, and O. Festor, "Energy-based routing metric for rpl," Ph.D. dissertation, INRIA, Accessed on Sep. 2017. [Online]. Available: https://hal.inria.fr/hal-00779519/document

[21] S. Capone, R. Brama, N. Accettura, D. Striccoli, and G. Boggia, "An energy efficient and reliable composite metric for rpl organized networks," in *Proc. IEEE Intl. Conf. on Embedded and Ubiquitous Computing (EUC)*, Milano, Aug 2014, pp. 178–184.

[22] O. Iova, F. Theoleyre, and T. Noel, "Using multiparent routing in rpl to increase the stability and the lifetime of the network," *Ad Hoc Networks*, vol. 29, pp. 45–62, 2015.

[23] Y.-R. Tan, "RPL-based Clustering Routing Protocol," Internet Engineering Task Force, Internet-Draft draft-tan-roll-clustering-00, Accessed on Sep. 2017, work in Progress. [Online]. Available: https://tools.ietf.org/html/draft-tan-roll-clustering-00

[24] M. Zhao, H. Y. Shwe, and P. H. J. Chong, "Cluster-parent based rpl for low-power and lossy networks in building environment," in *Proc. IEEE Consumer Communications and Networking Conf. (CCNC)*, Las Vegas, NV, Jan 2015, pp. 779–784.

[25] A. K. Patil and D. P. M. Hadalgi, "Evaluation of discrete event wireless sensor network simulators," *Intl.l Journal of Computer Science & Network*, vol. 1, no. 5, 2012.

[26] H. Sundani, H. Li, V. Devabhaktuni, M. Alam, and P. Bhattacharya, "Wireless sensor network simulators a survey and comparisons," *Intl. Journal of Computer Networks*, vol. 2, no. 5, pp. 249–265, 2011.

[27] A. R. Khan, S. M. Bilal, and M. Othman, "A performance comparison of open source network simulators for wireless networks," in *Proc. IEEE Intl. Conf. on Control System, Computing and Engineering (ICCSCE)*, Penang, Nov 2012, pp. 34–38.

[28] H.-y. Tyan, Y. Gao, J. Hou *et al.*, "Tutorial: working with j-sim," Accessed on Sep. 2017.

[29] T. Voigt, "Contiki cooja crash course," *Proc. Intl. School on Cooperative Robots and Sensor Networks*, 2012.

[30] P. Levis, S. Madden, J. Polastre, R. Szewczyk, K. Whitehouse, A. Woo, D. Gay, J. Hill, M. Welsh, E. Brewer *et al.*, "Tinyos: An operating system for sensor networks," in *Ambient intelligence*. Springer, 2005, pp. 115–148.

[31] P. Levis and N. Lee, "Tossim: A simulator for tinyos networks," *UC Berkeley, September*, vol. 24, 2003.

[32] T. Issariyakul and E. Hossain, *Introduction to network simulator NS2*. Springer Science & Business Media, 2011.

[33] G. Carneiro, "Ns-3: Network simulator 3," in *UTM Lab Meeting April*, vol. 20, 2010.

[34] A. Varga *et al.*, "The omnet++ discrete event simulation system," in *Proc. the European simulation multiconference (ESMâĂŹ2001)*, vol. 9, no. S 185. sn, 2001, p. 65.

[35] S. K. Hammerseth, "Implementing rpl in a mobile and fixed wireless sensor network with omnet++." Accessed on Sep. 2017. [Online]. Available: https://www.duo.uio.no/handle/10852/9016

[36] Z. Sheng, S. Yang, Y. Yu, and A. Vasilakos, "A survey on the ietf protocol suite for the internet of things: standards, challenges, and opportunities," *IEEE Wireless Communications*, vol. 20, no. 6, pp. 91–98, 2013.

[37] P. D. Marco, C. Fischione, G. Athanasiou, and P. V. Mekikis, "Mac-aware routing metrics for low power and lossy networks," in *Proc. IEEE INFOCOM*. Turin: IEEE, April 2013, pp. 13–14.

[38] P. D. Marco, P. Park, C. Fischione, and K. H. Johansson, "Analytical modeling of multi-hop ieee 802.15.4 networks," *IEEE Trans. Vehicular Technology*, vol. 61, no. 7, pp. 3191–3208, 2012.

[39] I. Sajan and E. M. Manuel, "Cross layer routing design based on rpl for multi-hop cognitive radio networks," in *Proc. IEEE Intl. Conf. on Signal Processing, Informatics, Communication and Energy Systems (SPICES)*, Kozhikode, Feb 2015, pp. 1–6.

[40] S. Duquennoy, O. Landsiedel, and T. Voigt, "Let the tree bloom: Scalable opportunistic routing with orpl," in *Proc. ACM Conf. on Embedded Networked Sensor Systems*. Roma: ACM, Nov 2013, p. 2.

[41] S. Borlase, *Smart Grids: Infrastructure, Technology, and Solutions*. CRC Press, 2012.

[42] A. Aijaz, H. Su, and A. H. Aghvami, "Corpl: A routing protocol for cognitive radio enabled ami networks," *IEEE Trans. on Smart Grid*, vol. 6, no. 1, pp. 477–485, 2014.

[43] E. Ancillotti, R. Bruno, and M. Conti, "The role of the rpl routing protocol for smart grid communications," *IEEE Communications Magazine*, vol. 51, no. 1, pp. 75–83, 2013.

[44] ——, "Reliable data delivery with the ietf routing protocol for low-power and lossy networks," *IEEE Trans. on Industrial Informatics*, vol. 10, no. 3, pp. 1864–1877, 2014.

[45] Q. D. Ho, Y. Gao, G. Rajalingham, and T. Le-Ngoc, "Robustness of the routing protocol for low-power and lossy networks (rpl) in smart grid's neighbor-area networks," in *Proc. IEEE Intl. Conf. on Communications (ICC)*, London, June 2015, pp. 826–831.

[46] A. Aijaz and A. H. Aghvami, "Cognitive machine-to-machine communications for internet-of-things: A protocol stack perspective," *IEEE Internet of Things Journal*, vol. 2, no. 2, pp. 103–112, 2015.

[47] T. N. Quynh, N. L. Manh, and K. N. Nguyen, "Multipath rpl protocols for greenhouse environment monitoring system based on internet of things," in *Proc. Intl. Conf. on Electrical Engineering/Electronics, Computer, Telecom. and Information Technology (ECTI-CON)*, Hua Hin, June 2015, pp. 1–6.

[48] F. Gara, L. B. Saad, R. B. Ayed, and B. Tourancheau, "Rpl protocol adapted for healthcare and medical applications," in *Proc. Intl.l Wireless Communications and Mobile Computing Conference (IWCMC)*, Dubrovnik, Aug 2015, pp. 690–695.

[49] R. Kelsey and J. Hui, "Multicast Protocol for Low-Power and Lossy Networks (MPL)," RFC 7731, Accessed on Sep. 2017. [Online]. Available: https://rfc-editor.org/rfc/rfc7731.txt

[50] W. Gan, Z. Shi, C. Zhang, L. Sun, and D. Ionescu, "Merpl: A more memory-efficient storing mode in rpl," in *Proc. IEEE Intl. Conf. on Networks (ICON)*, Singapore, Dec 2013, pp. 1–5.

[51] P. O. Kamgueu, E. Nataf, and T. N. Djotio, "On design and deployment of fuzzy-based metric for routing in low-power and lossy networks," in *Proc. IEEE Local Computer Networks Conf. Workshops (LCN Workshops)*, Clearwater Beach, FL, Oct 2015, pp. 789–795.

[52] T. Hayes and F. H. Ali, "Location aware sensor routing protocol for mobile wireless sensor networks," *IET Wireless Sensor Systems*, vol. 6, no. 2, pp. 49–57, 2016.

[53] J. Nurmio, E. Nigussie, and C. Poellabauer, "Equalizing energy distribution in sensor nodes through optimization of rpl," in *Proc. IEEE Intl. Conf. on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM)*, Liverpool, Oct 2015, pp. 83–91.

[54] G. Gardasevic, S. Mijovic, A. Stajkic, and C. Buratti, "On the performance of 6lowpan through experimentation," in *Proc. Intl. Wireless Communications and Mobile Computing Conference (IWCMC)*, Dubrovnik, Aug 2015, pp. 696–701.

[55] A. Le, J. Loo, Y. Luo, and A. Lasebae, "Specification-based ids for securing rpl from topology attacks," in *Proc. IFIP Wireless Days (WD)*, Niagara Falls, ON, Oct 2011, pp. 1–3.

[56] L. Zhang, G. Feng, and S. Qin, "Intrusion detection system for rpl from routing choice intrusion," in *Proc. IEEE Intl. Conf. on Communication Workshop (ICCW)*, London, June 2015, pp. 2652–2658.

[57] A. Le, J. Loo, Y. Luo, and A. Lasebae, "The impacts of internal threats towards routing protocol for low power and lossy network performance," in *Proc. IEEE Symposium on Computers and Communications (ISCC)*, Split, July 2013, pp. 000 789–000 794.

[58] C. Taylor and T. Johnson, "Strong authentication countermeasures using dynamic keying for sinkhole and distance spoofing attacks in smart grid networks," in *Proc. IEEE Wireless Communications and Networking Conference (WCNC)*, New Orleans, LA, March 2015, pp. 1835–1840.

[59] S. Seeber, A. Sehgal, B. Stelte, G. D. Rodosek, and J. SchÃűnwÃďlder, "Towards a trust computing architecture for rpl in cyber physical systems," in *Proc. Intl. Conf. on Network and Service Management (CNSM 2013)*, Zurich, Oct 2013, pp. 134–137.