doi:10.20944/preprints202011.0624.v1

An energy and load aware multipath routing protocol in the Internet of Things

Rogayye khaleghnasab[1] . Karamolah Bagherifard[1] . Bahman Ravaei[2]. Hamid Parvin[2] . Samad Nejatian[1]

Abstract

Internet of things (IoT) is a network of smart things. This indicates the ability of these physical things to transfer information with other physical things. The characteristics of these networks, such as topology dynamicity and energy constraint, challenges the routing problem in these networks. Previous routing methods could not achieve the required performance in this type of network. Therefore, developers of this network designed and developed specific methods in order to satisfy the requirements of these networks. One of the routing methods is utilization of multipath protocols which send data to its destination using routes with separate links. One of such protocols is RPL routing protocol. In this paper, this method is improved using composite metrics which chooses the best paths used for separate routes to send packets. We propose Energy and Load aware RPL (ELaM-IoT) protocol, which is an enhancement of RPL protocol. It uses a composite metric, calculated based on remaining energy, hop count, Link Expiration Time (LET), load and battery depletion index (BDI) for the route selection. In order to evaluate and report the results, the proposed ELaM-IoT method is compared to the ERGID and ADRM-IoT approaches with regard to average remaining energy, and network lifetime. The results demonstrate the superior performance of the proposed ELaM-IoT compared to the ERGID and ADRM-IoT approaches.

Keywords Internet of Things. Load aware. Energy-efficient. Gray System Theory. Multipath protocol

✉ Rogayye khaleghnasab
Khaleghnasab@gmail.com

✉ Karamolah Bagherifard*
k.bagheri@iauyasooj.ac.ir

✉ Bahman Ravaei
Ravaei@aut.ac.ir

[1] Department of Computer Engineering, Yasooj Branch, Islamic Azad University, Yasooj, Iran.
[2] Department of Computer Engineering and Information Technology, Amirkabir University of Technology, Tehran, Iran

1 Introduction

The Internet of Things (IoT) demand has recently increased. Firstly, the wireless sensor network (WSN) empowers pervasive sensing technologies. By the evolution of the WSN technology, the Internet of Things (IoT) was created through the application and proliferation of these sensing devices [1, 2]. IoT, as the next revolution, interconnects smart objects and develops an intelligent space. It is anticipated that there would be 24 billion IoT devices by 2020. By increasing connection and communication among IoT devices, considerable IoT traffic will be created by IoT applications. Given that IoT traffic is due to the communication among objects, the reliability of the transmission is important, particularly in a nearly unstable WSN, in comparison with the wired networks. We employ 500 sensor nodes distributed uniformly over the area of 3000∗3000m, as seen in Fig. 1.

A routing protocol decides how to send packets to other nodes. Routing protocols have two major divisions including Reactive and Proactive routing protocols. Routes are providing by the reactive protocols when it is needed. When it is necessary, control messages are transmitted by the path of data transfer, using these types of protocols. But, the needed time to find the route is increases. In addition, control messages are periodically exchanged by the proactive routing protocols immediately after start in order to search and propagate the routes. Local control messages together with messages across the entire network are sent by nodes to receive local nearby information and to share the structural information in all nodes of the network.

In this paper, this method is improved using composite metrics which chooses the best paths used for separate routes to send packets. We propose Energy and Load aware RPL (ELaM-IoT) protocol, which is an enhancement of RPL protocol. It uses a composite metric, calculated based on remaining energy, hop count, Link Expiration Time (LET), load and battery depletion index (BDI) for the route selection.

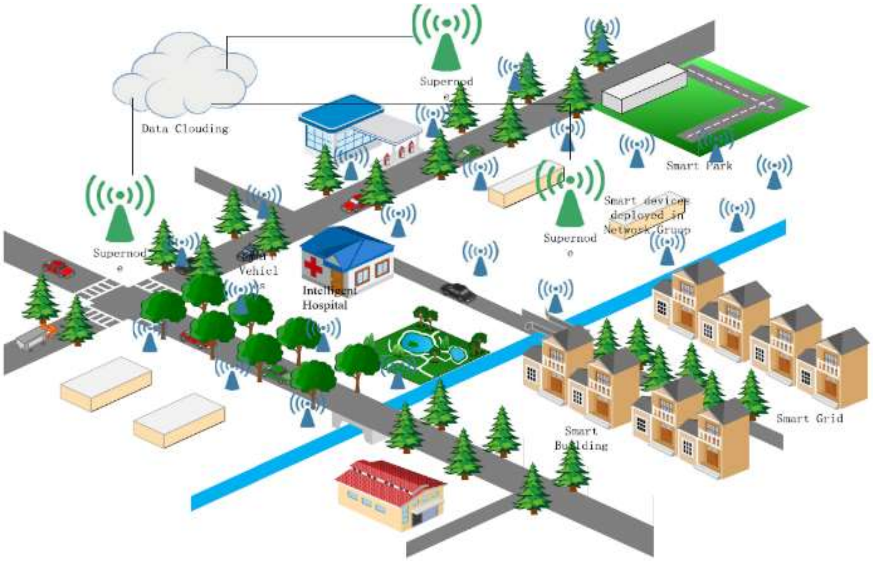


Fig. 1 The devices deployed in IoT [3].

The presented work is structured as the following. Section 2 presents related works. In Sect. 3 brings the proposed ELaM-IoT schema. The parameters used for assessing the performance are studied and simulation outcomes are deliberated in Section 4. Finally, conclusion of this research is discussed in Section 5.

doi:10.20944/preprints202011.0624.v1

2 Related works

In recent years, there have been many suggested researches on real-time routing protocols. And the central focus of them is divided into two main problems about multipath routing protocols. The first one is the protocol requirement to guarantee the reliability of real-time packets in order to decrease the number of blank regions created by loss and delay. The other one is the protocol requirement to stabilize the energy loss of the network and avoid early expiration of some nodes.

The proposed work main objective is to maximize the network lifetime by minimizing the node energy consumption. The contribution of this work is to introduce a combination of ETX, Load and BDI based composite metric in RPL. This composite metric follows the minimizable property. DODAG sends DIO control messages to all participant nodes. The participant node selects the best parent from DODAG rank. The rank calculates from minimum value of the composite metric in the DODAG. Finally, sender or participant node sends the data to DODAG root towards the best parent in the DODAG. Thus, it improves the packet delivery ratio, reduce the traffic load and improve network lifetime [1].

In [2] proposed a design guideline for routing metrics composition in LLN and this document is standardized by IETF. It is clearly stated the properties, rules and requirement of composite metrics in LLN. The composition of the primary metric can be combined additive and lexical manner. Additive property is suitable for composition of primary metric consists of either minimizable or maximization property. Fuzzy logic is suitable for composition of single metric consists of both minimizable and maximization. Lexicographic property is suitable for composition of single metric and it is inspected first metric and only if possible path have equal value then it considers the next metric from the composition.

In [3] evaluated the routing metric composition to improve the Quality of Service (QoS) in LLN. It focused on three things. a). it introduced a composite metric from the single metric such as Remaining energy (RE), Expected transmission count (ETX), Packet forwarding indication (PFI). b). It provided better QoS and it proved the efficiency using routing algebra. c). it achieved better performance and it is provided the optimal loop- free paths.

NLEE Algorithm: In the paper presented by Vellanki et al. in 2016, the effective energy protocol for improving energy efficiency in internet of things was introduced. The proposed algorithm, makes decisions that minimize upload using shortest paths. This method uses the expected remaining node energy countdown and total number of node transfers as the routing criteria to improve energy efficiency. This method controls the number of transferred and broadcasted packets to discover routes. Furthermore, route discovery is carried out using remaining energies and step counts of the nodes in the routes. Moreover, NLEE algorithm guarantees better utilization of the energy available in the nodes. It also regularizes routing delay while discovering the shortest path in the network [4].

SCOTRES Method: SCOTRES is a trust-based system for secure routing in ad-hoc networks which use smart devices to transmit information. The proposed method is described using five criteria. Energy criterion, takes into consideration the resource consumption of each node. Trust criterion increases the network lifetime. Topology criterion is aware of the node positions and enhances loading. Chanel health criterion, due to inappropriate channel conditions, protects the network against harmful attacks.

Reputation criterion evaluates each of the participants of specific network operations for identification of specialized attacks. On the other hand, trust criterion, general adaptation, evaluates the fulfilment against hybrid attacks. SCOTRES has two types: one is embedded systems, and the other is real systems. The evaluations represented in this paper demonstrated that this system has the highest protection rate, while maintaining the performance for setting up real applications [5].

ERGID Method: A routing protocol called Emergency Response IoT based on Global Information Decision (ERGID) was suggested in the study of Qui et al. in 2016 to increase the reliability of data transmission performance and efficiency of the emergence response to IoT. Especially, in this study a mechanism called delay iterative method (DIM) which is founded on delay approximation was designed to answer the problem of disregarding valid routes. Additionally, a transfer plan called "Remaining Energy Probability Choice" (REPC) was recommended for balancing the network load together with focusing on the remained energy of the node. Consequences and examination of the simulation indicates that ERGID have better performance with respect to EA-SPEED and SPEED approaches regarding end to end delay, packet dissipation rate, and energy loss. Also, in this study some applied examinations were performed using STM32W108 sensing nodes. It was detected that ERGID can increase the network ability for real-time response [6].

AOMDV-IOT Technique: In this study, the suggested technique called AOMDV-IOT is introduced. It is a routing technique and up to the destination, it can perform as the router. The recommended method is not offered just for the node. The enhancements are mostly appropriate in IoT which is a unique technique for it. The principle object in this technique is detecting and generating effective connections between the nodes and the internet using the AOMDV routing protocol in the IoT. The internet connection table (ICT) is added in the suggested routing protocol to every node. Every node has two tables in this method including: routing table and ICT. ICT consists of four units: terminal node number, terminal node IP address, lifecycle, and hop value. Even though ICT uses extra memory, instead it can store connection counts and consequently decreases transmission delay. Comparison of AOMDV, simulating outcomes show that AOMDV-IOT has improved efficiency with respect to end to end delay, packet loss, and frequency in IoT. In this research, the multi-objective ad-hoc generated distance vector for the internet of things has been enhanced in such an approach that it can dynamically choose the direct internet transmission route by regular update of internet link table. Simulating effects show that while the AOMDV-IOT routing protocol rises the two routing packets, average end to end delay of the route falls [7].

Adaptive Distributed Routing Method: FANET networks are a key part of the IoT and can offer messaging facilities for various devices in the IoT and cyber-permitted applications. But, moving unmanned aerial vehicles (UAV) in FANETs creates random network link and increases complexity of routing algorithms for these applications, particularly in real-time routing. In this research, an effective opportunistic distributed routing technique is suggested to explain the above-mentioned problem. For data transfer in this process, only the colleague nodes and local information are used by the transmitter. They maximize network use and preserve the end to end delay less than a stated threshold in order to care for variations of network and channel by designing and solving an optimization problem. Besides, they guess one stage delay for every communication of the transmitter node and use double parsing to alter the integrated problem into a distributed one. By this method, the transmitter nodes are only

doi:10.20944/preprints202011.0624.v1

permitted to contact with local information and approximate delay in packet routs. Simulation outcomes indicate that the introduced routing technique enhances the network performance regarding its energy efficiency, quantity, and end to end delay [8].

REL Method: In the next work, Machado et al. proposed an energy and link quality-based routing protocol (REL) for IoT applications. In order to improve reliability and energy efficiency, REF selects an estimator mechanism based on the end to end link and the remaining energy. Furthermore, REL proposes an event-based mechanism to maintain load balance and prevent premature energy loss in nodes and the network. REF provides an end to end route selection plan based on cross-layer information with minimum overhead. In order to achieve energy efficiency, the nodes send their remaining energy to the neighbouring nodes. In this paper, route selection process is carried out using end to end link quality evaluation and optimal energy information. A new method is used for link quality estimation. REL utilizes the wireless link quality and the remaining energy while routing in order to increase system reliability and support QoS for IoT applications. REL uses a reactive pattern for discovering routes. This results in reduced signalling overhead and improved scaling capability. Route discovery process consists of diffusing RREQ and RREP messages. In large scale networks with high node density, results suggest that in REL, lifetime was improved up to %26.6, latency up to %17.9, and packet delivery up to %12 when compared to AODV and LABILE [9].

MLB Method: In the IoT, large data transfers using wireless sensor networks has caused many problems. However, AODV routing stack in ZigBee protocol has no load balancing mechanism to handle corrupted traffic. Therefore, we develop multipath load balancing (MLB) to replace AODV routing protocol in ZigBee. MLB is proposed for collaboration with ZigBee wireless network in the large scale. In this scenario, ZigBee is used as communication media in wireless sensor networks. In order to create a reliable ZigBee stack, ZigBee network layer is placed in MLB. MLB provides alternative routing service for ZigBee network without altering the existing stack in ZigBee. When a ZigBee router transmits the IoT data forward, MLB guides the ZigBee network layer in selecting the next hop with minimum load towards the IoT gate [10]. Table 1, summarizes the investigated efforts to design multipath routing for IoT.

Table 1 Summary of the multipath routing schema for IoT literature.

References	Operation	Advantages	Disadvantages
NLEE [4]	Efficient energy protocol for improving energy efficiency in the internet of things	Improved latency – decreased power consumption	Overhead caused by counting the number of sent and control packets, hop count and remaining energy
SCOTRES [5]	Secure routing with emphasis on energy consumption of the devices and decreasing it	Increased network lifetime while using trust criterion in order to prevent hybrid attacks	-
ERGID [6]	Routing based on decisions made with general information	Improved data transfer performance and emergency response	The need to estimate delay in order to improve delay and network lifetime
AOMDV-IOT [7]	Discovering and establishing efficient link between nodes and the internet based on the AOMDV protocol	Decreased latency and decreased packet loss rate	More overhead because of storing two tables in each node and two extra routing packets

ADRM-IoT [8]	Reducing the complexity of routing algorithms using distributed adaptive routing	Improved energy efficiency, throughput, and end to end latency	The need to carry out exact calculations to calculate delay
REL [9]	Routing protocol based on link quality and energy	Improved reliability and energy efficiency	-
MLB [10]	Layer design and balancing load in order to create load balance and eliminate bottlenecks	Load balancing, decreased packet loss, and increased connections	Paying no attention to the remaining energy and lifetime of the node

3 The proposed ELaM-IoT schema

In the following section, we design an ELaM-IoT schema by employing the composite metrics. Five phases are included in the ELaM-IoT schema: in Sect, 3.1. The assumptions applied in the proposed ELaM-IoT is discussed, Sect 3.2. presents adding new parameters to RPL, designing the routing packets in ELaM-IoT is discussed in Sect. 3.3. In Sect. 3.4 neighbor discovery step is discussed. And the route discovery step is discussed in Sect. 3.5.

3.1 Phase 1: The assumptions applied in the proposed ELaM-IoT

The assumptions Considered in the proposed approach include:

1. Things existing in the network are not static; they should work independently.
2. Each thing has limited energy and the initial energy of each thing is EP_N where $EP_N \succ 0$
3. Things gather data with a constant rate from the environment.
4. In the proposed approach, energy is consumed to transmit local data among the nodes.
5. To gain spatial data, each node is equipped with a GPS system.

3.2 Phase 2: Adding new parameters to RPL

Because most of the devices are wireless, link stability fluctuation caused by movement or transfer medium characteristics in the internet of things affects the network performance. Efficiency of a dynamic routing protocol can be rated based on its ability to handle link unreliability and its computational and reconfiguration/rerouting overhead. Link stability as the basis of routing can lead to a protocol that has the following capabilities:

Remaining Energy (Re): One of the most important elements while choosing a route is the remaining energy in the nodes along that route. The higher the remaining energy in the nodes of a route and the lower their consumed energy, the more appropriate that route is to be selected. Remaining energy is calculated using Equation (1).

$$ER_N = \left(EP_N(t) - ECo_N(t)\right) \tag{1}$$

In Eq. (2): $\left\{ \begin{array}{l} ER_N(t):\ Remaining\ energy\ of\ the\ node \\ EP_N(t):\ Primary\ energy\ of\ the\ node \\ ECo_N(t)\ Consumed\ energy\ of\ the\ node \end{array} \right\}$

Hop Count (Hop): The Hop count parameter is the number of Hops between the origin node and the destination node. The lower the Hop count of a route, the better that route is because less energy needs to be used in order to transmit the packet.

Link Expiration Time (LET): It is the amount of time for which the links stays stable. The longer this time period is, the more stable the link between the nodes will be. This parameter depends on the movement speed of the nodes. The faster the nodes move, the more unstable the route between them will be and the sooner it will be destroyed. Link expiration time is calculated using Equation (2) based on the transmitted packets between the nodes.

$$LET(i,j) = \left(\frac{-(ab+cd) + \sqrt{(a^2+c^2)*R^2 - (ad-bc)^2}}{a^2+c^2} \right) \tag{2}$$

In Eq. (3): $\left\{ \begin{matrix} a = v_i * \cos\theta_i - v_j * \cos\theta_j, \\ b = x_i - x_j, \\ d = Y_i - Y_j, \\ C = v_i * \sin\theta_i - v_j * \sin\theta_j \end{matrix} \right\}$

The nodes are aware of their location using GPS. In the above equation there are two nodes i and j which are at (x_i, y_i) and (x_j, y_j) respectively. Their speeds are v_i, v_j and their movement angles are θ_i and θ_j. In the following section, details for each step are presented.

Load: Network data traffic is an amount of data transfer across the network at given amount of time. Load balance is a technique and it is used to balance the traffic across network. It is mainly concentrated on number of child present in each parent node. The participant node selects the parent node based on less number of child accumulated parent node in the DODAG. The traffic load calculates from Equation (3) and (4). If the number of children increases in a parent node in the DODAG, ELaM-IoT reconstructs the DODAG.

a. **To calculate the Load:** In ELaM-IoT, load of path(x) calculation is based on the cumulative of node traffic or child set.

$$Load\left(path\left(x\right)\right) = \left(\sum_{M=1}^{n} Node\_TrafficLoad\left(M\right) \right) \tag{3}$$

b. **To calculate the Node Traffic:** In ELaM-IoT, node traffic calculates from children count of the respective parent node

$$Node\_TrafficLoad\left(M\right) = \left(\sum_{i=1}^{n} children\_count \right) \tag{4}$$

doi:10.20944/preprints202011.0624.v1

Battery Depletion Index (BDI): Battery depletion Index (BDI) indicates that how much percentage of energy depleted from battery present in the node. The residual energy calculates from initial energy and remaining energy of the node [4]. The residual energy calculates from Equation (5).

$$RER(M_i) = \left(\frac{E_{remain}}{E_{initial}}\right) \tag{5}$$

The residual energy is a remaining energy in the node Mi and it is represented in terms of 0 to 1. The BDI calculation is calculated from Equation (6).

$$BDI(M_i) = (1 - RER(M_i)) \tag{6}$$

The BDI follows the deductive rule and BDI of Path Px calculates from Equation (7).

$$BDI(P_x) = \left(\prod_{i=1}^{n} BDI(M_i)\right) \tag{7}$$

Rank Calculation: In EL-RPL, DODAG rank calculates from parent rank and rank increase value. The rank increase calculates from step value and MinHopRankIncrease. The MinHopRankIncrease default value is 256 [7]. The step value calculates from objective and rank function and it is denoted in Equation (8).

$$Rank(N) = (W_1 * \mathrm{Re}(p_i)) + (W_2 * HopCount(p_i)) + (W_3 * LET(p_i)) \tag{8}$$
$$+$$
$$(W_4 * Load(p_i)) + (W_5 * BDI(p_i))$$

3.3 Phase 3: Designing the routing packets in ELaM-IoT

In the proposed method, all of the devices need to be equipped with GPS and have maximum initial energy. RPL routing packet format is expanded so that it can be used for ELaM-IoT routing. This is achieved by adding new fields to RPL routing packets. ELaM-IoT routing protocol, just like the base RPL protocol, has four packet formats. However, in the proposed ELaM-IoT method, these formats are altered and required fields are added to these packets. Details of these packets are presented below.

HELLO packet: This packet is used to discover neighboring devices in regular intervals. Adjacent nodes exchange their location obtained through GPS and remaining energy information using HELLO packets. After exchanging the HELLO packet, each node updates its routing table and the remaining energy of neighboring nodes and also calculates $SINR$ rate based on the received signal from the neighbor and link expiration time (LET) with the neighboring node based on its own location and the neighbor's location and also writes them into its table. New format of the $HELLO$ packet is shown in Table 2.

Table 2 New format of the HELLO packet.

Packet type Reserved	Unused
Origin IP address	Origin sequence number
Time stamp (origin time)	Node energy
Node location	Node speed

RREQ packet: The second packet is the route request (*RREQ*) packet. Each time a node tries to communicate with other nodes in the network, route discovery process needs to be carried out. Therefore, the node broadcasts the *RREQ* packet publicly to find an appropriate route to its destination *RREQ* packets consist of an *ID* to identify each packet, the destination IP address, sequence number, and network time stamp. Destination sequence number indicates the freshness of a route. We add the remaining node energy, *SINR* value, and the calculated *LET* with the last hop based on the *HELLO* message fields to the *RREQ* packet. Each node has calculated these parameters based on the Eq. (1) through Eq. (3) upon receiving the *HELLO* message and saved them in its table. Now, once the *RREQ* message is received, each node on this route adds these information and transfers to the next node along the route to the destination. New format of the *RREQ* packet is shown in Table 3.

Table 3 New format of the RREQ packet.

<table>
<tr><th>Packet type</th><th colspan="2">Reserved</th><th>Hop count</th></tr>
<tr><td colspan="2">RREQ public broadcast ID</td><td colspan="2">Destination IP address</td></tr>
<tr><td colspan="2">Destination sequence number</td><td colspan="2">Origin IP address</td></tr>
<tr><td colspan="2">Hop count</td><td colspan="2">Node remaining energy</td></tr>
<tr><td colspan="2">Battery Depletion Index</td><td colspan="2">Accumulated route</td></tr>
<tr><td colspan="2">Load</td><td colspan="2">LET</td></tr>
</table>

RREP packet: The third packet is the route reply packet. After receiving the broadcasted *RREQ* packets, many routes are discovered from the origin to the destination. Normally, *RREP* packet consists of an ID to identify unique packets, origin IP address, sequence number, and accumulated routes. In the proposed method, we get the destination of every *RREQ* packet from different routes and calculate the total number of hops, total remaining energy in each route, and total *SINR* and *LET* in the links of each route and add them to the *RREP* packet. Then, this packet is sent to the origin of that route. Therefore, we add the new total remaining energy of the route nodes, hop count, and total *SINR* and *LET* fields to the *RREP* packet. New format of the *RREP* packet is shown in Table 4.

Table 4 New format of the RREP packet.

<table>
<tr><th>Packet type</th><th colspan="2">Reserved</th><th>Hop count</th></tr>
<tr><td colspan="2">ID RREP</td><td colspan="2">Destination IP address</td></tr>
<tr><td colspan="2">Origin sequence number</td><td colspan="2">Origin IP address</td></tr>
<tr><td colspan="2">Accumulated route</td><td colspan="2">Battery Depletion Index</td></tr>
<tr><td colspan="2">Total remaining energy of the nodes along the route</td><td colspan="2">Total hop count along the route</td></tr>
<tr><td colspan="2">Total Load along the route</td><td colspan="2">Total LET along the route</td></tr>
</table>

RERR packet: Whenever a node discovers an error, it broadcasts a route error ($RERR$) packet with the destination sequence number and infinite hop count. The origin node or any other node along the route can rebuild the route by sending a $RREQ$ packet. If the origin node or any other node receives the $RRER$ packet, it needs to re-execute the route discovery process.

Test packet: after detecting nodes, the origin sends a test message through all routes in the format shown in table 5 to take the responses of all the nodes in the routes. In this way, we can calculate two mentioned parameters namely MER and SCS. New format of the $Test$ packet is shown in Table 5.

Table 5 New format of the $Test$ packet.

<table>
<tr><th>Packet type</th><th colspan="2">Reserved</th><th>Hop count</th></tr>
<tr><td colspan="2">Broadcasting ID the Test packet</td><td colspan="2">IP address of Middle node</td></tr>
<tr><td colspan="2">Measurement rate</td><td colspan="2">Source IP address</td></tr>
</table>

3.4 Phase 4: Neighbor discovery step

In the neighbor discovery step, nodes (devices) flood the network with $HELLO$ packets to find their neighbors. The $HELLO$ packet includes the origin IP address, remaining energy of the node, node location, node speed, sequence number, and time stamp. After the neighbor discovery step, every device knows all of its neighbors in the network and is aware of their location and remaining energy. The nodes also calculate the $Load$ and $Battery\ Depletion\ Index$ value for their immediate neighbors using the received signal and the noise rate and interference values. Also, using the location and speed of the neighboring node in the last step and their own location and speed, each node calculates the link expiration time (LET) of its link with the neighboring node. Each node stores this information for its immediate neighbors.

3.5 Phase 5: Route discovery step

When the origin node decides to send a packet to the destination, it floods the network with $RREQ$ packets to discover the suitable routes. $RREQ$ packet includes the IP address of the origin and destination, sequence number, hop count, remaining energy in the node, LET, load and battery depletion index, accumulated route. IP address of the origin and the destination are used to identify unique nodes in the network. The destination sequence number is used to show the suitable routes to the destination. Each node after receiving the $RREQ$ packet, retrieves its neighbor information and inserts it into its routing table. Then inserts the new information along with its own information into the $RREQ$ packet and sends it to the next node. Figure 2 demonstrates the flooding of $RREQ$ packets in the network in order to find routes leading to the destination.

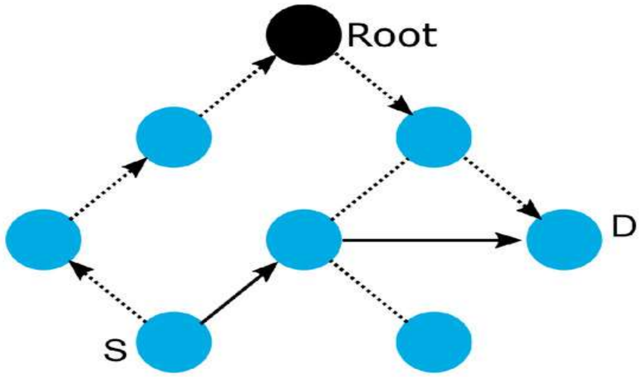


Fig. 2 Transmission of a P2P message from node S to node D. The dotted lines with an arrow represent the path created by RPL, while the solid lines with an arrow represent the path established by P2P-RPL

The destination node received multiple *RREQ* packets using different routes. Also, the *RREP* packet includes the node ID to identify unique packets, destination IP address, sequence number, lifespan in the network, and accumulated routes. The accumulated routes are a list of separate routes from origin to destination. Moreover, three new fields, namely the total *LET* of each route, load and battery depletion index, and remaining energy of each route calculated by the destination node using the *RREQ* packets are added to the *RREP* packet. After adding these fields, the destination node sends the *RREP* packet using all of the routes and stores this information in its routing table. The origin node, upon receiving the *RREP* packets from destination, stores the origin of these multiple routes in its routing table.

4 Evaluating the Performance

The suggested ELaM-IoT performance will be assessed in the next section for the multipath routing problem.

4.1 Performance metrics

The performance and efficacy of the proposed ELaM-IoT method is completely investigated in this section using comprehensive simulations. The obtained results will be compared with ADRM-IoT and ERGID methods discussed in [7] and [11]. The network lifetime and mean remaining energy will be assessed.

Average Remaining Energy: Equation (9) demonstrates that node's unused energy in an arbitrary time instance is the additional energy that is kept in the node after a communication with the receiver. The energy for the reception, fading effects, wasted energy in the system (E_{sys}), energy for transmission, etc. are the remaining energy examples. Table 6 presents the list of the parameters that are used for the *ARE* .

Table 6 Parameters utilized for average residual energy

Parameters	explanation
di_0	Reference distance larger than the Fraunhofer-distance
di	The distance that the packet is transferred on it
Lb	The number of bits per packet (BPP)
di^2	The power loss in the free space channel model
di^4	Power loss in the multipath fading channel model
E_{elec}	The energy that is dissipated when reception or transmission
$lb \in fsi$	Efficiency of Transmission
$lb \in mpi$	The channel Condition

$$Energy_{residual} = Energy_{initial} - \left\{ ET_X + ER_X + E_{sys} \right\} \quad \text{Where} \tag{9}$$

$$ET_X(1b, di) = \left\{ lbE_{elec} + lb\varepsilon_{fs} di^2, di < di_0 \right\} \tag{10}$$

$$= \left\{ lbE_{elec} + lb\varepsilon_{mpi} di^4, di \geq di_0 \right\}$$

Equations 10 and 11 are used for calculating the amount of energy that is used during the transmission of packet $ET_X(1b, di)$ and reception of packet (ER_X).

$$ER_X = lbE_{elec}. \tag{11}$$

The simulated parameter is given as: $\left\{ \begin{array}{l} E_{elec} = 100nJ/bit, \\ \varepsilon_{fsi} = 20pJ/bit/m^2, \\ \varepsilon_{mpi} = 0.0015pJ/bit/m^4 \end{array} \right\}$

In case of $di > di_0$, multipath fading impact happens, and energy wasting occurs during transmission. Nevertheless, as the current paper does not address the fading scheme, it is considered that the distance is fewer than the Fraunhofers distance. In addition, the channel state information will not be taken into account, while it is considered that the efficiency of transmission is 1.

Lifetime of Network: By definition, the lifetime of the network is the time that elapses between communication and sensing commencement with the receiver, and the time during which the final communication link to the receiver from active node is broken. Network lifetime for all nodes that are now active in communication with the receiver is defined as the lifetime aggregating for all the nodes at any instance of time. In case of clustering the network, the lifetime of the network is considered as the whole lifetime for all things [16]. Equation (12) calculates the value of NL.

$$NL = \left(\sum_{i=1}^{m} Things_i \right) \quad \text{Where} \quad Things_i \text{ is the lifetime of } i \text{ th things.} \tag{12}$$

4.2 Simulation setup and comparing algorithms

Since implementing and debugging IoTs in real networks is difficult, considering simulations as a basic design instrument is necessary. The primary benefit of simulation is simplification of analysis and verification of protocol, especially in large systems. In this part, the suggested method's performance is assessed by NS-3 as the simulation instrument, and then the results will be discussed. It should be noted that all ERGID, ADRM-IoT, and ELaM-IoT settings and parameters are considered as equal.

4.3 Simulation results and Analysis

The ELaM-IoT performance is analyzed in this section under the two scenarios (Table 5). Initially, 500 IoT things are deployed in the network area in a uniform manner. Table 7 gives some major parameters.

Table 7 Setting of simulation parameters.

Parameters	Value
Topology (m x m)	1000 x 1000
Simulation tool	NS-3
Transport	UDP/IPv6
Communication range of each node	160 m
Channel bandwidth	2 Mbps
Traffic type, rate	CBR, 15 packets/sec
Number of things, and Packet size	500, 128 Kbps
Number of connections, and Pause time	70, 100 sec
Full Battery	2000 mJ
RPL Parameter	Min Hop Rank Increase=128
Maximum mobility (varying)	5 m/sec - 25 m/sec
Simulation time (in Sec)	500-2000

Table 8 and 9 compares the performance of ELaM-IoT with that of ERGID and ADRM-IoT in terms of throughput, packet receiving rate, end to end delay, average residual energy, and network lifetime.

Table 8 *ARE* (in Joule) of various frameworks vs number of CBR sources.

Rate of Transmission (kb/s)	ARE (Joule)		
	$ADRM-IoT$	$ERGID$	$ELaM-IoT$
10	750	830	950
20	730	814	933
30	700	801	928
40	640	789	925
50	600	780	920
60	550	773	902
70	510	770	891
80	500	762	886
90	430	757	880
100	400	752	871

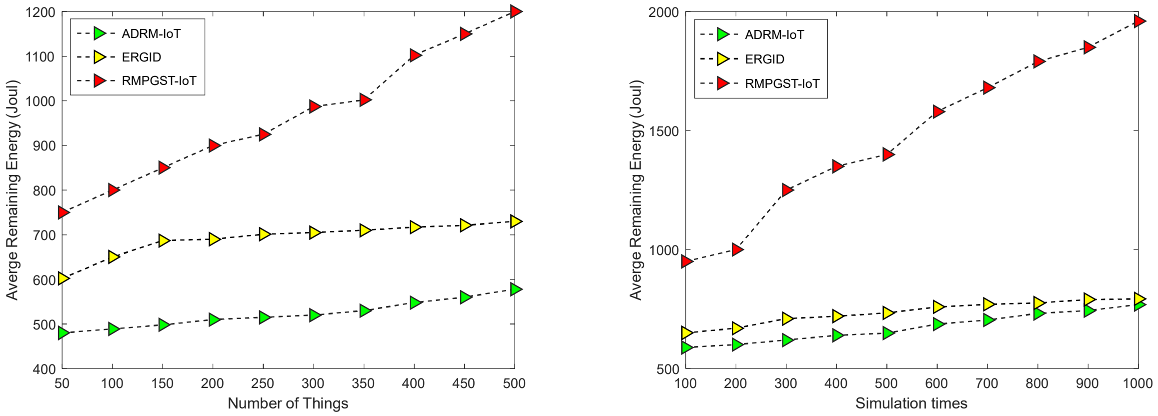
Table 9 *NL* (in Joule) of various frameworks vs number of CBR sources.

Rate of Transmission (kb/s)	NL (Sec)		
	ADRM − IoT	*ERGID*	*ELaM − IoT*
10	720	891	1400
20	680	800	1350
30	640	770	1300
40	600	730	1150
50	550	714	1080
60	503	704	975
70	475	680	904
80	430	674	850
90	410	645	760
100	400	612	710

Figure 3 shows the comparison of the ELaM-IoT proposed scheme, ERGID and ADRM-IoT models in term of *ARE* . (a) Number of Things, (b) Simulation time, (c) Speeds, and (d) Number of CBR sources respectively. This criterion presents the *ARE* in the nodes after routing has been carried out and is calculated using equation 13 which is calculated by subtracting the consumed energy from the initial energy. As seen in figure 3, the *ARE* in the nodes is calculated at 100 and 1000 seconds in every simulation. The simulation results present that the *ARE* in the nodes for the proposed ELaM-IoT is higher than the ERGID and ADRM-IoT methods. This is because in the proposed method, routing is carried out using routes which consist of nodes which are better than the nodes in other routes with respect to hop count, noise rate, *ARE* , and link expiration time criteria. Therefore, taking into account the hop count criterion leads to lower energy consumption, while selecting the route which consists of nodes with higher energy levels controls the network energy and increases the *ARE* . Therefore, the ELaM-IoT performs better in this regard as well. The *ARE* in ELaM-IoT, ERGID and ADRM-IoT algorithms is reduced by 700, 600 and 470%, respectively, while the number of things is increased by 940, 690 and 550%, respectively.

(a)

(b)



(c)

(d)

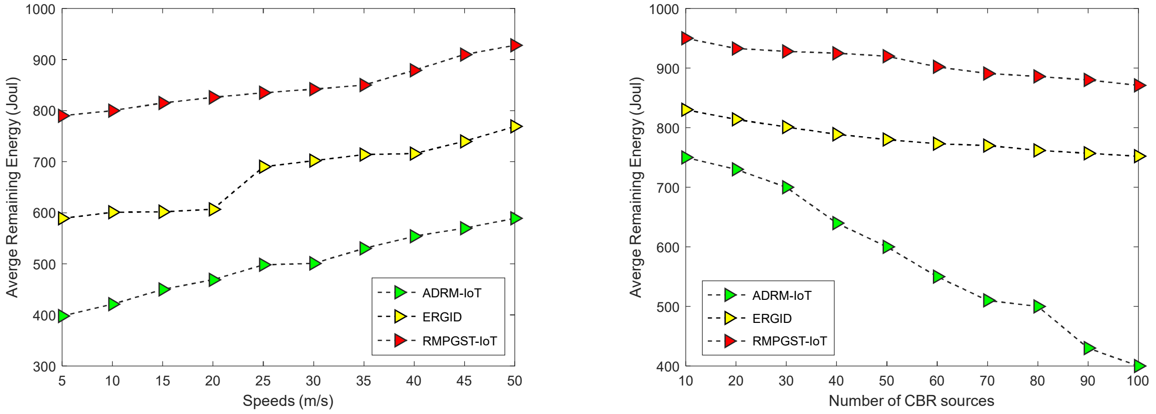
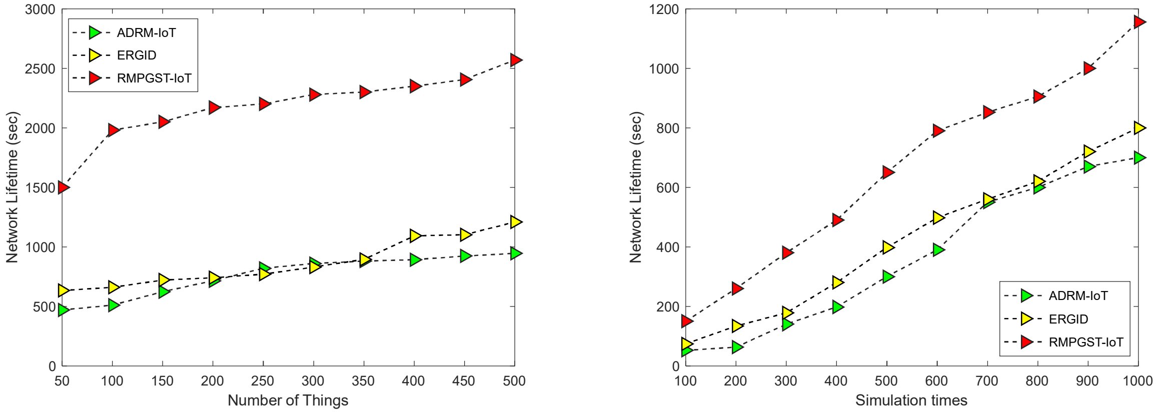


Fig. 3 Comparison of the ELaM-IoT proposed scheme, ERGID and ADRM-IoT approaches in term of Average remaining energy. (a) Number of Things, (b) Simulation time, (c) Speeds, and (d) Number of CBR sources.

Comparison of network lifetime in shown in Figure 4. As proved by the graph, the proposed (ELaM-IoT) method shows a large network lifetime in comparison with other present methods. Increasing the number of CBR sources will reduce the network lifetime. The proposed ELaM-IoT uses large network lifetime of 5200 rounds in 500 things when compared to existing approach. In 100 nodes, the network lifetime of existing approaches ERGID, and ADRM-IoT are 4800rounds, and 4100rounds respectively. In the ELaM-IoT method, by choosing high energy routes with fewer hops, premature deactivation of nodes in the network is prevented. Since the routes are selected for data transmission based on their remaining energy and fewer hops while also taking into consideration their noise rate and link expiration time, energy in the network nodes is depleted over a longer period of time and network lifetime is increase.

(a) (b)



(c) (d)

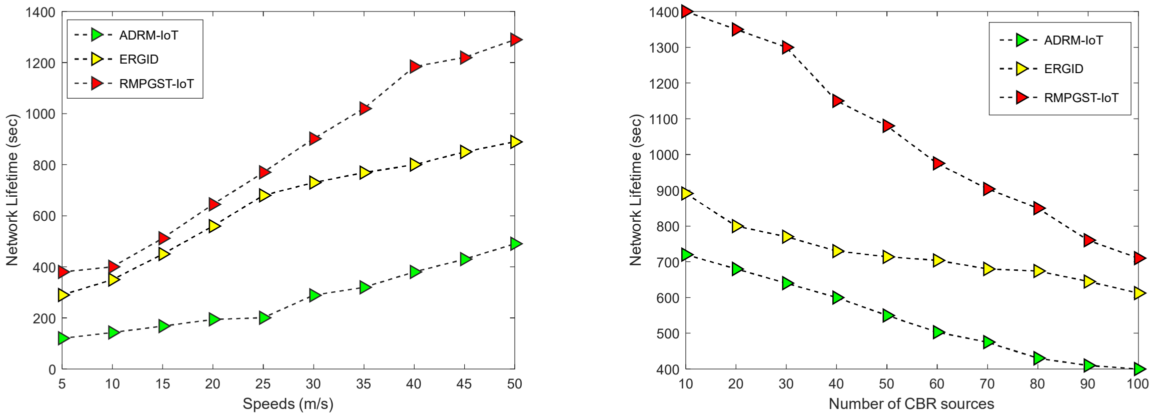


Fig. 4 Comparison of the ELaM-IoT proposed scheme, ERGID and ADRM-IoT approaches in term of Lifetime. (a) Number of Things, (b) Simulation time, (c) Speeds, and (d) Number of CBR sources.

Energy Balance: The energy analysis is done by the 50 key nodes gathered from the other 500 nodes. The remaining energy and lifetime of 200, 400, 600, 800, 1000 s are used for analysis. Figure 5 indicates ELaM-IoT lifetime and remaining energy. The secondary energy amendment strategy provides a better energy balance impact.

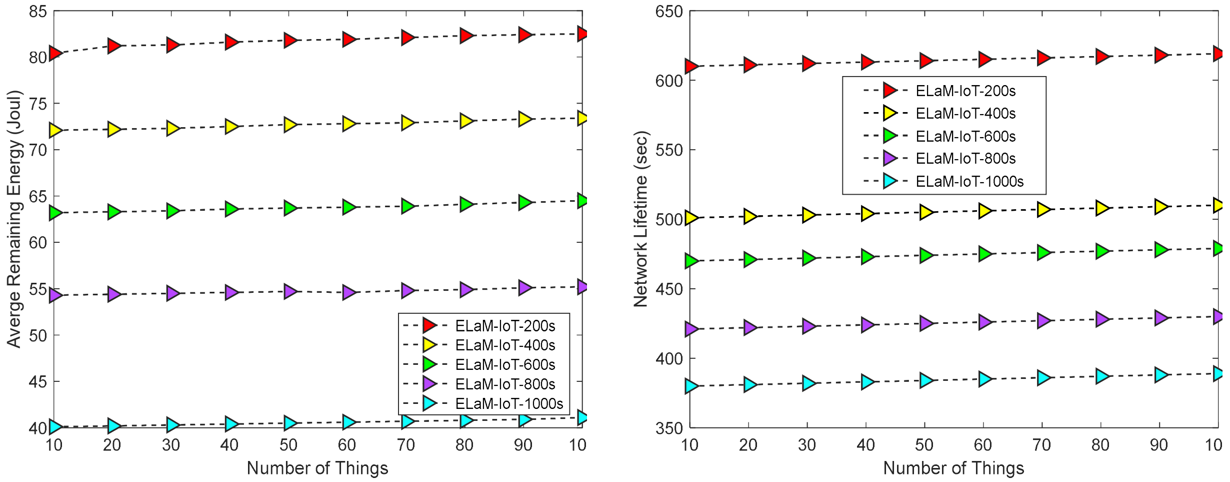


Fig. 5 Comparison of the ELaM-IoT proposed scheme, in terms of energy distribution curve and lifetime at different times.

5 Conclusion

In this paper, this method is improved using composite metrics which chooses the best paths used for separate routes to send packets. Energy and Load aware RPL (ELaM-IoT) protocol is proposed in this work that is an improved form of RPL protocol. A composite metric is used by it, which is calculated based on hop count, remaining energy, Link Expiration Time (LET), load and battery depletion index (BDI) for selection of route. Using NS-3, ELaM-IoT scheme's performance was analyzed, and it was indicated that it has a high-level performance with a high network lifetime (above 89.73%) and a high mean remaining energy (above 74.23%) in comparison with the present methods.

Reference

1. Sankar, S., & Srinivasan, P. (2018). Energy and Load Aware Routing Protocol for Internet of Things. International Journal of ADVANCED AND APPLIED SCIENCES, 7(3), 255-264.
2. Fotohi, R., & Jamali, S. (2014). A comprehensive study on defence against wormhole attack methods in mobile Ad hoc networks. International journal of Computer Science & Network Solutions, 2, 37-56.
3. Alsukayti, I. S. (2020). The support of multipath routing in IPv6-based internet of things. International Journal of Electrical & Computer Engineering (2088-8708), 10.
4. Fotohi, R., Heydari, R., & Jamali, S. (2016). A Hybrid routing method for mobile ad-hoc networks. Journal of Advances in Computer Research, 7(3), 93-103.
5. Tseng, C.H., *Multipath load balancing routing for Internet of things.* Journal of Sensors, 2016. 2016.
6. Hasan, M.Z. and F. Al-Turjman, *Optimizing multipath routing with guaranteed fault tolerance in Internet of Things.* IEEE Sensors Journal, 2017. 17(19): p. 6463-6473.
7. Demicheli, F. (2011). Design, implementation and evaluation of an energy efficient RPL routing metric.
8. Kharkongor, C., T. Chithralekha, and R. Varghese, *A SDN Controller with Energy Efficient Routing in the Internet of Things (IoT).* Procedia Computer Science, 2016. 89: p. 218-227.
9. Fotohi, R., Ebazadeh, Y., & Geshlag, M. S. (2016). A new approach for improvement security against DoS attacks in vehicular ad-hoc network. International Journal of Advanced Computer Science and Applications, 7(7), 10-16.
10. Hatzivasilis, G., I. Papaefstathiou, and C. Manifavas, *SCOTRES: secure routing for IoT and CPS.* IEEE Internet of Things Journal, 2017. 4(6): p. 2129-2141.
11. Qiu, T., et al., *ERGID: An efficient routing protocol for emergency response Internet of Things.* Journal of Network and Computer Applications, 2016. 72: p. 104-112.
12. Sarkohaki, F., Fotohi, R., & Ashrafian, V. (2017). An efficient routing protocol in mobile ad-hoc networks by using artificial immune system. International Journal of Advanced Computer Science and Applications (IJACSA), 8 (4).
13. Fotohi, R., & Bari, S. F. (2020). A novel countermeasure technique to protect WSN against denial-of sleep attacks using firefly and Hopfield neural network (HNN) algorithms. The Journal of Supercomputing, 1-27.
14. Tian, Y. and R. Hou. *An improved AOMDV routing protocol for internet of things*. in *2010 International Conference on Computational Intelligence and Software Engineering*. 2010. IEEE.
15. Shen, J., et al., *An efficient centroid-based routing protocol for energy management in WSN-assisted IoT.* IEEE Access, 2017. 5: p. 18469-18479.
16. AlZubi, A.A., M. Al-Ma'aitah, and A. Alarifi, A BEST-FIT ROUTING ALGORITHM FOR NON-REDUNDANT COMMUNICATION IN LARGE-SCALE IoT BASED NETWORK. Computer Networks, 2019.
17. Wen, S., et al., Energy-efficient and delay-aware distributed routing with cooperative transmission for Internet of Things. Journal of Parallel and Distributed Computing, 2018. 118: p. 46-56.
18. Machado, K., et al., A routing protocol based on energy and link quality for internet of things applications. sensors, 2013. 13(2): p. 1942-1964.
19. Vellanki, M., S. Kandukuri, and A. Razaque, Node level energy efficiency protocol for Internet of Things. Journal of Theoretical and Computational Science, 2016. 3.
20. Bouzebiba, H., & Lehsaini, M. (2020). FreeBW-RPL: A New RPL Protocol Objective Function for Internet of Multimedia Things. Wireless Personal Communications, 1-21.
21. Fotohi, R. (2020). Securing of Unmanned Aerial Systems (UAS) against security threats using human immune system. Reliability Engineering & System Safety, 193, 106675.

doi:10.20944/preprints202011.0624.v1

22. Zaminkar, M., Sarkohaki, F., & Fotohi, R. A method based on encryption and node rating for securing the RPL protocol communications in the IoT ecosystem. International Journal of Communication Systems, e4693.
23. Faraji-Biregani, M., & Fotohi, R. (2020). Secure communication between UAVs using a method based on smart agents in unmanned aerial vehicles. The Journal of Supercomputing, 1-28.
24. Zaminkar, M., & Fotohi, R. (2020). SoS-RPL: Securing Internet of Things Against Sinkhole Attack Using RPL Protocol-Based Node Rating and Ranking Mechanism. WIRELESS PERSONAL COMMUNICATIONS.
25. Jamali, S., & Fotohi, R. (2017). DAWA: Defending against wormhole attack in MANETs by using fuzzy logic and artificial immune system. the Journal of Supercomputing, 73(12), 5173-5196.
26. Mabodi, K., Yusefi, M., Zandiyan, S., Irankhah, L., & Fotohi, R. Multi-level trust-based intelligence schema for securing of internet of things (IoT) against security threats using cryptographic authentication. The Journal of Supercomputing, 1-25.
27. Jamali, S., Fotohi, R., Analoui, M. (2018). An Artificial Immune System based Method for Defense against Wormhole Attack in Mobile Adhoc Networks. TABRIZ JOURNAL OF ELECTRICAL ENGINEERING, 47(4), 1407-1419
28. Fotohi, R., Bari, S. F., & Yusefi, M. (2019). Securing Wireless Sensor Networks Against Denial-of-Sleep Attacks Using RSA Cryptography Algorithm and Interlock Protocol. International Journal of Communication Systems.
29. Seyedi, B., & Fotohi, R. NIASHPT: a novel intelligent agent-based strategy using hello packet table (HPT) function for trust Internet of Things. The Journal of Supercomputing, 1-24.
30. Fotohi, R.; Nazemi, E. An Agent-Based Self-Protective Method to Secure Communication between UAVs in Unmanned Aerial Vehicle Networks. Preprints 2020, 2020010229 (doi: 10.20944/preprints202001.0229.v1).
31. Jamali, S., & Fotohi, R. (2016). Defending against wormhole attack in MANET using an artificial immune system. New Review of Information Networking, 21(2), 79-100.
32. Behzad, S., Fotohi, R., Balov, J. H., & Rabipour, M. J. (2018). An Artificial Immune Based Approach for Detection and Isolation Misbehavior Attacks in Wireless Networks. JCP, 13(6), 705-720.
33. Sankar, S., Srinivasan, P., Ramasubbareddy, S., & Balamurugan, B. (2020). Energy-aware multipath routing protocol for internet of things using network coding techniques. International Journal of Grid and Utility Computing, 11(6), 838-846.
34. Pushpalatha, M., Anusha, T., Rao, T. R., & Venkataraman, R. (2020). L-RPL: RPL powered by laplacian energy for stable path selection during link failures in an Internet of Things network. Computer Networks, 107697.
35. Jemili, I., Ghrab, D., Belghith, A., & Mosbah, M. (2020). Cross-layer adaptive multipath routing for multimedia Wireless Sensor Networks under duty cycle mode. Ad Hoc Networks, 109, 102292.