Contents lists available at Mapta Publishing Group

Vol. 3, No. 1, January, 2021

Mapta Journal of Electrical and Computer Engineering (MJECE)

journal homepage: http://maptapublishing.com/index.php/mjece

ISSN: 2631-5718

A Novel Security Based Routing Method Using Ant Colony Optimization Algorithms and RPL Protocol in the IoT Networks

Navid Abapour[a,*], Parisa Ghane[b], Aynaz Shafiesabet[c], Rasoul Mahboub[a]

[a] *Department of Computer Science, Faculty of Science, University of Mohaghegh Ardabili, Ardabil, Iran*
[b] *Department of Electrical and Computer Engineering, Texas A&M University, USA*
[c] *Department of Computer Engineering, Islamic Azad University South Tehran Branch, Tehran, Iran*

Article Info

Article history:

Received Dec 8th, 2020
Revised Jan 26th, 2021
Accepted Feb 14th, 2021

Keyword:

ACO Algorithms
IoT Security
Reliability Engineering
Network Routing

Abstract

Recently proposed routing protocols, for the IoT networks platform, have been mostly based on reducing the data transfer's energy. These approaches typically assume that the data link layer protocols provide the required reliability for data transmission. However, the nature of the networks affects the quality of information transmission; high error rates lead to a loss of aggregated information. To optimize the routing quality, in this paper, we proposed a security-based method by employing RPL protocol and Ant Coloney Optimization (ACO) algorithms. Our method considers the destination nodes as the root and proposes an ACO-based routing process aiming for an increased security and reliability. Performance of the proposed method was compared with the state-of-the-art protocols. Our simulation results suggest that the proposed method is advantageous in terms of security and reliability parameters, such as throughput and number of packets, as well as the algorithm's running time complexity.

1. Introduction

The Internet of Things is a new paradigm that helps connect devices and heterogeneous objects and provides an integrated framework that allows interoperability across diverse contexts, and enables the ability to share information globally with any device [1]. This technology provides an Internet connection privilege for each device by providing a unique identity for each object. The main focus of this technique is to allow "anyone" or "anything" at "any time" to exchange information services from "anywhere" to "anywhere".

To achieve this, an intelligent protocol is needed that includes data transfer between heterogeneous devices. Using an intelligent protocol based on various parameters such as load balance, packet loss, bandwidth consumption and energy consumption in heterogeneous devices will help users to optimize routing in the Internet of Things [2]. Also, there is a popular protocol used in closed paths in the IoT environment, and it is considered as a standard for a flat routing protocol, which known as "RPL". In order to increase energy reliability and efficiency, the RPL traverses routes based on a link estimator mechanism, and selects the remaining energy and latency. In addition, the RPL proposes an event trigger mechanism to provide load balancing and prevent premature depletion of node energy in the network. The results show that RPL increases network life and service access as well as the quality of IoT services. It also provides redistribution of scarce network resources and reduces packet losses compared to the performance of known protocols.

Many researchers are trying to define a methodology for connecting heterogeneous objects through the Internet, which ultimately leads to the concept of the Internet of Things. Everything in IoT systems is a unique attribute that must be used by a unique address. In IoT systems applications, sensed data must be collected and sent to management nodes, and ultimately through reliable routing protocols. Routing protocols are created for two general purposes, the first is to improve data transfer and scalability and the second is to reduce energy consumption [2, 3].

* Corresponding author: navidabapour@gmail.com

IoT systems are made up of different networks in large-scale environments. However, most routing techniques in this type of network are focused on wireless sensor networks, which are considered to be the core of IoT systems [4-6]. Data transfer security is important for communication in human-human, human-machine or machine-to-machine interactions, and time also plays a very important role in data transmission, so the data must be routed in such a way that the least or Have the shortest route to reach the destination. Therefore, different routing protocols have been used to transmit data. In IoT systems, to improve the routing process, the ant colony path improvement algorithm has recently been used to find the shortest and best path, even in overlapping areas [7-9].

Considering Genetic algorithms, the connection of these ants is with the use of the chemical pheromone. When an ant moves in one direction, it releases a pheromone on the ground, causing subsequent ants to follow it. The pheromone has a predominance that is stimulated over a single period of time, so the higher the pheromone resistance of the ant, the newer the pathway. In fact, the goal of IoT integration is to communicate multiple times by monitoring a single self-contained system. The system also includes remote monitoring and monitoring, maintenance and management operations that collect and send data over the network. As a result, researchers are trying to improve the data transmission path and state that different system features may cause data transmission between nodes.

According to the general objectives in the above cases, the purpose of this study is to provide a suitable and safe routing algorithm to shorten and improve the route according to the parameters of end-to-end delay, packet loss rate, bandwidth, energy consumption rate, Control is the reduction of header bits, throughput, and load balancing to deliver sensed data to IoT systems. Therefore, using an intelligent protocol based on various parameters in heterogeneous devices will help to optimize the routing in the Internet of Things.

2. Related works

The Internet of Things is a new paradigm that helps connect devices and heterogeneous objects and provides an integrated framework that allows interoperability across diverse contexts, and enables the ability to share information globally with any device [1]. This technology provides an Internet connection privilege for each device by providing a unique identity for each object. The main focus of this technique is to allow "anyone" or "anything" at "any time" to exchange information services from "anywhere" to "anywhere".

According to the general objectives in the above cases, the purpose of this study is to provide a suitable and safe routing algorithm to shorten and improve the route according to the parameters of end-to-end delay, packet loss rate, bandwidth, energy consumption rate, Control is the reduction of header bits, throughput, and load balancing to deliver sensed data to IoT systems. Therefore, using an intelligent protocol based on various parameters in heterogeneous devices will help to optimize the routing in the Internet of Things.

Context-Awareness in Sea Computing Routing, which known as CASCR, is an intelligent protocol based on IoT's key technologies. In 2017, a novel method was presented by utilizing CASCR with the RPL routing protocol. This technique is used in a decentralized manner with the advantage of reducing latency and improving search performance. In this method, it is considered for delivering data packets and bypassing busy routes, which provides the realization of network latency. The general features of this technique are as follows:

- Information devices are embedded in various objects, so the sensors do the matching work. Devices also use their life cycle as an object.
- Independence: Objects are not passively controlled, but have a certain ability to be independent and ironic.
- Local interaction: Computations make full use of local principles and objects are mainly through local interaction to realize communication.
- Crowd Intelligence: The IoT computing model is a dynamic self-consistent system. The intelligent algorithm in a node can't get the result and must communicate with others using the embedded intelligent algorithm to make an intelligent decision [10].

ZigBee is a popular protocol used in closed paths in the IoT environment. Therefore, it is considered as a standard for a flat routing protocol. In 2014, an intelligent routing-based protocol was developed using ZigBee for IoT applications. In this protocol, in order to increase reliability and energy efficiency, the ZigBee traverses the paths based on a link estimator mechanism, and selects the remaining energy and the latency rate. In addition, ZigBee proposes an event trigger mechanism to balance the load and prevent premature depletion of nodes in the network. Performance appraisals were performed using simulations and experiments to measure the impact and benefits of ZigBee on small and large networks. The results show that ZigBee increase network life and access to services as well as the quality of IoT services. It also provides redistribution of scarce network resources and reduces packet losses compared to the performance of known protocols. After receiving all the events as input, this method analyzes all its components based on their resources and capacity [11].

Considering that load balancing is one of the major challenges in IoT systems and the dynamic distribution of workload between different nodes should be done in such a way that no additional load is placed on the resources and also the resource load should not be reduced too much, in 2017, a load balancing algorithm based on a genetic algorithm was introduced. In this algorithm, the goal is to reduce the overall execution delay, a number of tasks in the infrastructure system as a service, so that the resource load get balanced. The genetic load balancing algorithm works as follows:

- Randomly initializes a population of processing units after encryption and converts them to binary strings.
- The amount of viability of each node of the population is calculated (viability).
- Do the following as long as the number of repetitions allowed or the optimal solution is available:
  - ✓ Identify the chromosomes with the lowest eligibility and the highest eligibility and list them in pairs (selection).
  - ✓ Making a mating spot and choosing a random mating spot to create new offspring (mating).
  - ✓ Newborn mutation with a probability of 0.05 mutation
  - ✓ Given that the new child's place is the address of the new community, use this population for the next round of repetition (admission).
  - ✓ Test to check the end condition [3, 12, 13].

Furthermore, in 2020, another method was proposed based on multiple balance of parameters and Markov algorithm. In this type of routing, the next-hop node path is used in the repetition process of the ant colony algorithm to calculate the probability of node transfer in the decision, and the simulation results show that in this algorithm, the overhead generated by the messages is effectively reduced, and grid energy consumption is balanced [14].

In addition to using Min-Min [15], Min-Max [16], and two-step load balancing [17] methods, other researches have been done in this field, among which the following can be considered practical in IoT systems:

- Using genetic algorithms to reduce work scheduling time and balancing: This algorithm considers two factors: load balance and reduction of work execution time. The drawback of the proposed algorithm is that it does not consider any priority between tasks [18].
- ACO algorithms utilization for transferring data in different processors: Tasks are moved by ants between nodes in a graph that are system processors. The rule of this displacement is based on the following algorithm: first, each ant calculates its average load and then determines the local error based on its average load and previous ants. Using an error tolerance factor and the amount of footprints left by other ants, it is likely to stay or leave the processor and migrate [19].
- Utilizing an active clustering algorithm based on grouping similar nodes: A node starts the process and selects a different node as its interface node from its valid neighbor nodes. The interface node forms a connection between a neighbor and the same type of primary node. The interface node then disconnects the primary node from itself, and these processes are repeated. In this algorithm, the efficiency of the system increases with increasing resources and as a result, the operational power increases with the use of these efficient resources. On the other hand, as the diversity of the system increases, the quality of its output decreases [20].

3. Proposed Algorithm

Ant colony optimization for optimization problems in various branches has been successfully used as a promising algorithm and has clear advantages in adapting routing in communication networks. The following is an inter-node routing method based on ant colony that is performed in several different steps.

An ant is placed in each node at regular intervals to find its way to the base destination node. Each node ant then determines the next step according to the following formula:

$$p_{ij}^{k} = \frac{\left[\tau_{ij}(t)\right]^{\alpha}\left[LET_{ij}\right]^{\beta}}{\sum_{s\in N_i}\left[\tau_{is}(t)\right]^{\alpha}\left[LET_{is}\right]^{\beta}} \quad (1)$$

In Equation (1), p^{k}_{ij} is the probability that the ant k chooses to move from node i to node j, and it can be seen as a tolerance between the ability (which says that nodes with more *LET* should be selected) and the intensity of the actual sequence (If a lot of ants pass over the connection (V_i, V_j), then this connection is much more suitable for use). The amount of the pheromone sequence is the edge (V_i, V_j) and the visibility function of the node V_i to V_j. Also, α and β are

parameters that control the ratio of the importance of the sequence to visibility. N_i is a set of neighbors of node V_i in the tree that node can be selected by k ant in the next step.

```
function [paths] = ANT_Colony(paths, alpha, beta, node)
for i = 1:1:length(paths)
  paths(i).pheromone = 0.00001;
end
for ant = 1:1:numberofANTs
  for i= 1:1:length(paths)
    propability(i) = ((paths(i).pheromone ^ alpha) * (paths(i).RET ^ beta));
  end
  MaxPropability = 0;
  for i = 1:1:length(paths)
    if MaxPropability <= propability(i)
      MaxPropability = propability(i);
      antPath = i;
    end
  end
  paths(antPath).pheromone = paths(antPath).pheromone + 1;
  for i = 1:1:length(paths(antPath).step) - 1
    sendpacket = sendpacket + 1;
    dist = distancee(node(paths(antPath).step(i)), node(paths(antPath).step(i + 1)));
    time = time + timecalculation(dist, control_packet);
  end
  sendpacket = sendpacket + 1;
  dist = distancee(node(paths(antPath).step(i)), node(paths(antPath).step(i + 1)));
  time = time + timecalculation(dist, control_packet);
end
Max_Pheromone = 0;
for i = 1:1:length(paths)
  if paths(i).pheromone >= Max_Pheromone
    Max_Pheromone = paths(i).pheromone;
    BestPath = paths(i);
  end
end
paths = BestPath;
end
```

Figure 1. Routing by Ant colony algorithm. The process of sending information from the destination node to the applicant node is done by routing between other nodes in several steps.

The path information is collected by the passing ants, and the root node begins to analyze the data after the k ant arrives. The information collected by ants is defined as follows:

$$\left\{(V_0, d_{(V_0,V_1)}), (V_1, d_{(V_1,V_2)}), (V_2, d_{(V_2,V_3)}), ..., (V_{l-1}, d_{(V_{k-1},V_k)})\right\} \quad (2)$$

Where V_0 is the root node and S_k is the destination node. The discrete sequence of $\{V_0,V_1,V_2,\ldots,V_k\}$ nodes forms the path. In addition, to evaluate the path mentioned above, the *RET* value is defined as follows:

$$RET = \min\left\{LET_1, LET_2, LET_3, ..., LET_n\right\} \quad (3)$$

After calculating the duration of two-node link stability time (*LET*), the path stability time (*RET*) method can be used to find the longest lifespan compared to other paths with the highest reliability in data transmission. Route Stability Duration (*RET*) is expressed in terms of minimum Link Stability Duration (*LET*). Developers need to record information such as speed and direction in the path response message to calculate the discovery time duration of the RET path. In the route discovery phase, the route request message is sent to the neighbors. The message is sent step by step by neighbors who act as intermediaries until it is delivered to the intended source. After finding the source, the message (route response) is sent to the destination from the delivery route (vice versa). Position and direction are added in the reply message so that the duration of the link stability between the two peers can be calculated.

Initially, the *LET* value is zero; and each peer, based on the position and direction information recorded in the message, calculates the connection life time (*LET*) with the next peer (neighbor) and records the LET value, and in recording the *LET* value, the minimum value in each step is taken and this causes the *LET* value to be updated. It should be noted that at each step, the *LET* connection duration information is recorded in each peer routing table. This causes the intermediate peer, reply message, and long-term *LET* link stability information to be generated from their routing table if future (similar) source searches are performed. Eventually this process continues until the response message containing the minimum *LET* calculated from the entire path reaches the destination; finally, the path with the highest *RET* value is selected.

It's notable that according to the evaluation function, the best path among all the ants is obtained in the first iteration by the base station. The base station then broadcasts a message informing the nodes in the best way to update the pheromone according to the following equation:

$$\tau_{ij}(t+n) = (1-\rho)\tau_{ij}(t) + p\,\tau_{best} \tag{4}$$

The symbol ρ in equation (4) is the latency coefficient so that $(1-\rho)$ represents the reservation of the pheromone concentration until the last update time. After completing this process, the most appropriate path in the tree is determined and the message is sent.

Considering that the proposed method uses a post-discovery protocol, the results obtained in terms of convergence and stability are evaluated, which will be presented below. The parameters of the improved ant colony algorithm are shown in Table (I). Also, in Table (II) the IoT network environment is specified by the number of nodes.

Table 1. ACO Algorithm's Parameters

Parameter	Value
Number of ants	31
α	1
β	2
θ	0.1
Maximum repetition	200

Table 2. Simulation Parameters

Parameter	Value
Network size	100 × 100 m
Maximum number of packages	60
Number of nodes	100
IEEE standard	802.11bit
Type of network traffic	CBR
Radio packet transmission range	250 m
Maximum speed	20 m/s
Package smoothing factor	0.4%

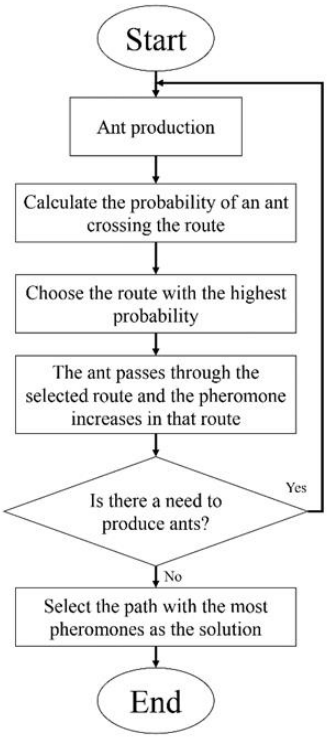

Figure 2. Proposed method's flowchart. The proposed method uses the idea of tree and mesh routing in IoT systems. Some of the main objectives of this method are to improve the load balance and packet loss rate, bandwidth and current latency. This is done based on the estimated duration of stability.

4. Power and Latency Comparison

This section evaluates the performance of the proposed ant colony protocol with RPL and SecTrust-RPL [4] protocol in terms of throughput and latency. In two cases, these criteria have been evaluated in terms of maximum packet speed and number of nodes, each of which is described below.

4.1. Comparison based on maximum speed

Figure (3) shows the latency for 20 nodes in which the mobility and speed of the nodes were variable. Depending on the shape, as the speed and mobility increase, the proposed protocol reduces the number of transfers expected. As a result, it increases system throughput indirectly and therefore has a higher throughput and less latency than the SecTrust-RPL protocol.

In the proposed protocol, the dynamic swarm distance method omits one person at a time and recalculates the distance between people. So this method can provide a better chance of keeping the person in the non-dominant set. Therefore, according to Figure (4), the throughput of the proposed protocol is higher than SecTrust-RPL.

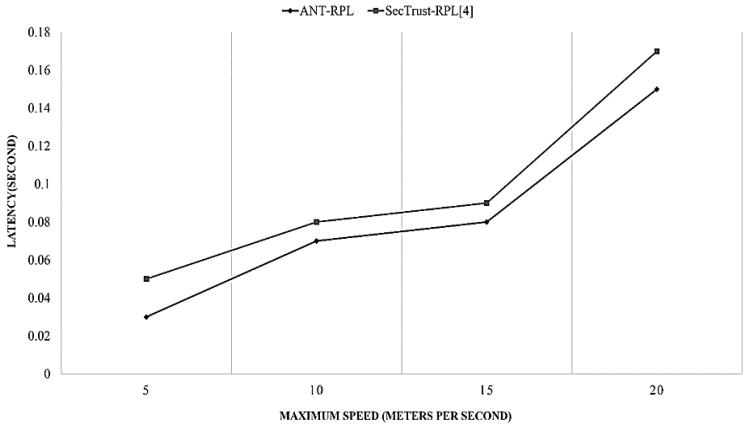

Figure 3. Delay rate due to increased speed

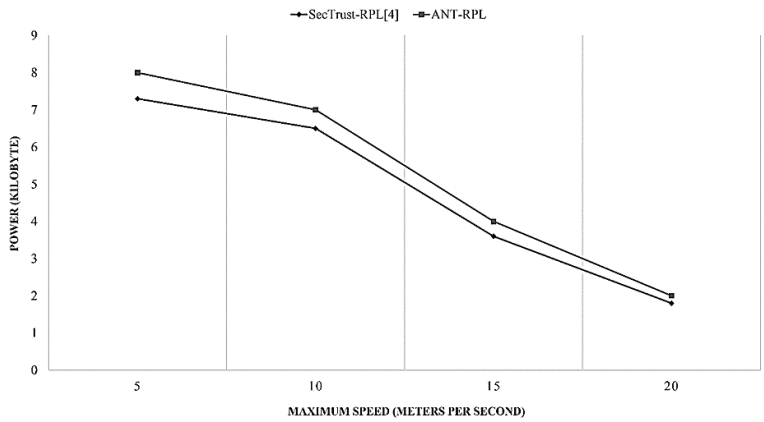

Figure 4. Power rate due to increased speed. The throughput for 20 nodes in which the mobility of the nodes was variable.

4.2. Comparison based on number of nodes

Figure (5) compares the transmission delay of two ant colony protocols with RPL and SecTrust-RPL with an increase in the number of nodes. Depending on the shape, when the number of nodes increases, the proposed protocol reduces the number of expected transfers. As a result, it increases system throughput indirectly and therefore has a higher throughput than the SecTrust-RPL protocol.

Figure (6) compares the throughput of the two ant colony protocols with RPL and SecTrust-RPL with an increase in the number of nodes from 20 to 100 nodes. According to the Figure (6), when the number of nodes increases, the proposed protocol reduces the number of expected transfers. As a result, it increases system throughput indirectly and therefore has a higher throughput than the SecTrust-RPL protocol.

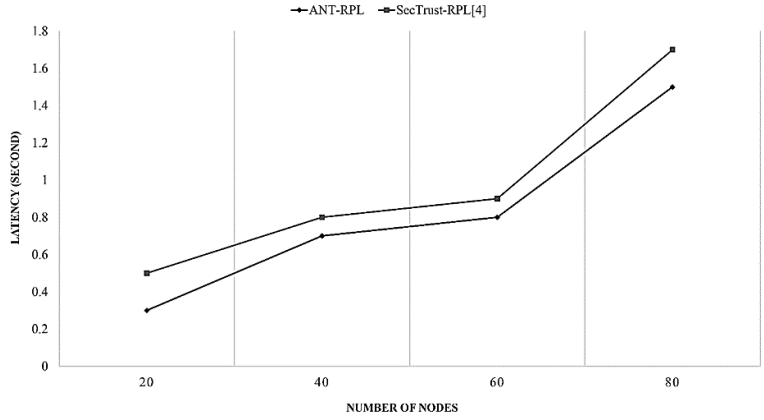

Figure 5. Delay rate due to increase in the number of nodes

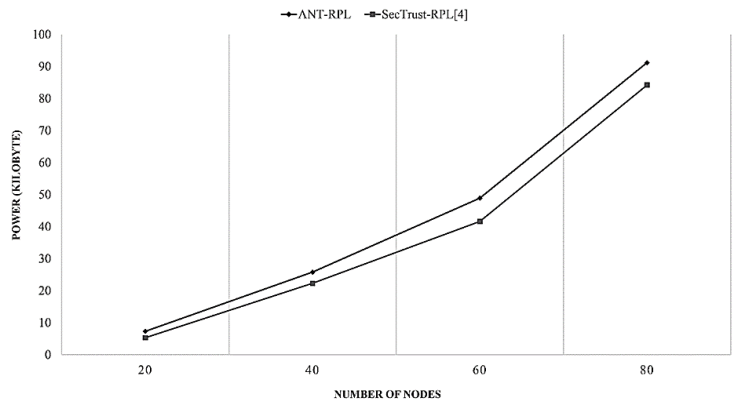

Figure 6. Power rate due to increase in the number of nodes

5. Conclusions

In this research, a new method for optimal security-aware routing with the RPL protocol on the Internet of Things is presented. Since the RPL protocol is a distance vector routing protocol that organizes nodes into a goal-oriented directionless graph, in this method the destination nodes that provide the Internet connection are considered as the root. . In this research, the routing process is proposed with the aim of improving the quality of service and further improving the routing process. An algorithm based on the ant colony algorithm is proposed. The proposed protocol was implemented with different parameters and related diagrams were expressed. The ant colony protocol with RPL to solve optimization problems does not give a definite answer and finds a near-optimal answer. To show the performance of each protocol, it is necessary to compare it with previous protocols; therefore, the results of this paper were compared with similar protocols in terms of throughput and number of packets and showed better results than other methods and the response time of ant colony protocol with RPL is shorter compared to the compared protocols.

References

[1] Y. Lu, W. Hu Secure routing for internet of things: A survey. The proceeding of School of Computer and Information Engineering, Harbin University of Commerce, Harbin, China, 2016. pp. 223 - 6.

[2] S. Maamar. Evaluation of qos parameters with rpl protocol in the internet of things. Proceedings of the International Conference on Computing for Engineering and Sciences2017. pp. 86-91.

[3] O. Said. Analysis, design and simulation of Internet of Things routing algorithm based on ant colony optimization. International Journal of Communication Systems. 30 (2017) e3174.

[4] D. Airehrour, J.A. Gutierrez, S.K. Ray. SecTrust-RPL: A secure trust-aware RPL routing protocol for Internet of Things. Future Generation Computer Systems. 93 (2019) 860-76.

[5] C. Vallati, E. Ancillotti, R. Bruno, E. Mingozzi, G. Anastasi. Interplay of Link quality estimation and RPL performance: An experimental study. Proceedings of the 13th ACM Symposium on Performance Evaluation of Wireless Ad Hoc, Sensor, & Ubiquitous Networks2016. pp. 83-90.

[6] M. Dorigo, M. Birattari, T. Stutzle. Ant colony optimization: artificial ant as a computational intelligence technique. university libre de bruxelles. IRIDIA Technical report Series, Belgium, Tech Rep. (2006).

[7] P. Thapar, U. Batra. Implementation of ant colony optimization in routing protocol for internet of things. Innovations in Computational Intelligence. Springer2018. pp. 151-64.

[8] H.-S. Kim, H. Cho, H. Kim, S. Bahk. DT-RPL: Diverse bidirectional traffic delivery through RPL routing protocol in low power and lossy networks. Computer Networks. 126 (2017) 150-61.

[9] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, M. Ayyash. Internet of things: A survey on enabling technologies, protocols, and applications. IEEE communications surveys & tutorials. 17 (2015) 2347-76.

[10] M. Bezunartea, B. Sartori, I. Francés, J. Tiberghien, A. Braeken, K. Steenhaut. Enabling dual-band operation with the RPL routing protocol. Proceedings of the 15th ACM Conference on Embedded Network Sensor Systems2017. pp. 1-2.

[11] H. Ali. A performance evaluation of rpl in contiki. 2012.

[12] M. Darbandi, A.R. Ramtin, O.K. Sharafi. Tasks mapping in the network on a chip using an improved optimization algorithm. International Journal of Pervasive Computing and Communications. (2020).

[13] S. Pourjabar, G.S. Choi. CVR: A Continuously Variable Rate LDPC Decoder Using Parity Check Extension for Minimum Latency. Journal of Signal Processing Systems. (2020) 1-8.

[14] T.-H. Lee, X.-S. Xie, L.-H. Chang. RSSI-based IPv6 routing metrics for RPL in low-power and lossy networks. 2014 IEEE International Conference on Systems, Man, and Cybernetics (SMC). IEEE2014. pp. 1714-9.

[15] A. Tavakoli, D. Culler. HYDRO: A hybrid routing protocol for lossy and low power networks. IETF Internet Draft2009.

[16] W. Kastner, G. Neugschwandtner, S. Soucek, H.M. Newman. Communication systems for building automation and control. Proceedings of the IEEE. 93 (2005) 1178-203.

[17] V.C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, et al. A survey on smart grid potential applications and communication requirements. IEEE Transactions on industrial informatics. 9 (2012) 28-42.

[18] G. Montenegro, N. Kushalnagar, J. Hui, D. Culler. Transmission of IPv6 packets over IEEE 802.15. 4 networks. Internet proposed standard RFC. 4944 (2007) 130.

[19] J.W. Hui, D.E. Culler. IP is dead, long live IP for wireless sensor networks. Proceedings of the 6th ACM conference on Embedded network sensor systems2008. pp. 15-28.

[20] N. Kushalnagar, G. Montenegro, C. Schumacher. IPv6 over low-power wireless personal area networks (6LoWPANs): overview, assumptions, problem statement, and goals. (2007).