Internet of Things Optimal Routing based on Markov-Reinforcement Learning Algorithm

Jamal M.Ali Radha
Ministry of Education , Kalar Directrade of Education , [1]jama4545l@gmail.com
Raza Y. Abdulrahman
[2]Ministry of Education , Shekhan Directrade of Education ,
[2]razayassin78@gmail.com

Abstract

By increasing Internet of Things (IoT) development, it will face new challenges due to its application in various fields of science and industry. One of these challenges is the routing problem in communication which has many effects in various parts and the quality criteria of the IoT in communication. In this research, a new approach provide with an effective and optimal method for routing in the IoT, which will use 6LoWPAN as the default protocol. This protocol has qualitative weaknesses and its goal is to improve and extend it as much as possible with the Markov Reinforcement Learning (MRL). Improving power consumption and reducing energy beside quality of services criteria optimization is the main targets of this approach. The results represented the improvement of the proposed approach compared to other similar protocols such as Z-WAVE and Zig Bee and the classic 6LoWPAN protocol.

Keywords: Internet of Things (IoT), Routing, 6LoWPAN Protocol, Markov Reinforcement
Learning (MRL)

إنترنت الأشياء التوجيه الأمثل على أساس خوارزمية التعلم المعزيز ماركوف

جمال محمد علي رضا
وزارة التربية ، مديرية تربية كلار jama4545l@gmail.com1
رضا يسين عبدالرحمن
وزارة التربية ، مديرية تربية شيخان razayassin78@gmail.com2

خلاصة

ان زيادة تطوير إنترنت الأشياء(IoT) ، ستواجه في المستقبل تحديات جديدة سبب تطبيقها في عدة مجالات منها العلوم والصناعة. أحد هذه التحديات هي مشكلة التوجيه في الاتصالات والتي لها تأثيرات عديدة في أجزاء مختلفة ومعايير جودة إنترنت الأشياء في الاتصالات. من خلال هذا البحثتسليط الضوءعلى نهج جديد يوفر طريقة فعالة ومثالية للتوجيه في إنترنت الأشياء، والذي سيستخدم 6LoWPANكبروتوكول افتراضي. يحتوي هذا البروتوكول على نقاط ضعف نوعية وهدفه هو تحسينه وتوسيع نطاقه قدر الإمكان باستخدام نظام ماركوف للتعلم المعزز .(MRL) إن تحسين استهلاك الطاقة وتقليل الطاقة إلى جانب تحسين معايير جودة الخدمات هو الأهداف الرئيسية لهذا النهج. وتمثل النتائج تحسين النهج المقترح مقارنة بالبروتوكولات المماثلة الأخرى مثل Z-WAVE و Zig Beeوبروتوكول 6LoWPANالكلاسيكي.

الكلمات المفتاحية: إنترنت الأشياء (IoT)، التوجيه، بروتوكول 6LoWPAN، تعزيز ماركوف التعلم (MRL)

Introduction

IoT is a computing concept to describe the future in physical objects connecting to the Internet one after the other and communicate with other objects [1]. IoT is closely related to the concept of radio frequency identification as a communication method, but also includes sensor technologies, wireless technologies, rapid response codes, etc. IoT has a layered architecture. First, there's the perception layer in which statistics is obtained from the physical world [1]. In the next step, the information is transmitted over the network. Finally, the information Is used in the software layer; therefore, IoT includes these items which has its own technologies. The application layer does not help build the IoT, but is cease hosts that uses the information received from the IoT; therefore, the focus on the technologies that IoT needs is focused on the two layers of perception and network. The first technology is related to those that receive information (perceptual layer). The next classification is related to those who make the network layer [2].

We are still facing these challenges during the research conducted in the field of improving communication protocols and routing optimization to find a solution, so that while there is a problem such as lack of power consumption and the use of powerful hardware due to the lack of enough space, it is possible to use routing protocols to cover the shortcomings and in parallel to provide users with topics such as the speed of data exchange and fast processing with high reliability [3].

The standard protocol defined on the physical layer And link layers of wi-fi non-public region networks and the IoT is IEEE 802.15.4. IEEE 802.15.4 uses a CSMA/CA Device with optional time slot and security features for the link layer or MAC. There are some of standard and non-standard protocols for implementing IoT networks. Zigbee and Z-Wave are among non-standards [4] and 6LoWPAN is a standard type that connects the main IoT network [4]. The routing protocol considered in this research is 6LoWPAN and the goal of its optimization with the help of Markov Reinforcement Learning (MRL) is to minimize the delay in transmitting and receiving data by improving power consumption and reducing energy. Also improve data throughput and reduce amount of noise in data.

In this research, our main idea is to increase the efficiency of the communication network between objects by improving the routing operations intelligence using different factors considering that so far the efforts to improve communication and increase network efficiency have been investigated from different perspectives. Based on the nature of the data, before transmitting and selecting the next node, decisions will be made using various predefined elements regarding routing and it seems that the use of this technique will lead to reducing the delay time, reducing

the overall network traffic, and also the lifetime of the network will increase. Therefore, a routing protocol should be considered. This research uses the 6LoWPAN routing protocol, which uses the Markov Reinforcement Learning (MRL) and its operators, including the initial population, crossover, mutation, reproduction, and iteration to improve energy consumption in nodes, data throughput and Signal to Noise Ratio (SNR).

Literature Review

In this section, the used protocol known as LoWPAN6 is discussed, as well as some studies similar to this research. This protocol includes low-cost wireless networks that support the IEEE 802.15.4 specification. However, this technology has many drawbacks, including small package sizes, low bandwidth, low power, bulky devices, radio connection reliability issues, battery drain, device lock-ups, and overheating. However, by combining with the Internet Protocol, the mentioned problems can be solve, thus LoWPAN6 is created. This protocol allows the transmission of IPv6 packets in IEEE 802.15.4 networks, which is a significant issue considering the increasing Quantity of objects related to the net. This protocol has significant Advantages as compared to non-preferred protocols together with ZigBee and Z-Wave which are mentioned below [5]:

✓ There is no need for gateways to translate various non-standard protocols which provided that all wireless sensor Networks use the standard net protocol.

✓ Flexibility will increased For the reason that new packages do not require specific modifications to protocols.

✓ Quick connection And compatibility with preceding current architectures.

✓ Plug and play state.

✓ Rapid development of applications in addition to the possibility of aggregating existing objects in web services that use the Internet protocol.

However, all nodes must agree on the same protocol for LoWPAN6 conversion. Most current Wireless Sensor Network (WSN) Protocols have constrained assist for operating on different interfaces. This has caused complications that make the formation of a WSN With exceptional protocols to speak with the wide Internet as a challenge and Sizeable hardware and software sources are Vital to transform WSN protocol information into related TCP/IP standards. This issue can add additional overhead to the system and reduce performance. While WSN protocols have been Advanced to help IPv6, the software layers that implement various LoWPAN6 services must support intra- Tool communication. The final purpose of the IoT Is to make this implementation definitely beneficial [5].

Until today, Diverse strategies had been used to optimize routing with the aim of ensuring security in the IoT. One of the most recent researches in this field is presented in [6], which uses a lightweight and geographically distributed Multicast

routing protocol. At first, nodes need a lot of calculations to make a decision on transmitting multicast data. If the net has protection holes, the Built multicast Paths might Additionally be very lengthy and there may additionally also be a loop in some parts. The motive of presenting this research is to solve the Existing demanding situations. In another research, the use of RPL protocol for routing in the IoT has been discussed [7]. The proposed approach of this research is a content-oriented method where the paths determined by the content. A higher data accumulation rate created Because of the routing of the correlated information to the commonplace Relay nodes for processing that is the first assignment that can be solved by the forward-looking approach. Also, delay reduction considered as another issue in this research. In [8], the use of SDN controller with an energy consumption-aware routing approach in the IoT considered. The energy consumption reduction of In Heterogeneous devices associated to the internet happens on this research. Also, an SDN controller used as a central manager To provide a at ease environment in the net.

In another study [9], the use of RPL routing protocol considered To lessen strength intake and growth the battery existence Of sensors in a WSN whose sensors are linked to the net. Likewise, a standard analysis of routing methods in electricity -wasting Networks which include WSNs With the aim of energy intake reduction in the IoT presented. In [10], the use of the Z-Wave routing protocol in a secure environment in a network based on the IoT discussed. Also, in [11], a geographic routing method presented in health monitoring systems based on the IoT environment.

In [12] Examined the answers, Demanding situations, possibilities and technology for the usage of cloud computing in the IoT. Also in [13], The strategies of the usage of fog computing inside the cloud and its answers are mentioned. In [14] provided a flexible IoT- Based security middleware primarily based on stop-to-end computing. Using superior schematic decision set of rules has been studied and simulated as the main approach. In [15], A assessment of protection Issues has been studied in fog computing and techniques in their utility in different networks, specially cloud computing, IOT, and so on. The scope of the usage of IoT-primarily Based totally fog computing has been extended to scientific subjects and their intelligence. In one of the maximum essential researches, The use of IoT computing platform in electronic health structures has been studied and answers, demanding situations, safety troubles and protocols have been mentioned [16]. The game concept systems in evolutionary mode [17] Used to address safety worrying situations in fog computing has been studied, simulated and modeled. In [18] studied strategies for securing fog computing in the IoT and Providing answers Based totally at the have a look at of assaults on cloud layers, fog and part

computing community. Also in [19] deals with the safety troubles of using IoT computing based at the kind of system and standards used.

In [20] offered a state of affairs aware of community Behaviors in fog and aspect computing with a Protection perspective. The development of a multilayer framework primarily based on earlier information has been taken into consideration in this studies to keep in mind The safety concepts in transmitting And receiving information. In [12+15] Using Cryptographic standards used to make sure information protection. Simultaneous use of cryptographic algorithms known as CCA and ABE has been taken into consideration on this studies, which represented the consequences of decoding and encrypting information on the time of transmitting and receiving, and a comfortable surroundings for fog computing has been created. [22], A case observe has been performed within the safety issues area and challenges of the two laptop structures such as fog and edge computing. Identification of strange behaviors and norms Is considered in diverse fog and facet computing protocols. In [23] The usage of software-defined net (SDN) technology and fog computing has been studied and Researched as a supply chain surroundings in transmitting and receiving facts so that you can security, Deployment, routing and clustering within the IoT. Privateness with reference to protection situations for Using cloud computing in the internet of things has also been studied and researched in [24] Which supplied a relaxed protocol with statistics privateness based on cryptographic concepts changed into the principle aim of the studies. In keeping with these studies, most of the cases within the field Of securing the usage of fog computing within the IoT, have supplied solutions, however have no longer provided a entire and accurate model. Therefore, modeling is hard and complicated and one of the troubles of this case is the inability to evaluate with distinctive techniques, due to the fact the appropriate evaluation standards for this works have not yet been developed.

Proposed method

First, the general architecture of the IoT should be considered. IoT network consists Of three kinds of nodes, including sensor nodes, sink nodes, and relays. Sink nodes are responsible for collecting and processing data from all sensors. IoT environment is contracted in a specific dimension which is two-dimensional, i.e. $X_{direction} \times Y_{direction}$ which will be in meters. In general, in this proposed approach, $S = \{1,2,3, \dots, s\}$ refers to nodes and $P = \{1,2,3, \dots, p\}$ refers to candidate nodes and also $N = \{1,2,3, \dots, n\}$ refer to a set of sinks. Every relay can establish a wireless hyperlink with any type of node or relay that is in its communication range, which is called R_c. The communication range of nodes is indicated by R_s, which should be $R_c \geq R_s$. In fact, it is assumed that nodes And relays can also have distinct transmission power. Sensor nodes Can lessen their transmission power to minimize

the amount Vital to maintain network connectivity. Relay nodes may have lower limits on power, so the equation $R_c \geq R_s$ holds.

An ordered vector is defined as OR_i for each sensor i which is accessible as Wireless relays. These relays are sorted From the nearest to the farthest region With recognize to node i. The j-th and k-th elements of OR_i are given as $OR_i(j)$ and $OR_i(k)$, Respectively, and they Represent the relays in j-th and k-th regions in the vector. So if $j < k$, then $OR_i(j)$ Is towards sensor i than relay node $OR_i(k)$. It should be noted that I_i is the index of a set of sorted vectors OR_i.

The cost of installing a relay in candidate vector j is shown as C_j^I and its capacity is shown as $v_i \ , \ \forall j \in P$. Moreover, The visitors generated with the aid of sensor i along sink k is in the form of given parameters i.e. $w_{ik} \ , \ i \in S \ , k \in N$. The rest of the communication parameters can be calculated according to the positions of nodes, relays or candidates and sinks. Node coverage parameters in an area are $a_{ij} \ , \ i \in S \ , \ j \in P$. a_{ij} is divided into two parts: 1) if its value is one, if it creates new links between a relay installed in candidate nodes j, 2) if its value is zero, other states are checked.

The sink coverage parameters are also in the form of $e_{jk} \ , \ j \in P \ , \ k \in N$ which has two parts that include 1) its value is one, if a relay installed node in candidate nodes j Can set up a hyperlink with sink k and 2) If its value is zero, other states are checked.

It is clear and obvious that a_{ij} is in the proximity of sensor i to candidate nodes j in the form of being placed in the diffusion condition between the same nodes. e_{jk} Is also associated with the distance among candidate node j and sink k. Finally, $b_{jl} \ , \ j,l \in P$ refer to the communication parameters between two different candidate nodes, which depends on the proximity of relay j and l in the network, which has two parts: 1) its value is one, if the candidate nodes j and l can communicate with a wireless link communicates and 2) its value is zero, other states are checked.

The choice variables of the hassle include node allocation variables, which are $x_{ij} \ , \ i \in S \ , \ j \in P$ and have two states: 1) its value is one, if node i Is assigned to a relay installed in candidate node j, 2) If its value is zero, other states are checked.

The variables of the installed relays are also $z_j \ , \ z \in P$ which has two conditions: 1) its value is one, if a relay is installed in candidate node j, 2) its value is zero, other states are checked. Finally, it is necessary to introduce the flow variables in the network, which is f_{jl}^k refers to the routed traffic flow in the destination link (j,l) to the sink, i.e. $k \in N$. The special variables include f_{ik}^t Refers to the entire site visitors waft among the relay established in candidate node j and sink k.

Energy and diffusion models based on channels are considered in this approach in routing. The Transmitted signals can arrive from the receiver when two deployed nodes are connected to each other which consists of three-way propagation through

the sensing area, refraction in the sensing area, reflection from nearby scattered data and then returning to the sensing area.

Also, the emission from the sensing area in the GHz frequency range is very small and can be ignored. In general, the lost paths based on the dB unit between the transmitter and the receiver of wireless devices are P_{dB}^{ij} and are calculated as a distance model as D_{ij} derived from equation (1).

$$P_{dB}^{ij}(D_{ij}) = P_{0,dB}^{ij} + 10n_{ij}log_{10}\left(\frac{D_{ij}}{D_{0,ij}}\right) + S \quad (1)$$

According to equation (1), $P_{0,dB}^{ij}$ is the lost paths based on the decibel unit, which is in a reference distance $D_{0,ij}$ and n_{ij} is the coefficient of lost paths, and $S \sim N(0, \sigma_s)$ is a normal variable that leads to the representation of the derivative in dB unit by different components, and the antenna gain is in various directions. In order to calculate Strength consumption in IoT networks, it is assumed that the sensing and processed energy is insignificant due to Conversation; therefore, the whole energy intake is represented by way of the whole transmission charge and the energy received from all of the wi-fi nodes of the network. The energy leads to the loss of some of the radio power of the network, which is displayed as E_{TXelec} and E_{RXelec} to run the circuit For the transmi ter and receiver. Also, $E_{amp}(n_{ij})$ represents the energy for the transmission amplifier and D_{ij} Is the gap between nodes i and j. In general, transfer energy is calculated as equation (2).

$$w[E_{TXelex} + E_{amp}(n_{ij})D_{ij}^{n_{ij}} \quad (2)$$

According to equation (2), wE_{RXelec} is the received energy, where w is the total number of transmitted or received bits. Next, it is necessary to present the improvement part of the 6LoWPAN protocol and the routing structure in the IoT with a Markov Reinforcement Learning (MRL)approach. In general, a multi-objective optimization solution is modeled in equation (3).

$$Min\ y = f(x) = (f_1(x), f_2(x), \dots, f_m(x))$$
$$subject\ to: \{x = (x_1, x_2, \dots, x_n) \in F_x \subset X\} \quad (3)$$

According to equation (3), $x \subset X$ is called the decision vector, X is the optimization space, $f \in Y$ is the target vector, Y is the target space, and the set of F_x is the set of solutions proposed to satisfy the constraints of the problem. The vector $f$is described by $f = (f_1, f_2, \dots f_m\}$ as a wise and required component, and $F_y \subset y$ will be a representation of the region F_x for the mapping $f(.): X \to Y$. A set of solutions to a problem multi-objective consists of all the decision vectors in the corresponding objective vectors that can be promoted in any dimension without degradation in another dimension. These solutions are known as the beam optimal set. Each

element of the beam optimal set of its non-inferior solutions to the optimization problem Multi-objectives are formed. In fact, the problem does not have any unique states and best solutions, but it has an effective set and alternate solutions, which is called the beam optimal set. Every point in this set is felt as an optimal state that cannot be improved at least one of the remaining components. The set of Non-ruled answers lies on a floor called the Pareto Optimal Frontier. In most cases, there may be many different solutions in the beam states and it is necessary to look at the objective function values to decide which values are relevant B and it is valuable, to be thrown away.

✓ A multi-objective optimization algorithm like the Markov Reinforcement Learning (MRL) directly deals with an objective function vector and looks for different multiple solutions to solve the problem to find an optimal and suitable state. In general, the multi-objective algorithms, especially Markov Reinforcement Learning (MRL) follow a series of points to solve the problem which are as follows:

✓ Ignoring a series of general features and considering only one feature that is important.

✓ Combining features with each other and adding them to each other or playing with features and then optimizing the objective function.

✓ Applying a multi-objective algorithm that looks for all non-dominated solutions. Non-dominant solutions are those that combine into a simple state under conditions with various objective functions. An independent non-dominated solution is a solution that has a state of improvement in one objective outcome at one or more deteriorations or degradations of other objectives compared to independent non-dominated solutions in a population.

Several important issues with Markov Reinforcement Learning (MRL)should be investigated and modeled in the 6LoWPAN routing protocol in the IoT environment. The multi-objective function looks for a solution to reduce the desired equations and the main research objectives. The first one is delay. The probability that delay d_p in an independent path k is less than t is estimated as an equation called Erlangen distribution which is in the form of equation (4).

$$p_r(d_p < t) = \frac{\left(\frac{\mu}{\alpha}\right)^{k\beta} t^{k\beta-1} e^{-(\frac{\mu t}{\alpha})\beta}}{(k-1)!} \quad (4)$$

According to equation (4), $\alpha > 0$ is the scale constant and β is the shaping parameter. The next topic is reliability on the route. Path finding reliability can be defined as the number of successful end-to-end transmissions of data for successful end-to-end delivery for hop-to-hop which is called ETX. For a route p, a series of links including $v_1, v_2, \dots, v_n$ with forward delivery rate as fd_{vi} and reverse delivery

rate as rd_{vi} is considered. The reliability metric in routing or ETX is calculated as equation (5).

$$etx_{vi} = \frac{1}{fd_{vi} \times rd_{vi}}$$
$$ETX(p) = etx_{v1} + etx_{v2} + \cdots + etx_{vn} \quad (5)$$

Then, the total reliability of routing in the 6LoWPAN protocol is calculated by maximizing the routing structure in all dimensions of the IoT for transmitting and receiving data by different nodes, which is in the form of equation (6).

$$R_{total} = \left(\frac{\sum_{p \in total} EXT(p)}{\sum_{p \in total} 1}\right) - 1 \quad (6)$$

Energy consumption should also be optimized. The energy consumed by the relay node will be calculated as equation (7).

$$E_r(b, d_{ij}) = \theta_1 b + \gamma b d_{ij}^m$$
$$E_R(b) = \theta_2 b \quad (7)$$

According to equation (7), d_{ij} is the Euclidean Distance among node i and j, θ_1 is the Transmission power coefficient, γ is the amplification coefficient, m represents the path loss that is in the interval $2 \leq m \leq 4$. θ_2 is the received energy coefficient and b represents the bit rate of the traffic in the relay nodes which depends on the bandwidth and delay as well as the Bit Error Rate (BER). It is possible to improve energy consumption-aware routing and increase network lifetime in the IoT network based on the proposed model and using the optimized 6LoWPAN protocol with Markov Reinforcement Learning (MRL).

Simulation and Results

At first, several objects connected to the IoT should be created that are located in a specific environment. The environment is assumed to be two-dimensional and the dimensions of the grid are 1000x1000 square meters. The number of existing nodes or objects is also assumed to be 100, each node has 0.5 Joules of initial energy, so IoT network in its initial state has 50 Joules of energy. The routing threshold for the 6LoWPAN protocol is also considered to be 0.1, which is the standard for this work. 6LoWPAN routing protocol is implemented in IoT. There is a need for Markov Reinforcement Learning (MRL) settings, which table (1) shows the values of its operators.

Table (1), the values MRL operators

Initial population	100

Genes elite number	20
Iteration	300
Crossover	2
Mutation	0.02

The throughput after applying the Markov Reinforcement Learning (MRL) on the structure of the 6LoWPAN routing protocol is shown in Figure (1).

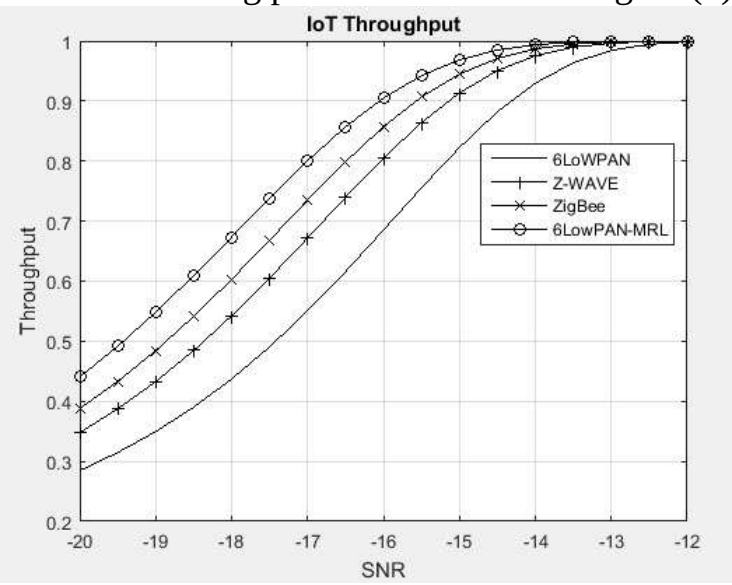

Figure (1), throughput after applying the MRL on the structure of the 6LoWPAN routing protocol

Based on Figure (1), it is clear that the throughput of the proposed approach which is called 6LoWPAN-GA has relative superiority in data throughput compared to other protocols such as Z-WAVE, ZigBee and 6LoWPAN. High throughput also ensures delay reduction in data transmission. The higher the throughput rate, the more suitable the transmission and receiving of data and certainly the lower BER. The amount of data transmit per transmission and receive will be 100,000 bytes by default. The number of initial errors in transmitting and receiving files is 16. Gray coding has been used to determine the BER in IoT which is quantified as follows:

gray_code=[0 1 3 2 4 5 7 6 12 13 15 14 8 9 11 10];

BER output result after applying the Markov Reinforcement Learning (MRL) on the 6LoWPAN routing protocol structure is shown in Figure (2).

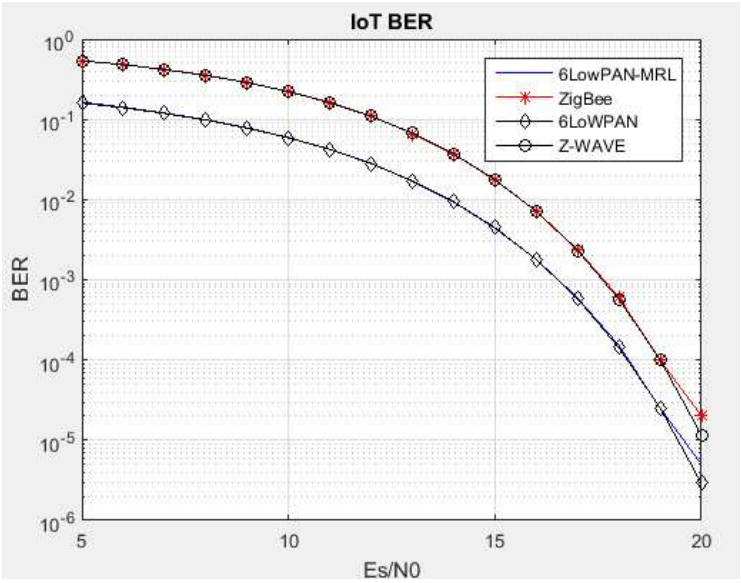

Figure (2), BER output result after applying the MRL on the 6LoWPAN routing protocol structure

Based on Figure (2), it can be said that the use of Markov Reinforcement Learning (MRL) has been able to improve the structure of 6LoWPAN routing protocol for BER very little. The diagram of the proposed method is the blue one and the classical structure diagram of the 6LoWPAN protocol is the black diamond one. Likewise, the BER of the two routing protocols, ZigBee and Z-WAVE, are similar and have an almost equal value. By zooming in on the last area in the BER, we can see the very small amount of optimization with the Markov Reinforcement Learning (MRL) which is shown in Figure (3).

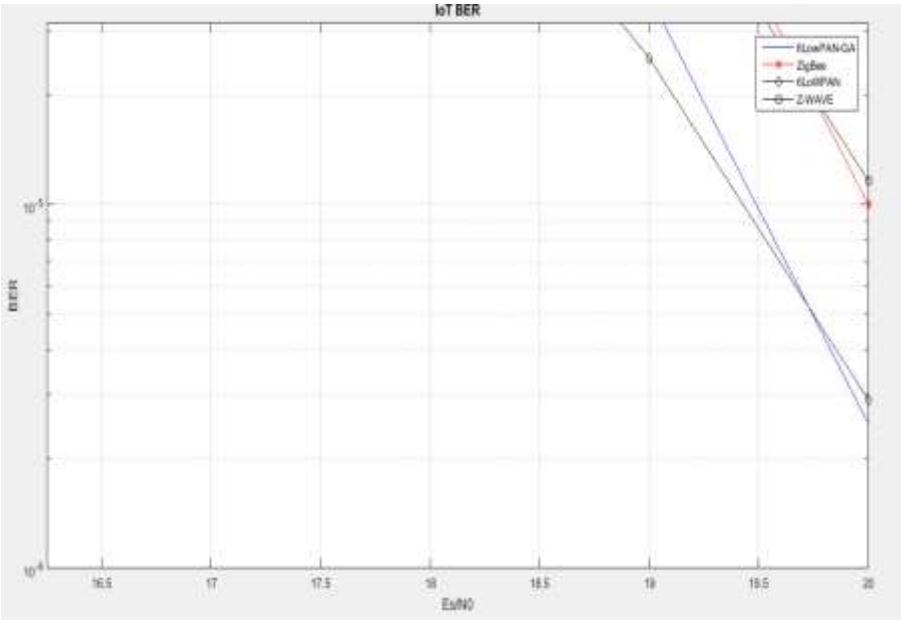

Figure (3), the difference BER between the optimization of the proposed approach and the classical model

At the end, the amount of energy consumption can be seen as shown in figure (4).

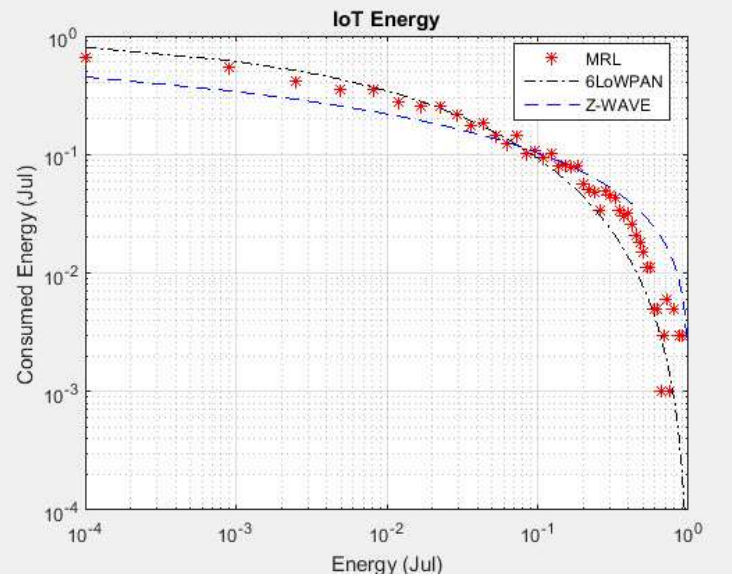

Figure (4), energy consumption after applying proposed approach

Based on the proposed approach, it can be seen that the optimization of the energy consumption of the red colored bars which have a certain energy consumption in different parts in different iterations, and it has been able to reduce the energy consumption by a very small amount compared to the classical model of the 6LoWPAN routing protocol and also optimizing Z-WAVE routing protocol. It can be stated that optimization has been done as much as possible. It is possible to see more diverse outputs from the results of this simulation in different executions due to the feature of Markov Reinforcement Learning (MRL) and random training. In this research, it has been tried to display the most optimal modes.

Conclusion

IoT aims to develop communication between different equipment and users. The main target of IoT is to establish long-distance communication, so that there is the least amount of delay in transmitting and receiving data. Certainly, every network faces a series of challenges with its development and the reason this problem is using in different environments. This case is not excluded from the IoT. Because of this, the challenges of the IoT are getting bigger and bigger with its ever-increasing extending. One of these challenges is routing problem in communication. The

routing problem is one of the most important problems in any network types, because if it is not solved, the network structure will be slow and high energy will be wasted, so users will be dissatisfied and errors will occur in it a lot. By solving the routing challenge, it is possible to have a reliable and appropriate network that has high power in various tasks and based on quality of services criteria, it will have high power in execution and efficiency. In this research, an attempt is made to improve the routing problem in the IoT which uses a standard protocol called 6LoWPAN. This protocol inherently has a suitable routing structure, but it's most important problem is the issue of energy or power along with the delay in transmitting and receiving data and their noise in large distances between two devices connected to the Internet. Therefore, in order to solve this problem, we will try to optimize it, and for this purpose, the Markov Reinforcement Learning (MRL) will be used. Markov Reinforcement Learning (MRL) initial population can be used with various operators such as crossover, mutation and reproduction in a specific iteration round in the qualitative criteria of the IoT routing problem. Among the most important parameters examined in this research, we can point out the delay in transmitting and receiving data, power consumption and energy reduction, data throughput and also the amount of noise in the data, trying to optimize all of these when routing with the 6LoWPAN protocol on the IoT. The obtained results indicated that the proposed approach has been able to be useful to some extent compared to the previous and classic 6LoWPAN self-routing methods.

References

[1] Buyya, Rajkumar, and Dastjerdi, Amir Vahid. (2016). Internet of Things. 1st Edition, Principle and Paradigms, Morgan Kaufmann, 378 pages.
[2] Raghunath, Bane Raman, and Mahadeo, Shivsharan Nitin. (2011). Network Intrusion Detection System (NIDS). First International Conference on Emerging Trends in Engineering and Technology, pp. 1272-1277.
[3] Baumann, R. Heimlicher, S. Strasser, M. and Weibel, A. (2007). A survey on routing metrics. February 2007.
[4] Pan, Meng-Shiuan, and Yang, Shu-Wei. (2017). A lightweight and distributed geographic multicast routing protocol for IoT applications. Computer Networks, 2017, Vol. 12, pp. 95-107.
[5] Baumann, R. Heimlicher, S. Strasser, M. and Weibel, A. (2007). A survey on routing metrics. February 2007.
[6] Pan, Meng-Shiuan, and Yang, Shu-Wei. (2017). A lightweight and distributed geographic multicast routing protocol for IoT applications. Computer Networks, 2017, Vol. 12, pp. 95-107.

[7] Jin, Yichao, Gormus, Sedat, Kulkarni, Parag, and Sooriyabandara, Mahesh. (2016). Content centric routing in IoT networks and its integration in RPL. Computer Communications, Internet of Things\: Research challenges and Solutions, Vol. 89-90, pp. 87-104.
[8] Kharkongor, Carynthia, Chithralekha, T. and Varghese, Reena. (2016). A SDN Controller with Energy Efficient Routing in the Internet of Things (IoT). Procedia Computer Science, Twelfth International Conference on Communication Networks, ICCN 2016, August 19– 21, 2016, Bangalore, India Twelfth International Conference on Data Mining and Warehousing.
[9] Krishna, G. Gautham, Krishna, G. and Bhalaji, N. (2016). Analysis of Routing Protocol for Low-power and Lossy Networks in IoT Real Time Applications. Procedia Computer Science, Fourth International Conference on Recent Trends in Computer Science & Engineering (ICRTCSE 2016), Vol. 87, pp. 270-274.
[10] Badenhop, Christopher W. Graham, Scott R. Ramsey, Benjamin W. Mullins, Barry E. and Mailloux, Logan O. (2017). The Z-Wave routing protocol and its security implications. Computers & Security, 2017, Vol. 68, pp. 112-119.
[11] Almobaideen, Wesam, Krayshan, Rand, Allan, Mamoon, and Saadeh, Maha. (2017). Internet of Things: Geographical Routing based on healthcare centers vicinity for mobile smart tourism destination. Technological Forecasting and Social Change, 2017, In Press, Corrected Proof.
[12] Mohammad Aazam, Sherali Zeadally, Khaled A. Harras. (2018). Offloading in fog computing for IoT: Review, enabling technologies, and research opportunities. Future Generation Computer Systems, Vol. 87, pp. 278-289.
[13] Mauro Tortonesi, Marco Govoni, Alessandro Morelli, Giulio Riberto, Niranjan Suri. (2018). Taming the IoT data deluge: An innovative information-centric service model for fog computing applications. Future Generation Computer Systems, In press, corrected proof, Available online 15 June 2018.
[14] Bidyut Mukherjee, Songjie Wang, Wenyi Lu, Roshan Lal Neupane, Prasad Calyam. (2018). Flexible IoT security middleware for end-to-end cloud–fog communication. Future Generation Computer Systems, Vol. 87, pp. 688-703.
[15] PeiYun Zhang, MengChu Zhou, Giancarlo Fortino. (2018). Security and trust issues in Fog computing: A survey. Future Generation Computer Systems, Volume 88, November 2018, Pages 16-27.
[16] Bahar Farahani, Farshad Firouzi, Victor Chang, Mustafa Badaroglu, Kunal Mankodiya. (2018). Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare. Future Generation Computer Systems, Vol. 78, Part 2, pp. 659-676.
[17] Yan Sun, Fuhong Lin, Nan Zhang. (2018). A security mechanism based on evolutionary game in fog computing. Saudi Journal of Biological Sciences, Vol. 25, Issue 2, pp. 237-241.

[18] Jianbing Ni, Kuan Zhang, Xiaodong Lin. (2017). Securing Fog Computing for Internet of Things Applications: Challenges and Solutions. IEEE Communications Surveys & Tutorials, Vol. 20, Issue 1.
[19] Binara N. B. Ekanayake, Malka N. Halgamuge, Ali Syed. Review: Security and Privacy Issues of Fog Computing for the Internet of Things (IoT). Cognitive Computing for Big Data Systems over IoT, pp. 139-174.
[20] R. Rapuzzi, and M. Repetto. (2018). Building situational awareness for network threats in fog/edge computing: Emerging paradigms beyond the security perimeter model. Future Generation Computer Systems, Vol. 85, pp. 235-249.
[21] Cong Zuo, Jun Shao, Guiyi Wei, Mande Xie, and Min Ji. (2018). CCA-secure ABE with outsourced decryption for fog computing. Future Generation Computer Systems, Vol. 78, Part 2, pp. 730-738.
[22] Rodrigo Roman, Javier Lopez, and Masahiro Mambo. (2018). Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges. Future Generation Computer Systems, Vol. 78, Part 2, pp. 680-698.
[23] Ola Salman, Imad Elhajj, Ali Chehab, and Ayman Kayssi. (2018). IoT survey: An SDN and fog computing perspective. Computer Networks, Vol. 143, pp. 221-246.
[24] Alexandre Viejo, and David Sánchez. (2018). Secure and Privacy-Preserving Orchestration and Delivery of Fog-Enabled IoT Services. Ad Hoc Networks, In press, accepted manuscript, Available online 15 August 2018.