
Scalable Computing: Practice and Experience, ISSN 1895-1767, http://www.scpe.org
© 2020 SCPE. Volume 21, Issue 2, pp. 203–216, DOI 10.12694:/scpe.v21i2.1667

A COMPREHENSIVE SURVEY OF THE ROUTING SCHEMES FOR IOT APPLICATIONS

DIPALI K. SHENDE, YOGESH ANGAL, AND S. S. SONAVANE*

Abstract. Internet of Things (IoT) is with a perception of 'anything', 'anywhere' and provides the interconnection among devices with a remarkable scale and speed. The prevalent intention of IoT is the datatransmission through the internet without the mediation of humans. An efficient routing protocol must be included in the IoT network for the accomplishment of its objectives and securing data transmission. Accordingly, the survey presents various routing protocols for secure data communication in IoT for providing a clear vision as the major issue in the IoT networks is energy consumption. Therefore, there is a need for devising an effective routing scheme to provide superior performance over the other existing schemes in terms of energy consumption. Thus, this review article provides a detailed review of 52 research papers presenting the suggested routing protocols based on the content-based, clustering-based, fuzzy-based, Routing Protocol for Low power and Lossy Networks, tree-based and so on. Also, a detailed analysis and discussion are made by concerning the parameters, simulation tool, and year of publication, network size, evaluation metrics, and utilized protocols. Finally, the research gaps and issues of various conventional routing protocols are presentedfor extending the researchers towards a better contribution of routing protocol for the secure IoT routing.

Key words: Internet of Things, routing protocol, energy consumption, routing protocol for low power, security, lossy networks.

AMS subject classifications. 68M12

1. Introduction. One of the emerging technologies, which enabled communication among things and people and between things, is the IoT [2]. IoT [27] is a new paradigm used for the pervasive communication establishment among the objects connected to the internet by employing distinct approaches [53]. The interconnection of networks connecting numerous devices for exchanging of information and services is called as 'Internet'. Any type of object, device or gadget playing the designated role for the provision of the effective communication between the objects and people is mentioned as the 'Thing' [54]. The evolution of IoT has brought out the device's proactive behavior rather than the reactive behavior of devices. The IoT applications are combined with the machine learning algorithms to makes the feature smarter [66]. The IoT comprises of a wide range of heterogeneous networks of varying processing powers, platforms, and capacities for expanding into the unreachable places [11]. The set of objects/ things enabled by IoT are Pervasive, Identification using unique address and Co-operation between things [55]. IoT has its application in a wide range of areas like smart environments, healthcare [63], environment monitoring [65], city surveillance, transportation,various firms [64], and energy monitoring,etc[3].

Over the past few years, the IoT has gained appealing research interest. The simplified IoT architecture has two layers, namely the perception layer and network layer, each provided with two sublayers. The perception layer has all the methods, which permit the gathering and perceiving of data. The data transmission in a transparent nature by utilizing the appropriate communication standards is handled by the network layer. The critical layer of this IoT architecture is the data management sub-layer, which is also known as amiddleware layer. The application service sub-layer is preferred over the data management sub-layer for the management of the data transmission and provision of user application interface [56]. The vital network systems [2] available for the communication between the distinct objects in IoT are Wireless Sensor Network (WSN), Radio-Frequency Identification (RFID) systems and RFID Sensor Network (RSN). In these networks, the nodes are located in a specified range concerning the application for collecting the necessary information, such as physical change, temperature, and motion [57]. As the node's transmission range is limited the collected information is forwarded to the intermediate nodes and this leads to higher energy consumption by the nodes [58]. Thus, the node's energy efficiency is concerned as avital factor, which influences the performance of distributed IoT networks [2].

*Sinhgad Institute of Technology, India (shendedipalik@gmail.com)

The IoT platform needs a potential networking framework and an appropriate routing scheme for supporting secure data communication and interconnection among devices.

One of the important aspects to be considered for improving the communication efficiency in IoT is the routing scheme adopted for the transmission path selection. The main aim of the routing protocol is to design and maintain interactions between the devices in the dynamic IoT network. The routing protocolis broadly classified into three,namely flat routing, hierarchical routing and geographic position assisted routing, based on the routing principle. In the flat routing, all the nodes are at the same level and they similarly receive their routing information; it is further classified into reactive protocols and proactive protocols. In the hierarchical routing, the network layer is partitioned into different levels based on the specific rules and this routing makes the network scale expansion easier. The geographic position assisted routing utilizes the node location information gathered from the users and it reduces the routing cost. The three primitive concerns [3] influencing the IoT routing are energy consumption, type of IoT middleware and mobility of devices. An effective protocol enhances the transmission efficiency and assures the judicial utilization of the available network resources [26].

The primary intention of this paper is to provide a detailed survey of the various routing protocols for the distinct IoT applications. This review deliberates the existing routing schemes for secure routing in the IoT network. The survey is made by considering the various methodologies utilized, implementation tools and the evaluation metrics, in the existing protocols. Additionally, the number of nodes considered for the simulation is concerned with the performance evaluation of the suggested routing protocols. The existing approaches have been categorized into distinct schemes, and then, thefurther survey is performed for the exploitation of research gap and issues. Thus, it acts as the motivation for the future extension of improved secure IoT routing protocols.

Therest of the paper is organized as follows:Section 2 discusses the existing routing schemes under nine categories. Section 3 discusses the analysis and discussion of the survey. In section 4, the research gaps and the future works are elaborated and the conclusion of this paper is givenin Section 5.

2. Literature Review. This section extensively discusses the review of the different IoT routing protocols for the secure routing in the IoT network. The categorization of distinct IoT protocols for the varying applications is pictorized in figure 2.1. The routing protocols are categorized into nine routing schemes namely, Ad-hoc On-demand Distance Vector (AODV) Routing, Content-based Routing, Dynamic Source Routing (DSR), Tree-based Routing, Software Defined Network (SDN) based Routing, fuzzy-based Routing, RPL, Intelligent method based routing and Clustering-based Routing. These routing schemes give the various algorithms and techniques opted for the secure routing in IoT. The investigation on the several routing schemes provides a clear view of the recommended methods along with itsadvantages and disadvantages.

The distinct methodologies employed in the research papers for the IoT routing is depicted in figure 2.2. From the considered research papers, 6% of the research papers used the Clustering-based routing protocol, 9% of the paper used Tree-based protocol, 6% of the research papers employed the content-based routing, and 8% of the research paper utilized the AODV protocol. The intelligent method based routing is adopted in 9% of the research papers, SDN based routing is practiced in 6% of the research works and the Fuzzy based routing is utilized in 9% of the research works. The DSR routing is adopted in 3% of the research papers and the RPL routing is practiced in the remaining 44% research works.

2.1. Using AODVRouting Protocol. AODV is a reactive protocol, which provides the secure route for the data by concerning the next hop and the routing table values of every node. The research papers employing the AODV routing protocol are discussed below,

Sang-Hyun Park et al. [2] designed an Energy-Efficient Probabilistic Routing (EEPR) algorithm for controlling the routing request packets transmission. EEPR enhanced the network lifetime, while minimizing the Packet Loss Ratio (PLR). The probabilistic control was made by utilizing the Expected Transmission Count (ETX) metric in the AODV protocol context and node's residual energy. The results revealed that the EEPR algorithm provided better network lifetime along with even consumption of node's residual energy.

Hamoud M. Aldosari et al. [28] modeled an independent single security layer for the management of security mechanisms within the network layers. AODV is therouting protocol used, and the security layer was incorporated for cross-validating the sender and the receiver to eradicate the attacks in the network. The simulation results revealed that this security layer assured better performance than the other models in the

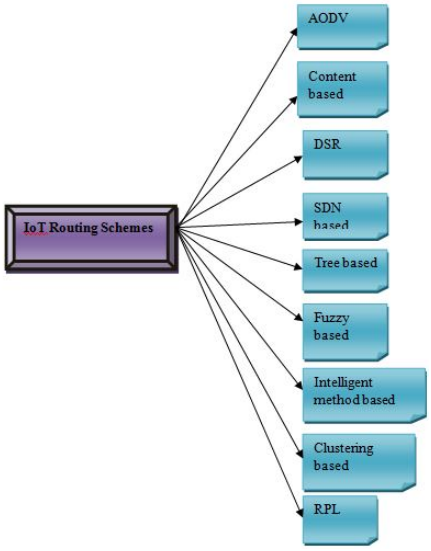

FIG. 2.1. *Categorization of distinct IoT protocols*

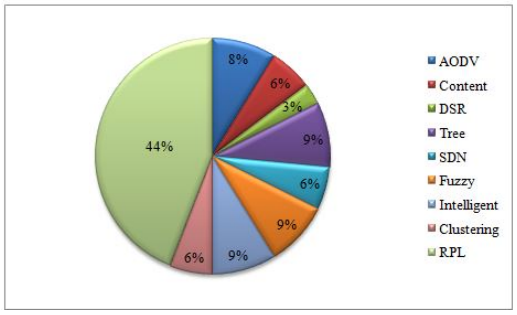

FIG. 2.2. *Distinct Methodologies for Routing in IoT*

aspect of throughput, End to End Delay (EED), Packet Delivery Ratio (PDR), Normalized Routing Load (NRL) and the number of dropped packets.

Greg Kuperman et al. [33] made research on the importance of the routing protocols in the efficient and reliable data communication in the multi-hop wireless network of the IoT environment. The link-based routing leads to the PLR, high maintenance cost, and unreliable data transmission within the network. The unfit nature of the link-based routing protocols for the wireless networks was explored in this research by comparing the performance of AODV and Optimized Link State Routing (OLSR) in terms of mobility, Routing Success Probability (RSP), thedistance between users, PDR and overhead.

2.2. Using Content-based Routing protocol. In the content-based routing protocols, the routing information is differentiated by concerning the content. The distinct research works employing the content-based routing are presented below.

Samia Allaoua Chelloug [3] modeled an Energy-Efficient Content-Based Routing (EECBR) protocol for reducing the energy consumption in the IoT applications. This was a context and content-based routing protocol utilizing a centralized virtual topology constructed for the event routing in a distributed manner from the publishers to the destined subscribers. The results of simulation deliberated that EECBR outperformed the other protocols with respect to thevariance of energy.

Yichao Jin et al. [8] designed the Content-Centric Routing (CCR) protocol for resolving the traffic congestion issue in IoT applications. In this protocol, the routing paths were predicted based on the content; this

improved the data aggregation ratio and thereby, minimized the network traffic. The simulation results justified that the CCR has superior reliability with improved energy conservation and minimum network latency.

2.3. Using DSR protocol. The DSR protocol is an on-demand mode protocol following the principle of the shortest path for the secure path selection. The research paper utilizing the DSR protocol is presented as follows,

Ying Wei [30] modeled an improved DSR protocol (DSR-s), for the efficient channel utilization in IoT networks by concerning the packet rate and shortest-path routing. The secure routing path was selected by considering the data transmission rate and the hop count. The DSR-s enhanced the performance by a complete utilization of channel and avoiding the congestion problem within the network was deliberated through the simulation outcome.

2.4. Using Tree-based Routing protocol. The tree-based routing protocol is devised based on the tree network formed by the integration of the bus network and the star network. The research works adopting the tree-based routing protocols are discussed below,

Tie Qiu et al. [4] designed an Efficient Tree-Based Self-Organizing Protocol (ETSP) concerning energy for the sensor networks of IoTs. In this protocol, all the nodes were classified into two types, namely the network nodes for broadcasting the packet to neighboring nodes and the non-network nodes for gathering the broadcasted packets. In order to improve the network lifetime and consumption of energy balance, the topology was subjected to dynamic modifications. The simulation results revealed that this protocol assures the superior RSP, but theaverage hop, PLR and self-organization time of this protocol didn't increase with the increase in network scaling.

Zhangbing Zhou et al. [9] designed an energy-efficient index tree (EGF-Tree) for minimizing the energy consumption in the IoT devices. This protocol was based on the minimal merging principle in sensor node skewness distribution and grid division. This protocol has aprevalent concentration on the recombination of theregion. The simulation results deliberated that the EGF-Tree outperformed the other original index tree regardingenergy consumption.

S. Lana Fernando and A. Sebastian [15] introduced an effective clustering scheme, called Minimum Spanning Tree Particle Swarm Optimization (MST-PSO). The primitive intention of this scheme wastheextension of network lifetime and minimization of the energy consumption and router dependency. The better performance of this algorithm over the other protocols with respect to energy consumption and network lifetime was illustrated by the simulation results.

G. Li et al. [62] introduced a multicast protocol, called heuristic algorithms for the solution of QoS constrained multicast routing problem, with incomplete information in WSN. Here, link measures were considered as the random variables for information aggregation. The major aim of this method was that it transformed the original probabilistic link descriptors, which reduced the tree selection to a deterministic problem. Then, the Hop Neural Networks (HNN) was applied which ensured the fast convergence to a suboptimal solution.

2.5. Using SDN based Routing protocol. The SDN controller utilizes a centralized routing protocol for collecting the network information.The research works practicing the SDN based routing protocols are discussed below,

Carynthia Kharkongor et al. [11] devised a routing mechanism using the SDN controller for providing secure data transmission among the heterogeneous devices. The primary intention of this mechanism was to minimize the energy consumption of heterogeneous devices by eliminating the approach of selfish nodes. The simulation results revealed that the routing by SDN controller provided better performance than the other protocols, like AODV, Destination Sequence Distance Vector (DSDV) and DSRwith respect to average EED, throughput, and PDR.

Chiara Buratti et al. [25] performed the comparative performance analysis of SDN entitled Software-Defined Wireless Networking (SDWN), ZigBee and IPv6 over Low power Wireless Personal Area Networks (6LoWPAN). The SDWN utilized the centralized network layer protocol, whose routing schemes were described by an external controller, whereas ZigBee and 6LoWPAN utilized the distributed routing protocol. The results demonstrated that the SDWN provided superior performance than the other two protocols in terms of traffic, payload size and network size. Jun Huang et al. [59] introduced two algorithms to construct the multicast routing tree for

multimedia data transmissions. These algorithms leveraged an entropy-based process to combine all weights into a comprehensive metric, and utilized it to search a multicast tree through the shortest path tree and spanning tree algorithms. These algorithms assisted multimedia communications in an IoT environment. Here, collecting and updating the network topology and QoS constraint information were facilitated by the application of SDN technologies in the IoT environment.

2.6. Using Fuzzy based Routing protocol. The fuzzy logic can predict the tradeoffs between the distinct network parameters, the research papers employed with the fuzzy-based routing are presented as follows,

Ning Li et al. [5] devised a Cross-Layer and Reliable Opportunistic Routing Algorithm (CBRT) by the inclusion of fuzzy logic and humoral regulation stimulated topology control with the opportunistic routing algorithm. The relative variance was used as the fuzzy logic system input and the increase in the number of inputs didn't affect the number of fuzzy rules. Here, the relaying priority concerning the utility of reliable nodes was determined by the source node. The CBRT protocol has improved network performance over the Extremely Opportunistic Routing (ExOR)protocol and there was no up-gradation in the computational complexity.

Aljawharah Alnasser And Hongjian Sun [23] designed a fuzzy logic-based trust model for the detection of intruder nodes in the smart grid networks for enhancing the security. By the utilization of this model, the detection rate and routing efficiency can be enhanced for all the regarded destructive behavior. The simulation results demonstrated that the model outperformed the lightweight and dependable trust system model in terms of PDR by up to 90%.

Dong Chen et al. [24] modeled a trust and reputation model for IoT (TRM-IoT) based on the trust establishment scheme for maintaining the cooperation between the network things concerning their behavior. The fuzzy set was incorporated into this scheme for the effective management of the relationship between trust and reputation. This model had eradicated the data packet forwarding failure, achieved a good PDR and minimized energy consumption.

2.7. Using RPL Routing protocol. RPL is a distance-vector tree-based standardized routing protocol designed for the secure routing in most of the IoT applications. The different research works practicing this routing scheme are elaborately discussed as follows,

Maha Bouaziz et al. [6] modeled an Energy-efficient and Mobility aware Routing Protocol (EC-MRPL) based on RPL. This protocol assured better energy conservation and preserved the connectivity between mobile nodes. EC-MRPL protocol concatenated an enhanced mobility detection scheme with the prediction based on the point of attachment and replacement scheme with insight about resource restrictions. The protocol mitigated the mobility issues and provided better performance than the RPL and the Mobility Aware Routing Protocol (MRPL) with respect tosignaling cost, energy consumption, handover delay, and data loss rate.

Mai Banh et al. [13] designed an energy balancing RPL along with the other routing metrics to deal with the link quality diversity. The diverse combination of energy consumption and ETX was concerned as the routing metrics. The method based on Radio Duty Cycle (RDC) was utilized for estimating the consumption of energy. This protocol assured better energy balance, maintaining good PDR and energy efficiency.

Harith Kharrufa et al. [16] modeled an enhanced Dynamic RPL (D-RPL) for distinct applications with dynamic network and dynamic mobility. A dynamic Objective-Function (D-OF) was included for enhancing the end-to-end delay, energy consumption, and PDR. Moreover, D-RPLhad retained the avoidance of loop and low packet overhead. The simulation results revealed the fact that this protocol has higher PDR, minimal EED along with acceptable energy consumption.

Sheeraz A. Alvi et al. [20] devised an enhanced RPL protocol for theInternet of Multimedia Things (IoMT), where the multimedia equipment provided the sensed data. This protocol reduced the energy consumption and carbon footprint emissions with theaddedinclusion of QoS requirements. The simulation outcome deliberated the beneficial gain with respect to the latency and energy efficiency.

Zeeshan Ali Khan et al. [21] designed a trust-based RPL routing (t-RPL) for the IoT devices in distinct applications. The primitive intention concerning the trust of every node was for the prominent IoT network management. The scheme enhanced the network flexibility, average delivery ratio and reduced the number of paths with malicious nodes compared to the other variants, like resilient RPL (r-RPL) and classical RPL (c-RPL).

Nabil Djedjig et al. [22] devised a Metric-based RPL Trustworthiness Scheme (MRTS) for improving the security in RPL by resolving the trust inference issues. The Destination OrientedDirected Acyclic Graph (DODAG) Information Object (DIO) was extended by the inclusion of a trust-based Extended RPL Node Trustworthiness (ERNT) metric and a Trust Objective Function (TOF). The ERNT was computed through the collaboration of nodes by concerning the behavior of nodes, such as energy, honesty, and selfishness. The simulation revealed enhanced performance in terms of security.

Natanael Sousa et al. [27] devised an Energy-Efficient and Path Reliability Aware Objective Function (ERAOF) and an objective function for RPL to be employed in the distinct IoT applications. This ERAOFwas designedbased on the routing metrics, like energy and link quality. The simulation outcome demonstrated that this method improved the energy efficiency, reliability of communication along with maintaining a high PDR.

Emilio Ancillotti et al. [37] presented research work for the exploration of RPL application in the Advanced Metering Infrastructure (AMI) arrangement. All the characteristics were evaluated for discovering the limitations and significance of the RPL protocol. The investigation deliberated that the RPL has good scalability and it suffers from unreliability problems because of the lack of link quality insight.

Mamoun Qasem et al. [38] presented a load-balanced objective function for the RPL to ensure the maximization of node lifetime. This objective function managed the total number of children nodes in a network and eliminated the potential extra overhead. The simulation results demonstrated that this objective function outperformed the other schemes with respect to the PDR, network lifetime and power consumption.

Ming Zhao et al. [39] made an exhaustive study on the RPL protocol and its standardized version Point-To-Point RPL (P2P-RPL) for supporting the Low Power Lossy Network (LLN) applications. The study explored the routing specifications, challenges and performance evaluation of both the protocols. The P2P-RPL protocol outperformed the standard RPL protocol in terms of flexibility, PDR, EED and control overhead.

José V. V. Sobral et al. [40] made the performance analysis of the reactive protocol Lightweight On-Demand Ad hoc Distance vector Routing (LOADng) protocol in two distinct types of traffics, namely P2P and MP2P. The protocol was a lighter version of the AODV protocol depending on the limited IoT resources. This protocol assured superior performance when employed in the MP2P applications rather than the P2P applications for the chosen scenarios. One of the limitations of this protocol is that with the increase in the network size, the performance decreases.

Olfa Gaddour et al. [41] modeled a fuzzy-logic objective function (OF-FL) for the RPL based LLNs. This objective function was a suitable approach as it integrated the four nodes with its link parameters, like EED, hop count, battery level and ETX, by utilizing the fuzzy logic. The simulation results demonstrated the performance enhancement in RPL with respect to the network lifetime, EED and PLR.

Baraq Ghaleb et al. [46] designed an Enhanced-RPL for alleviating the storage limitation issue in the preferred parent of thenode. A Downward Advertisement Object (DAO) was modeled for eliminating underspecification mechanism problem. This Enhanced-RPL provided better performance than RPL by 64 and 30 in theaspect of both control plane overhead and PDR, respectively.

Mai Banh et al. [48] explored the knowledge of RPL under the multiple RPL routing tree instance conditions. This RPL constructed a Directed Acyclic Graph (DAG) representation for the IoT network, there can be many DAG's for the same network but with varying routing metrics, like ETX, hop count and node power. The simulation outcome revealed that the scheme enhanced the performance in terms of PDR and latency by differentiating the network traffic and allowing them into distinct DAG's of the multiple RPL instances.

Ayman El Hajjar et al. [50] devised a Shared the Identifier Secure Link Objective Function (SISLOF) for the RPL assuring that only the nodes, which share an appropriate key, can take part in the RPL routing table. The simulation outcome demonstrated that the scheme enhanced the security within the IoT network, reduced the storage size along with maintaining a small ring size.

Quan Le et al. [60] introduced three multipath methods, Fast Local Repair (FLR), Energy Load Balancing (ELB), and combination of ELB-FLR depending on RPL and integrated them in a modified IPv6 communication stack for IoT. These methods were implemented in the OMNET++ simulator and the experiment results showed that these methods attained better network load balance, packet delivery rate, end-to-end delay, and energy efficiency.

2.8. Using Intelligent method based Routing protocol. The intelligent method based routing protocols are usually incorporated with distinct optimization algorithms for secure routing. The research works utilizing the intelligent method based routing protocols are presented below,

Praveen Kumar Reddy and Rajasekhara Babu [7] devised a protocol by integrating the Optimal Secured Energy-Aware Protocol (OSEAP) and Improved Bacterial Foraging Optimization (IBFO) algorithm. The protocol was mainly employed for improving the energy conservation and security between nodes in the IoT devices. The Fuzzy C-Means (FCM) clustering algorithm was included for the selection of an effective cluster head. The protocol provided better simulation results than the Secure Energy-aware routing protocol (SEAP) with respect to energy, throughput, and delay.

Sofiane Hamrioui and Pascal Lorenz [14] devised a routing algorithm, entitled Efficient IoT Communications based on Ant System (EICAntS), for enhancing the route selection process by the exploitation of ant colony system significances. This routing algorithm reduced the latency and enhanced the network lifetime, throughput and energy conservation.

Chengjie Wu et al. [32] designed an optimal algorithm based on integer programming and a greedy heuristic algorithm for extending the lifetime of Wireless HART (Highway Addressable Remote Transducer) networks. The integer programming was a linear programming relaxation algorithm. The graph routing was incorporated for prolonging the network lifetime. The experimentation was carried out in the physical testbed and the results elucidated that this algorithm enhanced the network lifetime by 60 maintaining the graph routing reliability.

2.9. Using Clustering-based Routing protocol. The clustering based routing protocol is developed by concerning the node with the highest degree as the cluster head. The research papers employed with the clustering based routing protocol are elaborated below,

Li Qing and Li Cong [26] modeled a node position based optimized clustering routing protocol utilizing the minimum distance routing competition scheme. The simulation results of this method deliberated the superior performance over the other routing protocols, such as AODV and DSR,in terms of network load and transmission delay. This method assures a stable cluster size in contrast to the other traditional clustering routing protocols.

Jau-Yang Chang [52] devised a distributed cluster computing energy-efficient routing scheme for minimizing the sensing node'sdata transmission distances by utilizing the concept of cluster structure. For the selection of an appropriate cluster head node, the center of gravity of the sensing nodes and the residual energy were computed. The simulation outcome deliberated that this scheme provided better performance than other methodologies in the aspects of network lifetime and energy conservation.

2.10. Using other Routing protocols. The other routing protocols utilized for the secure routing in the IoT environment are elaborated below,

Kássio Machado et al. [1] devised a routing protocol concerning the energy and link quality entitled Routing by Energy and Link quality (REL) for the applications of IoT. The route selection in REL was carried out based on the residual energy, end-to-end link quality estimator mechanism and hop count. The simulation results deliberated that REL increases the service availability, quality of service and network lifetime. This protocol assured uniform distribution of scarce network resources and minimized the PLR in comparison with the other eminent protocols.

Shahid Raza et al. [10] modeled a protocol entitled Lithe formed by the concatenation of the Constrained Application Protocol (CoAP) and Datagram Transport Layer Security (DTLS) for the resource-constrained IoT devices. The protocol provided authentication and confidentiality during communication.A DTLS header compression method was included with Lithe for minimizing energy consumption. The simulation results revealed that this protocol assures significant improvement in packet size, processing time, network-wide response times and energy consumption.

Shu-Chiung Hu et al. [12] modeled a ZigBee compatible energy-efficient multicast protocol for permitting the node to implement the devised procedure in adistributed manner. The management of neighbors by avoiding the unwanted data transmission was carried out with the support of the designed procedures and backoff mechanism. This protocol enhanced the lifetime of thenetwork, minimized the redundant packet and maintained the reliability of thenetwork.

Omar Said et al. [17] devised the adaptive versions of the Real-time Transport Protocol (RTP) and Real-Time Control Protocol (RTCP), i.e., IoT-RTP and IoT-RTCP, for the IoT applications. The primitive principle employed in these devised versions was the division of large multimedia sessions into simple sessions with the network status insight. The superior performance of these protocols was deliberated by the obtained simulation results by concerning the number of receiver reports, EED, PLR, delay jitter, energy consumption, and throughput.

Rehmat Ullah et al. [18] designed the composite multi-routing metric for the RPL network. These metrics were developed by concerning the queue utilization, minimal hop count, minimum ETX value and residual energy of node. This scheme outperformed the Queue Utilization based RPL (QU-RPL) regarding the average power consumption. The simulation results conveyed that this protocol minimized power consumption and improved the network's lifetime.

Zhikui Chen et al. [19] modeled a Context-Awareness in Sea Computing Routing Protocol (CASCR) for IoT applications concerning the insight on context. The data structure, quantitative algorithm, and workflow of the devised CASCR protocol were also discussed in this research. The improved network lifetime and energy efficiency were illustrated through the obtained simulation outcome.

Pedro Henrique Gomes et al. [29] designed a Time Slotted Channel Hopping (TSCH) mode with a controlled flooding-based routing protocol for participating in the competition of EWSN Dependability. In the network based on TSCH, the time was split into time slots and the channel hopping was utilized for eradicating the fading and interference issues. The protocol employed here increased the PBR and flexibility along with maintaining minimum latency and overhead.

M. Vellanki et al. [31] designed a Node Level Energy Efficient (NLEE) routing protocol for enhancing the energy efficiency in the IoT networks. The protocol acted as the deciding authority for determining the shortest hop count by considering the hop count of node path and residual energy. This scheme determined the secure shortest path between the source and the destination and maintained better energy conservation by the effective utilization of the energy of nodes.

Hicham Lakhlef et al. [34] designed an agent-based efficient broadcast protocol for mobile with few communication channels. The ideology behind this protocol was to split things managed by the agents into groups based on the channel number. This protocol assured effective performance without collision or conflict in the communication channels in terms of the number of broadcast rounds and runs.

Samad Riaz et al. [35] designed an energy harvesting scheme for the routing protocols and made a comparative performance analysis between the two routing protocols AODV and OLSR in an Energy Harvest enabled Device to Device communication network. The simulation results deliberated that the energy harvesting was a feasible process for improving the residual energy of the network; thereby, assuring prolonged network lifetime. The available residual energy improved the goodput of both the considered routing protocols.

Joanna Głowacka et al. [36] presented a cognitive mechanism based on trust for the OLSR to enable the awareness of thesituation in the IoT networks for intrusion detection. The main intention of this protocol was to explore the efficiency and robustness of the devised method through simulation. The results demonstrated that theprotocol was efficient, had improved the security and total trusted traffic in the network.

Badis Djamaa et al. [42] modeled a centralized/distributed resource discovery architecture employing a CoAP for the IoT application. By employing this architecture, the nodes in the network can identify the availability of Resource Directories (RDs) using a proactive RD discovery scheme. The performance analysis deliberated the enhanced performance of this architecture,in terms of resource economy, reliability and time efficiency, over the other traditional architectures.

Nawel Alioua et al. [43] modeled a Uniform Stress Routing Protocol (USR) for exploiting the routing issues in Low power and Lossy Networks (LLNs). This protocol utilized the axiom of uniform stress in the routing for the encouraging adaptation. This USR restricted the upper bound of required memory and it didn't acquire exaggerated control traffic.

Youhua Xia et al. [44] developed a Privacy-Aware Routing Protocol (PALXA) for secure communication in the IoT network. This protocol concatenated the Arrow-d'Aspremont-Gerard-Varet (AGV) mechanism depending on the theory of machine design with the reputation mechanism based on the subject logic for eradicating the internal attacks. This protocol outperformed the other protocols, like PALX and Pruned Adaptive IoT

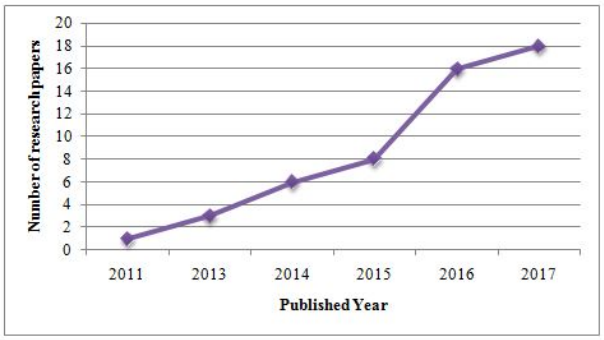

FIG. 3.1. *Analysis based on the year of publication*

Routing (PAIR), in theaspect of node survival percentage, throughput, and successful transmission rate.

Lutando Ngqakaza and Antoine Bagula [45] presented a frugal protocol entitled Least Path Interference Beaconing (LIBP) for the dissemination of sensor readings in IoT. LIBP was a lightweight path selection model, which constructed a routing spanning tree with its root at the sink node through a seasonal beaconing mechanism. This protocol assured enhanced performance with respect to the throughput, scalability, and failure recovery and power consumption over the other protocols, like RPL and Collection Tree Protocol (CTP).

Piergiuseppe Di Marco et al. [47] analyzed the interdependence between the MAC and the Internet Engineering Task Force (IETF) RPL routing protocol in IoT. Then, a mathematical framework was modeled for improving the standard by the cooperative optimization of the MAC and the parameters of therouting protocol. The routing layer parameters considered for the simulation were R-metric and Q-metric, and the node energy consumption was reduced by 20%.

Mohsen Hallaj Asghar and Nasibeh Mohammadzadeh [49] devised a critical routing protocol, entitled Message Queuing Telemetry Transport (MQTT), for building the connection between the physical world and the real world. The primary intention of this research was to improve the Message Queuing (MQ) Service components utilized for connecting the distinct software applications. The main significance of this scheme was easy implementation, light, reduced delay, and low bandwidth system.

Yuxin Liu et al. [51] designed an energy-efficient Fast data collectionfor nodes Far away fromthe sink and Slow data collection for nodes Close to the sink (FFSC) approach, for reducing the EED and configuration complexity of IoT network. This FFSC assured the better network lifetime and energy conservation when compared to the other direct forwarding and single fixed threshold methodologies.

Meng-Shiuan Pan and Shu-Wei Yang [61] introduced a lightweight and distributed geographic multicast routing protocol that had three phases. The first phase selected the intermediate nodes to reach the multicast destinations. The second phase eliminated the loops and trims routes constructed in the previous phase. The third phase ensured, if the selected multicast links could be merged. This technique decreased the transmission links and shortens path lengths in the constructed multicast paths. Also, it reduced the multicast latency.

3. Analysis and discussion. This section presents the analysis and discussion of the parameters considered for the secure routing, tools used and metrics used in the research papers for exploring the distinct routing protocols in the IoT platform.

Analysis based on the year. The analysis of 52 research papers utilized for the secure IoT Routing carried out in the aspect of the published year is elaborated in this subsection. The analysis made by concerning the year of publication is depicted in figure 3.1. Among the 52 papers chosen for the analysis, most of the research papers were published in 2017.

Analysis based on the objective parameters. This subsection deliberates the analysis carried out by considering the objective parameters, like energy, trust, and link quality, based on their different combinations. Figure 3.2 displays the analysis chart based on the considered parameters. Through this analysis, it is clearly shown that nearly 77% f the research papers have used energy as its objective. 12% f the research papers have used trust and 2% f the research papers have utilized the link quality as theobjective parameter. Nearly 7% f the

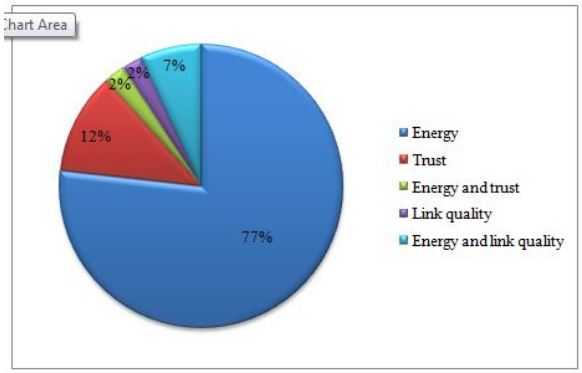

FIG. 3.2. *Analysis based on the objective parameters considered*

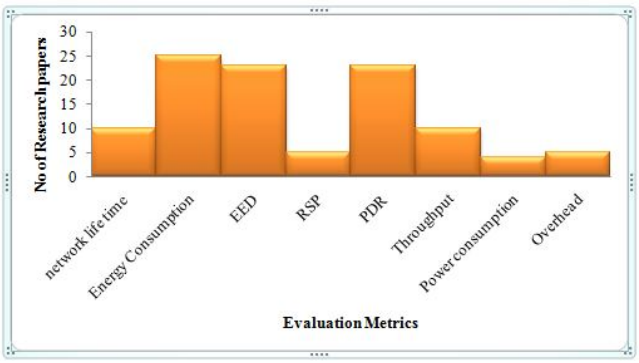

FIG. 3.3. *Analysis based on the evaluation metrics*

research papers are based on the combination of two objectives, i.e., energy and link quality and the remaining 2% f the research papers are based on the parameters, energy, and trust.

Analysis based on the evaluation metrics. This subsection demonstrates the analysis based on the different evaluation metrics used in the research papers. The analysis chart built based on the evaluation metrics, such as network lifetime, energy consumption, EED, RSP, PDR, Throughput, Power Consumption, and overhead are depicted in figure 3.3.

From figure 3.3, it is conveyed that nearly in 50% f the research papers, the simulation is donein terms of energy consumption, EED, and PDR. In the remaining papers, the simulation is carried out concerningthe network lifetime, RSP, throughput, overhead, and power.

Analysis based on Simulation Tool. The analysis carried out regarding the simulation tool used in the research works is presented in this subsection. Asdisplayed in table 3.1, the various simulation tools utilized are C, NS, NS2, NS3, Cooja, Omet ++, Matlab, C++, OPNET modeler, and Castalia. This table clearly elucidates that the Cooja simulator is employed in most of the research papers when compared to the researchs.

Analysis based on the network size. The analysis carried out by concerning the network size in different research works is demonstrated in this subsection. Table 3.2 shows the analysis based on the network size. From the table, it is deliberated that most of the research works have used nearly 50 to 100 nodes as their network size for the simulation.

4. Research gaps and issues. This section deals with the various research gaps and issues in the different IoT Routing protocols.

The simulation outcome illustrates that the routing setup delay of the EEPR algorithm [2] is marginally increased by 0.4ms and thereby, reducing the RSP of routing by 1.8%compared to the AODV protocol. In the routing tree based optimization algorithm, MST-PSO [15], the implementation time is higher when compared

TABLE 3.1
Analysis based on the Simulation Tool

Simulation Tool	*ResearchPapers*
C	[52]
NS	[30]
NS2	[2], [4],[5], [11],[17],[28],[48]
NS3	[24],[35],[39]
Cooja	[6],[13],[16],[18],[20],[22],[27],[37],[38],[41],[45],[46],[47],[48],[50]
Omnet ++	[1],[3],[14],[51]
[Matlab]	[7], [15], [19], [44]
[C++]	[12], [31], [32], [34]
OPNET modeler	[26],[33], [36]
Castalia	[40]

TABLE 3.2
Analysis based on Network Size

Number of nodes	*ResearchPapers*
0-10 nodes	[29], [42]
10-50 nodes	[[2],[11], [13], [16], [22], [23], [36], [45], [47]
50-100 nodes	[4], [7], [15], [18], [19], [20], [25], [27],[28], [30], [33], [35], [38], [40], [41]]
100-500 nodes	[1], [5], [8], [12], [14], [24], [26], [31],[37], [39]
500-1500 nodes	[21], [51]
1500-2500 nodes	[9], [50]

to the traditional networks. This could be resolved by the employment of the end devices instead of the base station for the cluster head selection. In the fuzzy logic-based CBRT [5], the main limitation is that the network lifetime, transmission range and throughput reduces with the increase in the number of nodes. In the content-based CCR protocol [8], the distinct types of content can be regarded by the improvement in the content definition by the incorporation of the emerging processing schemes. The SDWN routing protocol [25] are not preferred for the dynamic scenarios as it is mainly suitable for the static network environment with fixed node location with minimum mobility. The RPL routing protocol [37] is affected by unreliability issues and high PLR because of the lack of link quality insight, which thereby, results in the selection of unreliable links as suboptimal paths. In the link based routing [33], the routing delay is escalated along with the reduction in the RSP. The other drawbacks are the packet loss is severe because of the unreliability of control data, the message delivery is not ensured and the route maintenance and restoration is expensive.

The LOADng Routing Protocol [40] is not chosen as a scalable alternate as the protocol performance decreases with the increase in the network size. Hence, for the conclusive definition, a detailed study is to be made. By the employment of the RPL protocol provided with SISLOF [50] as an objective function, the IoT security is enhanced in the averaged sized universities. However, the storage size increases with the improvement in the network size. The research can be further extended by concerning the generated overhead for the network suitability discovery and the utilization of multiple DODAGs, for the secure routing between roots. In the NLEE algorithm [31], the hop count and the residual energy of nodes are concerned for the shortest path discovery. This algorithm leads to enhanced consumption of energy, which leads to an increase in setup delay for routing and reduces the RSP. The QoS metric can also be considered for performance improvement. The CASCR routing protocol [19] gathers the context knowledge from the neighboring nodes, leading to enhanced energy consumption by the nodes. This algorithm can be made self-optimizing by the provision of satisfactory context insight into the nodes.

Due to the conservativeness of the Chern off approximation in [62], the delay bound always met at the expense of consuming more transmit power. In [60], the FLR had the problem of large end-to-end delay which was caused by the increasing number of packets and the hop to transfer the packet to root. The results are good in [61], but it has limited effect. The data packet sizes did not bring much effect on the result since the transmitting and receiving times on data packets are short, and most energy was consumed while nodes are idle in their active mode. Issues, like an injection of false information into the network, wireless broadcast

of messages, and eavesdropping greatly negotiate the integrity of IoT communication. Moreover, due to the constrained nature and self-organizing attribute of IoT sensor nodes, the utilization of a solution centred on Certification Authorities (CA) via connected servers causes excessive obscurity for secure routing among IoT nodes.

In IoT, excessive energy consumption is a crucial problem, which is ignored by several existing methods. Also, the existing works based on energy and trust aware multicast routing in IoT have some drawbacks, like increased packet delay, link constrained problem, link optimization problem, tree optimization problem, and so on. Moreover, a few of literature works that are based on optimization algorithms are available in multicast routing and those optimization methods are not a very recent one and effective.

5. Conclusion. This paper provides a review of the classification of various routing protocols employed in the distinct IoT applications in the research papers. The primary aim of this article is to review and learn the several IoT routing protocols by analyzing the 52 research papers from IEEE (Institute of Electrical and Electronics Engineers), Google Scholar and Science Direct. The analysis is carried out in terms of year of publication, parameters, evaluation metrics, network size, simulation tool, and the adopted routing protocol. The research gaps and issues are also included in this article for directing the research towards the utilization of an effective routing protocol. Based on the discussion and analysis, it can be summarised that the energy consumption is the vastly concerned objective parameter in most of the research works for the discovery of better protocol. The evaluation metrics regarded in more than 50% of the research papers are energy consumption, EED and PDR.

REFERENCES

[1] K., Machado, D., Rosário, E., Cerqueira, A.A.F., Loureiro, A., Neto and J.N., Souza, *A routing protocol based on energy and link quality for internet of things applications*, sensors, 13 (2013), 1942-1964.

[2] S-H. Park, S., Cho and J-R., Lee, *Energy-efficient probabilistic routing algorithm for internet of things*,Journal of Applied Mathematics (2014).

[3] S.A., Chelloug, *Energy-Efficient Content-Based Routing in Internet of Things* , Journal of Computer and Communications, 3 (2015).

[4] T. Qiu, X. Liu, L. Feng, Y. Zhou and K. Zheng, *An efficient tree-based self-organizing protocol for internet of things*, IEEE Access, 4, (2016), pp.3535-3546,

[5] N. Li, J-F. Martinez-Ortega and V.H. Diaz, LU-*Intelligent Cross-layer and Reliable Opportunistic Routing Algorithm for Internet of Things*, Networking and Internet Architecture, (2017).

[6] M. Bouaziz, A. Rachedi, B. Abdelfettah, *EC-MRPL: An energy-efficient and mobility support routing protocol for Internet of Mobile Things*,In the proceedings of the 14th Annual IEEE Consumer Communications & Networking Conference (*CCNC*), Las Vegas, NV, USA, January (2017).

[7] P.K. Reddy and R. Babu, *An Evolutionary Secure Energy Efficient Routing Protocol in Internet of Things*, International Journal of Intelligent Engineering and Systems, 10 (2017), 337-346.

[8] Y. Jin, S. Gormus, P. Kulkarni and M. Sooriyabandara, *Content centric routing in IoT networks and its integration in RPL*, Computer Communications, vol.89 (2016), 87-104.

[9] Z. Zhou, J. Tang, L-J Zhang, K. Ning and Q. Wang, *EGF-tree: an energy-efficient index tree for facilitating multi-region query aggregation in the internet of things*, Personal and ubiquitous computing, 18 (2014), pp.951-966.

[10] S. Raza, H. Shafagh, K. Hewage, R. Hummen and T. Voigt, *Lithe: Lightweight secure CoAP for the internet of things*, IEEE Sensors Journal, 13 (2013), 3711-3720.

[11] C. Kharkongor, T. Chithralekha and R. Varghese, *A SDN Controller with Energy Efficient Routing in the Internet of Things (IoT)*, Procedia Computer Science, 89 (2016), 218-227.

[12] S-C. Hu, C-H. Tsai, Y-C. Lu, M-S. Pan and Y-C. Tseng, *An energy-efficient multicast protocol for ZigBee-based networks*, In the proceedings of the IEEE international conference on Wireless Communications and Networking Conference (WCNC), Doha, Qatar (2016), pp. 1-6.

[13] M. Banh, N. Nguyen, K-H. Phung, L. Nguyen, N.H. Thanh and K. Steenhaut, *Energy balancing RPL-based routing for Internet of Things*, In the proceedings of the Sixth IEEE International Conference on Communications and Electronics (ICCE), Ha Long, Vietnam (2016), pp.125-130.

[14] S. Hamrioui and P. Lorenz, *Bio-Inspired Routing Algorithm and Efficient Communications within IoT*, IEEE Network, 31 (2017), pp.74-79.

[15] S. L. Fernando and A. Sebastian, *IoT: Smart Homeusing Zigbee Clustering Minimum Spanning Tree and Particle Swarm Optimization (MST-PSO)*, International Journal of Information Technology (IJIT), 3 (2017).

[16] H. Kharrufa, H. Al-Kashoash, Y. Al-Nidawi, M. Q. Mosquera and A.H. Kemp, *Dynamic RPL for multi-hop routing in IoT applications*, In the proceedings of the 13th IEEE Annual Conference on Wireless On-demand Network Systems and Services (WONS), Jackson, WY, USA, pp. (2017), 100-103.

[17] O. Said, Y. Albagory, M. Nofal and F.A. Raddady, *IoT-RTP and IoT-RTCP: Adaptive Protocols for Multimedia Transmission over Internet of Things Environments*, IEEE Access, 5 (2017), pp.16757-16773.
[18] R. Ullah, T.D. Hieu, and B-S. Kim, *A Multi-Metric Routing Protocol for Low-Power and Lossy Networks*, KICS Conference (2017), 305-306.
[19] Z. Chen, H. Wang, Y. Liu, F. Bu and Z. Wei, *A context-aware routing protocol on internet of things based on sea computing model*, Journal of computers, 7 (2012), 96-105.
[20] S. A. Alvi, G.A. Shah, and W. Mahmood , *Energy efficient green routing protocol for internet of multimedia things*, In the proceedings of Tenth IEEE International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), Singapore (2015), 1-6.
[21] Z. A. Khan, J. Ullrich, A. G. Voyiatzis and P. Herrmann, *A Trust-based Resilient Routing Mechanism for the Internet of Things*, In the Proceedings of the 12th ACM International Conference on Availability, Reliability and Security ARES'17 (2017), pp. 1-6.
[22] N. Djedjig, D. Tandjaoui, F. Medjek and I. Romdhani , *New trust metric for the RPL routing protocol,"* ,In the Proceedings of the 8th IEEE International Conference on Information and Communication Systems (ICICS), Irbid, Jordan (2017), pp.328-335.
[23] A. Alnasser and H. Sun, *A Fuzzy Logic Trust Model for Secure Routing in Smart Grid Networks*, IEEE Access, 5 (2017), pp.17896-17903.
[24] D. Chen, G. Chang, D. Sun, J. Li, J. Jia and X. Wang, *TRM-IoT: A trust management model based on fuzzy reputation for internet of things*, Computer Science and Information Systems, 8 (2011), pp.1207-1228.
[25] C. Buratti, A. Stajkic, G. Gardasevic, S. Milardo, M. D. Abrignani, S. Mijovic, G. Morabito and R. Verdone, *Testing protocols for the internet of things on the EuWIn platform*, IEEE Internet of Things Journal 3 (2016), 124-133.
[26] L. Qing and L. Cong, *Efficient Cluster Routing Design under the Environment of Internet of Things Based on Location*, In the Proceedings of the IEEE International Conference on Intelligent Transportation, Big Data & Smart City (ICITBS), Changsha, China (2016), pp. 318-323.
[27] N. Sousa, J.V.V. Sobral, J.J. Rodrigues, R.A.L. Rabêlo and P. Solic, *ERAOF: A new RPL protocol objective function for Internet of Things applications*, In the Proceedings of the 2nd IEEE International Multidisciplinary Conference on Computer and Energy Science (SpliTech), Split, Croatia (2017), pp. 1-5.
[28] H.M. Aldosari, V. Snasel and A. Abraham, *A New Security Layer for Improving the security of internet of things (IoT),*, International Journal of Computer Information Systems and Industrial Management Applications 8 (2016), 275-283.
[29] P. H. Gomes, T. Watteyne, P. Ghosh and B. Krishnamachari. , *Competition: Reliability through Timeslotted Channel Hopping and Flooding-based Routing*, In the Proceedings of the ACM International Conference on Embedded Wireless Systems and Networks (EWSN '16), Graz, Austria (2016), pp.297-298,
[30] Y. Wei, *The Congestion Control Based on Routing Protocol in the Internet of Things*, In the Proceedings of the International Conference on Electronic Information Technology and Intellectualization (ICEITI) (2016).
[31] M. Vellanki, S. P. R. Kandukuri and A. Razaque, *Node Level Energy Efficiency Protocol for Internet of Things*, Journal of Theoretical and Computational Science, 3 (2016).
[32] C. Wu, D. Gunatilaka, A. Saifullah, M. Sha, P.B. Tiwari, C. Lu and Y. Chen, *Maximizing network lifetime of wireless hart networks under graph routing*, In the Proceedings of First IEEE International Conference on Internet-of-Things Design and Implementation (IoTDI), Berlin, Germany (2016), pp. 176-186.
[33] G. Kuperman, S. Moore, B-N. Cheng and A. Narula-Tam, *Characterizing deficiencies of path-based routing for wireless multi-hop networks*, In Proceedings of the IEEE International Conference on Aerospace, USA (2017), 1-9.
[34] H. Lakhlef, Michel Raynal and Julien Bourgeois , *Efficient Broadcast Protocol for the Internet of Things*, In the Proceedings of the 30th IEEE International Conference on Advanced Information Networking and Applications (AINA), Crans-Montana, Switzerland (2016), pp. 998-1005.
[35] S. Riaz, H. K. Qureshi and M. Saleem , *Performance evaluation of routing protocols in energy harvesting D2D network*, In the Proceedings of the IEEE International Conference on Computing, Electronic and Electrical Engineering (ICE Cube), Quetta, Pakistan (2016), pp. 251-255.
[36] J. Głowacka, J. Krygier and M. Amanowicz, *A trust-based situation awareness system for military applications of the internet of things*, In the Proceedings of the 2nd IEEE World Forum on Internet of Things (WF-IoT), Milan, Italy (2015), pp. 490-495.
[37] E. Ancillotti, R. Bruno and M. Conti, *The role of the RPL routing protocol for smart grid communications*, IEEE Communications Magazine, 51 (2013), pp.75-83.
[38] M. Qasem, A. Al-Dubai, I. Romdhani, B. Ghaleb and W. Gharibi , *A new efficient objective function for routing in Internet of Things paradigm*, In the Proceedings of the IEEE Conference on Standards for Communications and Networking (CSCN), Berlin, Germany (2016), pp. 1-6.
[39] M. Zhao, A. Kumar, P. H. J. Chong and R. Lu, *A comprehensive study of RPL and P2P-RPL routing protocols: Implementation, challenges and opportunities*, Peer-to-Peer Networking and Applications, 10 (2017), pp. 1232-1256.
[40] J. V. V Sobral, J.J. Rodrigues, K. Saleem and J. Al-Muhtadi, *Performance evaluation of LOADng routing protocol in IoT P2P and MP2P applications*, In the Proceedings of IEEE International Multidisciplinary Conference on Computer and Energy Science, Split, Croatia (2016), pp. 1-6.
[41] O. Gaddour, A. Koubâa, N. Baccour and M. Abid, *OF-FL: QoS-aware fuzzy logic objective function for the RPL routing protocol*, In the Proceedings of 12th IEEE International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt), Hammamet, Tunisia (2014), 365-372.
[42] B. Djamaa, A. Yachir and M. Richardson, *Hybrid CoAP-based resource discovery for the Internet of Things*, Journal of Ambient Intelligence and Humanized Computing, 8 (2017), pp.357–372.

[43] N.Alioua, K. Nakamura, M. Kamio, N. Koshizuka and K. Sakamura, *USR: Uniform stress routing protocol for constrained networks*, In Proceedings of 5th IEEE Global Conference on Consumer Electronics, Kyoto, Japan (2016), 1-3.
[44] Y. Xia, H. Lin and L. Xu,, *An AGV Mechanism Based Secure Routing Protocol for Internet of Things*, In the Proceedings of IEEE Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM), Liverpool, UK (2015), pp. 662-666.
[45] L. Ngqakaza and A. Bagula, *Least Path Interference Beaconing Protocol (LIBP): A Frugal Routing Protocol for the Internet-of-Things*, In the Proceedings of Springer International Conference on Wired/Wireless Internet Communications, 8458 (2014), 148-161.
[46] B. Ghaleb, A. Al-Dubai, E. Ekonomou and I. Wadhaj, *TA new enhanced RPL based routing for Internet of Things*, In the Proceedings of IEEE International Conference on Communications Workshops (ICC Workshops), Paris, France (2017), pp. 595-600.
[47] P. D. Marco, G. Athanasiou, P-V. Mekikis and C. Fischione, *MAC-aware routing metrics for the internet of things*, Computer Communications, vol.74 (2016), pp.77-86.
[48] M. Banh, H. Mac, N. Nguyen, K-H. Phung, N. H. Thanh and K. Steenhaut , *Performance evaluation of multiple RPL routing tree instances for Internet of Things applications*, In the Proceedings of IEEE International Conference on Advanced Technologies for Communications (ATC), Ho Chi Minh City, Vietnam (2015), pp. 206-211.
[49] M. H. Asghar and N. Mohammadzadeh, *Design and simulation of energy efficiency in node based on MQTT protocol in Internet of Things,*,In the Proceedings of IEEE International Conference on Green Computing and Internet of Things (ICGCIoT), Noida, India (2015), 1413-1417.
[50] A. E. Hajjar, G. Roussos, and M. Paterson. , *Secure routing in IoT networks with SISLOF*,In the Proceedings of the IEEE International Conference on Global Internet of Things Summit (GIoTS), Geneva, Switzerland (2017), 1-6.
[51] Y. Liu, A. Liu, Y. Hu, Z. Li, Y-J. Choi, H. Sekiya and J. Li, *FFSC: an energy efficiency communications approach for delay minimizing in internet of things*, IEEE Access, vol.4 (2016), pp.3775-3793.
[52] J-Y. Chang, *A Distributed Cluster Computing Energy-Efficient Routing Scheme for Internet of Things Systems*, Wireless Personal Communications, 82 (2015), pp.757-776.
[53] A. Zanella, N. Bui, A. Castellani, L. Vangelista and M. Zorzi, *Internet of things for smart cities," IEEE Internet of Things journal*, Internet of things for smart cities," IEEE Internet of Things journal, 1 (2014), pp.22–32.
[54] C. Lu, *Overview of Security and Privacy Issues in the Internet of Things*, Internet of Things (IoT): A vision, Architectural Elements, and Future Directions, 2014.
[55] O. Vermesan and P. Friess, *Internet of Things-From Research and Innovation to Market Deployment*, River Publishers, Aalborg (2014), vol.29.
[56] X. Jia, Q. Feng, T. Fan and Q. Lei, *RFID Technology and Its Applications in Internet of Things (IoT)*, In the proceedings of 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet), Yichang (2012), pp.1282-1285.
[57] G. Lee, *A cluster-based energy-efficient routing protocol without location information for sensor networks*, International Journal of Information Processing Systems, 1 (2005), pp. 49–54.
[58] X. Li, *Achieving load awareness in position-based wireless adhoc routing*, KITCS/FTRA Journal of Convergence, 3 (2012).
[59] J. Huang, Q. Duan, Y. Zhao, Z. Zheng, and W. Wang, *Multicast Routing for Multimedia Communications in the Internet of Things*, IEEE Internet of Things Journal, 4 (2017), pp. 215 – 224.
[60] Q. Le, T. Ngo-Quynh, and T. Magedanz, *RPL-based Multipath Routing Protocols for Internet of Things on Wireless Sensor Networks*, International Conference on Advanced Technologies for Communications (ATC), Hanoi, Vietnam, October 2014.
[61] M-S. Pan, and S-W. Yang, *A Lightweight and Distributed Geographic Multicast Routing Protocol for IoT Applications*, Computer Networks, 112 (2017), 95-107.
[62] G. Li, D. G. Zhang, K. Zheng, X. C. Ming, Z. H. Pan, and K. W. Jiang, *A Kind of New Multicast Routing Algorithm for Application of Internet of Things*, Journal of Applied Research and Technology, 11 (2013), 578-585.
[63] N. M. Ha and N. T. An, *Impact of work-family conflict on job performance of nurses working for hospitals in Ho Chi Minh city*, Science Journal 4 (2015).
[64] N. M. Ha, *The effect of growth on firm survival in vietnam*, April 2016.
[65] R. R. Andrade, I.F.F. Tinôco, F.C. Baêta, M. Barbari, L. Conti, P.R. Cecon, M.G.L. Cândido, I.T.A. Martins, C.G.S.T. Junior, *Evaluation of the surface temperature of laying hens in different thermal environments during the initial stage of age based on thermographic images*, Agronomy Research 15 (2017), 629-638.
[66] V.H. Arul. V.G. Sivakumar, R. Marimuthu, and B. Chakraborty, *An Approach for Speech Enhancement Using Deep Convolutional Neural Network*, Multimedia Research (MR), 2 (2019), 37-44.

Edited by: P. Vijaya
Received: Dec 9, 2019
Accepted: Apr 1, 2020