Engineering Science and Technology, an International Journal 22 (2019) 1–21

HOSTED BY

ELSEVIER

Contents lists available at ScienceDirect

Engineering Science and Technology, an International Journal

journal homepage: www.elsevier.com/locate/jestch

Review

Network optimizations in the Internet of Things: A review

N.N. Srinidhi *, S.M. Dilip Kumar, K.R. Venugopal

Dept. of CSE, University Visvesvaraya College of Engineering, Bangalore, India

ARTICLE INFO

Article history:
Received 27 February 2018
Revised 7 September 2018
Accepted 9 September 2018
Available online 22 September 2018

Keywords:
Congestion
Energy conservation
Network optimization
QoS
Reliability

ABSTRACT

The Internet was initially used to transfer data packets between users and data sources with a specific IP address. Due to advancements, the Internet is being used to share data among different small, resource constrained devices connected in billions to constitute the Internet of Things (IoT). A large amount of data from these devices imposes overhead on the IoT network. Hence, it is required to provide solutions for various network related problems in IoT including routing, energy conservation, congestion, heterogeneity, scalability, reliability, quality of service (QoS) and security to optimally make use of the available network. In this paper, a comprehensive survey on the network optimization in IoT is presented. The paper draws an attention towards the background of IoT and its distinction with other technologies, discussion on network optimization in IoT and algorithms classification. Finally, state-of-the-art-techniques for IoT in particular to network optimization are discussed based on the recent works and the review is concluded with open issues and challenges for network optimization in IoT. This paper not only reviews, compares and consolidates the recent related works, but also admires the author's findings, solutions and discusses its usefulness towards network optimization in IoT. The uniqueness of this paper lies in the review of network optimization issues and challenges in IoT.

Contents

* Corresponding author.
E-mail address: srinidhinagesh@gmail.com (N.N. Srinidhi).
Peer review under responsibility of Karabuk University.

https://doi.org/10.1016/j.jestch.2018.09.003
2215-0986/

1. Introduction

With the advent of wireless communication, the Internet, and ubiquitous computing have given rise to a new paradigm called Internet of Things (IoT), by that a large number of physical devices in billions are being connected to the Internet. These devices are connected to the Internet through different technologies such as cellular technologies like 2G/3G/4G/LTE/5G, Machine to Machine (M2M) technologies with various radio options like Bluetooth (IEEE 802.15.1), Wi-Fi (IEEE 802.11), ZigBee (IEEE 802.15.4). These devices depend on various critical characteristics to provide reliable communication for IoT environment that encompasses efficient network optimization, architecture, protocols, security aspects and various services associated to discrete application types. Current trend of IoT is contemplated as Internet of future and contains billions of heterogeneously interconnected things or devices that leverage the contemporaneous technology by extending borders of the world with virtual and physical things [1]. IoT during its dawning stage has created a major influence on the present emerging market with its usage and application prediction for the upcoming years. It is evaluated to have around 50 billion things and devices connected to the Internet by 2020 that boosts possibility for more and more research and development work in the field of IoT [2]. IoT empowers physical devices or sensors to quantify, execute defined task, utilize cloud for storage and to activate the alert system automatically during emergency situation with the assistance of Internet as its underlying technology. Consequently, IoT transforms existing traditional devices to function smarter by making use various gleaning technologies such as pervasive computing, artificial intelligence, embedded devices, different communication standards and technologies, various application services and different Internet standards. IoT is meant to provide smarter services by the interconnection of various things and objects. To provide smarter services in applications like smart home application, SAP future retail service, smart city, intelligent traffic monitoring system and many more requires data to be collected from different places, area and from different types of heterogeneous devices. These data are sent to the end user or to a subscriber on demand or on the proactive basis. However, to send these data to the subscriber infuses different types of network challenges. Since most of the devices used in IoT are limited memory and energy constrained, data should be routed efficiently, either in both push or in pull strategy [3]. To deliver the data efficiently, congestion and scalability in the network should be accounted otherwise sent data packets does not reach the destination efficiently, since data has to pass through many hops, new devices can add into network anytime in an unpredicted manner. In IoT, traffic should be managed in decentralized passion for the application like traffic management system, where individual nodes exchange information about their traffic, helps to schedule the traffic based on data rate from each source, to avoid traffic congestion [4]. Many IoT applications are meant for monitoring critical cases for example in fire detection, smoke detection, building health monitoring, intrusion detection applications, where a delay or jitter in the network is not ideal. In these applications, network should be robust enough to deliver the data to the intended system within a defined time and routing of these data should be done in an optimized manner. Because in multi-hop routing strategy to conserve energy most of the nodes are sleeping and node closer to the sink node should have to wake up to collect and deliver data to sink node without any delay and without compromising energy efficiency [5]. Network lifetime can be enhanced by selecting the single optimum path among available multiple paths by selecting a linear programming model [6]. Apart from the above factors, application like patient health monitoring and other medical applications requires reliability in data delivery and security while transferring data in the IoT network. These above mentioned factors challenges the usage and management of spectrum resources effectively for IoT application since, IoT is considered as part of future Internet which covers all kind of domains and industrial applications. If these network challenges are not addressed then shortfall of spectrum resources will be the bottleneck for further IoT development. In this contrast, high priority should be given for optimizing network resource utilization by billions of new wireless devices being connected to Internet in future to facilitate efficient spectrum utilization. Hence Efficient network optimization techniques are required for the management and delivery of IoT data in the network which have been discussed in this review paper.

1.1. Motivation

To the best of our knowledge, this is the first survey work which delineates about network optimization in IoT. Network optimization in IoT is gaining more attention due to the generation of massive amount of traffic in forthcoming years by IoT devices which are projected to be connected to global network in billions. Hence, IoT network needs to be optimized to reduce the effect of this traffic on other services which are using cellular and other network types. If the network challenges are not addressed then shortfall of spectrum resources will be an obstruction for further IoT development. This objective motivated us to propound this survey work considering various parameters with state of the art solutions to provide the readers with a description of the different work published in vision of network optimization in IoT which helps to appertain these techniques in solving network problems in future and what still remains to be addressed is stipulated through issues and challenges. This helps researchers to delve more to address solution in forthcoming days.

1.2. Contributions of this survey

Diverse survey works related to different aspects of the IoT are published so far. For example, Li et al. [1] cover various IoT

definitions, fundamental technologies, architecture and different IoT applications. In [2], the authors address the main communication enabling technologies, wired and wireless and actuator networks and upgraded communication protocols. The authors in [7], provides IoT in cloud centric vision, technologies and application domains which drive future IoT research are discussed. Granjal et al. [8], examines existing protocols and methods to secure IoT communications along with research challenges for further research in this area. Summary of present IETF standard and various IoT challenges have been discussed in [9]. Authors in [10], provide properties, survey, features, underlying technologies for the integration of IoT and Cloud. Fuqaha et al. [11], provides overview of protocols, technologies, horizontal integration of IoT services and use cases which details about how different protocols suitable for delivering appropriate IoT services.

The outline of the overall contributions of this paper relative to the recent literature in this field can be summarized as:

- This is the first paper of its kind which provides the need for network optimization in IoT.
- Provides different algorithm types with an objective of network optimization in IoT.
- Provides an overview and the summary of recent research work along with novel approaches published in the area of different network parameters like network routing, energy conservation, congestion control, heterogeneity, network scalability, reliability, quality of service and network security.
- Detailed strengths and limitations of recent papers published in the related network parameters.
- Compared to other survey papers in the field of IoT, this survey provides a comprehensive review of most of the network parameters issues and challenges which is unique from most of the existing survey work.

1.3. Paper organization

The rest of this paper is organized as follows. In Section II, we provide the background of IoT. In this section, we briefly describe the history and evolution of the IoT. Then we explain the difference between M2M, IoT, and Internet of Everything (IoE). In Section III, we conduct our main discussion based on network optimization in IoT where we present the need for network optimization in IoT, followed by different algorithms types for network optimization in IoT. Section IV, discusses state-of-the-art solutions for IoT network optimization. Finally, Section V discusses open issues and challenges and the conclusion is presented in Section VI. For additional clarity, the organization of the paper is depicted in Fig. 1.

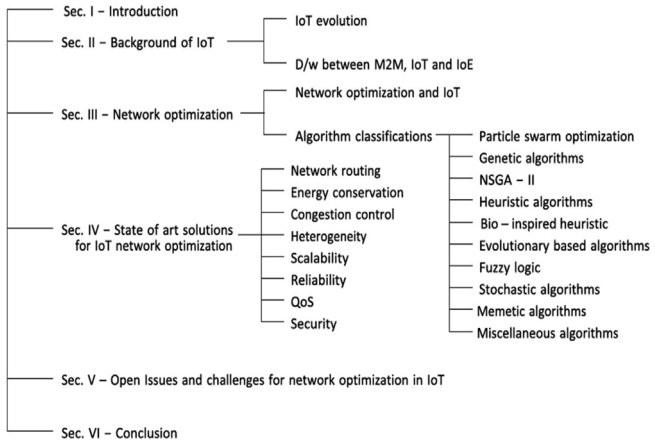

Fig. 1. Organization of the paper.

2. Background of IoT

2.1. IoT evolution

The term, IoT was first coined in 1999 by Kevin Ashton [12] to attract the management of P&G, where he was working on supply chain optimization using RFID. He wanted to make use of the Internet along with RFID to track and count the goods used in the corporate supply chain without the intervention of the humans. To achieve this, he convinced the P&G management and presented a new concept called IoT. After all, the IoT didn't get its attention worldwide until 2010.

But, IoT regained its popularity in mid-2010. Google started storing a large amount of data about users Wi-Fi networks that leads to the debate about Google's new strategy towards indexing physical world along with the Internet. In addition to this, China announced Internet of Things as their priority topic in the Five Year Plan in the same year. In 2011, Gartner research and the advisory firm have included IoT as an emerging technology in their hype cycle for emerging technology trends. In 2012, LeWeb which is a Europe's biggest Internet conference has conducted a conference on Internet of Things, in addition to these tech driven magazines like Forbes, Wired, etc. started using IoT as their top trending topic to describe the phenomenon [13]. International Data Corporation (IDC), market research, analysis and advisory firm have estimated that there would be a 8.9 trillion USD market for IoT by 2020 and Cisco predicts that there would be around 50 billion things connected to the Internet by 2020.

The Fig. 2 of Google search trends shows interest over time based entirely on the number of searches for the terms M2M, IoT and IoE.

2.2. Difference between M2M, IoT, and IoE

M2M has been in the application from the past decade and it is well known in the telecommunication field. Initially, M2M communication was used for linking one device to another, but now it's being used to transfer the data between multiple devices of the same kind, without the intervention of human whilst devices are communicating to each other through wired or wireless communication. M2M is a collection of distributed system of sensors and telemetry data. Some of the applications of M2M communication are telemetry, Wi-Fi thermostats, sensor network in oil-refinery, digital billboards, home and office security system, traffic control system, robotics and so on.

IoT is evolved form of M2M or M2M is a subset of IoT, i.e. if you consider M2M in a larger prospect you get IoT [13]. IoT connects different M2M technology together, leverages M2M to enable

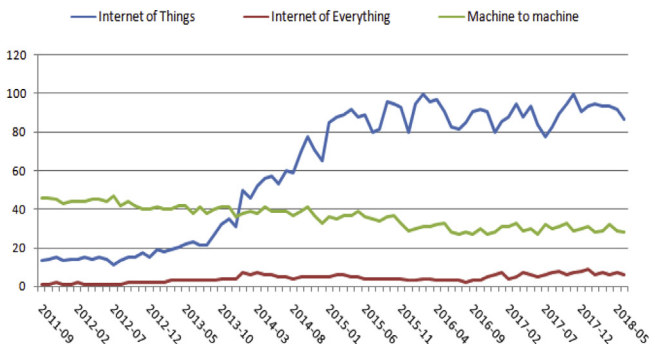

Fig. 2. Google search trends since 2011 for terms M2M, IoT and IoE.

new applications and incorporates an existing legacy M2M system to solve various business problems. Specific applications for IoT includes smart meters, connected cars, smart cities, wearable, smart supply chains in the field of retail and so on.

IoE concept emerged as advancement in the field of IoT. It is a superset of IoT and was introduced by Cisco to initiate a new marketing domain. IoE comprises of the wider concepts in the field of connectivity with respect to the modern connectivity use cases. In IoE, people, process, data, and things are networked to turn information into actions for creating higher opportunity and better experience. The Table 1 provides the differences among M2M, IoT and IoE.

Apart from above three major technologies, there are a few more types like Industrial Internet of Things (IIoT), also called as Industrial Internet that collectively brings advanced analytics, smart machines, and people together. IIoT consists of interconnected devices, in which system collects, transfers, analyzes, monitors and delivers valuable insights. These insights are helpful in providing smarter, quicker business decisions for industrial companies [14]. The IoT transport capability, that makes interconnected computing system and application to interact with the physical world, thus makes Web of Things (WoT) propounds networked things to coalesce into the web, making these resources available on the web through a standard procedure [15]. Thus IIoT, WoT and Internet itself constitutes a subset of IoE, is shown in the Fig. 3.

IoT devices can add into the network at any time in large number in an unpredicted manner, hence the network must be robust enough to provide scalability and additionally several individual applications are hosted on the network at any time which imposes additional traffic overhead to the network. IoT devices induct peak traffic into the network indefinitely when IoT devices put data into the network whenever changes are observed and if that traffic is from large setup, in such cases network should not be congested and efficient data routing must happen to reduce delay and to conserve the nodes energy.

Hence, IoT network optimization offers a lot of benefits for improving traffic management, operating efficiency, energy conservation, reduction in latency, higher throughput and faster rate in scaling up or deploying IoT services and devices in the network.

3. Network optimization

Generally, network optimization is defined as the technology used to improve the performance of the network for any

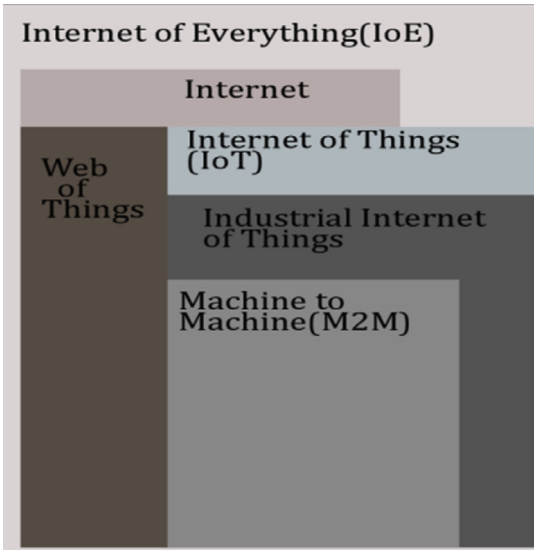

Fig. 3. Internet of Everything and its subsets.

environment. This plays an important role in IT, as day by day large amount of data from various kinds of devices and applications are being populated into the network. Network optimization offers various benefits such as faster data rate, data recovery, eliminating redundant data and to increase the response time of application and network. In this section, we will discuss need for network optimization in IoT, different algorithm types proposed by the authors to provide network optimization in IoT and these algorithm types are then compared with different network parameters in order to clarify different network parameter supported by these algorithm types.

3.1. Network optimization and IoT

Network optimization in IoT is gaining increased attention due to the expectation of a high increase in traffic from IoT things and objects, as billions of IoT devices are expected to connect global network in the coming years. Due to this, it is obvious for researchers and operators to provide efficient solution to optimize IoT networks to reduce the IoT generated traffic impacting other services in the network and to utilize network resource efficiently. The traffic generated by IoT devices is different from the cellular network

Table 1
Differences among M2M, IoT and IoE.

Attributes	M2M	IoT	IoE
Size	M2M is a subset of IoT.	IoT is a superset of M2M.	IoE is superset of IoT.
Key Components	M2M encompasses three keycomponents such as 1. Devices, which generates or receives the data from other devices. 2. Communication, for efficient transfer of data among devices and gateway. 3. Application, to provide services to the end user requirements.	IoT consists of four key components such as 1. Sensing or devices, for generating or receiving the data from other devices. 2. Communication, for transferring of data to Internet or between devices. 3. Storage services, for efficient storage of data into database or to cloud. 4. Application, to provide intended service.	IoE consists of four key components such as 1. People, considered as end nodes connected to the Internet for sharing information and activities. 2. Things, are devices that generate the data or receives data from other devices. 3. Data, used for analyzing and processing of useful information to take intelligent decision and control mechanism. 4. Processes, allows people, data and things to work together to deliver value.
Communication Type	Point-to-Point communication exists between the devices.	IP network exists between devices, by integrating various communication protocols.	IoE is a network connection of people, process, data and things.
Internet Requirement	M2M communication may exist without the Internet.	Devices in IoT require an active Internet in most of the cases.	Devices and their application require active Internet.
Integration Challenge	Integration challenge is limited, since M2M uses corresponding standard.	Integration challenge is higher due to use of different communication standard in its solution.	Higher degree of integration challenge compared to IoT.

due to heterogeneity in applications and device types. Additionally, IoT traffic needs to be regulated to monitor the working of IoT devices and its services. IoT application generates fewer amount of data, however integration of devices to the application generates the higher volume of traffic because of control plane messages. Hence this non-application traffic puts a significant additional burden on the network. So to overcome from this burden, efficient mechanism is required to address and optimize the control plane messaging from IoT devices.

3.2. Algorithms classification

Generally the optimization problem is made up of input factors, outputs, constraints and different objective function. Network optimization problem in IoT comprises many parts which will be combined using different combination and methods which address a particular type of network problem. In common, we found out two important methods for optimization (1) Applying known optimization framework for addressing the problem. (2) Scheming novel work based on a heuristic method for the problem. Above mentioned approaches are not mutually exclusive, however they are combined sometimes when the problem is too complex or known approaches provide inappropriate results. Heuristic approach consists of (a) Algorithm which provides a faster approximation solution for more complex problem example, convex optimization (b) Greedy approach which provides optimal solution by making assumptions. Both these approaches provide optimal solution for complex problems and both achieve performance near to optimal. Hence there won't be a single algorithm which provides optimal solution to network optimization problem in IoT. Different algorithm types proposed by the authors to address different network optimization problems are explained in the below subsection.

3.2.1. Algorithms based on particle swarm optimization (PSO)

PSO is a computational method which optimizes given problem by improving candidate solution iteratively in regard to the given quality. PSO originated based on the swarm behavior of animals, birds etc and their schooling nature. Due to the unique structure exhibited by these provides the necessary information that the intelligence does not concentrate on individuals, rather it is distributed among many individuals of the group. PSO attained extensive popularity in recent years and many research articles related to different optimization methods have been published using this technique. For example in [16], the authors have proposed immune orthogonal learning PSO algorithm which provides fast route recovery from the path failure due to mobility of the sink node and also provides alternative path for efficient path repair by using orthogonal learning strategy. The result proofs that the algorithm reduces communication overhead and increases lifetime of the network. The authors in [17], used PSO to evaluate different level of transmission power required for each node without making disconnected areas in the sensor cluster. Final results show that by using PSO, the method has saved more sensors energy in comparison with common nodes deployment with sole transmission power. Energy efficiency is a critical issue in cluster based capillary networks, where selecting process of cluster heads (CHs) has a notable effect on network performance. So authors in [18], proposed novel QPSO scheme for CHs selection, which improves energy efficiency and protracts the lifetime of the network when compared to evolutionary algorithms. Wen et al. [19] proposed Improved PSO (IPSO) to improve the precision measurement via weight factors calculated through experimental simulations. Results obtained from the experiment shows that this algorithm combines the factors of weight, reliability of information source fusion, redundancy in information and hierarchical structure consolidation in undetermined fusion scenarios. This fusion data will be extracted optimally by eliminating noise, interference, and this method reduces energy consumption by the sensors. The authors in [20], multi-objective particle swarm optimization algorithm to increase the broker profit while decreasing response time for a request and reduced energy consumption of the cloud broker exists between cloud computing and IoT.

3.2.2. Genetic algorithms (GA)

GA attempts to assign the suitable value to the competing solution for the problem by using natural evolution activity and also by using the survival of the fittest principle. GA can be used for both constrained and unconstrained optimized problems. Amol et al. in [21], propounds optimal routing algorithm k-means clustering algorithm and GA. Using, k-means clustering algorithm best cluster head and cluster formation can be achieved, and by using GA, optimal path can be selected. GA is relying on the energy value of the cluster head and length of the path, hence resultant path obtained by GA will have more reliability, higher speed and lifetime. In [22], the authors have proposed GA based clustering optimization method for constrained networks of accounting IETF CoRE standards for data transmission and CoRE interfaces, by this battery level at the nodes, transmission energy and node processing capability can be improved. With the aid of CoRE Interfaces energy consumption can be reduced, since it uses less control messages during the communication process. The authors in [23], have proposed heuristic-based genetic algorithm for the selection of efficient nodes to perform sensor data annotation in the network. This method uses multi-objective criteria to select the best candidates and chooses sensors having maximum storage space and energy level.

3.2.3. Non dominated sorting genetic algorithm II (NSGA-II)

NSGA-II is a non-dominated sorting-based multi-objective evolutionary algorithm for reducing computational complexity, non-elitism approach and need for specifying a sharing parameter [24]. Many researchers have chosen NSGA II to solve various multi-objective optimization formulation corresponds to various problems. For saving energy different routing algorithms have been proposed which is based on mono-objective optimization but author in [25], have proposed multi-objective evolutionary optimization algorithm, which decreases energy consumption of the network by optimizing distribution of sensors. Song et al. [26], combined quantum particle swarm optimization (QPSO) along with NSGA-II to boost operational efficiency of the industrial application. This combined algorithm achieves better tradeoff between QoS provisioning and energy consumption, and also improves network performance. To solve Energy optimization as a multi-objective problem instead of mono-objective evaluation authors in [27], proposed MOR4WSN based on NSGA-II choosing preeminent sensor distribution to maximize the network lifetime and also method to optimize results.

3.2.4. Heuristic algorithms

Heuristic algorithm is used to find solution out of many possibilities and provides relatively near solution to a complex problem in an easier and faster manner. There are many literatures available for network optimization based on heuristic algorithms. For example in [28], authors have proposed RPL routing protocol as a Robust Shortest Path Tree (RSPT), which improves resilience in network routing by considering uncertainty present in the link quality and to address cost of individual arc which is determined by feasible values instead of single value problem, they have extended a Scenario-Based heuristic (SBA) algorithm. Authors in [29], proposed Computational Intelligence (CI) to conserve energy and device resources by switching CI tasks from IoT devices to cloud

and also to save energy optimized heuristic based on dominance sort is used. So overall the performance of whole IoT devices has improved using this method. Kaustubh et al. [30], proposed a heuristic and opportunistic link selection algorithm (HOLA), which minimizes overall energy consumption and also balances the energy across the entire network. HOLA attains this by shifting device data to smart devices calibrated to factory settings. Authors in [31], used LTE technology to provide coverage for various IoT devices and to make this technology resource restraint and to facilitate efficient communication they have proposed LTE Random Access Channel (RACH) mechanism. This mechanism enables devices to access channels and to reduce transfer power, the authors have proposed Delayed Power Ramping Algorithm (DPRA), which is a heuristic based approach.

3.2.5. Bio-inspired heuristic algorithms

Approach Bio-inspired algorithms are the algorithms used widely for optimization and computational intelligence. Recently many research works for achieving network optimization in IoT have been published to address many issues. For example author in [32], proposed 6LoWPAN Local Repair Using Bio Inspired Artificial Bee Colony (ABC) routing protocol to reduce overhead on the network while discovering route to the destination, since LOAD, MLOAD and AODV for 6LoWPAN mesh network overloads the network while discovering the network using route request (RREQ) broadcast message. Authors in [33], developed a novel multi-objective optimization algorithm based on chaotic ant swarm (CAS). CAS utilize chaotic behavior of individual ant and self-organizing characteristics of ant colony to define rules for neighbor selection and to converge the algorithm to reduce Error Ratio, generational distance and Spacing. Maciej et al. [34], have proposed hive oversight for network intrusion early warning using DIAMoND methods to reduce delay in network intrusion detection. This method makes use of the bee's collaborative method of decision making and local information extraction algorithm to find and use critical resources around their surroundings to amplify intrusion detection in the network. Authors in [35], proposed method to enhance communication between Internet of macro/nano things, since their intermediate nodes refuses to communicate with other nodes to conserve energy and to reduce overhead on the network. To achieve this, authors proposed bio-inspired distributed model which uses voronoi based cooperation strategy and trust strategy to enhance the cooperation between nano-nodes.

3.2.6. Evolutionary algorithms (EA)

EA uses population based approach to *meta*-heuristic algorithm. EA provides approximate solution to almost all kind of problems since it doesn't make assumption while formulating the problem. Some of the works based on the EA are [36], where authors have proposed Optimal Secured Energy Aware Protocol (OSEAP) and Improved Bacterial Foraging Optimization (IBFO) algorithm for secure data transmission and to save energy while selecting the cluster head for data transfer between source and the destination. This method outperforms in terms of throughput, energy and delay when compared to previous methods. Failure of the host devices due to lack of energy is addressed by the authors in [37]. They have proposed method, which balances the energy consumption of the outdoor deployed devices by using evolutionary game based approach for service selection. This method restricts the congregation of devices through global interaction for service selection in case of concurrent applications. Authors in [38], proposed method to address heterogeneity in IoT networks. They have compared GA and Harmony Search (HS) in all aspect to show that traditional clustering methods will not result in efficient clustering. Biying et al. [39], proposed evolutionary algorithm to classify data for data identification and to manage huge amount of data from IoT. This algorithm does sensitivity analysis to search optimal solution and helps neural network to restructure to overcome from tedious input issue.

3.2.7. Algorithms based on fuzzy logic

Fuzzy logic is used to determine partial truth whose true value lies between complexly true and false. It uses linguistic variables lead by membership functions and interference rules to achieve truth values. To detect anomaly in the IoT traffic authors in [40], proposed fuzzy logic interference applied to stationary Poisson or self-similar traffic of the IoT network. They suggested modified sliding window and modified stochastic approximation for detecting anomaly in the traffic. Authors in [41], proposed variable categorized clustering algorithm (VCCA) using fuzzy logic is applied to IoT local network to select CH based which has got the highest network capability. To achieve this VCCA uses fuzzy inference system (FIS), which makes use of rule based variable to select CH of lower complexity and to have higher scalability among cluster variables. According to the authors this algorithm outperforms in terms of network performance for the term energy conservation, latency, throughput and network lifetime. Authors in [42], propounds fuzzy logic method applied to vehicular ad hoc network to build a smart car IoT application. The authors argued that the proposed algorithm optimizes network performance of the V2V network in double digits in terms of handoff between access point and the devices. Yijun et al. [43], a proposed encryption scheme based on fuzzy identity to secure data during transmission. The proposed scheme is very secure without any random oracles in the full model, provides better security and short public parameters. The authors suggested that this scheme is very suitable for secure communication of data in IoT environment. Automating the energy consumption in case of industrial equipment's which are energy intensive is very challenging. So to achieve these, authors in [44] proposed fuzzy comprehensive evaluation method, which monitors and helps in optimizing the energy required by energy intensive equipment's in industrial application and also evaluates the operational level.

3.2.8. Stochastic algorithms

Stochastic Algorithms used for optimization objective use random variables which comprise of random constraints or functions to resolve stochastic problems. Some of the literature based on these methods is explained here. For example in [45], authors proposed model to provide reliable IoT data transmission in wireless communication medium. To achieve this, they proposed improved distributed stochastic routing algorithm which reduces delay in delivering the IoT data while increasing packet delivery ratio by adopting Markov chain concepts to the proposed model. To establish connection among BS and IoT devices to support massive IoT network in cellular network authors in [46], proposed Random Access Channel (RACH) model. This model makes use of novel traffic aware spatio-temporal model to analyze proposed RACH model effect in the massive IoT network. This model helps to integrate and analyze different types of IoT device at different time to achieve optimized network objective. Due to higher complexity in IoT network, conventional countermeasure to provide security cannot be applied directly. To achieve this authors in [47], proposed stochastic game net (SGN) model to provide security in IoT. The model improved confidentiality, integrity and availability when compared to traditional methods. To provide reliable and effective wireless access for data generated by IoT in cellular networks Mohammad et al. [48], proposed geometry and queuing theory based model. This model resolves scalability problem foist by IoT on cellular network and provides an efficient way for data transmission.

3.2.9. Memetic algorithms (MA)

MA uses evolutionary or population based strategy to improve problem search. Some of the MA to provide network optimization in IoT has been discussed in this subsection. For example in [49], where authors have proposed novel authentication based smart transportation framework. The framework is used to decrease real time traffic, waiting time, processing time in toll plaza problem in transportation by making use of MA. In this framework MA plays an important role in computing optimized single point decision by making use of data collected from object, agent and some third party services. Authors in [50], proposed MA coupled with local and global optimization to resolve inverse problem. This algorithm helps to provide better solution for structural health monitoring application, which requires higher computation, delay resistant and faster response system.

3.2.10. Miscellaneous algorithms

In addition to the above explained common type of algorithm, there are many others which will be discussed in this section which helps to optimize IoT network. For example, in [51] authors proposed Bayesian approach to the network model for identifying intrusion in IoT network. This model has great capability of dynamically identifying prime nodes to provide better security feature, which can be achieved using historical data. Authors in [52], proposed artificial intelligence based algorithm to form clusters, to choose the optimized route and to perform multipath routing for achieving better QoS. In [53], Markov chain model to enhance the lifetime of the IoT devices using energy harvesting. This model defines set of policies to manage battery level and increases sensing the rate of IoT devices. Game theory based routing protocol has been proposed in [54], which is responsible for selecting best hop for forwarding data packets in opportunistic IoT. This protocol outperforms in terms of hop count reduction, message drop and overhead. Authors in [55], used lexicographic optimization approach to provide energy efficiency and QoS while selecting the IoT services.

3.3. Pivotal network parameters supported by different algorithm types

In this subsection, we have compared above mentioned algorithm types with different network parameters to provide different network parameters supported by these algorithm types.

1. Load balancing: Load balancing in the network during routing of data plays an important role to maximize network lifetime. Multipath metric consideration while routing will help in providing reliable communication of data with less chance of nodes failure in the network.
2. Network Lifetime Maximization: The load balancing parameter and failure management of the nodes along with energy efficient routing help in network lifetime maximization. Since battery life or nodes energy is limited, the mechanism should restrict or balance various network parameters to maximize network lifetime. Most of the algorithm helps in network lifetime maximization.
3. Failure Management: Link failure happens due to the failure of nodes in the network, results in signal degradation and reduces network lifetime. Hence mechanism should minimize link failures to provide reliable communication.
4. Quality of the link: This parameter provides QoS to the communication. In case of multipath, path is checked and data are forwarded in efficient path to reduce payload retransmissions and predicted delays. This parameter partly helps in network lifetime maximization as it reduces packet retransmission.
5. Energy Efficiency: Algorithms should provide an energy saving mechanism to minimize energy consumption of the nodes, which is a crucial part in IoT. Energy conservation can be considered in various aspects like routing, duty cycle reduction, congestion control and many others. Most of the algorithm provides energy conservation strategy to maximize network lifetime.
6. Heterogeneity: IoT is the combination of a various type of devices and services, the data from these devices are of heterogeneous form. Heterogeneity is considered in according to many factors such as various manufacturers, different hardware and software types, different protocols, etc. Algorithm should support heterogeneous environments and help with interoperability among different protocols. But most of the algorithm doesn't support heterogeneity.

Table 2 summarizes various vital network parameters supported by different algorithm types.

4. State-of-the-art solutions for IoT network optimization

There are lots of network optimization schemes which have been proposed for the optimal operation of IoT networks. The Fig. 4 provides a classification of relevant works done against each aspect of network optimization technique related to IoT. Outcome of this emerging technology is the generation of unprecedented amount of data. Data storage, routing, packet retransmission, mobility of nodes, interoperability among heterogeneous nodes and to provide security for data becomes critical issues. Today, Internet consumes 5% of generated energy, with these predictions it is necessary for the IoT devices to be energy efficient to provide reliable communication. To address these challenge this section provides elaborative survey briefing objectives, strength and limitations of various works related to different parameters like network routing, energy conservation, congestion, heterogeneity, scalability, reliability, QoS, and security has been discussed in the below with an objective of network optimization.

4.1. Network routing

Routing is a process of selecting the path for sending the data across a single or multiple networks. These data are generated by M2M or machine to object communication. These generated data should be routed to take the shortest path or the optimal path to reach the destination. The process of maintaining information about routes to deliver data is categorized into three types as

1. Reactive: This protocol creates routes only when source wants to send the data to destination, hence it is also known as on-demand routing protocol.
2. Proactive: This protocol maintains a routing table, which is periodically updated based on fresh destination list, hence it is known as table driven protocol.
3. Hybrid: This protocol is a combination of both reactive and proactive routing protocols.

Different methods are used to deliver data from source to destination, for example in [56], the authors have proposed a lightweight forwarding algorithm to facilitate multicast in LLN for service discovery in smart objects. This protocol uses local flooding technique for duty cycled devices using LLN with RPL, helps memory constrained devices to use multicast. This method avoids forward loops with the aid of bloom filters to identify duplicate packets and to prevent loops.

Table 2
Pivotal parameters supported by different algorithm types. Where Y = Yes, N = No and P = Partly.

Ref.	Load balancing	Network lifetime maximization	Failure management	Energy efficient	Link Quality	Heterogeneity
Hu et al. [16]	Y	Y	Y	Y	Y	N
Da silva et al. [17]	N	Y	N	Y	Y	N
Song et al. [18]	N	Y	N	Y	N	N
Sung et al. [19]	N	N	N	N	Y	N
Kumrai et al. [20]	N	Y	N	Y	N	N
Dhumane et al. [21]	Y	P	Y	N	Y	N
Martins et al. [22]	N	Y	Y	N	Y	N
Imran et al. [23]	N	Y	N	Y	Y	N
Kalyanmoy et al. [24]	N	N	N	N	N	N
Rodriguez et al. [25]	N	Y	N	Y	N	N
Liumeng et al. [26]	P	N	N	Y	Y	N
Rodriguez et al. [27]	N	Y	N	Y	N	N
Carvalho et al. [28]	Y	Y	N	Y	Y	N
Verma et al. [29]	N	Y	N	Y	N	N
Dhondge et al. [30]	Y	Y	Y	Y	P	Y
Shailendra et al. [31]	N	P	N	Y	N	N
Ismail et al. [32]	Y	P	N	Y	P	N
Huang et al. [33]	N	N	P	N	Y	N
Korczynski et al. [34]	P	N	N	N	N	N
Raz et al. [35]	Y	N	N	N	P	N
Praveen et al. [36]	P	Y	N	Y	Y	N
Jun et al. [37]	P	Y	N	Y	N	N
Hamza et al. [38]	N	Y	N	Y	N	N
Zhang et al. [39]	N	N	N	N	N	N
Sergey et al. [40]	N	P	N	N	P	N
Kwon et al. [41]	N	Y	N	Y	P	N
Choi et al. [42]	P	N	P	N	N	N
Mao et al. [43]	N	N	N	N	N	N
Li et al. [44]	N	N	N	Y	N	N
Ali et al. [45]	P	N	Y	N	Y	N
Jiang et al. [46]	Y	N	Y	N	P	N
Kaur et al. [47]	N	P	N	N	N	N
Gharbieh et al. [48]	P	N	N	N	P	N
Kuppusamy et al. [49]	N	N	N	N	N	N
Kus et al. [50]	N	N	N	N	N	N

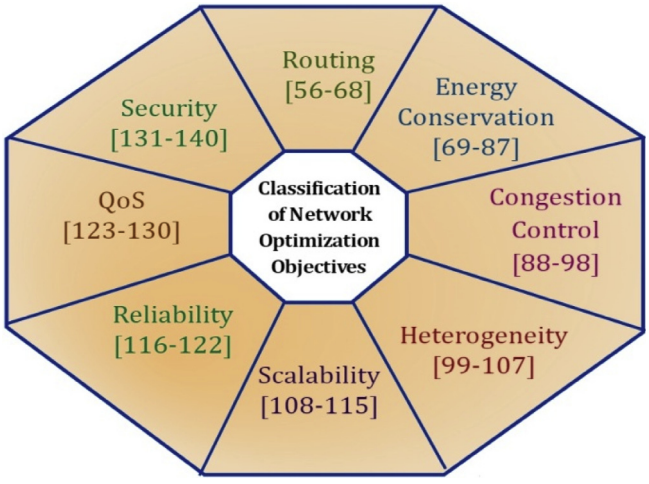

Fig. 4. Network Optimization Objectives Classification in IoT.

The authors in [57], proposed content centric routing (CCR), where content determines the routing. This method routes correlated data to achieve a high rate of data aggregation for reducing network traffic. Due to this method, network latency reduction and redundant data elimination can be achieved. Finally, this method is responsible for optimizing energy consumption, reducing network latency and to provide higher reliability to the network. Recent IoT applications are required to provide reliable mobile data collection from RPL/6LowPAN protocols with lesser latency, packet loss, and overhead. So to provide this requirement authors in [58], have proposed proactive hand-off mechanism with RPL, which has backward compatibility and productivity. This method showed an effective reduction in packet loss, delay and improved packet delivery rate (PDR) in the mobile scenario.

Tian at al. [59] proposed improved ad-hoc on demand multi-path distance vector (AOMDV) for IoT, which dynamically selects a stable internet path by regularly updating table related to the internet connection. This protocol requires additional two routing packets, but lowers end-to-end delay, packet loss, and discovery frequency. Table 3 summarizes other routing methods used to optimize IoT network.

4.2. Energy conservation

In order to prolong network lifetime, different energy saving methods and sleeping technique plays an important role in IoT applications. Below are the some of the communication standards which accounts for achieving this objective.

1. IEEE 802.11ah: Is a wireless networking protocol intended to conserve the energy than standard IEEE 802.11 [69]. IEEE 802.11ah has twice the communication range than that of standard IEEE 802.11 due to use of 900 MHz license free channel [70]. In order to save the energy IEEE 802.11ah has two power saving stations namely TIM stations and non-TIM stations. Buffered traffic information from the access point (AP) is periodically received by TIM stations, whereas Target Wake Time (TWT) mechanism is being used by non-TIM stations to reduce signaling overhead. TWT is a function which allows AP to define the specific time or set of time to access the medium by individual stations. Thus TWT reduce the energy consumption of the network and IEEE 802.11ah uses small signals instead of acknowledgement in order to conserve energy.

Table 3
Summarization of various network routing protocols.

Ref.	Optimization Objectives	Strength	Simulation Tool Used	Routing Used	Limitations
T. Qiu et al. [60]	Load balancing; minimize delay, packet loss & energy consumption.	Reduces energy consumption by avoiding frequent selection of low energy nodes as forwarding node. Balance of energy is ensured in the entire network	NS2	Proactive	Energy consumption is not validated on large scale network setup. Due to increase in transmission rate, loss rate also increases, due to network congestion.
N. Gozuacik et al. [61]	Load balancing; congestion control.	Generates a better load balanced network. Lower parent load density. Higher parent diversity. Minimized end-to-end delay. Reduced collision rate of the packet.	Cooja running on Contiki OS.	Proactive	RPL control messages like DIO and DAO number increases when there are more nodes with similar ETX values.
Y. Wei et al. [62]	Minimize transmission delay; increase transmission success rate.	This algorithm is meant for harsh environment, which many available architectures and protocols do not support. Under different packet size, DRTM maintains an adequate success packet transmission rate even during node failure.	Designed with C++ language	Reactive	Due to different moving speed of the node, success packet transmission rate decreases.
C. H. Barriquello et al. [63]	Increase scalability, routing performance in low link density.	Supports large-scale IPv6 enabled WSN for diverse applications in an urban IoT. GeoRank is an adaptive approach for scenarios with changing link densities.	Simulation based on Open Street Map (OSM) data set.	Reactive	Adds a constraint that mobile nodes must be one hop away from a static node.
K. Q. Abdelfadeel et al. [64]	Reduce memory footprint.	Both push and poll modes succeeded in discovering all nodes. Any number of devices can be added by announcing the services they provide.	Cooja running on Contiki OS	Reactive	Whenever TM technique is used for multicast, it fails in discovering nodes even for a small network topology. Performance of TM technique is subtle to the network size hence the discovery capability reduces whenever network size expands.
T. Qui et al. [65]	Minimize energy consumption; increase the network lifetime.	This method constructs a reliable tree-based network swiftly in larger network. Saves energy by deleting farthest nodes whose energy drops below a certain level. Balances self-organizing time, packet number and success rate of packet even during failure.	NS2	Proactive	To find connected nodes, a response is required whenever a data packet is sent. This responding process causes a delay while forming the tree. Congestion occurs when multiple broadcasts are done simultaneously.
L. Ngqakaza et al. [66]	Minimize energy consumption; increase scalability, throughput & recovery from failure.	Consumes less power compared to CTP and RPL. The method achieves a good trans- mission rate higher than 99%.	Cooja running on Contiki OS	Reactive	Average path lengths (hops) are higher in LIBP when compared to CTP and RPL.
S. A. Chelloug et al. [67]	Minimize energy consumption.	Increases lifetime of the IoT sensors. Builds a virtual topology to organize sensors instead of selecting the leader, which reduces communication cost.	Omnet++	Reactive	Method is best suited only for dynamic topology, not for static type.
S. Misra et al. [68]	Increase energy efficiency & fault tolerance.	Decreases overhead rate. PDR does not vary much when the percentage of mobility increases.	NS2	Reactive	Scaling of this method is not verified in larger networks.

2. ZigBee: This is a wireless protocol defined by layer 3 and above of IEEE 802.15.4. There are two types of nodes in the ZigBee network FFD which acts as coordinator and also as common node and other one is reduced function devices (RFD) which acts as only common node. Authors in [71], proposed synchronized sleeping technique (SST) to facilitate sleep mode to all the nodes of ZigBee network, including fully functional devices (FFD). In many applications routing is required for very limited amount of time. So SST allows FFDs to enter into sleep state during idle periods of network thus conserves the energy of devices. Additionally there are many methods which allow nodes to enter into sleep mode when there is no event to conserve energy.
3. Bluetooth Low Energy (BLE): BLE is also known as Bluetooth smart, which works in operating system of almost all mobile phones, desktops and laptops. BLE requires ten times less power than that of standard Bluetooth because BLE uses master/slave architecture wherein master defines the wake time of the slave so that slave can enter into sleep after it has sent all the information to the master. Thus this advantage makes BLE ideal for IoT applications since this can work even in coin sized battery cell.
4. Low Power Wide Area Network (LoRaWAN): LoRaWAN is targeted for battery operating devices thus making it ideal for IoT applications. This supports bi-directional communication, mobility, localization and security required by IoT application and more importantly it provides energy efficient protocol [72]. LoRaWAN supports large number of devices thus meeting scalability challenge and also facilitates energy harvesting technique which is required by IoT applications.

With all above mentioned communication standard BLE, ZigBee and IEEE 802.11ah are largely used in most of the IoT applications and LoRaWAN is an upcoming standard for IoT communication.

The nodes in the IoT should be energy efficient and the mechanism used in the algorithm should optimize the energy requirement for the devices [73]. Thriveni et al. [74] provided a method to improve the network lifetime and throughput by continuously monitoring the energy level of the nodes through flooding. Wang et al. [75] scrutinize the method to send IPv6 packets in BLE capable sensor networks through IPv6 stack implementation that does the header compression and decompression quickly so that energy conservation and transmission efficiency of the network is met effectively. In [76], the authors have proposed a mechanism wherein hardware and cloud platform exchanges information about the energy and sensors switch to sleep mode based on the battery value, the coefficient of variance (CoV) where sensor senses only when changes has been observed and conflict factor. Also here cloud predicts the maximum amount of incoming data in the next interval to that the resource to be allocated in prior to reducing the delay. In [77] authors propounds a framework called Self-Organized Things (SoT) that optimizes the energy requirement by IoT devices through energy efficient self scheduling algorithm that makes unwanted devices to enter into sleep mode and if possible covers the required area with the limited number of devices. This method is tested for different traffic loads and this method has guaranteed the better durability of about 150% and 220% increase in overall network lifetime showing that energy is conserved through this framework. The Quality of Information (QoI) in the multitasking environment is proposed in [78], where the energy management framework is used for controlling the duty cycle for sensors to achieve QoI and decision related to energy management are made dynamically during runtime to maximize the QoI level by preserving energy. Table 4 provides various energy optimizing solutions for IoT.

4.3. Congestion control

Energy According to the technical experts there could be around 25 billion Internet connected devices by 2020, as a result of the huge number of internet connected devices there could be a potential rise in the network congestion, hence efficient congestion control mechanism is required to address this issue. In [88], the authors propose a CoCoA mechanism to remove the CoAP restrictions on message rate and to provide flexible congestion control mechanism with secure protocol guarantee. CoCoA consists of three key elements such as adaptive retransmission timeout (RTO), calculates the packets required for retransmission, which has lost due to network congestion, variable backoff factor (VBF) which controls the retransmission rate by providing fast retransmission for good connection with small round-trip time (RTT) and slower retransmission rate for bad connection with large round-trip time (RTT) and RTO aging which monitors the RTO values, if these values are not updated for longer period then those values are removed from the system. To provide an efficient method to reduce channel congestion resulted from mass data transmission, the authors in [89] have discussed channel congestion from a different point of view and then, proposed a multiple layer solution which points at each layer comprising spectrum sharing, data processing architecture, data dimension reduction and data abandon protocol. Data dimension is reduced by context awareness and granular computing, the cognitive protocol is used to drop certain unnecessary data to reduce the congestion in the network channel. An enhancement to the IEEE 802.15.4 MAC protocol is presented in [90] to address the congestion problem happened as a result of the significant increase in sensor nodes to monitor the variety of vehicular applications in IoT enabled Intra-Vehicular Communication. This new enhancement strategy outperforms than the traditional protocol by setting parameters like backoff exponent (BE) and the number of backoff stages (NB) only when new data needs to be sent and it sets these values based on the history of saved BE and saved NB to reduce the congestion. To alleviate congestion problem in the network author in [91], proposes a data offloading mechanism based on the game model to reduce the congestion in IoT and also to increase QoS for cellular networks. Table 5 provides additional method to control congestion in IoT network.

4.4. Heterogeneity

Congestion in IoT is the result of combination of a various type of devices and services, the data from these devices are in heterogeneous form. So to handle these data in the network, an optimized mechanism is required, which is discussed in this section. Sterle et al. [99] have proposed heterogeneous OAM (H-OAM) framework for failure detection and control, and to monitor and measure the performance of heterogeneous network automatically. IoT system consists of heterogeneous connectivity, it is necessary to monitor, analyze and troubleshoot the network connectivity. Hence this framework provides a mechanism to address these issues by inspecting the data obtained from different layers of the communication stack. In [100], the authors have proposed sensor SAX method based on symbolic aggregate approximation (SAX) algorithm, which uses abstraction framework to optimize sensor data. This method is helpful in reducing the load on network imposed by massive amount data from heterogeneous IoT devices. In this method, parsimonious covering theory is used to perform the data abstraction. Amadeo et al. [101] propose a high level Named Data Networking (NDN) for IoT data, resulting from the interconnection of billions of heterogeneous devices. This method uses named contents, combined with the name based routing helpful in eliminating the IP address assignment problem and helps to search

Table 4
Summarization of various energy conserving solutions for IoT.

Ref.	Optimization Objectives	Strength	Evaluation	Limitations
J. Chen et al. [79]	Minimize energy consumption.	In this algorithm total energy consumption does not increase even though number of MEs increases in comparison with other schemes, i.e., the number of MEs has less impact on energy consumption. When the data request distribution of MEs is more concentrated, then also energy consumption is negligible.	Simulation	Computational over-head due to reward and the weight calculation function for evaluation.
S. Rani et al. [80]	Minimize energy consumption; maximize scalability & network lifetime.	Transmission delay is lesser than other schemes such as EESAA, MOD LEACH, T DEEC, SEP, and LEACH. Energy efficient in case of cluster topology.	Simulation	Causes problem in the dynamic environment (even though the failure of nodes due to energy factor has been considered in this protocol).
Y. W. Kuo et al. [81]	Minimize energy consumption, delay & radio resource management.	The proposed scheme considers both real-time requirement of individual IoT device and overall network performance. Better throughput when compared to RR and MAX-C/I scheme.	Simulation	Additional computational overhead due to fuzzy logic.
J. Tang et al. [82]	Minimize energy consumption.	Energy consumed during different time period based on ECH-tree is minimal when compared to traditional method. Considers the spatial and temporal features of sensors, which effectively minimizes the energy consumption in the WSN.	Simulation	Issues in the communication, due to the exploitation of temporal-correlated features of sensors.
S. Abdullah et al. [83]	Minimize energy in recovery & backup node selection; minimize energy during message scheduling.	Provides a mechanism for repairing of nodes by node repair probability. Network lifetime, power saver system, provides good performance in conserving energy and prolonging the network lifetime.	Simulation	No standard solution to select the new node whenever a working backup node dies and criteria need to be considered for the selection of nodes other than energy.
Z. Zhou et al. [84]	Minimize energy consumption.	Energy consumption for multi-region aggregation queries is reduced when compared to the original index tree.	Simulation	Index and discovery of REST or DPWS services are a big challenge.
J. Luo et al. [85]	Minimize energy consumption.	Minimizes energy consumption while guaranteeing good quality of communication in WSN-based IoT ENS PD guarantees both extended lifetime and largest conservation of energy.	Simulation and test bed	Optimal energy saving strategies are required for other practical queuing models of WSN based IoT applications, such as health care, inventory tracking, smart grids, home appliances, etc.
X. Tang et al. [86]	Minimize energy consumption; maximize efficiency of network topology discovery.	Applicable to the dynamic environment with different pairs of network sensors. Uses robust mobile agent in different network conditions to increase the speed of the network.	Simulation	If number of agent's increases, then the bandwidth requirement also increases.
S. Tozlu et al. [87]	Minimize energy consumption; maximize communication range.	Sensor network performs appreciably better for the out-of-network scenario. Provides power saving mechanism for Wi-Fi enabled devices.	Real-time experiment	During heavy network traffic, the AP becomes a bottleneck, which has adverse effect on latency and reliability.

Table 5
Summarization of various congestion control methods for IoT.

Ref.	Optimization Objectives	Strength	Evaluation	Control Mechanism	Limitations
J. L. Chen et al. [92]	Minimize congestion.	Analyzes congestion control strategy for MTC network. Insight and approach to develop high quality communication frameworks for IoT data test bed based on LTE communications systems.	Analysis.	Reducing paging overhead.	Frequently switching impacts on network quality. No effective mechanism addressed for error monitoring.
Y. Pan et al. [93]	Minimize congestion; maximize delivery of high priority data.	Adjusts data acquisition rate depending on the level of congestion in a distributed manner. Higher delivery rate of high priority data when network experiences different congestion levels.	Simulation OPNET.	Adjusting data acquisition rate	Rate of data delivery reduces considerably when the network is congested because this method makes sensors acquiring low-priority data to enter into sleep mode.
A. P. Castellani et al [94]	Minimize congestion.	Adds congestion control capabilities to 6LoWPAN based protocol stacks. Quantified for both unidirectional as well as bidirectional CoAP	Simulation.	Aggregating data packets on IP queues.	Does not improve end-to-end delay. Congestion control algorithms cannot adapt automatically to different topology, network type, and traffic flow model.
A. Betzler et al. [95]	Minimize congestion, delay; maximize reliability.	CoCoA + provides a higher degree of reliability and lower delays. This method is resilient against the sudden change in network traffic and adapts quickly to a different level of network congestion.	Simulation Cooja.	By fastening retransmission rate.	CoCoA + does not achieve the similar performance when compared to CoCoA, but, performs better or similar to default CoAP.
R. K. Lam et al. [96]	Minimize congestion; maximize throughput.	Provides a mechanism for repair of nodes by node repair probability Network lifetime and power saving system, provides good performance in extending the network lifetime.	Simulation MATLAB.	Transmission rate adjustment.	No standard solution is proposed to select a new node if the working backup node dies, and what should be the criteria for the selection of nodes other than energy.
H. A. Al Kashoash et al. [97]	Minimize congestion, packet loss, energy consumption; maximize PDR, throughput.	Reduces the amount of packet loss rate due to buffer overflow during congestion. This method improves network performance with respect to PDR, throughput, and energy consumption by selecting the least congested path from a leaf node to a sink node.	Simulation.	Selecting less congested path.	Does not use both traffic control and congestion control to support hybrid application that is common in IoT.
J. Huang et al. [98]	Minimize congestion; maximize throughput.	IRED congestion control mechanism achieves better throughput performance than the regular RED without sacrificing average delay performance.	Simulation OMNET++.	By setting up max & a min threshold level in the queue.	Does not consider the packet arrival from multiple sources.

contents in a large heterogeneous network. Table 6 provides various methods to address the heterogeneity challenge in IoT.

4.5. Scalability

Due to the use of embedded technologies in IoT, leads to large deployment of small sized and fewer memory devices like sensors and actuators in the real time applications. As these device numbers grow, data produced and network required, also grows unboundedly [108]. So handling these device data and to provide an efficient network to these devices is a big challenge task in IoT. In [109], the authors proposed a mechanism that optimizes the IEEE 802.15.4 networks by reducing 42% of packet transfer and 35% with respect to data transfer through header compaction which reduces and helps in achieving smaller header. This method is one of the best lightweight Extensible Authentication Protocol (EAP) and helps to deploy large scale devices in the network to facilitate scalability to the IoT network. To provide scalability authors in [110], proposed a storage management strategy to optimally use the limited storage space available in IoT devices. In this method, individual nodes maintain limited security information about the subset of nodes and when this method is validated, perform similar to the nodes with the ideal storage space hence, this method helps in scaling trust management scheme for a large number of nodes in the network and meets the scalability challenge. Table 7 provides various methods to address scalability in IoT network.

4.6. Reliability

Network technology used in the IoT is unmanned in most of the applications and reliability is the most important quality parameter. In [116], the authors have proposed novel L2AM metrics to RPL to consider minimum cost path during routing. This method considers route on the basis of data reliability defined by ETX and residual energy present in the node. Due to this metric, it is possible to increase overall network lifetime with better network reliability. Kyriazisa et al. [117] proposed decentralized management mechanism for providing reliable and smarter service to IoT network work. This approach uses situational acquisition, knowledge and analysis strategy to be aware of the unconditional situation to the IoT system. Additionally, this uses a concept called privelets to provision confidentiality and to protect the personal data. In this application, components are executed on the basis of day instead of moving data into the application that helps sensitive data to preserve. The authors in [118], proposed RERUM framework built on network protocols, and interfaced for hardware. This enhances available reliability, security, and trustworthiness of the IoT. This framework uses privacy-by-design concept through that data are not be exposed to the third person and helps to maintain data privacy. Table 8 provides other methods to improve reliability in IoT.

4.7. Quality of service (QoS)

The IoT network's QoS parameters are considered from various views and dimensions such as bandwidth, delay, packet loss rate, avoid interference and jitter. Hence, QoS need to be defined differently for different technology. It is very difficult to achieve QoS efficiently in wireless networks, due to the gap in the segment that is a resultant of management and resource allocation of the shared wireless media [7]. In [123], authors proposed discontinues reception/transmission

(DRX/DTX) mechanism for 3GPP LTE-A to guarantee the traffic bit rate, packet delay, and rate of packet loss with saving energy of user devices in IoT applications in QoS context. To utilize the resource of LTE air interface optimally, the authors in [124] have

Table 6
Summarization of various methods addressing heterogeneity challenge in IoT.

Ref.	Objectives	Strength	Evaluation	Limitations
W. Kim et al. [102]	To maximize user throughput and robust connectivity in IoT.	Improves per user and network throughput with load balancing in the dual connectivity and also for dynamic TDD configuration. Algorithm provides an efficient mechanism to support heterogeneous network.	Simulation.	Does not address fluctuating user traffic demand and mobility.
M. Surligas et al. [103]	To provide concurrent transmission and reception of multiple standards and channels, within the same radio band with single workstation.	Supports concurrent data transmission to multiple standards and channels on adjacent frequencies of SDR devices.	Simulation and Test bed.	Require additional changes to the Physical software implementation, which limits its portability. Buffers are required for acknowledgment.
L. Zhang et al. [104]	To reduce overhead and power consumption for different communication networks.	Improves the transmission efficiency Provides module that meets different communication distance requirement, hence the method decreases the deployment and development cost of the system efficiency.	Test bed.	The key problem of the energy consumption needs to be solved. Not suitable for the application of the large scale system.
S. M. Oteafy et al. [105]	PAIR routing protocol to support diverse heterogeneous IoT components.	This method has capability to route information over different heterogeneous nodes of the IoT, especially during multiple owners. The utility function presented here assimilates buffer space, load balancing and link maintenance.	Simulation.	This method is inherently application specific, and their current state of the art fails to integrate on a global scale.
J. Guo et al. [106]	RAM-RPL to achieve an adaptive mode of operation in heterogeneous M2M networks.	This method outperforms than standard RPL in terms of PDR and control message overhead reduction while maintaining similar packet latency. Utilizes extra resources allocated by powerful nodes and transfers routing workload from fever powerful nodes to more powerful nodes.	System Model.	The control message transmission rate surges due to more data packet transmission.
E. Jung et al. [107]	Delegation approach to support diversity among the devices.	Devices with different network connectivity will integrate due to the cooperation of the agents rather than direct communication between heterogeneous devices.	Real-time.	Each agent must be aware of every other agent. Does not provide scalability to aid large number of devices.

Table 7
Summarization of various methods to provide scalability in IoT.

Ref.	Objectives	Strength	Evaluation	Limitations
E. Cerritos et al. [111]	To provide highly scalable architecture and to dynamically decide load balancing.	Achieves high resource utilization and fast response time. Faster response time in high traffic load.	Test bed.	Checks only in high and low traffic load, does not evaluate the impact of other types of operations and patterns.
A. Bader et al. [112]	To facilitate multi hop networking for energy efficient and highly scalable IoT.	Using blind cooperative transmission in combination with multi-hop networking reduces overhead on underlying protocol helps in better network scalability.	Simulation.	The advantage degrades whenever the new hop is introduced.
M. Kovatsch et al. [113]	To provide scalable service to support conceivable large scale IoT applications.	Provides higher throughput and fully utilizes the resources of today's multi-core systems. Significantly improves back end scalability service for a vast number of connected devices.	Real-time.	Didn't considered security aspects.
J. Jermyn et al. [114]	To provide scalability for IoT on LTE networks, determining to what extent mobile networks could be overwhelmed by plenty of devices attempting to communicate.	Determines which type of M2M traffic presents a larger challenge and provides a mechanism for efficient network scalability. Due to this method, traffic load appears to scale up in early as the number of connected devices increases.	Simulation. & test bed	Some of the M2M device categories, such as asset tracking, exhibit a much quicker signaling and data traffic load raise which exhibits potential challenge for this method.
A. Saxena et al. [115]	To eliminate the requirement for any additional access control at the endpoints and to facilitate large scale IoT systems deployment.	Prevents unauthorized communication, thereby saves overall bandwidth. Provides features such as decentralized access control database, lightweight endpoints, easy revocation and device discovery.	Real-time.	Does not address mechanisms for scaling large number of resource constraint IoT devices.

Table 8
Summarization of various methods to provide reliability in IoT.

Ref.	Objectives	Strength	Evaluation	Limitations
D. Macedo et al. [119]	To address the dependability problems such as reliability and availability, since a device failure might keep people at risk or result in financial loss.	Capable of predicting the dependability problem of IoT devices or applications.	Mathematical Model.	Failed to consider reward models to assess the financial costs related to different redundancy strategies.
L. Li et al. [120]	To provide probabilistic approach to formally delineate and analyze the cost and reliability related properties of the service composition in IoT.	Success probability of the composite service can be calculated with the current IoT settings of the devices.	Analysis.	Focused only on a single composite service.
N. Maalel et al. [121]	For delivery of high priority events from many scattered objects without packet loss, packet loss recovery and route quality evaluation in the IoT.	Protocol provisions an adaptive routing path selection based on link quality. Provides hop-by-hop packet loss recovery mechanism, which makes intermediate nodes to take responsibility of loss detection and recovery.	Analysis.	This method is not validated in real time scenario.
J. Kempf et al. [122]	To provide architectural guidelines to deal with reliability issues from packet transmission to network lifetime and application behavior in IoT.	Describes reliability problems present in the link layer, transport layer, and the application layer in context to sensor networks and proposes possible solution.	Analysis.	Generalized reliability discussion is done throughout the paper, which does not give solution for the current reliability problem.

tested the packets of different size in LTE uplink, obtained result showed that the packets with smaller size have achieved nearly half of the throughput than compared to a larger sized packet. This result provides a way for packet aggregation at the IoT gateway's mobile edge to optimize various QoS parameters like Latency, packet loss, jitter and bandwidth utilization required by a large number of small packets. In [125], the authors have proposed a QoS architecture that provides a mechanism for controlling transfer and translation from top to bottom layer. This architecture also provides cross-layer management facility and brokers to lower layer to provide control mechanism. With this architecture, it is possible for researchers and developers to further optimize the QoS of IoT. Table 9 provides different QoS methods for achieving QoS in IoT.

4.8. Security

Security is the vital requirement for securing data transporting in the network, hence it is the optimal requirement to provide an efficient mechanism to secure data from different kind of breaches. In [131], the authors have proposed DTLS based two-way authentication architecture for it. This method uses the RSA algorithm for cryptography and it is built to work on the standard communication stack. This security architecture requires less energy, memory overhead, and latency, hence it is very well suited for IoT memory constrained energy efficient IoT devices. To secure IoT communication authors in [132], have proposed a secure multi-hop routing protocol (SMRP), uses security methods in its routing protocol which helps in faster cryptographic performance helps this to run on memory constraint hardware chips. This feature allows system to minimize power consumption and heat generation. To secure IP based IoT authors in [134], have proposed a mechanism that initially uses Host Identity Protocol (HIP) and later combined with DTLS provided a good result. This mechanism provides a better solution for key management, securing communication and secure network access. This mechanism uses less memory footprint and is very well suited for securing IoT network. In [135], the author has proposed token based authentication method, where each query with signature is used to validate the correct data. Table 10 provides other security methods for IoT network.

5. Open issues and challenges for network optimization in IoT

Evolution of IoT in support to communication infrastructure aids new services for various fields like home network, smart city, retail, logistics, medical and aeronautics. However, this evolution poses new issues and challenges to manage the usage and management of network. Joint initiative by industries like Alcatel Lucent, Orange, Thales etc., along with Carnot Institute identified some of the potential challenges related to IoT and Smart networked objects in [141], to provide awareness among various industries and academicians. Along with these challenges, this section provides various open issues and challenges for optimizing IoT network.

1. Network routing: The efficient network relies on network topology and network architecture. An efficient routing mechanism needs to be addressed for sending the packets inside the mesh network topology, since we have considered IEEE 802.15.4 as one of the underlying technology for IoT, hence issues and challenges are addressed with respect to IEEE 802.15.4. Routing in the mesh network can happen in either network layer or in the link layer. In the IETF terminology link layer routing is called mesh-under, where single IP hop is formed by multiple link layer hops. Similarly, mesh

Table 9
Summarization of various methods to provide QoS in IoT.

Ref.	Objectives	Strength	Evaluation	Limitations
L. Li et al. [126]	To provide a three layer QoS scheduling model for service oriented IoT.	This method optimizes the scheduling performance of IoT network and minimizes the resource costs. Provides QoS support for distinct applications in IoT and increases lifetime of IoT network.	Simulation.	Method has not accounted packet delay, loss, and control mechanism in case of congestion.
G. Vithya et al. [127]	To provide QoS routing method by setting up priority in the network.	Packets are ordered in priority queue and are configured, aligned to achieve the best transmission in time with low latency. Robust to both topology failures and traffic variations.	Test bed.	The priority is given based on the highest number of frames in the cluster, that makes critical data from lower number frames cluster to wait in critical scenario until its term.
I. Awan et al. [128]	To investigate the QoS of delay sensitive things and the matching traffic generated over the network.	Provides an analytical model for evaluating the performance of smart devices under different traffic states to meet the QoS constraints. Uses buffer management, makes high priority traffic continues its arrival by impel out low priority traffic to circumvent loss of emergency related data packets.	Simulation.	This method is only an analytical model, which is not validated in real time scenario.
Z. Ming et al. [129]	To provide QoS requirements of IoT composite services.	The algorithm is fast enough to meet real-time requirements of IoT.	Test bed.	Uncertainty analysis of QoS is not performed in this method.
M. Aazam et al. [130]	To increase QoS based on previous Quality of Experience (QoE) and Net Promoter Score (NPS) records.	Fog computing provides the solution by bringing cloud resources to the edge of the underlying IoT and other end nodes. Provides better reliability and reduces jitter.	Simulation & Test bed.	Strenuous in predicting the resources consumed by heterogeneous devices.

Table 10
Summarization of various mechanisms to provide Security for IoT network.

Ref.	Objectives	Attacks addressed	Strength	Evaluation	Limitations
S. Raza et al. [136]	To provide IDS for IoT to provide security from routing attacks.	Spoofing, sink-hole, & selective forwarding attacks.	This method is feasible to use in the context of RPL, 6LoWPAN, and the IoT. Detects all malicious nodes which instigate sinkhole and selective forwarding attacks.	Simulation.	Positive rate of this method is not 100% i.e., raises few false alarms during detection process. Detects only some types of network attacks in IoT.
H. Perrey et al. [137]	To provide a generic scheme for topology authentication in RPL.	Resource exhaustion, black hole & interception.	Provides enhancements to the VeRA protective scheme, by detecting and mitigating two new rank order attacks like rank chain forgery and rank replay attack. Enhances security by TRAIL (Trust Anchor Interconnection Loop), which discovers and isolates bogus nodes.	Test bed.	Trail method introduces additional overhead on RPL, during tree construction. Requires optimization of the algorithm to reduce dependency on network size.
P. Pongle et al. [138]	For detecting worm hole attack and attacker in IoT network.	Wormhole attacks.	Identifies the Wormhole attack, and by using received signal strength, identifies attacker nodes. The proposed IDS system is very easy to extend further for different types of network attack in IoT.	Simulation & test bed.	This method only takes a fixed number of UDP packets for attack detection. Utilizes additional RAM and ROM from memory constrained nodes.
Q. M. Ashraf et al. [139]	To provide single hop, single gateway based node registration technique for IoT.	Resource exhaustion & interception.	This method includes support for scalability, security, and user friendliness. In worst scenario also, the PDR of 100% is achieved.	Simulation.	The scope of registration is only limited to smart home setup. Average time to register is not validated for increased number of nodes.
P. Kasinathan et al. [140]	To provide DoS detection architecture for 6LoWPAN based IoT.	Denial of service.	The architecture integrates IDS into the network framework. IDS run on a host computer to reduce the resource constraint problem and provide more capability to detect complicated attacks.	Test bed.	The intrusion prevention system (IPS) is not designed in this method. To surveil large networks, distributed sniffing detection mechanisms are required.

routing in the network layer is known as route-over, where each link layer hop is an IP hop and routing takes place between these IP hops [142].

a) Issues:
- To provide an effective routing mechanism in the link layer.
- To provide routing in the network layer to happen efficiently with less overhead.
- To select best energy efficient algorithm among various types.

b) Challenges:
- Routing in link layer or mesh-under is addressed by constructing a spanning tree [69], but this method suits only for static routes. However the challenge is to provide optimal routing mechanism dynamically since it adds additional overhead whenever a new node wants to join the network dynamically, where address reallocation and table update need to be performed to adapt for topology changes.
- Routing in the network layer or route-over, is addressed by IPv6 Routing Protocol for Low power and Lossy Networks (RPL), reduces the over head of maintaining the table at non-root nodes, but due to insertion of routing information to the packet header traversing downwards, introduces overhead to network due to smaller maximum transmission unit (MTU). Hence the challenge is to reduce the overhead introduced by routing protocol and facilitate devices with a smaller MTU to work optimally.
- The challenge is to choose ideal energy efficient algorithms among different available types because different algorithm uses different methods in selecting the cluster head and technique in route selection [143].

2. Mobility: Mobility related to network refers to changing of mobile IP subnet from its point of attachment to the IP backbone network. Simple mobile structure constitutes single or multiple mobile nodes and mobile routers of the mobile network with defined topology. In complex mobile structure, mobile nodes or other mobile structure visit the mobile network. The prime requirement for mobility in the network is handover i.e. changing of mobile node's point of attachment to the network [144]. There are two types of mobility with the context of the network as micro-mobility and macro-mobility. Micro-mobility refers to the movement of subscribers within the two points of the same network and macro-mobility refers to the movement between the networks.

a) Issues:
- To provide macro-mobility in the network with better QoS.
- To provide better QoS in the case of micro-mobility in the network.
- To provide an optimized route in nested mobility.

b) Challenges:
- Mobile IP (MIP) provides macro-mobility in the network and achieves efficient packets routing, hand-off, lower packet loss, etc., but the challenge is to reduce the overhead rate since MIP has a higher overhead rate.
- Micro-mobility is also addressed by using MIP, but the degradation of service in Voice over IP (VoIP) happens due to frequent handoff. So bi-directional tunneling is used for network mobility, but this approach is not able to address advanced issues like seamless mobility, means hand-off delay and lowering the packet loss rate [145]. Hence the most efficient method is required for addressing these challenges.
- The challenge is to provide an optimized route for nested mobility, i.e. optimal path should be selected to send packets between a corresponding node and the mobile node, within the same mobile network without considering how deep the mobile, the network is nested [146].

3. Multicast: Multicast is used in the network basically to show or to notify their presence to other nodes in the group or to request the resource from the concerned source whenever there is no idea from whom it has to be requested [141].

a) Issues:
- Different rate of data transmission in different protocols.
- Track or to recover the missed out packets at the link layer.
- Multicast packet loss due to sleeping of nodes to conserve energy.
- Multicast Protocol for Low Power and Lossy Networks (MPL) is addressed only for ZigBee communication.

b) Challenges:
- Transmission of data packets at uniform speed is challenging since different protocol standard sends data packet at the different rate due to which recipient faces multiple different rates of incoming packets.
- Most of the wireless protocol acknowledgment at the link layer is disabled for multicasting, due to which sender cannot able to track or recover the missed out packets at the link layer. Hence challenge is to provide a mechanism to recover such missed out packets.
- To perpetuate energy nodes enters into sleep mode, where some of the packets sent during multicast would be dropped and in multi-hop communication scenario of mesh network, nodes need to be awake for forwarding the packets till it reaches the recipient which pushes energy limited nodes to be awake for prolonged time, makes these nodes energy to exhaust swiftly than intentional [142]. So it is the challenge to address this issue.
- MPL is proposed instead of IPv6 neighbor discovery optimization for 6LoWPAN, where there is no need for maintaining the table on topology information, but the challenge is to make this suitable for all communication types since it suits only for ZigBee communication.

4. Security: Security is a key requisite for any device connected to the Internet, due to the higher degree of vulnerability to attack. People trust the product or technology only when the product and its data is secured enough to withstand from malicious activities. Less secured IoT devices lead to an entry point for attack and attackers to reprogram or make it malfunction. Poorly designed devices or application exposes itself for data theft, thus the less secure device connected to the Internet affects the security and pliability of the Internet not only locally but globally [147]. For example, less secured smoke detection sensor device connected to the Internet are more prone to attack and sends false/spam messages or email about the status to its recipient after infected with malware.

a) Issues:
- To provide security for data present in IoT network from various types of attacks.
- Exposition of the network due to flaws in the technology and its implementation.
- Penetration into the network through side channel attack

b) Challenges:
- IoT network security comprises of security for content in the network, security from an illegal resource authorization and from intruders. Network is designated to transfer information and the sent information should be secured

from impish activities such as man-in-the-middle attack, denial of service (DoS) attacks, virus injection, data eavesdropping, illegal system access and much more. Hence challenge is to propose single mechanism which provides security from these types of attacks.
- Security vulnerability at network happens due to two main reasons like security risk of entire IoT network setup and flaws during technology and protocols implementation and modeling [148]. Adding or removing of devices in wireless networks could be performed at any time creates wireless network to expose themselves for spiteful activity or susceptible to security breach. This characteristic provides a means for intruder to add malicious nodes across ideal nodes which degrades the network quality. So the challenge is to provide security mechanism during this situation.
- Attempt to break into the system by finding the weakness in the cryptography system's physical implementation through electromagnetic leaks, timing information, energy consumption and many others lead the intruder to penetrate into the system [149]. So challenge for the designer is to implement stronger cryptography algorithm.

Apart from the above mentioned issues and challenges, Table 11 provides various types of network attacks to IoT network.

5. Heterogeneity: Heterogeneous network encompasses the different type of integrated network, where the end user/device can communicate with these communication modalities, which have different capacity and characteristic constraint such as wired, wireless and satellite communication modalities having different capacity and characteristics. Heterogeneity is the vital issue that IoT applications are facing when different types of devices or protocols are made to interoperate [147].

a) Issues:
- Achieving performance of the applications used in the heterogeneous network.
- Conservation of energy in the heterogeneous network.
- Resource integration for the heterogeneous network.
- To provide robustness in the heterogeneous network.
- To provide trustworthiness and security for the heterogeneous network.

b) Challenges:
- The primary challenge is to deploy high performance applications in the heterogeneous network and achieving the same performance from these applications without modifying network or technology. Secondly, challenge in the trade-off between exposing or hiding network state or variability, when to expose or to hide the network state on the basis of time and magnitude [156].
- Heterogeneous network drains more energy when compared to the homogeneous network due to inefficient resource management and lesser flexibility. This makes a challenge for energy aware IoT devices to preserve energy for longer usage.
- Due to the shortfall of resource integration and problems associated with differences in the modalities heterogeneous network is harder to utilize.
- Heterogeneous network is more prone to failure due to their complex network structure and poor resource management than the homogeneous network. The network should robust their performance during perturbations or failure in the intermediate network. Robustness of the heterogeneous network is a challenging task in the critical application of the Internet controlled power grid and many others [157].
- Heterogeneous network is less secure than the homogeneous network, due to complexity in network structure and area exposed. The trustworthiness of the heterogeneous network needs to be addressed by efficient architectural design, implementation and application usage, which is a challenging task due to the higher degree of network complexity [158].

6. Interoperability: Interoperability is due to heterogeneity among protocols and communication stack of objects or devices. Different devices in IoT applications use different network technologies. So there exist many issues and challenges to provide interoperability among these underlying technologies [159].

a) Issues:
- Populating the data from end devices directly to the Internet.
- Establishing the interoperability among various different device types.
- A non standard approach used in the developing and manufacturing devices.
- Establishing interoperability among various flavors and cloud types.

b) Challenges:
- Legacy devices and systems don't communicate with IP based devices and don't support TCP/IP protocol directly without the use of gateway in between them. For example, in ZigBee v1, HART and many others without exerting gateway in between these devices, the generated data will not be forwarded to Internet.
- Discrepancy in protocols and communication occurs between original equipment manufacturers (OEM) devices, wherein one manufacturer device does not support other manufacturer devices. Additionally, devices use the different type of operating systems and versions, this contradicts interoperability among devices. So the challenge is to develop and use of open source frameworks, which are accepted universally [160].
- Due to lack of standardization and lesser documentation during the IoT devices design and configuration has a negative impact on the network resource utilization and on interoperable devices to which these devices are connected to the Internet.
- There are different types of cloud services available and different devices use different cloud services, which poses a challenge for the device's storage interoperability [161].

7. Scalability: Scalability in a short word defined as the system should autonomously handle IoT entities growing rapidly at the edge network to ease up network performance. Devices in IoT can increase drastically in short period of time. Hence network should be robust enough to provide services to these devices [162].

a) Issues:
- To support inter-organizational communication in large scale operation.
- To select best load balancing technique.
- To select best architecture for better scalability.
- To provide autonomous M2M communications among neighbor nodes in case of concurrent data

b) Challenges:
- To provide inter-organizational communication involving larger entities requires autonomous interactions and requires collaboration between them, which is a challenging task [108].

Table 11
Different Types of Network Attacks.

Type of attack	Nature of attack	Impact on network Performance	Counter measures	Limitations
Selective Forwarding [146,147]	Malicious node behaves like black hole and may refuse to forward certain messages and drops them	Interruption to route path	Heart beat protocol, end-to-end packet Loss and PHACK [148]	Additional mechanism need to be integrated to prevent the attack.
Wormhole [149,150]	Modifies the intended or actual path by intermediate intruding nodes	Digital signature based Approach	Interruption to traffic flow and route topology	Nodes should know each other's signature, which consumes more computational time.
Sybil Attack [149,150]	Malicious node represents itself with multiple identities	Central authority method	Traffic unreachable to attacked node	Central authority like admin, acts as a certifying authority by which each node has exact one key, but for larger network it is difficult to implement and follow this approach.
Impersonation Attack [151,154]	A malicious node identifies itself by using legitimate id	Reduces network life time	User mobility profiling	Additional work is required to test effectiveness and its compatibility with real time systems.
Sinkhole attacks [149,150]	Intruder node creates fake route and sends route information as this is the optimum route available	Creates heavy traffic in the network	Intrusion detection system (IDS)	Detects only when penetration happens.
Hello flooding attack [149,150,153]	Malicious node sends hello message to legitimate node to form a route	Drains more sensor nodes battery power	Cryptography technique	Two devices with the same secret key can communicate to each other, but in this case, attacker node can spoof its identity and could generate the attack.
Blackhole or packet drop attack [152,155]	Attacker node drops all the packets in the route up to its origin	Packet drop, control overhead and increase in traffic	IDS based on anti-black hole mechanism	Helps in isolating the malicious node, but fails in case of collaborative attack.

- To select best method for balancing the load among different devices and congestion less routes plays a crucial role since this increase availability and scalability [162].
- To select best software architecture which plays a vital role in scalability or else it will end up in increasing hardware requirement.
- Challenge is to establish autonomous communication among neighboring IoT entities in an opportunistic manner.

8. Overhead and Packet retransmission: Overhead is defined as the excess computational time, bandwidth or other network resources that are required for specific task. Overhead is caused due to improper selection of methods while transporting of packets.

Meanwhile packet retransmission is caused due to lost or damage of packets while transmitting. Reasons for packet retransmission are many, but in IoT application it must be minimized to reduce power consumption. Reducing overhead on the network simultaneously reduces need for packet retransmission.

a) Issues:
- To select best security method that adds less overhead on the network.
- Choosing appropriate data reduction model to reduce overhead of data.
- Determining best routing protocol which incur less routing overhead.
- To select best congestion control mechanism for reducing packet retransmission.
- To select best method for packet retransmission
- To select less energy consuming mechanism for packet retransmission during mobile nodes.

b) Challenges:
- Choosing best security method for encryption and decryption of packets is important as these processes will add additional overhead on the network performance [133].
- Data reduction model restricts the data during collection, transmission and processing of data size which not only reduces data overhead but also increase overall IoT performance. So the challenge is to select best data reduction model.
- To maintain up-to-date information about routes, routing algorithm sends small sized packets like HELLO packet to check whether neighbor nodes are active or not, called routing packets. These packets don't carry data packets. However these routing packets increase overhead in the network since they use same bandwidth, which are used by data packets in most of the cases. Hence it is necessary to select best routing algorithm which incur lesser routing overhead [57].
- Challenge is to select best congestion control mechanism which helps to select congestion free path for sending of data and to discard unnecessary packet leading to congestion through packet discarding method to avoid packet retransmission [89].
- To select best method for packet retransmission is a critical requirement since most of the protocols in IoT application use UDP instead of TCP to conserve energy and to provide low latency application requirement.
- To select electing best energy efficient protocol which consumes less energy for retransmitting of packets during mobile scenarios since chances of loosing packets are higher during nodes mobility [145].

6. Conclusion

Several advancements in IoT have been already seen in the literature and also in the real-time applications where the network of sensors and mobile devices are interconnected and linked to the Internet through IP-based technologies. With network optimization as one of the main challenges that IoT would face in the forthcoming years. This review paper depicts comprehensive survey on the most important aspects through some of the novel approaches related to network optimization for IoT communication is presented. Various algorithm types for multi-objective problems, robust shortest path tree problem, QoS aware energy efficient cooperative clusters, hierarchical sensor networks, approaches for optimizing energy efficiency in IoT, opportunistic link selection method and secure energy efficient routing protocol

are presented in order to improve network utilization. Different IoT network parameters like routing, energy conservation, congestion, heterogeneity, scalability, reliability, QoS, and security is presented by reviewing recent papers in the relevant parameters. In this various power saving scheduling scheme, energy efficient uplink radio resource for Management of LTE-A relay networks in IoT, CoAP Congestion Control mechanism, multiple layer design for Mass data transmission for emergency applications, scalable cloud services, compact and extensible authentication protocol for IoT has been discussed to address challenges that the network is facing and to improve efficient wireless spectrum utilization. Diverse recent related works are reviewed to define the state-of-the-art techniques for network optimization in IoT with stress on the important factors and the limitations that need to be addressed in the future research papers are explicitly classified and distinguished with respect to different network parameters of IoT. Eventually various issues and challenges of IoT network optimization are delineated. Packet retransmission, challenge in selecting efficient method for reducing network overhead, different network attack types, interoperability challenge existing between various devices types due to heterogeneity and issues related to mobility of nodes are discussed. The outcome of this paper highlights the importance of network optimization in IoT, with ample amount of bibliography contents desired to help new researchers embark to work on optimizing network for future IoT applications.

Acknowledgements

The authors would like to thank the reviewers for their constructive criticisms and valuable comments, which have been very useful in improving the quality of the paper. This research work has been funded by the Science and Engineering Research Board (SERB-DST) Project File No: EEQ/2017/000681. Authors sincerely thank SERB-DST for intellectual generosity and research support provided.

References

[1] S. Li, L. Da Xu, S. Zhao, The internet of things: a survey, Inf. Syst. Front. 17 (2) (2015) 243–259.
[2] L. Atzori, A. Iera, G. Morabito, The internet of things: a survey, Comput. Networks 54 (15) (2010) 2787–2805.
[3] J. Francois, T. Cholez, T. Engel, CCN Traffic optimization for IoT, in Fourth International Conference on the Network of the Future (NoF), 2013, pp. 1–5.
[4] N. Accettura, M. R. Palattella, G. Boggia, L. A. Grieco, M. Dohler, Decentralized traffic aware scheduling for multi-hop low power lossy networks in the internet of things, in IEEE 14th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM), 2013, pp. 1–6.
[5] Y. Liu, A. Liu, Y. Hu, Z. Li, Y.-J. Choi, H. Sekiya, J. Li, FFSC: an energy efficiency communications approach for delay minimizing in internet of things, IEEE Access 4 (2016) 3775–3793.
[6] T.S. Prakash, G. Badrinath, K. Venugopal, L.M. Patnaik, Energy aware topology management in Ad Hoc, Wireless Networks (2006) 1.
[7] J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, Internet of things (IoT): a vision, architectural elements, and future directions, Future Gener. Comput. Syst. 29 (7) (2013) 1645–1660.
[8] J. Granjal, E. Monteiro, J.S. Silva, Security for the internet of things: a survey of existing protocols and open research issues, IEEE Commun. Surveys Tutorials 17 (3) (2015) 1294–1312.
[9] Z. Sheng, S. Yang, Y. Yu, A. Vasilakos, J. Mccann, K. Leung, A survey on the IETF protocol suite for the internet of things: standards, challenges, and opportunities, IEEE Wireless Commun. 20 (6) (2013) 91–98.
[10] A. Botta, W. De Donato, V. Persico, A. Pescapé, Integration of cloud computing and internet of things: a survey, Future Gener. Comput. Syst. 56 (2016) 684–700.
[11] Ala Al-Fuqaha, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari, Moussa Ayyash, Internet of things: a survey on enabling technologies, protocols, and applications, IEEE Commun. Surv. Tutorials 17 (4) (2015) 2347–2376.
[12] K. Ashton, That internet of things thing, RFiD J. 22 (7) (2009) 97–114.
[13] K.L. Lueth, Why the Internet of Things is Called Internet of Things: Definition, History, Disambiguation. URL https://iot-analytics.com/internet-of-things-definition/.
[14] G. Digital, Industrial Internet of Things. URL https://www.ge.com/digital/blog/everything-you-need-know-about-industrial-internet-things.
[15] V. Stirbu, Towards a restful plug and play experience in the web of things, in IEEE International Conference on Semantic Computing, 2008, pp. 512–517.
[16] Y. Hu, Y. Ding, K. Hao, L. Ren, H. Han, An immune orthogonal learning particle swarm optimisation algorithm for routing recovery of wireless sensor networks with mobile sink, Int. J. Syst. Sci. 45 (3) (2014) 337–350.
[17] G.L. da Silva Fré, J. de Carvalho Silva, F.A. Reis, L.D.P. Mendes, Particle Swarm optimization implementation for minimal transmission power providing a fully-connected cluster for the internet of things, in International Workshop on Telecommunications (IWT), 2015, pp. 1–7.
[18] L. Song, K.K. Chai, Y. Chen, J. Loo, S. Jimaa, J. Schormans, Qpso-based energy-aware clustering scheme in the capillary networks for internet of things systems, in IEEE Wireless Communications and Networking Conference (WCNC), 2016, pp. 1–6.
[19] W.-T. Sung, C.-C. Hsu, Iot system environmental monitoring using IPSO weight factor estimation, Sens. Rev. 33 (3) (2013) 246–256.
[20] T. Kumrai, K. Ota, M. Dong, J. Kishigami, D.K. Sung, Multi-objective optimization in cloud brokering systems for connected internet of things, IEEE Int. Things J. 4 (2) (2017) 404–413.
[21] A.V. Dhumane, R.S. Prasad, J.R. Prasad, An optimal routing algorithm for internet of things enabling technologies, Int. J. Rough Sets Data Anal. (IJRSDA) 4 (3) (2017) 1–16.
[22] J. Martins, A. Mazayev, N. Correia, G. Schütz, A. Barradas, Gacn: self-clustering genetic algorithm for constrained networks, IEEE Commun. Lett. 21 (3) (2017) 628–631.
[23] I. Khan, J. Sahoo, S. Han, R. Glitho, N. Crespi, A genetic algorithm-based solution for efficient in-network sensor data annotation in virtualized wireless sensor networks, in 13th IEEE Annual Consumer Communications & Networking Conference (CCNC), 2016, pp. 321–322.
[24] K. Deb, A. Pratap, S. Agarwal, T. Meyarivan, A fast and elitist multi-objective genetic algorithm: NSGA-ii, IEEE Trans. Evol. Comput. 6 (2) (2002) 182–197.
[25] A. Rodriguez, A. Ordóñez, H. Ordoñez, R. Segovia, Adapting NSGA-ii for hierarchical sensor networks in the IoT, Procedia Comput. Sci. 61 (2015) 355–360.
[26] L. Song, K.K. Chai, Y. Chen, J. Schormans, J. Loo, A. Vinel, Qos-Aware Energy-Efficient Cooperative Scheme for Cluster-Based IoT Systems, IEEE Syst. J. (2017).
[27] A. Rodriguez, P. Falcarin, A. Ordonez, Energy optimization in wireless sensor networks based on genetic algorithms, in SAI Intelligent Systems Conference (IntelliSys), 2015, pp. 470–474.
[28] I.A. Carvalho, T.F. Noronha, C. Duhamel, L.F. Vieira, A scenario based heuristic for the robust shortest path tree problem, IFAC-PapersOnLine 49 (12) (2016) 443–448.
[29] A. Verma, S. Kaushal, A.K. Sangaiah, Computational intelligence based heuristic approach for maximizing energy efficiency in internet of things, in Intelligent Decision Support Systems for Sustainable Computing, 2017, pp. 53–76.
[30] K. Dhondge, R. Shorey, J. Tew, Hola: Heuristic and opportunistic link selection algorithm for energy efficiency in industrial internet of things (IIoT) systems, in 8th International Conference on Communication Systems and Networks (COMSNETS), 2016, pp. 1–6.
[31] S. Shailendra, A. Rao, B. Panigrahi, H.K. Rath, A. Simha, Power efficient RACH mechanism for dense IoT deployment, in IEEE International Conference on Communications Workshops (ICC Workshops), 2017, pp. 373–378.
[32] N.H.A. Ismail, R. Hassan, 6lowpan local repair using bio inspired artificial bee colony routing protocol, Procedia Technol. 11 (2013) 281–287.
[33] J. Huang, L. Xu, C.-C. Xing, Q. Duan, A novel bio-inspired multi-objective optimization algorithm for designing wireless sensor networks in the internet of things, J. Sens. (2015).
[34] M. Korczynski, A. Hamieh, J.H. Huh, H. Holm, S.R. Rajagopalan, N.H. Fefferman, Hive oversight for network intrusion early warning using diamond: a Bee-inspired method for fully distributed cyber defense, IEEE Commun. Mag. 54 (6) (2016) 60–67.
[35] N.R. Raz, M.-R. Akbarzadeh-T, A Bio-Inspired model for emergence of cooperation among nanothings, in Iranian Conference on Intelligent Systems (ICIS), 2014, pp. 1–6.
[36] P.K. Reddy, R. Babu, An evolutionary secure energy efficient routing protocol in internet of things, Int. J. Intell. Eng. Syst. 10 (3) (2017) 337–346.
[37] J. Na, K.-J. Lin, Z. Huang, S. Zhou, An Evolutionary Game Approach on IoT service selection for balancing device energy consumption, in IEEE 12th International Conference on e-Business Engineering, 2015, pp. 331–338.
[38] K. S. Hamza, F. Amir, Evolutionary clustering for integrated WSN-RFID networks, in 10th International Conference on Informatics and Systems, 2016, 267–272.
[39] B.Y. Zhang, W. Hu, J. Feng, W.H. Sun, Data classification in internet of things based on evolutionary neural network, Adv. Mater. Res. 659 (2013) 202–207.
[40] S. Ageev, Y. Kopchak, I. Kotenko, I. Saenko, Abnormal traffic detection in networks of the internet of things based on fuzzy logical inference, in XVIII International Conference on Soft Computing and Measurements (SCM), 2015, pp. 5–8.
[41] J.H. Kwon, M. Cha, S.-B. Lee, E.-J. Kim, Variable-categorized clustering algorithm using fuzzy logic for internet of things local networks, Multimedia Tools Appl. (2017) 1–20.

[42] J.-Y. Choi, J. Jeong, Design and performance analysis of cost-optimized handoff scheme based on fuzzy logic for building smart car IoT applications, Int. Inf. Inst. (Tokyo) 18 (10) (2015) 4339.
[43] Y. Mao, J. Li, M.-R. Chen, J. Liu, C. Xie, Y. Zhan, Fully secure fuzzy identity-based encryption for secure IoT communications, Comput. Stand. Interfaces 44 (2016) 117–121.
[44] Y. Li, Z. Sun, L. Han, N. Mei, Fuzzy Comprehensive Evaluation Method for Energy Management Systems Based on an Internet of Things, IEEE Access. (2017).
[45] Z. Ali, Z.H. Abbas, F.Y. Li, A stochastic routing algorithm for distributed IoT with UnReliable wireless links, IEEE 83rd Vehicular Technology Conference (VTC Spring), 2016, pp. 1–5.
[46] N. Jiang, Y. Deng, X. Kang, A. Nallanathan, Random access analysis for massive IoT networks under a new spatio-temporal model: a stochastic geometry approach, arXiv (2017). preprint arXiv: 1704.01988.
[47] R. Kaur, N. Kaur, S.K. Sood, Security in IoT network based on stochastic game net model, Int. J. Netw. Manage (2017).
[48] M. Gharbieh, H. ElSawy, A. Bader, M.S. Alouini, Spatio-temporal stochastic modeling of iot enabled cellular networks: scalability and stability analysis, IEEE Trans. Commun. (2017).
[49] P. Kuppusamy, B. Kalaavathi, Novel authentication based framework for smart transportation using IoT and memetic algorithm, Asian J. Res. Soc. Sci. Humanities 6 (10) (2016) 674–690.
[50] W. Kus, W. Mucha, Memetic inverse problem solution in cyber-physical systems, Adv. Tech. Diagn. (2016) 335–341.
[51] F. Sun, C. Wu, D. Sheng, Bayesian networks for intrusion dependency analysis in water controlling systems, J. Inform. Sci. Eng. 33, 4.
[52] N.T. Long, N.D. Thuy, P.H. Hoang, Research on applying hierarchical clustered based routing technique using artificial intelligence algorithms for quality of service of service based routing, internet of things and cloud computing, Spec. Issue Qual. Serv. Serv. Based Routing 3 (6–1) (2015) 1–8.
[53] C. Tunc, N. Akar, Markov fluid queue model of an energy harvesting IoT device with adaptive sensing, Perform. Eval. 111 (2017) 1–16.
[54] S.J. Borah, S.K. Dhurandher, I. Woungang, V. Kumar, A game theoretic context-based routing protocol for opportunistic networks in an IoT scenario, Comput. Netw. 129 (2) (2017) 572–584.
[55] M.E. Khanouche, Y. Amirat, A. Chibani, M. Kerkar, A. Yachir, Energy-centered and QoS-aware services selection for internet of things, IEEE Trans. Autom. Sci. Eng. 13 (3) (2016) 1256–1269.
[56] M. Antonini, S. Cirani, G. Ferrari, P. Medagliani, M. Picone, L. Veltri, Light weight multicast forwarding for service discovery in low-power IoT networks, in 22nd International Conference on Software, Telecommunications and Computer Networks (SoftCOM), 2014, pp. 133–138.
[57] Y. Jin, S. Gormus, P. Kulkarni, M. Sooriyabandara, Content centric routing in IoT networks and its integration in RPL, Comput. Commun. 89 (2016) 87–104.
[58] H. Fotouhi, D. Moreira, M. Alves, mRPL: boosting mobility in the internet of things, Ad Hoc Networks 26 (2015) 17–35.
[59] Y. Tian, R. Hou, An improved AOMDV routing protocol for internet of things, in International Conference on Computational Intelligence and Software Engineering, 2010, pp. 1–4.
[60] T. Qiu, Y. Lv, F. Xia, N. Chen, J. Wan, A. Tolba, ERGID: an efficient outing protocol for emergency response internet of things, J. Network Comput. Appl. 72 (2016) 104–112.
[61] N. Gozuacik, S. Oktug, Parent-aware routing for IoT networks, in Internet of Things, Smart Spaces, and Next Generation Networks and Systems. ruSMART 2015, NEW2AN 2015, 2015, pp. 23–33.
[62] Y. Wei, J. Wang, J. Wang, A Delay/disruption tolerant routing algorithm for IoT in harsh environment, in 6th International Conference on Intelligent Networks and Intelligent Systems (ICINIS), 2013, pp. 143–146.
[63] C.H. Barriquello, G.W. Denardin, A. Campos, A geographic routing approach for IPv6 in large-scale low-power and lossy networks, Comput. Electr. Eng. 45 (2015) 182–191.
[64] K. Q. AbdelFadeel, K. Elsayed, 6LoWDIS: a lightweight service discovery protocol for 6LoWPAN, in IEEE International Conference on Communications Workshops (ICC), 2016, pp. 284–289.
[65] T. Qiu, X. Liu, L. Feng, Y. Zhou, K. Zheng, An efficient tree-based self-organizing protocol for internet of things, IEEE Access 4 (2016) 3535–3546.
[66] L. Ngqakaza, A. Bagula, Least Path interference beaconing protocol (LIBP): a Frugal Routing Protocol for the Internet-of-Things, Wired/Wireless Internet Communications. WWIC 2014, 2014, pp. 148–161.
[67] S. Chelloug et al., Energy-efficient content-based routing in internet of things, J. Comput. Commun. 3 (12) (2015) 9.
[68] S. Misra, A. Gupta, P.V. Krishna, H. Agarwal, M.S. Obaidat, An adaptive learning approach for fault-tolerant routing in internet of things, in IEEE Wireless Communications and Networking Conference (WCNC), 2012, pp. 815–819.
[69] N.N. Srinidhi, S.D. Kumar, R. Banu, Internet of things for neophytes: a survey, international conference on electrical, electronics, communication, computer, and optimization techniques (ICEECCOT), 2017, pp. 234–242.
[70] Wi-FiAlliance, Wi-Fi Alliance Introduces Low Power Long Range Wi-Fi HaLow. URL https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-low-power-long-range-wi-fi-halow.
[71] J. Azevedo, F. Santos, M. Rodrigues, L. Aguiar, Sleeping zigbee networks at the application layer, IET Wireless Sen. Syst. 4 (1) (2013) 35–41.
[72] L. Alliance, LoRa Alliance Technology. URL https://www.lora-alliance.org/What-Is-LoRa/Technology.
[73] A. Gomez-Goiri, I. Goiri, D., Lopez-de Ipina, Energy-Aware Architecture for Information Search in the Semantic Web of Things, Int. J. Web Grid Serv. 6 10 (3) (2014) 192–217.
[74] J. Thriveni, K. Vishwanath, K. Venugopal, L. Patnaik, Probabilistic average energy flooding to maximize lifetime of mobile, Ad Hoc Networks (2007) 65–68.
[75] H. Wang, M. Xi, J. Liu, C. Chen, Transmitting IPv6 packets over bluetooth low energy based on BlueZ, 2013, in 15th International Conference on Advanced Communications Technology (ICACT), pp. 72–77.
[76] N. Kaur, S.K. Sood, An energy-efficient architecture for the internet of things (IoT), IEEE Syst. J. 11 (2017) 796–805.
[77] O.U. Akgul, B. Canberk, Self-organized things (SoT): an energy efficient next generation network management, Comput. Commun. 74 (2016) 52–62.
[78] C.H. Liu, J. Fan, J.W. Branch, K.K. Leung, Toward QoI and energy-efficiency in internet-of-things sensory environments, IEEE Trans. Emerging Top. Comput. 2 (4) (2014) 473–487.
[79] J.-J. Chen, J.-M. Liang, Z.-Y. Chen, Energy-Efficient uplink radio resource management in LTE-advanced relay networks for internet of things, in International Wireless Communications and Mobile Computing Conference (IWCMC), 2014, pp. 745–750.
[80] S. Rani, R. Talwar, J. Malhotra, S.H. Ahmed, M. Sarkar, H. Song, A novel scheme for an energy efficient internet of things based on wireless sensor networks, Sensors 15 (11) (2015) 28603–28626.
[81] Y.-W. Kuo, L.-D. Chou, Power saving scheduling scheme for internet of things over LTE/LTE-advanced networks, Mobile Inform. Syst. (2015).
[82] J. Tang, Z. Zhou, J. Niu, Q. Wang, An energy efficient hierarchical clustering index tree for facilitating time-correlated region queries in the internet of things, J. Network Comput. Appl. 40 (2014) 1–11.
[83] S. Abdullah, K. Yang, An energy efficient message scheduling algorithm considering node failure in IoT environment, Wireless Pers. Commun. 79 (3) (2014) 1815–1835.
[84] Z. Zhou, J. Tang, L.-J. Zhang, K. Ning, Q. Wang, EGF-tree: an energy-efficient index tree for facilitating multi-region query aggregation in the internet of things, Pers. Ubiquitous Comput. 18 (4) (2014) 951–966.
[85] J. Luo, D. Wu, C. Pan, J. Zha, Optimal energy strategy for node selection and data relay in WSN-based IoT, Mobile Networks Appl. 20 (2) (2015) 169–180.
[86] X. Tang, X. Niu, S. Ali, Research on energy-aware topology strategy based on wireless sensor in internet of things, Int. J. Comput. Intell. Syst. 7 (6) (2014) 1137–1147.
[87] S. Tozlu, M. Senel, W. Mao, A. Keshavarzian, Wi-Fi enabled sensors for internet of things: a practical approach, IEEE Commun. Mag. 50 (6) (2012) 134–143.
[88] A. Betzler, C. Gomez, I. Demirkol, J. Paradells, CoAP Congestion Control for the Internet of Things, 2016.
[89] Y. Liu, Z. Chen, X. Lv, F. Han, Multiple layer design for mass data transmission against channel congestion in IoT, Int. J. Commun. Syst. 27 (8) (2014) 1126–1146.
[90] M.A. Rahman, M.N. Kabir, S. Azad, J. Ali, On mitigating Hop-to-hop congestion problem in IoT enabled intra-vehicular communication, in 4th International Conference on Software Engineering and Computer Systems (ICSECS), 2015, pp. 213–217.
[91] Y. Park, S. Kim, Game-based data offloading scheme for IoT system traffic congestion problems, EURASIP J. Wireless Commun. Netw. (2015).
[92] J.-L. Chen, H.-C. Hsieh, Y. T. Larosa, Congestion control optimization of M2M in LTE networks, in 15th International Conference on Advanced Communications Technology (ICACT), 2013, pp. 823–827.
[93] Y. Pan, Y. Li, J. Zhang, Congestion-aware data acquisition for internet of things, in Proceedings of 2014 International Conference on Cloud Computing and Internet of Things, 2014, pp. 131–134.
[94] A.P. Castellani, M. Rossi, M. Zorzi, Back pressure congestion control for CoAP/6LoWPAN networks, Ad Hoc Networks 18 (2014) 71–84.
[95] A. Betzler, C. Gomez, I. Demirkol, J. Paradells, CoCoA+: an advanced congestion control mechanism for CoAP, Ad Hoc Networks 33 (2015) 126–139.
[96] R. K. Lam, K.-C. Chen, Congestion control for M2M traffic with heterogeneous throughput demands, in IEEE Wireless Communications and Networking Conference (WCNC), 2013, pp. 1452–1457.
[97] H.A. Al-Kashoash, Y. Al-Nidawi, A.H. Kemp, Congestion-aware RPL for 6L0WPAN networks, in Wireless Telecommunications Symposium (WTS), 2016, pp. 1–6.
[98] J. Huang, D. Du, Q. Duan, Y. Sun, Y. Yin, T. Zhou, Y. Zhang, Modeling and analysis on congestion control in the internet of things, in IEEE International Conference on Communications (ICC), 2014, pp. 434–439.
[99] J. Sterle, U. Sedlar, M. Rugelj, A. Kos, M. Volk, Application-driven OAM framework for heterogeneous IoT environments, Int. J. Distribut. Sensor Netw. (2016).
[100] F. Ganz, P. Barnaghi, F. Carrez, Information abstraction for heterogeneous real world internet data, IEEE Sens. J. 13 (10) (2013) 3793–3805.
[101] M. Amadeo, C. Campolo, A. Iera, A. Molinaro, Named data networking for IoT: an architectural perspective, in European Conference on Networks and Communications (EuCNC), 2014, pp. 1–5.
[102] W. Kim, Adaptive resource scheduling for dual connectivity in heterogeneous IoT cellular networks, Int. J. Distribut. Sensor Netw. (2016).
[103] M. Surligas, A. Makrogiannakis, S. Papadakis, Empowering the IoT Heterogeneous Wireless Networking with Software Defined Radio, 2015, pp. 1–5.

[104] L. Zhang, An IOT system for environmental monitoring and protecting with heterogeneous communication networks, in 6th International ICST Conference on Communications and Networking in China (CHINACOM), 2011, pp. 1026–1031.
[105] S.M. Oteafy, F. M. Al-Turjman, H.S. Hassanein, Pruned adaptive routing in the heterogeneous internet of things, in IEEE Global Communications Conference (GLOBECOM), 2012 pp. 214–219.
[106] J. Guo, P. Orlik, K. Parsons, K. Ishibashi, D. Takita, Resource aware routing protocol in heterogeneous wireless machine-to-machine net-works, in IEEE Global Communications Conference (GLOBECOM), 2015, pp. 1–6.
[107] E. Jung, I. Cho, S.M. Kang, IoTSilo: the agent service platform sup-porting dynamic behavior assembly for resolving the heterogeneity of IoT, Int. J. Distribut. Sensor Netw. 10 (1) (2014).
[108] P. Misra, Build a Scalable Platform for High-Performance.URL http://www.tcs.com/SiteCollectionDocuments/About%20TCS/Scalability-IoT-Applications-0616.pdf.
[109] M.P. Pawlowski, A.J. Jara, M.J. Ogorzalek, Compact extensible authentication protocol for the internet of things: enabling scalable and efficient security commissioning, Mobile Inform. Syst. (2015).
[110] A.J. Jara, V.P. Kafle, A.F. Skarmeta, Secure and scalable mobility management scheme for the internet of things integration in the future internet architecture, Int. J. Ad Hoc Ubiquitous Comput. 13 (4) (2013) 228–242.
[111] E. Cerritos, F.J. Lin, D. de la Bastida, High scalability for cloud-based IoT/M2M systems, in IEEE International Conference on Communications (ICC), 2016, pp. 1–6.
[112] A. Bader, M.-S. Alouini, Blind cooperative routing for scalable and energy-efficient internet of things, in IEEE Globecom Workshops (GC Wkshps), 2015, pp. 1–6.
[113] M. Kovatsch, M. Lanter, Z. Shelby, Californium: scalable cloud services for the internet of things with CoAP, in International Conference on the Internet of Things (IOT), 2014, pp. 1–6.
[114] J. Jermyn, R.P. Jover, I. Murynets, M. Istomin, S. Stolfo, Scalability of machine to machine systems and the internet of things on LTE mobile networks, in IEEE 16th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2015, pp. 1–9.
[115] A. Saxena, P. Duraisamy, V. Kaulgud, SMAC: Scalable access control in IoT, in IEEE International Conference on Cloud Computing in Emerging Markets (CCEM), 2015, pp. 169–176.
[116] S. Capone, R. Brama, N. Accettura, D. Striccoli, G. Boggia, An energy efficient and reliable composite metric for RPL organized networks, in 12th IEEE International Conference on Embedded and Ubiquitous Computing, 2014, pp. 178–184.
[117] D. Kyriazis, T. Varvarigou, Smart, autonomous and reliable internet of things, Procedia Comput. Sci. 21 (2013) 442–448.
[118] H.C. Pohls, V. Angelakis, S. Suppan, K. Fischer, G. Oikonomou, E.Z. Tragos, R.D. Rodriguez, T. Mouroutis, RERUM: Building a Reliable IoT upon Privacy-and Security-Enabled Smart Objects, in IEEE Wireless Communications and Networking Conference Workshops (WCNCW), 2014, pp. 122–127.
[119] D. Macedo, L. A. Guedes, I. Silva, A Dependability evaluation for internet of things incorporating redundancy aspects, in Proceedings of the 11th IEEE International Conference on Networking, Sensing and Control, 2014, pp. 417–422.
[120] L. Li, Z. Jin, G. Li, L. Zheng, Q. Wei, Modeling and Analyzing the reliability and cost of service composition in the IoT: a probabilistic approach, in IEEE 19th International Conference on Web Services, 2012, pp. 584–591.
[121] N. Maalel, E. Natalizio, A. Bouabdallah, P. Roux, M. Kellil, Reliability for emergency applications in internet of things, in IEEE International Conference on Distributed Computing in Sensor Systems, 2013, pp. 361–366.
[122] J. Kempf, J. Arkko, N. Beheshti, K. Yedavalli, Thoughts on reliability in the internet of things, in Interconnecting smart objects with the Internet workshop, 1, 2011, pp. 1–4.
[123] J.-M. Liang, J.-J. Chen, H.-H. Cheng, Y.-C. Tseng, An energy-efficient sleep scheduling with QoS consideration in 3GPP LTE-advanced networks for internet of things, IEEE J. Emerging Sel. Top. Circuits Syst. 3 (1) (2013) 13–22.
[124] E. Piri, J. Pinola, Performance of LTE uplink for IoT backhaul, in 13th IEEE Annual Consumer Communications & Networking Conference (CCNC), 2016, pp. 6–11.
[125] R. Duan, X. Chen, T. Xing, A QoS Architecture for IoT, in International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing, 2011, pp. 717–720.
[126] L. Li, S. Li, S. Zhao, QoS-aware scheduling of services-oriented internet of things, IEEE Trans. Ind. Inf. 10 (2) (2014) 1497–1505.
[127] G. Vithya, B. Vinayagasundaram, QOS by priority routing in internet of things, Res. J. Appl. Sci., Eng. Technol. 8 (21) (2014) 2154–2160.
[128] I. Awan, M. Younas, W. Naveed, Modelling QoS in IoT applications, in 17th International Conference on Network-Based Information Systems, 2014, pp. 99–105.
[129] Z. Ming, M. Yan, QoS-aware computational method for IoT composite service, J. China Univ. Posts Telecommun. 20 (2013) 35–39.
[130] M. Aazam, M. St-Hilaire, C.-H. Lung, I. Lambadaris, mefore: QoE based resource estimation at fog to enhance QoS in IoT, in 23rd International Conference on Telecommunications (ICT), 2016, pp. 1–5.
[131] T. Kothmayr, C. Schmitt, W. Hu, M. Brünig, G. Carle, DTLS based security and two-way authentication for the internet of things, Ad Hoc Networks 11 (8) (2013) 2710–2723.
[132] P. L. R. Chze, K. S. Leong, A secure multi-hop routing for IoT communication, in IEEE World Forum on Internet of Things (WF-IoT), 2014, pp. 428–432.
[133] S. Kumari, M. Karuppiah, A.K. Das, X. Li, F. Wu, N. Kumar, A secure authentication scheme based on elliptic curve cryptography for IoT and cloud servers, J. Supercomputing (2017) 1–26.
[134] O. Garcia-Morchon, S. L. Keoh, S. Kumar, P. Moreno-Sanchez, F. Vidal-Meca, J. H. Ziegeldorf, Securing the IP-based internet of things with HIP and DTLS, in Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks, 2013, pp. 119–124.
[135] R. Tanuja, Y. Shruthi, S. Manjula, K. Venugopal, L. Patnaik, Token based privacy preserving access control in wireless sensor networks, in International Conference on Advanced Computing and Communications (ADCOM), 2015, pp. 45–50.
[136] S. Raza, L. Wallgren, T. Voigt, SVELTE: real-time intrusion detection in the internet of things, Ad Hoc Networks 11 (8) (2013) 2661–2674.
[137] H. Perrey, M. Landsmann, O. Ugus, T.C. Schmidt, M. Wahlisch, TRAIL: topology authentication in RPL, arXiv (2016). preprint arXiv:1312.0984.
[138] P. Pongle, G. Chavan, Real time intrusion and wormhole attack detection in internet of things, Int. J. Comput. Appl. (9) (2015) 121.
[139] Q. M. Ashraf, M. H. Habaebi, G. R. Sinniah, J. Chebil, Broadcast Based Registration Technique for Heterogenous Nodes in the IoT., 2014.
[140] P. Kasinathan, C. Pastrone, M. A. Spirito, M. Vinkovits, Denial-of-service detection in 6lowpan based internet of things, in IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), 2013, pp. 600–607.
[141] Smart networked objects and internet of things, white paper published by association instituts carnot, 2011.
[142] W. Shang, Y. Yu, R. Droms, L. Zhang, Challenges in IoT Networking via TCP/IP Architecture, Tech. Rep., NDN Project, Tech. Rep. NDN-0038 (2016).
[143] M. Elhoseny, A.E. Hassanien, Extending Homogeneous WSN lifetime in dynamic environments using the clustering model, in Proceedings of the International MultiConference of Engineers and Computer Scientists, 2019, pp. 73–92.
[144] S. Manjula, C. Abhilash, K. Shaila, K. Venugopal, L. Patnaik, Performance of AoDV Routing Protocol using Group and Entity Mobility Models in Wireless Sensor Networks 2, 2008, pp. 1212–1217.
[145] Y.-K. Hsiao, Y.-W. Lin, A Mobility management scheme for internet of things, in Mobile, Ubiquitous, and Intelligent Computing. Lecture Notes in Electrical Engineering, 2014, pp. 569–575.
[146] S.M. Ghaleb, S. Subramaniam, Z.A. Zukarnain, A. Muhammed, Mobility management for IoT: a survey, EURASIP J. Wireless Commun. Networking 2016 (1) (2016) 1–25.
[147] P. Porambage, M. Ylianttila, C. Schmitt, P. Kumar, A. Gurtov, A.V. Vasilakos, The quest for privacy in the internet of things, IEEE Cloud Computing 2 (2016) 36–45.
[148] D. Chasaki, C. Mansour, Security challenges in the internet of things, Int. J. Space-Based Situated Comput. 5 (3) (2015) 141–149.
[149] C. Lu, Overview of Security and Privacy Issues in the Internet of Things. URL http://www.cse.wustl.edu/~jain/cse574-14/ftp/security.pdf.
[150] L.K. Bysani, A.K. Turuk, A survey on selective forwarding attack in wireless sensor networks, in International Conference on Devices and Communications (ICDeCom), 2011, pp. 1–5.
[151] A. Liu, M. Dong, K. Ota, J. Long, PHACK: An Efficient Scheme for Selective Forwarding Attack Detection in WSNs, Sensors 15 (12) (2015) 30942–30963.
[152] P. Pongle, G. Chavan, A Survey: Attacks on RPL and 6LoWPAN in, IoT (2015) 1–6.
[153] V.P. Singh, S. Jain, J. Singhai, Hello flood attack and its counter-measures in wireless sensor networks, IJCSI Int. J. Comput. Sci. Issues 7 (3) (2010) 23–24.
[154] M. Barbeau, J. Hall, E. Kranakis, Detecting impersonation attacks in future wireless and mobile networks, in Secure Mobile Ad-hoc Networks and Sensors, 2006, pp. 80–95.
[155] F.-H. Tseng, L.-D. Chou, H.-C. Chao, A survey of black hole attacks in wireless mobile ad hoc networks, Hum. Cent. Comput. Inform. Sci. 1 (1) (2011).
[156] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, W. Zhao, A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications, IEEE Internet Things J. 4 (5) (2017) 1125–1142.
[157] C.-C. Chu, H.H.-C. Iu, Complex networks theory for modern smart grid applications: a survey, IEEE J. Emerging Sel. Top. Circuits Syst. 7 (2) (2017) 177–191.
[158] E. De Poorter, I. Moerman, P. Demeester, Enabling direct connectivity between heterogeneous objects in the internet of things through a network-service-oriented architecture, EURASIP J. Wireless Commun. Networking 1 (2011) 1–14.
[159] I. Ishaq, D. Carels, G.K. Teklemariam, J. Hoebeke, F.V.D. Abeele, E.D. Poorter, I. Moerman, P. Demeester, IETF standardization in the field of the internet of things (IoT): a survey, J. Sens. Actuator Networks 2 (2) (2013) 235–287.
[160] Altimeter, Interoperability: The Challenge Facing the IoT. URL https://www.prophet.com/thinking/2014/02/interoperability-the-challenge-facing-the-internet-of-things/.
[161] S. E. Karen Rose, L. Chapin, The Internet of Things An Overview. URL http://www.internetsociety.org/sites/default/files/ISOC-IoT-Overview-20151022.pdf.
[162] M. Gomes, R. da Rosa Righi, C. A. da Costa, Internet of things scalability: analyzing the bottlenecks and proposing alternatives, in 6th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2014, pp. 269–276.