A Systematic Review of IoT Communication Strategies for an Efficient Smart Environment

Alireza Souri1*, Aseel Hussien[2] , Mahdi Hoseyninezhad[1] and Monire Norouzi[1]

1Young Researchers and Elite Club, Islamshahr Branch, Islamic Azad University, Islamshahr, Iran

2Department of the Built Environment, Liverpool John Moores University

*Corresponding E-mail: a.souri@srbiau.ac.ir Co-author Email: a.hussien@ljmu.ac.uk,

mahdi74.hoseyni@outlook.com, m.norouzi@iiau.ac.ir

Abstract. The massive increase in actuators, industrial devices, health-care devices, and sensors, have led to the implementation of the Internet of Things (IoT), fast and flexible information technology communication between the devices. As such, responding to the needs in speedily way, and matching the smart services with modified requirements, IoT communications have facilitated the interconnections of things between applications, users, and smart devices. In order to gain extra advantage of the numerous services of the Internet. In this paper, the authors first, provided a comprehensive analysis on the IoT communication strategies and applications for smart devices based on a Systematic Literature Review (SLR). Then, the communication strategies and applications are categorized into four main topics including device to device, device to cloud, device to gateway and device to application scenarios. Furthermore, a technical taxonomy is presented to classify the existing papers according to search-based methodology in the scientific databases. The technical taxonomy presents five categories for IoT communication applications including monitoring-based communications, routing-based communications, health-based communications, Intrusion-based communications, and resource-based communications. The evaluation factors and infrastructure attributes are discussed based on some technical questions. Finally, some new challenges and forthcoming issues of future IoT communications are presented.

Keywords. Internet of Things (IoT), communication strategy, application, smart device, systematic review.

1. Introduction

The Internet of Things (IoT) is a significant paradigm where smart devices are interconnected and able to exchange information and resources with each other according to intelligent applications of users. IoT communications are capable of collecting, integrating, processing and transmitting an analysis of exchanged information automatically to make the system intelligent [1]. In addition, the IoT devices have been applied to the different topics such as smart city, industry 4.0, smart home-care, intelligent military, intelligent manufacturing, healthcare and medical systems [2, 3], intelligent transportation and etc. therefore, in order to realize the effective procedure of the IoT development, a reliable connection network of IoT is required for each smart device or actuator to be transmitted to its application and usefulness gateway directly or ultimately [4, 5].

Besides, the existing communication strategies provide a set of network utilizations, which are used to associate modern computers or mobile devices and other smart policies, by implementing a specific topology and transfer technology to permit operators for interconnecting and sharing activated resources in the IoT environment. Nevertheless, IoT communications have a vital challenge in lifetime users' compatibility as its play a key role to facilitate smart devices [6]. According to the prominence of IoT communications for smart devices, and applied applications, the presentation of a comprehensive review is essential, which helps the researchers' requirements in this research topic. In support of this notion, Tayeb et al. [7] and Zaidan et al. [8] presented two survey articles on the IoT frameworks in industrial environments and smart city respectively by focusing on the existing case studies and applied algorithms. Also, some review papers such as Akpakwu et al. [9] and Montori et al. [10] have proposed a survey on the 5G and machine to machine wireless communication strategies for IoT environments respectively.

To the best of our knowledge, this paper is the first attempt for a systematic review on IoT-based communication strategies. Consequently, this research study provides a Systematic Literature Review (SLR) method for the existing IoT communication strategies for smart devices and applied applications comprehensively. This research further, categorizes the current and forthcoming communication strategies in five main classes including; monitoring-based communications, routing-based communications, health-based communications, intrusion-based communications, and resource-based communications.

The key contributions of this research review are presented as follow:

- Providing a technical classification of the IoT communications strategies for smart devices and applied applications according to the existing challenges and the important subjects.
- Presenting a comprehensive analysis of the existing communications strategies based on the SLR method.
- Examining the important characteristics of the IoT communications strategies to enhance their efficiencies in forthcoming directions.
- Discussing the new challenges and forthcoming issues of future IoT communications that can be useful in the next future generation of the Internet.

Therefore, this research study is structured as follows: Section 2 presents a brief description of preliminaries and backgrounds of the IoT communications for smart devices and applications. Also, the selection strategy implemented in this research study is presented according to the SLR method. In Section 3, a technical taxonomy for classification of existing papers in the IoT communications strategies is presented. A brief summery and technical categorization of each related study are presented in the Section 3, whilst section 4 provides the comparison analysis and a discussion effort for the reviewed studies. Besides, Section 5 presents new challenges and forthcoming issues of future IoT communications. Finally, Section 6 concludes the paper.

2. Background

In this section the authors illustrate a brief summary of the IoT communication architecture, strategies, communications types, and technologies with some key attributes. Also, the authors presented the strategy implemented for the papers selection in order to find the best and suitable related research study for this review [11]. IoT refers to a set of actuators, smart devices, sensors that make up intelligent systems that can connect together using the infrastructure of the Internet [12]. Different IoT architectures have been proposed by different researchers, as such there is no constant IoT architecture [13].

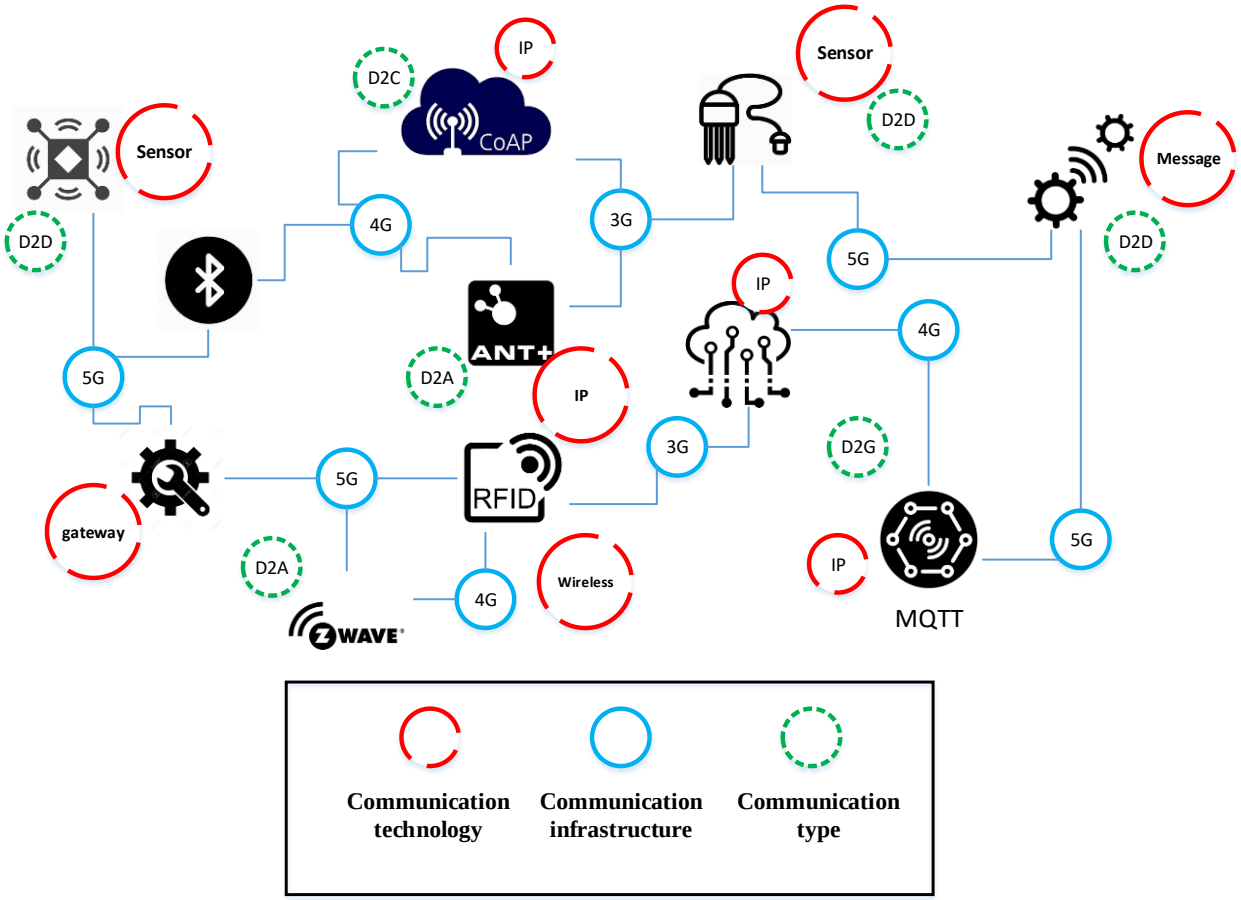

Figure 1. The communication features in IoT environment [14].

Based on Figure 1, there are four classical communication types for IoT environment that can be connected to anything at any time with any network topology and any service as follows [15, 16]:

- Device-to-Device (D2D) communication: provides more than two smart devices that communicate between each other directly without any application server using existing communication technologies such as IP technology, wireless technology, and sensor technology.
- Device-to-Application (D2A) communication: presents a safe user-centric connection between IoT applications and smart devices that have been embedded to the human life using content-centric, messaging technology, cloud technology and sensor technology.
- Device-to-Gateway (D2G) communication: Provides a secure connection between local gateway as a middleware service provider (such as smartphone or laptop) and the smart

devices with a translation method such as gateway technology, and messaging technology. Also, the smartphones as mobile-based IoT devices can be used as a gateway in the device to gateway communication type.

- Device-to-Cloud (D2C) communication: presents a directional interconnection between IoT devices and cloud service providers to transfer information and resources with controlling messages and sensors using existing communication technologies such as sensor technology, cloud-based technology, messaging technology, IP technology, and wireless technology [17]:

In order to connect the smart devices in IoT environment, some key technologies are applied such as, wireless technology, sensor technology, messaging technology, gateway technology, and IP technology [18, 19]. Besides, the communication types can have two main characteristics including application-wise or topology-wise.

Likewise, the IoT communication strategies are used for numerous scenarios in the human life for instance; medicine, ubiquitous, vehicle transportations, social communications, commercial efforts, education, military, industry, and home-care [20-22]. Also, there are famous communication infrastructures including, 3G, 4G and 5G cellular network technologies that communicate with mobile broadband services and IoT smart devices. Recently, 5G network technology has new paradigm for communicating smart IoT devices and cyber physical systems with high accuracy [23, 24].

3. IoT device communication strategies

In this section, we analyze existing research studies on the IoT communication strategies for efficient smart environments. First, we describe briefly, research selection strategy based on systematic literature review (SLR). Also, we present a technical taxonomy for categorization of the existing research studies.

3.1 Paper selection strategy

This research study adopts a SLR to identify the gap within the previous literature, which had not previously been investigated. In the first step, the existed string keywords “Internet of things” OR “IoT” AND “communication” AND “device” OR “machine” are searched in the Web. The

authors have restricted the search scope to research studies between 2014-Feb 2019 that completely emphasis on the IoT communications through smart devices written in English.

In the second step, the replicated papers, thesis, review and survey articles, book chapters, and non-index Web of science articles have been excluded. Finally, 38 research article have been considered to discuss for technical analysis. Figure 2 depicts a summery on the distribution of the published articles in scientific publishers by year. According to Table 1, to enhance quality of the research methodology in this review, just journal articles have been considered to analyze the IoT communication strategies.

According to the SLR method adopted, the authors, have designed Methodological Queries (MQ) based on the scope of the IoT communications strategies as follows:

- MQ 1: Which IoT communication strategies are applied in this literature?
- MQ 2: Which main scenarios are considered for IoT communication strategies?
- MQ3: Which communication type is provided for connection of IoT devices?
- MQ4: Which communication technologies are applied for the IoT devices?
- MQ5: What are the evaluation factors usually applied to the IoT communication strategies?
- MQ6: What are the forthcoming directions and open issues for IoT communication strategies?

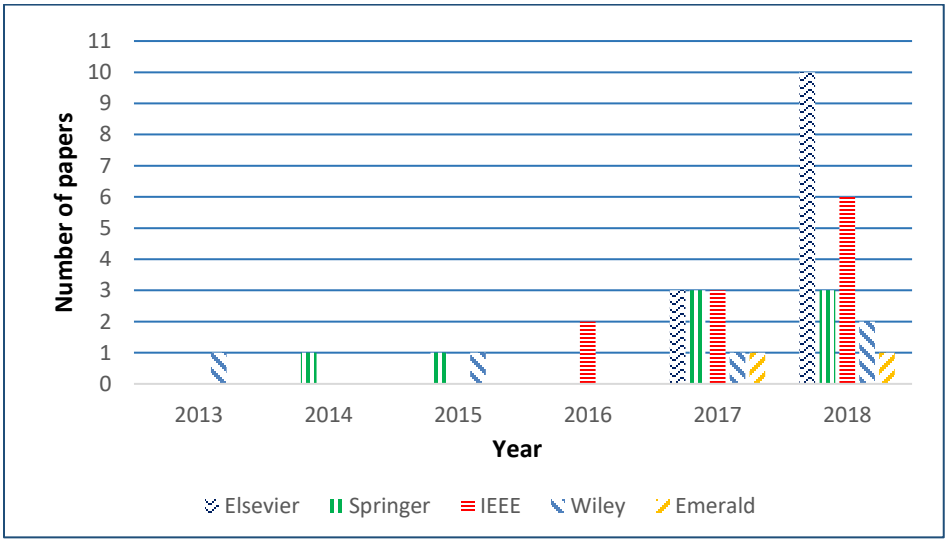

Figure 2. The percentage of research paper verity with publisher per year.

Table 1. Total founded research studies in the IoT communication papers

Database	Number of initial search	Relevant papers
Science Direct	825	13
Springer	1121	8
IEEE	1302	11
Wiley	423	5
Emerald	127	1
Total articles	38	

3.1 Analyzing existing research studies

According to Figure 3, this section illustrates a technical taxonomy for IoT communication strategies. The Authors categorize communication strategies into five main environments including monitoring-based communications, routing-based communications, health-based communications, intrusion-based communications, and resource-based communications.

Figure 3 provides a relationship between the communication technologies that cover by each IoT communication type. In order to analyze the IoT communication types of each environment, D2D, D2A, D2G, and D2C types are categorized to the next level. The monitoring-based communications include the D2D, D2A and D2C communication types that interconnect with sensor, wireless, and IP communication technologies between smart devices. In the routing-based communications, the authors have four sub-layers for the communication types including D2D, D2A and D2G communication types. These communication types interact with sensor, wireless, gateway and IP communication technologies between smart devices and users. The health-based communications [25, 26] contain the D2D and D2A communication types that interconnect with sensor, gateway, messaging and IP communication technologies between IoT devices, applications and users. As such, the intrusion-based communications include the D2A and D2C communication types that interconnect with sensor, wireless, messaging and IP communication technologies between smart devices. Finally, the resource-based communications include all of the D2D, D2A, D2G and D2C communication types by interconnecting on messaging, wireless and gateway communication technologies for intelligent devices and IoT applications.

3.1.1 Monitoring-based communications

Monitoring-based communication strategies present a high level discovery and screening for end to end devices, cloud providers and IoT applications that user can use some data transfer features such as video streaming management, measuring environmental aspects and natural resources, and density detection on the manufacturing and industrial equipment.

Zhou et al. [27] present a high risk Infrared malicious monitoring control for smart TV devices in IoT environment. In this remote control, a TV box platform has been designed and implemented to show the protecting the high risk attacks for improving security and bit error rate in the multimedia devices in IoT environment. This research suffers from a sequential converted channels to receive the existing messages between TV box and remote control to monitor the data transmission that the transmission time is increasing. While Hejselbaek et al. [28] provide a propagation-based monitoring system for Forest Terrain in IoT devices. The monitoring system was implemented to measure the organic and experimental models of forest destinations. The proposed monitoring system used wireless technology to estimation of response time, bandwidth factors in the environmental IoT devices. However, Kertesz et al. [29] present an android-based mobile simulation application to visualize and monitor the data management of IoT communication devices. The monitoring management is done with sensor-based technology to overcome the device management scalability with cost efficient approach. Some weaknesses of this research are as follows: (1) the gathering table of the sensors is very simple and restricted memory, (2) the routing methodology has not been illustrated between sensors that support the scalability of the monitoring data streams in IoT environment.

In another paper [26], Paul et al. proposed a graph-based communication model for dynamic and mobile smart devices in IoT environment to monitor and discover the optimum path and minimum energy, and cost between devices. The main defect of this research is that the authors ignored the battery life of sensors in a medical monitoring system with respect to simple routing protocol in the optimum path.

On the other hand, Wang et al. [31] present a self-adaptive and monitoring system to data access control using load-dispatching method in IoT environment. A load capacity method is applied to predict the load performance of each sensor node in the IoT communication strategy. To support a safety monitoring scenario, this research provided a dynamic load balancing method for

enhancing the data access control to decrease computation time, cost, and utilization in the IoT environment.

Table 2 depicts a technical analysis of some important metrics related to existing monitoring-based communications in the IoT environments. The D2D type has most usage for monitoring conditions in variant areas such as home-care, social networks, commercial, medical and industrial environments.

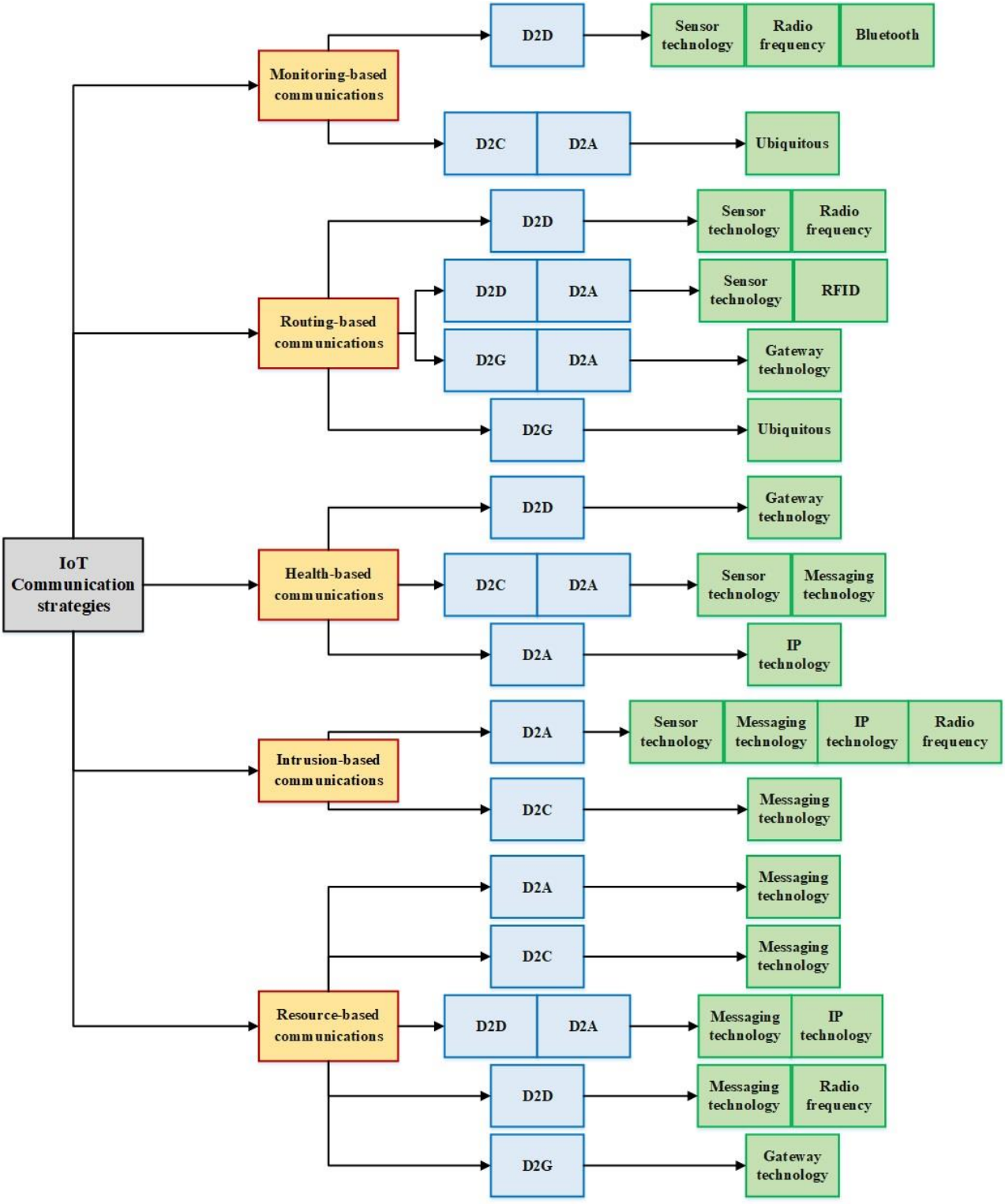

Figure 3. The proposed taxonomy for the IoT communication strategies.

Table 2. Comparison of the evaluation factors for the monitoring-based communications

Ref	Main context	IoT-based technology	IoT-based scenario	Communication type	Evaluation factors	Validation
[27]	High risk Infrared malicious monitoring control for smart TV	Wireless technology	Home	D2D	Security, bit error rate	Empirical
[28]	Propagation-based monitoring system for Forest Terrain	Wireless technology	Social	D2D	Response time, bandwidth	Case study
[29]	Android-based mobile simulation application to visualize and monitor the data management	Sensor technology	Commercial	D2D	Scalability, cost	Case study
[30]	Graph-based communication model for dynamic and mobile smart devices	Sensor technology	Medical	D2D	Energy, cost	Empirical
[31]	Self-adaptive and monitoring system to data access control	Sensor technology	Industry	D2C - D2A	Computation time, cost, and utilization	Case study

3.1.2 Routing-based communications

In the routing-based communication strategy, discovering a safe and optimal path is considered to manage some important aspects of IoT networks in routing problem such as traffic, energy consumption, packet delay, and response time. The authors have described an analytical comparison of existing approaches in this field as follows:

Debroy et al. [32] present an optimal spectrum-based routing protocol according to dynamic access communication management in IoT environments. The authors proposed a multi-hop routing

scenario to achieve a reachable connectivity between IoT devices with minimum energy consumption. The simulation results with MATLAB shows an efficient cost benefit and energy saving routing strategy for dynamic access communication devices. The main weakness of this work is that the authors have not considered a heterogonous environment to connect the smart devices in IoT platform.

Mukherjee et al. [33] present an on-the-fly routing mechanism for MANET in a smart city-based IoT environment. The authors proposed a hierarchical multi-level architecture to cover high mobility of routing mechanism in the static IoT environment. The experimental results were simulated using Omnet++ tool that presented low delay and high packet receiving rate with minimum energy consumption. The main defect of this paper is that the authors proposed a static device to device IoT environment for routing mechanism in MANET.

Sharma et al. [34], suggest a 5G-based routing discovery protocol for IoT devices in body area networks. An auto-flight vehicle scenario is presented to evaluate energy consumption of the routing discovery for mobile devices in IoT. A numerical analysis was evaluated for achieving the best performance of energy, cost, and delay factors using MATLAB and NS-2. The main weakness of this work is considering single auto-flight vehicle to connect the mobile devices in vehicular communications.

Bi et al. [35] develop a soccer robot system based on an enhanced routing discovery mechanism in IoT environment. A manual remote control was proposed to navigate the mobile sensor nodes in the game system. The mechanical perspective of the proposed robot was evaluated with a real platform in the IoT environment. The communications between devices were supported using a decision making system that navigates the routing discovery mechanism according to the activities of robot players for minimizing Energy, response time, and delay. The main weakness of this development is considering a manual remote control for navigating and routing discovery for robot system.

Chen et al. [36] present a new social-based routing method for multi-hop IoT communications to support probable trusted connectivity. This paper proposes a channel information status between the specified and unknown devices that evaluate trust probability, and distance rate factors according to a rank-based model. The statistical and numerical analysis were performed using Monte Carlo simulations. The main weaknesses of this research are as follows: (1) the routing

method with probable trusted connectivity is depend on randomized location of base stations. (2) If a base device station changes its location dynamically, the probable trusted connectivity cannot be supported with this routing method. (3) The computation time for routing method has not been discussed because when number of base stations are increased, the computation time is growth exponentially.

Cuka et al. [37] propose an opportunistic-based routing mechanism using fuzzy logic. Some evaluation factors such as response time, storage, energy and security have been compared with other algorithms. The main disadvantage of this work is omitting a dynamic device selection strategy for routing algorithm that is increases the overhead of IoT communications.

Table 3 shows a comparison analysis for existing routing-based communications in the IoT environments. The commercial scenarios have most usage for routing algorithms based on radio and sensor technologies as communication technologies.

Table 3. Comparison of the evaluation factors for the routing-based communications

Ref	Main context	IoT-based technology	IoT-based scenario	Communication type	Evaluation factors	Validation
[32]	Dynamic spectrum-based multi-hop routing protocol	Wireless technology and Sensor technology	Commercial	D2D	Energy consumption	Empirical
[33]	Hierarchical routing architecture in MANET	Gateway-based	Commercial	D2G – D2A	Delay, packet receiving rate, minimum energy consumption.	Case study
[34]	5G-based routing discovery protocol in body area networks	Sensor technology	Vehicle	D2A	Energy, cost, delay	Empirical
[35]	Soccer robot system	Sensor technology and wireless technology	Commercial	D2D – D2A	Energy, response time, and delay	Empirical
[36]	Social-based routing method for multi-hop IoT communications	Wireless technology	Social	D2D	Trust probability, and distance rate	Empirical

[37]	Opportunistic-based routing mechanism using fuzzy logic	Gateway-based	Ubiquitous	D2G	Response time, storage, energy and security	Case study

3.1.3 Health-based communications

Health-based communication strategies are related to the medical environments that use IoT technology to manage the health-care information and medical equipment. Existing research studies in this topic are explain and discuss as follows:

Santamaria et al. [38] present a message queuing-based wearable device for body sensor area network in IoT environment. The authors proposed a fuzzy logic method to show the body activity recognition by filtering and refinement of data that are gathered form IoT environment. The experimental results have been evaluated using a real case measurement with classification and clustering methods to decrease the error rate of recognition and energy consumption of IoT nodes. This research has ignored the transfer cost for gathering data from IoT devices in smart environment as the main weakness.

Woo et al. [39] propose a reliable-based personal healthcare scenario to evaluate fault-tolerant medical information services in IoT environment. The applied reliable-based scenario used a baseline configuration for showing the daisy chain of recovery messages in backup of medical information. The proposed scenario could recover the medical information from faulty messages in gateway. One of the main weaknesses of this research is that the authors have not illustrated a time period for estimation of fault messages in the backup procedure.

Bae [40] evaluates a verification method on the user healthcare information for analyzing existing attacks in the IoT medical communications. In this research, a privacy protection scenario was proposed using inter-device communication level that to avoid each impostor’s hacking in a safe wireless communication environment. The statistical testing was carried out using Casper specification rules in Failures-Divergences Refinement (FDR) checker tool. The experimental results showed that the proposed method satisfied a safety and deadlock-free conditions in the IoT medical device environment. The main weakness of this testing is that the author proposed a

sequential operators for verifying the authentication of privacy attacks in the IoT device communications.

Table 4 illustrates a side-by-side evaluation for existing health-based communications in the IoT environments. The medical scenario have just usage for health conditions based on IP and sensor technologies as communication technologies.

Table 4. Comparison of the evaluation factors for the health-based communications

Ref	Main context	IoT-based technology	Communication type	Evaluation factors	Validation
[38]	Message queuing-based wearable device for body sensor area network	Sensor technology, messaging technology	D2C – D2A	Error rate, Energy	Case study
[39]	Reliable-based personal healthcare to evaluate fault-tolerant medical information	Gateway-based	D2D	Reliability, fault tolerant	Case study
[40]	Verification method on the user healthcare information	IP technology	D2A	deadlock-free, safety	Empirical

3.1.4 Intrusion-based communications

In the intrusion-based communication strategy, some safety factors such as security, trust and privacy are considered to support a safe interaction between IoT applications and cloud providers. In this subsection the authors have explained existing research studies in this topic as follows:

Matheu-García et al. [41] present a secure framework based on risk assessments and testing to communicate the smart devices in IoT deployments. This research proposes a three-level security valuation including identification, estimation, and evaluation. After applying three-level valuation to the communication of IoT devices, a three-level testing evaluation is specified for validating secure monitoring method including design and implementation, maintenance, analysis and

summary. To map the three-level security valuation on the three-level testing evaluation methods, a certification framework is presented according to weaknesses of IoT devices, relations between devices and independent vulnerabilities of the smart devices in IoT technology. The experimental results showed efficiency, execution time and packet error rate factors for proposed framework. The main weakness of this research is omitting multiple aggregations of risk assessments for IoT devices to support scalability and more efficiency.

Mukherjee et al. [42] provide a flexible-based security middleware approach using session resumption method in IoT end-to-end communications. Some critical factors including power management, memory and energy consumption, network bandwidth and resource-awareness are evaluated according to the proposed secure IoT middleware approach. To discover the optimal security structure selection, the authors have used machine learning methods that evaluate composition of different protocol components in offline and online levels. In the experimental results, some scenarios have been tested using different virtual machines to decrease memory and energy consumption. The main weakness of this research is that the author used a simple K-means clustering algorithm to categorization of the flexible-based secure decider components in IoT communications.

Randhawa et al. [43] present a novel energy-aware method based on the authenticated encryption method in the IoT communications. The authors proposed a combinatorial offloading secure operations to evaluate the energy consumption, memory saving and low computation time factors. In this research, the data congestion has not been considered to combination of secure operations in the authenticated encryption method as a main weakness.

Yang et al. [44] propose a cyberspace-based automatic fingerprint method to detect vulnerable IoT devices using neural network algorithm. To predict the real experiments, three layers have been designed for detecting smart devices in the cyberspace IoT communications. According to classification results, the proposed automated fingerprinting method was outperform than other works based recall, precision, and error rate factors. The main defect of this research is that the authors have not considered a dynamic attack for evaluating the vulnerable IoT devices.

Dao et al. [45] present a secure authenticated key agreement method based on peer to peer communication in the Lightweight IoT devices. The proposed authenticated method is based on a social network scenario including user convenience in some attack levels. The experimental results

provided some critical factors such as storage management, probability, cost and response time to improve the feasibility of the proposed authenticated key agreement method. The main weakness of this paper is omitting the authenticated transfer rate between multi-users that effects on the communication cost.

Jin et al. [46] propose a ring learning-based encryption protocol using homomorphic user authentication management in IoT environment. The proposed protocol supports safety and security with decreasing response time and space complexity for decoding data transfer procedure. The simulation results have been evaluated with Eclipse tool with a message passing technology. The main defect of this paper is that the authors could not provide safety condition for a scalable IoT environment with restricted devices.

Lee et al. [47] present a trust-based mobile protection approach with supporting domain isolation in the IoT environment. This approach uses a secure execution engine to support secure domain in authentication and access control. Also, to manage the mobile security of existing devices, a secure storage and key management scenario have been provided for encrypting and decoding resource safely. The experimental results showed that the file size and execution time factors of the proposed approach are lower than other approaches. The main weakness of this study is that the overhead is increased when the number of messages are increased.

Patil et al. [48] propose cryptography-based virtualization method to evaluate data congestion and interconnected nodes using neural network in IoT environment. The experimental results have been evaluated with MATLAB that reduced delay and response time. The main disadvantage of this study is ignoring the classification of unexpected communication nodes to normalize the congestion value.

Bagci et al. [49] propose a secure-based IP combination approach to storage and transfer safe resources using datagram transportation layer in IoT infrastructure. The proposed approach satisfies some quantities such as saving safe resources and reduce memory consumption in the software and hardware encryption methods.

Køien [50] propose a service access-based authentication method using random provisional personality structure in the IoT communications. This method supports user location privacy according to various requested services. The authors could manage proposed privacy using

provisional access key method in some specification principles. The experimental analysis showed that the existing principles have been satisfied with the provisional access key method to provide user privacy. The main defect of this research is that the authors have not considered an implementation effort for evaluating proposed method in some real scenarios with respect to improve the execution time and security conditions.

Table 5 shows a technical analysis for existing intrusion-based communications in the IoT environments. The commercial scenarios have most usage for intrusion algorithms based on messaging technologies as communication technologies in the D2A communication type.

Table 5. Comparison of the evaluation factors for the intrusion-based communications

Ref	Main context	IoT-based technology	IoT-based scenario	Communication type	Evaluation factors	Validation
[41]	Secure framework based on risk assessments	Messaging technology	Ubiquitous	D2A	Successibility, execution time and packet error rate	Empirical
[42]	Flexible-based security middleware using session resumption	Messaging technology	Ubiquitous	D2C	memory and energy consumption	Case study
[43]	Energy-aware method based on the authenticated encryption method	Wireless technology	Ubiquitous	D2A	Memory, computation time and energy	Case study
[44]	Cyberspace-based automatic fingerprint method	IP technology	Industry	D2A	Recall, precision, and error rate	Empirical
[45]	Secure authenticated key agreement method based on	Messaging technology	Social	D2A	Storage management, probability, cost and response time	Case study

	peer to peer communication					
[46]	Ring learning-based encryption protocol using homomorphic authentication	Messaging technology	Ubiquitous	D2C	Safety, security, response time, space complexity	Case study
[47]	Trust-based mobile protection approach with supporting domain isolation	Messaging technology	Ubiquitous	D2A	File size and execution time	Empirical
[48]	Cryptography-based virtualization method to evaluate data congestion	Messaging technology	Ubiquitous	D2A	Delay and response time	Case study
[49]	secure-based IP combination approach to storage and transfer safe resources	IP technology	Ubiquitous	D2A	Memory consumption	Case study
[50]	Service-based authentication using random structure	IP technology	Commercial	D2A	Privacy	Case study

3.1.5 Resource-based communications

The resource-based communication strategies provide optimal resource management for smart devices, cloud service providers, IoT applications, user-centric applications and gateways. In the resource-based communication strategy, some computing and communicating problems have been discussed such as resource allocation, scheduling, wireless mobile transferring, and load balancing and vehicular communications.

Khaled et al. [51] propose a RESTFul-based translator framework to manage resource transferring based on Atlas communication protocol in IoT environment. This framework provides a feasible

energy consumption rate for the smart spaces in the heterogeneous Atlas IoT communication. The scalability and cost factors have been evaluated in this study using Eclips environment. On the other hand, Yamada et al. [52] propose a resource traffic management approach based on communication timing method for MANET in cellular IoT devices. This approach enhances latency of communication devices based on evaluating each utility function for IoT devices.

Chen et al. [53] present an energy-aware microscopic communication method for IoT sensors. The authors proposed a millimeter scheme wireless communication structure to evaluate resources sharing between 3D antennas with high estimation rate. Saving battery life and energy reduction are main advantages of this approach. Of course, the scalability and precision have not been investigated in this method when the number of sensors are increased in the IoT environment.

Furthermore, Ito et al. [54] present a state reduction method to utilize time division and cost benefit selection for status of the cellular IoT devices in 4G mobile communications. This method used a device triggering energy saving status to enhance the recovered applications reliability when a failure condition is occurred. The simulation results have been achieved with comparing some algorithms such as adaptive range, exponential binary and uniform range methods to minimize energy, execution time, and reliability using OMNET++. The main defect of this research is that the authors ignored the overhead of the resource transferring in the IoT environment.

Khaled et al. [55] develop a description language for specifying the smart things in the Web using Atlas IoT architecture. The experimental results have been investigated with IP smart things to manage computation time and energy consumption of applied resources in the IoT communications. The simplicity of the scenario programming to manage the applied resources with small environment is specified as a main weakness of this research.

Lianghai et al. [56] present cellular remote device clustering for saving battery life of smart transmission devices in the IoT environment. In this paper, the existing resources of the sensors are clustered based on packet size, battery capacity, energy consumption, distance rate and number of sensors. The experimental results have been achieved benefit batter life and resource availability for existing sensors.

Liu et al. [57] propose a cellular device to device resource allocation model for avoiding traffic congestion and energy reduction in the IoT green environment. The proposed resource allocation

model supports the local base station transition and minimization of energy consumption for dual battery utilization.

In Lv et al. [58] it was argued that, a QoS-based micro multiple-access resource allocation in the cellular IoT communications. The existing communication resources are transmitted via millimeter wave channels in the cellular IoT devices. The analytical experiments have been illustrated based on Monte Carlo simulation that include the probability of the pairing micro devices to guarantee the expected QoS factors such as execution time, density. The main weakness of this paper is that the authors have not been considered the communication cost between micro devices as a weight.

Moon et al. [59] present a random-access resource management approach for enhancing success ration of the IoT devices with minimum delay connectivity. This approach have provided channel estimation and blind decrypting for each resource transition in the IoT environment. The simulation results have been concluded with NS3 environment that evaluated access probability, ordinary delay and access throughput for each resource transmission. Ignoring congestion for the resource transition with high density can be specified as the main disadvantage of this paper.

Song et al. [60] propose a data propagation-based resource allocation method using twofold graph model in the IoT environment. This method provides a three-level method for paring IoT devices using a heuristic replace matching algorithm to decrease paring ratio, and computation time. Considering a small problem size for evaluation of the proposed resource allocation method is the main defect in the simulation setup.

Shokrollahi et al. [61] propose a distributed service-oriented valuable smart device approach to communicate the configurations of the IoT service roles and applying QoS rules for guarantying durability and minimum latency factors. The experimental results have been investigated with a linear connection between appropriate services to minimize reliability, and computation time in a simulation environment. There are some defects in this paper as follows: (1) the authors have not considered a relative analysis with other service–oriented algorithms, and (2) the scalability has not been evaluated for a distributed IoT environment.

Bouzouita et al. [62] present a recursive crowd resourcing method for evaluating the number of IoT devices in a 5G communication environment. This approach has been analyzed according to

a data congestion perspective to enhance resource connection control using appropriate IoT devices. The authors have evaluated the efficiency of the estimation accuracy for each device connection based on an allocated response time. The error estimation is very ignorable in this method because the congestion parameter has been considered as a public constant.

Antunes et al. [63] propose a context-aware multi-level resource management approach based on mobile edge computing for the heterogeneous IoT applications. The authors have provided a physical methodology for global resource management based on the scalable reaction time perspective and a software methodology for local management based on storage, scheduling and authentication of information management in a context-aware policy management. The simulation analysis has been evaluated just with restricted IoT resources. The scalability, bandwidth and memory consumption and CPU utilization have been analyzed in the simulation results. The main weakness of this approach is that the authors have not considered the cost of tasks transitions for migrating resource from smart devices in the IoT.

Naranjo et al. [64] propose a Fog-based smart city model for IoT applications. The proposed model covers three main communication types for devices and IoT applications to support QoS factors of existing resources with minimum power consumption.

Table 6 shows an evaluation report for existing resource-based communications in the IoT environments. The ubiquitous scenarios have most usage for resource management approaches based on messaging and wireless technology technologies as communication technologies in the D2D communication type.

Table 6. Comparison of the evaluation factors for the resource-based communications

Ref	Main context	IoT-based technology	IoT-based scenario	Communication type	Evaluation factors	Validation
[51]	RESTFul-based translator framework to manage resource transferring	Messaging technology	Ubiquitous	D2C	Scalability, Cost	Case study
[52]	Resource traffic management approach based on	Messaging technology	Vehicle	D2A	Latency	Empirical

	communication timing method					
[53]	Energy-aware microscopic communication method	Gateway-based	Commercial	D2G	Saving battery life and energy reduction	Empirical
[54]	State reduction method to utilize time division and cost benefit selection	Messaging technology	Ubiquitous	D2D	Energy, execution time, reliability	Case study
[55]	Description language for specifying the smart things in the Web	IP technology	Ubiquitous	D2D – D2A	Computation time, Energy	Empirical
[56]	Cellular remote device clustering for saving battery life	Messaging technology	Ubiquitous	D2D	Packet size, battery capacity, energy consumption, distance rate	Empirical
[57]	Cellular device to device resource allocation model	Messaging technology	Vehicle	D2D	Energy consumption	Empirical
[58]	QoS-based micro multiple-access resource allocation in the cellular IoT communications	Wireless technology	Ubiquitous	D2D	Execution time, density	Case study
[59]	Random-access resource management approach for enhancing success ration	Messaging technology	Ubiquitous	D2D	Access probability, ordinary delay and access throughput	Case study
[60]	Data propagation-based resource allocation method	Messaging technology	Ubiquitous	D2D	Paring ratio, Computation time	Case study
[61]	Distributed service-oriented valuable smart device approach	Messaging technology	Ubiquitous	D2D – D2A	Reliability, Computation time	Case study

[62]	Recursive crowd resourcing method for evaluating the number of IoT devices	Messaging technology	Ubiquitous	D2A	Accuracy estimation error	Empirical
[63]	Context-aware multi-level resource management approach based on mobile edge computing	Messaging technology	Ubiquitous	D2A	Scalability, bandwidth and memory consumption and CPU utilization	Empirical
[64]	Fog-based smart city model for IoT applications	Messaging technology	Social	D2C	Power consumption	Case study

4. Discussion

In this section, a comparative discussion and evaluation is considered for existing IoT communication research studies. The comparative reports and evaluation are related to the proposed MQs in section 2:

- MQ 1: Which IoT communication strategies are applied in this literature?

Figure 4 shows a statistical comparison of the applied IoT communication strategies based on content of the illustrated taxonomy (Fig 3). The authors have categorized IoT communication strategies into five main topics including monitoring-based communications, routing-based communications, health-based communications, intrusion-based communications, and resource-based communications. The resource-based communications has highest percentage of the IoT communication strategies by 35% usage in the literature. Of course, the intrusion-based has 26%, the routing-based has 16%, the monitoring-based has 14% and the health-based has 8% usage in the IoT communications.

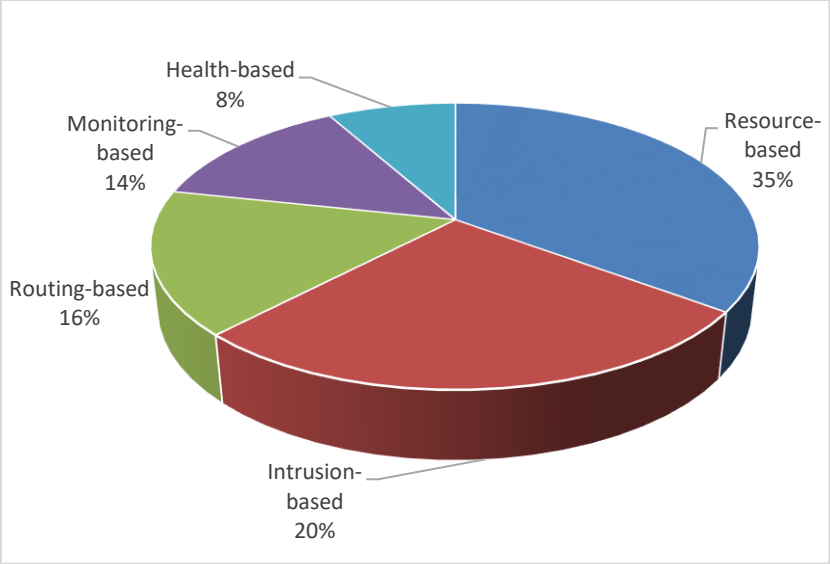

Fig. 4. Percentage of the presented IoT communication strategies.

- MQ 2: Which main scenarios are considered for IoT communication strategies?

The applied main scenarios that considered for the IoT communication strategies are shown in Figure 5. The authors have observed that ubiquitous scenarios have most considered with 17 research articles, and commercial scenarios have 7 studies. In the total number of the IoT communication strategies, ubiquitous environments are most popular communication platform to present and evaluate the communication of IoT applications and smart devices. Also, commercial scenarios, medical case studies, and vehicle environments have most published paper in the IoT communication strategies. In the monitoring-based communications, the home-care, industrial, social, commercial and medical scenarios as the important environments have been applied to evaluate the IoT communication strategies. In the routing-based communications, the commercial scenarios have been presented to illustrate the IoT communication platform. In the health-based communications, just medical perspectives have been used to evaluate the IoT communication strategies. In the intrusion-based communications and the resource-based communications, ubiquitous environments have most usage for presenting the IoT communication scenarios.

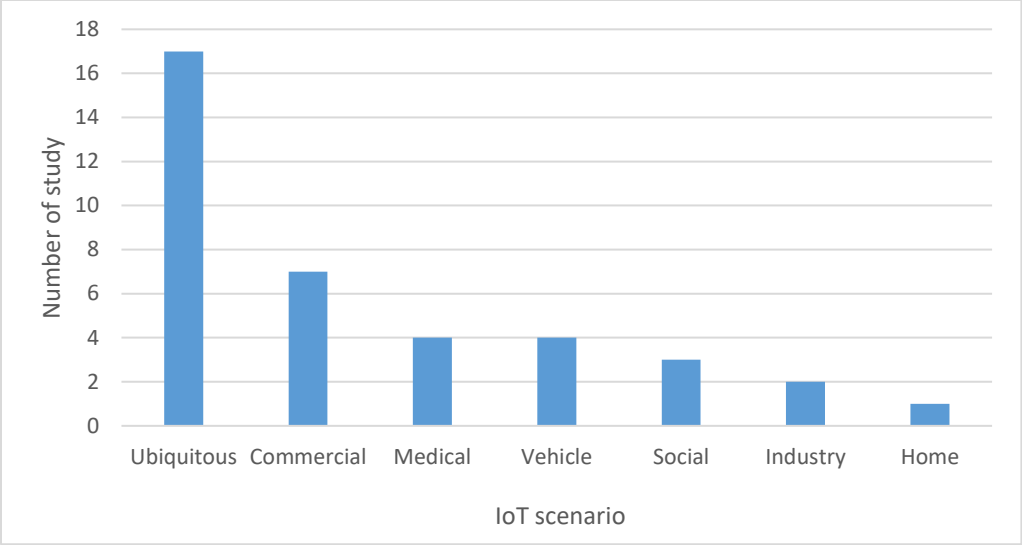

Fig. 5. Percentage of the applied main scenarios in IoT communications.

- MQ3: Which communication type is provided for connection of IoT devices?

According to Figure 6, 19 research studies have evaluated IoT communication strategies on the D2A platform. In addition, 16 research papers used D2D communication type to assess and analyze the existing case studies. Also, D2C and D2G communication types have been evaluated in the IoT case studies with 5 and 3 papers respectively.

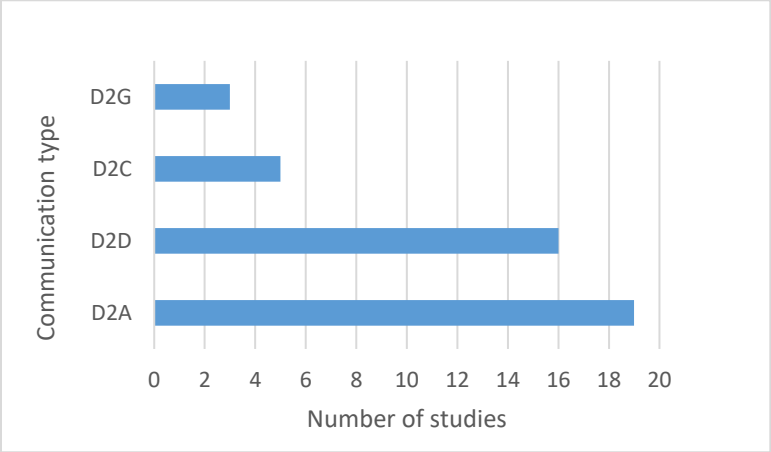

Fig. 6. Percentage of the communication types in IoT environments.

- MQ4: Which communication technologies are applied for the IoT devices?

The applied communication technologies for smart devices and IoT applications are compared in Figure 7. The statistical percentage of the applied technologies presents that the messaging

technology has greatest usage in the IoT communications with 17 research studies. Of course, some studies have a hybrid usage for communication technologies in their case studies.

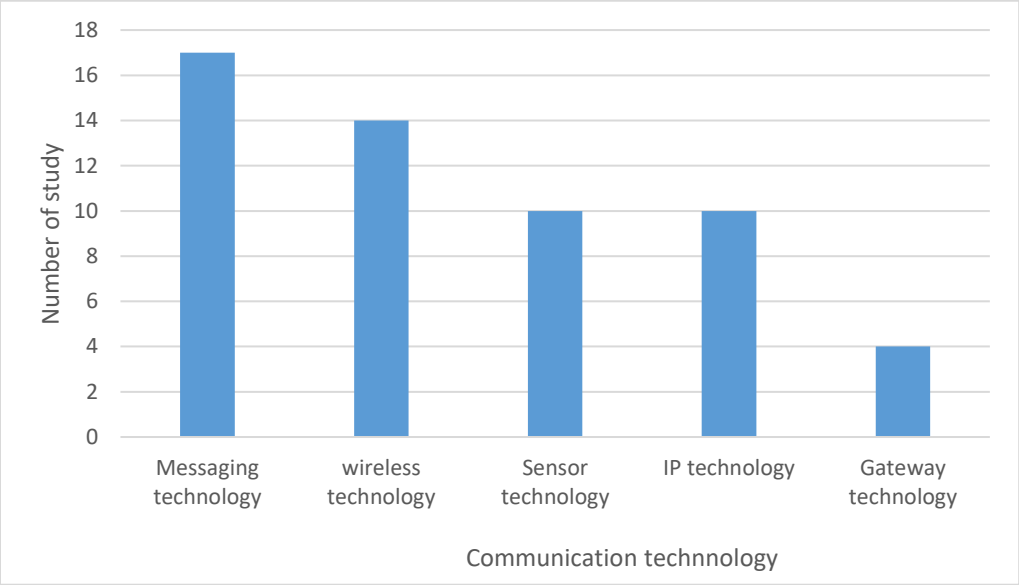

Fig. 7. Percentage of communication technologies for the IoT devices.

- MQ5: What are the evaluation factors usually applied to the IoT communication strategies?

The evaluation factors are analyzed and compared as the enhancement effort for each study in the IoT communication strategies according to Figure 8. The comparison descriptions of the evaluation factors illustrate that the time (aggregation of response time, computation time and execution time), bandwidth, energy and latency have most usage in the IoT communications by 18%, 16%, 16%, and 13% percentage. However, scalability and availability as the important issues in the IoT communication can be evaluated as an open challenge in the device to device and device to application methodologies. However, a few research studies have considered existing evaluation factors such as accuracy, precision, successability, privacy, error rate, reliability, space complexity, memory consumption and speed up that we categorized them to "Other" in the Figure 8.

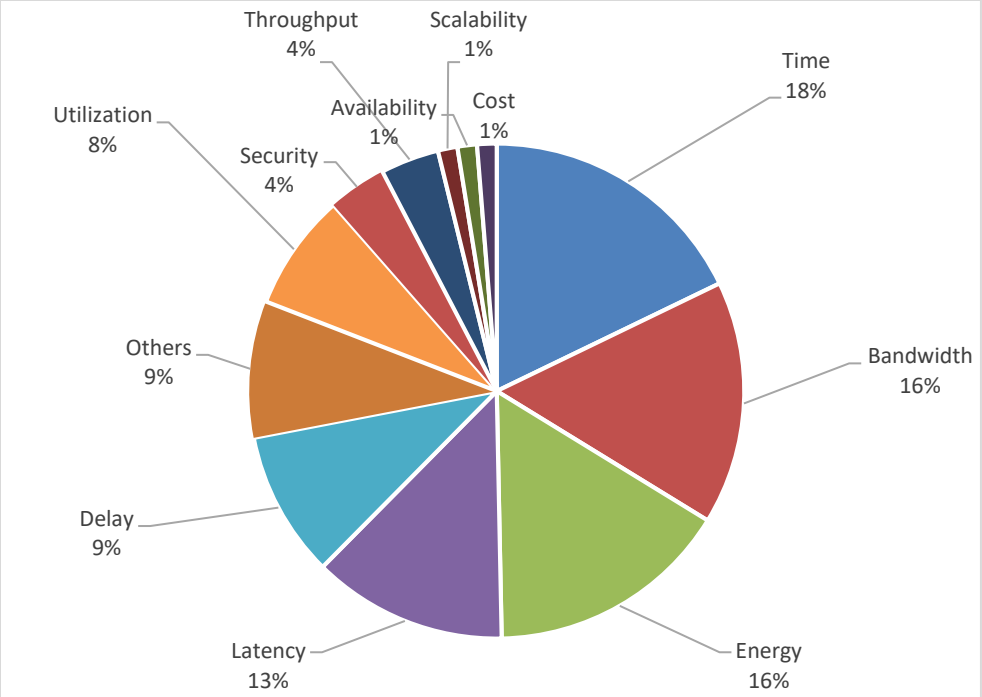

Fig. 8. Percentage of evaluation factors for analyzing IoT communications.

5. Forthcoming and open issues of IoT communications

According to the previous section, some new research directions and open challenges are presents to finding forthcoming studies and issues in the IoT communications. The Authors have answered new open issues and forthcoming challenges base on MQ6.

- MQ6: What are the forthcoming directions and open issues for IoT communication strategies?

Scalability and mobility: these factors have several challengeable points to IoT communication strategies such as vehicular IoT networks, monitoring and social commitments that have not addressed the supporting scalability and mobility criterions. For enhancing scalability factor in IoT communications, the number of covered sensors should be optimized based on transmission technologies in IoT [65]. Hybrid cloud providers can apply to represent smart services of IoT end users to provide upstream scalability by worldwide perspective of the IoT communications. There are some new efforts to this open issue including virtual migration problem, and dynamic device mobility. Also, mobility condition can positive influence on the smart city case studies to connect the IoT applications and users [66].

Privacy and security: One of the important challenges in the realization of the IoT communication is its security and privacy. From the security point of view authentication, distributed denial of service, trust and access control have been identified as the main security challenges [67, 68]. Public key infrastructure and trusted execution environment techniques can prove beneficial for this problem [69]. The IoT works with sensors and actuators, they need the utmost care of handling the devices since some physical damages also may happen because of mishandling the actuators, the hackers would try to disturb the normal working of such devices. A complete security standard with proper confidentiality, integrity, and authentication should be implemented for IoT communications [70, 71].

Interoperability: This factor is a key feature for communication between IoT applications, cloud providers and smart devices [72]. Some key challenges of this area are including a scalable architecture to interact with the smart objects and data centers, a dynamic and adaptive interoperability architecture for ultra-large scale IoT communications [73].

Trust and access control: trust management in communication strategies is an important challenge to increase [74, 75]. Trustworthiness management can be effective on the relationships between smart objects and IoT applications to improve a safe data delivery [76]. Also, access control management can be influence on the safe and trustable communication between smart devices and IoT applications [77]. Categorizing access control management for a set of communication strategies should be guaranteed to enhance the access level of each device and application in the IoT environment.

Energy consumption: IoT devices such as sensors, mobile agents, wireless technology, and cameras are physically distributed, and interacted with the IoT applications that have more energy efficient in comparison of the centralized topologies. In addition, achieving Industry 4.0 is not an easy thing, as its involves many aspects, and faces many type of challenges and difficulties, e.g. scientific, technological, economical, and social challenges [78]. For example, minimizing power consumption is one of the main challenges on the IoT communication strategies that can be supported with supply chain management in industrial environments.

6. Conclusion and limitations

This paper presented a systematic review on IoT communication strategies for an efficient smart environment. Based on the SLR mechanism, existing peer-reviewed articles were provided for technical analysis on this topic. The existing research studies were categorized into five main categories monitoring-based communications, routing-based communications, health-based communications, intrusion-based communications, and resource-based communications. The Authors observed that the resource-based communication category is the most popular approach by 35% usage. As stated by the technical discussion, the device to application is the most popular communication type by 52% usage in the IoT communication strategies. In each category, important evaluation metrics were analyzed according to the time, latency, bandwidth, energy and delay in the IoT communication strategies with most evaluation than other factors such as availability, throughput, cost and utilization. In addition, the Authors observed that the ubiqutouse scenarios have the most usage with 38% for evaluation of the IoT communication strategies. Moreover, the messaging technology is most usable communication technology to connect the smart devices and IoT applications. Furthermore, there are some limitations in this analysis as follows: (1) the non-English papers, conference papers, book chapters and technical thesis were ignored in the review, (2) Non-index papers with low quality were omitted in this analysis, (3) the Authors have restricted the search scope to research studies between 2014-Feb 2019. In the future research, some new open issues such as trustworthiness and access control management for IoT communication strategies, smart health-care communication efforts [79], educational-based IoT communications, social IoT communication approaches, privacy-based communication protocols can be considered for new research efforts and open challenges in the IoT communication strategies.

References

1. Dizdarević, J., et al., *A Survey of Communication Protocols for Internet of Things and Related Challenges of Fog and Cloud Computing Integration.* ACM Computing Surveys (CSUR), 2019. **51**(6): p. 116.
2. Luo, Y., et al., *A novel mobile and hierarchical data transmission architecture for smart factories.* IEEE Transactions on Industrial Informatics, 2018. **14**(8): p. 3534-3546.
3. Al-khafajiy, M., et al., *Towards fog driven IoT healthcare: challenges and framework of fog computing in healthcare*, in *Proceedings of the 2nd International Conference on Future Networks and Distributed Systems*. 2018, ACM: Amman, Jordan. p. 1-7.
4. Çorak, B.H., et al. *Comparative Analysis of IoT Communication Protocols*. in *2018 International Symposium on Networks, Computers and Communications (ISNCC)*. 2018. IEEE.

5. Badawy, M.M., Z.H. Ali, and H.A. Ali, *QoS provisioning framework for service-oriented internet of things (IoT).* Cluster Computing, 2019.
6. Asghari, P., A.M. Rahmani, and H.H.S. Javadi, *Service composition approaches in IoT: A systematic review.* Journal of Network and Computer Applications, 2018. **120**: p. 61-77.
7. Tayeb, S., S. Latifi, and Y. Kim. *A survey on IoT communication and computation frameworks: An industrial perspective*. in *2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC)*. 2017. IEEE.
8. Zaidan, A.A., et al., *A survey on communication components for IoT-based technologies in smart homes.* Telecommunication Systems, 2018. **69**(1): p. 1-25.
9. Akpakwu, G.A., et al., *A survey on 5G networks for the Internet of Things: Communication technologies and challenges.* IEEE Access, 2017. **6**: p. 3619-3647.
10. Montori, F., et al., *Machine-to-machine wireless communication technologies for the Internet of Things: Taxonomy, comparison and open issues.* Pervasive and Mobile Computing, 2018.
11. Al-Sarawi, S., et al. *Internet of Things (IoT) communication protocols*. in *2017 8th International Conference on Information Technology (ICIT)*. 2017. IEEE.
12. Siboni, S., et al., *Security Testbed for Internet-of-Things Devices.* IEEE Transactions on Reliability, 2018. **68**(1): p. 23-44.
13. Asghari, P., A.M. Rahmani, and H.H.S. Javadi, *Internet of Things applications: A systematic review.* Computer Networks, 2019. **148**: p. 241-261.
14. Matthieu, C. and G. Ramleth, *Security and rights management in a machine-to-machine messaging system*. 2015, Google Patents.
15. Jo, M., et al., *Device-to-device-based heterogeneous radio access network architecture for mobile cloud computing.* IEEE Wireless Communications, 2015. **22**(3): p. 50-58.
16. Yang, G., et al., *IoT-based remote pain monitoring system: From device to cloud platform.* IEEE journal of biomedical and health informatics, 2018. **22**(6): p. 1711-1719.
17. Le, M., S. Clyde, and Y.-W. Kwon, *Enabling multi-hop remote method invocation in device-to-device networks.* Human-centric Computing and Information Sciences, 2019. **9**(1): p. 20.
18. Da Xu, L., W. He, and S. Li, *Internet of things in industries: A survey.* IEEE Transactions on industrial informatics, 2014. **10**(4): p. 2233-2243.
19. Lin, J., et al., *A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications.* IEEE Internet of Things Journal, 2017. **4**(5): p. 1125-1142.
20. Shelby, Z., K. Hartke, and C. Bormann, *The constrained application protocol (CoAP)*. 2014.
21. Standard, O., *MQTT version 3.1. 1.* URL http://docs. oasis-open. org/mqtt/mqtt/v3, 2014. **1**.
22. Matthieu, C. and G. Ramleth, *Machine-to-machine instant messaging*. 2015, Google Patents.
23. Javed, R.H., et al. *ApproxCT: Approximate Clustering Techniques for Energy Efficient Computer Vision in Cyber-Physical Systems*. in *2018 12th International Conference on Open Source Systems and Technologies (ICOSST)*. 2018.
24. Ejaz, W., et al., *Internet of Things (IoT) in 5G Wireless Communications.* IEEE Access, 2016. **4**: p. 10310-10314.
25. Luo, Y., et al., *Workshop networks integration using mobile intelligence in smart factories.* IEEE Communications Magazine, 2018. **56**(2): p. 68-75.
26. MacDermott, A., T. Baker, and Q. Shi. *Iot Forensics: Challenges for the Ioa Era*. in *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*. 2018.
27. Zhou, Z., et al., *Potential risk of IoT device supporting IR remote control.* Computer Networks, 2018.
28. Hejselbaek, J., et al., *Empirical Study of Near Ground Propagation in Forest Terrain for Internet-of-Things Type Device-to-Device Communication.* IEEE Access, 2018. **6**: p. 54052-54063.

29. Kertesz, A., T. Pflanzner, and T. Gyimothy, *A Mobile IoT Device Simulator for IoT-Fog-Cloud Systems.* Journal of Grid Computing, 2018.
30. Paul, A. and S. Rho, *Probabilistic Model for M2M in IoT networking and communication.* Telecommunication Systems, 2015. **62**(1): p. 59-66.
31. Wang, J., et al., *A self-adaptive load-dispatching control framework for device data accessing in IoT-based systems.* International Journal of Communication Systems, 2017. **30**(12): p. e3260.
32. Debroy, S., et al., *SpEED-IoT: Spectrum aware energy efficient routing for device-to-device IoT communication.* Future Generation Computer Systems, 2018.
33. Mukherjee, S. and G.P. Biswas, *Networking for IoT and applications using existing communication technology.* Egyptian Informatics Journal, 2018. **19**(2): p. 107-127.
34. Sharma, V., et al., *Energy efficient device discovery for reliable communication in 5G-based IoT and BSNs using unmanned aerial vehicles.* Journal of Network and Computer Applications, 2017. **97**: p. 79-95.
35. Bi, Z., et al., *IoT-based system for communication and coordination of football robot team.* Internet Research, 2017. **27**(2): p. 162-181.
36. Chen, G., J. Tang, and J.P. Coon, *Optimal Routing for Multihop Social-Based D2D Communications in the Internet of Things.* IEEE Internet of Things Journal, 2018. **5**(3): p. 1880-1889.
37. Cuka, M., et al., *Implementation and performance evaluation of two fuzzy-based systems for selection of IoT devices in opportunistic networks.* Journal of Ambient Intelligence and Humanized Computing, 2018.
38. Santamaria, A.F., et al., *A real IoT device deployment for e-Health applications under lightweight communication protocols, activity classifier and edge data filtering.* Computer Communications, 2018. **128**: p. 60-73.
39. Woo, M.W., J. Lee, and K. Park, *A reliable IoT system for Personal Healthcare Devices.* Future Generation Computer Systems, 2018. **78**: p. 626-640.
40. Bae, W.-S., *Verifying a secure authentication protocol for IoT medical devices.* Cluster Computing, 2017.
41. Matheu-García, S.N., et al., *Risk-based automated assessment and testing for the cybersecurity certification and labelling of IoT devices.* Computer Standards & Interfaces, 2019. **62**: p. 64-83.
42. Mukherjee, B., et al., *Flexible IoT security middleware for end-to-end cloud–fog communication.* Future Generation Computer Systems, 2018. **87**: p. 688-703.
43. Randhawa, R.H., A. Hameed, and A.N. Mian, *Energy efficient cross-layer approach for object security of CoAP for IoT devices.* Ad Hoc Networks, 2018.
44. Yang, K., Q. Li, and L. Sun, *Towards automatic fingerprinting of IoT devices in the cyberspace.* Computer Networks, 2018.
45. Dao, N.-N., et al., *Achievable multi-security levels for lightweight IoT-enabled devices in infrastructureless peer-aware communications.* IEEE Access, 2017. **5**: p. 26743-26753.
46. Jin, B.-W., J.-O. Park, and H.-J. Mun, *A Design of Secure Communication Protocol Using RLWE-Based Homomorphic Encryption in IoT Convergence Cloud Environment.* Wireless Personal Communications, 2018.
47. Lee, Y.-k., et al., *Secure mobile device structure for trust IoT.* The Journal of Supercomputing, 2017. **74**(12): p. 6646-6664.
48. Patil, S.S., A. Mihovska, and R. Prasad, *An IoT Virtualization Framework for Fast and Lossless Communication.* Wireless Personal Communications, 2014. **76**(3): p. 449-462.
49. Bagci, I.E., et al., *Fusion: coalesced confidential storage and communication framework for the IoT.* Security and Communication Networks, 2016. **9**(15): p. 2656-2673.

50. Køien, G.M., *A privacy enhanced device access protocol for an IoT context.* Security and Communication Networks, 2016. **9**(5): p. 440-450.
51. Khaled, A.E. and S. Helal, *Interoperable communication framework for bridging RESTful and topic-based communication in IoT.* Future Generation Computer Systems, 2019. **92**: p. 628-643.
52. Yamada, Y., et al., *Temporal traffic smoothing for IoT traffic in mobile networks.* Computer Networks, 2018. **146**: p. 115-124.
53. Chen, Y., et al., *Energy-Autonomous Wireless Communication for Millimeter-Scale Internet-of-Things Sensor Nodes.* IEEE Journal on Selected Areas in Communications, 2016. **34**(12): p. 3962-3977.
54. Ito, M., et al., *Reducing State Information by Sharing IMSI for Cellular IoT Devices.* IEEE Internet of Things Journal, 2016. **3**(6): p. 1297-1309.
55. Khaled, A.E., et al., *IoT-DDL–Device Description Language for the "T" in IoT.* IEEE Access, 2018. **6**: p. 24048-24063.
56. Lianghai, J., et al., *Applying Device-to-Device Communication to Enhance IoT Services.* IEEE Communications Standards Magazine, 2017. **1**(2): p. 85-91.
57. Liu, X. and N. Ansari, *Green Relay Assisted D2D Communications With Dual Batteries in Heterogeneous Cellular Networks for IoT.* IEEE Internet of Things Journal, 2017. **4**(5): p. 1707-1715.
58. Lv, T., et al., *Millimeter-Wave NOMA Transmission in Cellular M2M Communications for Internet of Things.* IEEE Internet of Things Journal, 2018. **5**(3): p. 1989-2000.
59. Moon, S., H.-S. Lee, and J.-W. Lee, *SARA: Sparse Code Multiple Access-Applied Random Access for IoT Devices.* IEEE Internet of Things Journal, 2018. **5**(4): p. 3160-3174.
60. Song, W., Y. Zhao, and W. Zhuang, *Stable Device Pairing for Collaborative Data Dissemination With Device-to-Device Communications.* IEEE Internet of Things Journal, 2018. **5**(2): p. 1251-1264.
61. Shokrollahi, S. and F. Shams, *Rich Device-Services (RDS): A Service-Oriented Approach to the Internet of Things (IoT).* Wireless Personal Communications, 2017. **97**(2): p. 3183-3201.
62. Bouzouita, M., et al., *Estimating the number of contending IoT devices in 5G networks: Revealing the invisible.* Transactions on Emerging Telecommunications Technologies, 2018: p. e3513.
63. Antunes, J.B., et al., *ManIoT: A 2-tier management platform for heterogeneous IoT devices and applications.* International Journal of Network Management, 2018. **28**(5): p. e2034.
64. Naranjo, P.G.V., et al., *FOCAN: A Fog-supported smart city network architecture for management of applications in the Internet of Everything environments.* Journal of Parallel and Distributed Computing, 2018.
65. Al-khafajiy, M., et al. *IoT-Fog Optimal Workload via Fog Offloading*. in *2018 IEEE/ACM International Conference on Utility and Cloud Computing Companion (UCC Companion)*. 2018.
66. Ren, J., et al., *Serving at the edge: A scalable IoT architecture based on transparent computing.* IEEE Network, 2017. **31**(5): p. 96-105.
67. Mohammadi, V., et al., *Trust-based recommendation systems in Internet of Things: a systematic literature review.* Human-centric Computing and Information Sciences, 2019. **9**(1): p. 21.
68. Abbas, N., et al., *A Mechanism for Securing IoT-enabled Applications at the Fog Layer.* Journal of Sensor and Actuator Networks, 2019. **8**(1): p. 16.
69. Song, T., et al. *A Privacy Preserving Communication Protocol for IoT Applications in Smart Homes*. in *2016 International Conference on Identification, Information and Knowledge in the Internet of Things (IIKI)*. 2016.
70. Zhang, S., et al., *Physical layer security in massive internet of things: delay and security analysis.* IET Communications, 2018. **13**(1): p. 93-98.

71. Baker, T., et al., *A secure fog-based platform for SCADA-based IoT critical infrastructure.* Software: Practice and Experience, 2019. **0**(0).
72. Aloi, G., et al., *Enabling IoT interoperability through opportunistic smartphone-based mobile gateways.* Journal of Network and Computer Applications, 2017. **81**: p. 74-84.
73. Noura, M., M. Atiquzzaman, and M. Gaedke, *Interoperability in Internet of Things: Taxonomies and Open Challenges.* Mobile Networks and Applications, 2019. **24**(3): p. 796-809.
74. Campolo, C., A. Molinaro, and A. Iera, *A reference framework for social-enhanced Vehicle-to-Everything communications in 5G scenarios.* Computer Networks, 2018. **143**: p. 140-152.
75. Chen, R., J. Guo, and F. Bao, *Trust management for SOA-based IoT and its application to service composition.* IEEE Transactions on Services Computing, 2014. **9**(3): p. 482-495.
76. Amadeo, M., et al., *IoT Services Allocation at the Edge via Named Data Networking: From Optimal Bounds to Practical Design.* IEEE Transactions on Network and Service Management, 2019.
77. Abbassi, I.H., et al. *TrojanZero: Switching Activity-Aware Design of Undetectable Hardware Trojans with Zero Power and Area Footprint*. in *2019 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. 2019. IEEE.
78. Zhou, K., T. Liu, and L. Zhou. *Industry 4.0: Towards future industrial opportunities and challenges*. in *2015 12th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD)*. 2015. IEEE.
79. Pace, P., et al., *An edge-based architecture to support efficient applications for healthcare industry 4.0.* IEEE Transactions on Industrial Informatics, 2019. **15**(1): p. 481-489.