Internet of Things: Vision, Future Directions and Opportunities

Laith Farhan and Rupak Kharel

Abstract Internet of things (IoT) is considered to revolutionize the way internet works and bring together the concepts such as machine to machine (M2M) communication, big data, artificial intelligence, etc. to work under a same umbrella such that cyber space and human (physical systems) are more intertwined and thus ubiquitous giving rise to cyber physical systems. This will involve billions of connections and smart products communicating with each other mostly without human intervention to achieve smart objectives. The idea of IoT has enticed significant research attentions since the massive connectivity bring varieties of challenges and obstacles including heterogeneity, scalability, security, big data, energy requirements, etc. The chapter looks into providing a concise review of the concepts on IoT and applications describing the main features, vision, and future directions. Furthermore, open issues and challenges that need addressing by the research community and some potential solutions are discussed.

Introduction to Internet of Things

During the last decade, Internet of Things (IoT) has attracted intensive attention due to a wide range of applications in industrial, biomedical observation, agriculture, smart cities, environmental monitoring and other fields (Fig. 1) [1]. IoT is the internetworking of physical devices used in our daily lives that use standard communications architectures to provide new services to end users [2].

It is envisioned that by 2020 the future Internet will include tens of billions of smart objects/devices [3]. IoT technology provides better services to end users via real-time data processing, communications and visualization. IoT can be extended to almost everything from refrigerator to washing machine, wristwatches to smartphones, home

L. Farhan (✉) · R. Kharel
Manchester Metropolitan University, Manchester, UK
e-mail: l.al-bayati@mmu.ac.uk

L. Farhan
University of Diyala, Baqubah, Iraq

S. C. Mukhopadhyay et al. (eds.), *Modern Sensing Technologies* ,
Smart Sensors, Measurement and Instrumentation 29,
https://doi.org/10.1007/978-3-319-99540-3_17

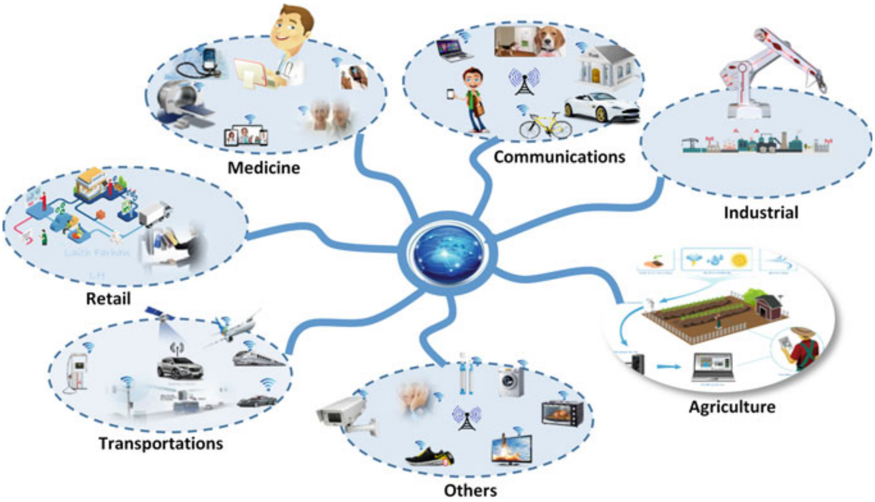

Fig. 1 Network of the future

security to alarm system, etc. [4]. For example, smart refrigerators can tell us the end of the validity of food using bar-codes or which items to buy during our shopping in the market. On the other hand, imagine that we can control our house from anywhere. By using smart phones or tablets with just simple touch we can set a desired temperature or turn lights on or off before getting home. These are examples of just a few applications out of thousands being currently developed every day in the field of IoT.

The massive growth in the number of devices connected to the internet (up to 100 billion devices), poses a huge range of challenges. In the future IoT will not be islands of isolated systems, but will be an integration of many islands of connected systems, applications, services and underlying devices. At the moment, each of these devices and services work on their own architectures, data format, and own existing protocol stacks. They are all still at early stages of development. Hence, the communication between these objects is insecure, suffers from interoperability and integration issues [5]. Furthermore, the sources of energy required to power these devices are very precious due to the fact that most of them are powered by battery or by means of energy harvesting. Therefore, there is a need for comprehensive review of existing unconstrained and constrained devices protocols with the view of developing unified, dynamic, standardized, energy efficient and intelligent protocol stacks with recourse to node identity (both capacity and capability). So far, most of these new challenges and concerns have started to attract the attention of academic researchers and companies.

IoT Applications, Future Directions and Challenges

Many researchers and early adopters have come up with promising solutions to overcome the problems and challenges in realizing IoT applications. However, IoT opens up new horizontal challenges that demand latest research and capacities to address them. In this section, we briefly highlight the key challenges for the future IoT systems (see Fig. 2). Wireless Sensor Networks (WSN) are considered as one of the fundamental underlying technologies for IoT. Therefore, the study has also considered some previous works in the WSN field.

Fault Tolerance

Fault tolerance is one of the most important issues in the area of WSN and IoT applications. Both technologies involve large number of heterogeneous sensor nodes spread over a large geographic area to perform a specific task. The explosive growth of the connected devices demands higher reliability and performance from modern

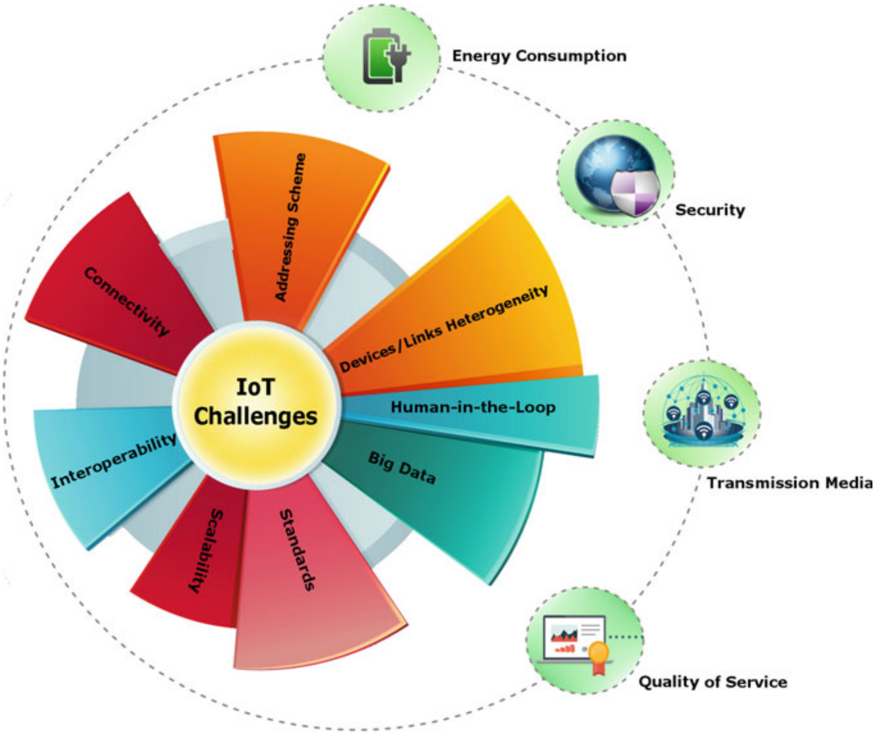

Fig. 2 IoT challenges and opportunities

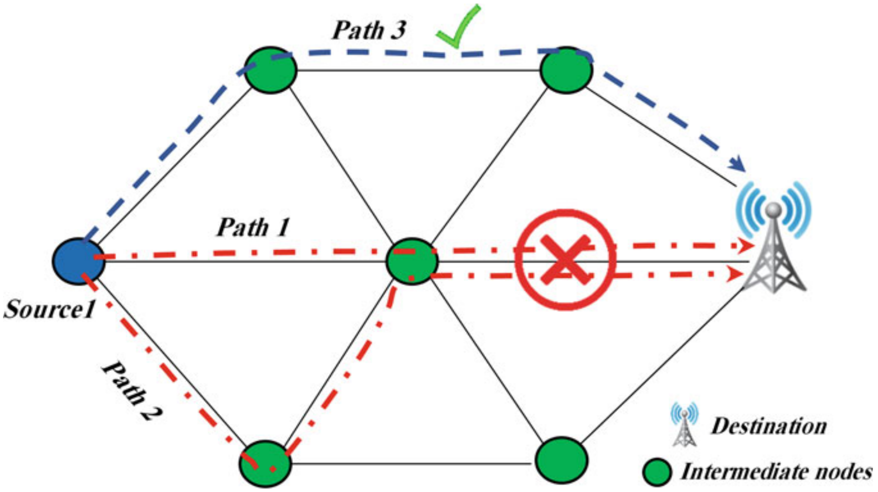

Fig. 3 Multi-level paths between source and destination

networks. Some sensor nodes may be blocked or fail due to exposure to harsh environments, interference, physical damage or lack of power [6]. Probability of sensor node failure increases with rise in number of sensors and increasing sensing field. Such nodes failure should not affect the overall task of the sensor network [7]. Most of WSNs and IoT routing protocols should have the ability to recover from the failure of a sensor node [8]. The sensor is reported as a failure node when a node cannot receive or communicate messages with neighbor nodes for a specific period of time and thus excluded from the routing path. The problem becomes worse when two or more sensor nodes fail in the same area. The network might cripple very quickly because other nodes cannot find a route to the ultimate receiver. Therefore, a routing protocol must follow new links dynamically to deliver the data collected by other devices to the intended destination. Also, multi levels of redundancy may be needed in a fault tolerant sensor networks as can be seen in Fig. 3. It clearly shows that source 1 sends its data to the destination via intermediate nodes. Unfortunately, path 1 and 2 are failing to carry the data to the final destination due to malfunctioning of some nodes. Therefore, the topology might require to find new path for packets and reorganize the network.

Many design goals are related to routing policy such as energy consumption, small delay, high throughput, limited variance of the connection quality, etc. Authors in [9] present expected transmission count (ETX) algorithm that performs up to two times better than minimal hop-count for long links in term of throughput. The ETX strategy is to find high throughput paths on multi-hop wireless communication. It minimizes the expected total number of packets transmission (including retransmissions) that requires to successfully deliver data to the final destination. Another study [10] implements new routing technique called balanced energy adaptive routing (BEAR) for IoT networks. The proposed method operates in three phases: (i)

Sensor nodes share the information related to their locations and residual energy. (ii) BEAR protocol elects neighbor nodes and selects the facilitator and successor nodes based on the node locations. (iii) Data transmission: The results of BEAR show improvement of network lifetime by up to 55%. In [11], authors investigate a novel context-aware routing (CAR) method for IoT applications. The proposed scheme improves the current request response model, during the exchange in peer to peer fashion. The simulation results of CAR show reduction in the total wasted time in network delay and improvement of network service and bandwidth.

Quality of Service (QoS)

The concept of QoS is relatively new in the area of IoT. There are a few number of researches currently dealing with this feature. In many applications, gathering data needs to be delivered within a certain time to the ultimate receiver otherwise the data will be of less value. The QoS requirements are met with differentiated services and delay management, packet loss, and bandwidth parameters in a network. These requirements become the secret to a successful end-to-end service. We review the most critical challenges faced in IoT infrastructures while implementing QoS requirements and are listed below and seen in Fig. 4.

- **Scalability**: IoT field is widely supported by an increasing number of devices that should not affect the QoS.
- **Communication range**: Most of these devices are limited in the transmission range that lead to a major source of QoS degradation in IoT nodes problem. Therefore, a node should depend on other intermediate nodes to be able to communicate

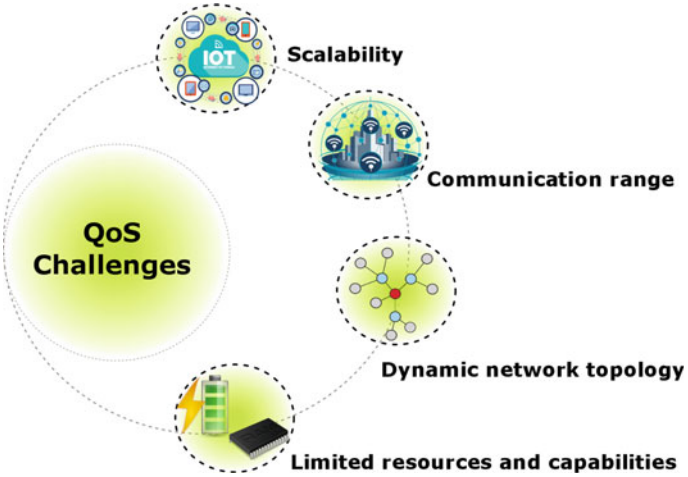

Fig. 4 Quality of service challenges

with others out of transmission range. These intermediate nodes act as relays for packets.
- **Dynamic network topology**: IoT network should have dynamic topology due to route changes, node power failures, link failure, etc. Therefore, QoS of these applications should not be affected with dynamic changes.
- **Limited resources and capabilities**: As already mentioned, most of the connected devices are constrained nodes to its ecosystem which have limited memories, CPU capabilities, power sources and bandwidth. Therefore, the QoS should be aware of limited resources and capabilities of these IoT-objects.

As a result, quality of service needs research and stabilization for implementation, optimization and management. In Ref. [12], authors present a general model to support the QoS aware deployment of multi-components IoT cloud infrastructures. The proposed model introduces suitable operational systemic qualities of fog facilities. Another study, authors [13] show a hybrid push-pull traffic scheme for data exchange in IoT environment. The proposed algorithm reduced 50% of network load and throughput compared with traditional IPv6 and showed minimal packet drop.

Humans in the Loop (HITL)

As IoT technology proliferates and things become more sophisticated, many of these new applications will require some form of human interaction. Human-in-the-loop allows the user to change the outcome of an event or process. For example, self-driving cars (also known as auto cars) are a great example when we mention HITL. The car mostly drives itself, but it still needs human to be alert in the case of emergency. When the sensor system sense something unusual on the road (e.g., there is snow, construction, fire, possible collision, etc.), it probably has to hand the control of the car to human. For example, consider a controversial, unfortunate and ethical scenario, such as a self-driving car going to crash inflicting either significant third-party damages or serious injuries to the driver. Should human make the final decision rather than an artificial intelligence algorithm in such circumstances (Fig. 5)?

Transmission Media (TM)

TM is the physical path that establishes the connection and carries the data from the sender to the receiver. IoT networks use different types of technology to transmit and receive the data such as RFID, Bluetooth, LiFi, Zigbee, LoraWAN, Sigfox, etc. The traditional problems associated with transmission media (e.g., bandwidth, high error rate, fading, inference, etc.) exist for IoT applications as well. Each transmission medium requires specialized energy, network hardware, bandwidth that has to be

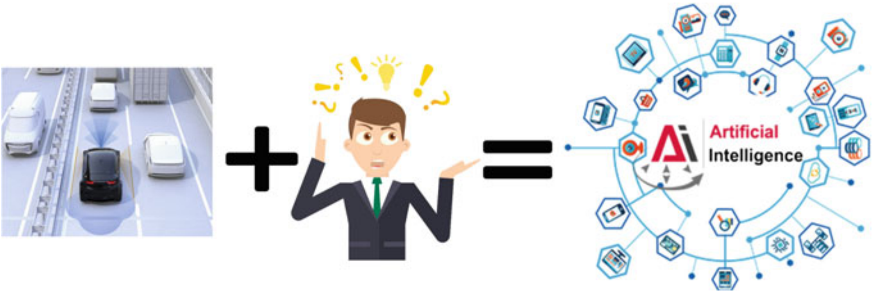

Fig. 5 Human in the loop challenges

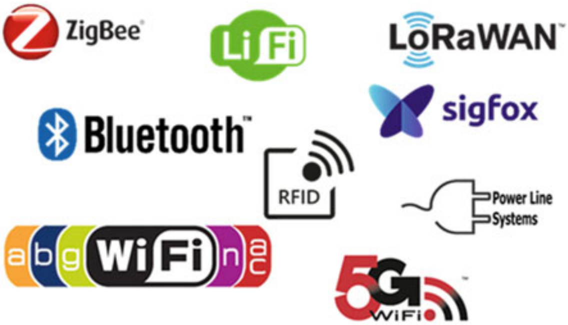

Fig. 6 Different technologies of IoT

compatible with that medium. Therefore, optimizing the TM is a challenge in IoT environment to sustain and prolong the lifetime of networks.

According to study in [14], authors discuss and analyse the capacity and coverage of LoRaWAN and Sigfox in a large-scale area. They measured the interference in the European frequency 868 MHz. The study illustrated both technologies provided uplink and downlink failure rates of less than 1%. Furthermore, improvement of indoor coverage up to 99% is also shown. In a different study [15], authors design full-duplex wireless information transfer and use backscatter antennas to reduce latency and energy consumption from reader to the target. The proposed scheme suppressed interference from coexisting links. It also enabled simultaneous backward/forward information transfer (Fig. 6).

Big Data

Internet of things leverage massive amount of data aggregated via smart objects and is one of the most striking features of this new technology. It will be necessary to develop techniques that convert this data into usable knowledge. Every two years,

Big Data Challenges
Velocity
Volume
Veracity
Variety
Value

Fig. 7 The "5V" challenges

data is doubling in size and is expected to reach 44 Zettabytes in the next four years [16].

The "5V" (Value, Velocity, Volume, Variety, and Veracity) are important challenges in IoT applications as can be seen in Fig. 7 and explained below:

- **Velocity**: refers to the speed at which the data is being collected, transferred and processed. The speed of processing data is different based on the type of application. For some applications, the arrival of data can be handled within a short time while in other applications, real-time processing is required such as analytics programs.
- **Variety**: refers to the different types of data collected by end devices such as smart-phones, machines, sensors, etc. The data content is unstructured of different types such as audio, video, images, XML format, plain text, CSV format, etc. The variety of data should be organized and processed in a meaningful and consistent way.
- **Veracity**: means making sure that the data gathered and stored are accurate. This might mean filtering out any unwanted or corrupted data to enhance quality of applications.
- **Volume**: is the amount of all types of data that is collected, stored, retrieved, updated from different sources. IoT is creating enormous amount of data that is rising exponentially. The question is can we incorporate volume and velocity together?
- **Value**: Once the massive data is gathered accurately, the next step is to get the value out of the data. Therefore, various algorithms such as feature extraction,

trend analysis using artificial intelligence that enables informed decision, within the required time frame, is another challenge.

There are several contemporary big data management and analytics applications that can be applied in the area of IoT. Authors in [17] focus on the real-time data coming from IoT devices in a smart building. The framework presents new technique on analysis and storage of high-speed data generated by sensors. The system shows the monitoring and control of a large amount of data without human intervention and improved users experience. Previous study in [18] reported an integrated IoT architecture for gas and water smart meter. The intelligent model provides the information to the utility and customers for a large amount of data. The proposed system shows benefits for utility companies and customers such as reduce energy consumption, automatic and real-time meter reading that saved physical meter reading and thus maintaining environmental sustainability.

Security

The security problem is one of the major challenges of networks over the years. Thus, security, privacy and trust are critical factors for IoT applications as well. When packets are routed through different links and devices to reach ultimate receiver on the internet, measures should be taken so that the confidentiality and integrity of the data is maintained. Moreover, most of the IoT devices are low power constrained devices, therefore, already established cryptographic solutions cannot be directly applied in the IoT scene [16]. Also, currently, the integration of application in the network infrastructure is focused on only achieving the functionality rather than holistically considering the security requirements when the application is designed. This is leaving door open for attacks and hacking attempts. Cybersecurity experts have warned that IoT is one of the most vulnerable technology and they expect more targeted attacks on existing and emerging infrastructures, e.g., data theft, physical injury, DDoS attack, ransomware for smart homes or smart cars, etc. Four key IoT security challenges can be seen in Fig. 8:

- **Trust and data integrity**: is to ensure the data has not changed from the moment it is sensed until it reaches the final destination. It also involves verifying the data and validating the verification certificate.
- **Trillion points of vulnerability**: with each device getting connected to IoT represents a potential risk. This leads to questions: how confident can an organization be of the data gathered and the integrity of the data sent? How to make sure data has not been interfered or compromised with?
- **Data protection**: is the law required to be designed to protect and control individual and organization data gathered by sensors or applications and stored to be part of a filing system.

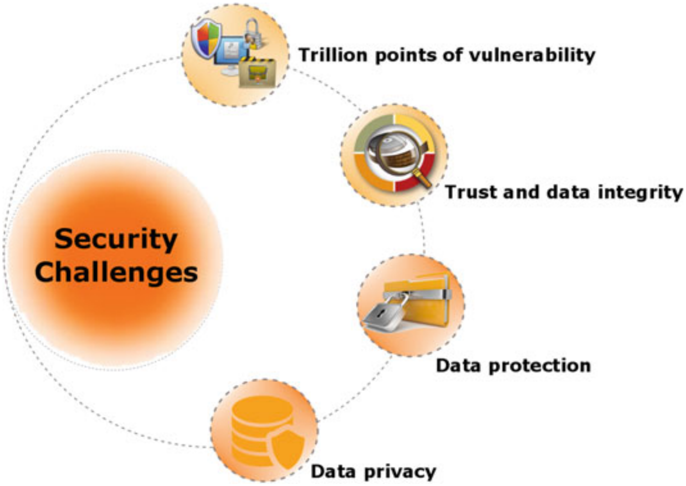

Fig. 8 Security challenges

- **Data privacy**: is to protect the data from exposure in the IoT environment. For instance, any logical or physical entity can be given a unique address and the ability to communicate automatically over the network.

A novel dynamic defence frame for IoT security has been implemented in [19]. The proposed method is divided into two phases: (i) The first stage applies based on recognition of security threats. (ii) The second stage uses real data provided by first stage. The authors provide a great solution method to ensure IoT security. With the same objective, authors in [20] propose a lightweight trust design to identify and isolate common routing attacks for IoT applications. In this protocol, the SecTrust framework mitigate routing attacks by enhancing the integrity and confidentiality of the IoT routing protocols. A new lightweight privacy-preserving data aggregation protocol has been investigated by [21] to enhance IoT security. The LPDA scheme supports fault-tolerance and efficiently aggregate IoT devices. It also early filters false data infected by attackers.

Addressing Schemes

Uniquely identifying objects is a critical issue for the operation and success of IoT applications. IoT-objects require to uniquely classify thousands of devices and to manage and control them remotely through the internet. A few most critical features of creating unique address are reliability, uniqueness, scalability and persistence [3]. These smart devices require a suitable and unique address that will make them able to communicate each other and become part of the internet. Internet protocol version 4 (IPv4) uses 32-bit addresses and provides capacity for only 4.3 billion IP addresses which are almost out of addresses. The next generation is IPv6 and it uses 128-bit addresses and has massive address abundance 3.4×10^{38} or (340 trillion trillion trillion) [22, 23]. A group of researchers [24] design a lightweight addressing scheme to solve IoT heterogeneity and scalability problems. In this model, virtual domain and multi encoding have been used to implement the nodes addressing. The proposed scheme shows suitable and fixable interconnection between WSNs and internet based on IPv6 over 6LowPAN. As highlighted by [25], authors propose identification and addressing scheme for IoT devices where they used distributed address allocation algorithm to implement automatic ID for IoT nodes. This work also presents addressing scheme combining cluster tree algorithm with AODV routing protocol. It implements nodes addressing scheme in the local and wide area of IoT networks. To this end, a unified addressing scheme for IoT is a very popular research field and a big challenge.

Devices/Links Heterogeneity

Another important feature of the vision of IoT is the variety of devices and links since it will be working on different sets of protocol suite, data formats, operating systems, etc. In WSNs, most of the sensors are homogeneous, i.e., having the same power, communication, capacity, and processor in term of computation. While IoT technology implements a wide variety of networks, links, and devices connectivity to provide different services [1]. Thus, heterogeneous nature of links and objects play a critical role in the interconnection of the IoT devices and thus add a unique challenge to address. Therefore, the question might be, is it possible to have a unified architectural model that can be deployed that it is able to support these wide ranges of devices and applications? In [26] an architecture is presented for heterogeneity of devices and networks based on SDN-Docker techniques. The proposed work reveals the feasible architecture and communication established between IoT devices through an SDN-based network. The DIAT scheme is a simple, scalable distributed architecture for large-scale IoT networks. It is specially designed to overcome the interoperability among various devices and deployments [27].

Mobility, Geography

Internet of things with mobile sink are expected to increase the flexibility of provide services and gathering data in large-scale sensing fields and detecting environments. The use of geographical position of nodes is necessary to detect nodes locations and simplify routing for WSNs and IoT networks. In such systems, it requires each node to determine its own location as well as the positions of its neighbour nodes. This information can be obtained with

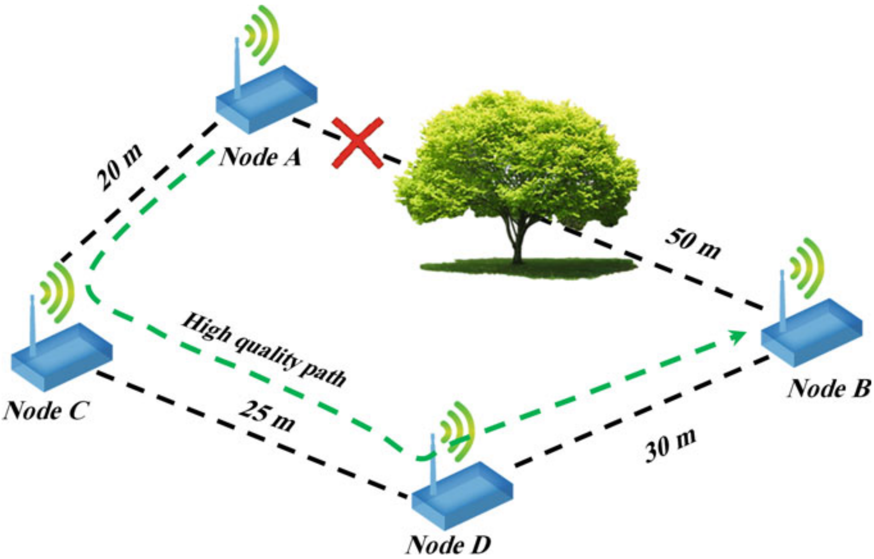

Fig. 9 Although the direct link from node A to B is less distance, the quality of path is more efficient to route traffic over node C and D that accepts a geographically longer path

the help of global positioning system (GPS) [28]. With this location information, a message can be routed to the ultimate receiver after including these information into routing algorithm in various ways [29]. Direct communication, whenever possible, is certainly the best way for data dissemination [22]. However, the quality of a link can be significantly decreased by obstacles such as buildings, trees, walls (see Fig. 9). Therefore, the researchers should take into consideration a signal strength metric than by using the geographical distance.

The 5G and 4G Technologies Enabled IoT

The fourth generation (4G) technology has been widely used in the IoT and continuously evolving to match the needs of the future networks [30]. The main generations evolved from 1G to 4G, recently work is progressing on 5G. With each technology, new features are added and issues are resolved. The 4G technology with long term evolution (LTE) provide high quality video stream and audio over end-to-end user with high bandwidth speed that could reach up to 1 Gbps. While the fifth generation (5G) is the next technology of mobile internet networks and is expected to be operational in next two years [31]. It is the extension of 4G LTE however with 10 times faster, higher data rates, more secure, lower latency, long battery lifetime, and reliable connections on smartphones and other devices than ever before (see Fig. 10). It expects to handle about

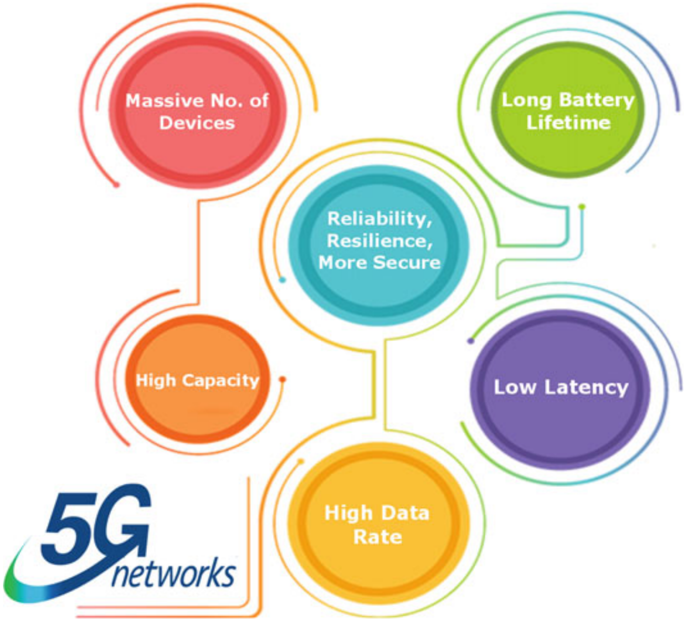

Fig. 10 5G enabled IoT innovation

more than 1000 times of mobile data than recent cellular systems. These features will certainly be expected to make the next generation is the optimal network and solution for IoT applications. This finding provides evidence that the 5G platform will help the IoT technology to meet the requirements of applications and market demands. In additional, it will become the solution of IoT applications such as non-orthogonal multiple access, non-orthogonal waveforms, massive MIMO systems, machine to machine (M2M) communications, etc.

Internet of Things Enabled by LiFi Technology

Light Fidelity (LiFi) is the wireless technology that uses the visible light communication networks instead of radio waves for data transmission. It is low cost and efficient technology due to it uses only LED lamp to transmit data. This technology provides highspeed, lightweight, secure and fully networked wireless via light. As we are aware that the light travels faster than the radio waves. Therefore, the data could be transferred 250 times faster than the high-speed broadband [32]. In additional, the technology involves visible light wavelength rather than radio waves that can lead to human disorders.

As the market for IoT-devices grows and tiny sensors are embedded to more and more things, buildings. Thus, these things produce huge amount of data and require

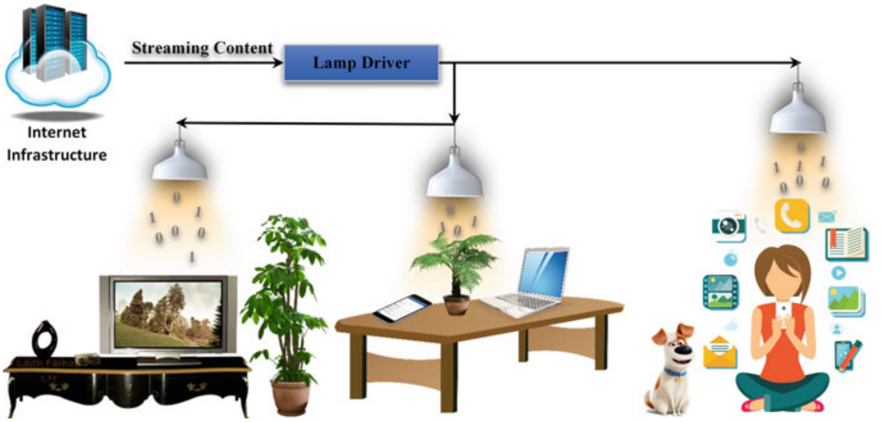

Fig. 11 LiFi-technology enabled IoT innovation

faster data transmission to reach the target. Therefore, LiFi technology offers many key benefits and best solutions for IoT networks in recent decade (Fig. 11).

Power Line Communication (PLC) for IoT Applications

PLC is a communication technology that carries data on a conductor and sending it over existing power cables. Nowadays, power supply lines not only use for power transmission but it also for data communication as a second job. It offers great ecosystems advantages and opens up a wide field for different applications [33]. A wide range of PLC technologies are used for different purposes such as smart grid, home automation, IoT, etc. Internet of Things is recently popular field and an innovation buzzword. It has several applications that will enable a smarter world such as smart home, smart cities, intelligent enterprise. At the concept of smart home, there is always an electronic network linked each other. So, with the PLC platform make it possible to create communications between a variety of devices/things by using any existing cable network. This finding provides a great opportunity that minimizes the cost to deploy and further expansion of the network [34] (Fig. 12).

Conclusion

In summary, with the emergence of IoT, new regulatory approaches to ensure its energy, scalability, Heterogeneity, human-in-the-loop, big data, etc. become necessary. The IoT revolution is expanding connectivity via the internet and a wide range of applications (e.g., actuators, sensors and other embedded systems). This will have

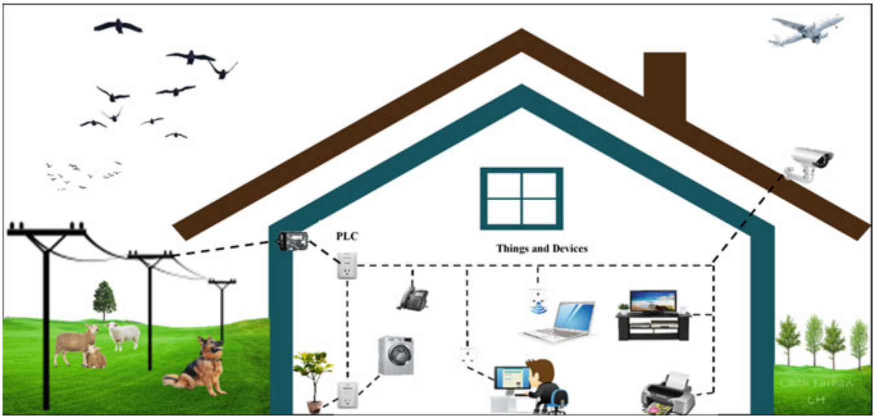

Fig. 12 PLC-technology enabled IoT innovation

an effect on the quality, different life styles and the way we behave and interact with humans, machines and devices in the future. Therefore, new research challenges and problems will emerge due to the largescale device proliferation and their intercommunication. This chapter gives an overview of the key issues related to the IoT services and technologies. A number of researcher challenges have been described, which are expected to become a major research trends in the next decade. A number of previous works and new technologies have been analysed, and most relevant WSN and IoT applications were presented.

Acknowledgements The authors would like to thank Ministry of Higher Education and Scientific Research (Iraq) and University of Diyala for the funding to conduct the research. Also, many thanks to Manchester Metropolitan University for their help and support.

References

1. S. Li, L. Da Xu, S. Zhao, The internet of things : a survey, Inf. Syst. Front. **17** (April 2014), 243–259 (2015)
2. W. Stallings, *Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud* (2015)
3. J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, Internet of Things (IoT): A vision, architectural elements, and future directions. Futur. Gener. Comput. Syst. **29**(7), 1645–1660 (2013)
4. A. Abuarqoub, M. Hammoudeh, B. Adebisi, S. Jabbar, A. Bounceur, H. Al-Bashar, Dynamic clustering and management of mobile wireless sensor networks. Comput. Netw. **117**, 62–72 (2017)
5. L. Farhan, R. Kharel, O. Kaiwartya, M. Quiroz-castellanos, A. Alissa, A concise review on Internet of Things (IoT)—problems, challenges and opportunities, in*11th International Symposium Communication System Networks, Digital Signal Processing, Hungary* (2018)
6. E. Pignaton de Freitas et al., Handling failures of static sensor nodes in wireless sensor network by use of mobile sensors, in *2011 IEEE Working International Conference* on *Advanced Information Networking* and *Applications* (2011)

7. L. Farhan, R. Kharel, O. Kaiwartya, M. Quiroz-castellanos, LQOR: link quality-oriented route selection on Internet of Things networks for green computing, in *11th International Symposium on Communication Systems Networks, Digital Signal Processing Hungary* (2018)
8. K.Y. Bendigeri, J.D. Mallapur, S.B. Kumbalavati, Recovery based fault tolerance in wireless sensor networks, in *International Conference* on *Electrical*, *Electronics Communication* and *Computational Optimum Technologies* (2017)
9. D. Couto, D. Aguayo, J. Bicket, R.M.A, High throughput path metric for multi-hop wireless routing. Wirel. Netw. **11**(4), 419–434 (2005)
10. N. Javaid, S. Cheema, M. Akbar, N. Alrajeh, M.S. Alabed, N. Guizani, Balanced energy consumption based adaptive routing for IoT enabling underwater WSNs. IEEE Access **5**, 10040–10051 (2017)
11. F. Al-turjman, M. Gunay, CAR approach for the Internet of Things approche de la CAR pour l' internet des objets. Can. J. Electr. Comput. Eng. **39**(1), 11–18 (2016)
12. A. Brogi, S. Forti, QoS-aware deployment of IoT applications through the fog. IEEE Internet Things J. **4662**(c), 1–1 (2016)
13. S. Muralidharan, B.J.R. Sahu, N. Saxena, A. Roy, PPT: a push pull traffic algorithm to improve QoS provisioning in IoT-NDN environment. IEEE Commun. Lett. **21**(6), 1417–1420 (2017)
14. B. Vejlgaard, M. Lauridsen, H. Nguyen, I.Z. Kovacs, P. Mogensen, M. Sørensen, *Interference impact on coverage and capacity for low power wide area IoT networks* (IEEE Wirel. Commun. Netw. Conf, WCNC, 2017)
15. W. Liu, K. Huang, X. Zhou, S. Durrani, Full-duplex backscatter interference networks based on time-hopping spreading spectrum. IEEE Trans. Wirel. Commun. **1276**(c), 1–16 (2017)
16. L. Farhan, A.E. Alissa, S.T. Shukur, M. Alrweg, U. Raza, R. Kharel, A survey on the challenges and opportunities of the Internet of Things (IoT), in *11th International Conference* on *Sensor Technologies* (2017)
17. M.R. Bashir, A.Q. Gill, A. Iot, Towards an IoT big data analytics framework : smart buildings systems, in *14th International Conference on Smart City* (2016)
18. J. Lloret, J. Tomas, A. Canovas, L. Parra, An integrated IoT architecture for smart metering. IEEE Commun. Mag. **54**(12), 50–57 (2016)
19. C. Liu, Y. Zhang, H. Zhang, A novel approach to IoT security based on immunology, in *Proceedings—9th International Conference* on *Computational Intelligence* in *Security, CIS 2013* (2013), pp. 771–775
20. D. Airehrour, J. Gutierrez, S.K. Ray, A lightweight trust design for IoT routing, in *2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, 14th International Conference on Pervasive Intelligence and Computing, 2nd International Conference on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech)* (2016), pp. 552–557
21. R. Lu, K. Heung, A.H. Lashkari, A.A. Ghorbani, A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced IoT, in *Spec. Sect. Secur. Priv. Appl. Serv. Futur. Internet Things*, vol. 5 (2017), pp. 3302–3312
22. L. Farhan, R. Kharel, O. Kaiwartya, M. Hammoudeh, B. Adebisi, Towards green computing for Internet of things: energy oriented path and message scheduling approach. Sustain. Cities Soc. **38**(July 2017), 195–204 (2018)
23. L. Farhan, A.E. Alissa, S.T. Shukur, M. Hammoudeh, R. Kharel, An energy efficient long hop (LH) first scheduling algorithm for scalable Internet of Things (IoT) networks, in *11th International Conference* on *Sensor Technologies* (2017)
24. B. Luo, Z. Sun, Research on the model of a lightweight resource addressing. Chin. J. Electron. **24**(4), 832–836 (2015)
25. R. Ma, Y. Liu, C. Shan, X.L. Zhao, X.A. Wang, Research on identification and addressing of the Internet of Things, in *Proceedings—2015 10th International Conference on P2P, Parallel, Grid, Cloud Internet Computing 3PGCIC 2015* (2016), pp. 810–814
26. I. Bedhief, M. Kassar, T. Aguili, SDN-based architecture challenging the IoT heterogeneity, in *2016 3rd Smart Cloud Networks System SCNS 2016* (2017), pp. 14–16

27. C. Sarkar et al., DIAT: a scalable distributed architecture for IoT. IEEE Internet Things **2**(3), 230–239 (2015)
28. L. Farhan, L. Alzubaidi, M. Abdulsalam, A.J. Abboud, M. Hammoudeh, R. Kharel, An efficient data packet scheduling scheme for Internet of Things networks, in *Diyala Third* Scientific *Conference* of *Engineering Science, 1st Diyala Inernational. Conference* of *Engineering Science 2018* (2018)
29. R. Baumann, S. Heimlicher, M. Strasser, A. Weibel, A survey on routing metrics, in *TIK Report 262, ETH-Zentrum, Computer Engineering* and *Networks* Laboratory (2007)
30. S. Li, L. Da Xu, S. Zhao, 5G Internet of Things: a survey. J. Ind. Inf. Integr., (January), 1–10 (2018)
31. M.B. Yassein, S. Aljawarneh, Challenges and features of IoT communications in 5G networks, in *2017 International Electrical* and *Computing Technologies* and *Applications* (2017)
32. M. Aswin, A.R.G, L.V.S.M, Iot enabled by Li-Fi technology, in *Proceedings of Nattional Conference on Communications and Informatics-2016* (2018)
33. G. Bernhard, A.M. Lehmann, J.B. Huber, A power line communication topology module for NS-3 and DCE, in *IEEE International Conference* on *Smart Grid Communications*, no. October, pp. 295–301 (2017)
34. A.A. Zhilenkov, D.D. Gilyazov, I.I. Matveev, Y.V. Krishtal, Power line communication in IoT-systems, in *2017 IEEE Conference* of Russian *Young* Researchers in *Electrical* and *Electronic Engineering* (2017)