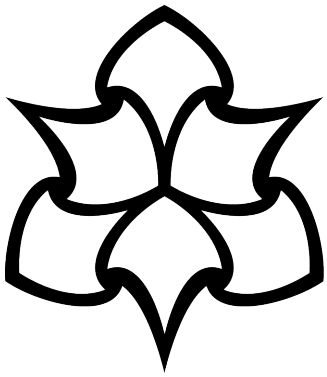

A Concise Review on Internet of Things (IoT) - Problems, Challenges and Opportunities

Laith Farhan*, Rupak Kharel†, Omprakash Kaiwartya‡, Marcela Quiroz-Castellanos§, Ali Alissa¶ and Mohamed Abdulsalam†
*School of Engineering, Manchester Metropolitan University, UK, University of Diyala, Iraq
†School of Engineering, Manchester Metropolitan University, UK
‡School of Science & Technology, Nottingham Trent University, UK
§Artificial Intelligence Research Center, Universidad Veracruzana, Mexico
¶School of Computer Science, University of Plymouth, UK

***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 paper looks into providing a concise review of the concepts on IoT and applications describing the main components and features. Furthermore, open issues and challenges that need addressing by the research community and some potential solutions are discussed.**

***Index Terms*—Internet of things (IoT); wireless sensor networks (WSNs); challenges and opportunities.**

I. Introduction

Internet of Things is a symbiosis of various technologies and is going to change drastically what can be achieved from the internet currently. IoT works with various enabling and emerging technologies such as wireless sensor networks (WSNs), sensor technologies, machine learning and artificial intelligence (AI), big data and analytics, etc. At the heart of IoT is WSNs, consisting of sensors deployed in a sensing area to monitor specific phenomenons (such as environmental monitoring) and collect data [1]. Furthermore, even more pervasive network configuration are being developed where all possible devices (mostly of heterogeneous nature) connect with each other to sense, gather and analyse data of different nature to act upon the intelligence gained from deep insights of the data. These actions are mostly without human interaction [2]. The word IoT was first made popular by Kevin Ashton in 1999, when he implemented radio frequency identification (RFID) for application in supply chain management [3]. Since then IoT has been used to define a paradigm of any possible devices or things that can be connected to the internet for data collection, knowledge formation and automation. The concept of IoT has generated a lot of attention by governments, industries and researchers. According to a forecast from the U.S. National Intelligence Council (NIC) in 2008 "by the 2025 internet sensors may be implemented in everything such as plants, food packets, vehicles, furniture, etc". In the world population of 7.2 billion in 2015, there were 25 billion devices connected to the internet, i.e. 3.47 connected devices per person. This number is expected to rise to 50 billion with 6.58 connected devices per person (with a world population of 7.8 billion) [4].

The communication in the IoT applications will normally constitute the following connections as seen in Fig. 1 [5]:

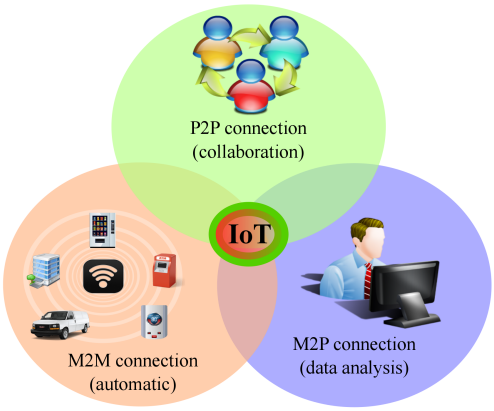

Fig. 1: Internet of Things (IoT) elements.

- **People to People (P2P) connection:** is the data transfer from one person to another. It occurs through video call, telephone call, and social communications. It is usually called collaboration connection.
- **Machine to People (M2P) connection:** is the data transfer from machines such as computers, sensors or others to users to analyse it. For example; weather forecasting uses smart devices to gather the data from the environment and send it back to the administrators in the control center for further analysis.
- **Machine to Machine (M2M) connection:** is the data transfer between devices without human interactions. For instance, a car talking to another car about its speed, lane change or braking intentions, etc.

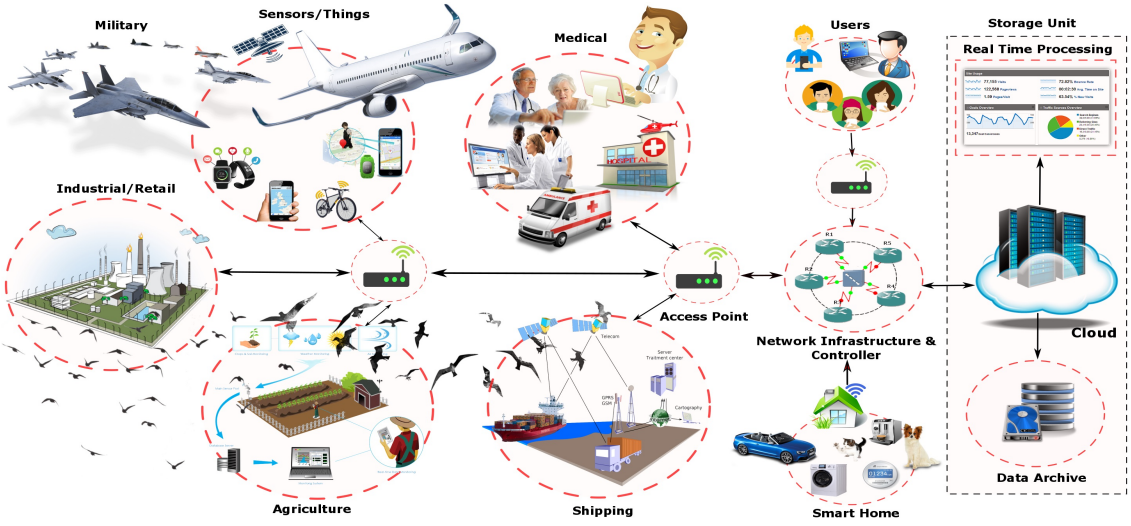

Fig. 2: Internet of things (IoT) architecture.

The communication of IoT networks combining three main categories based on their technology elements can be summarized into a simple relation as below:

$$IoT = Human + Physical\ Objects\ (sensors, controllers, actuators, devices, computing, storages) + Internet$$

Figure 2 shows the interconnection among the various applications based on the IoT technology with some use-cases and examples.

IoT has several applications that will enable a smarter world. Smart cities with functionalities such as smart parking, smart lighting, smart road and congestion control, waste management, etc. will make urban life efficient and smooth. Furthermore, various environmental monitoring application to monitor air pollution, earthquake early detection, forest fire detection, etc can be implemented to protect human life and resources. Another application is on water supply where intelligence can be incorporated to understand the water demand and monitor water quality. This will not only help achieve the sustainability goal but will also have major impact on human health. Smart meters are already part of many household to monitor the electricity and gas usage. This will help people understand the energy consumption and will allow the supplier to analyse demand real time. IoT is also being applied in industry and factory and it is expected to bring a fourth industrial revolution, Industry 4.0, where IoT and digital technology will help ensure maximum efficiency, reduced manufacturing cost with increased quality. Smart agriculture and farming is another area where IoT will have major impact in the near future. With global population expected to be close to 8 billion by 2025 and 9.6 billion by 2050, the food production is required to be increased by 70% by 2050 to keep up with the demand. IoT can provide solutions and methods for precision crop monitoring and disease diagnosis using different data sources, remote sensing, ground sensing/camera phone images. Various sensors located in the fields will allow farmer to obtain detailed maps of topography and resources in the area. Also data such as acidity, temperature, moisture level of the soil will provide valuable insight to increase crops productivity. Moreover, climate forecasts and weather predictions can be tied with smart irrigation. Finally, IoT is also set to revolutionize the health sector. Various application such as fall detection, patient surveillance, intelligent drug delivery, early detection of cancers and other diseases, etc will change the way how health sector will operate in the future. All of these advantages will not come without problems and limitations such as heterogeneity and scalability issues, privacy, security and trust issues, energy optimization issues and problems due to massive datasets.

The structure of this paper is going to be as the following: Section I introduced an overview of IoT technology and applications. In section II, we explore various challenges and opportunities of IoT system such as addressing schemes, big data, energy consumption, transmission media, human-in-the-loop, devices/links heterogeneity and massive scaling. Issue of security and quality of service are also presented in the section II. Finally, we make some concluding remarks in section III.

II. Challenges and Impediments

Despite the proliferation of many applications of IoT these days it is still in its early stage and therefore several challenges and restriction are present which is summarized in Fig. 3. WSNs is one of the key underlying enabling technology for IoT therefore this study has also taken into account some previous works in the field of WSNs. In what follows, we shall shed light on some of the design issues and challenges that is currently hindering IoT to achieve its fullest potential.

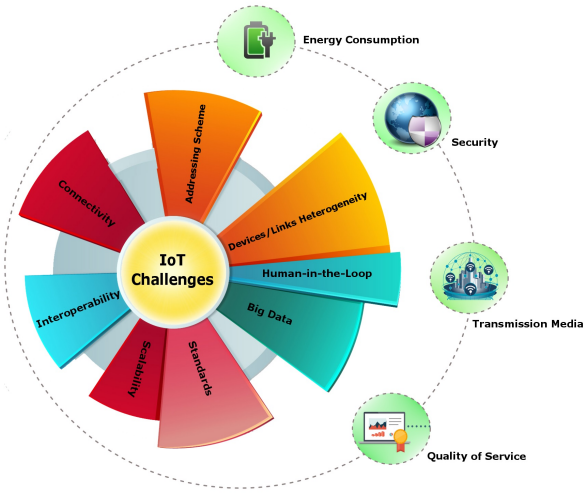

Fig. 3: IoT Challenges and Impediments.

A. Addressing Schemes

Uniquely identifying objects is a critical issue for the operation and success of IoT applications. IoT applications require to uniquely classify thousands of devices and to manage and control them remotely through the internet. The few most critical features of creating unique address are reliability, uniqueness, scalability and persistence [6]. 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) [4]. A group of researchers [7] designed a lightweight addressing scheme to solve IoT heterogeneity problem. 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. [8] proposed 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.

B. Big Data

IoT leverage massive amount of data collected and aggregated via smart objects and is one of the most striking features of IoT. It will be necessary to develop techniques that convert this data into usable knowledge. Every two years, data is doubling in size and is expected to reach 44 Zettabytes in the next four years [9].

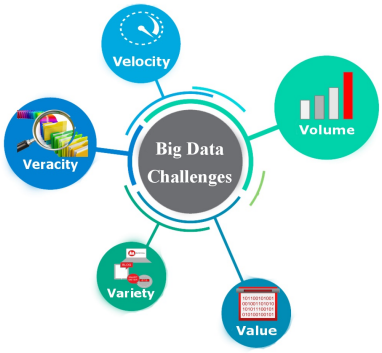

Fig. 4: The "$5V$" Challenges.

The "$5V$" (Value, Velocity, Volume, Variety, and Veracity) are important challenges in IoT applications as can be seen in Fig. 4.

- **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 the application.
- **Volume:** is the amount of all types of data that is collected, stored, retrieve, 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 AI 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 IoT field. Authors in [10] 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 showed the monitoring and control of a large amount of data without human intervention and improved users experience. Previous study in [11] has 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 showed 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.

C. Energy Consumption

IoT creates billions of devices and networks with large variety connected to the internet. Energy is considered as a crucial resource for IoT smart devices because most of the applications are powered by battery or uses energy harvesting techniques. This means it is not prudent to waste the energy by transmission of unneeded data and protocol overheads that existing protocols such as HTTP, TCP, etc., do. Hence, designing energy efficient network architecture and intelligent routing mechanism is still a great challenge in IoT networks [2]. The study by [12] introduced a new scheduling algorithm for nodes located between two or more sensing fields. S-MAC protocol intended the border nodes that consume a large amount of energy and adopted different sleep and listen schedules. These nodes switch to the listening mode often due to diversified scheduling. The work focused on minimizing the energy consumption for border nodes and hence extended the lifetime in WSNs. Authors in [13] used technique of clustering the sensing field into groups where each group have message broker that collects the information from sensors and delivers it to the intended destination. The proposed algorithm revealed the effectiveness and efficiency in terms of energy consumption and service response time. Work done in [14] proposes heterogeneous dual processor a fast coreH and ultra-low power near threshold coreL respectively. The proposed work increased system performance without packets deadline and uses slightly less power. If IoT is to have sustainable impact then energy consumption is right at the top of the agenda. A typical scenario where battery runs out of the nodes demanding change in the battery is not feasible since this means battery change in millions of nodes for a particular application. Therefore, IoT should work more or less in a throw away mechanism where nodes last for as long as possible and is discarded once the life ends.

D. 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, etc. In WSNs, most of the sensors are homogeneous, i.e., having the same power, communication, and equal capacity in terms of computation. IoT implements a wide variety of networks, links, and devices connectivity to provide different services. Thus, heterogeneous nature of links and objects play a critical role in the interconnection of the IoT devices and thus adds a unique challenge to address. Therefore, the question might be, is it possible to have a unified architectural model that can be deployed such that it is able to support these wide ranges of devices and applications? In [15] an architecture is presented for heterogeneity of devices and networks based on SDN-Docker techniques. The proposed work showed 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 [16].

E. 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 or receive the data such as RFID, Bluetooth, Zigbee, LoraWAN, Sigfox, etc. The traditional problems associated with transmission media (e.g., high error rate, bandwidth, fading, inference, etc.) exists for IoT as well. Each transmission medium requires specialized energy, network hardware, the bandwidth that has to be compatible with that medium. Therefore, optimizing the TM is a challenge in IoT applications to sustain and prolong the lifetime of networks.

According to study in [17], author have discussed and analysed 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 up-link and downlink failure rates of less than 1%. Furthermore, improvement of indoor coverage up to 99% is also shown. In a different study [18], authors designed full-duplex wireless IT and used backscatter antennas to reduce latency and energy consumption from reader to the target. The proposed scheme suppressed interference from co-existing links. It also enabled simultaneous backward/forward information transfer.

F. 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. 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. 5:

- **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

Fig. 5: Security Challenges.

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.
- **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.

G. Quality of Service (QoS)

In many applications, gathering data needs to be delivered within a certain time to the intended destination else the data will be of less value. The QoS requirements are met with differentiated services and delay management, packet loss, and bandwidth parameters on a network. These requirements become the secret to a successful end-to-end service. Therefore, quality of service needs research and stabilization for implementation, optimization and management. In reference [22], the authors present a general model to support the QoS-aware deployment of multi-components IoT cloud infrastructures. The proposed model introduced suitable operational systemic qualities of fog facilities. Another study, authors [23] showed 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.

H. 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 talk about 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, in 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 algorithm in such circumstances?

I. Massive Scaling

The number of sensor nodes deployed in the world may be in order of tens of billion or even more. Massive scaling is a serious challenge which influences the routing protocols. Scalability is the increasing number of devices and networks after IoT is launched. Therefore, any routing scheme must be fit and be scalable enough for these huge number of sensor nodes [24]. In [25], the authors suggested unique integration scheme between named data network and pub/sub systems. This approach achieved scalable IoT cloud services. In another study [26], authors enhance the scalability for the efficient IoT cloud integration which supports dynamic management and resource provisioning. The reported results illustrate MQTT and CoAP protocols can guarantee support for constrained and unconstrained devices and also network scalability.

J. The 5G and 4G Technologies enabled IoT

The fourth generation (4G) technology has been widely used in the IoT and has continuously evolved to match the needs of the future networks [27] and recent work is progressing towards fifth generation (5G). With each technology, new features are added and issues are resolved. 4G technology with long term evolution (LTE) provides high quality video stream and audio over end-to-end user with high bandwidth speed that could reach upto 1 Gbps. 5G is the next technology for mobile internet networks and is expected to be operational in the next two years. It is the extension of 4G LTE however 10 times faster, higher data rates, more secure, lower latency, long battery lifetime and reliable connections on smartphones and other devices [28]. It expects to handle about 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.

III. Conclusion

To this end, significant progress has been made in the IoT technology for a wide range of applications that utilize various enabling and emerging technologies. IoT simply integrates and interconnects large number of devices utilizing the latest communication infrastructure and computing prowess. This allows to exchange and collect data in a seamless manner forming useful knowledge. IoT is a concept that is going to change how internet works and integrate cyber and physical space in an ubiquitous manner. As much as the benefits IoT potentially have, it also suffers from various challenges and problems and a concise summary is provided in this paper. For a successful adoption of IoT, counter measures should be taken at the architectural and design level with a holistic approach.

Acknowledgment

The authors would like to thank Ministry of Higher Education and Scientific Research (Iraq) and the University of Diyala for the funding to conduct the research and Manchester Metropolitan University (UK) for the support.

References

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE Communications Surveys Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.

[2] L. Farhan, R. Kharel, O. Kaiwartya, M. Hammoudeh, and B. Adebisi, "Towards green computing for Internet of Things: Energy oriented path and message scheduling approach," *Sustainable Cities and Society*, vol. 38, pp. 195 – 204, 2018.

[3] L. Shancang, X. Li, Da, and Z. Shanshan, "The Internet of Things: a survey," *Information Systems Frontiers*, vol. 17, no. 2, pp. 243–259, Apr 2015.

[4] M. R. Palattella, N. Accettura, X. Vilajosana, T. Watteyne, L. A. Grieco, G. Boggia, and M. Dohler, "Standardized protocol stack for the Internet of (Important) Things," *IEEE Communications Surveys Tutorials*, vol. 15, no. 3, pp. 1389–1406, 2013.

[5] L. Farhan, L. Alzubaidi, M. Abdulsalam, A. J. Abboud, M. Hammoudeh, and R. Kharel, "An efficient data packet scheduling scheme for Internet of Things networks," in *Proc. IEEE Diyala Third Scientific Conference of Engineering Sciences and 1st Diyala International Conference of Engineering Sciences*, Jan 2018.

[6] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645 – 1660, 2013.

[7] B. Luo and Z. Sun, "Research on the model of a lightweight resource addressing," *Chinese Journal of Electronics*, vol. 24, no. 4, pp. 832 – 836, 2015.

[8] R. Ma, Y. Liu, C. Shan, X. L. Zhao, and X. A. Wang, "Research on identification and addressing of the Internet of Things," in *Proc. IEEE 10th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), Krakow*, no. 4, Nov 2015, pp. 810–814.

[9] L. Farhan, A. E. Alissa, S. T. Shukur, M. Alrweg, U. Raza, and R. Kharel, "A survey on the challenges and opportunities of the Internet of Things (IoT)," in *Proc. IEEE 11th International Conference on Sensing Technology, Sydney*, Nov 2017.

[10] M. R. Bashir and A. Q. Gill, "Towards an IoT big data analytics framework: Smart buildings systems," in *Proc. IEEE 18th International Conference on High Performance Computing and Communications, Sydney*, 2016, pp. 1325–1332.

[11] J. Lloret, J. Tomas, A. Canovas, and L. Parra, "An integrated IoT architecture for smart metering," *IEEE Communications Magazine*, vol. 54, no. 12, pp. 50–57, Dec 2016.

[12] D. Saha, M. R. Yousuf, and M. A. Matin, "Energy Efficient Scheduling Algorithm For S-Mac Protocol In Wireless Sensor Network," *International Journal of Wireless & Mobile Networks*, vol. 3, no. 6, pp. 129–140, 2011.

[13] S. Abdullah and K. Yang, "An Energy Efficient Message Scheduling Algorithm Considering Node Failure in IoT Environment," *Wireless Personal Communications*, vol. 79, no. 3, pp. 1815–1835, dec 2014.

[14] Z. Wang, Y. Liu, Y. Sun, Y. Li, D. Zhang, and H. Yang, "An energy-efficient heterogeneous dual-core processor for Internet of Things," in *Proc. IEEE International Symposium on Circuits and Systems (ISCAS), Lisbon*, May 2015.

[15] I. Bedhief, M. Kassar, and T. Aguili, "SDN-based architecture challenging the IoT heterogeneity," in *Proc. IEEE 3rd Smart Cloud Networks Systems (SCNS), Dubai*, Dec 2016.

[16] C. Sarkar, A. U. N. S. N., R. V. Prasad, A. Rahim, R. Neisse, and G. Baldini, "DIAT: A scalable distributed architecture for IoT," *IEEE Internet of Things Journal*, vol. 2, no. 3, pp. 230–239, June 2015.

[17] B. Vejlgaard, M. Lauridsen, H. Nguyen, I. Z. Kovacs, P. Mogensen, and M. Sorensen, "Interference impact on coverage and capacity for low power wide area IoT networks," in *Proc. IEEE Wireless Communications and Networking Conference (WCNC), San Francisco*, March 2017.

[18] W. Liu, K. Huang, X. Zhou, and S. Durrani, "Full-duplex backscatter interference networks based on time-hopping spread spectrum," *IEEE Transactions on Wireless Communications*, vol. 16, no. 7, July 2017.

[19] C. Liu, Y. Zhang, and H. Zhang, "A novel approach to IoT security based on immunology," in *Proc. IEEE Ninth International Conference on Computational Intelligence and Security, Leshan, China*, Dec 2013, pp. 771–775.

[20] D. Airehrour, J. Gutierrez, and S. K. Ray, "A lightweight trust design for IoT routing," in *Proc IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, Auckland*, Aug 2016, pp. 552–557.

[21] R. Lu, K. Heung, A. H. Lashkari, and A. A. Ghorbani, "A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced IoT," *IEEE Access*, vol. 5, pp. 3302–3312, 2017.

[22] A. Brogi and S. Forti, "QoS-aware deployment of IoT applications through the fog," *IEEE Internet of Things Journal*, vol. PP, no. 99, pp. 1–8, 2017.

[23] S. Muralidharan, B. J. R. Sahu, N. Saxena, and A. Roy, "PPT: A push pull traffic algorithm to improve QoS provisioning in IoT-NDN environment," *IEEE Communications Letters*, vol. 21, no. 6, pp. 1417–1420, June 2017.

[24] L. Farhan, A. E. Alissa, S. T. Shukur, M. Hammoudeh, and R. Kharel, "An energy efficient long hop (LH) first scheduling algorithm for scalable Internet of Things (IoT) networks," in *Proc. IEEE 11th International Conference on Sensing Technology, Sydney*, Nov 2017.

[25] S. Han and H. Woo, "NDN-based Pub/Sub system for scalable IoT cloud," in *Proc. IEEE International Conference on Cloud Computing Technology and Science (CloudCom), Luxembourg*, Dec 2016, pp. 488–491.

[26] P. Bellavista and A. Zanni, "Towards better scalability for IoT-cloud interactions via combined exploitation of MQTT and CoAP," in *Proc. IEEE 2nd International Forum on Research and Technologies for Society and Industry Leveraging a better tomorrow (RTSI), Bologna*, Sep 2016.

[27] S. Li, L. D. Xu, and S. Zhao, "5G Internet of Things: A survey," *Journal of Industrial Information Integration*, 2018.

[28] M. B. Yassein, S. Aljawarneh, and A. Al-Sadi, "Challenges and features of IoT communications in 5G networks," in *2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA)*, Nov 2017.