International Journal of Engineering & Technology, 7 (2.7) (2018) 131-137

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research Paper



Performance evaluation of IOT systems – basic issues

K.V. Sowmya[1*], Dr. JKR Sastry[2]

Department of Electronics and communication engineering, KLEF (Deemed to be University), Vaddeswaram, Guntur
*Email: sowmyakambhampati@kluniversity.in

Abstract

Internet of things (**IOT)** is a layered network and generally heterogeneous as communication between small things like digital cameras and big things like servers has to happen. The communication speeds of various devices connected on to **IOT** are in great variance affecting the performance of the entire network. The small devices connected on to IOT are fragile in the sense that they tend to fail quite often affecting the performance of the network. The small devices are low in energy depletion of which is rather fast. The small devices also have heavy latency. Many such issues exists that effect the performance of an IOT network. In this paper, various issues/bottlenecks that hamper the performance of an IOT network are and a mitigation strategy for improving the performance of the IOT networks is discussed**.**

Keywords: *Performance Bottlenecks, IOT, power management of small devices, latency of small devices, performance mitigation strategies for small devices*

1. Introduction

Internet of things (IoT) is the most focused subject especially for collecting the data through low end sensors and transmitting the same to the high end data server through gate ways. The low end data collecting devices such as sensors are low in energy, designed to deal with low band widths and the latency of data transmission is very high.

IoT networks are developed through use of hierarchy of sub-nets. Communicating data collected by low end sensors to high end data servers through hierarchy of networks in real-time most reliably is the one of the most important issue.

The communicating devices are heterogeneous, meaning they use different protocols for communication. Ability to achieve greater performance when communication has to be done using heterogeneous protocols is yet another issue.

Many applications are being developed to run on an **IoT**. Choosing a network topology suited to the kind of applications being implemented is one of the Major issues. Optimum selection of network resources as required for establishing the required speeds for communication is yet another most important issue.

Addition of cognitive intelligence into IoT network is required so as to adjust the network as per the prevailing condition at the time of data transmission. Addition of cognition into IoT networks enhances the performance of the IoT.

Numbers of issues are to be considered to enhancing the performance of an IoT network considering the kind of application to be implemented.

This paper presents some of the basic issues and prioritization of the same for enhancing performance of the IoT networks.

2. Related work

The subject on IOT is of recent origin and not much elaboration has been done on basic issues like performance, fault tolerance, security etc. Some contributions have been dealt in the literature the elaboration of which is provided in the following paragraphs.

The use of IoT is growing rapidly. Millions of sensing devices are being connected to IOT. Many industries that include utilities, healthcare, logistics, home automation, space management etc. are groping into use of IOT for data acquisition, storage and analysis [1]. The problem collecting data from multiple sources and disseminating the same to multiple consumers is being tackled through use of IoT. Middleware elements are being added to be able to collect streams of raw data, process an fuse the same and disseminate the same to multiple consumers in parallel streams. One issue is the kind of intelligent to be added to the middleware such that the data capturing, processing and dissemination of the same without affecting the real time requirement of the IoT implementation.

IOT is read and related with many other fields such as smart computing, cloud computing, high performance computing, grid computing smart computing etc. Use of IOT along with other fields of computing has been the future. The connection between the IOT and other fields of computing must be explored especially from the performance point of the IOT networks. A study has been presented [2] that relate High performance computing to IOT In the study several devices have been discussed which enable high performance computing within IOT networks. Several combinatorial optimization issues that relate to high performance considering IOT and HPC have been presented.

Wireless Local area networks (WLAN) in 1GHz band are expected to be used extensively as a part and parcel of the IOT network. WLANs are also expected to be used in machine to machine (M2M) applications as well. A new standard IEEE

Copyright © 2018 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

802.11 is drafted that supports long range, energy efficient communication in dense network environments. The standard is aimed at significant performance improvements in high contention areas. To achieve high performance a mechanism called restricted access window (RAW) has been included into the standard. The performance of RAW has been analyzed [3] considering various holding schemes and new holding scheme has been proposed which is based on states of the transmitting and receiving stations. It has been shown that the scheme improves saturation throughput and energy efficiency of the network thereby improving the performance of the network. The new standard 802.11ah improves the overall network performance especially when used for establishing communication among devices that are connected on to IOT. The standard also helps in seamless integration of these devices with other devices designed into the network.

Selecting an appropriate communication technology for establishing IOT for a specific application such as monitoring water resources within a specific area is one the most important challenges that must be met. Wireless technologies are extensively used for effecting communication among devices connected on to IOT. Wireless technologies are in existence in various forms and modes. Selecting the most important technology that leads to high performance is one of the most important issues [4]. Experiments are conducted for selecting best versions of the wireless standards and compute the impact of the same considering the performance of those technologies under many varied environment such as straight road, open ground, moderately and densely wooded area, inside concrete building and the top of high raised buildings. The deployment of these communication devices into a network in most appropriate manner is one of the basic challenges that one should meet considering the performance of IOT networks.

Performance evaluation of an IOT network in real-time is the most critical issue. Communication among the devices is the real issue in an IOT network. Communication among the devices has become quite complicated with the invention and introduction of numerous devices that can be connected on to IOT. Several applications can be implemented using IOT. Information can be collected from various things which are interconnected using many other things. IOT technologies should be such that the real time requirements of certain applications must be met with. The responses to certain requirements must be met in real time. Performance evaluation of the IOT systems which are expected to give real time response is quite complicated. Modelling the performance evaluation of the IOT network that is expected to provide real time response has been presented [5]. Feedback control theory has been applied for modelling the performance evaluation. In this work, things in the network are represented as control objects. The overall system model that represents IOT is developed using things as control objects. The model as such is validated through numerical analysis by varying different parameters and noticing the performance of the system.

Many IOT based applications exists that involve transmitting secure images over the network. Applications that can be categorized as smart which include heath care, structures, transportation etc. requires exchange of images and videos. Very high performance of IOT is required when images or videos are to be transmitted over the network as continuous streaming is required and also that the data sizes are too huge. Prototyping of such a system is required before embarking on the development of the real and full pledged system. A modular and extensible architecture for building an IOT system that caters for communicating the images and videos has been proposed [6]. The prototypes can be built using the off-the-shelf components and the proposed architecture. A prototype has been developed using the architecture for implementing target tracking and acquisition system. The architecture has been used for implementing proportional-integral-derivative control, custom target acquisition algorithm, and sliding-window-based algorithm. More modules can be added for implementing more complex applications such as search-and-rescue, automatic object tracking, and traffic congestion analysis.

Hardware architecture for a new compression algorithm (BPG – Better portable Graphics) has been proposed using the quadrotor architecture. BPG out performs JPEG (Joint photographic experts Group) when it comes to image compression and quality of the image. The architecture has been presented with the objective for achieving real time image compression. The architecture has also been used for the development of a prototype representing a secure digital camera integrated with a secure image compression using BPG. The architecture could be extensively used for implementing an IOT application dealing with high performance imaging. Prototyping of the application has been done using Simulink.

The predictability of the behavior of the IOT devices that use the wireless communication is complex. Modelling of the behavior of the devices and IOT networks becomes especially when wireless communication is used becomes quite important in the absence of which it is quite difficult to assess the performance of the IOT networks. An IOT network as such can be represented as two node, three node and multi node network. A two node IOT can be implemented using a bidirectional wireless communication systems. It is necessary to model security and energy awareness of such a system even if little knowledge exists on the synergetic effect considering the awareness about security and energy consumed by such systems under the influence of many environmental conditions such as noise. A modelling framework has been presented that help modelling security-energy-environment which can be used as QoS for IOT networks. IOT units can be modelled using feature-based methodology which is adopted from software engineering domain. One can arrive at feature models that can describe security-environment-performance relationship under constraints imposed by certain applications. Using the feature models one can select configurations that are best suited for a given IOT application with respect to QoS requirements [7]. Feature models help representing abstract relationships between various domain factors. However experiments are to be conducted to arrive concrete values for modelled features. An experimental system has been described that can measure energy consumption under the influencing factors. Both abstract and concrete models can be used for reasoning QoS of IOT networks.

Effecting machine-to-machine communication when the sensors, gate ways and remote servers are connected unreliable, loss of communication links intermittently and also unreliable links is a challenge especially when no compromise can be made on the real-time response requirements.

The efficiency and speed of communication is very must dependent on the kind of protocol used for effecting the communication. The performance of an IoT based system is dependent on the kind of protocol used. It becomes necessary to compare existing protocols from the performance point of view given environmental conditions in which the IoT system is expected to be used. The IoT protocols that include MQTT (Message Queuing Telemetry Transport), DDS (Data Distribution Service), CoAP (Constrained Application Protocol) and UDP-based protocol must be compared to find the performance with reference to a specific application in use. The performance of an IoT system can be computed in terms of use of bandwidth, data latency and reliability. An appropriate protocol must be chosen considering all kinds of protocols that can be used [8].

IoT based applications generally deal with sensitive applications. Any attacking on the data sensed by the device will affect the functioning of entire application. The data may also be transmitted by the unconnected device on to the network as well. Ever device must be authenticated so the devices are allowed to transmit the data. I will be too complex and time consuming if every device has to be authenticated when numerous devices are connected on to the network. The performance of an IoT network suffers when too many measures are to be used for securing the information

sensed and transmitted over the network. Group based authentication is one such method that reduces the delay in transmission enormously [9].

IoT market is becoming competitive. IoT devices are available in different forms starting from small devices to complex devices that include intelligent and smart devices. Developers' different low-cost, low performance CPU based systems and high cost, high performance GPUs and FPGAs. Both types of options through several design challenges in terms of effort required for design and development. A design flow is presented that trades off cost, power, performance, and volume of transactions handled. The designing of computer vison related to application has been presented using the design flow [10].

Many network topologies are in use for constructing IOT based networks. It is not possible to provide a single network can provide the quality of service required by different types of applications that run on different environments. There can be several IOT based solutions for implementing the same application. It becomes an issue to select most suitable solution for a given application. A framework has been proposed using which one can select most suitable IOT based solution for implementing an application in a specified environment [11]. The framework helps to assess the performance of a solution chosen to implement an application under a defined environment. The performance evaluation of several solutions can then be compared to find the best solution. A modelling technique has been built into the framework which has been proved to find the best solution to at least 85% accuracy.

Network coding technique can be conveniently used within IOT with an aim of reducing the energy requirements for running an IOT. The applications implemented through IOT can be modified to include network coding so as to enhance the performance of the application. It has been presented to show how network coding helps in improving the performance considering the communication that takes place among the IOT devices [12]. The network coding based communication has been effected within two important components of IOT which include IOT core network where data is sensed and transmitted, and distributed cloud storage where data captured in the core network layer is stored.

An adaptive network coding scheme is implemented in the core network where data is sensed and transmitted. Transmission efficiency can be improved through this method. The efficacy of the scheme is also roved the comparison of the performance of the scheme with the performance of similar such schemes. A storage allocation strategy has also been presented considering the network coded distributed cloud storage which aims at determining most reliable allocation that distributes n data elements into N data centers

IOT networks are characterized by real-time communication, and decision making capability of the sensors deployed for data collection which are integrated into many of the real life objects. It is necessary to predict the performance of IOT based networks so as to determine performance bottlenecks if any exists, design optimal sleep/wakeup schedules and application aware performance tuning [13]. However predicating performance is most difficult task due the varying needs of the applications and due to the existence of resource constrained sensors. The factors that affect the performance of the IOT networks must be analyzed may be using some simulation models. It is also necessary to assess the impact caused by the behavior of a node in the network on overall performance of the network. Markova Chains can be effectively used for the purpose. The probabilities of steady state transition of transmit and receive states can be computed using protocol execution traces which can then be used for predicting throughput.

Several M2M networks can be arranged hierarchically such that energy efficient routing protocols can be implemented for data transmission between source and sink via cluster heads in a WSN. Periodic network congestion caused by heavy M2M network can be managed through implementing load balancing thereby achieving high levels of network performance.

The network life time can be extended by clustering multiple sinks in a low wireless personnel area network with IPv6 protocol. The performance of such network can be optimized through non liberalization of integer data. The network performance optimization is solved through use of self-organizing cluster head to sink algorithm (SOCHSA), discrete particle swarm optimization (DPSO) and genetic algorithm (GA) as evolutionary algorithms [14].

Computational results prove that DPSO outperforms GA regarding complexity and convergence, thus being best suited for a proactive Internet of Things network. The mechanism proposed satisfies different network performance requirements of M2M traffic by instant identification and dynamic rerouting.

Securing the IoT devices has become one of the most important issues. Implementing cryptography within these devices is complex, expensive and also causes very heavy latency in the communication. Custom hardware that has been included in it the cryptography needs to be upgraded from to time when the new versions are to be implemented.

There is an urgent and critical need for reconfigurable, low-power and high-performance cryptography implementations for IoT devices. Use of FPGA provides such an opportunity to develop devices that can be reconfigured from time to time. FPGAs can be used for implementing symmetric cryptography, asymmetric cryptography, and secure hash functions. It has been proved that FPGA-based reconfigurable cryptographic components consume between1.8×and 4033×less energy and run between1.6×and 2983× faster than the software implementation. At the same time, the FPGA implementation of cryptographic operations is more flexible compared to custom hardware implementations of cryptographic components [15]

In IoT more and more application specific standards are being released from time to time. Smart metering is being achieved by the energy sector as it enhances the customer satisfaction. Smart metering is leading to smart metering network. A new cellular technology for providing wide area coverage for IoT and for facilitating MTC has been released [16]. It has been presented the way the technology can be sued for implementing smart metering. The capacity of such a system to handle energy quantum has also been presented.

The eco system of IoT has been growing tremendously changing the people around the world are going to live in. The device that are connected on to IoT are low power devices and are used form small scale setup that leave no room for building security in those devices. The power of the devices in terms of processing and storage is not good enough that the robust security algorithms can be built. The performance of a device when security is built into is a big issue. There are many cryptographic libraries which are in existence and include FLECC_IN_C and Crypto++ that contain many cryptographic algorithms. The suitability of these libraries for building security within the devices in terms of performance in constrained environment of those devices must be verified so that the best one can be selected and implemented [17].

LoRA and NB-IoT are two wireless communicating technologies which are being used for implementation IoT application in specific locational (Indoor/Outdoor) conditions (temperature, humidity etc.). The performance of the wireless communication differs from location to location and due to the conditions existing in those locations [18]. The performance is also dependent on the root connecting the devices to the gateway especially. The performance of the wireless communication can be judged based on the loss of packets that may happen when communication takes place. The loss of packets is very much dependent on the distance between the devices and the gateway, the transmission power, payload, antenna angle, time of the day and weather conditions. The pattern that can be noticed in the loss of packets can also be observed. The number of packet losses is very much dependent on

the type of wireless technologies used to establish connection between the devices and the gateway.

3GPP introduced a new access technology called narrowband IoT (NB-IoT) for supporting machine to machine communication services over wide area [19]. A model is required for estimating probability of success and average access delay of RA (Random access) so that suitability of narrowband for effecting communication among devices and in between the devices and gateway.

The issue of managing the devices that are connected on to an IoT to ensure functional and operational performance has gained paramount importance these days, especially so when the number of devices connect to IoT have been growing tremendously. The devices must be managed such that the full functional performance of the devices is ensured.

Software defined networking (SDN) has been introduced to overcome some of the problems encountered when traditional networking has been used [20]. Through SDN, the logical and control layer are separated making it possible to implement the administrative functions in the control layer. The performance of SDN over use of traditional network for building IoT has been assessed. The comparison of architectures of both has also been made and proved that SDN yields better performance over traditional networking when some specific environmental conditions exist.

In an IOT network typically more number of small devices are sued which are energized by limited number of energy sources. One of the main challenges of IOT networks is to extend the longevity of small devices. Clustering techniques are generally adapted to address the issue of energy management among small devices. Quality of service, performance of the IOT networks yet another challenge that must be addressed when clustering is adapted for the purpose of energy management [21]. The issue of clustering must be analyzed from the perspectives of energy efficiency, reliable communication, and latency awareness and performance optimization. Several protocols are used for effecting communication among devices when the low end devices are clustered.

Implementing IOT within 3G/4G/5G networks is a challenge. Smart network selection is one of the most important issues that must be addressed for improvement of the performance of any of the IOT network.

Performance optimization could be simple when the IOT network containing several sub-nets is homogeneous and static in behavior. Performance optimization is quite complex when the IOT network is made of huge number of small devices which are heterogeneous in nature.

Collection of very important data for taking smart and critical decisions is being achieved through connecting and communication through many types of physical objects. Smart decisions make human life simple, safe and efficient.

Wireless sensor networks (WSN) are important source for information gathering which are connected routable gateways> the connectivity of this sort forms into a IOT network. Various types of devices are connected to form a WSN and devices can either sense scalar or multimedia data and the collected data has to be transmitted to reach the sink where the data is stored. The devices are quite limited in memory, processing power, bandwidth for communication. There is no local secondary storage on such devices.

The most important challenge is to move the collected data through different layers of a network reaching to the sink where the data is stored, analyzed and decisions are taken based on the analysis results. One of the main challenges is to move the data from source to sink in real time that high level of reliability. The challenge to achieve transmission of data from source to sink is the controlling of network paths such that the data form source to sink through IoT gateway reaches in real-time with most accuracy. The reliability of such paths is also one of the most important issues that one must ensure. The criticality of the data and data traffic varies from application to application and therefore needs to be managed accordingly. This leads to a requirement of managing the networking resources most optimally. The performance issue in this case is the time taken to transfer the data from sources to sink and the accuracy with which the data is transmitted. The performance off course is dependent on the ability to segregate data according to the criticality of the application and transmits data according the varied speeds. Appropriate and suitable resource management is the key for optimal performance of IoT networks. A resource reservation mechanism [22] has been proposed for achieving optimal resource utilization. The mechanism helps allocating sufficient resources for prominent and critical data which leads to reducing the delay time and thereby leading to increase in the performance of the system

IoT network is a heterogeneous, mixed, and uncertain ubiquitous network. Several applications can be made to run on the same network or the network can be altered suiting to a particular application. The applications are expected to provide intelligence service to the end users. Currently used IoT networks lack intelligence and a result the performance of the applications running on IoT is not satisfactory. Building intelligence into IoT will enhance the performance of the IoT networks.

Cognitive IoT addresses the issue of building intelligence into IoT networks and thereby increasing the performance in the delivery of data from source to sink. It is possible to collect current network conditions, carry the analysis of perceived knowledge, perform adaptive actions, and make intelligent decisions when intelligence is added to IoT. The performance of the IoT networks can be enhanced when intelligence is added to IoT based networks. The topology of IoT networks is modelled considering the inclusion of cognition process related technologies and the trades have been analyzed through a game theory adapted for the purpose [23].

3. Investigations and findings

IoT systems are huge and complicated as the networking is done in many layers. The number of devices connected on to IoT network is ever increasing. Iot networks are fragile due to the existence many small devices. Reliability of IoT network as such is quite low. The devices connected on to IoT are heterogeneous in nature and there is a need for frequent protocol conversion. Small devices are low in power and latency of those devices is high affecting the performance of the IoT network. IOT network generally designed to achieve the real time requirements of certain application. The environmental conditions vary from application to application leading to choice of most suitable communication technologies.

Most of the time sensitive information is collected and sent across a network to be stored in a remote severs. The form factor of the devices is so small that securing the same is quite difficult as implementation of cryptographic algorithms requires huge computing resources. The performance of the devices generally suffers when security related algorithms are in-built into these devices.

Many technologies are coming up especially the wireless technologies the performance of which greatly varies given the environment conditions, distance to which the communication must be effected, the area where the communication must be effected etc. Choice of proper communication technology has influence on the performance of communication system.

The performance of the devices in IOT network is most crucial. The devices must learn the environmental conditions and behave accordingly to be able to perform efficiently and optimally. One has to implement intelligence into devices so that the devices will perform to the optimum. Cognitive IoT addresses the issue of building intelligence into IoT networks and thereby increasing the performance in the delivery of data from source to sink.

The networking of IoT is achieved through use of several networking resources. The speed of communication is dependent on the path chosen between the source and sink. There could be many paths existing between a source and sink. One has to choose the best possible path considering environmental condition, area where the IoT network is situates, technology used for communication etc. The communication over a network is dynamic. For effecting the desired communication over a specific path, resource reservation methods are required

IoT systems are huge and complicated as the networking is done in many layers. The number of devices connected on to IoT network is ever increasing. Iot networks are fragile due to the existence many small devices. Reliability of IoT network as such is quite low. The devices connected on to IoT are heterogeneous in nature and there is a need for frequent protocol conversion. Small devices are low in power and latency of those devices is high affecting the performance of the IoT network. IOT network generally designed to achieve the real time requirements of certain application. The environmental conditions vary from application to application leading to choice of most suitable communication technologies.

Most of the time sensitive information is collected and sent across a network to be stored in a remote severs. The form factor of the devices is so small that securing the same is quite difficult as implementation of cryptographic algorithms requires huge computing resources. The performance of the devices generally suffers when security related algorithms are in-built into these devices. Building security within every device in terms of access control, authorization etc. is complex and time consuming and also leads to wastage of resources. Different securing mechanisms especially the group based securing system when sued will help in ensuring the desired performance of the IoT devices. Security implementation must be dynamic and configurable and must be enforced only when required such the overburden due to implantation of security algorithms us reduced as much as possible. Flexible hardware specific implementation of security will not only help securing the devices but also leads to high performance IoT based systems.

Many technologies are coming up especially the wireless technologies the performance of which greatly varies given the environment conditions, distance to which the communication must be effected, the area where the communication must be effected etc. Choice of proper communication technology has influence on the performance of communication system.

The performance of the devices in IOT network is most crucial. The devices must learn the environmental conditions and behave accordingly to be able to perform efficiently and optimally. One has to implement intelligence into devices so that the devices will perform to the optimum. Cognitive IoT addresses the issue of building intelligence into IoT networks and thereby increasing the performance in the delivery of data from source to sink.

The networking of IoT is achieved through use of several networking resources. The speed of communication is dependent on the path chosen between the source and sink. There could be many paths existing between a source and sink. One has to choose the best possible path considering environmental condition, area where the IoT network is situates, technology used for communication etc. The communication over a network is dynamic. For effecting the desired communication over a specific path, resource reservation methods are required. Prioritizing of network resource is one of the most important issues that must be taken into account.

The devices are low energy devices. The energy gets depleted fast in such devices. The issue of clustering must be analyzed from the perspectives of energy efficiency, reliable communication, and latency awareness and performance optimization. Several protocols are to be used for effecting communication among devices when the low end devices are clustered. Self-clustering nodes will help in dynamically changing the clustering mechanisms such that clustering is under taken as per the prevailing conditions

IoT networks can be established either through traditional networking or software defined networking. SDN separates the logical layer and control layer. Through control layer devices can be manages such that better performance of those devices can be achieved.

Networking and communication technologies must ne selected such that high reliability of communication is achieved. Models are required such that probability of success and average access delay are assessed so that most appropriate technology suited to the application and environment conditions can be selected. Choice of appropriate is also important for improving the performance of communication systems. Modelling of performance of the IoT network is necessary so that one will be able to assess the performance characteristics of an IoT based network. Yet another area that can be considered for improving the performance of an IoT based network is Network coding. Network coding can be done either at device level or storage level. Network coding improves the performance of the IoT network quite tremendously.

Choice of most appropriate communication technology is the key for optimum perforce of IoT based networks. All possible communication technologies must be assessed especially in terms of loss of packets and time to communicate so that most suitable technology can be selected thereby improving the performance of the IoT based systems.

Many new IoT standards are coming up day to day which are suitable for implementing specific IoT networks. Choice of a standard is most important for implementing an IoT network which yields high performance.

The designing of a IoT network must be done considering the trade of between cost, power, performance, and volume of transactions handled.

Selection of a protocol for effecting most efficient communication is one of the most important key for the development of IoT networks. Several protocols must be assessed for its suitability considering the performance and the most suitable protocol must be selected. A comparative analysis of the protocols that can be sued for effecting communication within IoT must be assessed before selecting the most suitable protocol.

.Modelling of the behavior of the devices and IOT networks becomes especially when wireless communication is used becomes quite important in the absence of which it is quite difficult to assess the performance of the IOT networks. An IOT network as such can be represented as two node, three node and multi node network. A two node IOT can be implemented using a bidirectional wireless communication systems. It is necessary to model security and energy awareness of such a system even if little knowledge exists on the synergetic effect considering the awareness about security and energy consumed by such systems under the influence of many environmental conditions such as noise.

Performance improvement of IoT networks can be achieved by combining other types of systems such as high computing system with IoT based systems. High performance of IoT is required especially when images, videos and graphics are to be continuously streamed.

Thus all basic issues that affect the performance of the IOT based system have been traced. The basic issues include networking, communication technologies, protocols, clustering, security etc. The basic issues that affect the performance of IoT networks have been tabulated and shown in Table 1.

4. Conclusions

The scope of IoT networks is huge that include applications, standards, protocols, devices, technologies, security, reliability, response requirements, performance, latency, energy, environmental conditions, location of implementation and many

such consideration. Among all the things performance of IoT networks is crucial. It is important to trace out all issues that affect the performance of a specified IoT network. The performance bottlenecks as such must be identified and resolved. In this paper all basic issues that must be addressed keeping in view of the performance of IoT networks is presented which can be used for varying further research. Table 1 basic issue affecting the performance of IoT networks

Serial Number	Basic issue	Element Number of basic issue	Basic element description
1	Networking	1.	Selection of most appropriate network suitable for implementing an application and performance evaluation of the same
		2.	Implementing SDNs
		3.	Network Coding
		4.	Network Resource prioritizing and reservation
2	Protocols	1.	Performance analysis of protocols
3	Clustering	1.	Clustering devices
		2.	Self-organising cluster heads
		3.	Clustering techniques for different networks
4	Security	1.	Group based Authentication system
		2.	Implementing security using cryptographic devices
		3.	Performance analysis security algorithms
5	Communication technologies	1.	Choice of appropriate wireless technology
		2.	Performance analysis of new channels
6	Middleware requirements	1.	Collection of data from devices and dissemination of the same to sinks
7	Sandwiching IoT with other technologies	1.	Combining HPC with IoT for streaming Videos, audios and graphic
8	IoT standards	1.	Evaluating the suitability of standards keeping the performance of IoT based Applications
9	Devices	1.	Performance analysis of devices
		2.	Decision making capability of the devices
		3.	Impact of a node on the overall performance of a network
		4.	Building intelligence into device through in-built cognition
10	Modelling	5.	Modelling for performance analysis
		6.	Performance evaluation through feedback control
		7.	Security-energy performance relationships
		8.	Modelling performance of a network
11	Designing	1.	Secured Image communication
		2.	Designing considering Trade-off between cost, energy, latency, reliability

References

[1] K. Vandikas and V. Tsiatsis, "Performance Evaluation of an IoT Platform," *2014 Eighth International Conference on Next Generation Mobile Apps, Services and Technologies*, Oxford, 2014, pp. 141-146.doi: 10.1109/NGMAST.2014.66

[2] D. E. Baz, "IoT and the Need for High Performance Computing," *2014 International Conference on Identification, Information and Knowledge in the Internet of Things*, Beijing, Investigating the Performance of the Random Access Channel in NB-IoT 2014, pp. 1-6.doi: 10.1109/IIKI.2014.8

[3] M. Qutab-ud-din, A. Hazmi, B. Badihi, A. Larmo, J. Torsner and M. Valkama, "Performance analysis of IoT-enabling IEEE 802.11ah technology and its RAW mechanism with non-cross slot boundary holding schemes," *2015 IEEE 16th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, Boston, MA, 2015, pp. 1-6. doi: 10.1109/WoWMoM.2015.7158204

[4] N. Rathod *et al*., "Performance analysis of wireless devices for a campus-wide IoT network," *2015 13th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt)*, Mumbai, 2015, pp. 84-89. doi: 10.1109/WIOPT.2015.715105

[5] K. Sato, Y. Kawamoto, H. Nishiyama, N. Kato and Y. Shimizu, "A modelling technique utilizing feedback control theory for performance evaluation of IoT system in real-time," *2015 International Conference on Wireless Communications & Signal Processing (WCSP)*, Nanjing, 2015, pp. 1-5.doi: 10.1109/WCSP.2015.7341303

[6] E. Kougianos, S. P. Mohanty, G. Coelho, U. Albalawi and P. Sundaravadivel, "Design of a High-Performance System for Secure Image Communication in the Internet of Things," in *IEEE Access*, vol. 4, pp. 1222-1242, 2016.doi: 10.1109/ACCESS.2016.2542800

[7] Algimantas Venckauskas1, Vytautas Stuikys, Robertas Damasevicius and Nerijus Jusas," Modelling of Internet of Things units for estimating security-energy-performance relationships for quality of service and environment awareness", 2016 security and communication networks, in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.1537

[8] Y. Chen and T. Kunz, "Performance evaluation of IoT protocols under a constrained wireless access network," *2016 International Conference on Selected Topics in Mobile & Wireless Networking (MoWNeT)*, Cairo, 2016, pp. 1-7.doi: 10.1109/MoWNet.2016.7496622

[9] W. T. Su, W. M. Wong and W. C. Chen, "A survey of performance improvement by group-based authentication in IoT," *2016 International Conference on Applied System Innovation (ICASI)*, Okinawa, 2016, pp. 1-4.doi: 10.1109/ICASI.2016.7539800

[10] Deming Chen, Jason Cong, Swathi Gurumani, Wen-mei Hwu, Kyle Rupnow ✉, Zhiru Zhang, "Platform choices and design demands for IoT platforms: cost, power, and performance tradeoffs ",IET Cyber-Phys. Syst., Theory Appl., 2016, Vol. 1, Iss. 1, pp. 70–77

[11] Declan T. Delaney , and Gregory M. P. O'Hare," A Framework to Implement IoT Network Performance Modelling Techniques for Network Solution Selection", In Proceedings of the 7th International Conference on Internet and Distributed Computing Systems, IDCS 2014, Calabria, Italy, 22–24 September 2014; Volume 8729, pp. 312–324.

[12] J. Li, Y. Liu, Z. Zhang, J. Ren and N. Zhao, "Towards Green IoT Networking: Performance Optimization of Network Coding Based Communication and Reliable Storage," in *IEEE Access*, vol. 5, pp. 8780-8791, 2017.doi: 10.1109/ACCESS.2017.270632

[13] S. Sankaran, "Modeling the performance of IoT networks," *2016 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, Bangalore, 2016, pp. 1-6.doi: 10.1109/ANTS.2016.7947807

[14] W. Twayej, M. Khan and H. S. Al-Raweshidy, "Network Performance Evaluation of M2M With Self Organizing Cluster Head to Sink Mapping," in *IEEE Sensors Journal*, vol. 17, no. 15, pp. 4962-4974, Aug.1, 1 2017.doi: 10.1109/JSEN.2017.2711660

[15] B. Zhou, M. Egele and A. Joshi, "High-performance low-energy implementation of cryptographic algorithms on a programmable SoC for IoT devices," *2017 IEEE High Performance Extreme*

Computing Conference (HPEC), Waltham, MA, 2017, pp. 1-6. doi: 10.1109/HPEC.2017.8091062

[16] M. Pennacchioni, M. G. Di Benedette, T. Pecorella, C. Carlini and P. Obino, "NB-IoT system deployment for smart metering: Evaluation of coverage and capacity performances," *2017 AEIT International Annual Conference*, Cagliari, 2017, pp. 1-6. doi: 10.23919/AEIT.2017.8240561

[17] Nuzhat Khan, Nazmus Sakib, Ismot Jerin, Shaela Quader and Amitabha Chakrabarty," Performance Analysis of Security Algorithms for IoT devices", in 2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC)

[18] Shie-Yuan Wang, Yo-Ru Chen, Tzu-Yang Chen, Chia-Hung Chang, Yu-Hsiang Cheng, Chun-Chia Hsu, and Yi-Bing Lin," Performance of LoRa-based IoT Applications on Campus",

[19] Ruki Harwahyu, Ray-Guang Cheng, Chia-Hung Wei," Investigating the Performance of the Random Access Channel in NB-IoT",

[20] M. B. Yassein, Q. Abuein and S. A. Alasal, "Combining software-defined networking with Internet of Things: Survey on security and performance aspects," *2017 International Conference on Engineering & MIS (ICEMIS)*, Monastir, Tunisia, 2017, pp.7. doi: 10.1109/ICEMIS.2017.8273027.

[21] L. Xu, R. Collier and G. M. P. O'Hare, "A Survey of Clustering Techniques in WSNs and Consideration of the Challenges of Applying Such to 5G IoT Scenarios," in *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1229-1249, Oct. 2017.doi: 10.1109/JIOT.2017.2726014

[22] Shubha Rao V and M. Dakshayini, "Priority based optimal resource reservation mechanism in constrained Networks for IOT applications," *2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, Chennai, 2016, pp. 1228-1233.doi: 10.1109/WiSPNET.2016.7566332

[23] Mingchuan Zhang, Haixia Zhao, Ruijuan Zheng, Qingtao Wu and Wangyang Wei," Cognitive Internet of Things: Concepts and Application Example", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 6, No 3, November 2012 ISSN (Online): 1694-0814