Data Transmission and Capacity over Efficient IoT Energy Consumption

Khalid ALoufi[1] , Kaleem Malik[2] , Tariq Naeem[2] and Rizwan Mir[3]

[1]School of Computer Science and Engineering, Taibah University, Saudi Arabia;
[2]Department of Computer Science, Air University, Multan Campus, Multan, 60000 Pakistan;
[3]Department of Computer Science, Virtual University, Lahore, Pakistan;

Summary
The research on preserving energy resources to increase Internet of Things (IoT) device lifespan in the remote areas has high precedence. The energy consumption in an IoT network is mostly affected by the volume and processing requirements for the data transformation. Theretofore, the constrained network and constrained devices have different design and performance to be considered in energy performance of an IoT system. In this research, the power consumption with regards to the capacity of the memory and the data transmission is analyzed. It is assumed that the location and specifications of the constrained IoT device have an effect over the network and devices performance. One of the performance metrics is the energy consumption with regards to the data size, storage, processing and transmission with respect to the device location, processing power and storage capacity. This research intends to present a model of power requirement for the specific specifications of IoT devices in different network topologies.

Key words:
Internet of Things (IoT), energy consumption, IEEE 802.15.4, Constrained Application Protocol (CoAP), data transfer, data size.

1. Introduction

Mobile networks have been well thought-out as a helpful choice to give availability to Internet of Things (IoT). Especially, mobile network allows universal exposure, portability and encourage working with nearby Wi-Fi nets [1]. The energy is affected by the memory space used and the processing power required for data transmission and storage. The utilization of low power remote sensors with back up networks in production has expanded over the previous decade. The device inherent constraints of memory work have an unfriendly impact on power utilization inculcating a shorter battery life [2]. Consequently, a new mechanism to accomplish versatility, energy efficiency and reliability are required with standard explanations for network correspondences.

In the research [3], the authors portrayed and justified the need for a powered access control technique for CoAP systems. They introduced an exploration study. A study of additional security components that can be valuable in arrangement with CoAP in guarded embedded frameworks. It also recognizes the deficiencies of these techniques and approaches to motivate and make another entry point for CoAP frameworks. The plan of power proficient CoAP for small gadgets to lessen overhead and the execution of a constrained network to show its performance is the key work of the authors.

The issue of systems utilizing different protocols was discussed by [4]. The authors proposed an answer dependent on protocol interpretation and an investigation of how to deal with explicit protocol error messages while trying to build interoperability in systems of this sort. The primary research commitment of [4] was the investigation of the security features associated with translation concerning protocols.

A reasonable CoAP application protocol for 6LoWPAN systems is exhibited in table 1, whereas table 2 shows a general IoT stack model. The security instruments must be institutionalized to conserve interoperability, if not standardized interoperability will be compromised.

Table 1: Header overhead on different layers for 6LoWPAN networks.

Network Layer	Header overhead	Achieved attributes in IoT
Physical	None	Availability
Link	6-26 bytes	Authentication and integrity
Adaptation	8 bytes	Integrity
Network	16 bytes	Authentication, integrity, resiliency, robustness and resistance
Application	16 bytes	Authorization, authentication, integrity, confidentiality, resiliency, robustness and resistance

The motivation of [5] is to give bootstrapping services and organization to improve trustworthiness and zero-design abilities. In this paper, a few cases for services are exhibited, comprising manufacturing business and IoT gadgets. The exploration, advancement and testing of low-power benefits utilized by a resource controlled IoT gadget to execute the design for sensors is the fundamental contribution of the authors.

Manuscript received December 5, 2019
Manuscript revised December 20, 2019

The utilization of IoT with various case studies has extended the importance in the course of recent years. The work of [6] presented an Industrial IoT juncture for assessing the ability to adjust to the power utilization of every device connected showing improvement in estimating the lifetime of the individual node. The paper likewise examines the effect of each applied systems to investigate the power utilization and postponements; these IoT networks incorporate correspondence, for instance, get control of the device and managing the node.

Table 2: Internet Of Things Stack

Layer	OSI Layers	TCP/IP	IoT	
7	Application	Application	MQTT	CoAP
6	Presentation			
5	Session			
4	Transport	Transport	TCP	UDP
3	Network	Internet	IP	IPv6
				6LoWPAN Adaptation Layer
2	Data Link	Network Access	IEEE 802.15.4 MAC	
1	Physical		IEEE 802.15.4 PYS	

The road map of paper is section 2 depicts the related literature of the work done so far in the field. Section 3 introduces a model with a technique for fulfilling the needs of low energy consumption in IoT. The proposed framework is analysed in section 4. After the result and discussion section research is being concluded. In conclusion, settles the paper with future direction.

2. Related Work

Better energy consumption also promises to provide longer response time, high level of communication and better reliability of data while the process of transformation without losing any fruitful information over the Internet of Things (IoT) based network. Whereas, power management can also be dealt with many other methods like producing energy through the mediums like air, wind or solar-based units built-in the remote nodes. But still these matters will also require IoT devices to get bigger in size which in most of the cases is not desirable [7]. And it will go against to have a remote coverage when gaining data from the areas where such devices require higher deployment. Specifically, situations covering the remote regions during the analytical observatory programs like military tactical planning, or natural disaster prediction [8].

Societies have turn out to be increasingly interlinked, since the Internet has developed and matured, as the applications used to upgrade day-to-day lives. This has promoted the development of IoT. IoT is thought of as an achievement of the progressing digital technology. According to its definition [9] and [10], information from the surrounding, assembled by billions of sensors and devices associated, in some typological structure, to the Internet, will be promptly accessible to number of applications. Similarly, presenting the data about the physical world to web applications, web services are the basic structure of the present web, which can be raised to an innovative level.

Resource-constrained devices that converse through lossy, low bit rate remote systems, are the basis of IoT [9]. Because of memory, power and computational constraints in these miniaturized resources, new and innovative protocols have been built up that can work in resource constrained devices [10]. Resource constrained devices in wireless network converse with one another through low bit rate in IoT setting. For instance, 802.11n and 802.11ah protocols present an arrangement of energy-saving methods to fine-tune WiFi technology to low4 power IoT resource-constraint devices. Another model is IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN) that permits IPv6 packets to be transmitted over IEEE 802.15.4 based systems [11, 12] and [13].

IEEE 802.15.4 is a notable network system standard in IoT. It has been created by the Personal Area Network (PAN) of IEEE [14]. It is intended to alleviate the issue of the constrained transmission power of IoT devices. It focuses on the physical and MAC layers of the ISO layered stack. The IEEE 802.15.4 is famous to propose a maximum of 250 Kbit/s as a data rate with an output power that does not surpass 1mW. Data packets' size is of 127 bytes making it a reasonable technology innovation for less interactive IoT frameworks over constrained devices.

A factual outline of systems utilized in IoT condition from different telecommunication companies is depicted in Table 3. GSM began with voice calls; however, it presently has a platform equipped for backing up portable broadband and interactive media facilities. The LTE-M (Long Term Evolution for Machines) and NB-IoT (Narrowband Internet of Things) systems depend on results institutionalized by 3GPP. LTE-M can be utilized to cost-effective interface sensors observing the performance for example resource trailing and buyer wearable gadgets with a Low Power Wide Area (LPWA) innovative technology giving low-level gadget complication and expanded coverage. Similarly, NB-IoT limits the power utilization of associated devices. Sigfox permits a forty (40) km range. A basic REST API can retrieve it. LoRa, ZigBee and Z-Wave are likewise parts of IoT systems. A specific web transfer protocol, Constrained Application Protocol (CoAP) by IETF RFC 7252, is utilized with devices in controlled networks in IoT. A four-byte fixed header and a reduced encoding of selections empower small texts that effect no or little

fragmentation. It can convey various sorts of payloads and can distinguish which payload type is being utilized.

Table 3: IoT networks with respective attributes.

	Bandwidth	Battery Lifetime	Data Rate	Protocol
GSM [15]	880-960 MHz	talk-time/2	890-915 MHz	LAPD
LTE-M [16]	108 MHz	10 years	1 Mbit/s	VoLTE
NB-IoT [17]	180kHz	>10 years	100 kbits/s	NB-IoT
Sigfox [18]	10Hz	10 years	868-902 MHz	HTTP
LoRa [19]	125-500 kHz	10 years	510-928 MHz	LoRaWAN
ZigBee [20]	2.4GHz	2 years	868-915 MHz	IEEE 802.15.4
ITU-T G.9959 [21]	865-926 MHz	>10 years	9.6-100 kbit/s	Z-Wave
IETF RFC 7252 [22]	10 kbit/s	2.95-3.47 years	1 byte/s	CoAP

3. Data, Energy and IoT

To have a system with a better level of data access over the network nodes, it is not safer to have data fragmented into smaller pieces. Energy consumption and data cost increases over the IoT devices while transferring or receiving data segments while making fragmentation less effective for data transformation throughout the IoT devices. Fragmentation with the cost of header repetition brings higher consumption of energy while providing low performance in using IEEE 802.15.4 standard based networks [14].

3.1. Saving Energy with Standardized Data Sizes

Avoiding fragmentation becomes the key area of this research by bringing a mechanism to overcome the energy crisis while deploying IoT devices over the remote areas.
By utilizing only, the smaller size payloads for the data which will fit in the message. Whereas, reducing the chances of fragmenting data while transferring over the network in remote areas decreases the probability of early energy consumption while information is coming through linking heterogeneous IoT devices. And this mechanism also enhances chances of getting higher throughput from the devices while introducing multiple networks one for low-level data-size as payloads over the network while another one will be responsible for high volume data communication.

3.2. Data Storage and Application Limits

The proposed model provides a mechanism which suggests division of a data entity over the RAM prior to transferring forward. So, an IoT device may contain a partial part of data distribution to enhance the capability of batteries or energy sources in having higher life span while deployed in any remote area. Such constraints can get apply or programmed while message sending at the level of application protocol of the Network.
The data size reduction increases the domain area of IoT as being reduced into smaller segments to have interoperability among different heterogeneous devices. So constrained application protocol header for message packaging is further divided into smaller headers incorporated such that to capture network bigger picture, starting from UDP header into IP header and then into frame header shown in figure 1.

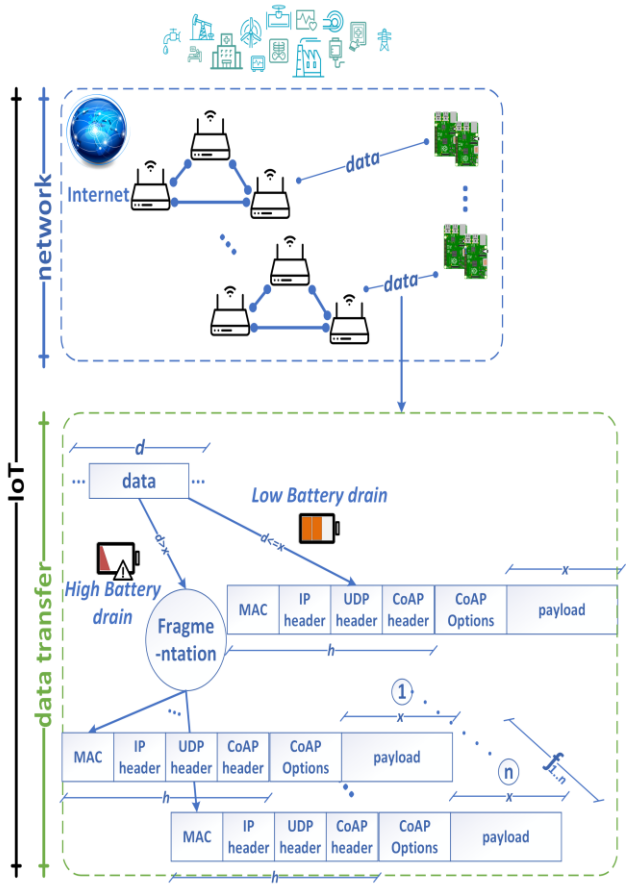

Fig. 1 Model depicting effect of fragmentation over the IoT network energy consumption

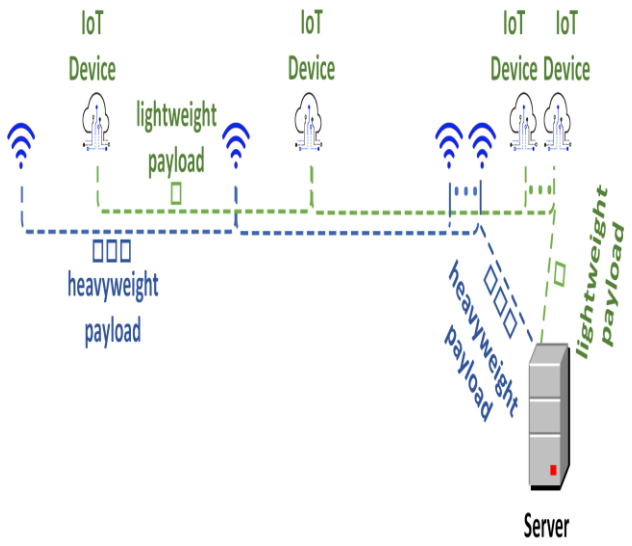

Fig. 2 Model for IoT Multi-Layered Network Mechanism

3.3. IoT Multi-Layered Network Mechanism

To understand the proposed mechanism of IoT multi-layered network, as shown in figure 2, two networks are being deployed in the same area to cover data transformation effectively. Among these two networks, one is for IoT devices communication and another network layer is to support heavy data transformation between nodes if needed.

A threshold will be introduced to check whether data to be transmitted fits in mare payload of IoT message or not. If data increases from threshold then in is send using secondary network layer created in effort to decrease pressure from primary IoT network layer. The methodology implemented placed fragmented text on another parallel system in IoT condition. Since extensive lengthy messages require some serious energy in fragmentation, the IoT devices are exempted from such messages. The IoT devices, instead, get data commands whereas the fragmented text is placed on another parallel network in IoT. Similarly, the server easily processes extensive lengthy fragmented messages because it is connected to a power source.

4. Mathematical Modeling and Analysis

This section of the research represents through mathematical modeling and analysis the impact of the data size variations while observing constrained device memory management.

4.1. Constrained Device Memory Management

IoT ecosystem is implemented using different application protocols, such as Constrained Application Protocol (CoAP) [22]. The data size d sent one time if it can fit in one CoAP data payload. Otherwise, the data must be fragmented to x fragments. Then the header part, h bytes, is repeated x times. The number of fragments x is d/s, where s is the CoAP data payload. h is 127−43 if 43 bytes is assumed as the CoAP data size, d. The repeated header, h, is considered as an overhead, represented by the linear function ($h * x$).

The size of the message, d, of the IoT model is not designed for fragmentation. If the message size is not limited, such as the case of some communication protocols, the message sent once. The header percentage reach a negligible percentage of the total message size if the message sent only once. However, after fragmenting the message to the header is repeated several times. The percentage of the overhead as a result of the repeated header of a messages of size 500 bytes is shown in figure 3 using equation 1. The more fragment generated, the more the overhead of the header is.

$$h\% = (43 * x) / (500+43 * x) \quad (1)$$

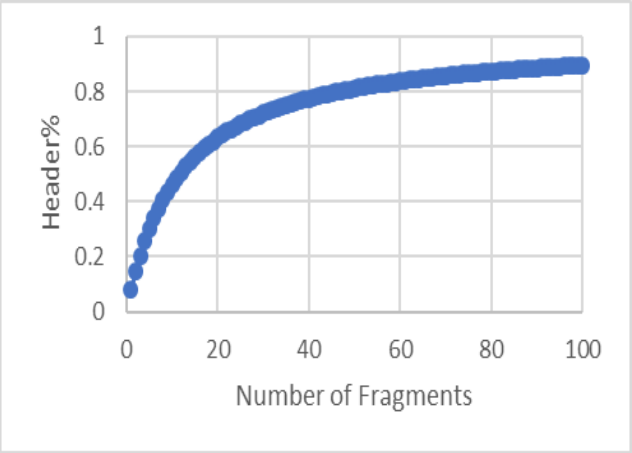

Fig. 3 Header percentage to the number of fragments of a message of 500 [bytes].

On the other hand, figure 4 and 5 shows the relationship between the data or header, respectively, to the number of fragments. As the number of fragments increases, the data or header share is decreasing. Keeping the message balanced between the header and the data, will keep the transmission reasonable according to the network topology or to the application requirement.

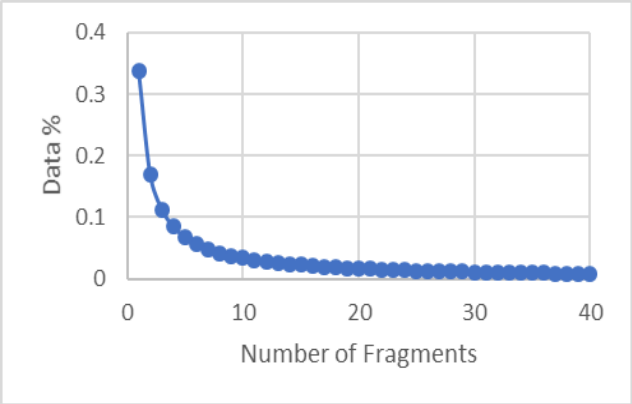

Fig. 4 The relationship between the percentage of data to the number of fragments

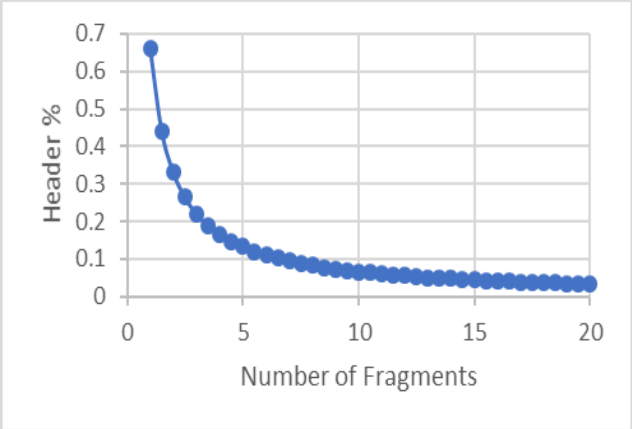

Fig. 5 The relationship between the percentage of the header to the number of fragments needed as the data size increase

As the number of fragments increases the percentage of the header is decreasing according to equation 2, where *f* is the number of fragments, *h* is the header payload, as shown in figure 5.

$$f = h/(127 * x) \quad (2)$$

As the single data size of an application increases, the number of fragments increases linearly as shown in figure 6. Figure 6 shows the difference between different data payload, which are 24, 43 and 63 bytes. Figure 6 shows that fragmentation is not appropriate for the constrained environment because messages has a maximum size of 127 bytes. Figure 7 shows the data payload with respect to data percentage of the total message size. The data percentage of the message size ranges from about .2 to .5, which also shows that the data is limited in each message. If an IoT device or a resource would like to share big size, then a different channel of transmission should be used as mentioned earlier in section 3.

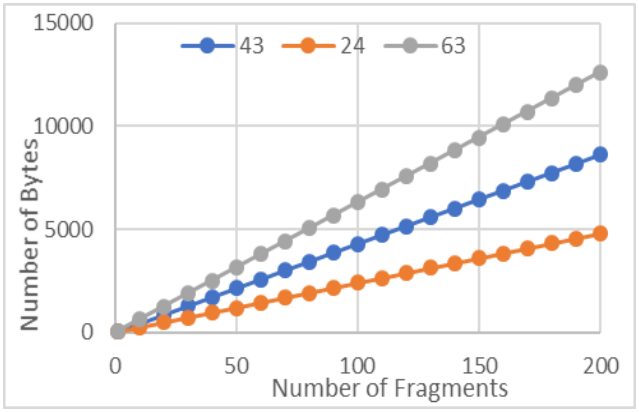

Fig. 6 The Number of Fragments vs the size of the application data

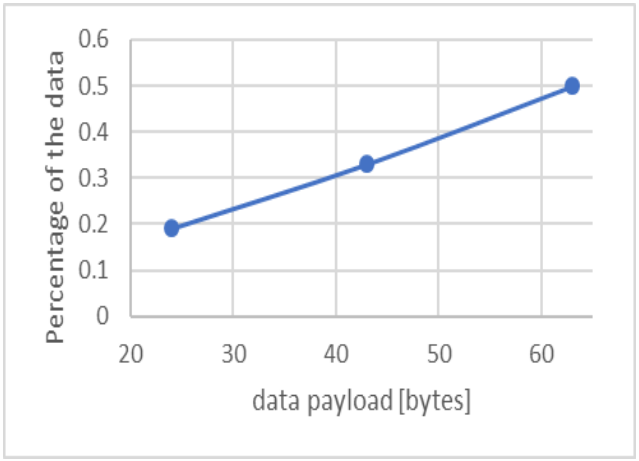

Fig. 7 The relation between the data payload and data Percentage of the message

The RAM or flash memory size should be enough to use for operating systems (OS) and application data. The RAM size calculation of such a system requires to consider the OS and the application data as shown in equation 3.

$$M_{RAM} = OS_{RAM} + APP_{RAM} \quad (3)$$

$$APP_{RAM} = 127 * (n1 + n2) \quad (4)$$

$$M_{ROM} = OS_{ROM} + APP_{ROM} \quad (5)$$

Constrained Devices (CD) has a RAM of APPRAM bytes reserved for OS and code. The data sources are assumed to send data in CoAP messages, 127 Bytes each. The

CoAP total data size is measured by equation 4, where n1 is the number of CoAP messages of connections and n2 is the number of cached CoAP messages. So, the RAM required is the number of bytes required by the OS and the data as shown in equation 5, which defines the APPRAM in equation 3.

Memory or the flash memory, ROM, is the part of constrained device to host the OS or the boot loader and application protocols or codes for the sensors, as shown in equation 5.

The different application will require different CD specifications. For example, Contiki OS for constrained devices requires about 10KB of RAM and about 30 KB of ROM, which is about class 1 device. Using CoAP implementation with the RIOT OS requires about 200KB of ROM and 100KB of RAM, which is about class 2 device. Each of IoT OS can be customized to smaller memory, hence applied to a smaller class [13].

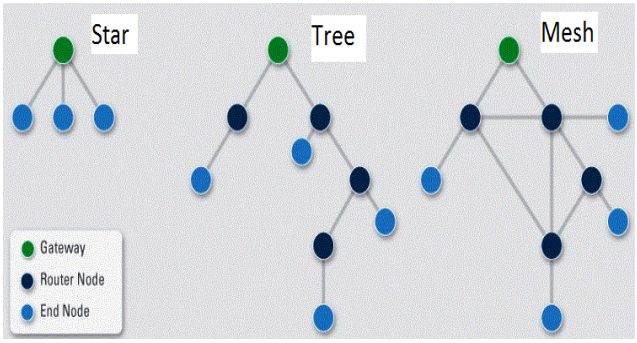

Fig. 8 different WSN Topology

WSN topology is mostly either star, tree or mesh as shown in figure 8. In any networks topologies, the CD is also sending other sources data. Consequently, the cost of a project may be affected by the network topology. In a mesh network, all CD should have the same requirements. In a tree network, the higher in the tree, the higher requirements. For star, the RAM required for x connections is shown in figure 9(A).

In figure 9(A), the required RAM for mesh WSN is shown in equation 7. Figure 9(B) shows the required RAM for Tree WSN as represented in equation 8, where g is the depth of the tree. Designing a WSN has different consideration, however, for the constrained model of IoT, the location of the CD and the network design affect directly the specification if the CD. CD requires specific RAM size depending on the application, location and topology in the WSN as shown in figure 9(A) and 9(B).

$$M_{ROM} = OS + 127 * x \quad (6)$$

$$M_{ROM} = OS + 127 * (x - 1) \quad (7)$$

$$M_{ROM} = OS + 127 * (2^{g+1} - 1) \quad (8)$$

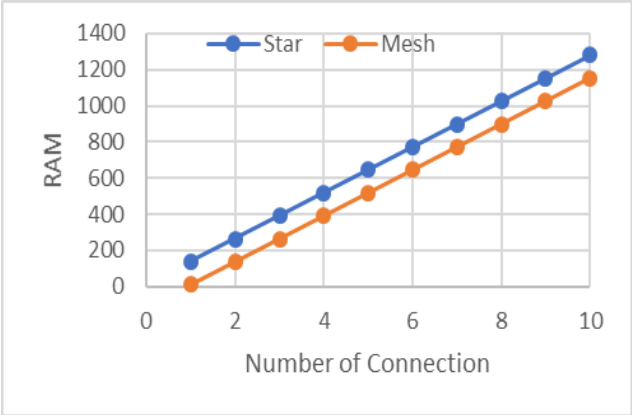

Fig. 9(A) RAM vs number of connections for Star and Mesh WSN Topology

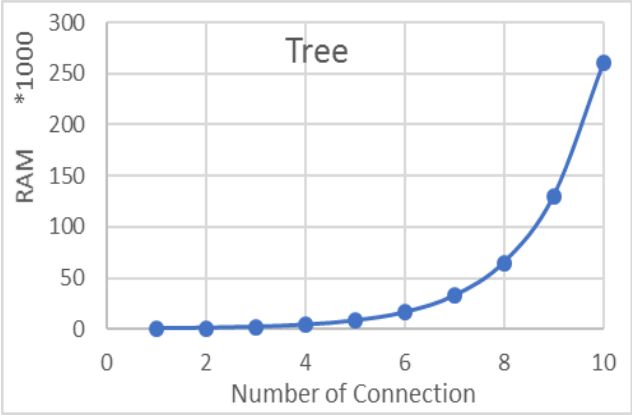

Fig. 9(B) RAM vs number of connections for Tree WSN Topology

4.2. Hybrid Data and Energy Model

Energy is the total amount of power used over time. IoT devices are expected to have limited energy, therefore, it is required to use it efficiently. Each time a transmission occurred a power is spent, and energy is degraded. Power is mainly consumed by CPU, Low Power Mode (LPM), *Tx* and *Rx* as shown in equation 9.

$$P_{DEV} = P_{CPU} + P_{LPM} + P_{Tx} + P_{Rx}. \quad (9)$$

$$P_{DEV} = x * Pt \quad (10)$$

$$P_{SYS} = n * x * Pt = n * P_{DEV} \quad (11)$$

On the other hand, each node will have some tasks to do (Pt), as shown in equation 10, such as processing over sensors data, transmitting a data, Tx or receiving a data from other nodes, Rx. Whereas, equation 11 shows the power required of the whole system, where n is the number of nodes in a specific part of the whole system. While this is important for running the system, however, it is not critical for reliability, since one or more failing nodes cannot break the system depending on the topology selected.

5. Results and Discussion

To show the results of the model, a simulation is developed using the Cooja simulator for Sky Mote Type #2. Figure 10 shows the network topology with a traffic between nodes. Figure 11 shows the power consumption of each node collected by node 1. As represented in figure 10, power consumption is distributed between CPU, LPM, Tx and Rx. Figure 12 shows part of the nodes messages.
Therefore, the lifetime of an IoT battery can be computed by knowing the expected number and types of tasks (x) and how much energy each task will require (Pt).

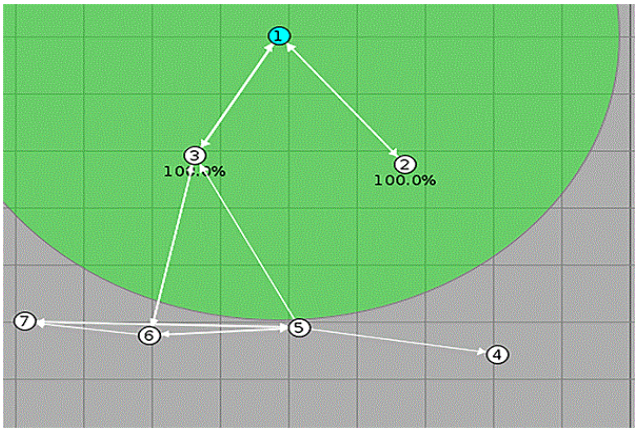

Fig. 10 IoT Network Topology

However, system administration can have lower threshold as a metric indication to manage the system. For example, if the power reaches a specific measure, an algorithm to load balance can be invoked or replacing some batteries.
In the case where the node is going to consume high energy or require different protocol, the node must use a high-speed parallel network over node with high specification IoT devices compared to the constrained IoT devices. For example, if the IoT device is a camera and going to send high volume of data, then the constrained network will be over consumed and have degraded performance since nodes in the way will use over estimated energy as mentioned earlier.
For one task from the simulation approximation, LPM consumes 2mW, CPU consumes 5mW, Tx consumes .5mW and Rx consumes 5mW.

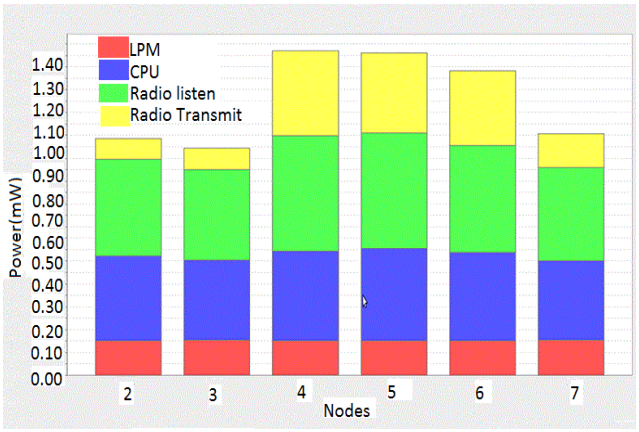

Fig. 11 Average Power Consumption

```
01:00.698 ID:6 Client sending request to:[IPv6]:61616/helloworld!
01:00.795 ID:4 Client sending request to:[IPv6]:61616/helloworld!
01:00.849 ID:7 Client sending request to:[IPv6]:61616/.well-known/core
01:01.162 ID:5 Client sending request to:[IPv6]:61616/light
01:01.236 ID:3 Client sending request to:[IPv6]:61616/light
01:01.406 ID:2 Incoming packet size: 4
01:01.442 ID:3 Incoming packet size: 18
01:01.445 ID:3 Response transaction id: 11 payload: 226;233
01:05.573 ID:2 Response transaction id: 11Client sending request to:[IPv6]:61616/helloworld!
01:05.588 ID:6 Client sending request to:[IPv6]:61616/.well-known/core
01:05.685 ID:4 Client sending request to:[IPv6]:61616/helloworld!
01:05.738 ID:7 Client sending request to:[IPv6]:61616/light
01:05.782 ID:2 Incoming packet size: 4
01:06.052 ID:5 Client sending request to:[IPv6]:61616/helloworld!
01:06.236 ID:3 Client sending request to:[IPv6]:61616/light
01:06.442 ID:3 Incoming packet size: 16
01:06.446 ID:3 Response transaction id: 12 payload: 72;65
01:10.574 ID:2 Response transaction id: 12Client sending request to:[IPv6] :61616/helloworld!
01:10.592 ID:6 Client sending request to:[IPv6]:61616/.well-known/core
01:10.688 ID:4 Client sending request to:[IPv6]:61616/light
01:10.742 ID:7 Client sending request to:[IPv6]:61616/light
01:11.030 ID:2 Incoming packet size: 4
01:11.055 ID:5 Client sending request to:[IPv6]:61616/light
01:11.237 ID:3 Client sending request to:[IPv6]:61616/light
01:11.568 ID:3 Incoming packet size: 18
01:11.572 ID:3 Response transaction id: 13 payload: 174;167
01:15.573 ID:2 Response transaction id: 13Client sending request to:[IPv6]:61616/light
01:15.587 ID:6 Client sending request to:[IPv6]:61616/light
01:15.685 ID:4 Client sending request to:[IPv6]:61616/light
01:15.739 ID:7 Client sending request to:[IPv6]:61616/helloworld!
01:16.052 ID:5 Client sending request to:[IPv6]:61616/helloworld!
```

```
01:16.237 ID:3  Client sending request to:[IPv6]:61616/.well-known/core
01:16.404   ID:2    Incoming packet size: 18
01:16.408   ID:2    Response transaction id: 14 payload: 240;233
01:16.445   ID:3    Incoming packet size: 75
01:16.453 ID:3 Response transaction id: 14 payload: </helloworld>;
n="HelloWorld",</led>;n="LedControl",</light>;n="Light"
01:20.574 ID:2  Client sending request to:[IPv6]:61616/.well-known/core
01:20.587   ID:6    Client sending request to:[IPv6]:61616/light
01:20.685   ID:4    Client sending request to:[IPv6]:61616/helloworld!
```

Fig. 12 Part of Nodes Messages; IPv6@= fe80:0000:0000:0000:0212:7401:0001:0101

Whenever the node is regular IoT node, then the node is classified as Class x, *Cx*, node as shown in Table 4, whereas only three IoT classes of devices are defined [23]. In this mode, the nodes of the first three classes in Table 4 will be considered as constrained IoT devices.

The fourth class of devices, class x, will be considered as a regular IoT device. Therefore, the IoT presented model will have two parallel networks, one is constrained and the other one is regular.

Table 4: Classes of IoT Devices

Name	data (RAM)	code (ROM)	IP Support	Cons-trained
Class 0, C0	10 KB	100 KB	No	Yes
Class 1, C1	~ 10 KB	~ 100 KB	Yes	Yes
Class 2, C2	~ 50 KB	~ 250 KB	Yes	Yes
Class x, Cx	»50 KB	»250 KB	Yes	No

Therefore, for IoT application, the hybrid network system is managed to have two parallel networks using the IoT stack model mentioned earlier. One node can either implemented using one of application protocols.

If an IoT node require specific task, then the node specification should in compact with its use either as an edge node or regular network node, however, with high specification. Figure 13 shows one situation where node 7 are collecting data from other nodes. It will consume much energy compare to other network nodes only by one command.

Consequently, the power consumption of node 7 has increased in a big difference from other nodes, which means this node will consume its energy much faster than other nodes. Figure 13 also shows that the most consumption of energy are done by the Radio listening, Rx. About 35mW are consumed by the Antenna, which almost 99% of the power consumed by this node. The power consumption of an IoT device will depends on the task requirements.

Benchmarks has shown that Raspberry Pi 4 B+ consumes much energy compared to constrained devices. For example, it consumes 350mA (1.9W) when Idle, and 980mA (5.1W) when 400% CPU load [24].

6. Conclusions

IoT is one of the emerging technologies with different design specifications. In the networking prospective, IoT can use the well-established solid best practices in network design and management. However, there is a great number of option when it comes to selecting the specification of IoT devices and the associated IoT stack models and data structuring using the semantic web standards. Semantic web of things (SWoT) is also emerging to help structuring the data of IoT devices for standardizing application development.

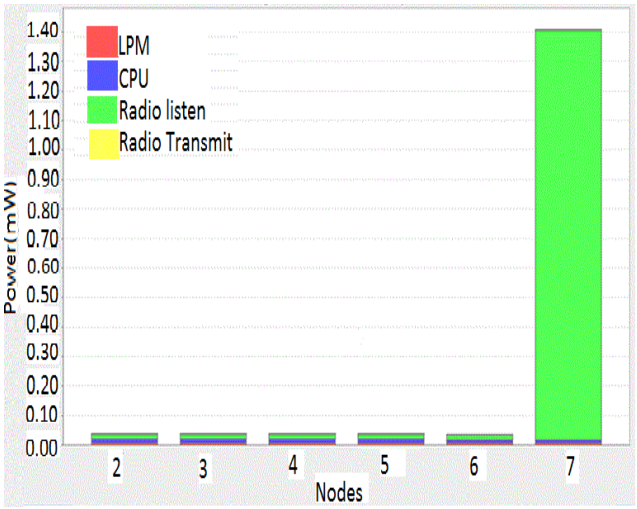

Fig. 13 Collect View Command on node 7

The tradeoff between data transmission and energy consumption is a dependent on the application. The IoT application is a designing technique that depends on the device task. Application of collecting environments data requires CD with efficient energy consumption from either class 0, class 1 or class 2. For some applications, when the device can have a permanent power supply or the power battery can be easily replaced or charged, the devices of class x.

This research has shown that selecting the IoT device will depends on its task and location over the network and of the application used. Therefore, the study has suggested developing a parallel network of IoT devices depending on the specification of the IoT device and the application used. Different Application protocols are available for implementing in the IoT devices as well as different operating Systems (OS).

However, each will have its requirement. There is a big challenge for network engineers in selecting the best devices and application developer after that to build a system that coop with the hardware.

IoT application developers are either dynamic or stack with one type of IoT device. However, not every IoT device are appropriate for every application. Therefore, every device has its functionality and appropriate OS and application.

References

[1] P. Andres-Maldonado, P. Ameigeiras, J. Prados- Garzon, J. Navarro-Ortiz, J. M. Lopez-Soler, Narrowband IoT data transmission procedures for massive machine-type communications, IEEE Network 31 (6) (2017) 8–15.

[2] P. Pu˜nal Pereira, Efficient iot framework for industrial applications, Ph.D. thesis (2016).

[3] P. P. Pereira, J. Eliasson, J. Delsing, An authentication and access control framework for coap-based internet of things, in: IECON 2014-40th Annual Conference of the IEEE Industrial Electronics Society, IEEE, 2014, pp. 5293–5299.

[4] H. Derhamy, J. Eliasson, J. Delsing, P. P. Pereira, P. Varga, Translation error handling for multi-protocol soa systems, in: 2015 IEEE 20th Conference on Emerging Technologies & Factory Automation (ETFA), IEEE, 2015, pp. 1–8.

[5] J. Delsing, P. Varga, L. Ferreira, M. Albano, P. P. Pereira, J. Eliasson, O. Carlsson, H. Derhamy, The arrowhead framework architecture, in: IoT Automation, CRC Press, 2017, pp. 79–124.

[6] P. P. Pereira, Efficient iot framework for industrial applications, Ph.D. thesis (2016).

[7] K. Wang, Y. Wang, Y. Sun, S. Guo, J. Wu, Green industrial internet of things architecture: An energy-efficient perspective, IEEE Communications Magazine 54 (12) (2016) 48–54.

[8] Jabbar, Sohail & Ahmad, Mudassar & Malik, Kaleem & Khalid, Shehzad & Chaudhry, Junaid & Aldabbas, Omar. (2018). Designing an Energy-Aware Mechanism for Lifetime Improvement of Wireless Sensor Networks: a Comprehensive Study. Mobile Networks and Applications. 10.1007/s11036-018-1021-3.

[9] P. Krawiec, M. Sosnowski, J. M. Batalla, C. X. Mavromoustakis, G. Mastorakis, Dasco: dynamic adaptive streaming over coap, Multimedia Tools and Applications 77 (4) (2018) 4641–4660.

[10] W. U. Rahman, Y.-S. Choi, K. Chung, Performance evaluation of video streaming application over coap in iot, IEEE Access 7 (2019) 39852–39861.

[11] Thubert, P., Hui, J.: Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks.RFC 6282 (2011). DOI 10.17487/RFC6282.URL https://rfc-editor.org/rfc/rfc6282.tx

[12] N. Kushalnagar, G. Montenegro, C. Schumacher, et al., Ipv6 over lowpower wireless personal area networks (6lowpans): overview, assumptions, problem statement, and goals.

[13] Aloufi, Khalid. 6LoWPAN Stack Model Configuration for IoT Streaming Data Transmission over CoAP. International Journal of Communication Networks and Information Security. 11. 304-3012, (2019)..

[14] A. F. Molisch, K. Balakrishnan, C.-C. Chong, S. Emami, A. Fort, J. Karedal, J. Kunisch, H. Schantz, U. Schuster, K. Siwiak, Ieee 802.15. 4a channel model-final report, IEEE P802 15 (04) (2004) 0662.

[15] M. Rahnema, Overview of the gsm system and protocol architecture, IEEE Communications magazine 31 (4) (1993) 92–100.

[16] R. Ratasuk, D. Bhatoolaul, N. Mangalvedhe, A. Ghosh, Performance analysis of voice over lte using low-complexity emtc devices, in: 2017 IEEE 85th Vehicular Technology Conference (VTC Spring), IEEE, 2017, pp. 1–5.

[17] R. Ratasuk, B. Vejlgaard, N. Mangalvedhe, A. Ghosh, Nb-iot system for m2m communication, in: 2016 IEEE wireless communications and networking conference, IEEE, 2016, pp. 1–5.

[18] S. Sigfox, Sigfox technical overview (2017).

[19] L. Alliance, A technical overview of lora and lorawan, White Paper, November. 20

[20] D.-M. Han, J.-H. Lim, Smart home energy management system using ieee 802.15. 4 and zigbee, IEEE Transactions on Consumer Electronics 56 (3) (2010) 1403–1410.

[21] B. Fouladi, S. Ghanoun, Security evaluation of the z-wave wireless protocol, Black hat USA 24 (2013) 1–2.

[22] Z. Shelby, K. Hartke, C. Bormann, The constrained application protocol (coap).

[23] C. Bormann, M. Ersue, A. Ker¨anen, Terminology for Constrained-Node Networks, RFC 7228 (4 2014). doi:10.17487/RFC7228. URL https://rfc-editor.org/rfc/rfc7228.txt

[24] J. Geerling, raspberry-pi-dramble, https://github.com/geerlingguy/ raspberry-pi-dramble (2015). 21

Khalid Aloufi is an associate professor in the Department of Computer Engineering, Taibah University, Madinah, Saudi Arabia. He received his Ph.D. and M.Sc. degrees in informatics from Bradford University, UK, in 2002 and in 2006 respectively. His B.Sc. degree in computer engineering was received in 1999 from King Fahd University of Petroleum and Minerals (KFUPM), Saudi Arabia. From 2002 to 2006, he was part of the networks and performance engineering research group at Bradford University. Aloufi has been the dean of the College of Computer Science and Engineering at Taibah University, Saudi Arabia.

Kaleem Razzaq Malik was born in Multan, Punuab, Pakistan in 1984. He received the M.S. degrees in computer science from the National University of Computer and Emerging Sciences, Lahore, PAK in 2008 and the Ph.D. degree in computer science from University of Engineering and Technology, Lahore, PAK, in 2018.

He is now working as Associate Professor in Air University, Multan Campus, Multan, Pakistan from March 2018 - date performing duties like Teaching and Research. He has worked as Assistant Professor in COMSATS Institute of Information

Technology, Sahiwal, Pakistan from December 2015 – March 2018 and as Lecturer in Department of Software Engineering, Government College University Faisalabad, Pakistan from June 2013 – November 2015 (2 year 5 months) performing duties like Teaching. He has also worked as instructor of computer science in Virtual University of Pakistan. University level more than 10 years of teaching experience.

He has published various articles in eminent National and International Journals with more than 100 citations and a book chapter titled "`Technique for Transformation of Data from RDB to XML Then to RDF"'. He has performed the role of reviewer for many top ranking international well reputed SCIE Indexed Journals of Springer, IEEE and Elsevier. He has been member of technical program committee of International Conferences His interests include Bigdata, Cloud Computing, Data Sciences, and Semantic Web.

Tariq Naeem received his B.S. (2006-2009) and M.S. (2010-2011) degrees from Department of Computer Science, University of Peshawar, Pakistan. During 2012-2013, he stayed in Bakhtar University, Kabul Afghanistan as a lecturer in Department of Computer Science. In addition, from 2013 to 2015, he worked as an IT trainer in USAID Power Distribution Program to train the employees of PESCO, NEPRA and MEPCO on various modules of SAP-ERP. He is now a lecturer in the Department of Computer Science at Air University Multan Campus, where he has been since 2016.

Rizwan Riaz Mir received the B.S. and M.S. degrees in Computer Science from Allama Iqbal Open University (A.I.O.U.), Pakistan in 2005 and Institute of Management and Sciences (IMS), Pakistan in 2013, respectively. During 2007-Present, he stayed in Virtual University of Pakistan (VUP) as Instructor in Computer Science Department. He is currently a PhD Scholar in Department of Computer Science, University of Management and Technology, Lahore, Pakistan.