Categorization of Internet Protocol Addressing Standards for Sustainable Global Internet of Things Devices

Michael F. Adaramola[1*], Oluwagbemiga O. Shoewu[2], Mary A. Adedoyin[2] and Emmanuel B. Balogun[3]
1. Electrical and Electronics Engineering Department, Lagos State University of Science and Technology, Ikorodu, Lagos State, Nigeria.
2. Electronics and Computer Engineering Department, Lagos State University, Epe Campus, Lagos State. Nigeria.
3. Faculty of Education, Science Technology and Mathematics, University of Canberra, Canberra, Australia.
*Email: adaramola.m@mylaspotech.edu.ng, mfadaramola@yahoo.com and michaeladaramola6@gmail.com

Abstract
This paper surveys the challenges and solutions of the astronomical growing demand of Internet devices available in the global network and Internet of Things (IoT). It is obvious that the availability of these internet infrastructures had led to the depletion of assigned Internet Protocol version 4.0 (IPV4) addresses worldwide. It extensively and equally studies the categories of IP address standards and features for sustainable IoT infrastructures. At the moment, four out of the Regional Internet Registry (RIR) namely: Annenberg Research Network on International Communication (ARNIC), Reseaux Internet Protocol (IP) Europeens (RIPE), Latin America and Caribbean Network Information Center (LACNIC), and Asian Pacific Network Information Center (APNIC) have exhausted their allocated IPV4 addresses. The Africa Network Information Centre (AFRICNIC) which is known as Regional Internet Registry for Africa (Africa's RIR) is also reportedly depleted. The study examined the limitations of IPV4, the features of IPV6 and different methods of operating IPV6 standard. Findings show that the American Registry for Internet Numbers (ARIN) and others are still operational while the current population of the world is over 8billion people with a projection of 9.5billion people by the year 2050. It is vivid that IPV6 can conveniently accommodate 2^{128}=3.4028 x 10^{38} devices at a global scale. The research work has equally show that the acquisition and implementation of IPV6-based infrastructures could only be the possible solution to sustain Internet of Things (IoT) devices worldwide.

Keywords: Internet of Things, IoT Infrastructures, Internet Protocol Address, IP Address Depletion, Migration, Implementation, Global Scale.
DOI: 10.7176/JIEA/15-2-04
Publication date: May 28th 2025

1. Introduction

The Internet has already made a tremendous impact in many countries all-over the world, but it is only the beginning. The internet will dominate as the resource for sharing data as networks of the communities, campuses, establishments, cities, homes become more powerful and robust. There are many aspects of seamless Internet of Things communications systems which include Radio Frequency Identification (RFIDs), Wireless Sensor Networks (WSNs), Mobile Ad-Hoc Networks (MANETs),Vehicular Ad-Hoc Networks (VANETs) and one of the most important aspects is the ability to interface physical networks with multiple operating systems [1-7]. The internet protocol is mainly the software designed for this interface. Users, application programs and higher layers of protocol software use the internet protocol addresses to communicate [[7-11]. Obviously, this is the essence of the communication that occurs throughout the internet world. The internet protocol remains important issue for several reasons. It is non-proprietary, open, and it offers ways to merge voice and data traffic on a common platform (i.e. convergence). The IP networks meet the requirements for interoperability and integration, scalability, mediation, reliability, manageability, security, and have tremendous global reach. Each version of the internet protocol has similar characteristics and abilities [12-18]. IPV6 has taken advantage of IPV4's history and will be the only protocol that will meet the needs of public network in Nigeria. This paper is organized as follows: Section 2 broadly enumerated the reviewed recent related works on Internet of Things (IoT) infrastructures. Section 3 discusses the limitations of the internet protocol version 4.0 (IPV4) addresses. Section 4 studies the various categories of internet protocol version 6.0 (IPV6) addresses standard. The various sustainable comparative features of IPV6 addresses were discussed in Section 5. Finally, we conclude this paper in Section 6.

2. Reviewed Recent Related Works

Cibira G., et al, (2022) a novel concept based on statistical detection and monitoring of sensing signals in IoT environment was presented. This technique successfully performed in an ICT-based and IoT environment [19].

Lakshmanna K., et al, (2022) the major efforts that were achieved in the field of deep learning (DL) for the IoT technology were surveyed and summarized. The survey was implemented in the IoT environments using deep learning on the IoT devices [20].

Schelhaas W., et al, (2022) the network performance in the IoT system by incorporating the long Short-term Memory (LSTM) algorithm in the IoT environment using machine learning (ML) and deep learning (DL) was proposed [21].

Oktian Y., et al, (2022) a bandwidth trading framework to utilize block-chain and software defined networking was introduced. This was implemented and tested in an ICT-based institution [22].

Bzai J., et al, (2022) the literature on the classification of three perspective applications using machine learning (ML)-enabled IoT was discussed [23].

Subramani N., et al (2022) a technique to reduce the energy consumption for IoT nodes and increased the efficiency in addition to route adjustment scheme was proposed. The IoT devices were used in the IoT environment in course of testing the proposed method [24].

Hui J., et al (2022) a dynamic algorithm for internet data bandwidth allocation was proposed. In addition, the neural network was used to predict and improve its polling mechanism. This was implemented using machine learning (ML) and deep learning (DL) in the IoT-based environment [25].

Nakhlestani A., et al (2021) a voltage regulator referred to as low drop-out (LDO) was modeled, designed and constructed. This regulator was used to enhance data bandwidth availability for IoT applications in IoT environment. The LDO regulator model was incorporated with a special communication circuits in its implementation [26].

Pratap A., et al (2020) the maximization of the number of tasks for the IoT-based 5G network environment was presented and proposed. This was adequately examined in an ICT-based environment [27].

Islam M., et al (2019) a communication trial to enhance the bandwidth for IoT-based applications for an ICT-based organization and IoT environment was proposed. This trial was achieved only from a communication perspective [28].

Medeiros V., et al (2019) a multi-objective approach to guide the routing process in mixed IoT traffics in IoT environment based on the use of Machine Learning (ML) and Deep Learning (DL) was proposed. This approach was tested using only a data set of elderly health care scenario captured [29].

Ghanbari Z., et al (2019) the investigations and survey about resource allocation algorithm and methods in IoT environments was proposed. It supports IoT devices and it ended up as a survey [30].

Zhao X., et al (2018) an information flowchart model to minimize usage of bandwidth for IoT applications for an ICT-based institution and IoT environment was proposed [31].

Ma Z.,et al (2017) two different methods to optimize the allocation of bandwidth for heterogeneous IoT traffics were proposed[32].

Marquesone R., et al (2017) bandwidth consumption architecture in an organization without the specification of the IoT technology was designed and implemented [33].

Liu Z., (2017) a model to adapt the bandwidth in wireless sensor network (WSN) in an institution also considered that the WSN is the same for Internet of Things (IoT) was presented [34].

2. Limitations of Internet Protocol Version 4.0

The IPV6 is simpler than IPV4 for a couple of many reasons. The designers had twenty years of experience before IPV6 was designed and implemented. In a nutshell, there has been time to identify the weaknesses in IPV4 and make several corrections. Some of these weaknesses are highlighted as follows:

3.1 Security

The security need to be present both inside and outside of any establishment or institution is very germane to the sustainability of network and IoT devices. Therefore, public networks in Nigeria as an example will not accept outsiders (i.e. intruders) being able to monitor the activities inside the entire networks of organization.

Presently, IP security which constitutes the core of medical internet of things (MIoT) and industrial internet of things (IIoT) had been implemented in both IPV4 and IPV6. Since it has been implemented in IPV4, there are very few differences between the two protocols when it comes to security [35-42]

It is vivid that IPV4 will not be able to sustain the volume of devices that will be needed in public network. Eventually, Classless Inter-Domain Routing (CIDR) will not provide the level of aggregation required, and Network Address Translation (NAT) will be available. NAT already has limitations and IP security is gaining more popularity because of Virtual Private Networks (VPNs). NAT is just a temporary solution to an existing problem; it is not a long-term solution. CIDR is still not supported in all parts of the internet. Even if the addresses were not completely depleted, the addresses would still need to be managed carefully. It is already difficult to manage a depleting address space and will only become more difficult in the next generation.

3.2. Volume

The IPV4 is limited to 4.2 billion devices communicating on the global network at any given point in time. It is already estimated that the globalization of IoTs will attain an astronomical increase of 5.5 billion by 2025. For better analysis, IPV4 uses 32 bit, the total internet protocol addressing space is estimated as IPV4 = 2^{32} = 4.2949 x 10^{9} = 4.295 Billion addresses which can never survive in another one year [43-49].

However, this space will not be enough in the next generation. The volume of devices will increase dramatically as smart Medical internet of things (MIoT), Vehicular internet of things (VIoT), Industrial internet of things (IIoT), and Agricultural internet of things (AIoT) devices are developed and incorporated into the public networks in all the countries of the world. Many organizations today have computers, laptops, palmtops, GSM Mobile phones with internet connections, but this does not resemble the public internet networks of the next generation. They will have a high density of nodes and will consist of many complex systems that are made up of many individual devices [48-55].

3.3 Data Flow

The key to effective data flow is the ability to efficiently handle packets in IoT environments. The less handling that is needed to allow the packets to traverse the network optimally, the more flexible the protocol will be. Obviously, IP has mostly been used for data applications that are suitable for a best effort delivery system. Streaming video and voice has not been widely distributed via the Internet because of bandwidth limitations and the lack of Qualify of Service (QoS).This is very peculiar to the large-scale enterprise WAN and Internet Services. Data flow is not efficient in IPV4. The IPV4 headers vary in size, which means the routers have to calculate the length of an IPV4 payload, which creates additional overhead. IPV4 was not designed to handle the needs of voice, video and other that need quality of service.

4. Internet Protocol Version 6.0 Address Categories

There are three categories of addresses in IPV6 addressing – anycast, unicast and multicast. The IPV6 addresses are assigned to interfaces not nodes. It is not necessary for all of the interfaces to have specific IP addresses, thus saving address space. If two nodes are merely passing traffic they do not need to have IPV6 addresses [56-58].

4.1 Anycast

Anycast addresses are a single address assigned to more than one interface and are designed so that only a single node will receive the datagram, usually the closest node. For example, if a request is sent out to get the time from a timeserver, the message will be addressed to any router that has an associated timeserver. However, it is most effective if the closest available timeserver responds. Once the datagram reaches the closest timeserver, the node will respond and the original datagram will not travel any further. This is helpful for certain types of services that do not require a relationship between the client and the server. The other uses for any cast any identifying a set of routers that belongs to an internet of things (IoT) and internet service provider, a set of routers that are part of a particular subnet, and a set of router that provides an entry to a particular routing domain.

There are currently two limitations placed on anycast addresses. First, an anycast address cannot be used as a source address and second, an anycast address can only be assigned to a router [59-65].

4.2 Unicast

There are several forms of Unicast addresses: Aggregatable global Unicast (AGU) address, Network Service Access Point (NSAP) address, Internet work Packet Exchange (IPX) hierarchical address, the site-local address, the link-local address and the IPV4 capable address. Unicast addresses are designed assuming that the routing decisions are based on a longest prefix match.

The node can be made a ware of as much or a little of the address as needed, depending on the node's function. The address may be viewed as a single piece of information or the information can be parsed into smaller pieces. In the end, the address still needs to be 128–bits, and will identify a node interface. The unicast address is designed to support current provider aggregation and a new type of aggregation called exchanges. The option selected was exchange-based addresses. These addresses are allocated through the internet provider. An address block is assigned to a service provider and the subscriber accesses the network through the provider. There is little maintenance required on behalf of the subscriber.

There are five parts of a unicast address. The first part is the 3-bit prefix (010), which is then followed by the Top Level Aggregator (TLA). The TLA can either be a provider or an exchange point. The routing tables will only need to have one entry per TLA. The TLA's are 13-bits, which imply that there is a possibility of having 8,192 exchange points or backbone providers. There are 8–bits reserved between the TLA and the next frame. The next address component is the Next Level Aggregator (NLA) which is 32–bits long and will be used to allow ISPs to implement their own addressing hierarchy. The site-level aggregation identifier is given to organizations for example, Cadbury Nigeria PLC for their internal network structure and is 10 bits long. This portion of the address supports 65,535 individual subnets per site. This should be sufficient for all but the largest organizations. The last field in the address is the interface identifier. A unicast address may be viewed as a two-field entity, one identifies the network and the other identifies the nodes interface. The interface identifiers are required as part of the addressing architecture, and they are fundamentally based on the IEEE EUI-64. This 64-bit identifier which is used to uniquely identify each and every network interface, which means that there can be 18 billion different addresses, which is only half of the IPV6 addressing space. Mathematically, 2^{64}=1.8447 x 10^{19} Addresses is equivalent to 18 billion addresses.

There are three levels of the hierarchy: public topology, site topology and interface identifier. The public topology is the public internet transit services. This is the global part of the network that requires unique global addresses. There have been two different segments of the address space allocated to support this ability. There are two types of local-use unicast addresses: link–local and site-local. The Link–local addresses are used in auto-address configuration; neighbour discovery, or where there are no routers present. These addresses are intended to identify hosts on a single network link. Site-local addresses are used internally within the site network and cannot be used in the global network. Routers will not forward packets with site-local or link-local source addresses [66-74].

4.3 Multicast

With multicast, each transaction is only carried over each link once. The transmission is dropped off' and duplicated at each node. This can lead to great improvements in efficiencies over distributed LANs. In addition, unlike point-to-point communication, multicasting is easily sealable. The network and the IoTs do not feel the brunt of an increase in traffic, even if the number of users is greatly increased; multicasting achieves this by having three basic requirements:

(i) Routers must be able to efficiently locate route to many LANs at once
(ii) Only a single copy of each packet should be sent on any shared link
(iii) Traffic should only be sent on links that have at least one recipient

There are many uses for multicasting. The need for multicasting continues to grow as the number of users increase and new applications are more feasible. Multicasting can add significant functionality without impacting the network. There are three general categories for multicast applications:

(1) One-to-many (single source to multiple receivers)
(2) Many-to-One (multiple sources to one receiver)
(3) Many-to-Many (any number to hosts sending to the same multicast group address and receiving from it)

Research work showed that an organization called Mboore Systems Limited was established to implement and test multicasting in the early 1990's. So, Mboore is an overlay network that has been used to accelerate the early usage of multicasting through the internet. We understand that IPV4 has a designed range of addresses that have been identified for multicast. Although a class of addresses has been identified, a majority of IPV4 routers are not multicast enabled router at the source and the destination. Tunneling is used to forward multicast packets throughout the rest of the network. The Mboore solution does not fully capitalize on the efficiencies and capabilities of a truly multicast enabled network. It is the basic building block of telecommunication networks. It has also tremendously power the worldwide internet with high-speed and low-power MOS integrated circuits. Advances in MOSFET or MOS technology have been the most important contributing factor in the rapid rise in bandwidth in telecommunication networks. It is noteworthy to state that continuous MOSFETs scaling along with various advances in MOS technology has enabled both Moore's law (Transistor counts in integrated circuit chips doubling every two years) and Edholm's law (Communication internet data bandwidth doubling every one and half years (18 months)). The packets must be encapsulated and assigned a unicast address while traversing the non-multicast enable portion of the entire Wide Area Network. The designers of IPV6 wanted to ensure that all IPV6 nodes could take advantage of multicasting. The multicast addressing that is used in IPV6 can be identified by all routers and all of the experience that has been gained in Mboore's IPV4 multicasting has been incorporated into IPV6 multicasting. Lastly, multicasting has been part of the development of IPV6 since the beginning, so in a fully deployed IPV6 network multicasting is a seamless and advantageous in the implementation of hyper-sensitive internet of things (IoT) devices and infrastructures [75-83].

5. Internet Protocol Version 6.0 Features

5.1 IPV6 Autoconfiguration

The IPV6 incorporates the Dynamic Host Configuration Protocol (DHCP) which allows the host to obtain all of the relevant information. It also supports automated address changes, mobile hosts, and dead neighbour detection. Link-local addresses can be determined by using the link-local prefix and a unique token that will give the node its unique identity. The link-local address is then used to initiate membership in all nodes multicast group. A solicitation message is sent out if a router advertisement message is not received during one of the regular intervals. The solicitation message will be sent three times to ensure that there isn't a router on the network. If no router responds, then the node will continue to use its link-local address and only communicate with the nodes on the local network. After this address is established the node will send out another message with the address that it was assigned. If another node responds, it will reveal a duplication of addresses by exposing a collision. Address resolution and neighbour discovery are handled differently than IPV4. Neighbour discovery combines the Address Resolution Protocol (ARP), the Internet Control Message Protocol (ICMP), Router Discover messages and the ICMP Redirect message found in IPV4. Routers and neighbours will advertise their availability or solicit an advertisement in order to determine if they are available, to verify addresses, and to establish link-layer addresses. Neighbour discovery defines where the node is on the network, and the path that the diagram must travel in order to reach the destination. Nodes also use neighbour discovery to determine the links layer addresses for nodes that are on attached links and to purge addresses that have become invalid. This allows for nodes to determine which routers are will routers are willing to forward packets on their behalf, and which nodes are reachable and which nodes or not. Neighbour discovery also allows for new paths when the current path fails.

There are a couple of key improvements from IPV4 to IPV6. The first is that router discovery is part of the base protocol set and no additional packet exchange is needed to resolve link-layer address because the router advertisements carry the addresses and prefixes for a link. Router advertisements make address auto configuration possible. It is glaring that more multicast addresses are available to handle address resolution and the address resolution process is much more direct without having to affect unnecessary nodes. Redirects contain more data about the first hop, which means fewer messages will be generated. The protocol is more media-independent than ARP because address resolution is at the ICMP layer, and makes IP authentication and security mechanisms possible [84-92].

There are IPV6 advertisements that would replace common IPV4 advertisements. Some of the advertisement is consolidated and some are more efficient to minimize the impact on the network.

5.2 IPV6 Security

One of the keys of internet-level security is that it simplifies the development of secure applications. It will be the baseline for application developers to build on and it will mean that security is available on all operating system platforms. As more data is shared, the more threats there is to networked systems and the higher the livelihood for invasions of privacy and confidentiality. This is critical in the campus, military and IoT environment where much of the data is extremely official and confidential. Confidentiality must be maintained and only authorized personnel can access the information collected and stored. When IPV6 was in its infancy, security was a high priority. With the onset of a new protocol, the opportunity presented itself to be able to complement security with the data link layer, instead of relying on higher level protocols. The IP layer security only protects the IP datagrams which is not detrimental to the functionality of the entire network. The IP security is basically transparent to the user, and can create a foundation for other forms of security to be incorporated. IP traffic is susceptible to interception, sniffers, denial of service and spooling. Interception occurs when the data transmitted from one node to another is taken from an unauthorized third party. A sniffer is a program that monitors and analyzes network traffic, detecting bottlenecks and problems. Some of these sniffers not only analyze traffic, the actual payload data can be read. Denial of service can happen when an authorized user cannot access the network resources. This happen by flooding the host with requests or unnecessarily sending data only to block the flow of other data. Spooling occurs when a packet is altered to misrepresent the packets' origin. For a long time security was not considered important at the internet layer. In most circumstances security issues have been handled in higher layers. Spooling denial of service, hijacking and interception of connections have raised the level of interest of security in the IETF.

IP security (IPsec) is security architecture for the internet protocol. It is not intended to make the internet secure, it is intended to make IP secure. IPsec defines security services that can be used at the IP layer for IPV4 and IPV6. The goals for IP security are to authenticate, maintain the integrity and confidentiality of the IP packets. These are three areas that are very important in the campus network. The security services that are a component of IPsec is Access control connectionless integrity, Data origin Authentication Defense against replay attacks, Encryption and Traffic flow confidentiality. All of these functions will be made possible by the use of encapsulating security payload headers and authentication headers. The Encapsulating Security Payload (ESP) Header is designed to allow IP nodes to send and receive datagram whose payload is encrypted. Some of its function overlaps with the authentication headers, but ESP adds a level of confidentiality by transforming the data. This header is designed to provide confidentiality of datagrams through encryption, authentication of data origin through the use of public key encryption, anti-replay services through the same sequence number mechanism and limited traffic flow confidentiality through the use of security gateways.

ESP does allow for attackers to study traffic because it appears to be a regular datagram, the only difference is that the payload is encrypted. Tunneling and security gateways can also be used with ESP. Security associations rely on the use of Keys. This is prevalent in the large enterprise network. Efficient deployment of security will rely on the existence of an efficient key distribution method and the key-management procedures determine the security parameter index as well as providing the keys. There are several proposals that are under examination at the current time. Simple key-management for Internet protocols (SKIP), Internet Security Association and Key-Management Protocol (ISAKMP) and manual key distribution. When IPV6 packets are sent, they all convey a security parameter index (SPI). Each node must know the SPI to determine the security context, whether it is one node or a group of nodes in a multicast environment. Both authentication and encryption are based on a concept of security association [93-101].

A security Association normally includes the parameters listed below, but might indicate additional parameters as well:

- Authentication algorithm and mode of algorithm used with the IP Authentication Header
- Key(s) used with the authentication algorithm in use with the Authentication Header.
- Encryption algorithm, algorithm mode and transformation used with the IP Encapsulating security payload.
- Key(s) used with the encryption algorithm in use with the EPS.

A. IPV6 Data Flow

In public network, Internet bandwidth on demand and the ability to control the flow of packets will be important issues. There will be a need for a constant flow of data in and out of the public networks, which will require steady bandwidth. There will also be a need for data transmission that is busty and sporadic. In addition, there will be voice transmission which is relatively low in bandwidth but requires continuous streaming. Whether it is busty, streaming or real-time, IP is expected to be one protocol that will be able to handle all types of communications. Bandwidth will need to continually increase as files continue to grow in size and more information will be accessed remotely. The arrangement of the IPV4 is shown in Figure 1.

<table>
<tr><td>Version</td><td>JHL</td><td>Types of service</td><td colspan="2">Total length</td></tr>
<tr><td colspan="3">Identification</td><td>Flags</td><td>Fragment offset</td></tr>
<tr><td>Time-to-leave</td><td colspan="2">Protocol</td><td colspan="2">Header Checksum</td></tr>
<tr><td colspan="5">Source Address</td></tr>
<tr><td colspan="5">Destination Address</td></tr>
<tr><td colspan="4">Options</td><td>Padding</td></tr>
</table>

Figure 1: IPV4 Arrangement

Note, the header length field found in IPV4 is not necessary in IPV6 because all IPV6 headers are the same. IPV4 headers can be as short as 20 bytes and as long as 60 bytes. The IPV4 datagram length is the entire datagram including headers. Routers calculate the length of an IPV4 payload by subtracting the Header length from the datagram length; IPV6 does not need to process this calculation. The type of service is really made up of two sub-fields precedence and type of service. Precedence is the level of priority and the type of service bits defined, namely: a delay bit, a throughput bit and a reliability bit. These types of service bits were designed to compute a default route, the shortest route, the largest throughput or most reliable route. The precedence indicator is used for queuing purposes. There are eight preference values, and works on the premises that the packet with the highest priority will be sent first. The fragmentation and reassembly process use the identification, flags and offset fields. When an IPV4 packet is fragmented, it is given complete IP headers, which are copied from the original packet. If one fragment is lost, the entire packet must be resent. In IPV6, only the source router does the fragmentation while in IPV4 fragmentation can be done at any intermediary node. In IPV6, all intermediary nodes ignore the fragmentation extension headers which improve efficiency as the packets are routed. IPV6 has some major changes over IPV4 when it comes to the header. With all of the additional tools available in IPV6, multimedia will become even more a reality or at least start to address some of the real expectations of multimedia. The timing issues and bandwidth requirements have been addressed with IPV6. In public network where large amounts of traffic can cause delays and bottlenecks. One of the ways of dealing with vast amount of data is by maximizing the use of bandwidth. Multicasting will be an easy solution of disseminating a large amount of data to many users without typing up valuable network resources. There are applications that will continue to emerge as a result of multicasting. It will be important to have the ability to join a newsgroup and a weather forecasting group. Even when it comes to conducting research such as the census, the many-to-one capability that multicasting offers will be a tremendous help.

In addition, the data that is being sent doesn't have to be broadcast out into the entire world. It is only sent to the users who request it or need to receive it. An Anycast addressing will give the ability for efficiency as well when it comes to keeping all of the docks up-to-date. The other advantage of IPV6 is the source router will fragment the payload prior to sending them into the network if sufficient bandwidth is not provided between the source and destination [100-109]. IPV6 Headers includes the following: Version, Class, Flow Label, Payload Length, Next Header, Hop Limit, Source Address and Destination Address. The arrangement of the IPV6 is shown in Figure 2.

<table>
<tr><td>Version</td><td>Class</td><td colspan="3">Flow label</td></tr>
<tr><td colspan="3">Payload Length</td><td>Next Header</td><td>Hop Limit</td></tr>
<tr><td colspan="5">Source Address</td></tr>
<tr><td colspan="5">Destination Address</td></tr>
</table>

Figure 2: IPV6 arrangement

The IPV6 header, which is 40 octets, is approximately twice the size of an IPV4 header, but provides some simplification from the IPV4 header. All headers have a fixed format, there is no longer a checksum, and the hop-by-hop segmentation procedure has been removed. There are eight (8) fields in the IPV6 header, namely:

i. Version (4 bits)
ii. Traffic class (8 bits)
iii. Flow Label (20 bits)
iv. Payload Length (20 bits)
v. Next Header (8 bits)
vi. Hop Limit (8 bits)
vii. Source Address (128-bit)
viii. Destination Address (128-bit)

The version field indicates the version of IP in use. The traffic class filed contains a value that identified the priority level for delivering packets. Each individual packet can have a different priority even if it originated from the same source. There are two ranges of priorities 0–7 and 8–15. Priorities 0–7 are reserved for low priority packets. If traffic is heavy like the large-scale enterprise, the packets will back off. These packets do not need to arrive in real time and can be delayed. Priorities 8-15 are used for non-congestion controlled or real-time traffic. The packets that are sent at 15 are critical for maintaining a constant rate, and the packets at 8 are still real-time traffic, but the transmission would not suffer tremendously if the packet was lost.

The flow label gives the source the ability to label a sequence of packets, which requires the router to give the packets special handling. All packets belong to the same flow must have the same source, destination, priority and flow label. A flow label can be used to establish routes that give better service, including lower delay or bigger bandwidth. Each and every packet that has flow labels changes the handling within the router, which can cause difficulties within the cache of the router. The payload length defines the length of the packet following the header. The minimum payload is 576 octets which has the ability to have payload greater than 65,535 bytes called Jumbo” payloads. The field identifies jumbo packets by setting the payload length to zero and then specifying the length in the Hop-by-Hop extension header.

The Next Header field identifies the header that is immediately following the IPV6 header. These extension headers are used to specify special case treatment of some packets.

The extension headers could be an Authentication Header, an Encapsulation Security Header, a Routing Header, an upper layer Header, a fragment Header, Destination options Header or a Hop-by-Hop options Header. There is a recommendation for the order in which these extension headers are placed in the IPV6 packet. The Hop Limit identifies the number of hops the packet can travel from its source to the destination. This is a counter that decrements by one at each hop count. Once the field reaches zero, the packet is discarded. IPV6 has the ability to measure the maximum number of hops that can occur as the packet is forwarded. This replaces the Time-to-leave field found in IPV4, and no longer use time as a component. The source address field contains the 128-bit address of the originator and the destination address field contains the destination address. The interface identifiers are required as part of the addressing architecture, and are based on the IEEE EUI-128. This 128-bit identifier which is used to uniquely identify each and every network interface, which means that there can be 3.4028 x 10^{38} different addresses, which is tremendously greater than that of IPV4 addressing space. The IPV6 with 128-bit will definitely make 2^{128}=3.4028 x 10^{38} addresses available for the future devices and machines at a global scale [109-117].

6. Conclusion

In this paper, the several limitations of IPV4 were fully examined. Study shows that IPV6 does not possess the limitations of IPV4. In a nutshell, there are enough unique addresses available in IPV6 to sustain the expected astronomical growth of network devices and Internet of Things (IoT) infrastructures and devices well into the next generation. With the 128-bit IPV6 addressing space, we have 2^{128}=3.4028 x 10^{38} IP addresses available. No doubt, this expansion of address will accommodate the future growth expected in every sector. The urgent need to migrate from IPV4 standard to that of IPV6 now becomes the all-important assignment of every institution, company, institution of higher learning, enterprise and organization in all the nations.

Finally, IPV6 is extremely robust, scalable, efficient, and of high standard. Therefore, it will inevitably sustain the internet backbone of the next generation in Nigeria and other countries of the world.

References

[1] Adeel A., et al., (2019) A Survey on the Role of Wireless Sensor Networks and IoT in Disaster Management, in: T.S. Durrani, W. Wang, S.M. Forbes (Eds.), *Geological Disaster Monitoring Based on Sensor Networks, Springer,* Singapore, pp. 57–66
DOI: https://doi.org/10.1007/978-981-13-0992-2_5

[2] Adel Abusitta, Glauco H. S. De Carvallio, Omar Abdel Wahab, Talal Halabi, Benjamin C. M. Fung and Saja A. Mamoori, (2023) Deep Learning-enabled Anomaly Detection for IoT Systems, *Journal of Internet of Things,* Vol. 2 Issue 10,
DOI: https://doi.org/10.1016/j.iot.2022.100656

[3] Ahmad Showail, Rashid Tahr, Muhammad Fared Zaffar, Muhammad Haris Noor and Muhammed Al-Khatib, (2022) An Internet of Secure and Private Things: A Service-oriented Architecture, *Journal of Computers and Security*, ISSN: 0167-4048, DOI: https://doi.org/10.1016/j.cose.2022.102776

[4] Ahmad T. Suliman, Maha Kadadha, Rabeb Mizouri, Hadi Otrok, Ernesto Damiani and Mahmoud Al-Qutayri, (2023) Block-check:: A Consortium Block-chain-based Conformance Checking Framework for Business Processes, *Journal of Internet of Things*, Vol. 2 Issue 2, DOI: https://doi.org/10.1016/j.iot.2022.100652

[5] Ahmed Nasrallah, Venkatraman, Balsubramanian, Akhilesh S. Thyagaturu, Marin Reisslein, and Hesham ElBakoury, (2021) Reconfiguration Algorithms for High Precision Communications in Time Sensitive Networks: Time-aware Shaper Configuration with IEEE 802.1QCC, *ITU Journal on Future and Evolving Technologies,* Vol. 2 Issue 1 pp 13-34

[6] Aimilios Tzavaras, Nikolaos Mainas, Euripides G. M. Petrakis, (2023) Open-API Framework for the Web of Things, *Journal of Internet of Things*, Vol. 2 Issue 8,
DOI: https://doi.org/10.1016/j.iot.2022.100675

[7] Alfredo J. Perez, Farhan Siddiqui, Sherali Zeadally and Derek Lane, (2023) A Review of IoT Systems to Enable Independence for the Elderly and Disabled Individuals, *Journal of Internet of Things,* Vol. 2 Issue 12,
DOI: https://doi.org/10.1016/j.iot.2022.100653

[8] Ali Shakil, Mohammad Ali Khalighi, Pierre Pudlo, Cyril Leclerc, Dominique Laplace, Francois Hamon and Alexandre Boudonne, (2023) Outlier Detection in Non-stationary Time Series Applied to Sewer Network Monitoring, *Journal of Internet of Things*, Vol. 2 Issue 11, DOI: https://doi.org/10.1016/j.iot.2022.100654

[9] Amichai-Hamburger Y, Fine A and Goldstein A., (2004) The Impact of Internet Interactivity and Need for Closure on Consumer Preference Computers in Human Behaviour, *IEEE/ACM Transaction on Networking*, Vol. 5, pp 103-117

[10] Andrey Garnaev, Wade Trappe, Narayan B. Mandayama and H. Vincent Poor, (2021) A Multi-Link Communication Connectivity Game Under Hostile Interference, *ITU Journal on Future and Evolving Technologies,* Vol. 2 Issue 1, pp 101-112

[11] Aparma Sinha, Deepraj Chowdhury, Ssandeep Sharma, Yashava Raj Sherke and Debanjan Das, (2023) nCare: Fault-aware Edge Intelligence for Rendering Viable Sensor Nodes, *Journal of Internet of Things*, Vol. 2 Issue 11,
DOI: https://doi.org/10.1016/j.iot.2022.100643

[12] Ashutosh Dhar Dwivedi and Gautam Srivastava, (2023) Security Analysis of Lightweight IoT Encryption Algorithms: SIMON and SIMECK*, Journal of Internet of Things,* Vol. 2 Issue 11,
DOI: https://doi.org/10.1016/j.iot.2022.100677

[13] Balasubramaniam S., Vijesh Joe C., SivaKumar T. A., Prasanth A., Suthesh Kumark, Kavith V. and Rajesh Kumar D., (2023) Optimization Enabled Deep Learning-Based DDoS Attack Detection in Cloud Computing, *International Journal of Intelligent Systems,* DOI: https://doi.orrg/10.1155/2023/2039217

[14] Bian J., et al., (2022) Machine Learning in Real-time Internet of Things (IoT) Systems: A Survey, *IEEE Internet of Things Journal* (9) (11) pp 8364– 8386.

[15] Brandon Foubert and Nathalie Mitton, (2021) Rodent: A Flexible Topsis-based Routing Protocol for Multi-technology Devices in Wireless Sensor Networks, *ITU Journal on Future and Evolving Technologies,* Vol. 2 Issue 1, pp 89-100

[16] Butler Lampson, Venkatachary Srimirvasan and George Varghese, (1999) IP Lookups Using Multi-way and Multi-column Search, *IEEE/ACM Transaction on Networking,* Vol.7 No. 3, June, 1999 pp 324-334

[17] Bzai J., et al., (2022) Machine Learning-enabled Internet of Things (IoT): Data, Applications, and Industry Perspective, *Electronics Journal* (1) (1) pp 1–33

[18] Cai Zhi, Shu Yuyu, Su Xing, Guo Limin and Ding Zhiming, (2023) Internet of Things: A Traffic Data Interpolation Method for IoT Sensors based on Spatio-Temporal Dependence, *Journal of Internet of Things*

[19] Chatterjee A. and Ahmed B., (2022) IoT Anomaly Detection Methods and Applications: A Survey, *Internet of Things* (1) (9),
DOI: https://doi.org/10.1016/j.iot.2022.100568

[20] Chauhan N., Banka H. and Agrawal R., (2021) Adaptive Bandwidth Adjustment for Resource Constrained Services in Fog Queuing System, *Cluster Computing* 24 pp 3837–3850

[21] Chen J., Touati C. and Zhu Q., (2020) Optimal Secure Two-layer IoT Network Design, *IEEE Transaction Control Networking Systems* (7) (1) pp 398–409

[22] Chen, (2023) FSMFA: Efficient Firmware-secure Multi-factor Authentication Protocol for IoT Devices, *Journal of Internet of Things*, Vol. 2 Issue 8,
DOI: https://doi.org/10.1016/j.iot.2023.100685

[23] Comer, Douglas (1997), Computer Networks and Internets, 2nd Edition, prentice Hall, New Jersey, USA

[24] Dave Miller, (2006) Data Communications and Networks, 1st Edition, McGraw- Hill New York USA

[24] De A., Roy B., Bhattacharya A. and Bhattachaqee A., (2021) Bandwidth-Enhanced Ultra-wide Band Wearable Textile Antenna for Various WBAN and Internet of Things (IoT) Applications, *Radio Sciences* 56 (11) pp 1– 16

[25] Dharminder Chaudhary, Tanmay Soni, Kondeti, Lakshmi Vasudar and Kashi Saleem, (2023) A Modified Lightweight Authenticated Key Agreement Protocol for Internet of Drones, *Journal of Internet of Things*, Vol. 2 Issue 10,
DOI: https://doi.org/10.1016/j.iot.2022.100669

[26] Dibal P. Y., Onwuka E.N., Zubair S., Nwankwo E. I., Okoh S. A., Salihu B. A. and Mustaphab H. B., (2023) Processor Power and Energy Consumption Estimation Techniques in IoT Applications: A Review, *Journal of Internet of Things,* Vol. 2 Issue 12, DOI: https://doi.org/10.1016/j.iot.2022.100655

[27] Dina Fauzy, Sharin M. Moussa and Nagwa I. Badri, (2023) An IoT-based Resource Utilization Framework Using Data Fusion for Smart Environments, *Journal of Internet of Things,* Vol. 2 Issue 11,DOI: https://doi.org/10.1016/j.iot.2022.1006425

[28] Emmanoul Fountoulakis, Nikolaos Pappas and Anthony Ephremides, (2021) Dynamic Power Control for Time-critical Networking with Heterogeneous Traffic*, ITU Journal on Future and Evolving Technologies,* Vol. 2 Issue 1, pp 1-12

[29] Enjie Lin, Youbing Zhao and Abimbola Efunogbon, (2023) Boosting Smarter Digital Health Care with 5G and Beyond Networks, *ITU Journal on Future and Evolving Technologies,* Vol. 4 Issue 1

[30] Evizal Abdu Kadir, Sharul Kamal Abdul Rahn, Raed Shibair and M. Himdi, (2021) B5G and 6G: Next Generation Wireless Communications Technologies, Demand and Challenges, *Journal of IEEE-Xplore* ISBN: 9781665412247 DOI:10.1109/:COTEN52080.2021.94934

[31] Ghanbari Z., et al., (2019) Resource Allocation Mechanisms and Approaches on the Internet of Things, *Cluster Computing* 22 pp1253– 1282

[32] Goncalves, Marcus, Niles and Kitty (1998) IPV6 Networks, 1st Edition, McGraw-Hill, New York, USA

[33] Habeeb F., et al., (2022) Dynamic Bandwidth Slicing for Time-critical IoT Data Streams in the Edge-cloud Continuum, *IEEE Transaction Industrial Information* (18) (11) pp 8017–8026

[34] Hsu S., Lin C., Wang C. and Chen W., (2018) Breaking Bandwidth Limitation for Mission-critical IoT Using Semi-sequential Multiple Relays, *IEEE Internet of Things Journal* (5) (5)) pp 3316–3329

[35] Hui J., Gan C., Liu X. and Zhan N., (2022) A Dynamic Bandwidth Allocation Algorithm Based on Differentiated Service Cycle in Multi-service Hybrid VPON: Fiber Integration Optimizations, pp 1–18
DOI: https://doi.org/10.1080/01468030.2022.2150588.

[36] Huitema, Christian (1995), Routing In the Internet. 1st Edition, Prentice Hall, New Jersey. USA.

[37] Huitema, Christian (1996), IPV6-The New Internet Protocol, 2nd Edition, Prentice Hall, New Jersey, USA

[38] Irfan M., et al., (2021) Non-wearable IoT-based Smart Ambient Behaviour Observation System, *IEEE Sensors Journal* (2) (8) pp 20857–20869
DOI: https://doi.org/10.1109/ JSEN.2021 3097392

[39] Islam M., et al., (2019) A Modified Meander Line Micro-strip Patch Antenna with Enhanced Bandwidth for 2.4GHz ISM-Band Internet of Things (IoT) Applications, *IEEE Access* 7 127850–127861.

[40] Istvan Godor, Iman Grida and Ben Yahia, (2022) Topics from Networks Management and Operations, *Journal of Internet of Network Management*, 2022; 32e2182 pp 1-2
DOI: https://doi.org/10.1002/nem.2182

[41] Ito Y., Koga H. and Iida K., (2016) A Bandwidth Reallocation Scheme to Improve Fairness and Link Utilization in Data Centre Networks, in: *IEEE International Conference on Pervasive Computing and Communication Workshops* (PERCOMW Workshops), Sydney, Australia, 1st –4th March, 2016 7457064, pp14-18

DOI: https://doi.org/10.1109/percomw

[42] James F. Kurose and Keith W. Ross, (2000) Computer Networking: A Top Down Approach Featuring the Internet, 1st Edition, Addison – Wesley, USA

[43] Jianbing Liang, Shiehu Chen, Zilling Wei, Shuang Zhao and Wei Zhao, (2022) HAG Detector: Heterogeneous DGA Domain Name Detection Model, *Journal of Computers and Security,* Vol. 120, DOI: https://doi.org/10.1016/j.cose.2022.102803

[44] Kassim M., Ismail M., Jumori K. and Yusuf M. I., (2012) A Survey: Bandwidth Management in a IP-based Network, *International Journal of Computer and Information Engineering*, (16) (2)

[45] Lakshman T. V. and Madhow U., (1994) Performance Analysis of Window-Based Flow Control using TCP/IP (High Performance Networking V), *IEEE/ACM Transaction on Networking,* Vol. 9 North Holland, pp 135-150.

[46] Lakshman T. V., Upamanyu Madhow and Berhard Suter, (2000), TCP/IP Performance with Random Loss and Bi-directional Congestion, *IEEE/ACM Transaction on Networking*, Vol.8 No. 5, October, 2000, pp 541-555

[47] Lakshmanna K., et al., (2022) A Review on Deep Learning Techniques for IoT Data, *Electronics Journal* 11 (1604)
DOI: https://doi.org/10.3390/electronics11101604

[48] Loshin, Peter (1999), IPV6 Clearly Explained 1st Edition, Morgan Kaufman, San Francisco. USA.

[49] Love Allen Chijioke Ahakonye, Cosmas Ifeanyi Nwakanma, Jae-Min Lee and Dong-Seong Kim, (2023) SCADA Intrusion Detection Scheme Exploiting the Fusion of Modified Decision Tree and Chi-square Feature Selection, *Journal of Internet of Things*, Vol. 2 Issue 8, DOI: https://doi.org/10.1016/j.iot.2022.100676

[50] Lusani Mamushiane, Joyce Mwangama and Albert Lysko, (2021) Controller Placement Optimization for Software Defined Wide Area Networks (SDWAN), *ITU Journal on Future and Evolving Technologies*, Vol. 2 Issue, pp 45-65

[51] Ma Q. et al., (2021) BOND: Exploring Hidden Bottleneck Nodes in Large-scale Wireless Sensor Networks, *IEEE/ACM Transaction Sensor Networking* (17) pp 1–21.

[52] Ma Z., Zhao Q. and Huang J., (2017) Optimizing Bandwidth Allocation for Heterogeneous Traffic in IoT, *Peer-to-Peer Networking 10* pp 610–621

[53] Made Adi Paramartha Putra, Adinda Riztia Putri, Ahmad Zainudin, Dong-Seong Kim, Jae-Min Lee (2023) ACS: Accuracy-based Client Selection Mechanism for Federated Industrial IoT, *Journal of Internet of Things,* Vol. 2 Issue 9 DOI: https://doi.org/10.1016/j.iot.2022.100657

[54] McNealis, Martin (1998), IP crossroads: Migrate to IPv6 or evolve with IPV4. Packet Magazine Archives

[55] Medeiros V., Silvestre B. and Borges V., (2019) Multi-objective Routing Aware of Mixed IoT Traffic for Low-cost Wireless Backhauls, *Journal of Internet Services Applications*, (10) (9) DOI: https://doi.org/10.1186/s13174-019-0108-9

[56] Mengting Yao, Qingqing Gan, Xiaoming Wang and Yuhao Yang, (2023) A Key-insulated Secure Multi-server Authenticated Key Agreement Protocol for Edge Computing-based VANETs, *Journal of Internet of Things*, Vol. 2 Issue 10,
DOI: https://doi.org/10.1016/j.iot.2023.100679

[57] Mhd Rashed Al Koutayni, Gerd Reis and Didier Stricker, (2023) DeepEdgeSoC: End-to-end Deep Learning Framework for Edge IoT Devices, *Journal of Internet of Things*, Vol. 2 Issue 8, DOI: https://doi.org/10.1016/j.iot.2022.100665

[58] Michael F. Adaramola and Michael A. K. Adelabu, (2015) A survey of IP Address for Next Generation Internet Services, *Journal of Computer Engineering and Intelligent Systems* IISTE, (6) (1), pp 1-5.

[59] Michael F. Adaramola, Oluwagbemiga O. Shoewu, Ayoade B. Ogundare and Emmanuel B. Balogun, (2024) Contemporary Perspective on Science, Technology and Research, Vol. 3 Chapter 1: Taxonomy of Internet Protocol Addressing Standards for Next Generation Internet Services, *International Book Publisher,* London, UK pp 1- 16
Print ISBN: 978-81-969009-5-3, eBook ISBN: 978-81-969009-2-2
DOI: 10.9734/bpi/cpstr/v3/19985D

[60] Miller, Mark A. (1998), Implementing IPV6, 1st Edition, M&T Books, New York, USA

[61] Mirsacid Hasseini Shirvani and Mohammad Masdari, (2023) A Survey on Trust-based Security in Internet of Things Challenges and Issues, *Journal of Internet of Things*, Vol. 2 Issue 8, DOI: https://doi.org/10.1016/j.iot.2022.1006420

[62] Mohammadsadeq Garshashi Herabad, (2023) Communication Semi-synchronous Hierarchical Federated Learning with Balanced Training in Heterogeneous IoT Edge Environments, *Journal of Internet of Things*, Vol. 2 Issue 11,
DOI: https://doi.org/10.1016/j.iot.2022.100642

[63] Nakhlestani A., Kaveri S., Radfar M. and Desai A., (2021) Low-power-area-efficient LDO with Loop-gain and Bandwidth Enhancement using Non-dominant Pole Movement Technique for IoT Applications, *IEEE Transaction Circuits Systems Express Briefs* 68 (2) pp 692–696.

[64] Nazil Tekin, Abbas Acar, Ahmet Aris, A. Seleuk Uluagae, Vehbi Cagri Gungor, (2023) Energy Consumption of On-device Machine Learning Models for Intrusion Detection, *Journal of Internet of Things*, Vol. 2 Issue 12,
DOI: https://doi.org/10.1016/j.iot.2022.100670

[65] Oktian Y., et al., (2022) Block-chain-powered Bandwidth Trading on SDN-enabled Edge Network, *IEEE Access* 10 (2022) pp114024–114039

[66] Oliver Bucklay, Duncan Hodges, Jonathan Windle, Sally Earl, (2022) CLICKA: Collecting and Learning Identity Cues with Keystroke Dynamics, *Journal of Computers and Security*, Vol.120, DOI: https://doi.org/10.1016/j.cose.2022.102780

[67] Omar Said, (2023) A Bandwidth Control Scheme for Reducing the Negative Impact of Bottlenecks in IoT Environments: Simulation and Performance Evaluation, *Journal of Internet of Things*

[68] Onossovski V and Terekhov A., (2010) Modern Interactive Internet Services In Proceedings of *7th Conference of Open Innovations Framework Programme* FRUCT 2010

[69] Orsini G., Posdorfer W. and Lamersdorf W., (2021) Saving Bandwidth and Energy of Mobile and IoT Devices with Link Predictions, *Journal of Ambient Intelligent Human Computing* 12 pp 8229–8240

[70] Padmalaya Nayak and G. Swapraa, (2023) Security Issues in IoT Applications Using Certificateless Aggregate Singncryption Schemes: A Overview, *Journal of Internet of Things,* Vol. 2 Issue 11, DOI: https://doi.org/10.1016/j.iot.2022.100641

[71] Prabhat Kumar and S. Suresh, (2023) Deep TransHAR: A Novel Clustering-based Transfer Learning Approach for Recognizing the Cross-domain Human Activities Using GRUs (Gated Recurrent Units) Networks, *Journal of Internet of Things*, Vol. 2 Issue 1, DOI: https://doi.org/10.1016/j.iot.2023.100681

[72] Pratap A., et al., (2020) Bandwidth-constrained Task Throughput Maximization in IoT-enabled 5G Networks, *Pervasive Mobile Computing* pp 6-9,
DOI: https://doi.org/ 10.1016/j.pmcj.2020.101281

[73] Prosper Zanu Sotenga, Karim Djouani and Anish Matthew Kurien, (2023) A Virtual Network Model for Gateway Media Access Control Virtualization in Large Scale Internet of Things, *Journal of Internet of Things*, Vol. 2 Issue 12,
DOI: https://doi.org/10.1016/j.iot.2022.100668

[74] Rahman M., Islam M., Uddin M. and Stea G., (2022) A Survey of Block- Chain-Based IoT e-Healthcare: Applications, Research Issues and Challenges, *Internet of Things*
DOI: https://doi.org/10.1016/j.iot.2022.100551

[75] Rajesh Kumar, Siddharth Sharma and Chrag Vachhani Nitish Yadav, (2022) What Changed in the Cyber-security after COVID-19, *Journal of Computers and Security*, Vol. 120 DOI: https://doi.org/10.1016/j.cose.2022.102821

[76] Raouia Masmoudi Ghadhbane and Joyce Fernandez-Mayoralas, (2021) Performance of a Parallel Hamming Coding in Short-frame OFDM Sensor's Network, *ITU Journal on Future and Evolving Technologies,* Vol. 2 Issue 1, pp 77-87

[77] Rashmi Priya Sharma, Ramesh Dharavath and Damodar R. Edler, (2023) IoFT-FIS: Internet of Farm Things Based Prediction for Crop Pest Infestation Using Optimized Fuzzy Inference System, *Journal of Internet of Things*, Vol. 2 Issue 8,
DOI: https://doi.org/10.1016/j.iot.2022.100649

[78] Ricardo Villalon-Fonsera, (2022) The Nature of Security: A Conceptual Framework for Integral-Comprehensive Modeling of IT Security and Cyber-security, *Journal of Computers and Security,* Vol.120,
DOI: https://doi.org/10.1016/j.cose.2022.102805

[79] Rolando Herrero, (2023) Mechanism IPV6 Adaption in LoRa Topologies, *Journal of Internet of Things,* Vol. 2 Issue 11,
DOI: https://doi.org/10.1016/j.iot.2022.100647

[80] Sara Cavallero, Nicolis Decah, Giampaolo Cuozo, Chiara Buratti, Davide Dardari and Roberto Verdone, (2023) Terahertz Networks for Future Industrial Internet of Things, *ITU Journal on Future and Evolving Technologies,* Vol. 4 Issue 1

[81] Schelhaas W., (2022) Predicting Network Performance in IoT Environments Using Long Short-term Memory (LSTM), [Accessed 14/11/2022].
Scribd:http://tinyurl.com/2ht66mjpv
DOI: https://doi.org/10.5281/zenovo.10450773

[82] Senmiao Wang, Luli Sun, Sujuan Qin, WenMin Li and Wentao Liu, (2022) KRTunnel: DNS Channel Detector for Mobile Devices, *Journal of Computers and Security,* Vol.120, DOI: https://doi.org/10.1016/j.cose.2022.102818

[83] Seyed Mostafa Bozorgi, Mehdi Golsotkhtaabaramiri and Semaneh Yazdani, (2023) A Smart Optimizer Approach for Clustering Protocol in UAV-assisted IoT Wireless Networks, *Journal of Internet of Things*, Vol. 2 Issue 7,
DOI: https://doi.org/10.1016/j.iot.2023.100683

[84] Shalli Rani, Divya Gupta, Norber Herenesar and Guatam Srivastava, (2023) Block-chain-enabled Cooperative Computing Strategy for Resource Sharing in Fog Networks, *Journal of Internet of Things,* Vol. 2 Issue 7,
DOI: https://doi.org/10.1016/j.iot.2022.100672

[85] Sheng Yu, Li Xie, Qilie Huang, (2023) Inception Convolution Vision Transformers for Plant Disease Identification, *Journal of Internet of Things,* Vol. 2 Issue 8,
DOI: https://doi.org/10.1016/j.iot.2022.100650

[86] Shenker S., Zhang L. and Clark D. D., (1990) Some Observations on the Dynamics of Congestion-control Algorithm, *Computer Communications Revision*, October, 1990 pp 30-39

[87] Shwadhin Sharma and Eduardo Aparicio, (2022) Organizational and Team Culture as Antecedents of Protection Motivation Among IT Employees, *Journal of Computers and Security,* Vol.120, DOI: https://doi.org/10.1016/j.cose.2022.102774

[88] Sinche S., et al., (2020) A Survey of IoT Management Protocols and Frameworks, *IEEE Communication Survey Tutorials* (22) (2) pp1168–1190

[89] Sobin C., (2020) A Survey on Architecture, Protocols and Challenges in IoT, *Wireless Personal Communication* (1) (12) pp1383–1429

[90] Stoyanova M., et al., (2020) A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues, *IEEE Communication Surveys Tutorials* (22) (2) pp 1191–1221.

[91] Subramani N., et al., (2022) Controlling Energy Aware Clustering and Multi-hop Routing Protocol for IoT Assisted Wireless Sensor Networks, *Concurrency Computing* 34 (21) DOI: https://doi.org/10.1002/cpe.7106

[92] Sundas Iftikhar, Mirza Mohammad Mufleh Ahmad, Shreshth Tuli, Deepraj Chowdhury, Minxian Xu, Sukhpal Singh Gill and Steve Uhlig, (2023) HunterPlus: AI-based Energy-efficient Task Scheduling for Cloud-Fog Computing Environments, *Journal of Internet of Things*, Vol. 2 Issue 12, pp 1-17
DOI: https://doi.org/10.1016/j.iot.2022.100667

[93] Sundas Iftikhar, Sukhpal Singh Gill, Chenghao Song, Minxian Xu, Mohammad Sadegh Aslanpour, Adel N. Toosi, Junhui Du, Huaming Wu, Shreya Ghosh Deepraj DatasetCuadrado, Blesson Varghese, Omer Rana, Schahram Dustdar and Steve Uhlig, (2023) AI-based Fog and Edge Computing: A Systematic Review, Taxonomy and Future Directions*, Journal of Internet of Things*, Vol. 2 Issue 12, DOI: https://doi.org/10.1016/j.iot.2022.100674

[94] Taha Mansomi, Mohammed Reza Sedeghi Moghadan, Fatemeh Monshizadeh and Ahad Zareravasan, (2021) IoT Data Quality Issue and Potential Solutions: A literature Review, *Journal of Internet of Things*

[95] Taha Mansouri, Mohammad Reza Sadeghi, Moghadam, Fatemeh Monshizadeh, Ahad Zareravasan, (2023) IoT Data Quality Issues and Potentials Solutions: A Literature Review, *Journal of Internet of Things*, Vol. 2 Issue 5, pp 1-15

[96] Terry W. Ogletree and Mark E. Soper, (2006) Upgrading and Repairing Networks, 5th Edition, Que Publishing, USA
URL:http://uu.diva-ortal.org/smash/get/diva2:1597391/FULLTEXT01.pdf

[97] Tomas Surada Reira, Juan-Ramon Bermejo Higuera, Javier Bermejo Higuera,
Jose- Javier Martmez Herraiz, Juan-Antonio Sicilia Montalvo (2023) A New Multi-
Label Dataset for Web Attacks CAPEC Classification Using Machine Learning
Techniques, *Journal of Computer and Security,* Vol. 120
URL: https//www.creativecommons.org/licenses/by/4.0
DOI: https://doi.org/10.1016/j.cose.2022.102788

[98] Vadim Nozdrin, (2021) Economic Efficiency of Spectrum Allocation, *ITU Journal on Future and Evolving Technologies*, Vol. 2 Issue 1, pp 67-75

[99] Valeria Lukaj, Francesco Martella, Maria Fazio, Antonio Celesti and Massimo Villari, (2023) Establishment of a Trusted Environment for IoT Service Provisioning Based on X3DH-Based Brokering and Federated Block-chain, *Journal of Internet of Things*, Vol. 2 Issue 10,
DOI: https://doi.org/10.1016/j.iot.2023.100686

[100] Vern Paxson (June, 1999) End-to-end Internet Packet Dynamics, *IEEE/ACM Transactions on Networking*, Vol. 7 No. 1, June, 1999 pp 277- 292

[101] Wang F., et al., (2020) A Dynamic Bandwidth Allocation Scheme for Internet of Things in Network-slicing Passive Optical Networks, in: *IEEE Computing, Communications and IoT Applications Conference* (ComComAp), 20-22 December, 2020 Beijing, China, pp1–5

[102] Wang R., et al., (2019) Performance Bottleneck Analysis and Resource Optimized Distribution Method for IoT Cloud Rendering Computing System in Cyber-enabled Applications, *Journal of Wireless Computer Networking*, (7) (9),
DOI: https://doi.org/10.1186/s13638-019-1401-9

[103] Waqar Ali Aziz, Vasos Vassiliou, Taqwa Saheed, Andreas Pitsillides and Marios Lestas, (2023) On the Use of Intelligent Meta-surfaces in Data Centres, *ITU Journal on Future and Evolving Technologies*, Vol. 4 Issue 1

[104] Wo-Chang Feng, Dilip D. Kandlur, Debanjan Saha and Kang G. Shin, (1999), Understanding and Improving TCP Performance Over Networks with Minimum Rate Guarantees, *IEEE/ACM Transaction on Networking*, Vol. 7 No. 2, April, 1999, pp 173- 187

[105] Wright G. R. and Stevens W. R., (1995) TCP/IP Illustrated: The Implementation, Vol. 2 Boston MAC, Addison Wesley

[107] www.cisco.com/ohiostate.edu/hypertext/information/rfc.html (2012)

[108] www.cisco.com/warp/public/732/ipV6/index.html (2011)

[109] www.ipmulticast.com/ (2012)

[110] www.ora.Com/Reference/dictionary/terms/ip/InternetProtocolMulticast.htm (2012)

[111] www.rit.edu:8080/Proxy/www.faulkner.Com/products/facts/default.html (2012)

[112] www.whatis.com/ip (2012)

[113] Xuhui Ding, Yue Zhang, Jiaxuan Li, Boyan Mao, Yuting Gao and Gaoyang Li, (2023) A Feasibility Study of Multi-mode Intelligent Fusion Medical Data Transmission Technology of Industrial Internet of Things Combined with Medical Internet of Things, *Journal of Internet of Things*, Vol. 2 Issue 1,
DOI: https://doi.org/10.1016/j.iot.2023.100689

[114] Yingjie Tian, Weizhi Gao, Qin Zhang, Pu Sun and Dongkuan Xu, (2023) Improving Lon-tailed Classification by Disentangled Variance Transfer, *Journal of Internet of Things*, Vol. 2 Issue 11, DOI: https://doi.org/10.1016/j.iot.2023.100687

[115] Zhao X., Lucani D., Shen X. and Wang H., (2018) Reliable IoT Storage: Minimizing Bandwidth Use in Storage without Newcomer Nodes, *IEEE Communication Letters* (22) (7)) pp1462–1465

[116] Zhi Cai, Yuyu Shu, Xing Su, Limin Guo and Zhiming Ding, (2023) A Traffic Data Interpolation Method for IoT Sensors Based on Spatiotemporal Dependence, *Journal of Internet of Things,* Vol. 2 Issue 7,
DOI: https://doi.org/10.1016/j.iot.2022.100648

[117] Zigang Chen, Zhiquan Cheng, Wenjun Luo, Jin Ao, Yuhong Liu, Kai Sheng and Long Chen, (2023) FSMFA Efficient Task Scheduling for Cloud-Fog Multi-factor Authentication Protocol for IoT Devices, *Journal of Internet of Things*, Vol. 2 Issue 8 DOI: https://doi.org/10.101 6/j.iot.2023.100685