

## Efficient addressing schemes for internet of things

Venkatesh Thamarai Kannan, Rekha Chakravarthi

Department of Electronics and Communication Engineering, Sathyabama Institute of Science and Technology, Chennai, India

### Article Info

#### Article history:

Received Nov 9, 2020

Revised Mar 30, 2022

Accepted Apr 12, 2022

#### Keywords:

Internet of things

Internet protocol version 6

addressing

OSI protocol

Wireless sensor-network

### ABSTRACT

The internet of things (IoT) defines the connectivity of physical devices to provide the machine to machine communication. This communication is achieved through various wireless standards for sensor node connectivity. The IoT calls from the formation of various wireless sensor nodes (WSNs) in a network. The existing neighborhood discovery method had the disadvantage of time complexity to calculate the cluster distance. Our proposed method rectifies this issue and gives accurate execution time. This paper proposed mobility management system based on proxy mobile IPv6 as distributed PMIPv6 with constrained application protocol (CoAP-DPMIP) and PMIPv6 with constrained application protocol (CoAP-PMIP). It also provides the optimized transmission path to reduce the delay handover in IoT network. The PMIPv6 described the IPv6 address of mobile sensor device for efficient mobility management. The network architecture explains three protocol layers of open systems interconnection model (OSI model). The OSI layers are data link layer, network layer and transport layer. We have proposed the distance estimation algorithm for efficient data frames transmission. This paper mainly focuses the secure data transmission with minimum loss of error. The evaluation result proved that proposed technique performance with delay, energy, throughput and packet delivery ratio (PDR). Also, it measures the computational time very effectively.

*This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.*



### Corresponding Author:

Venkatesh Thamarai Kannan

Department of Electrical and Computer Engineering, Sathyabama Institute of Science and Technology

Chennai, India

Email: venkateshphd15@gmail.com

## 1. INTRODUCTION

Wireless sensor network (WSN) plays as the key entity for accessing internet of things (IoT). The more devices within IoT network, and their access to internet, have faced complexities in integration and establishing connection between those devices [1]. WSN comprised of the spatial distributed autonomous device by utilizing the sensors to the environmental conditions. Wireless sensor network has limited properties in computation power, memory, energy, and bandwidth. It is the small physical size that can be embedded in the physical environment. Mainly, the sensing devices can communicate the data wirelessly. From the wireless network system that incorporates the gateway which affords the wireless connectivity. The WSN generally contains ten to thousands of nodes, which communicate by wireless channels for the sharing of information. This sensor network is the network of multiple tiny disposable minimum power of devices are called nodes. From WSN is expected to integrate into the internet of things (IoT), also the internet performs dynamically whether joining the sensor nodes and utilize to work together and complete their tasks. IoT is the physical object network or things, which can interact with each other to share the information. But, the WSN becomes a part of the internet while analyzing and investigating the difficulties involved by this integration. Choi and Koh [2] studied and proposed the dual mobility management system depends on the

proxy mobile IPv6 (PMIPv6) as distributed PMIPv6 with constrained application protocol (CoAP-DPMIP) and PMIPv6 with constrained application protocol (CoAP-PMIP). The CoAP-DPMIP plays the role of local mobility anchor (LMA) which was disseminated to every mobile access gateways (MAG) [2]. Therefore, this system could be providing an enhanced transmission path and reduced the delay handover. The LMA, and CoAP-PMIP were utilized to deliver the network based mobility supports sensor devices. Every device is registered with IPv6 address, LMA. The data transmission was done by using LMA. The proposed schemes of PMIPv6 based CoAP was used for effective mobility management and described the address of IPv6 of mobile sensor device which are followed as hashed unconventional prefoldin RPB5 interactor (URI) of the sensor device and the prefix of MAG. Another related study [3] discussed the internet protocol version6 with minimum power of wireless and personal area network (PAN) for the IoT. It analyzed and developed for the resource constrained of internet protocol (IP) based on the systems. The number of devices was increased and the number of traffic would develop together by data. IoT would have multiple numbers of smaller devices with sensitive and they are profitable to put the essential constraint in the total system of bandwidth. The internet protocol (IP) are the communication protocols on transmission control protocol/internet protocol (TCP/IP) suite and that the normal usage of different function likes packet structure, routing, and delivering packets. However, IPv6 had the latest version of the IP melodramatically had to increase the number of addresses. The proposed method of link-layer was connected and sorts of different links. The feature key was required through the link layer and to support the IP as length indication, addressing, error checking, framing and features of broadcasting and uni-casting. The features of IPv6 low power wireless personal area network (6LoWPAN) are followed to support the 16-bit or 64-bit addressing was provided. The proposed method was increased security support from the wireless network. Therefore, this security methodologies had easy to spoof the nodes or packets and easy to eavesdrop.

Lastly, IP are utilized to modify, fine-tune, and change to enable the era of IoT. Also, the proposed method had heterogeneous features like targeting at minimum power protocol and user datagram protocol (UDP) headers, neighbor discovery and network auto-configuration, supporting the concept of fragmentation. The IoT connection framework is evaluated for their performance through assessing all the factors including mobility-energy, usage of network, execution-time, node energy, network delay and the delay by IoT-node [4]. There are some studies implemented the IoT mobility management challenges on cluster binding and updating the method based on PMIPv6 [5]. It made the better utilization of the group character on IoT and specifically extended the PMIPv6. It introduced the group identifier to maintain the group binding and reduced the signaling cost and also described the full operation flow in detail. The PMIPv6 is based on group binding update methodology had designed to optimization of binding operation and updated for the operations on mobility sessions to identify the group.

In similar to that study, analysis [6] contributed the generic techniques on mapping the pub-sub middleware to the IPv6 multicast. To decrease the network overhead, and then the subsequent of the multicast method was embedded in the concrete models as low flexible but it consists of lightweight of the implicit multicast model. Also, versatile are the costlier explicit multicast model. The estimations are displayed the proposed framework to improve the scalability. It reduced all over network traffic and achieved the best energy efficacy. Here, the bandwidth consumption had the multicast sensor which was reduced by up to 54% for the 10 subscribers and 66% for the next 20 subscribes. These obtained the benefits by the limited memory in footprint and corresponded to the extra usage of total flash memory as 4.7% also, the total random access memory (RAM) as 1.3%. Lastly, it provided the techniques based on the bath beneficial and feasibility of IoT things. In future, the encoding scheme and derivation function for the investigation of implicit model. That left the enough bits and the function or unused bits being utilized to support the dissimilar quality of services (QoS) levels. The concepts and features, evolved [7] IoT which had the technology would change daily life. It was easier to utilize and develop the needs of its users. However, discussed the simple definition for the IoT, and it gave the detail view of WSN based on the IoT. Besides, the 6LoWPAN were introduced the solutions for sensor networks by the least power to connect with the network. IoT was gathered the various domains and innovative ideas. The use case of management of constrained network and devices (COMAN) were characterized by the network management to monitor the network parameters, network status, detecting faults, maintain normal operation of a network. Such applications defined for the constrained network management as medical applications, automated metering infrastructure (AMI), environmental monitoring, and infrastructure monitoring. Here, the management protocol was used to connect the huge number of related devices by IoT and it provided better quality to the consumer then reactive the network face to change. Then, we viewed the complexity of the network from the Internet of Things that increased day today and took into account the devices that are connected to the network. Their management becomes a significant need for two-management protocol they are, sensory neuron membrane protein (SNMP) and last normal membrane protein (LNMP). This would allow the easy way of deployment and more comfortable usage for the end-user by the best quality service. The following

difficulties are identified in the existing methodologies: i) the selection of cluster is very difficult in that time of new data enclosed and ii) the distance measurement of cluster error data cannot give the execution time accurately. The small data can easily cluster and identify the error but the huge amount of data has such difficulties to cluster and detect the error to overwhelm the issues this paper proposed as: i) to cluster the big data by applying such novelties, ii) to reduce the cluster error from the selection of data by using a distance estimation algorithm, and iii) to measure the computational time as effectively.

The mobility analysis and network assessment [8] surveyed the advanced relate by the mobility and routing in the 6LoWPAN networks. Currently, the scientific and industrial community starts the multiple misconceptions around the usage of internet protocol in all the proposed nodes. The proposed techniques might be a convergence solution to link the dissimilar link layer protocols and physical layer protocols were enabled to connect the proposed devices to the network. The wireless mesh had support to consider the best-fit routing protocol for the LoWPAN. Because of the capability to self-configured and self-organized. Router-over and mesh-under techniques could be utilized to support the mesh routing on the proposed networks. From this, it specified both advantages and disadvantages. The normal routing protocols utilized on the route over techniques were adapted from the mobile ad hoc network (MANET) protocols. The design of the method that addresses the mobility requirements and simultaneous routing is crucial to attaining the IoT vision. The existing IoT mobility management system [9] offered the advanced protocol of glowbal IP for the extension of devices that were previously deployed and inherit technologies to IPv6. It permits a user to generate the network layer homogeneity and global communications over IPv6. Also, the glowbal IP resolves the deficiency of optimization from 6LoWPAN with esteem to the global communications that required from 26 to 41 bytes for the proposed of 6LoWPAN header. While the access address identifier (AAID) was required an only 5-byte header and the identification of the session was carried out by the method of AAID. Then the investigation had shown how to achieve the network-based data systems via recent domain name system (DNS) positioning, with the multicast DNS and DNS service directory. This allowed a system to define the data in a network. The devices such as model, family, web services, and features were offered to interrelate with it. Lastly, this had estimated in a multiprotocol card, and this system signifies the least delay and mapping tasks to define the global IP as an appropriate technology to be positioned. Transmit packet coding (TPC) is presented in vehicular ad-hoc network (VANET) framework to check out efficient multi-casting and reliability. The network-devices is utilized for minimizing the transmitted packets count [10].

In the scenario of cluster based WSN, the cluster heads would collect and fuse those data-packets obtained from sensor-nodes. The packets from fused data-packets were forwarded to SN-Sink node. This process aids sensor-network to do energy balance, and prolongs their life-time effectively. But still these sensor-nodes in WSN may subject to certain intrusions or disconnection of sensor signals in-between. The time taken to establish the transmission path for these data in IoT network may be longer corresponding to their location. There occurred considerable delay in handing over the data in IoT-networks. In cluster distance calculation in IoT sensor nodes, it takes prolonged time to measure this sensor nodes detection for establishing the clear transmission path for delay handover within IoT network. By using existing methods neighborhood discovery method in mobility management system in IoT sensor networks, this time complexity could not be solved. Hence it is necessary to overcome this issue and ought to aid in execution time calculation accurately. The study implemented mobility management system on the basis on Proxy mobile IPv6 as CoAP-DPMIP and CoAP-PMIP. This framework generated the optimized path for data transmission to minimize the delay handover within IoT network. The PMIPv6 elaborated IPv6 address of this mobile sensor-device for effective mobility-management. The architecture of network enumerated open systems interconnection (OSI) protocol layers. These OSI layers are data-link layer, network layer and transport layer. This mobility management operation is explored through distance estimation algorithm for transmission of data frames effectively. As a whole, the study focusses on secure transmission of data with minimum error loss in data. The outcomes of this evaluation evidenced that this proposed-framework showed better results with respect to throughput, packet delivery ratio (PDR) and delay energy. The computational time is also determined through this evaluation effectively. The results of this evaluation proved that our proposed framework in distance estimation algorithm attained lower time-consumption. The analysis in their performance that framework exhibited better throughput rate, packet delivery ratio, and energy value and lesser delay time.

The major contributions of the paper are stated: i) this proposed-framework in this study of IPv6 based hierarchical machine to machine (M2M) network using CoAP-DPMIP and CoAP-PMIP is capable to provide extensive-spacing in reaching out unique-address globally, ii) this mobility-management system acquired IP address automatically and in cluster distance calculation, without the interventions of human demands for dynamic host-configuration protocol (DHCP) servers. The remaining portion of this paper is schematized: section 2 demonstrates the conventional mechanism associated with the several clustering techniques in big data analytics by such datasets. Section 3 provides the proposed distance estimation

algorithm for measuring the distance as effectively and accurately. Section 4 exhibits the performance study of the projected mechanism and in conclusion, section 5 concludes the proposed work.

## 2. RELATED WORKS

This section describes the literature review of the clustering efficiency in big data algorithms. For the demands in IoT framework, a study [11] recommended the techniques for the analysis and extraction of networking evidence was utilized in the proposed method of 6LoWPAN. In this work, they developed the series of complementary devices that were included as facilitates and automates analysis. Thus, it allowed the investigation to focus on the task, which required the domain expertise. However, these devices are fast, reliable and produced fewer false positives. Also, it demonstrated to reconstruct the network layers of two and tree topologies. It correlated the information to extract the subset of nodes which formed the network. Moreover, it aimed to study the requirements that are essential to satisfy before reconstruction of the complete topology. In this proposed work, hundreds of devices were deployed largely and also had potential to attain better results on the selected nodes. In combination, the traffic is analyzed by techniques that used multiple-image correlation for congestion analysis to detect the particular attack patterns. In upcoming work, it is aimed to extend the device that supports the analysis of RAM dumps took from devices. It also, supported the anorectal malformation (ARM) and MSP430 cortex-based devices.

This IoT sensor framework enabled efficient connection of application devices and in their tasks coordination. These applications are employed in various fields including automation process in industries, smart home application and in health-care implementation. For these purposes, various protocols is applied in providing efficient device or mobile communication for resource-limited IoT devices [12].

Similarly in data transmission analysis [13] implemented in the semantic and unified data model by the ontology in accessing and data storage. Novel usage of IoT technology application in the real time mobile environment provided the results as: i) in data, intensive provided platform used to access the large data scales, ii) then the methodological were demonstrated the different IoT data could access ubiquitously, and iii) the usage of the proposed model of ubiquitous data accessing method in IoT (UDA-IoT) has encapsulated the unified format of resources.

Hence in overcoming these type of issues one of the study [14] implemented the novel framework depends on the RFC-5949 that is known as fast handovers for PMIPv6. Though, the mobility system for the sensor nodes depends on the mobility of network PMIPv6 was efficient. But, it reduced the packet loss by the help of the proposed method and the data packets were buffered at the nMAG which were delivered to the mobile node (MN)/mobile router (MR)/mobile host (MH). After the handoff (HO) process completion, with minimum loss or without loss, the HO signaling message was exhibited both of the proposed PMIPv6 and sensor fast proxy mobile IPv6 (SFPMPv6) mobility protocol. These are very much clear in which the proposed SFPMPv6 minimized the termination or connection interruption. Also, the packets were buffered at the new mobile access gateway (nMAG) or previous mobility access gateway (pMAG), so there is less packet loss. Finally, the proposed method of SFPMPv6 would improve the performance as reducing the packet loss to the larger extension. So, the proposed protocol reduced the signal costing and mobility cost when compared with PMIPv6 and MIPv6.

One of another implementation that aids in providing efficient and secure smart-home gateway is achieved through Raspberry Pi-hardware in IoT framework [15]. Another study presented the concept of identifier and also, proposed the effective and novel (CCHA) context aware of clustering in hierarchical Addressing for nomadic things in IoT and clustering of ubiquitous things to accomplish the robustness, and scalability. In the proposed method of CCHA, the context was integrated by hierarchical and clustering addressing for the identifier format. The experimental results are shown how the proposed method was beneficial to create dissimilar namespace and outcomes in terms of energy, throughput, and end-to-end delay into the better performance of the network. Then the comparison of proposed method, with the existing method as for better results. So, the proposed techniques of CCHA are less prone to fail with the possibility of make the right choice as CCHA in IoT and nomadic networks. In future research, it would be extended to addressing scheme and identifier format to ensure security. Likewise, the monitoring system for home security purposes, is explored through Raspberry Pi-system. Various sensors are interconnected in the model. Telegram media is utilized to transfer notification from these sensors to tool-users [16].

Various techniques evolved for implementing the electrocardiogram (ECG) wireless wearable monitoring system in the IoT platform to integrate the different applications and nodes [17]. It provided the battery life time, and maximum quality of ECG signal. The system was allowed the monitoring multi patients on the reasonably as indoor area. The ECG sensor had exhibited the low record of energy per effective number of quantized levels (EEQNL) of solution and merit with available integrates and discrete frontends. Certainly, the proposed ECG based sensor had the high performance of analog to digital converter (ADC),

and microprocessor radio combo. It provided the best performance in name of noise and power consumption than the multiple proposed systems. The other proposed remarkable system are low marginal to the sensor. It enabled a single low-cost gateway to achieve multiple sensors. The disadvantage of the proposed techniques is related to the sensors, correlation, and transducer techniques to which improves strength and reliability. The protocol analysis [18] elucidated the challenges of relating the protocol of TCP and IP to the IoT networks. Which ascend from the transport layer and network layer. Also, we discussed how the application layer protocols such as CoAP delivered the own solutions to desire the functionalities of lower layer failed to support. The disparity was made on the extra evident that compared to the recent IoT stack. To desire the architecture from the application of view point, first developed the TCP/IP protocol stack via wired connectivity. The protocol stack was evolved using the IP specification and fundamental assumption to design the architecture. The proposed techniques of architecture changed to move the representational state transfer (REST) linked components and into the eventually arrived with the core network layer. It had the more efficacies to the application layer solutions. A novel IoT stack would use in the information-centric network (ICN) that was implemented and designed the required functionalities for more efficacy of the network. The lightweight mutual-authentication protocol is applied on the basis of CoAP-constrained application-protocol, employed for IoT-devices for secure level of data-transmission [19].

For this secure data transmission [20] developed an algorithm on ECG signal of classification, implementation, and analysis of embedded platform in IoT. This proposed algorithm was suitable for the proposal of an ECG diagnosis device that had the maximum amount of time monitoring on the patient. The usage of discrete wavelet transform (DWT) for the analysis of ECG and also used the classifier of support vector machine (SVM). The application of implementation was read by the ECG signal and analysis flow as heartbeat detection, filtering, heartbeat segmentation, feature extraction, and classification was performed. This analyzed the overall framework of the ECG signal to select the optimal, computation demand, and configurations from the design space exploration (DSE). This DSE was performed all combination of DWT coefficients. It reduced the exploration time but calculated at once from the database of heartbeat detection. The main goal of the classifier is to produce the maximized computational cost and maximized accuracy. This implementation was achieved by the embedded with the IoT platform. It is convert the code and designed as the chip like low power consumption, and small core products. Therefore, the better classifier had achieved the accuracy as 98.9% and then the execution time and total average time for the optimal configurations best of the output were detected. In the real-time process, the feature vector size on 18 and support vectors of 2493.

Similarly another study [21] presented to demonstrate the cloud and IoT infrastructure could simply be organized to utilize the one lab federation of test beds. The IoT context was developed by the novel hardware device's novel communication protocols and the novel method was used to analyze and collect the data. The challenges of IoT to address with a federation of test beds which offered to access the virtual machines, FIT cloud, virtual wall, wired servers, and cloud with Planet Lab. From the federation of a test, beds were provided to the FIT wireless, W-I Lab. Wireless test beds. Next, the FIT IoT Lab was very large with physical devices to deploy the FIT equipex and then the novel IoT technologies rely on the dissimilar hardware devices when monitor by the energy consumption of the same time. One lab federation of the test beds provided to the users on a single point to access the web portal. These experimentations could automate by utilizing the scripts and to provide the different setup as the service. This extension leads to enable the results and to create the applications on the top of service. The multiple applications could be detected that the robots or humans present in the room mean proposed nodes of FIT IoT Lab were deployed. It would be used for the light-sensing and temperature in the context of smart building applications.

This type of sensor network communication [22] introduced the standard and background to supports the IPv6 based hierarchical machine-to-machine communications. The challenges were investigated to the enormous IPv6 access, based on the hierarchical machine to a machine communication network by the different IoT applications. The main benefits of the proposed approach of IPv6 based hierarchical M2M network are: i) able to afford the extensive spacing of globally reached a unique address, ii) automatically acquired the IP address without the human needs for the DHCP servers, and iii) it is not required by the low energy consumption and low cost on the M2M devices. In the end, the systematic distributed access control framework was used for improved the network, achieved fairness, and deal with the dynamic network. Also, the potential algorithms and optimal control was developed for the proposed control framework. The results of the evaluation were exhibited the essential performance in terms of application differentiation and utility maximization.

The IoT devices infrastructure [23] explicated the present novel techniques of frequently changed IPv6 address to add the extra layer on the security purpose in the IoT. A protocol was utilized in the wireless sensors that founded as smart meters and home automation systems. The proposed techniques of 6LoWPAN were allowed the IoT to extend of WSN. The field of the proposed system was included the security against fragmentation attacks and the encryption congestion on the IPsec. To launch the malicious fragment, that is

increased the availability of moving target IPv6 defense (MT6D) tunnels congestion by integrity and confidentiality.

The network framework [24] For healthcare system environments this paper expounded a moderate IoT depends on the 6LoWPAN. To recover the effectiveness, costs, and overall quality in healthcare, proposed IoT based architecture was used. To start from the gathered bio-signals that are integrated with the medical sensor nodes of 6LoWPAN by analog based front-end devices. Lastly, the contextual data and present health were saved in a cloud server for the end-users. In the network, it also included the tunneling gateway based on packets routing from the sensor nodes to the. Thus, it also examined the power consumption and architecture for dissimilar scenarios. Therefore, verify the proposed architecture was suitable for the applications by the streaming data in health protection environments. In the coming work, the additional layer would be added to the proposed technique stack to improve security and efficacy. Also, the data compression and data filtering algorithms would apply on the node level to protect the battery power and network bandwidth.

The mapping phenomena [25] expounded a mapping among the every technology of native addressing and IPv6 address to follow the group of rules. Exactly, this presented a technology on IPv6 addressing proxy in that draws every device to the dissimilar sub networks. It creates the prefix addresses of IPv6 and afforded by the ISP for every user, building, and home. The IPv6 address provides a general addressing scheme depends on IPv6 to overall devices, with regards to device technology. Thus, this deals with a homogeneous and scalable solution to interrelate by devices that do not support the IPv6 addressing. The IPv6 address proxy had developed in multi-protocol card and calculated successfully in their interoperability, scalability, and performance by the protocol was created over IPv6. The benefits of mapping legacy-addressing spaces to IPv6 as, mapping to IPv6 permits the hiding of the particular aspects of the technologies that were utilized with the sensor, to offer a structure, which works on independent of the technology. The features of IoT, their concepts, protection mechanism and IoT applications with authorized microbial electrolysis cells (MEC) drives globally [26]. Likewise, IoT analysis [27] illustrated an innovative internet stack by the group of adaptation layers starting from the non-internet protocol to the IPv6 depends on the network layer. To work the different access for the services and applications.

### 3. PROPOSED WORK

This section illuminates the proposed distance estimation algorithm for measuring the distance as effectively and accurately. There are various sensor nodes are presented in network, and some of the nodes have an identifier such as media access control (MAC) and some of the nodes do not have the identifier. In network, to achieve the perfect data transmission, every node in network should have a unique identifier. So, the distributed address allocation schemes are ensured with continuous running of self-adaptive network. An addressing scheme is used for creating communication between the network devices. Using the addressing scheme, information is forwarded from one location to another. Figure 1 defines the representation of network architecture with various protocols.

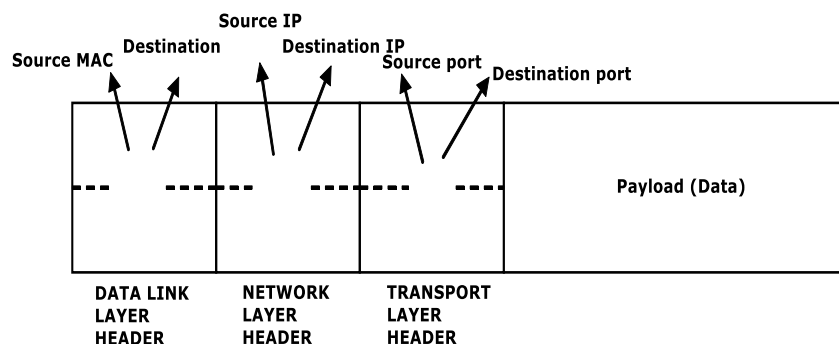


Figure 1. Network architecture

#### 3.1. Data link layer (layer 2)

In OSI layer, the data link layer transmits the message or data frames from the network layer. It sends the data frames between the two devices without any traffic and error using the physical layer, so it is called an error-free delivery layer. It also includes error detection information as data packaging from the

network layer. In receiver section the data link layer received the input data frame and it sends it to the next network layer. Based on received data frames, this layer generates the error based information. After receiving the overall data frames, these frames are compared to its error detection value with input of data frames. If the frames are matched then they received correctly. The error control protocol is used to provide the acknowledgment to the sender that is positive or negative. The positive acknowledgment defines the successful frame received without any errors. And negative acknowledgment defines the error in data frames.

The data link layer is described with MAC. MAC uses the source machine for sending the Ethernet frame to the device which is going to involve the 'routing' process of the IP data frame. A 6-byte with 48 bit field called as MAC address and it is also represented by a 6-field of hexadecimal number that is 89-A1-32-2B-C3-85. Two bytes long in each field. Each incoming and out coming data frame of the networking device has the connection with link interface, and each interface had a unique MAC address. Generally, there are no two interfaces shares the same MAC addresses. A header of the data link-layer contains both a source interface and a destination interface of MAC addresses.

### 3.2. Network layer (layer 3) addressing

The data link layer works as the service provider for the network layer and it provides end-to-end communication. This layer transfers the network packets from source IP to destination IP through various networks. A 4-byte with 32-bit field called IP address and that is represented by a 4-field dot-separated number that is represented by 192.2.32.84. Each field have one byte long in address. Each data in a network must have an IP address and it should to be identified the data frame communication. A network layer header contains both source node IP addresses and destination node IP addresses. The length of the network packet must be included with network layer header.

### 3.3. Transport layer (layer 4)

The transport layer also develops the end to end communication and the services are provided by a transport protocol. In the header, each data frame contains the source and destination port address. In this layer, A 2-byte with 16-bit field called as port number, which is represented by 4,892. In the communication the port number identifies the two end hosts. Any host can run on various network applications in same time and every application requires to identifying by another host communication to a targeted application.

The destination port number defines the destination server based on their requested service. It mainly depends on the delivery. The source port number is randomly generated by the sending device for identifying the conversation between the devices. Therefore the identifiers are used to uniquely identify an object. For a representation of object, the identifiers must be uniqueness.

In the proposed algorithm, first, initiate the neighbor discovery process. If a source sends the data, then set the clock time. Second, initiate the route discovery procedure. Select the intermediate nodes based on the clustering distance. Then source selects a route (RTS) to destination from its cache. If the route does not have the destination, then again starts the route discovery procedure. If the route contains the nodes belongs to the primary suspect list, the cluster near nodes are switched ON in the listening node. Then calculate particle swarm optimization (PSO) metrics for each node and each path to make the routing table. At the end, it sends the data packet with a secure key.

### 3.4. Internet protocol version 6 addressing (IPv6)

The IPv6 protocol can support the large number of connected devices that is expected to be part of the IoT. It potentially supports  $2^{128}$  of unique IP addresses. It can provide unique addresses to each node. The intelligent resolution system used in IoT-A and it allows avoiding subtleties such as meaningful real-world information's within the IP address. In IPv6, the prefix form contains identical for all the hosts in network forms. The suffix part, uniquely identified the tag itself, this identification should be based on its built-in identification number.

This paper proposed DNS name auto configuration (DNSNA) method that auto-configures the DNS names of IoT devices for IoT device sand manages the DNS naming. In the IoT network, the users easily analyze the IoT devices of DNS names based on DNSNA for remote controlling and monitoring. For the resolution of IoT devices and DNS name generation, proposed DNS name auto configuration method, such as home network and road network. For IoT home devices it provides an efficient DNS name services. Since auto configured DNS names contains the device model of the categories, home residents can easily identifies the DNS names devices.

The node addressing scheme had high efficient if it reduces the overhead header that is identified with every data packet. This addressing scheme works better if the absence of collisions at allocation time and it is also works with the collision-free network. To minimize the overhead associated allocation scheme address itself and it should be distributed and not centralized. In network size increasing, the addressing scheme should scale well.

Our proposed model enhanced with IPv6 Addressing scheme in terms of hierarchical architecture to identify the device quickly and respond to the device for further actions. And also it can be enhanced by providing privacy for users by hiding their address by converting it into hash values. Identification or addressing schemes: i) Clock skew addressing (CLOSA) and ii) N-dimensional addressing.

#### Algorithm-1: Distance estimation algorithm

*Protocol Functional Steps:*

Step 1: Begin REQ to the network, initiate the process of Neighbor Discovery;

Step 2: if (the Source sends the data) then

Step 3:  $t_s = \text{set clk time (node (Source))}$  where CLK-Clock

Step 4: Initiate the Route Discovery Procedure

Step 5: Select the intermediate nodes based on the Clustering Distance

$(\text{Int\_Node}_i, \text{Int\_Node}_j) < \text{Mins (Distance)}$ ;

Calculate Distance based on RERR msg.,

$$\text{Distance (n1, n2)} = \sqrt{(X\_Pos2 - X\_Pos1)^2 + (Y\_Pos2 - Y\_Pos1)^2}$$

Where n1= (X\_Pos1, Y\_Pos1) and n2=(X\_Pos2, Y\_Pos2)

Step 6: From the cache source selects a route (RTS) to Destination;

Step 7: if (absence of route to Destination in its cache)

Go to Step 4;

Step 8: if (route defines the nodes belongs to the primary suspect list)

Cluster Head nodes near to the indicated nodes are switched ON in the promiscuous listening mode;

Step 9: if (Current source node clock time  $t_s$ )

mod check time == 0)

{  
     Send Routing Table;  
     Calculate PSO metrics of each node;  
     Calculate overall PSO metrics of each path;  
     Make entry in the routing table;  
     Transmit the data packet with Secure key;  
     Go to Step 6;  
 }

Step 10: if (receives suspect list || malicious list)

{  
     If (receives suspect list)  
     {  
         Update the primary suspect list  
     }  
     If (receives malicious information)  
     {  
         Update malicious list and primary suspect list;  
     }  
     If (end of data)  
     {  
         Do-nothing;  
     }  
     Else  
         Go to Step 6;  
     }  
     If (receives RERR)  
     {  
         Go to Step 6;  
     }  
 }

Step 11: End if;

### 3.5. Clock skew addressing (CLOSA)

The clock skew addressing (CLOSA) is a new addressing scheme and it assigns unique IPv6 address to every node in the IoT network. The CLOSA establishes the uniqueness for each node of skew extracting and it converts the IPv6 address. It eliminates the requirements of duplicate address detection (DAD) and does not requires the allocation tables.

Figure 2 defines the tree based addressing and stochastic addressing in IoT. Each node has the transmission path from source to destination. It finds the minimum path for transmission and the data packets are transferred. The tree based addressing contains the certain network topologies and it defined top of the tree depth and run out of addresses in branches. The stochastic addressing scheme assigns the network addresses randomly and avoiding topology constrains on network deployments. This addressing scheme assigns the short addresses randomly to new devices. When the new device is generates, it gets the random address from its parent.



**3.6. N-dimensional addressing**

It utilizes the available address space without losing of address. To reduce the loss we have proposed the n-dimensional addressing. For assigning the router nodes, this method involves a space partitioning approach. It mainly solves the memory requirements problem and address wastage problem. For example, the 16-bit address space contains two subspaces. The first 8 bits are assigned for x-axis and second unassigned bits for the y-axis. It is called a single address space (x, y). The x-axis defines the router node of the tree-based routing network and the y-axis defines the corresponding value to the sensor node, which is connected to the router in the x-axis. Figure 3 defines the representation of N-dimensional addressing with various nodes.

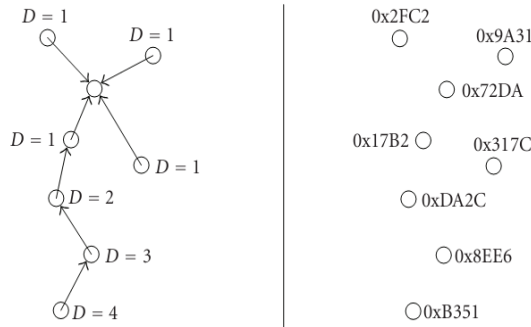


Figure 2. Tree-based addressing/stochastic addressing

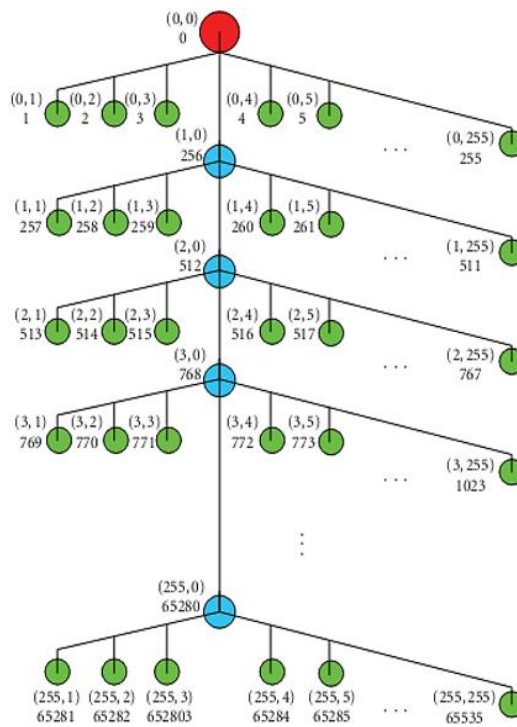


Figure 3. Representation of N-dimensional addressing

**4. PERFORMANCE ANALYSIS**

This section exhibits the performance study of the projected mechanism. The packet delivery ratio and end-to-end delay, throughput, and energy metrics are also assessed for a varying number of nodes deliberated are exhibited following the simulation time with the assistance of the NS-2 simulator shown in Table 1. The Figure 4 defines the output of the nam file. The source determines the shortest path of the neighborhood and sends the data frame. The evaluation result proves the data transmission with the minimum rate of error, delay, energy, throughput and packet delivery ratio (PDR).

Table 1. Simulation parameters

Simulation Parameter	Value
Version-NS2	ns-allinone-2.35
Protocol	AFFOADV
Area OG Coverage	1000X1000 m
Simulation Time	200
Type of Antenna	Omni Antenna
Energy Mode	Energy Mode(true)
Initial energy	10000mjoules
No of Nodes	150
Length of Queue	64
Data Rate	Variable
Type of Interface	Wireless Physical Interface
Radio Range for Node	~250 m

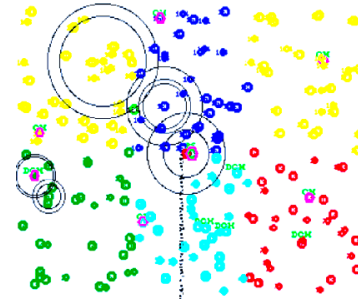


Figure 4. Representation of nam file

#### 4.1. Packet delivery ratio (PDR)

The proportion acquired between overall numbers of data packets and it is efficaciously disseminated to a specific destination following the overall number of packets and transmitted from the source node accounts for PDR. The Figure 5 represents the numerical variations in PDR values are obtained for a particularly simulated environment with various simulation times. The PDR value increased based on simulation time. At the end the ratio of packet delivery attained the value of simulation time.

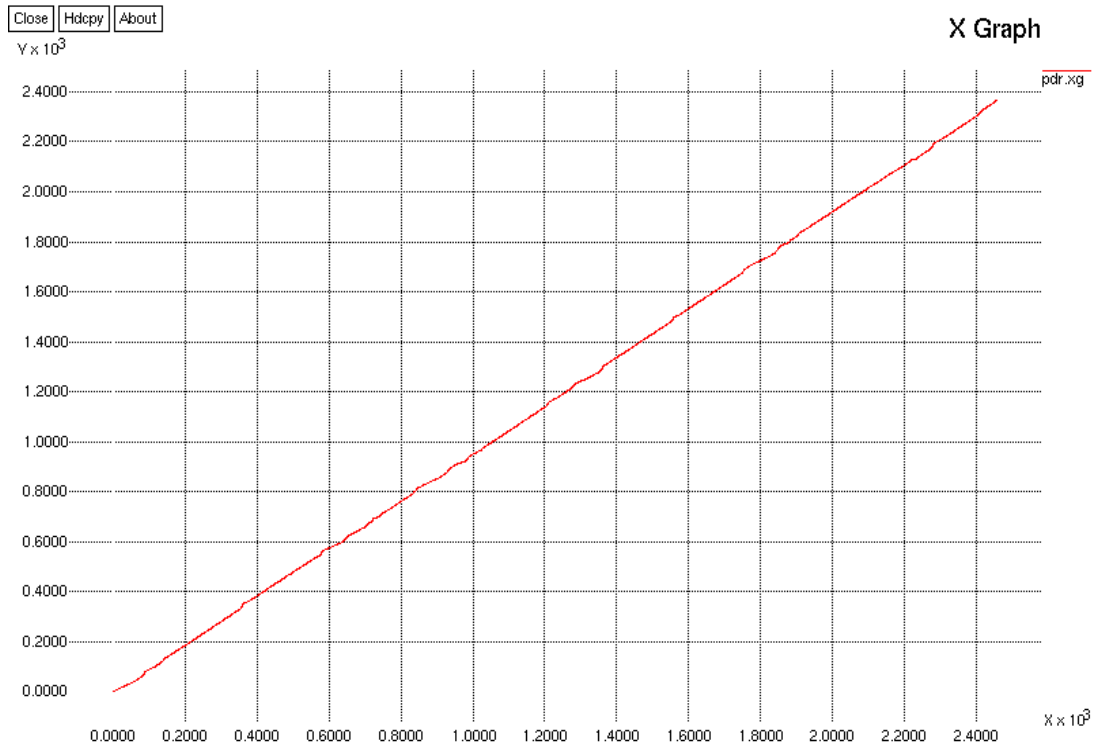


Figure 5. Representation of packet delivery ratio (PDR)

#### 4.2. Throughput

For network, the throughput is obtained as the proportion of the overall number of packets disseminated to the destination within a confined number of time. Figure 6 defines the throughput representation for varying amount of simulation time. The throughput has the same value from 2.0000 to 8.0000 simulation time. Then, the value of throughput increased and decreased based on simulation time.

$$Throughput = \frac{\text{Number of data packets sent (bits)}}{\text{time (secs)}}$$

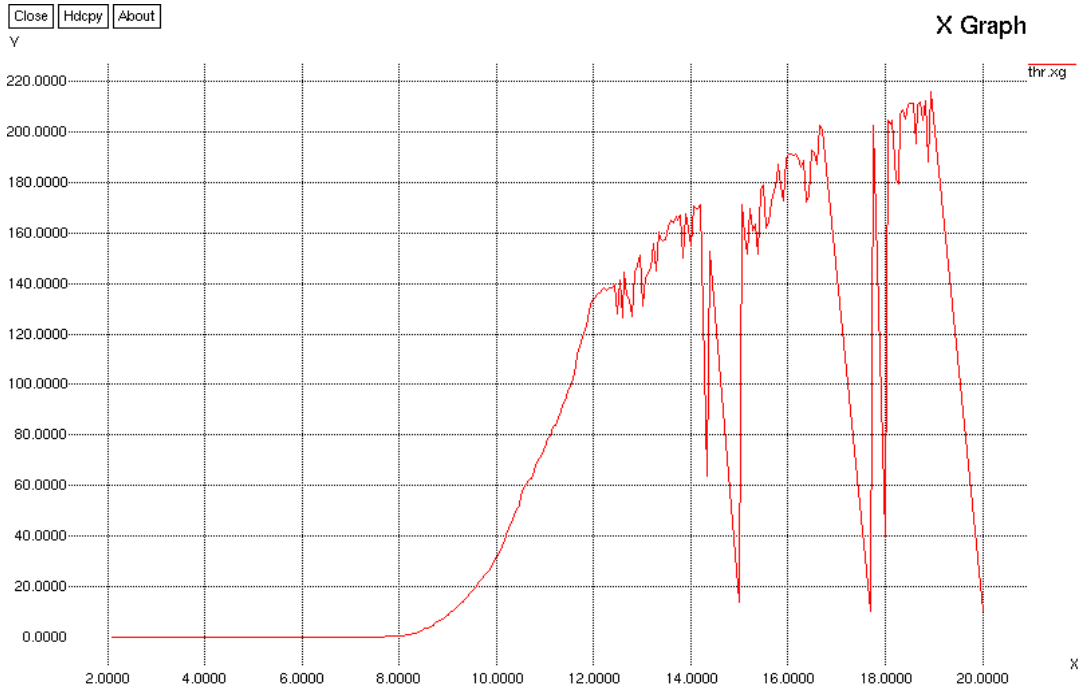


Figure 6. Representation of throughput

### 4.3. Delay analysis

End-to-end delay is contained as an impact of overall time obligated for commencing cluster realization and trailing information dissemination. The Figure 7 represents the variations of end-to-end delay concerning the simulation period. The delay analysis increased in the simulation time of 1.40000. Energy: Each sensor node has the initial energy  $E_0$  and n number of targets. Every cluster has same energy consumption. The Figure 8 represents the energy consumption with various simulation periods. The energy will increase if the simulation time has minimum value. The maximum energy value is 49.5237.

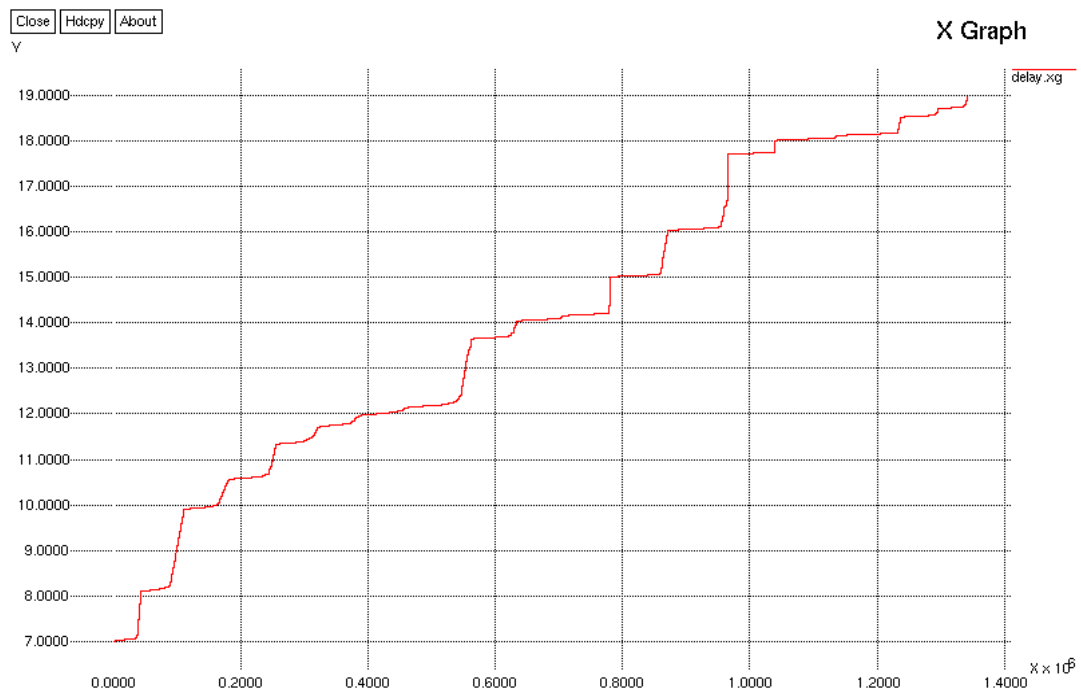


Figure 7. Representation of delay

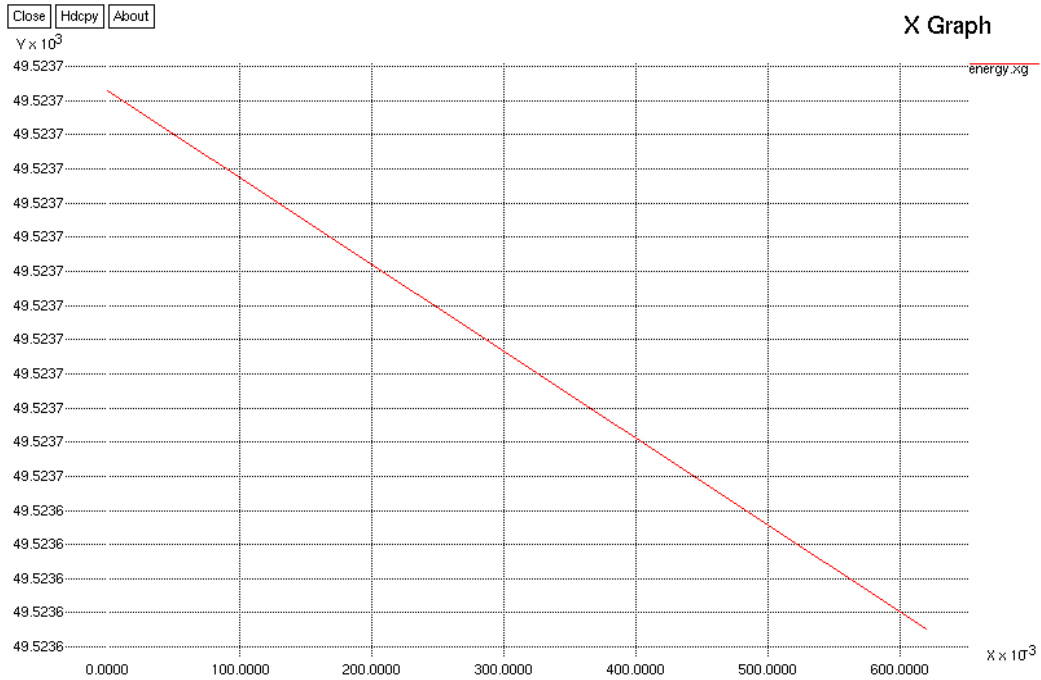


Figure 8. Representation of energy

**4.4. Comparison analysis**

The performance of the framework is assessed through this comparison analysis section. The performance of this framework is analyzed by using various parameters such as hand over delay factor, data packet loss value, throughput value, end to end delay value and the energy consumption rate. In this Figure 9, the handover delay time of data packets is determined for existing methods using PMIPv6 and PB-PMIPv6. This handover delay time is calculated for proposed distance estimation algorithm framework. It is depicted from the results that proposed-framework exhibited lesser handover delay time of data-packets within IoT network. It seems that this proposed-framework possess lesser delay time showing the efficiency of framework, reducing the time complexity. Figure 10 enumerated the comparison analysis of data packet loss values of all existing protocol models with that of proposed-framework. The data packet loss seems to have lesser value for CoAP-DPMIP and CoAP-PMIP mobility management system in comparison to other existing techniques. The data-packet loss ratio value is higher for other systems using PMIPv6 and PB-PMIPv6 protocols. From this data evidence, it is clearly showed the efficiency of proposed-framework, exhibiting less data loss while in data transmission in IoT sensor data transmission.

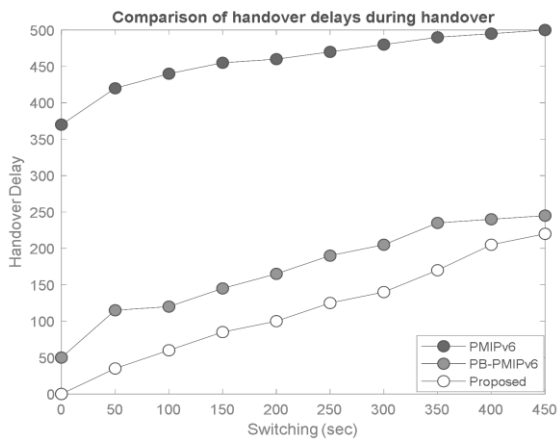


Figure 9. Handover delay time comparison analysis of proposed framework with existing methods

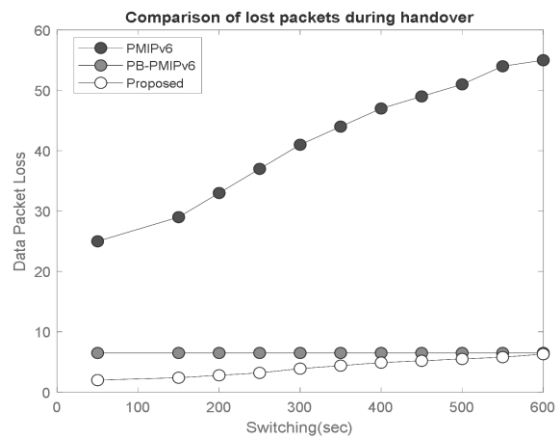


Figure 10. Data packet loss comparison analysis of proposed framework with existing methods

Figure 11 represents the comparison results of throughput value between existing methods and proposed-framework. From the figure it enumerated that proposed-framework exhibited higher throughput value in comparison with other existing systems using PMIPv6 and PB-PMIPv6. This has clearly depicted about the framework efficiency in terms of throughput parameter.

Figure 12 described about the comparison results of end to end delay time of proposed-framework with existing mobility management system using PMIPv6 and PB-PMIPv6. From this above analysis, the end to end data delivery delay time of existing methods is made comparison with proposed-framework. From the outcomes of the results, it is depicted that this end to end data packets delivery delay time is lesser in compared to other mobility management-system using PMIPv6 and PB-PMIPv6. This has clearly described about the efficiency of proposed-framework to transmit the data packets rapidly with reduced data loss.

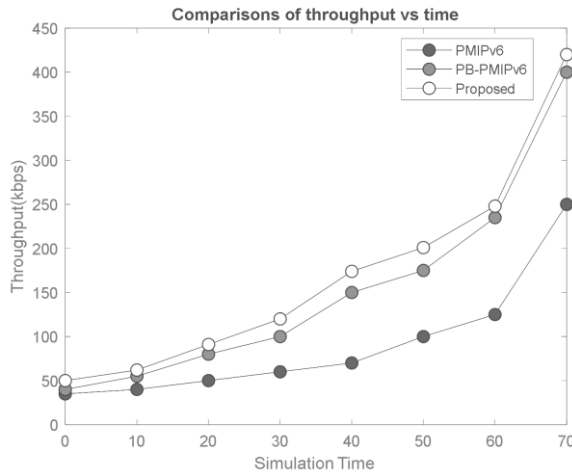


Figure 11. Throughput comparison analysis of proposed framework with existing methods

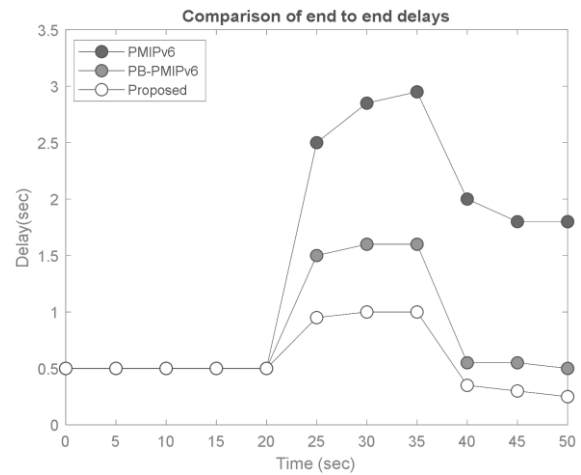


Figure 12. Performance analysis of proposed framework with existing methods in delay time parameter

Figure 13 explains about comparison results of energy consumption value of existing methods and proposed-framework. The energy consumption value of proposed-framework is lesser in comparison with other existing mobility management system using PMIPv6 and PB-PMIPv6. The proposed-framework utilizes lesser energy consumption in comparison with other existing cluster distance measurement algorithms for mobility management system using PMIPv6 and PB-PMIPv6. This shows the higher efficiency capacity of proposed model using CoAP-DPMIP and CoAP-PMIP.

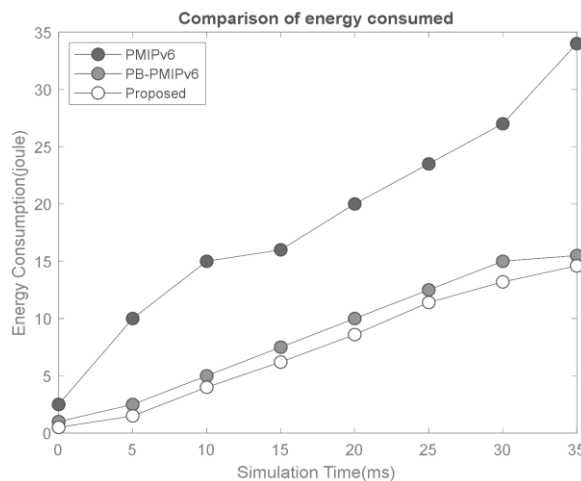


Figure 13. Performance analysis of proposed framework with existing methods in energy consumption parameter

## 5. CONCLUSION

IoT had the large number of devices and it increases the traffic together with data. To overcome this problem, this paper explained unique identifiers with the various addressing schemes for communication devices, and then it converts into IPv6 unique address. It also reduces the wastage problem. Our proposed scheme does not require duplicate address detection with allocation tables and no additional memory storage for routing. It gives the effective distance measurement of the cluster. In the evaluation result, we proved our algorithm achieved with minimum time consumption. In performance analysis, we have proved energy, delay, throughput and packet delivery ratio (PDR). The future work will be applying the address schemes in the ZigBee sensor network and should compute this algorithm with the ZigBee sensor network.





## REFERENCES

- [1] M. U. H. Al Rasyid, M. H. Mubarrok, and J. A. Nur Hasim, "Implementation of environmental monitoring based on KAA IoT platform," *Bulletin of Electrical Engineering and Informatics (BEEI)*, vol. 9, no. 6, pp. 2578–2587, Dec. 2020, doi: 10.11591/eei.v9i6.2578.
- [2] S.-I. Choi and S.-J. Koh, "Use of proxy mobile IPv6 for mobility management in CoAP-based internet-of-things networks," *IEEE Communications Letters*, vol. 20, no. 11, pp. 2284–2287, Nov. 2016, doi: 10.1109/LCOMM.2016.2601318.
- [3] C. L. Devasena, "IPv6 low power wireless personal area network (6LoWPAN) for networking internet of things (IoT)-analyzing its suitability for IoT," *Indian Journal of Science and Technology*, vol. 9, no. 30, Aug. 2016, doi: 10.17485/ijst/2016/v9i30/98730.
- [4] T. Alam, "Performance evaluation of blockchains in the internet of things," *Computer Science and Information Technologies*, vol. 1, no. 3, pp. 93–97, Nov. 2020, doi: 10.11591/csit.v1i3.p93-97.
- [5] J. Guan, I. You, C. Xu, and H. Zhang, "The PMIPv6-based group binding update for IoT devices," *Mobile Information Systems*, vol. 2016, pp. 1–8, 2016, doi: 10.1155/2016/7853219.
- [6] S. Akkermans, R. Bachiller, N. Matthys, W. Joosen, D. Hughes, and M. Vucinic, "Towards efficient publish-subscribe middleware in the IoT with IPv6 multicast," in *2016 IEEE International Conference on Communications (ICC)*, May 2016, pp. 1–6, doi: 10.1109/ICC.2016.7511254.
- [7] N. Benamar, A. Jara, L. Ladid, and D. El Ouadghiri, "Challenges of the internet of things: IPv6 and network management," in *2014 Eighth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, Jul. 2014, pp. 328–333, doi: 10.1109/IMIS.2014.43.
- [8] L. M. L. Oliveira, A. F. de Sousa, and J. J. P. C. Rodrigues, "Routing and mobility approaches in IPv6 over LoWPAN mesh networks," *International Journal of Communication Systems*, vol. 24, no. 11, pp. 1445–1466, Nov. 2011, doi: 10.1002/dac.1228.
- [9] A. J. Jara, M. A. Zamora, and A. Skarmeta, "Glowbal IP: an adaptive and transparent IPv6 integration in the internet of things," *Mobile Information Systems*, vol. 8, no. 3, pp. 177–197, 2012, doi: 10.1155/2012/819250.
- [10] O. A. Hammood *et al.*, "An effective transmit packet coding with trust-based relay nodes in VANETs," *Bulletin of Electrical Engineering and Informatics (BEEI)*, vol. 9, no. 2, pp. 685–697, Apr. 2020, doi: 10.11591/eei.v9i2.1653.
- [11] V. Kumar, G. Oikonomou, T. Tryfonas, D. Page, and I. Phillips, "Digital investigations for IPv6-based wireless sensor networks," *Digital Investigation*, vol. 11, pp. S66–S75, Aug. 2014, doi: 10.1016/j.diin.2014.05.005.
- [12] H. G. Hamid and Z. T. Alisa, "A survey on IoT application layer protocols," *Indonesian Journal of Electrical Engineering and Computer Science (IJECCS)*, vol. 21, no. 3, pp. 1663–1672, Mar. 2021, doi: 10.11591/ijeecs.v21.i3.pp1663-1672.
- [13] B. Xu, L. Da Xu, H. Cai, C. Xie, J. Hu, and F. Bu, "Ubiquitous data accessing method in iot-based information system for emergency medical services," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 2, pp. 1578–1586, May 2014, doi: 10.1109/TII.2014.2306382.
- [14] R. A. Khan and A. H. Mir, "Sensor fast proxy mobile IPv6 (SFPMPv6)-A framework for mobility supported IP-WSN for improving QoS and building IoT," in *2014 International Conference on Communication and Signal Processing*, Apr. 2014, pp. 1593–1598, doi: 10.1109/ICCSP.2014.6950117.
- [15] R. Prasad, P. N. Mahalle, and N. R. Prasad, "Novel context-aware clustering with hierarchical addressing (CCHA) for the internet of things (IoT)," in *Fifth International Conference on Advances in Recent Technologies in Communication and Computing (ARTCom 2013)*, 2013, pp. 267–274, doi: 10.1049/cp.2013.2246.
- [16] I. G. M. N. Desnanjaya and I. N. A. Arsana, "Home security monitoring system with IoT-based Raspberry Pi," *Indonesian Journal of Electrical Engineering and Computer Science (IJECCS)*, vol. 22, no. 3, pp. 1295–1302, Jun. 2021, doi: 10.11591/ijeecs.v22.i3.pp1295-1302.
- [17] E. Spano, S. Di Pascoli, and G. Iannaccone, "Low-power wearable ECG monitoring system for multiple-patient remote monitoring," *IEEE Sensors Journal*, vol. 16, no. 13, pp. 5452–5462, Jul. 2016, doi: 10.1109/JSEN.2016.2564995.
- [18] W. Shang, Y. Yu, R. Droms, and L. Zhang, "Challenges in IoT networking via TCP/IP architecture," Technical Report NDN-0038. NDN Project, 2016.
- [19] A. Ayoub, R. Najat, and A. Jaafar, "A lightweight secure CoAP for IoT-cloud paradigm using Elliptic-curve cryptography," *Indonesian Journal of Electrical Engineering and Computer Science (IJECCS)*, vol. 20, no. 3, pp. 1460–1470, Dec. 2020, doi: 10.11591/ijeecs.v20.i3.pp1460-1470.
- [20] D. Azariadi, V. Tsoutsouras, S. Xydis, and D. Soudris, "ECG signal analysis and arrhythmia detection on IoT wearable medical devices," in *2016 5th International Conference on Modern Circuits and Systems Technologies (MOCAST)*, May 2016, pp. 1–4, doi: 10.1109/MOCAST.2016.7495143.
- [21] L. Baron *et al.*, "OneLab: On-demand deployment of IoT over IPv6," in *IEEE Infocom 2016-International Conference on Computer Communications*, 2016, pp. 1–3.
- [22] Y. Li, K. K. Chai, Y. Chen, and J. Loo, "Distributed access control framework for IPv6-based hierarchical internet of things," *IEEE Wireless Communications*, vol. 23, no. 5, pp. 17–23, Oct. 2016, doi: 10.1109/MWC.2016.7721737.
- [23] M. Sherburne, R. Marchany, and J. Tront, "Implementing moving target IPv6 defense to secure 6LoWPAN in the internet of things and smart grid," in *Proceedings of the 9th Annual Cyber and Information Security Research Conference on-CISR '14*, 2014, pp. 37–40, doi: 10.1145/2602087.2602107.
- [24] T. N. Gia, N. K. Thanigaivelan, A.-M. Rahmani, T. Westerlund, P. Liljeberg, and H. Tenhunen, "Customizing 6LoWPAN networks towards internet-of-things based ubiquitous healthcare systems," in *2014 NORCHIP*, Oct. 2014, pp. 1–6, doi: 10.1109/NORCHIP.2014.7004716.





- [25] A. Jara, P. Moreno-Sanchez, A. Skarmeta, S. Varakliotis, and P. Kirstein, "IPv6 addressing proxy: mapping native addressing from legacy technologies and devices to the internet of things (IPv6)," *Sensors*, vol. 13, no. 5, pp. 6687–6712, May 2013, doi: 10.3390/s130506687.
- [26] A. Rahman, G. Wu, and A. M. Liton, "Mobile edge computing for internet of things (IoT): security and privacy issues," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 18, no. 3, pp. 1486–1493, Jun. 2020, doi: 10.11591/ijeecs.v18.i3.pp1486-1493.
- [27] A. J. Jara, S. Varakliotis, A. F. Skarmeta, and P. Kirstein, "Extending the internet of things to the future internet through IPv6 support," *Mobile Information Systems*, vol. 10, no. 1, pp. 3–17, 2014, doi: 10.1155/2014/831974.

## BIOGRAPHIES OF AUTHORS



**Venkatesh Thamarai Kannan**     has received the Master's degree in Digital Communication and Networking from Kalasalingam University, Srivilliputhur, India in 2011. Currently, he is a Ph.D. student in the Department of Electronics and Communication Engineering, Sathyabama Institute of Science and Technology, Chennai, India and he is working as an Assistant Professor (Sr.G) in KPR Institute of Engineering and Technology, Coimbatore, Tamilnadu, India. His research interests fall in the area of Internet of things, networking and Wireless sensor networks. He has published more than 10 papers in National and International Journals/Conferences. He is a Life time member of IE(I) and ISTE. He can be contacted at email: [venkateshphd15@gmail.com](mailto:venkateshphd15@gmail.com).



**Rekha Chakravarthi**     has graduated from Madras University in 2001 with Bachelor's Degree in Electronics and Communication Engineering. She has received her M.E degree in Applied Electronics Engineering from Sathyabama Institute of Science and Technology, Chennai in 2004. She has more than 17 years of teaching experience. Presently she is working as an Associate Professor in the department of Electronics and Telecommunication Engineering, Sathyabama Institute of Science and Technology, Chennai. Her areas of interest include Wireless Sensor Networks, Mobile networks and High Performance Networks. She has published more than 30 papers in National and International Journals/Conferences. She can be contacted at email: [rekha\\_2705@yahoo.co.in](mailto:rekha_2705@yahoo.co.in).