Enhancing Traffic Routing Inside a Network through IoT Technology & Network Clustering by Selecting Smart Leader Nodes

Radwan S.Abujassar

Department Information Technology and Computing,
Arab Open University Kuwait,Alardiya Industrial, Kuwait

Abstract. IoT networking uses real items as stationary or mobile nodes. Mobile nodes complicate networking. Internet of Things (IoT) networks have a lot of control overhead messages because devices are mobile. These signals are generated by the constant flow of control data as such device identity, geographical positioning, node mobility, device configuration, and others. Network clustering is a popular overhead communication management method. Many cluster-based routing methods have been developed to address system restrictions. Node clustering based on the Internet of Things (IoT) protocol, may be used to cluster all network nodes according to predefined criteria. Each cluster will have a Smart Designated Node. SDN cluster management is efficient. Many intelligent nodes remain in the network. The network design spreads these signals. This paper presents an intelligent and responsive routing approach for clustered nodes in IoT networks. An existing method builds a new sub-area clustered topology. The Nodes Clustering Based on the Internet of Things (NCIoT) method improves message transmission between any two nodes. This will facilitate the secure and reliable interchange of healthcare data between professionals and patients. NCIoT is a system that organizes nodes in the Internet of Things (IoT) by grouping them together based on their proximity. It also picks SDN routes for these nodes. This approach involves selecting one option from a range of choices and preparing for likely outcomes problem addressing limitations on activities is a primary focus during the review process. Predictive inquiry employs the process of analyzing data to forecast and anticipate future events. This document provides an explanation of compact units. The Predictive Inquiry Small Packets (PISP) improved its backup system and partnered with SDN to establish a routing information table for each intelligent node, resulting in higher routing performance. Both principal and secondary roads are available for use. The simulation findings indicate that NCIoT algorithms outperform CBR protocols. Enhancements lead to a substantial 78% boost in network performance. In addition, the end-to-end latency dropped by 12.5%. The PISP methodology produces 5.9% more inquiry packets compared to alternative approaches. The algorithms are constructed and evaluated against academic ones.

Keywords: Optimized Link State Routing Protocol (OLSR) ,Internet of Things (IoT)* , Smart designated node (SDN)* , Predictive Inquiry Small Packets (PISP), Nodes Clustering-Based on IoT (NCIoT)

1 Introduction

This section will elucidate the conceptualization of the Internet of Things (IoT) and its consequentiality within the framework of smart cities. The phrase "IoT," short for the Internet of Things, refers to a network consisting of interconnected items, cars, and appliances that interact and share data over the Internet. In the context of smart cities, the Internet of Things (IoT) plays a crucial role in the efficient management of resources, enhancing the quality of life for residents, and promoting sustainability. The Internet of Things (IoT) allows for the acquisition, dissemination, and examination of data by various devices, therefore improving the automation and enhancement of several urban services, such as transportation, energy management, waste management, and public safety. This section will examine the significance and ramifications of the Internet of Things (IoT) in the progression of intelligent urban environments. By leveraging Internet of Things (IoT) technology, metropolitan areas can actively monitor and efficiently manage their resources

DOI: 10.5121/ijcnc.2024.16201

in real-time, hence leading to improved efficiency in the allocation and utilization of these resources. The adoption and execution of these measures not only serves to improve the overall welfare of residents but also aids in the reduction of waste and gates environmental consequences, promoting enduring urban sustainability. Moreover, the data generated by Internet of Things (IoT) devices holds the potential to provide substantial insights for urban planners and politicians. This significant knowledge enables individuals to make educated decisions and implement targeted solutions that effectively address specific challenges in urban settings. The Internet of Things (IoT) allows for the seamless integration of various devices and systems, enabling the real-time monitoring and administration of urban infrastructure. The interconnectivity between various components improves the efficiency of resource use and promotes the effectiveness of decision-making processes. In addition, the Internet of Things (IoT) enables the development of innovative applications and services that enhance the overall quality of life in metropolitan areas. These include intelligent housing, sophisticated healthcare systems, and efficient transit options. The incorporation of Internet of Things (IoT) technology holds significant significance in the establishment of sustainable and resilient urban environments due to the ongoing expansion and growing challenges faced by cities. The main aim of the proposed NCIoT protocol is to efficiently distribute information over two distinct paths. It is advisable to prioritize the primary choice, while considering the alternative option as a backup plan in case of any unforeseen complications. The use of predictive inquiry small packets (PISP) messages into cluster topologies enhances the routing protocol's ability to gather supplementary information on node distances and surrounding nodes. The NCIoT protocol is responsible for initiating the primary route selection process, which has been previously defined through the routing protocol. Consequently, the proposed approaches would utilize the Nodes Clustering-Based on IoT (NCIoT) to collect extensive data pertaining to the nodes from the routing table. Following this, the nodes will be programmed to function in an intelligent manner, allowing them to effectively reroute traffic through other pathways as required. The strategy that has been provided places emphasis on not only the occurrence of failure, but also the possibility of congestion and overload inside the networks. In the present day, the network is vulnerable to the impact of malicious individuals, unwanted messages, and several other obstacles that impede users' access to necessary services. The analysis involves considering a set of possible routes, followed by a detailed evaluation and assessment of the selected route based on certain constraints. The establishment of the Node Clustering on IoT (NCIoT) has been shown to contribute to the improvement of stability. By selecting a route that maximizes the lifetime (LT) as recommended by the Smart designated network (SDN), while also choosing the fastest path to reduce latency. An effective DNA The proposed methodology presents a selection procedure that considers the mobility characteristics of the node, including its velocity and the comparative velocity of the nearby nodes within the cluster as shown in Figure 1.

The structure of this article is as follows: In **section 2**, we discussed the impact of the Internet of Things (IoT) on networks and proposed solutions through the development of PISP messages. The purpose of these messages is to reduce the frequency of using "HELLO" messages, as they contribute to increased latency in checking the connectivity between nodes within a clustered grid Internet of Things (IoT) network. In **section 3**, an overview of relevant literature and research on enhancing node clustering in the context of the Internet of Things (IoT) for smart cities is provided. In this study, we will discuss many CBR protocols that have been developed or improved for implementation in a clustered grid topology, including LEACH, LEACH-e, and RCBRP. In the aforementioned **section 4**, our novel algorithm, along with its associated methodologies, has been presented and

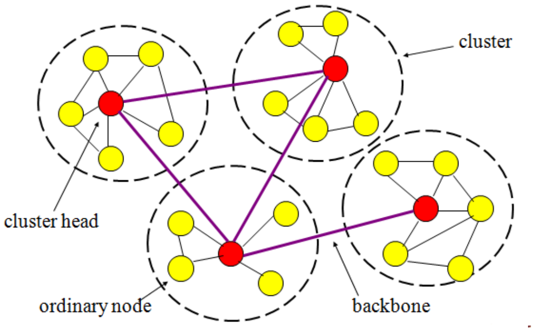

Fig. 1. Clustering Characteristics

juxtaposed against other relevant studies. Furthermore, we have presented the theoretical modeling equations together with a portion of the code implemented in the suggested protocol. **Section 5** provides an overview of the simulation parameters, along with a comprehensive presentation and analysis of the obtained results. Lastly, **section 6** provides the concluding remarks.

2 Improved node clustering by using IoT

Improving the clustering of nodes within the Internet of Things (IoT) framework, especially in the domain of healthcare applications within smart cities, has considerable importance. The integration of Internet of Things (IoT) device clusters inside healthcare settings facilitates improved examination and exploitation of gathered data. The application of clustering methods enables improved surveillance of patient welfare and permits healthcare professionals to swiftly respond to emergency circumstances. Nevertheless, this particular approach also engenders concerns regarding privacy and security due to its propensity to increase the probability of unauthorized persons acquiring personal patient information. Further investigation is necessary to emphasize the importance of data analysis and monitoring in healthcare settings, particularly about Internet of Things (IoT) devices, to enhance patient outcomes and overall population health. Investigating the specific approaches utilized for node clustering in Internet of Things (IoT) devices within healthcare settings can provide readers with a deeper understanding of the operating processes and potential benefits of this technology. The examination of measures implemented by healthcare organizations and specialists to safeguard privacy and security in response to escalating concerns stemming from the aggregation of Internet of Things (IoT) devices is of utmost importance. The analysis of the measures taken by healthcare organizations and specialists to protect privacy and security in response to increased risks resulting from the aggregation of Internet of Things (IoT) devices is highly significant. In summary, the optimization of node clustering within the Internet of Things (IoT) realm has a notable impact on advancing healthcare outcomes and facilitating the development of a more sustainable urban environment, as seen in the accompanying figure 2.

The main purpose of this research is to investigate and analyze the phenomena under investigation to achieve a more thorough understanding of its underlying components and consequences. The study's importance lies in its ability to enhance the existing body of knowledge in the field, as well as its potential to offer insights and guidance for future research efforts and practical applications [1]. The optimization of network performance is facilitated by enhanced node clustering in the context of the Internet of Things (IoT),

Fig. 2. Smart Cities with Node Connections via Different Connection

provide a notable advantage. The enhancement of communication and data transmission within a network may be attained by the arrangement of nodes into clusters based on their closeness and functionality. This methodology enables the implementation of efficient procedures, leading to enhanced response times and reduced latency. Furthermore, the use of increased node clustering enables improved resource allocation and utilization. This is achieved by enhancing the collaboration among nodes, which leads to a more efficient distribution of processing power and storage capacity. The aforementioned enhancement not only contributes to the improved performance of the Internet of Things (IoT) system but also plays a substantial part in attaining energy efficiency and reducing costs.

2.1 IoT Challenges and Prospects

The academic community has shown considerable interest and conducted extensive search on the difficulties and potential associated with the Internet of Things (IoT). To ensure the optimal performance of Internet of Things (IoT) nodes, it is crucial to develop a robust and interconnected network architecture. The successful execution of this objective requires the establishment of comprehensive service frameworks that conform to mutually agreed-upon criteria. By implementing this approach, the functionalities and capabilities of different applications, situations, and user requirements may be greatly improved. The development of Internet of Things (IoT) applications, albeit an ongoing process, poses several obstacles that need solutions. The difficulties at hand cover several factors like cost, power consumption, processing capacity, low latency, self-organization, distributed intelligence, and systems technology. The Internet of Things (IoT) presents a variety of issues. Despite the multitude of connections and opportunities presented by the Internet of Things (IoT) for end users and industry insights across many application fields, there exists a discernible lack in the construction of an effective architecture and standardized technological framework. The lack of this element poses a barrier to the smooth incorporation of the physical and virtual domains within a cohesive structure [1]. Several significant concerns have been discovered as follows. The discipline of architecture has a significant issue with the proliferation of various types of sensors, such as physical, chemical, biometric, and photo sensors. These sensors, in conjunction with networked smart devices and sophisticated technologies have a pivotal impact on the advancement of Internet of Things (IoT) applications.

These developments are highly dependent on several disciplines and their respective architectural designs or circumstances. In addition, the interrelationships among these devices enable wireless, spontaneous, and automatic communication. The efficacy of architectural services is augmented by the use of decentralization, mobility, and heightened complexity. Technical challenge: The wide range of application areas within the Internet of Things necessitates the creation of different scenarios and architectures. This, in turn, requires the development of numerous technologies to support the complex services provided by the Internet of Things. The presence of heterogeneity poses a significant challenge in the implementation of intelligent Internet of Things (IoT) systems. The subject matter under consideration refers to wireless networks, with a special emphasis on the idea of Wireless Networks[2][3][4]. An obstacle encountered within the realm of hardware for the Internet of Things (IoT) pertains to the incorporation of intelligent devices into intelligent systems. The optimization of inter-device communication is crucial for the successful deployment and supply of services in Internet of Things (IoT) applications. Scholars place a high emphasis on the advancement of hardware design, specifically focusing on the creation of a wireless trackable system that demonstrates qualities of being cost-effective, compact in size, and highly functional.

3 Background and Related Work

This paper provides an overview of node clustering in the context of the Internet of Things (IoT) and highlights the issues associated with this approach. Node clustering in the context of the Internet of Things (IoT) pertains to the systematic procedure of categorizing IoT devices into distinct groups, taking into consideration specific criteria or attributes. This technique has the potential to streamline network management, enhance communication efficiency, and optimize system performance. Nevertheless, node clustering in the context of the Internet of Things (IoT) several number of issues. The issues encompassed in this context are to the scalability of the clustering algorithm, the dynamic characteristics of IoT networks, and the heterogeneity exhibited by IoT devices. The resolution of these difficulties is of utmost importance in order to attain efficient and dependable node clustering in the Internet of Things (IoT). An illustrative counterexample highlighting the issues pertaining to node clustering in the Internet of Things (IoT) can be observed in a hypothetical situation where the clustering method exhibits inadequate scalability. In the context of a vast Internet of Things (IoT) network with numerous devices, the clustering algorithm may have difficulties in managing the substantial volume of data and processing demands [2]. Consequently, this might result in delayed reaction times and potential system malfunctions. In the given situation, it is possible for the clustering algorithm to erroneously cluster nodes, leading to ineffective distribution of resources and inferior system performance. Moreover, if the clustering algorithm is dependent on a centralized methodology, it has the potential to serve as a singular point of vulnerability, so compromising the overall functionality and resilience of the Internet of Things (IoT) network. In addition, in the event that the clustering algorithm lacks robustness in dealing with outliers or noisy data, there is a possibility of misclassifying significant nodes, hence resulting in severe system malfunctions. Moreover, the clustering algorithm's centralized approach may create a notable bottleneck in communication and decision-making procedures, impeding the ability to respond in real-time in dynamic Internet of Things (IoT) settings[3]. Nevertheless, the utilization of decentralized clustering algorithms in Internet of Things (IoT) networks present a comprehensive counterexample to the concern of a single point of failure. The distribution of the clustering process among numerous nodes enhances the network's resilience by eliminating the presence of a singular point of failure capable of causing a complete system shutdown. In addition, the algorithm can effectively classify significant nodes even when confronted with noisy data by including robust outlier identification approaches, hence mitigating the potential for system failures [4]. Moreover, the implementation of a decentralized method might lead to enhanced expediency and efficiency in communication and decision-making procedures. Nevertheless, it is important to consider a comprehensive counterexample that illustrates a situation in which the process of distributed clustering produces inconsistent outcomes as a result of communication delays or failures occurring between nodes. In instances of this nature, the network's ability to withstand and recover from disruptions may be undermined due to potential inaccuracies in the classification of critical nodes, hence resulting in system faults [3][5]. In addition, the decentralized approach may give rise to coordination difficulties and disagreements among nodes, leading to longer decision-making processes and potentially affecting the overall efficiency of the network. A Critical Examination of Current Node Clustering Techniques in the Context of Smart Cities Healthcare systems possess the capacity to offer significant insights into issues and constraints associated with existing methodologies. The author introduces a novel Robust Cluster Based Routing Protocol (RCBRP) that aims to improve performance by optimizing energy utilization. The clustering approach is employed to choose CH based on predetermined criteria, and each cluster is further broken into smaller sections. This study outlines six distinct steps, namely initialization, setup phase, distance computation, cluster formation, selection of cluster head (CH), selection of secondary cluster head (SCH), and energy conservation [6][7]. This section introduces a novel Robust Cluster Based Routing Protocol (RCBRP) that aims to improve performance by optimizing energy utilization. The clustering approach is employed to choose CH based on predetermined criteria, and each cluster is further broken into smaller sections. This study outlines six distinct steps, namely initialization, setup phase, distance computation, cluster formation, selection of cluster head (CH), selection of secondary cluster head (SCH), and energy conservation. On the other hand, the author introduces a novel Robust Cluster Based Routing Protocol (RCBRP) that aims to improve performance by optimizing energy utilization. The clustering approach is employed to choose CH based on predetermined criteria, and each cluster is further broken into smaller sections [8]. This study outlines six distinct steps, namely initialization, setup phase, distance computation, cluster formation, selection of cluster head (CH), selection of secondary cluster head (SCH), and energy conservation.[9]. The non-functional nodes are removed from the communication network. The effectiveness of the proposed plan RCBRP is assessed by comparing its results with those of its equivalents. The primary parameter of the routing protocol is to identify the sensor nodes that are currently operational[10]. The GEEC algorithm demonstrates superior performance compared to the previous two algorithms, since it operates for a duration of 680 rounds. The most optimal algorithm, which has been proposed, remains active for a total of 720 rounds. The RCBRP protocol demonstrates much superior performance in comparison to the LEECH, LEECH-C, and EECRP procedures. The first node experiences failure after 80 rounds in LEECH-C, 400 rounds in LEACH, 380 rounds in GEEC, and 380 rounds in EECRP [11][12][13]. Future research should prioritize the development of novel algorithms that possess the capability to adapt dynamically to the evolving network architecture and effectively manage the diverse data demands of distinct healthcare applications [14]. The concept of nodes clustering technology pertains to the procedure of categorizing nodes inside a network into groups based on specific traits or characteristics. This technology plays a crucial role in diverse domains like data analysis, machine learning, and social network analysis. The utilization of nodes clustering technology allows researchers and analysts to acquire valuable insights into the intricate systems' structure, behavior, and relationships by recognizing clusters or communities inside a network. The provided data can be utilized to identify irregularities, forecasting forthcoming patterns, and formulating well-informed judgments [15] [16]. In the context of data analysis, the utilization of node clustering technology facilitates the identification of patterns or trends inherent in a given dataset, hence enhancing the comprehensibility and interpretability of the data. Clustering techniques in the field of machine learning are employed to effectively group data points that exhibit similarities, hence enhancing the precision of predictions and classifications [17]. Furthermore, within the realm of social network analysis, the utilization of nodes clustering technology can be important in discerning communities or cohorts of individuals that exhibit comparable interests or behaviors. This analytical approach yields valuable insights that can be leveraged for targeted marketing initiatives or the allocation of resources [18][19].

A multi-rate Wi-Fi network can limit the bandwidth of high-rate links to that of low-rate links, as explained in this article. In this study, we present an MTF AP selection technique, a refinement of Mininet Wi-Fi processes. MTF uses access point throughput and station count as selection measures for association decisions. Simulations indicate that MTF delivers enhanced performance, particularly in multi-rate settings [20]. Various routing protocols have been documented for diverse contexts to enhance network performance in scenarios where nodes experience mobility or failure [21–24]. In the study conducted by the authors [25], many characteristics and settings of Mobile Ad hoc Networks (MANETs) were identified, including bandwidth (BW), resource availability, and energy constraints. Several proactive routing protocols, including Destination-Sequenced Distance-Vector Routing (DSDV), Optimized Link State Routing Protocol (OLSR), Cluster **HEAD** Gateway Switch Routing Protocol (CGSR), and Wireless Routing Protocol (WRP), employ message-triggered mechanisms to detect link failures [26, 27]. Based on the aforementioned messages, it can be inferred that the routing protocol possesses the capability to establish and uphold routes leading to its intended destination. In reactive routing protocols such as Dynamic Source Routing (DSR), Ad hoc On-Demand Distance Vector (AODV), and Temporally Ordered Routing Algorithm (TORA), the utilization of network resources will be optimized due to the creation of new paths between nodes only in the event of a failure. This approach effectively reduces the overhead associated with path establishment. The authors of [28, 29] discovered that the Optimized Link State Routing (OLSR) protocol employed Multi Point Relay (MPR) nodes for transmitting link state messages in order to generate a routing table. Within the context of the Optimized Link State Routing (OLSR) protocol, there exist two distinct categories of broadcasts that are transmitted, namely **HELLO** messages and Topology Control (TC) messages. To assess the status of connectivity, each node will periodically transmit a **HELLO** message to its neighboring nodes at intervals of two seconds. This approach is adopted as a waiting period of six seconds is deemed excessively lengthy. The transmission control (TC) message is derived from the data gathered through the **HELLO** messages [30] [31]. The duration of re-routing traffic is influenced by the intervals at which **HELLO** messages are sent. Consequently, this delay results in a higher rate of data packet loss and a decrease in overall throughput [32]. Regarding the density of nodes, Broch et al. (1998) conducted a study in which a total of 60 nodes were generated and dispersed throughout a terrain area measuring 1200m x 800m. The network configuration implemented the Random Waypoint Mobility Model, which incorporated nodes with varied speeds ranging from 2.5 m/s to 15 m/s [33]. The findings of this study, however, indicate that the impact of high node density was not statistically significant due to the presence of node mobility. This phenomenon can be attributed to the inherent resilience of radio connections, which exhibit a relatively slow rate of disconnection from neighboring nodes [34].

Characterisation of Network Stability and Connections In the domain of mobile ad hoc networks, it has been noted that every individual node exhibits a unique physical location due to the intrinsic capacity of nodes to move freely inside the network. The network's stability is contingent upon the velocity of movable nodes, whether it is characterized by sluggish or rapid movement. The constant alteration of the network topology in local communities, achieved by adding or removing nodes, leads to an increased load of control messages. The aforementioned cost stems from the necessity to periodically update the routing table for proactive protocols, such as connection status or distance vector. The transmission range of ad hoc networks might be limited as a result of the limiting capabilities of individual nodes. The analysis of the provided information is crucial. In the subject of ad hoc networks, two often employed conceptual models are the free space model and the ground reflection two-way model. The employment of the free space propagation model confers benefits owing to its dependence on a basic reference model.

4 Proposed Algorithm for the Nodes Clustering

The procedure of computing network clustering across several locations and subsequently broadcasting PISP packets to obtain comprehensive information about each cluster is illustrated in the flowchart shown in Figure 3. To choose the most appropriate local route for establishing an alternative path,the algorithm needs to calculate the distances between all nodes. Every individual node in the network will be assigned a specific position within its respective zone. Consequently,algorithm 1 will be employed to calculate the distance between nodes to identify all neighboring nodes that fall within the expected radio propagation range of 250 meters. Subsequently, the algorithm will ascertain a path to the desired destination by considering the minimum number of intermediate steps required. If the Euclidean distance between two nodes is less than 250 meters, the algorithm will classify them as proximate nodes. In situations when there are numerous adjacent nodes, the system initiates a process to assess and determine which neighboring node offers a viable route to the target, therefore establishing a new major pathway. The computer algorithm assesses a feasible alternate pathway by ascertaining the trajectory from the origin to the destination utilizing the principal routing table. The nodes that are associated with the primary pathway will be disregarded in the subsequent stage of the alternative pathway. Each node is assigned a position (X, Y) inside the given terrain area's radio propagation range, chosen randomly. Algorithm 1 incorporates the utilization of nodes inside the topology to facilitate the dissemination of concise control messages. The purpose of these messages is to inquire with neighboring nodes on the accessibility and dependability of alternative routes on data transmission. The backup paths serve as supplementary options to the primary pathway, which is stored in the main routing table and directed towards the intended destination.

The mechanism may be categorized into two distinct components. The initial duty entails the calculation of the main thoroughfare, which is established based on the positional separation between nodes. The second responsibility entails the creation of an alternate route, which is established by taking into account the neighboring nodes inside the identical cluster. Figure 4 illustrates the transmission behavior of each node in the network. After the initial transmission, each node sends a condensed PISP packet to gather detailed information about the neighboring nodes of the HEAD. The transmission of PISP packets

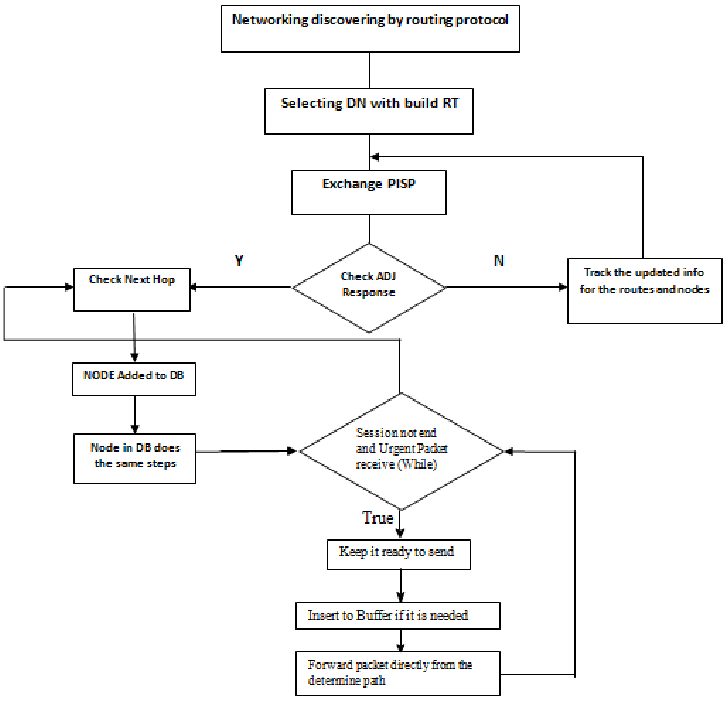
Networking discovering by routing protocol
Selecting DN with build RT
Exchange PISP
Check ADJ Response
Y
N
Check Next Hop
Track the updated info for the routes and nodes
NODE Added to DB
Node in DB does the same steps
Session not end and Urgent Packet receive (While)
True
Keep it ready to send
Insert to Buffer if it is needed
Forward packet directly from the determine path

Fig. 3. Diagram for Collecting Info and Network Clustering

Algorithm 1 *ClusteringwithPath* The algorithm generates a collection of alternative routes for each feasible route in the routing database.

```
procedure $FindingPath(T_r, s, d, edges\_to\_avoid)$
$T_r$: Node available
$V$: Vertex $G(V, E)$
$\mathit{\Gamma}(v)$: The collection of neighboring vertices to a given vertex$v$
$s$: Source or Head
$d$: Final Destination
$p_a(s, d) \leftarrow \emptyset$
$q_{sub} \leftarrow \emptyset$
$Enqueue(Q, (q_{sub}, s))$
while $Q \neq \emptyset$ and $path_a(s, d) = \emptyset$ do
    $(q_{sub}, x) \leftarrow Front(Q)$
    for all $k \in \mathit{\Gamma}(r)$ do
        $e \leftarrow (x, r)$
        if $(q_{sub} \cup e) \cap edges\_to\_avoid = \emptyset$ then
            if $P_r(T_r, k, d) \cap edges\_to\_avoid = \emptyset$ then
                $p_a(s, NHop) \leftarrow q_{sub} \cup e \cup P_r(T_r, k, d)$
            else
                $Enqueue(Q, (q_{sub} \cup e, k))$
            end if
        end if
    end for
end while
end procedure
```

is initiated by the nodes within the set A, G, H to identify their surrounding nodes and establish the membership of nodes within the same cluster. This procedure further enables the identification of the nodes that exhibit connections with other clusters. Node A selectively delivers data packets to its adjacent nodes B and C, while intentionally excluding node D. The reason for this exclusion is the fact that node D serves as the initial hop on the principal path and may be selected by the pre-existing protocols. The node that encompasses components B and C evaluate to ascertain the presence of any adjacent nodes that are not part of the primary node's route. Furthermore, this study will investigate the connectivity of nodes to other clusters in the scenario when the destination is situated in a distinct cluster. Nodes E, F, and C send an acknowledgment to inform the Head that they can relay the packets on behalf of node D in case node D encounters any more issues.

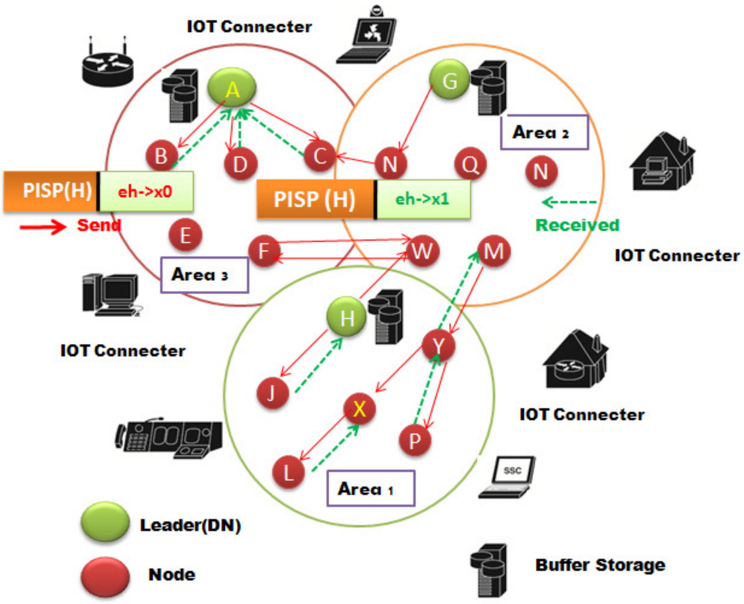

Fig. 4. SDN Head and Area clustering

The routing data displayed in Table 1 indicates that a secondary route exists between the destination and the neighboring node, which differs from the primary path. The dense arrow symbolizes the initial transition that takes place within the cluster, traversing Area1, Area2, and Area3, from the origin to the endpoint. For greater specificity, the arrangement of nodes can be denoted as follows: A->D->F->E. The purpose of a node A inquiry into whether neighboring nodes C or B provide information regarding the accessibility of an alternate path to the target is to ascertain whether those nodes have connections to other clusters via distinct nodes. Subsequent to the inquiry, we shall elaborate on the Nodes Clustering Based on the IoT (NCIoT) proposal and its algorithmic implementation for determining the **Head** entity's optimal positioning. The equations incorporate factors such as distance and power consumption.

4.1 Theoretical Analysis for the Proposed Algorithm

In a network, packets are directed toward their intended destination by utilizing quality criteria that favor factors such as lower prices or shorter distances. Various routing approaches might be exemplified within the given environment. Nevertheless, the network

-	**A**	**B**	**C**	**D**	**E**	**F**
A	–	➠ B	➠C	➠D	–	–
B	A	–	–	➠D	E	–
C	A	–	–	D	F	–
D	➠A	➠B	➠C	–	E	➠ F
E	–	➠B	–	D	–	➠F
F	➠ H	➠N	➠ D	➠E	**-**	**-**

Table 1. Checking Many Routes via Adjacent

protocols successfully guarantee the continuous maintenance of an updated routing table by periodic updates. It is hypothesized that there is a graph, represented as G=(V, E), where V represents the set of nodes and E represents the set of edges that link different nodes. The establishment of a virtual connection between nodes is facilitated by utilizing the information contained in the routing table, which is actively handled by the proposed protocol. The suggested solution assumes that the routing between nodes has been established, and the packet begins transmission at time RT_{r0}. All the information regarding the journey between the source and destination is represented as $\mathit{\Gamma}(V_n)$. Consequently, the pathway from the point of origin to the intended endpoint will be delineated in the subsequent manner: The variable $Path_{RT_{r(i+1)}}(s,d)$ is started as an empty set.

The network design needs to encompass the integration of a defined quantity of nodes, represented as N. Based on the calculation of graph trees, the number of edges may be expressed as 2n̂. The occurrence of this phenomenon can be attributed to the existence of several pathways for each individual node. Let V be a set comprising elements V0, V1, V2,..., and n-Vi. It is assumed that the source node is denoted as V0. The symbol ∞ is used to denote the initial cost of arc(i, j). At the outset, we define a collection V = {V0, V1, V2,..., VnVi} comprising all nodes. Additionally, a set S = {V0} is utilized to hold the nodes that possess the shortest path. The source node is represented as {V0}, and the set G_K is defined as empty, indicating a graph with K alternative edges leading to the destination. Choose a vertex W from the set V1-S, where D[W] denotes the minimum distance, assuming S is the beginning vertex V0. Incorporate the element W into the set S. To update the value of D[V] for each vertex V in the set V1-S, the minimum value is computed between the current value of D[V] and the sum of D[W] and the weight C[W, V]. The set S is to be updated by including the elements V0, V1, ..and Vd. If the primary route becomes unavailable, the subsequent calculations will proceed according to the following outline: Let S be the set produced by the addition of the element w and the removal of the member K from S. Perform the following actions for each vertex v in the set V, with the except of the items S and K. The equation may be expressed in the following manner: The value of D[v] is equivalent to the lesser value between D[v] and the sum of D[w] and C[w, v].Therefore, a random variable $X_j \in \{0,1\}$ has been introduced to describe the connection status between two nodes, referred to as A and B, in a particular subregion. The index represented by j indicates the specific point in time when A sends the update message to the HEAD node. The provided sequence, represented as $X_{0,1}$,.....,X_j={X_j}$_j$ $^\infty$=1, is an example of a sequence. In this concept, the Markov chain represents the succession of random variables {X_j}$_j$ $^\infty$. The proposed methodology has exhibited its capacity to calculate an alternative route that might potentially function as the most efficient path from the origin to the destination. In some circumstances, this alternative for backup may be considered the most optimal and advantageous strategy for the new routing table. In Section 5, the study has shown that the proposed algorithm has effectively enhanced the transmission of traffic from the source to the destination.

- The networks encompassed by Smart Devices incorporate the algorithm that has been put out.

$$P_r = P_t G_t G_r (\frac{h_t^2 h_r^2}{d^4}) \tag{1}$$

Where G$_t$ represents the gain of the transmitter antenna, G$_r$ represents the gain of the receiver Wireless signal, d represents the distance between the antennas in meters, h$_t$ represents the height of the transmitter antenna, and h$_r$ represents the height of the reception antenna shown in equation 1.

$$d = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2} \tag{2}$$

- if (d < outbound) Add the node that is located in the nearby nodes to the list of nodes that are adjacent for each node on the topology.
- Check the distance between the nodes in close proximity to determine which one will serve as the primary next hop as we use the equation number 2.
- Find the alternative route to the main destination via NNHop.

This study presents an analysis of the hardware components and operational mechanisms of the sensor node as shown in table 2. Specifically, it explores three distinct ZigBee settings: ZigBee coordinator, ZigBee router, and ZigBee end devices, each serving unique functions. The voltage consumption of the sensor node is divided between 3.3 volts and 5 volts. Consequently, a regulator is employed to facilitate the conversion between High Voltage (HV) and Low Voltage (LV), as well as vice versa. In contrast to the Arduino Uno version, the Arduino Pro Mini requires bootloader programming, necessitating the use of an FTDI 232 as a bootloader. Zigbee is a wireless communication technology that operates at a frequency of 2.4 GHz or 2400 MHz. Consequently, the wavelength λ of Zigbee can be calculated using the formula $\lambda = c/f*$, where c represents the speed of light, which is approximately $3x10^8$ meters per second. The power received by the receiver, expressed in decibels (dB), will consistently decrease as the distance (d) between the transmitter and receiver increases, as indicated by equation 3. The starting power received by the receiver (Pr0) when the distance (d) is equal to 1 meter may be observed in equation 4 and equation 5. The initial test parameter is the received signal strength (RSS) in decibels per milliwatt (dBm) under the condition of Free Space propagation, where the exponent (n) of the Free Space path loss model is set to 2. The Receiver Signal Strength (RSS) is determined by comparing equation 6 with the measured values obtained during the experiment or field measurement. On the other hand, the attenuation is calculated using equations 7, 8, and 9.

Hardware	**Information**
Microcontroller Arduino Pro mini	Processor, ADC, Data Serial Communication.
XBee S2c End Device	Wireless sensor Network type to sending Pulse sensor data to Coordinator node
XBee S2c Coordinator	Wireless sensor Network type to receive Pulse sensor data from ZED or ZR to Base Station
XBee S2c Router	Wireless sensor Network type to sending Pulse sensor data to Coordinator node from ZED and Communicate between each Router at Mesh network
Battery 3.7 Volt 1000 mAh	Supply power to the sensor node

Table 2. Mobile Node H/W [35]

$$P0 = P_t x(\frac{\lambda}{\pi 4})^2 G_t G_r \frac{P_t}{P0} = \frac{(4\pi d)^2}{(\lambda)^2} = \frac{(4\pi f d)^2}{c^2} \tag{3}$$

$$P_r = P0 \div d^2 \tag{4}$$

$$FreeSpace = 20\log_d + 20\log_f - 27.5 \tag{5}$$

$$FreeSpace2450MHz = -(20\log d + 40.3) \tag{6}$$

The constant variable, represented as C, plays a crucial role in wireless signal attenuation inside the Free Space scenario, with a precise numerical value of 27.5. As the distance (d) between two points grows, there will be a proportional rise in the value of L Free Space (-dB). Equation 4 specifies that the frequency utilized by Zigbee is 2.45 GHz. The aforementioned equation facilitates the calculation of the Power Receiver in decibel milliwatts (dBm).

$$P_r = P_t + G_r + G_t + L \tag{7}$$

The received power (P$_r$) can be mathematically represented as the multiplication of the transmitted power (P$_t$) and the ratio of the wavelength λ to the product of 4, and the distance. The equation can be expressed in an alternative form as $G_t G_r^2$ in equations 8 and 9 The power received, denoted as P$_r$, is impacted by many factors. The analysis incorporates the components of transmitted power, denoted as P$_t$, which are measured in units of either Watts or milliwatts. In addition, the carrier wavelength, represented by the symbol λ and measured in meters, is of significant significance. An additional crucial determinant in the equation is the spatial separation between the transmitting device and the receiving device, denoted as d and quantified in units of meters. Furthermore, the power received is subject to the influence of the transmitter's antenna gain (G$_t$) and the receiver's antenna gain (G$_r$). The term ”antenna gain” refers to the measurement of power radiation in a certain direction. However, the mathematical expression for calculating the increment in decibels can be represented as:

$$P_{db} = 10\log_{10}(\frac{P_{out}}{P_{in}}) \tag{8}$$

The equation for free space loss in an ideal omni-directional antenna can be expressed as follows in equation 9 :

$$P_t = \frac{(4\pi d)^2}{(\lambda)^2}, P_r = \frac{(4\pi f d)^2}{c^2} \tag{9}$$

where P_t represents the transmitted power, P_r represents the received power, d represents the distance between the transmitter and receiver, λ represents the wavelength of the signal, f represents the frequency of the signal, and c represents the speed of light. In the proposed algorithm we have implemented the forwarding packets for checking all nodes the networks as below equation 10 11.

$$\begin{gathered} \forall PISP = \sum allocpkt() + HeaderIPsim * sim :: access(PISP) \\ \forall Node = \prod_{s}^{N} find(Source, NNH) + PSequence \\ \sum Scheduler :: instance().clock() \times \sum_{0}^{n} DestPort + TimeMax \end{gathered} \tag{10}$$

$$\begin{gathered}\sum HeaderIP = Hdr\_IP + \prod Fwrd.resched(TimeMax)\\ \forall(allocPacket, DestPort) = \sum allocPacket = (rate \times 1500)/(size \times 8)\end{gathered} \tag{11}$$

$$\forall HPacket.port = rout[Node- > addr][DestPort] \in Node- > queue[DestPort]$$
$$hdr\_PISP- > TTL = Scheduler :: instance().clock();$$
$$hdr\_PISP- > access(p)- > size() = \sum size\_(rate \times 1500)/(size\_IP \times 8);$$

$$(S, NH) = \left\{ \begin{array}{ll} ||\forall addr = org\_source \times instance().clock()||, & \text{if } time \leq 1sec \\ ||Rout[S][NHop] = \sqrt{(x_2\ -\ x_1)^2\ +\ (y_2\ -\ y_1)^2}||, & \text{if } NH \neq Dest \end{array} \right\}$$
$$\forall addr = org_source \times Scheduler\ \ instance().clock()$$
$$\forall Rout[IPsourse][NNH] = \prod_{s}^{d} (NH) \forall Rout[NodeS][IP\_DEST] \notin \forall Rout[S][NH]$$
$$PISP\_Header = \sum_{s}^{D} \sum_{s}^{N} Routing[i][j]$$

When the **allocate packets** function initiates the distribution of inquiry packets to adjacent nodes based on their proximity, the simulation time incorporates the instance clock-measured durations of transmission and reception. After the collection of all pertinent data in accordance with Equation 10, the transmission of CBR or UDP packets will initiate in the form of binary data. From one step to the next, these packets will be forwarded until they reach their intended destination. The principal computational algorithm is denoted by Equation 11, and it consists of monitoring any updates concerning each cluster and calculating the distance. It has been observed that messages transmitted from a source to a destination through an intermediary node return to the source in an enigmatic manner. In the first scenario, the source node makes a request to its nearby node for a path of higher quality than its own. To meet the second requirement, the origin must discover a different path that avoids loops without casting suspicion on its nearby nodes. The third stipulation has to do with the particulars of the situation under consideration. The term "clustering topology" describes the structure or layout of clusters inside a system or network. We will attempt to explain in detail how our novel approach to cluster network analysis operates in this paper. On the primary route, every node engages in communication with multiple neighboring nodes. Then, a neighboring node within the same cluster is selected as a secondary option. Furthermore, the complete path for each cluster is computed by each neighboring node, enabling accessibility from across regions. Every router along the primary path possesses the capability to autonomously ascertain a secondary path for data forwarding. This is achieved through the utilization of the present routing information of each node, which might comprise a pre-established path. To illustrate how to discuss our protocol, we will concentrate on a particular subject within topology. Within the existing topology, each node is assured of having a minimum of two neighboring nodes. The neighboring nodes are cognizant of the fact that the leader node is responsible for furnishing all the necessary information for the other nodes to select the optimal alternate route. To reach the ultimate destination D from the starting location S, one may choose from the following paths: $S \to adj \to NH... \to D$ The total weights for all the topology$\sum W_0 = X$; X: Total weights for all arcs on the topology.

Then: $\mathit{\Delta} W = \sum W_0 = X$; If we make the assumption that the algorithm has computed the best second paths between S and D, it can be expressed as follows: $P_s \to D$

$S \rightarrow NH \rightarrow NNH \rightarrow ..... \rightarrow D$. At the conclusion of each simulation period, the aggregate count of **PISP** Control Overhead messages generated corresponds to the cumulative total of all messages produced. Additionally, during this process, we have computed all **PISP** packets and collected all relevant information by employing the routing mechanism and incorporating alternative next-hop options into the updated routing table. Subsequently, all gathered information is transmitted to the HEAD cluster node within the entirety of the IoT network. The packet header for the **PISP**, as depicted below, remains consistent with the header generated by the algorithm under consideration. The header exclusively includes the IP source, IP destination, and acknowledgement, together with the identifier of the subsequent hop if it has been modified. The optimization of the sending and receiving time from the head nodes is enhanced by taking into account the time it takes for the data to leave the head node and return to it. Ultimately, all packets generated by the **PISP** will gather the necessary data specific to the cluster they are producing. This part introduces a revolutionary Node clustering based on the Internet of Things (NCIoT) routing protocol. It outlines the procedures and tactics we will employ to improve the routing stability of an NCIoT network. First, we demonstrate how to segment the IoT network into stationary clusters. Second, a unique distributed **HEAD** cluster election mechanism is proposed, which allows for the selection of a next hop for forwarding packets through it in the event of network problems. Clustering allows for more control and monitoring of data packets as they travel from the source to the destination. This will cause the bf HEAD cluster to be notified of any changes in its cluster by utilizing the **PISP** inquiry packets that they are sending regularly without any effect on the network and controlling them to be in the same cluster, rather than forwarding to any other unrelated cluster all notation has defined in table3.

Notation	**Definition**
NH	Next Hop
ADJ	Adjacent Node
Dest	Destination
NNH	Next Next Hop
Dist	Distance
alt	Alternative Node
sim	simulation time
S	Source
H	Head Node
Point	The node on the Route

Table 3. Algorithm Notation and Definition

4.2 Computing control PISP process

This study aims to evaluate the capacity of network nodes to utilize packets generated by **PISP** for multiple purposes. These purposes include gathering information and delivering it to the cluster head, as well as examining the accessibility of paths between adjacent nodes and determining the number of feasible paths between a given source and destination. Furthermore, the objective of this study is to ascertain the most favorable quantity of nodes within each cluster. In the context of ad hoc networks, the focus will be on examining the requisite node mobility within the transmission range to facilitate efficient communication. When the process of node mobility commences, the nodes proceed to create direct connections. The **PISP** message regulates the flow of data traffic by providing notifications to the central node of any updates. Consequently, when nodes receive a notification, they react by instructing the **HEAD** to reroute the traffic through the next adjacent node. Alternatively, if there are nodes with shorter distances, the packets are sent through them to expedite delivery to the destination, thereby minimizing packet loss. In response to a received message, each adjacent node offers an acknowledgment by broadcasting a packet that contains a field indicating either ”0x” or ”1x”. When the acknowledgment packets are designated as ”1x,” it indicates that the next node has an alternate routing path and can function as a backup node in case of any modifications within the cluster. When the acknowledgement packets are assigned a value of ”0x”, it signifies that the specific node is incapable of operating as a backup near intended destination. After the extraction of the packet, the source node will analyze its contents in order to ascertain whether they include the value ”1x.” When a packet containing a ”1x” identifier is detected, the source node will incorporate the associated node, which responds with a ”1x” as the first hop in its alternative route using distinct NH. Upon receiving a packet with the hexadecimal prefix ”0x,” the source node will proceed to authenticate the answers given by its adjacent nodes. Consequently, if all acknowledgment headers received from surrounding nodes collectively display a value of ”0x”, it can be deduced that the transmission of traffic is not viable. Consequently, the third stage of the **PISP** control entails the identification of an alternative pathway from the adjacent node to a distinct node, as seen in algorithm 2.The packet header for the **PISP**, as depicted below, remains consistent with the header generated by the algorithm under consideration. The header exclusively includes the IP source, destination, and acknowledgment, together with the identification of the subsequent hop if it has been modified. The optimization of the sending and receiving time from the head nodes is enhanced by accounting for the time it takes for the data to leave the head node and return to it. Ultimately, the **PISP** packets will gather the necessary data pertaining to the cluster they are generating.

Algorithm 2 Cluster Area Info via PISP

```
$point = search_adj(S, NearestNode);$
$i \leftarrow NumberofAdjacent$
while $i \geq NumberofAdjacent$ do
    $array_rout[point][adj]! = INF$
    if $rout[point][adj] == adj\textbf{and}rout[point][NHOP] \neq PrimaryAdj$ then
        $NextHop[adj] = ara_rout[point + NH][adj]$
        $i \leftarrow adj + 1$
        $ClusterRoute[point][NH] = rout[NextHop[adj]][NH]$
    end if
end while
```

The focal point of consideration in this context is a specific node that is either the head node or a neighboring node within the clustered region. The search_adjacent method initiates by disseminating the **PISP** packets to gather comprehensive data regarding the nodes within the cluster. An array is employed as a buffer to store any adjacent nodes that are not part of the major protocolś main channel, including LEACH, LEACH-e, and RCBRP. Every node will initiate the process of reading the subsequent hop until it reaches its final destination. The **PISP** facilitates the efficient acquisition of clustered route information and ensures timely updates for the head nodes regarding the cluster information. To determine the number of **PISP** messages transmitted throughout the simulation period, the remaining power consumption and lifetime of the selected head or designated node are divided by the duration of the message exchange period between nodes, as seen below:

$$GPISP = \sum_{s}^{N} PISP \div Sim\_time \tag{12}$$

G: Generated number of PISP
Sim_Time : Simulation Time
When a head node is present in each cluster area, it establishes a default state for the status of all nodes. The communication between nodes should be established by utilizing the **HELLO** message over the default routing protocol. The primary objective of this paper is to increase knowledge of Head, a protocol that can potentially decrease the volume of **HELLO** messages created during the exchange of **PISP** packets. This reduction is achieved by employing smaller and faster **PISP** packets, as seen in the simulation results. Once a nearby node crosses the threshold point and enters the cluster zone, it is automatically designated as a member of the cluster. Subsequently, a **PISP** message is transmitted to the head, contingent upon the condition that the HEAD gets the **PISP** message within a certain duration of time denoted as ”T” seconds. In this particular instance, we are presented with two distinct scenarios. The **PISP** message is generated by the HEAD. In the event that any nodes become part of the cluster area or any neighboring node leaves the cluster, it is imperative to take into account the potential failure or disruption of connections.The objective of this study is to determine the number of control **PISP** packets present in each cluster through a systematic calculation process.

5 Simulation Experiment

A network simulation using NS2 was conducted to assess the performance of the proposed upgraded **NCIoT** protocol in networks with high and low node densities. The simulation results of the **NCIoT** protocol were compared with other relevant study protocols, namely **LEACH-e, LEACH, and RCBRP**. The evidence obtained through NS2 simulation provided strong support for the utilization of IoT technology by nodes to enhance their responsiveness and preparedness in various connection scenarios. A radio propagation range was employed, utilizing a transmission power of 0.28 watts. The system lets individual nodes transmit or receive data packets to or from next to them within a maximum range of 250 meters. The researcher employed the IEEE 802.11b protocol at the data-link and physical levels to facilitate the sharing of multimedia content via wireless networks. The network simulator utilized the random WayPoint mobility model, with a roaming region measuring 1600 x 1600 m^2. During the simulation, the movement or relocation of each node within clusters occurred. The initial velocity, which was measured at 1

Parameter	**Value**
Wireless LAN Medium Access Control (MAC)	IEEE 802.11
Maximum range Distance between Mobile Nodes	250 m
Roaming area	1600 X 1600 m^2
Number of Nodes test	25,50,100 up to 500
Minimum Node Speed Movement	0 to 1 m/s

Table 4. Simulation Parameter

m/s, was comparatively modest. Nevertheless, this velocity selection will become evident and significant in subsequent analyses and correlations. The duration of each simulation was 500 seconds. The experiment was carried out in a series of ten trials, after which the mean value was calculated. The packet was 512 bytes in length and was limited to 1024 bytes in length; the bit rate was set to 2 MB/s. The ability of a wireless connection to be shared within an ad hoc configuration network is a widely acknowledged fact. About density, the initial simulated scenario comprised an aggregate of 200 to 500 nodes, evenly distributed across each cluster region. A traffic rate of 512 kb/s was recorded between the source and destination nodes throughout the simulation. The subsequent section presents the simulation results, which have been formatted as line graphs. The parameters for these graphs are specified in Table 4. The concept of ”packet loss ratio” refers to the proportion of deleted packets about the total number of transmitted packets. The average end-to-end delay is a metric used in statistics to quantify the mean duration of time that elapses between the commencement of data packet transmission and its final arrival. Calculated as follows, throughput is the quantity of packets that have been received during a specified simulated period without interruption or interference.

Prior to assessing the performance concerns associated with network topologies in relation to computing a backup path over a Mobile Ad hoc Network (MANET), it is crucial to identify the network factors that may impact the Quality of Service (QoS) of video data being broadcast. The present study centers its attention on three parameters that have the potential to provide a more comprehensive understanding of the impact of video traffic tactics. To assess the impact of node density, it is imperative to acknowledge that higher densities exhibit greater longevity when contrasted with lower or moderate densities. This phenomenon occurs because of the decreased capacity of the latter to effectively identify and sustain novel pathways as the nodes progressively disperse over various clusters, hence heightening the likelihood of generating a disconnected topology. Areas with nodes exhibit more stability when they undergo slower movement, hence enabling the preservation of services for extended durations. The packet latency, throughput, and packet delivery ratio were tested after partitioning the networks into many clusters.

5.1 Performance and Analyses Evaluation

At each cluster, an assessment is conducted on our suggested protocol and another protocol of a similar kind, with the focus on evaluating the stability of the route between the source and the destination. The Node clustering based on the Internet of Things(**NCIoT)** protocol determines the complete clustered region by considering the connectivity distance between all areas. The **NCIoT** protocol is employed to determine the appropriate Base Station or **HEAD**node by gathering information from all nodes through the dissemination of PISP inquiry packets. The selection of the **HEAD** by the **NCIoT** is determined by considering its historical background, database information, and lifespan. Each node within the cluster is regarded as an intelligent device that is designed to remain within the confines of the cluster. In the event of instability or malfunction, neighboring nodes are notified of the issue by PISP inquiry packets. Furthermore, to guarantee the interconnectivity and stability of all clusters along a certain route, the **NCIoT** protocol incorporates the assessment of route validity. It is crucial to acknowledge that the **NCIoT** protocol operates in real-time and exhibits dynamic behavior. Consequently, whenever a packet reaches a cluster, the **HEAD** node initiates the **NCIoT** protocol recursively across all cluster regions. This recursive application is based on the computed distance between nodes, as demonstrated in the aforementioned equation. Based on this, the closest node will relay the data packet until it reaches the intended destination. Numerous scholarly studies are presently examining cluster routing protocols, including **LEACH, LEACH-e, and RCBRP**, which are documented in the existing body of research. RCBRP employs a sequential cluster selection approach to facilitate route construction. The selection process is contingent upon real-time traffic conditions and node density, as well as the traffic load and distance of the route in question relative to the intended destination.

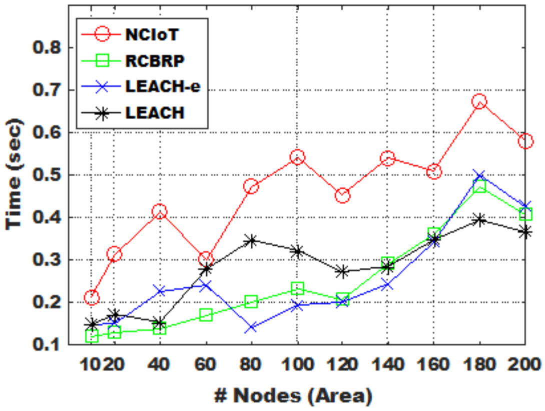

Fig. 5. Throughput Network

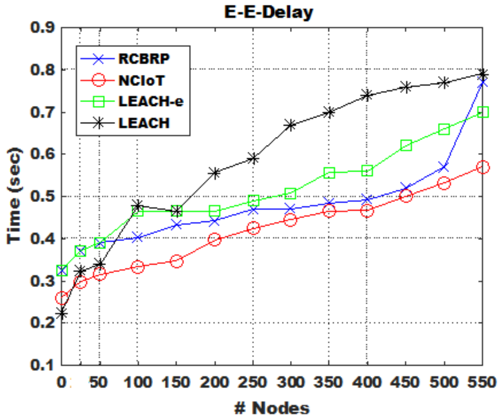

Fig. 6. End to End Delay

The Node clustering based on the Internet of Things **NCIoT** employs a node selection mechanism that identifies nodes leading to the nearest subsequent cluster, which in turn has the shortest path hop by hop to the target. When compared to existing (CBR) protocols, the simulation results provide evidence of the efficacy of the **NCIoT** algorithms. These algorithms have been shown to enhance network throughput by 50% and reduce end-to-end latency by 17%. In this study, we conduct a comparative analysis of the **NCIoT** protocol about the **LEACH, LEACH-e, and RCBRP** protocols.According to the data depicted in Figures 6 and 5, it can be observed that the **NCIoT** protocol exhibits superior performance compared to the **LEACH, LEACH-e, and RCBRP** protocols. The selection of routes with high stability is a key factor in determining throughput and end-to-end delay in the context of the **NCIoT** protocol. This selection process is based on the historical performance and available resources of the **HEAD**. The **RCBRP** algorithm finds the cluster with the required route to the destination regardless of any event that occurred, such as the stability of all nodes, overhead, or collision. Also, **LEACH, LEACH-e, and RCBRP** selects a series of clusters by considering real-time node density with power consumption, the traffic load on the respective road segment, and the travel distance to the destination without considering the stability of the routes. The figures [7,8] are the average throughput, the percentage of the throughput, the average end-to-end delay, and the percentage of the end-to-end delay, respectively. The **NCIoT** algorithm significantly improves the networks performance by increasing the throughput percentage by 50-60% compared to **LEACH, LEACH-e, and RCBRP**.

The measurement of the continuity index for each scenario is depicted in Figure 9. Live video broadcasting can be deconstructed into segments with similar dimensions. Within the framework of a live broadcast system, it is noted that every node participates in the presentation of similar content for a specific segment. Therefore, the continuity index can be defined as follows:

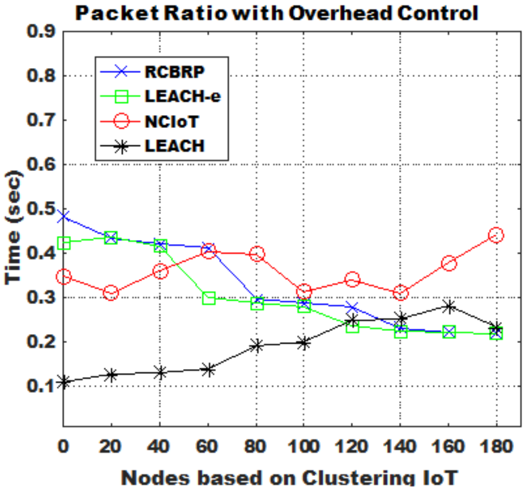

Fig. 7. Packet Over All Ratio Received

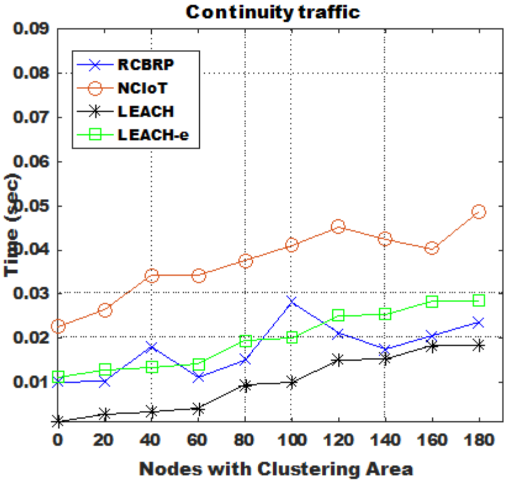

Fig. 8. Continuity Index

$$ContinuityIndex = Np/Ns, \tag{13}$$

In this context, Np represents the quantity of blocks that are received before to the designated playback dates, whereas Ns denotes the overall count of blocks inside a single content. A **NCIoT** network with dimensions of 1600m x 1600m was established, followed by the

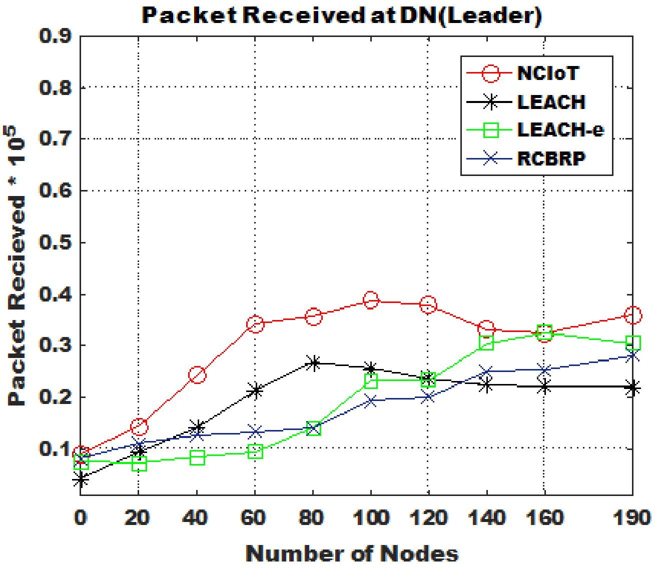

Fig. 9. Continuity of Receiving Data Packets

partitioning of the network into area clusters with a radius of 125 meters. The cumulative output of traffic generators supplies the network structure with intelligent nodes that are interconnected within the Internet of Things (IoT). Multiple numbers of nodes are generated in each simulation run. Consequently, after all the nodes have been integrated into the **NCIoT** network, we commence the reception of outcomes. To enhance the authenticity of our simulation, Sumo maintains a sufficient spatial separation between neighboring structures to mitigate the occurrence of collision scenarios.

The number of active nodes over time as determined by the NCIoT and LEACH methodologies is depicted in Figure 10. The provided figure shows cases how NCIoT exhibits a 20% increase in the mean number of operational nodes when compared to LEACH, LEACH-e, and RCBRP protocols. resolves the routing problem by employing fuzzy logic to model cluster-head selection, thereby surpassing competitors. In conjunction with the quantity of operational nodes, the network lifetime exerts an impact on IoT systems. The duration of an Internet of Things (IoT) system is ascertained by tally-marking the number of iterations from the system's inception until a specific proportion of the initial operational nodes remain. In this study, we conduct a comparative analysis of the aforementioned protocol, namely **LEACH, LEACH-e, and RCBRP**; To assess their similarities and differences. The mean and the proportion of individuals who send a greeting message, specifically **"HELLO**," in comparison to those who use the Predictive Inquiry Small Packets (PISP) are provided, in that order. The calculation of the proportion of **HELLO** messages transmitted by nodes is determined by dividing the entire count of **HELLO** messages sent out by the overall count of messages sent out. Simultaneously, we conduct measurements on the **PISP** packets and ascertain that the **PISP** exhibits a lower overhead compared to **HELLO**, as indicated by its relatively modest size. The **NCIoT** protocol effectively minimizes the transmission of **HELLO** messages by generating them at a rate of only 5.9%. This reduction is achieved by selectively propagating **HELLO** messages in three specific scenarios: whenever the **HEAD** node enters the cluster zone, when clever node locations exit the cluster zone, and when a new **HEAD** node declares itself to the cluster. In contrast, a significant quantity of greeting messages is produced by the **LEACH, LEACH-e, and RCBRP** algorithms. This phenomenon can be attributed to the regular transmission of **HELLO** messages by all of these protocols. In this context, Np represents the quantity of blocks that are received prior to playback deadlines, whereas Ns denotes the entire amount of blocks within a given content. To assess the effectiveness of the **NCIoT** protocol, a comparative analysis is conducted with three alternative protocols: **LEACH, LEACH-e, and RCBRP**. These protocols share the characteristic of transmitting control overhead signals either every 5 seconds or when their deviation from the originally established motion function exceeds 10 m/s. Furthermore, the **NCIoT** protocol adheres to a typical practice of broadcasting **HELLO** messages at regular intervals

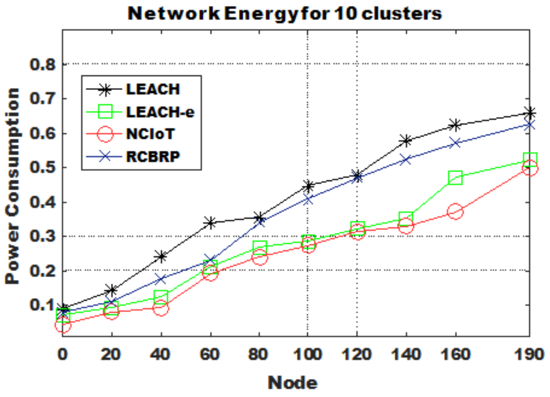

Fig. 10. Comparison Energy

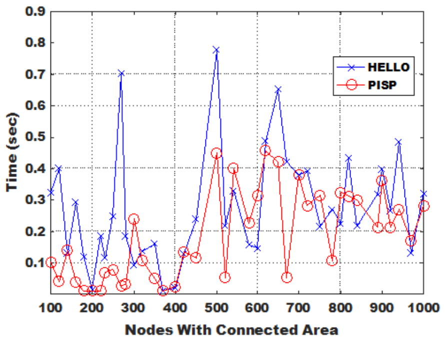

Fig. 11. Hello with PISP Utilization

of 10 seconds. Additionally, we employ the tiny **PISP** inquiry to ensure the node database information remains up to current. Figure 11 presents a comparison of the performance of **LEACH, LEACH-e, and RCBRP** in terms of the quantity of **HELLO** messages created. To provide a comprehensive analysis, we calculate the average performance and contrast it with **NCIoT**. The **NCIoT** protocol disseminates **HELLO** messages in many contexts, including when the **HEAD** is assigned and enters the cluster zone when the **HEAD** quits the cluster zone, and when a new **HEAD** proclaims its presence to the cluster. The use of **NCIoT** resulted in a significant reduction in the quantity of nodes generated inside each cluster.

6 Conclusion

The current study examined the influence of dynamic node displacement and various velocities (namely, walking and cycling) on the backup path. The repositioned nodes foresee the required movement of vehicles. The study above shows that there are numerous instances of node failures when establishing connections. As a result, it is necessary to update the routing table to appropriately represent the dynamic changes inside the network. This document offers a thorough introduction and detailed elucidation of the NCIoT protocol. The NCIoT protocol requires the head or base station to repeatedly initiate communication, considering the stability of the path, in order to establish contact with the target cluster. Each packet that a cluster receives undergoes examination, as previously mentioned. The assessment of whether the durability and power efficiency of the head node have been previously improved will impact the result. Geographical regions are classified according to their source, destination, and the route that has the highest minimum average throughput among all possible options. The simulation findings demonstrate that the NCIoT protocol surpasses traditional clustered routing protocols in terms of both route performance and end-to-end latency. In addition, the NCIoT protocols improve network efficiency. The main goal of the PISP (Protocol Independent Spanning Tree Protocol) is to reduce the number of Hello messages that are transmitted across clusters. The aim is achieved by using a new method to determine the best time for updating or exchanging control overhead messages between the primary node and its nearby node. The PISP packets is specifically developed to effectively distribute inquiry packets across networks, hence reducing the time needed for constructing routing tables and updating network topology.

References

1. Ioana-Victoria Nițulescu and Adrian Korodi. Supervisory control and data acquisition approach in node-red: Application and discussions. *IoT*, 1(1):76–91, 2020.
2. Neelakandan Subramani, Santhosh Kumar Perumal, Jagadish Shivappa Kallimani, Sakthi Ulaganathan, Sanjay Bhargava, and Sangeetha Meckanizi. Controlling energy aware clustering and multi-hop routing protocol for iot assisted wireless sensor networks. *concurrency and computation: practice and experience*, 34(21):e7106, 2022.
3. Michaelraj Kingston Roberts and Poonkodi Ramasamy. An improved high performance clustering based routing protocol for wireless sensor networks in iot. *Telecommunication Systems*, 82(1):45–59, 2023.
4. Tania Taami, Sadoon Azizi, and Ramin Yarinezhad. An efficient route selection mechanism based on network topology in battery-powered internet of things networks. *Peer-to-Peer Networking and Applications*, 16(1):450–465, 2023.
5. J Vijitha Ananthi and P Subha Hency Jose. Performance analysis of clustered routing protocol for wearable sensor devices in an iot-based wban environment. *Intelligent Technologies for Sensors: Applications, Design, and Optimization for a Smart World*, page 253, 2023.
6. Chettan Rajan Dongarsane, D Mahesh Kumar, and Swati Sankpal. Performance evaluation of sa-la routing protocol for wsn integrated iot. *Suranaree Journal of Science & Technology*, 30(2), 2023.

7. Rakesh Kumar Lenka, Manjur Kolhar, Hitesh Mohapatra, Fadi Al-Turjman, and Chadi Altrjman. Cluster-based routing protocol with static hub (crpsh) for wsn-assisted iot networks. *Sustainability*, 14(12):7304, 2022.
8. Shun Yang, Xian'ai Long, Hao Peng, and Haibo Gao. Optimization of heterogeneous clustering routing protocol for internet of things in wireless sensor networks. *Journal of Sensors*, 2022:1–9, 2022.
9. Maryam Shafiq, Humaira Ashraf, Ata Ullah, Mehedi Masud, Muhammad Azeem, NZ Jhanjhi, and Mamoona Humayun. Robust cluster-based routing protocol for iot-assisted smart devices in wsn. *Computers, Materials & Continua*, 67(3), 2021.
10. Sankar Sennan, Youseef Alotaibi, Digvijay Pandey, Saleh Alghamdi, et al. Eacr-leach: Energy-aware cluster-based routing protocol for wsn based iot. *Computers, Materials & Continua*, 72(2), 2022.
11. Muhammad K Khan, Muhammad Shiraz, Qaisar Shaheen, Shariq Aziz Butt, Rizwan Akhtar, Muazzam A Khan, and Wang Changda. Hierarchical routing protocols for wireless sensor networks: functional and performance analysis. *Journal of Sensors*, 2021:1–18, 2021.
12. Jian Shen, Anxi Wang, Chen Wang, Patrick CK Hung, and Chin-Feng Lai. An efficient centroid-based routing protocol for energy management in wsn-assisted iot. *Ieee Access*, 5:18469–18479, 2017.
13. Milad Mohseni, Fatemeh Amirghafouri, and Behrouz Pourghebleh. Cedar: A cluster-based energy-aware data aggregation routing protocol in the internet of things using capuchin search algorithm and fuzzy logic. *Peer-to-Peer Networking and Applications*, 16(1):189–209, 2023.
14. Himani K Bhaskar and AK Daniel. Energy-efficient multilevel routing protocol for iot-assisted wsn. In *Proceedings of International Conference on Recent Trends in Computing: ICRTC 2022*, pages 615–626. Springer, 2023.
15. Li Dong-liang, Lu Bei, and Wang Hai-hua. The importance of nature-inspired metaheuristic algorithms in the data routing and path finding problem in the internet of things. *International Journal of Communication Systems*, 36(10):e5450, 2023.
16. S Balakrishnan and K Vinoth Kumar. Hybrid sine-cosine black widow spider optimization based route selection protocol for multihop communication in iot assisted wsn. *Tehnički vjesnik*, 30(4):1159–1165, 2023.
17. P Paruthi Ilam Vazhuthi, A Prasanth, SP Manikandan, and KK Devi Sowndarya. A hybrid anfis reptile optimization algorithm for energy-efficient inter-cluster routing in internet of things-enabled wireless sensor networks. *Peer-to-Peer Networking and Applications*, 16(2):1049–1068, 2023.
18. Naveen Gandhi Anbullam and Joe Prathap Pathrose Mary. A survey: Energy efficient routing protocols in internet of things (iot). In *AIP Conference Proceedings*, volume 2854. AIP Publishing, 2023.
19. Sercan Yalçın and Ebubekir Erdem. Teo-mcrp: Thermal exchange optimization-based clustering routing protocol with a mobile sink for wireless sensor networks. *Journal of King Saud University-Computer and Information Sciences*, 34(8):5333–5348, 2022.
20. Hassen A. Mogaibel and Majed Hashim. Maximum throughput first access point selection scheme for multi-rate software-defined wireless network. In *International Journal of Computer Networks & Communications (IJCNC)*, volume 15, pages 115 –134, 2023.
21. X. Zeng, R. Bagrodia, and M. Gerla. Glomosim: a library for parallel simulation of large-scale wireless networks. In *Proceedings. Twelfth Workshop on Parallel and Distributed Simulation, 1998. PADS 98.*, pages 154–161. IEEE, 1998.
22. R. Dube, C. Rais, K. Wang, and S. Tripathi. Signal stability-based adaptive routing (ssa) for ad hoc mobile networks. In *Personal Communications, IEEE*, volume 4, pages 36–45. IEEE, 1997.
23. C. Toh. A novel distributed routing protocol to support ad-hoc mobile computing. In *Conference on Computers and Communications, 1996., Conference Proceedings of the 1996 IEEE Fifteenth Annual International Phoenix*, pages 480–486. IEEE, 1996.
24. D. Johnson, D. Maltz, and J. Broch. Dsr: The dynamic source routing protocol for multi-hop wireless ad hoc networks. *Ad hoc networking*, 5:139–172, 2001.
25. D. Kim, J. Garcia, and K. Obraczka. Routing mechanisms for mobile ad hoc networks based on the energy drain rate. *IEEE Transactions on Mobile Computing*, 2(2):161–173, 2003.
26. D. Park and M. Corson. A highly adaptive distributed routing algorithm for mobile wireless networks. In *Proceedings of Conference of the IEEE Computer and Communications Societies. Driving the Information Revolution (INFOCOM) Sixteenth Annual Joint*, page 1405. IEEE Computer Society, 1997.
27. J. Moy. Link-state routing in routing in communications networks. http://www.faqs.org/rfcs/rfc2328.html, 1995. M.E. Steenstrup, Prentice Halls.
28. P. Narula, S. Dhurandher, S. Misra, and I. Woungang. Security in mobile ad-hoc networks using soft encryption and trust-based multi-path routing. *Computer Communications*, 31:760–769, 2008.
29. C. Dhote, M. Pund, R. Mangrulkar, and R. Makarand. Article: Hybrid routing protocol with broadcast reply for mobile ad hoc network. *International Journal of Computer Applications*, 1(10):108–113, 2010. Published By Foundation of Computer Science.

30. E. Baccelli and J. Antonio. Ospf over multi-hop ad hoc wireless communications. *International Journal of Computer Networks & Communications IJCNC*, 2(5):37–56, 2010.
31. BM Shruthi and Channakrishna Raju. A comprehensive analysis on trust based secure routing protocol used in internet of things (iots). In *2023 International Conference on Applied Intelligence and Sustainable Computing (ICAISC)*, pages 1–4. IEEE, 2023.
32. J. Broch, D. Maltz, D. Johnson, Y. Hu, and Jetcheva. A performance comparison of multihop wireless ad hoc network routing protocols. In *Proceeding of International Conference Mobile Computing and Networking (MobiCom) ACM*, pages 85–97, 1998.
33. W. Wei and A. Zakhor. Multipath unicast and multicast video communication over wireless ad hoc networks. In *Proceedings. First International Conference on Broadband Networks,BroadNets*, pages 496–505. IEEE, 2004.
34. Abdelkader Benelhouri, Hafida Idrissi-Saba, and Jilali Antari. An evolutionary routing protocol for load balancing and qos enhancement in iot enabled heterogeneous wsns. *Simulation Modelling Practice and Theory*, 124:102729, 2023.
35. Puput Dani Prasetyo Adi and Akio Kitagawa. Quality of service and power consumption optimization on the ieee 802.15. 4 pulse sensor node based on internet of things. *International Journal of Advanced Computer Science and Applications (IJACSA)*, 10(5):144–154, 2019.

7 Acknowledgments

This research was supported and funded by Arab Open University-Kuwait Branch under decision number 23024

Authors

Radwan Abujassar is currently Associate professor at the Information Tecnology and Computing (ITC) Faculty at Arab Open University which is following the OU University in UK. Dr Radwan was in the computer Engineering department of the faculty of Engineering at the Bursa Orhangazi University in Turkey. Dr. Radwan received his B.Sc. degree from Applied Science University, Amman, Jordan in 2004, and M.Sc. degree from New York Institute of Technology in 2007, both in computer science. His Ph.D. degree in computing and electronic in the field of IP recovery in IGP and MANET networks from University of Essex, UK in 2012. His research interests include Network and Controls, Routing Protocols, Cloud Computing and Network security.