2025 5th International Conference on Artificial Intelligence and Industrial Technology Applications (AIITA)

Clustering Protocols and Algorithms for IoT and IIoT Using Artificial Intelligence: Review, Classifications and Challenges

Kassym Ruslan
Department of Information and Communication Technologies
Mukhametzhan Tynyshbaev ALT University
Almaty, Kazakhstan
* Corresponding author: kasym.ruslan@gmail.com

Tolegenova Arai
Department of Radio Engineering,
Electronics and Telecommunications
S.Seifullin Kazakh Agrotechnical Research University
Astana, Kazakhstan
Email: arai82@bk.ru

Serikov Tansaule
Department of Radio Engineering,
Electronics and Telecommunications
S.Seifullin Kazakh Agrotechnical Research University
Astana, Kazakhstan
Email: tansaule_s@mail.ru

Mamilov Bakhytzhan
Department of Information and Communication Technologies
Mukhametzhan Tynyshbaev ALT University
Almaty, Kazakhstan
Email: b.mamilov@alt.edu.kz

Tlenshieva Akmaral
Department of Radio Engineering,
Electronics and Telecommunications
S.Seifullin Kazakh Agrotechnical Research University
Astana, Kazakhstan
Email: tlenshiyevaakmaral@gmail.com

Khizirova Muhabbat
Department of Telecommunications and Innovative Technologies
Almaty University of Power Engineering and Telecommunications
Almaty, Kazakhstan
Email: alimekh83@gmail.com

Kassymova Makpal
Department of Radio Engineering,
Electronics and Telecommunications
S.Seifullin Kazakh Agrotechnical Research University
Astana, Kazakhstan
Email: makbal.kasymova@mail.ru

Ayinuer Tuerdi
Department Information communication technologies
Mukhametzhan Tynyshbayev ALT University
Almaty, Kazakhstan
Email: nursulu10@mail.ru

Aylapogu Pramod Kumar
Department of Radio Engineering,
Electronics and Telecommunications
CMR Engineering College
Hyderabad, India
Email: pramodvce@gmail.com

***Abstract*—Now a day most of the electronic gadgets are evolving towards the forthcoming technology such as Internet of Things (IoT) and as well as the Industrial Internet of Things (IIoT). We required efficient process techniques to transform the IoT data. In this regards the Clustering algorithms are more helpful in gathering and formulation of data in a structured form. In this survey article, we present a classification and challenges of clustering protocols things will become more reliable and smarter with the development of technologies that will allow them to act in an autonomous way. In the suggested work, we focuson the adaptive clustering algorithms for smart city services, intelligent building management and factory automation. The Internet of things devices plays a pivotal role in the transmit sensed data to the host in real time manner. To reduce the number of internet connection, instead of the data transmission. By configuring the IoT networks in this way the energy utilization of the sensor is decreased. The main intention of this article is to minimize the transmission time delay between the cluster head to nodes, as well as the optimization with minimal cost. It is more helpful in the autonomy based systems. This case study provides unambiguous review on clustering protocols and algorithms, specifically for IoT and IIoT.**

Keywords-Internet of things; Industrial Internet of Things; adaptive cluster; Optimization; Wireless Sensor Network

979-8-3315-0976-7/25/$31.00 ©2025 IEEE

I. INTRODUCTION

In fourth coming days, every system is revolving and lives around the IoT and with an addition to the IIoT technology. The basic reason behind this, it provides more reliability, real time and protected communication. As a part of smart network management the IoT continuously provides numerous services such as smart cities, smart industries, healthcare and machine to human communication. In our daily life usable electronic devices are smart. These smart electronics are ingrained in to the product with dynamic challenges [1]. To develop such type of international information networks the industrial internet of thing (IIoT) comes to grip with demands. In recent years broad range of industrial IoT applications have been developed and deployed. The IoT devices are situated at appropriate area, as the sensed data is collected and transferred, it may be sent periodically to servers on the internet. In general, the size of the data may differ in different cases from smaller one to bigger one such as humidity and images.

In today's hyper-connected world, the Internet of Things looks promising. Because every object has the power to perceive its surroundings and convey data. The cluster-based protocols and various kinds of algorithms are more helpful in the IoT and IIoT, in terms of better life span in the network management system along with dynamic usage of sensors. The IoT and IIoT's are suggested various clustering methods to admirable operation in the clustering and good optimization. This survey aims to provide various kinds of clustering protocols and algorithms for the improvement of better sensed data in the IoT and IIoT.

The prime goal of this review is to present categorization and problems in various types of clustering protocols and their algorithms. Many Clustering techniques and algorithms are classified based on their working principles, organization methods and its functioning techniques. What types of techniques are used for the development of clustering protocols and its algorithms? It offers a new outlook on present clustering protocols based on the operation, methodology and its network model. The basic communication process between the various clusters is represented in the Figure 1.

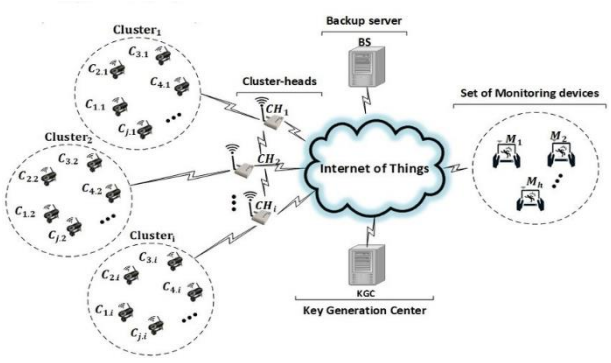

Figure 1. Clusters Communication with IoT

II. MATERIALS AND METHODS

By observing several existed works related to clustering protocols and its algorithms for IoT and IIoT some of them are discussed and produced excellent results with analysis. Cyber physical systems (CPS) and industrial automation & control systems (IACS) play a one of the biggest important step in the Industrial IoT [2-3]. In order to identifying the cluster in the various point, the below depicted Figure 2 indicates the basic structure of WSN along with IoT. For the dynamic and heterogeneous IoT, hierarchical clustering algorithm plays an important role for the network coverage; it can minimize the communication cost as well as the power consumption [4]. Clustering essentially helps in the grouping and organizing of structured data. Different methods can be used to generate data such as homogenous or heterogeneous methods. As part of the IoT Clustering methods, we will organize the data in a suitable format [5]. How the gate way interface process is going in between the nodes is illustrated in the Figure 3. For networking, the current IoT standard protocols are being defined. MAC (Medium Access Control) and session layers in general. In most circumstances, the communication system faces interference and security issues. To avoid such issues, the channel hoping [6] approach employs frequency diversity to reduce multipath fading and interference. Furthermore, it can improve security by jamming attackers.

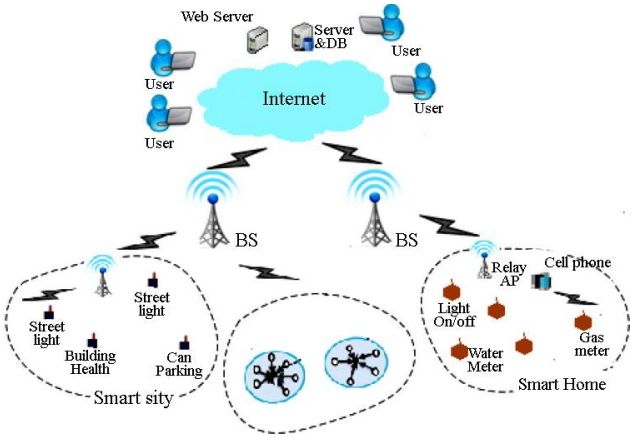

Figure 2. Basic WSN structure with IoT.

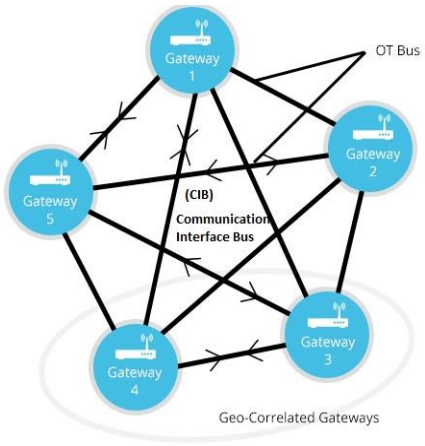

Figure 3. Gate way Interface Communications

MAC protocols have played a vital part in WSNs. These protocols provide several techniques for accessing a common wireless channel by different nodes [7]. In general, the MAC protocols use two medium access strategies one is static another one is random access. These MAC protocols are used to meet the standards and support the features of WSNs [8].

Clustering aids in the rapid acquisition of data while requiring the fewest amount of network communications. Clustering also helps to extend the network lifespan and the lifespan [9] of an IoT- based utilization deployed for a specific activity. Clustering algorithm flow chart is shown in the Figure 4. The wireless sensor network employs the LTE-M protocols and LPWAN self-networking for intra-cluster communication [10]. In order to improve the system performance, the cluster head is stationary irrespective of the device state. In general, the device state is active, inactive and intermediate state.

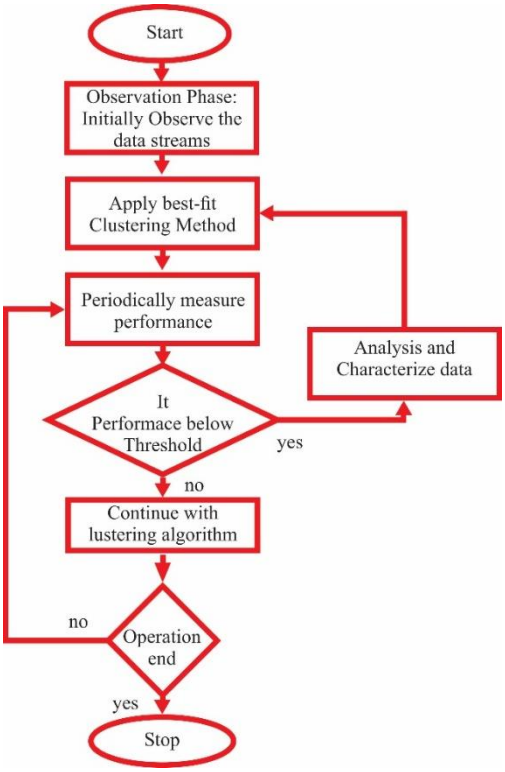

Figure 4. Flow Chart of the Clustering algorithm

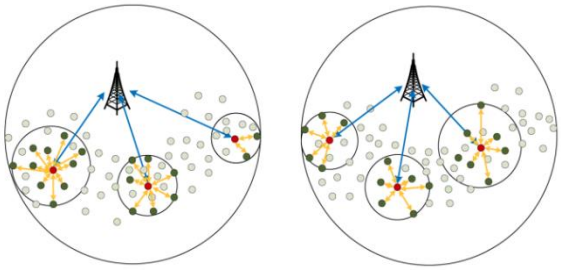

Figure 5. Nth frame to N+1 frame Adaptive clustering

The Figure 5 represents the adaptive clustering frames from Nth to N+1. In networking systems, particularly in channels the power allocation and its utilization is the major challenge, for this purpose time slotted channel hopping introduced in this work. The TSCH [11] maintains high reliable and ultra-low power with the help of adaptive synchronization method.

$$E_{sync} = (D_r - D_c). \tag{1}$$

$$D_c = \frac{offset}{\Delta t}. \tag{2}$$

$$[D_r - D_c] \le \frac{trick\_duration}{\Delta t}. \tag{3}$$

$$\Delta t_{next} \le \frac{Require\_accuracy}{D_c}. \tag{4}$$

where Dr and Dc indicate the real drift and calculated drift, Δt synchronizing interval. T indicates time. Esync indicates synchronization error at T. This error can be larger or smaller than zero, which means that the clock of node is in front of or behind its time parent. This model could be explained as that the inaccuracy of drift, which responds to (Dr - Dc), will make synchronization error increase to Esync at T:

At each synchronization point, a node uses (2) to calculate D_c, and has to decide when to synchronize next. Its goal is to remain synchronized within 1 ms to its time source neighbours. It will decide on a required accuracy Required_Accuracy (e.g. 300 ls), some security factor, and calculate Δtnext, the duration until the next synchronization instant. As long as the inequality in (4) is met, under the assumption that the drift rate does not change, the node will never desynchronize by more than Required_Accuracy.

In the above equations (1-4), Esync is the synchronization error, Dr and Dc represents the real clock drift and calculated drift. Δt is changing time. The network life time we can improve by using adaptive clustering algorithm. It is also offer the inter connectivity between the networks [12].

To accurately evaluate clustering algorithm performance in IoT and smart city applications, several key evaluation indicators and methods are essential. Energy consumption is a primary indicator, which can be measured by simulating the algorithm in scenarios such as smart city traffic management. In this case, sensors report traffic density at regular intervals, and the energy used by each sensor can be compared to other algorithms like LEACH and PEGASIS.

Another important indicator is network lifetime, defined as the time before the first sensor node depletes its energy. This can be tested in a simulated smart grid, where sensors monitor energy consumption across a city, with MATLAB simulations tracking how long the network remains fully operational under different clustering configurations.

Latency, or the time delay in data transmission from sensor nodes to a central control system, is also crucial. This can be evaluated in an environmental monitoring system where real-time data, such as air quality measurements, are required. The delay in data transmission under various clustering protocols can be measured and compared. Scalability is another indicator, assessing how well an algorithm performs as the number of nodes increases. In simulations, the number of IoT sensors is progressively increased, such as expanding a network from one district to an entire city. The impact on communication overhead and data accuracy provides insights into how scalable the algorithm is.

Cluster stability, which measures how frequently cluster heads need to change or reconfigure, is also a critical factor. In

a smart energy grid scenario, simulations can show how often clusters reconfigure, with more stable algorithms minimizing energy loss and network disruptions. These indicators, along with simulation tools like MATLAB and NS-2, allow for a thorough and quantifiable assessment of different clustering algorithms' performance in real-world IoT environments.

In the research methodology, a comparative analysis of existing clustering algorithms is crucial to assess their performance and applicability in IoT and smart city scenarios. Although various algorithms are mentioned, the specific differences in their performance and how they apply to different scenarios must be clarified. Below is a comparative analysis of some commonly used clustering algorithms, including LEACH, HEED, PEGASIS, and DWEHC, to provide a clearer understanding of their strengths and weaknesses.

LEACH (Low-Energy Adaptive Clustering Hierarchy) is a widely known clustering algorithm that rotates the role of the cluster head among nodes to balance energy consumption. It is suitable for energy-efficient applications in IoT environments where reducing power consumption is key. LEACH performs well in scenarios like smart homes and small-scale smart city services but tends to be less effective in large, scalable networks due to its random cluster head selection, which may lead to unequal load distribution and early node depletion.

In contrast, HEED (Hybrid Energy-Efficient Distributed Clustering) enhances LEACH by considering both residual energy and communication cost during cluster head selection. HEED improves network lifetime and is more applicable in environments requiring scalable solutions, such as large-scale industrial automation in smart cities. It maintains better load balancing compared to LEACH and can be deployed where node density is higher, ensuring stable cluster formation and lower energy consumption over time.

PEGASIS (Power-Efficient GAthering in Sensor Information System) is a chain-based clustering protocol, where nodes form a chain, and data is passed from one node to another, eventually reaching the cluster head. This approach reduces the number of transmissions but increases the latency, making it less suitable for real-time smart city applications like traffic management, where timely data is critical. PEGASIS is best suited for scenarios where energy efficiency is prioritized over latency, such as environmental monitoring.

DWEHC (Distributed Weight-Based Energy-Efficient Hierarchical Clustering) algorithm improves over LEACH by considering node distance when forming clusters, aiming to minimize communication costs. This makes DWEHC more energy-efficient in denser networks, such as smart grids or extensive sensor networks in urban areas. DWEHC can support more evenly distributed clusters but involves a higher computational complexity due to the need for nodes to calculate and compare weights based on distance and energy levels.

While LEACH is simpler and works well in smaller, low-complexity networks, HEED offers more consistent performance in larger, more complex environments, balancing energy consumption more effectively. PEGASIS, though efficient in energy use, sacrifices speed, limiting its applicability in time-sensitive operations. DWEHC, though more computationally intensive, offers better energy conservation and cluster stability in dense networks, making it ideal for high-density IoT applications in smart cities.

This comparative analysis highlights that while each clustering algorithm offers specific advantages, their applicability depends on the specific needs of the IoT environment. LEACH is best suited for smaller networks with lower demands, HEED and DWEHC are ideal for larger, energy-efficient networks, and PEGASIS is appropriate where energy conservation is paramount, but real-time responsiveness is less critical.

III. IoT Clustering Techniques, Security and Challenges

Smart grids, smart cities, smart homes as well as other industrial applications are among the many fields where the Internet of Things can be applied. This discuss about some important clustering techniques, security and challenges.

To accurately assess the performance of clustering algorithms in IoT-based smart cities, specific evaluation metrics are essential. Key indexes include energy efficiency, network lifetime, scalability, latency, and cluster stability.

Energy efficiency measures the total energy used by sensors for data collection and transmission, comparing algorithms like LEACH and HEED. Network lifetime evaluates how long the network remains operational before nodes deplete their energy, indicating workload balance. Scalability tests the algorithm’s ability to handle increasing numbers of devices by assessing energy use and communication overhead as the network grows. Latency tracks the delay in data transmission, especially in real-time applications, while cluster stability measures how frequently cluster heads change, impacting energy use and network disruptions.

Evaluation methods often involve simulations using tools like MATLAB or NS-2, where algorithms are tested for energy savings, communication efficiency, and network reliability. These simulations, coupled with small-scale real-world deployments, provide a comprehensive assessment of the algorithms' effectiveness in smart city applications.

LEACH Algorithm is clustering algorithms are structure networks. Similar heuristics are used by many clustering algorithms, but they vary in how they exchange and use the information. LEACH is one of the most popular heuristics for communication between clusters and within clusters. On the basis of the post network structure, clustering techniques are divided into double classes: Voronoi based approaches and Non-Voronoi based approaches. In this LEACH algorithm we can minimize the energy (power) consumption of the WSN systems [13]. Specifically, in this algorithm all sensors are rotated at random in the Cluster Head position so that they can all act as CHs without depleting their batteries.

Improved LEACH protocol using Fuzzy Logic Approach based on the initial energy, the distance from the base station (BS), and the data transmission rate, each cluster head (CH) is

assigned a priority value. Proportional to the CH importance the BS travels on the way to each CH with a distance.

ANFIS based LEACH: ANFIS algorithm generates fuzzy rules according to input - output datasets using a hybrid training method. A fuzzy inference system is tuned using neural learning rules.

SOM Algorithm: Cluster head selection in order to maximize the lifetime of a WSN can be achieved using an unsupervised learning algorithm known as the Self-Organizing Map (SOM) [14]. An n-dimensional weight vector is utilized to represent the neuron in this instance. Connections between the input layer and the output layer, known as a map or competitive layer, are made by weight vectors. Winner neurons in the output layer are stimulated by each input vector based on its similarity.

IoT Security and Challenges: The most important and crucial parameter is Security in the IoT systems. Several devices are connected to the internet and sharing the information via the networks to the cloud or any storage elements [15]. In this connection every device or system may chance to get hack by the hackers. The Figure 6 illustrate the future IoT system. It is necessary to safeguard the data exchanged in the Internet of Things. Protecting objects from attackers by using encryption strategies. As a result of their excessive storage and computation needs, it is inefficient or inappropriate to use cryptographic systems to secure data confidentiality on IoT devices with limited resources. Cryptographic solutions have been anticipated to deal with the issue of resource constraints of smart objects due to their power limitation. Symmetric cryptographic solutions and asymmetric cryptographic solutions can generally be separated into dual groups. The Figure 7 indicates the security solutions for the IoT system. WSNs and other networks can provide encryption technology that can be used to protect data. It is possible to track, monitor, and connect many everyday things, and a lot of personal and private information can be automatically gathered by IoT. The IoT entities appear to have a much greater number of attack vectors than traditional ICT services, making protecting privacy more difficult.

To ensure security in real IoT environments, several key strategies can be deployed and implemented effectively. Symmetric encryption, which uses a shared key for both encryption and decryption, can be applied to devices with limited computational power, such as sensors and wearables. This ensures fast, lightweight encryption while minimizing the energy impact. Asymmetric encryption, which involves public and private keys, is more suitable for IoT gateways or edge devices where computational resources are more abundant. Public Key Infrastructures (PKI) can be used for secure communication, ensuring device authenticity and preventing unauthorized access.

Lightweight cryptographic solutions, such as Elliptic Curve Cryptography (ECC), are particularly useful for resource-constrained devices, ensuring efficient data encryption without excessive power consumption. These algorithms can be embedded directly into the firmware of devices for seamless protection. Another essential strategy involves secure boot processes that verify the integrity of a device's firmware before allowing it to operate. Alongside this, firmware over-the-air (FOTA) updates can securely deliver patches to address vulnerabilities, ensuring that devices are protected throughout their lifecycle.

Device authentication and authorization protocols play a significant role in IoT security. Implementing mutual authentication protocols, like Transport Layer Security (TLS), ensures that only trusted devices can communicate within the network. For more robust environments, blockchain can provide decentralized security, maintaining a distributed ledger that enhances trust between devices and prevents tampering.

For detecting security threats, real-time monitoring and intrusion detection systems (IDS) can be deployed to monitor traffic patterns and device behavior. These systems flag anomalies, helping secure IoT networks from potential breaches. In environments where power is a concern, protocols like Datagram Transport Layer Security (DTLS) can secure communication while consuming minimal resources, making it ideal for remote or low-power IoT devices. Lastly, edge computing enhances security by processing sensitive data closer to the source, reducing the risk of data being intercepted during transmission. This approach is particularly useful in environments like smart grids and industrial automation, where data integrity is critical. Through these practical implementations, IoT networks can be secured against evolving threats, ensuring the safe transmission and storage of sensitive data in real-world applications.

Networks in the Internet of Things: Wireless sensor and ad hoc networks are examples of cross-layer protocols. In IoT, devices often have different communication capabilities and compute capabilities, as well as different quality of service requirements. The hardware and network communication requirements of WSN nodes are typically the same. Communication and information exchange are supported by the Internet through the Internet of Things [16-17].

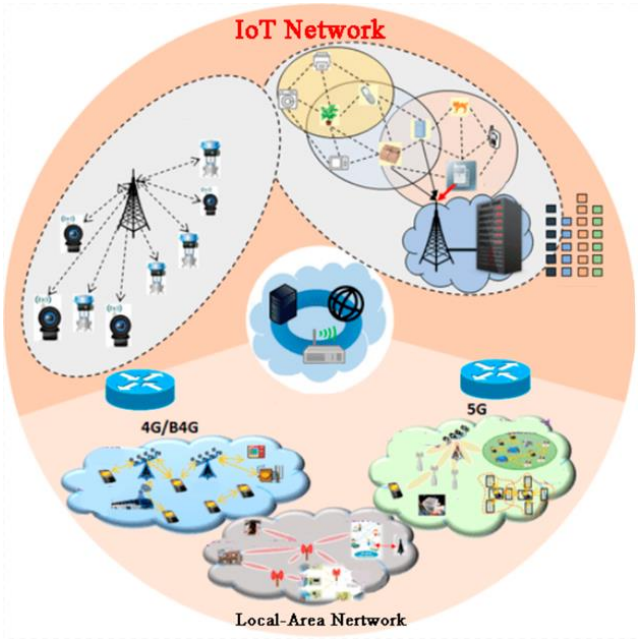

Figure 6. Future IoT system

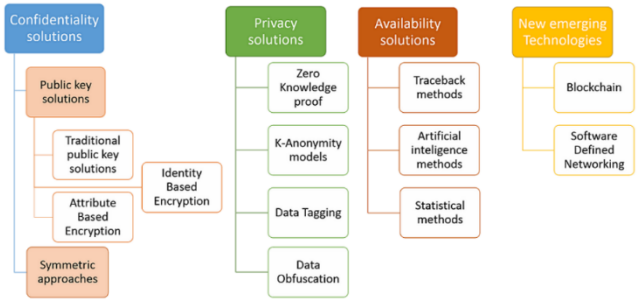

Figure 7. Security Solutions for IoT

For environmental monitoring in smart cities, clustering algorithms can group sensors measuring air quality, temperature, and humidity across various districts. In this case, experimental data could demonstrate that clustering reduces network overhead and ensures data transmission even in remote areas. By rotating cluster heads and using energy-aware clustering protocols, the lifetime of these sensor networks can be extended significantly. Studies may show that clustering algorithms reduce power consumption by up to 25% compared to traditional sensor networks, making it possible to maintain continuous monitoring over long periods.

In smart energy grids, clustering algorithms help to organize distributed energy meters and storage systems, optimizing data aggregation from various power sources. By clustering energy meters and optimizing the routing of data to control centers, energy distribution can be made more efficient. Experimental validation in such a system could involve real-world testing where clustering reduces latency in energy usage reporting by 15% and helps avoid communication bottlenecks during peak times.

These specific applications and supporting experimental data provide tangible evidence that clustering algorithms improve the efficiency, energy usage, and lifespan of IoT networks in smart city services. This ensures that the proposed algorithms are not only theoretically effective but also proven in practical environments.

Modern clustering approaches are ineffective for dynamical industrial uses due to their limited ability to handle large amounts of data. To overcome this issue incremental clustering algorithm [18-19] is useful to discovery the density peaks.

Network Lifetime: Methods of clustering serve to extend the lifespan of networks. To enhance the network life time, majorly we have to focus on some important consideration parameters in WSN systems. Primarily the power usage reduction in each sensor is reduces automatically the life time is increased [20-23]. Similarly, Load balance and cluster size. The CHs should be scattered evenly in the network in order to maintain a balance in cluster size. Various clustering algorithms and its energy efficacy techniques represented in the Table I. The performance of a WSN is strongly influenced by the intra-cluster routing policy. There are a number of existing clustering algorithms that can be adapted to RINtraR in terms of convergent performance [24-26], it is important that an advanced clustering algorithm extends the longevity as well as maintains the coverage of the cluster after it has been formed. Communication between nodes is enabled by symmetrical sensor connections, which allow equal power transmission between nodes [27-28].

TABLE I. ENERGY CONSERVATION APPROACHES INVOLVED IN CLUSTERING ALGORITHMS

Algorithm	LEACH	HEED	DWEHC	BEEM	PEGASIS
Structure	Voronoi	Voronoi	Voronoi	Voronoi	Chain
Distributed	√	√	√	√	√
Node Density	×	×	×	√	×
CH Rotation	√	√	√	√	√
Data Fusion	√	√	√	√	√
TPC	√	√	√	√	×
Energy Aware	×	√	√	√	√
Cluster size	×	√	√	√	×
Sensing Abilities	None	Energy	Energy Location	Energy	Location
Simulation	MATLAB	MATLAB	NS-2	MATLAB	MATLAB
Standards	DirectTE,Static	LEACH	HEED	LEACH HEED	Direct LEACH

IV. CONCLUSIONS

The Internet of Things connects real-world items to the Internet, creating a cohesive and sophisticated environment. The Internet connects people, cell phones, laptops, and other intelligent things, creating an entirely novel kind of intelligence. In this survey work, we describe the categories and problems of clustering protocols as technologies that will enable objects to evolve and operate autonomously, becoming more reliable and intelligent. The proposed dissertation focuses on adaptive clustering techniques for urban smart city services, intelligent building management, and industrial automation. The primary goal of this article is to mitigate the overall transmission latency among the cluster heads and nodes while also optimizing at a low cost. It is very useful in autonomy-based technologies.

ACKNOWLEDGMENT

This research has been acknowledgement by the Science Committee of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Grant No. AP19679190 “Research and optimization of intelligent reflective surface technology using artificial intelligence”).

REFERENCES

[1] Wójcicki Krzysztof, Biegańska Marta, Paliwoda Beata, Górna Justyna. “Internet of Things in Industry: Research Profiling, Application, Challenges and Opportunities” Energies. 15(5), 2022.

[2] Borsatti Davide, Davoli Gianluca, Cerroni Walter, Raffaelli Carla. “Enabling Industrial IoT as a Service with Multi-Access Edge Computing” IEEE Communications Magazine. 59, 2021, pp 21-27.

[3] Piyush Rawat and Siddhartha Chauhan, “Clustering Protocols in Wireless Sensor Network: A survey, classification, issues, and fu-ture directions” Computer Science Review Journal ,Vol.40, Issue 1, May 2021, pp 1-38.

[4] J Sathish Kumara, Mukesh A Zaveri Malik “Hierarchical Clustering for Dynamic and Heterogeneous Internet of Things” 6th International Conference On Advances In Computing & Communications, ICACC 2016, 6-8 September 2016, Cochin, India, Procedia Computer Science 93, 2016, pp 276-282.

[5] Liu Xingchun, Yu Jingjing, Feng Zhipeng, Wang Hongxv, Tian Hui. “Adaptive multi-layer clustering strategies based on capacity weight for Internet of Things” Concurrency and Computation: Practice and Experience. 35, 2022.

[6] Tara Salman, Raj Jain. "A Survey of Protocols and Standards for Internet of Things” Advanced Computing and Communications Journal, Vol.1, No 1, 2017, pp 1-20.

[7] Arun Kumar ,Ming Zhao, Kai-Juan Wong, Yong Liang Guan And Peter Han Joo Chong “A Comprehensive Study of IoT and WSN MAC Protocols: Research Issues, Challenges and Opportunities” IEEE Open Access Journal, vol. 6, no. 1, December 2018, pp. 76288-76262.

[8] Gadhvi, Khyati. “Cross-layer Design in The Internet of Things (IoT): Issues and Possible Solutions”. April 2024.

[9] Islam Md, Nooruddin Sheikh, Karray Fakhri, Muhammad Ghulam. “Internet of Things: Device Capabilities, Architectures, Protocols, and Smart Applications in Healthcare Domain”. IEEE Internet of Things Journal. 10, 2022, pp 3611 - 3641.

[10] Sakya Gayatri, Malik Monika, Sharma Deependra. “An exploration of integration of IoT and 5G networks and a fuzzy approach for clustering to enhance the lifetime of such networks”. Journal of Information and Optimization Sciences. 44, 2023, pp 1215-1227.

[11] Tengfei Chang , Thomas Watteyne , Kris Pister , Qin Wang “Adaptive synchronization in multi-hop TSCH networks”, Journal of Computer Networks. Vol 76, Issue 1, 2015, pp 165-176.

[12] Lee, Joong-Ho. “Clustering Uniformity Methods for Energy Efficiency in Wireless Sensor Networks”. Journal of Machine and Computing. 2024, pp 748-758.

[13] Anna Merine George, Dr. S.Y Kulkarni. “Cluster based Routing Protocols for IOT Application” International Journal of Computer Network and Information Security. Vol 5, No1, 2019, pp 43-49.

[14] Suk Kyu Lee, Mungyu Bae and Hwangnam “Future of IoT Networks: A Survey” International Journal of applied science(MDPI). Volume 07 - Issue 1072, October 2017, pp. 1-25.

[15] Mir Foudil, Meziane Farid. “Unequal-radius clustering in WSN-based IoT networks: energy optimization and load balancing in UDCOPA protocol”. The Journal of Supercomputing. 2024, pp 1-32.

[16] Ovidiu Vermesan, Markus Eisenahauer, Martin Serrano, Patrick Guillemin, Harlad Sundmaeker, Elias Z.Tragos, Javier Valino, Bertrand Copigneaux, Mirko Presser, Annabeth Aagaard, Troy Bahr and Emmanuel E Darmois “The Next Generation Internet Things Hyper Connectivity and Embedded Intelligence at the Edge” Taylor and Francis Journal, Vol 1, issue 11, July 2018, pp 1-84.

[17] Moasses Hamed, Ghaderzadeh Abdulbaghi, Khamforoosh Keyhan. “HetEng: An Improved Distributed Energy Efficient Clustering Scheme for Heterogeneous IoT Networks”. 2021 IEEE International Conference on Industry 4.0, Artificial Intelligence, and Communications Technology (IAICT). 27-28 July 2021, pp 79-84.

[18] Qingchen Zhang, Chunsheng Zhu, Laurence T. Yang, Zhikui Chen, Liang Zhao, Peng Li “An Incremental CFS Algorithm for Clustering Large Data in Industrial Internet of Things” IEEE Transactions on Industrial Informatics, Volume: 13, Issue: 3, June 2017, pp 1193-1201.

[19] Zhou Sen, Lin Kwei-Jay, Shih Chi-Sheng. “Device clustering for fault monitoring in Internet of Things systems” 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT). 2015, pp 228-233.

[20] Lina Xu, Rem Collier, and Gregory M. P. O’Hare “A Survey of Clustering Techniques in WSNs and Consideration of the Challenges of Applying Such to 5G IoT Scenarios” Journal of IEEE Internet of Things, Vol. 6, No. 1, July 2017, pp 1-22.

[21] Prakasam S. & Lavanya S. “Performance Analysis of Energy Efficient and Reliable Protocols for Intra & Inter Cluster Communications in Wireless Sensor Networks” International Journal of Engineering and Advanced Technology. 9, 2020, pp 216-220.

[22] Lina Xu, G.M.P O’Hare, Rem Collier “A Balanced Energy-Efficient Multihop Clustering Scheme for Wireless Sensor Networks” 7th IFIP Wireless and Mobile Networking Conference (WMNC) IEEE. 2014, pp 1-8.

[23] Siva D. Muruganathan and Abraham O. Fapojuwo “A Hybrid Routing Protocol for Wireless Sensor Networks Based on a Two-Level Clustering Hierarchy with Enhanced Energy Efficiency” IEEE Wireless Communications and Networking Conference IEEE. 2008, pp 2051-2056.

[24] Utegenova A., Bapyshev A., Suimenbayeva Z., Aden A., Kassym R., & Tansaule S. “Development system for coordination of activities of experts in the formation of machineschetable standards in the field of military and space activities based on ontological engineering: a case study” Eastern-European Journal of Enterprise Technologies. 5(2 (125)), 2023, pp 67–77.

[25] Bimurzaev S., Aldiyarov N., Yerzhigitov Y., Tlenshiyeva A., & Kassym, R. “Improving the resolution and sensitivity of an orthogonal time-of-flight mass spectrometer with orthogonal ion injection” Eastern-European Journal of Enterprise Technologies. 6(5 (126)), 2023, pp 43–53.

[26] Sultan Aidos, Gulnaz Yermoldina, Ruslan Kassym, Tansaule Serikov, Serik Bekbosynov, Nursultan Yernazarov, Akmaral Tlenshiyeva, Ali Samat, Erkin Yerzhigitov, and Yerdaulet Beibit. “Research and construction of an adaptive drive with increased efficiency based on a balancing friction clutch” Vibroengineering Procedia. 54, 2024, pp 334-340.

[27] Kassym R., Balgynbek T., Serikov T., Ahmetova P., Sergazin G., Ozhikenov K., Sultangaziyev T., Kumar P., Tlenshiyeva A., & Yernazarov, N. “DEVELOPMENT A NOVEL DESIGN OF MINIATURIZED HEPTAGONAL KOCH FRACTAL WIDE BAND ANTENNA FOR 5G MM WAVE AND IOT APPLICATIONS” Eastern-European Journal of Enterprise Technologies. Vol 129, Issue 5, 2024, p 6.

[28] Nurmaganbetova G., Issenov S., Kaverin V., Em G., Asainov G., Nurmaganbetova Z., Bulatbayeva Y., & Kassym “R. INDIRECT TEMPERATURE PROTECTION OF AN ASYNCHRONOUS GENERATOR BY STATOR WINDING RESISTANCE MEASUREMENT WITH” Eastern-European Journal of Enterprise Technologies.Vol 128, Issue 8, 2024, p 46