International Journal of Safety and Security Engineering
Vol. 14, No 3., June, 2024, pp. 999-1006
Journal homepage: http://iieta.org/journals/ijsse

Efficient and Secure Data Aggregation for Resource-Constrained IoT Environments

Abhijith H.V.

Department of Information Science and Engineering, JSS Academy of Technical Education, Bengaluru 201301, India

Corresponding Author Email: abhijithhv.mithra@gmail.com

https://doi.org/10.18280/ijsse.140329

Received: 18 March 2024
Revised: 2 June 2024
Accepted: 18 June 2024
Available online: 24 June 2024

Keywords:
data aggregation, resource constraints, efficiency, data compression, data transmission, data integrity, IoT (Internet of Things)

ABSTRACT

The Internet of Things (IoT) has ushered in an era of interconnected devices and sensors that generate vast amounts of data. While the potential of IoT is vast, resource- constrained IoT environments present unique challenges, particularly in the context of data aggregation. This research focuses on developing secure data aggregation scheme tailored to resource-constrained IoT environments. In these settings, limitations on processing power, memory, and bandwidth necessitate innovative solutions to ensure both the efficiency and security of data collection and transmission. This research proposes a comprehensive framework that optimizes data aggregation algorithms. The key objectives of this research are to enhance data aggregation efficiency by minimizing redundant data transfer, optimizing data compression, and reducing the burden on constrained resources. The findings of this research provide valuable insights for IoT applications operating under resource limitations. By improving the efficiency and security of data aggregation in resource-constrained IoT environments, this research contributes to the realization of the full potential of IoT technologies in scenarios where resources are limited.

1. INTRODUCTION

The Internet of Things (IoT) is ushering in an era of unprecedented connectivity, transforming the way data is generated and utilized across various domains. IoT systems, comprising a multitude of sensors and devices, have the potential to revolutionize industries, enhance quality of life, and advance our understanding of the world. However, this proliferation of data sources presents a significant challenge, particularly in resource-constrained IoT environments.

With the proliferation of internet-based systems like cloud computing and new wireless technologies, the Internet of Things (IoT) has flourished in recent decades, allowing us more freedom and convenience in our many everyday activities [1-4]. The Internet of Things (IoT) is a system of interconnected computing devices, services, and data stored in general purpose physical objects that may perform predefined tasks autonomously via the Internet and with little to no human interaction [5-7]. The Internet of Things (IoT) refers to the linking of several diverse systems over a network [8, 9]. Sense, networking, cloud computing, and applications are the four layers that make up the architecture of IoT-based systems [6, 10, 11]. Scalability and self- governing capabilities are provided by every layer of the Internet of Things architecture [12, 13]. What follows is an explanation of the Internet of Things' four-layer design.

Resource constraints, encompassing limitations in processing power, memory, and network bandwidth, are a defining characteristic of many IoT deployments. These constraints stem from the necessity for cost-effective, energy-efficient devices capable of operating in remote or hostile environments. As a result, traditional data aggregation techniques optimized for resource-rich environments fall short when applied in resource-constrained IoT contexts.

This research is driven by the urgent need for innovative data aggregation solutions that combine efficiency with security in resource-constrained IoT environments. The objective is clear: to enable the seamless and secure flow of data while respecting the constraints imposed by the edge devices and sensors in these settings [14, 15].

In this paper, we present a holistic approach to tackle this challenge. We propose a framework that leverages optimized data aggregation algorithms, efficient compression methods, and advanced encryption protocols to address the dual imperatives of efficiency and security. Our work seeks to bridge the gap between the potential of IoT data and the realities of constrained IoT environments.

The outcomes of this research not only promise to enhance the efficacy of data aggregation but also to bolster the security and privacy of sensitive information in resource-constrained IoT applications. The subsequent sections of this paper will delve into the specific challenges, methodologies, and results of our efforts, providing insights that are instrumental in unlocking the full potential of IoT technology in resource-constrained scenarios [16].

This work is a vital step toward a future where efficient and secure data aggregation becomes the cornerstone of resource-constrained IoT environments, enabling their widespread adoption and impact across a spectrum of industries and applications.

Efficiency in resource-constrained IoT environments is essential because it allows IoT applications to operate

effectively and reliably within the limitations of the available resources. By optimizing resource utilization, reducing data overhead, and ensuring timely data processing, efficient IoT solutions can maximize the benefits of IoT technology while mitigating the challenges posed by constrained resources [17, 18].

This paper contributes with an efficient data aggregation scheme which is based on spatial approach. This scheme reduces redundant data communications significantly. Section 2 of the paper provides literature review about the domain. Aggregation procedure is covered in section 3. Section 4 highlights the results and conclusion is provided in section 5.

2. RELATED WORK

Bhajantri and Mujawar [1] provided an overview of cloud computing security risks and defences Cloud computing gives internet-based access to servers, storage, applications, networking, and more. Cloud computing allows access to third-party cloud service providers' pooled resources. Its advantages include minimal operating costs, efficiency, scalability, and adaptability.

Lockl et al. [2] are the authors of the study. "Design principles for blockchain-based Internet of Things applications," published in the journal "Towards faith in Internet of Things ecosystems," The term "Internet of Things" (IoT) refers to the notion of physical items that are linked to the Internet and having the ability to identify themselves, sense their surroundings, network with other devices, and perform processing. The transmission of data to centralised servers in the cloud for processing is often the foundation around which Internet of Things architectures are built.

Apostolopoulos et al. [3] collaborated on this study. With regard to the Internet of Things, cognitive data unloading in edge computing for mobile devices Offloading data to servers that are part of Mobile Edge Computing (MEC) is an appealing option for Internet of Things (IoT) gadgets that have limited resources, as it helps to reduce the amount of computing effort that these devices experience. As a result of the fact that users' cognitive Internet of Things devices exhibit behaviour that is both loss averse as well as gain seeking, the purpose of this article is to examine the possibility of selective information offloading to media edge computing servers.

The work by Tange et al. [4] systematically assesses the safety requirements and opportunities for fog computing in commercial Internet of Things (IoT) applications. The concept of the Internet of Things (IoT) has a number of important applications, one of which is in industrial settings. In point of fact, the Industrial Internet of Things (IIoT), which is more commonly known as Industry 4.0, has the potential to revolutionise production and manufacturing by utilising a large number of networked embedded sensing devices and combining them with emerging computing technologies such as fog/cloud computing and artificial intelligence and other similar technologies.

Singh [5] suggested Internet-of-Things with blockchain technology: State-of-the-art and potential challenges.IoT stands for the Internet of Things, which refers to a category of cyber–physical platforms (CPSs) that have an impact on internet technology with the purpose of facilitating interactions among the physical and digital worlds. A more comprehensive shift towards the concept of pervasive or ubiquitous technology is presented.

Liu et al. [6] suggested a "dynamic duty cycle," and it is a technique that helps wireless sensor networks improve their latency and energy efficiency. As a result of the limitations of devices in terms of their capacity for computing and storage, conventional security methods encounter a great deal of difficulty throughout the procedure of data transfer. For the purpose of transferring data that is in an insecure network condition, networks need to spend more energy and have bigger transmission requirements.

A Cloud-based secure service providing for Internet of Things devices using blockchain proposed by Rehman et al. [7]. IoTs, which stands for the Internet of Things, are a rapidly expanding field in the current day. The Internet of Things (IoT) gadgets are becoming more popular as technologycontinues to progress. Nevertheless, there is a rise in the security concerns associated with the providing of services and the exchange of data. Several different security strategies are now in use. On the other hand, because to the restricted storage and compute resources that these techniques possess, they are not appropriate for Internet of Things devices.

Butun et al. [8] illustrated the security consequences of fog-based computing on the Internet of Things utilizing Internet of Things devices and sensors has quickly expanded, which has also produced an increase in the creation of data (information and logs), the utilisation of bandwidth, and other phenomena associated to the Internet of Things occurrences. When it comes to the Internet of Things (IoT), a standard specification for incorporating the use of fog computing is now in the process of developing.

A prospective architecture for blockchain-based management of heterogeneous IoT nodes, by Tseng et al. [9]. There's a chance that the Internet of Things will revolutionise our understanding of IT. A wide range of academic fields, including those concerned with communications, network security, business, and management, have conducted substantial research on the Internet of Things (IoT).

Singh et al. [10] presented a smart city infrastructure based on blockchain and fog technology for the internet of everything. The Internet of Everything (IoE) applications in smart cities employ fog computing (FC) to lower latency and energy usage for heterogeneous communication techniques. Both wireless and cable connections may be used by fog computing nodes. The development of the transaction linkage of instantaneous responses applications is the purpose of smart city applications.

Sharma et al. [11] presented a cloud storage using blockchain technology with comprehensive literature review. The importance of Blockchain technology and the high demand for new developments in the field have sparked ongoing research in a wide range of academic and professional disciplines. Despite its early stages of testing, the blockchain is seen as a forward-thinking solution to tackle modern tech issues including decentralisation, identification, trust, character, data ownership, and information-driven decisions.

Li et al. [12] provided an assessment of the current state of the art in industrial blockchain," As the underlying along with backbone technological advances of Bitcoin, Blockchain has garnered a lot of attention all over the world in recent years due to its distinctive qualities, which include decentralisation, openness, immutability, anonymity, and so on. These qualities enable Blockchain to establish a trust foundation by recording point-to-point decentralised transactions in an immutable manner through the attached timestamp, which in turn

improves system efficiency and reduces costs without relying on a central agent.

The work on exploring the Sustainable Development of the Intermediate Role in Blockchain was suggested by Tseng and Shang [13]. Cost, growth in markets, distribution channels, business relationships, and supply chain management are all components of traditional business models. A departure from the conventional style of operation has been brought about as a result of the growth of a digital economy as well as the technology of digital networks.

A specific to the application protocol architecture for wireless microsensor networks was published in the study of Heinzelman et al. [14].

The ability to effectively monitor a distant environment is made possible for users by networking collectively a large number of inexpensive microsensor nodes. This is accomplished by intelligently integrating the data from each of the nodes. In order to function properly, these networks need protocols for wireless communication that are not only energy efficient but also provide minimal latency.

A load-balanced node clustering strategy for wireless sensor networks employing an enhanced memetic algorithms based meta-heuristic technique was proposed by Chawra and Gupta in their work [15]. Issues with energy-holes and uneven load distribution plague the majority of currently-used node clustering techniques. The WSN's lifespan is drastically reduced as a result of these issues.

Venugopal et al. [16] proposed a Two-Hop Routing for WSNs Based on Link Reliability. Using memory and computationally efficient approaches, the protocol estimates the connection metrics and reduces package deadline miss ratio (DMR) despite addressing power efficiency, two-hop latency, and link dependability. The protocol leads to a longer lifespan for sensor networks and a reduced packet deadline miss ratio, according to numerical data.

A secured decentralised generic transaction ledger was suggested by Wood [17]. Global information transmission is now very inexpensive due to the widespread availability of internet connections throughout the globe. Bitcoin and other tech-based movements have proven that the internet can power a decentralised, globally accessible, and essentially free value-transfer system via consensus mechanisms, voluntary adherence to the social contract, and the power of default.

Improving energy efficiency using content-driven dynamic and adaptive scheduling in wireless sensor networks suggested by Khan et al. [18]. Wireless sensor networks (WSNs) are made up of small, inexpensive sensors that can sense, communicate, and do computation. The limited resources of these systems are a constant source of contention, with energy efficiency being the most contentious and important problem in WSNs.

Sert et al. [19] insisted on collecting data in multihop sensor networks with wireless connections made efficient using a two-tier decentralised fuzzy logic protocol, this is to make multihop WSN data combining procedures more efficient. For energy-efficient aggregation needs, clustering is a useful tool. Nodes that are part of a cluster send data packets to nodes that are at the head of the cluster, which in turn sends the data payloads to the base station for reception.

Sert and Yazici [20] suggested an increasing rule- based fuzzy clustering algorithms' energy efficiency for wireless sensor networks through the use of CLONALG-M. A significant amount of work has been spent realising and defining these functions since the majority of rule-driven fuzzy clustering systems use subject matter experts in trial-and-error procedures to find and specify the rules of fuzzy clustering as well as the types of membership functions thatexist at the output. Therefore, achieving an ideal fuzzy system is nearly impractical or unfeasible.

Sert et al. [21] worked on Security breaches and defence strategies in wireless sensor networks for surveillance. Wireless sensor networks (WSNs) that are primarily used for surveillance have several data collection needs, which lead to the creation of monitoring wireless sensor networks (SWSNs). The majority of SWSNs function by detecting their surroundings and sending the information they gather to a sink for use in decision-making procedures like event, item, or categorization identification.

Internet of Things-based clinical sensor management of data and transmission using blockchain technology was elaborated by Wang in his work [22]. As a result of the constant improvement that technology has made over the course of the last few years, the healthcare business has seen a number of groundbreaking changes. Several terrible illnesses have been made easier to treat thanks to advancements in technology such as the Internet of Things, computing via the cloud, blockchain-based technologies, lab-on-chip, non-invasive as well as minimally invasive operations, and so on.

A cloud-based versus blockchain-based Internet of Things and comparative survey was done by Memon et al. [23]. Its popularity has expanded as a result of technological improvements; nevertheless, problems and hazards associated with the Internet of Things are expanding significantly along with the surge in the number of devices that are linked to the internet.

A collaborative intrusion detection system that is enabled by a deep blockchain framework for the purpose of protecting Internet of Things and cloud networks was done by Alkadi et al. [24]. The incorporation of Blockchain technology with intrusion detection systems has been the subject of much study. The goals of these two technologies are to enhance data privacy and identify both present and future cyberattacks, respectively. Within the context of these methodologies, learning-based ensemble models have the potential to not only guarantee data privacy but also assist the detection of complicated harmful episodes.

The blockchain randomised neural network model for cybersecure IoT as well as 5G network infrastructure in smart cities was suggested by Serrano [25].

3. PROPOSED WORK

The proposed work aims to address the challenges of data aggregation in resource-constrained IoT environments by developing an efficient and secure data aggregation framework. Leveraging advancements in cryptography, data compression, and optimization techniques, the framework will prioritize energy efficiency and security while aggregating data from IoT devices with limited computational resources.

Key components of the framework include node deployment, network establishment, spatial aggregation and lightweight encryption algorithms to secure data transmission and lightweight authentication algorithm to avoid false alarms.

3.1 Symbols and notations

- *N*: IoT sensor node count.
- *Ni*: Index of a specific sensornode.
- *Di*: Raw data collected by sensor node *i*.
- *Cj*: Cluster formed by nodes in proximity or sharing similar characteristics.
- *Hj*: Cluster head responsible for aggregation in cluster *Cj*
- *Ei*: Energy level of sensor node *i*.
- *K*: Encryption key for secure communication.
- *H*(*Di*,*K*): Encryption function for data *Di* using key *K*.
- *Agg*(*Cj*): Aggregation function for cluster *Cj*.
- *Ri*: Resource utilization of sensor node *i*.
- transmit transmit: Time taken for data transmission.
- aggregate aggregate: Time taken for data aggregation.
- sleep*P*sleep: Power consumption during sleep mode.

3.2 Mathematical model

3.2.1 Data collection

In the context of efficient and secure data aggregation for resource-constrained IoT environments, the data collection process can be represented mathematically. Let's denote the raw data collected by a sensor node Ni as Di, which is a function f of sensor readings. The equation for data collection can be expressed as:

$$(sensor\ readings)Di = f(sensorreadingsi) \tag{1}$$

Here, sensor readings sensor readings i represents the specific measurements or observations gathered by the sensor node Ni. The function f encapsulates the transformation or processing applied to these raw sensor readings to generate the corresponding raw data Di.

The nature of f depends on the type of sensors and the data they are capturing (e.g., temperature, humidity, pressure).

The actual form of the equation will vary based on the characteristics of the sensor and the specific requirements of the IoT application. It could involve straightforward measurements, transformations, or even pre-processing steps to reduce the data size or enhance its quality before aggregation [20].

3.2.2 Cluster/grid formation

Let D be the set of distances between each pair of sensor nodes in the network, and T be a predefined threshold distance for cluster formation. The cluster formation process can be expressed as:

$$C_j = \left\{ n_i \in N | distance\left(n_i, n_k\right) \le T, \forall n_k \in N \right\} \tag{2}$$

This equation states that a cluster Cj consists of all sensor nodes (Ni) in the network (N) for which the distance to any other node (Nk) is less than or equal to the predefined threshold T. In other words, nodes within a certain proximity to each other are grouped into the same cluster.

The specific distance metric and clustering criteria may vary based on the requirements and characteristics of the WSN application. This equation provides a general representation of the cluster formation process, and the actual implementation may involve additional considerations such as energy levels, network connectivity, or node density [21].

3.2.3 Data encryption

Data encryption is a crucial aspect of securing data in a resource- constrained IoT environment. The Advanced Encryption Standard (AES) is commonly used for symmetric key encryption in such scenarios. Below is the encryption equation using AES-CCM (Counter with CBC-MAC) mode, a widely adopted mode for efficient and secure encryption in IoT.

The encryption equation for data Di using the AES-CCM mode can be expressed as follows:

$$C_i = \text{AES}-\text{CCM}_{\text{Encrypt}}\left(K, Nonce, D_i, A, M_i, L, T\right) \tag{3}$$

The AES-CCM encryption process involves combining the encryption key, nonce, data, associated data, and additional parameters to produce a secure and authenticated ciphertext. The authentication tag (T) is generated as part of the process, providing integrity and authenticity assurance.

It's important to note that the specific implementation details, such as key management, nonce generation, and parameter choices, depend on the cryptographic library or protocol being used in the IoT environment. Additionally, the use of secure key exchange mechanisms or pre-shared keys is essential to ensuring the confidentiality and integrity of the encryption process.

3.2.4 Aggregation scheme

The aggregation scheme involves combining data from multiple sensor nodes in a cluster to generate aggregated information. The specific equation for the aggregation scheme (Agg(Cj)) depends on the nature of the data and the desired form of aggregation. Here are a few examples of aggregation schemes along with their respective equations:

$$C_j : \text{Agg}\left(C_j\right) = g\left(\left\{D_i\right\}\right) \tag{4}$$

3.2.5 Dynamic routing

Dynamic routing in the context of IoT involves adapting the routing paths based on changing network conditions, resource availability, and energy levels of the nodes. The routing time in dynamic scenarios can be influenced by factors such as congestion, node mobility, and link quality. Below is a simplified equation to represent the dynamic routing time in a resource-constrained IoT environment:

$$T_{\text{dynamic routing}} = \alpha \cdot \frac{\text{Congestion Level}}{\text{Link Quality}} + \beta \cdot \frac{\text{Node Mobility}}{\text{Energy Level}} \tag{5}$$

This equation reflects the dynamic nature of routing adjustments, where the time taken for dynamic routing is influenced by both network congestion and the mobility of nodes. The weights α and β can be adjusted based on the specific importance of congestion and mobility in a given IoT scenario.

This is a simplified form, and the real implementation of routing that is dynamic may entail advanced algorithms and assumptions depending on the unique needs and features of the Internet of Things environment. It is crucial to note because this is a simplified structure [22].

3.3 Secure data aggregation framework architecture

Three different levels of nodes are deployed. Figure 1 shows

the conceptual framework implementation where data source is IoT devices or sensors which sends the data to aggregator node. Then aggregation technique will be implemented at the aggregator level. After aggregation data pass through security layer and privacy module. Figure 2 shows network architecture.

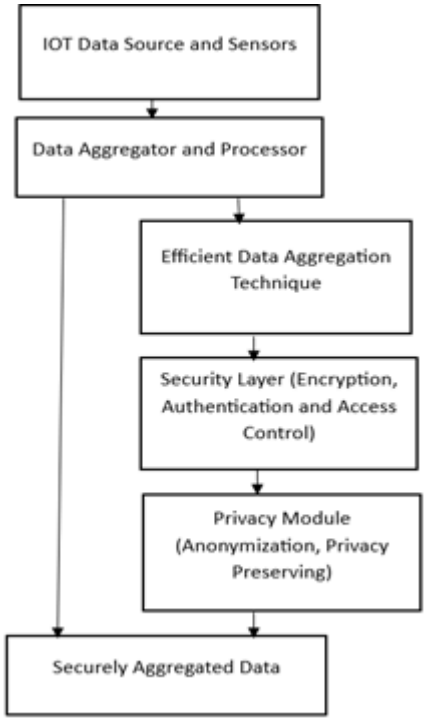

Figure 1. Conceptual framework implementation

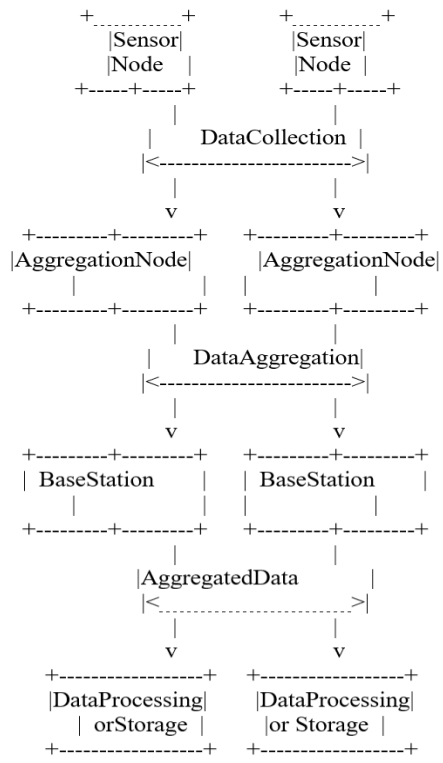

Figure 2. Network architecture

1) **Base level sensor nodes**: They are limited power sensor nodes which can sense and transfer the data to aggregator node.

2) **Aggregator nodes or grid head:** They are like cluster head or grid head. They collect and aggregate the data from multiple sensor nodes.

3) **Base Station:** They are at the top level of hierarchy, they receive aggregated data from aggregator node

3.4 Network establishment

Aggregator node initiates the Network establishment procedure with the base level sensor node. Figure 3 shows the network establishment between aggregator node and base level sensor node. Following are the steps involved in the network establishment procedure.

- Aggregator node broadcasts the Aggregator Advertisement (A-Adv) Packet to all the base level sensor nodes in the grid.
- Base level sensor node make an entry about the aggregator node in its memory and send Aggregator registration (A-Reg) Packet to aggregator node as a response to A-Adv Packet.
- Aggregator node make an entry about the base level sensor node in its grid table and send ACK Packet to base level sensor node to confirm that Network establishment is successful.

Similar procedure is carried out between aggregator node and base station for network establishment.

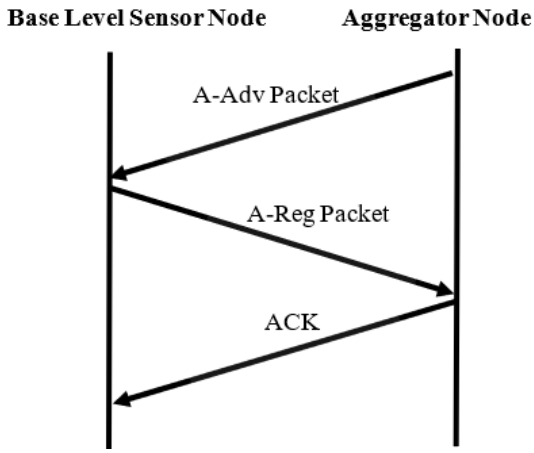

Figure 3. Network establishment

3.5 Aggregation procedure

Aggregation is performed at aggregator node only if the nodes has sent the data within event range and spatial aggregation is based on the number of nodes generating similar sensed value in a particular time interval. In proposed spatial aggregation, Rule based discission making model is used by aggregator node to decide whether data needs to be transmitted to next level or not. Figure 4 shows the flowchart of proposed aggregation technique adopted by aggregator node.

Security: The Aggregated Data can be encrypted using any of the existing Lightweight Cryptographic algorithm and for ensuring node authentication and to avoid false alarms suitable authentication algorithm can be used.

Algorithm: Data aggregation

1) Aggregator Node ‘a’ gathers sensed data ‘s’ from base level nodes ‘g’

2) N=No. of g sent similar data to 'a'

3) If s € Event Range AND N>Threshold, go to step 4, otherwise discard data

4) Aggregated Data S={s1,s2,s3..} where s1, s2, s3 are sensed data of node1, node2

5) Send data to next level

6) stop

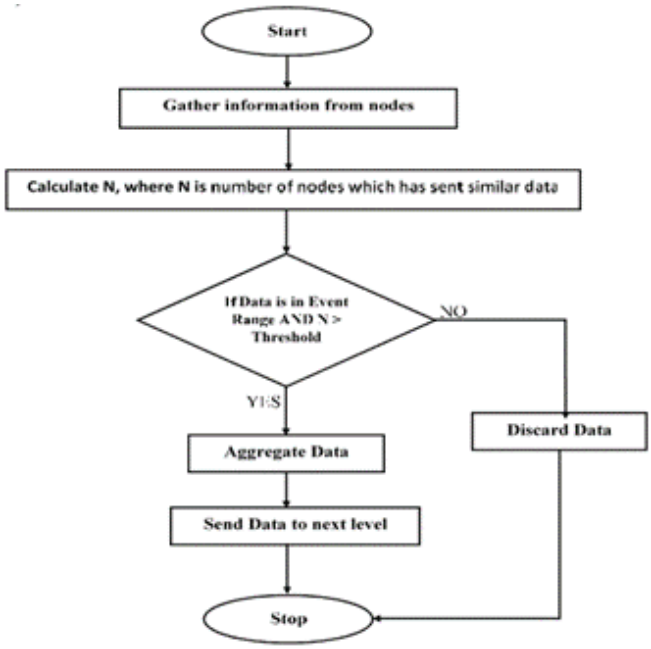

Figure 4. Aggregation procedure

4. RESULTS

Proposed framework is simulated using MATLAB. Table 1 shows the simulation parameters used. Figure 5 Shows Simulation setup. In the Figure 5, green node is base station, red node is aggregator node and blue node is base level sensor node.

Table 1. Simulation parameters

Parameter Type	Parameter Value
Application area	800×800 m^2
Grid range	100 m
Number of base level sensor nodes in each grid	4
Energy	4J
Transmission Range	25m
Number of aggregator node in each grid	2 (1Grid Head)
Energy	12J
Transmission Range	40 m
Number of base station	1
Number of surface buoyant nodes in each group of Level-2 Cell	1
Simulation Time	150sec
Payload length	512 Bytes

4.1 Energy consumption

In the Simulation setup, µAMPS energy model was considered for measuring the energy consumption in sensor nodes and network.

According to µAMPS energy model, 1.07 mJ/bit of energy will be consumed by transmission operation (Tx) and 0.27mJ/bit of energy is consumed in receiving operation (Rx). In MATLAB simulation setup every node will maintain residual energy field which get updated for every transmission and receiving operation. Simulation was performed by adopting proposed aggregation procedure as described in Figure 4 at aggregator node. Then same was compared with basic aggregation techniques. Figure 6 shows energy consumption in different techniques. From the results it is clear that with proposed scheme, network energy consumption will be less compared to other techniques.

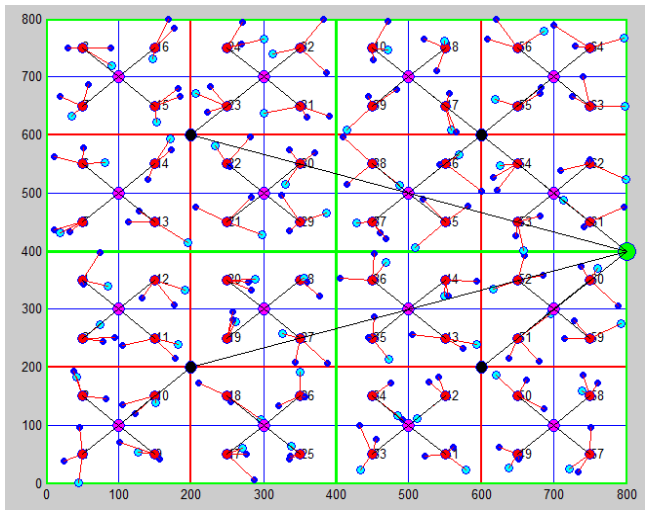

Figure 5. Simulation setup

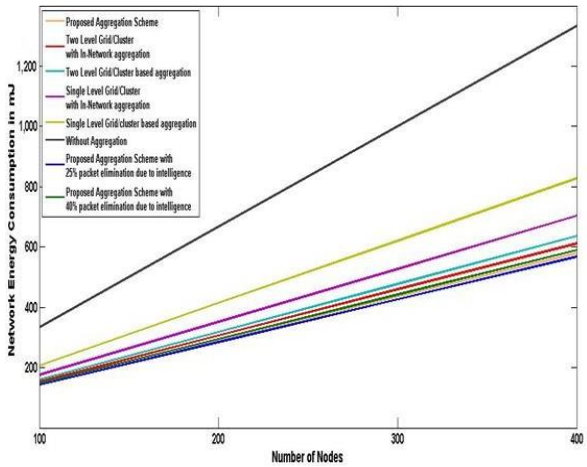

Figure 6. Energy consumption

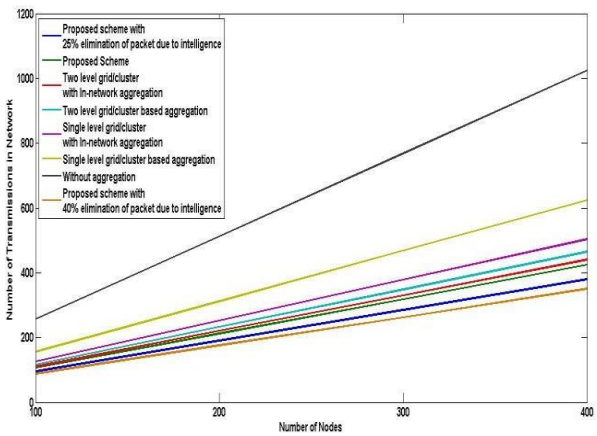

Figure 7. Redundant transmission

4.2 Redundant transmission

Main aim of data aggregation is to reduce the redundant transmission in the network. Redundant transmission can be measured by recording number of transmission per iteration in network and number of redundant data reaching the destination node per iteration or round. Figure 7 shows the graph of simulation results. Number of redundant transmission using proposed scheme and other techniques were compared. From the results obtained, it is clear that proposed scheme reduces redundant data transmission compared to other techniques.

5. CONCLUSION

In this paper, we set out to address the formidable challenges of data aggregation in resource-constrained IoT environments, where computational, memory, and bandwidth limitations intersect with the critical need for efficient and secure data handling. Our research objectives were to develop a framework that optimizes resource utilization, maintains data transmission efficiency, and ensures robust security requirements. Trough the simulation study, with the proposed work, redundant data transmission in the network is significantly reduced compared to traditional aggregation scheme. Network energy consumption is also reduced compared to traditional techniques.

REFERENCES

[1] Bhajantri, L.B., Mujawar, T. (2019). A survey of cloud computing security challenges, issues and their countermeasures. In 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, pp. 376-380. https://doi.org/10.1109/I-SMAC47947.2019.9032545

[2] Lockl, J., Schlatt, V., Schweizer, A., Urbach, N., Harth, N. (2020). Toward trust in internet of things ecosystems: Design principles for blockchain-based IoT applications. IEEE Transactions on Engineering Management, 67(4): 1256-1270. https://doi.org/10.1109/TEM.2020.2978014

[3] Apostolopoulos, P.A., Tsiropoulou, E.E., Papavassiliou, S. (2020). Cognitive data offloading in mobile edge computing for internet of things. IEEE Access, 8: 55736-55749. https://doi.org/10.1109/ACCESS.2020.2981837

[4] Tange, K., De Donno, M., Fafoutis, X., Dragoni, N. (2020). A systematic survey of industrial internet of things security: Requirements and fog computing opportunities. IEEE Communications Surveys & Tutorials, 22(4): 2489-2520. https://doi.org/10.1109/COMST.2020.3011208

[5] Singh, G. (2019). Internet-of-Things with blockchain technology: State-of-the art and potential challenges. In Handbook of Multimedia Information Security: Techniques and Applications, Springer, Cham, pp. 775-795. https://doi.org/10.1007/978-3-030-15887-3_37

[6] Liu, Y., Liu, A., Zhang, N., Liu, X., Ma, M., Hu, Y. (2019). DDC: Dynamic duty cycle for improving delay and energy efficiency in wireless sensor networks. Journal of Network and Computer Applications, 131: 16-27. https://doi.org/10.1016/j.jnca.2019.01.022

[7] Rehman, M., Javaid, N., Awais, M., Imran, M., Naseer, N. (2019). Cloud based secure service providing for IoTs using blockchain. In 2019 IEEE Global Communications Conference (GLOBECOM), Waikoloa, HI, USA, pp. 1-7. https://doi.org/10.1109/GLOBECOM38437.2019.9013413

[8] Butun, I., Sari, A., Österberg, P. (2019). Security implications of fog computing on the internet of things. In 2019 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, pp. 1-6. https://doi.org/10.1109/ICCE.2019.8661909

[9] Tseng, L., Wong, L., Otoum, S., Aloqaily, M., Othman, J.B. (2020). Blockchain for managing heterogeneous internet of things: A perspective architecture. IEEE Network, 34(1): 16-23. https://doi.org/10.1109/MNET.001.1900103

[10] Singh, P., Nayyar, A., Kaur, A., Ghosh, U. (2020). Blockchain and fog based architecture for internet of everything in smart cities. Future Internet, 12(4): 61. https://doi.org/10.3390/fi12040061

[11] Sharma, P., Jindal, R., Borah, M.D. (2020). Blockchain technology for cloud storage: A systematic literature review. ACM Computing Surveys (CSUR), 53(4): 1-32. https://doi.org/10.1145/3403954

[12] Li, Z., Zhong, R.Y., Tian, Z.G., Dai, H.N., Barenji, A.V., Huang, G.Q. (2021). Industrial blockchain: A state-of-the-art survey. Robotics and Computer-Integrated Manufacturing, 70: 102124. https://doi.org/10.1016/j.rcim.2021.102124

[13] Tseng, C.T., Shang, S.S. (2021). Exploring the sustainability of the intermediary role in blockchain. Sustainability, 13(4): 1936. https://doi.org/10.3390/su13041936

[14] Heinzelman, W.B., Chandrakasan, A.P., Balakrishnan, H. (2002). An application-specific protocol architecture for wireless microsensor networks. IEEE Transactions on Wireless Communications, 1(4): 660-670. https://doi.org/10.1109/TWC.2002.804190

[15] Chawra, V.K., Gupta, G.P. (2020). Load balanced node clustering scheme using improved memetic algorithm based meta-heuristic technique for wireless sensor network. Procedia Computer Science, 167: 468-476. https://doi.org/10.1016/j.procs.2020.03.256

[16] Venugopal, K.R., Kumaraswamy, M., Venugopal, K.R., Kumaraswamy, M. (2020). LRTHR: Link-Reliability based two-hop routing for WSNs. In QoS Routing Algorithms for Wireless Sensor Networks, Springer, Singapore, pp. 23-44. https://doi.org/10.1007/978-981-15-2720-3_2

[17] Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper, 151(2014): 1-32.

[18] Khan, M.N., Rahman, H.U., Almaiah, M.A., Khan, M.Z., Khan, A., Raza, M., Al-Zahrani, M., Almomani, O., Khan, R. (2020). Improving energy efficiency with content-based adaptive and dynamic scheduling in wireless sensor networks. IEEE Access, 8: 176495-176520. https://doi.org/10.1109/ACCESS.2020.3026939

[19] Sert, S.A., Alchihabi, A., Yazici, A. (2018). A two-tier distributed fuzzy logic based protocol for efficient data aggregation in multihop wireless sensor networks. IEEE Transactions on Fuzzy Systems, 26(6): 3615-3629. https://doi.org/10.1109/TFUZZ.2018.2841369

[20] Sert, S.A., Yazici, A. (2021). Increasing energy efficiency of rule-based fuzzy clustering algorithms using CLONALG-M for wireless sensor networks. Applied Soft Computing, 109: 107510. https://doi.org/10.1016/j.asoc.2021.107510

[21] Sert, S.A., Onur, E., Yazici, A. (2015). Security attacks and countermeasures in surveillance wireless sensor networks. In 2015 9th International Conference on Application of Information and Communication Technologies (AICT), Rostov on Don, Russia, pp. 201-205. https://doi.org/10.1109/ICAICT.2015.7338546

[22] Wang, H. (2020). IoT based clinical sensor data management and transfer using blockchain technology. Journal of ISMAC, 2(3): 154-159. https://doi.org/10.36548/jismac.2020.3.003

[23] Memon, R.A., Li, J.P., Ahmed, J., Nazeer, M.I., Ismail, M., Ali, K. (2020). Cloud-based vs. blockchain-based IoT: A comparative survey and way forward. Frontiers of Information Technology & Electronic Engineering, 21(4): 563-586. https://doi.org/10.1631/FITEE.1800343

[24] Alkadi, O., Moustafa, N., Turnbull, B., Choo, K.K.R. (2020). A deep blockchain framework-enabled collaborative intrusion detection for protecting IoT and cloud networks. IEEE Internet of Things Journal, 8(12): 9463-9472. https://doi.org/10.1109/JIOT.2020.2996590

[25] Serrano, W. (2021). The blockchain random neural network for cybersecure IoT and 5G infrastructure in smart cities. Journal of Network and Computer Applications, 175: 102909. https://doi.org/10.1016/j.jnca.2020.102909