International Journal of Global Perspective in Academic Research

Journal homepage: https://ijgpar.org/index.php/journal/index

Energy Efficient Secured PSO Optimized Clustering and Data Aggregation Routing Protocol for Wireless Sensor Networks

K. Yesodha[1*], M. Krishnamurthy[2], M. Selvi[3], K. Thangaramya[3], Santhosh Kumar SVN[4], Kannan Arputharaj[5]

1 Department of Computer Science, Hindustan Institute of Technology and Science, Padur, Chennai, Tamil Nadu, India

2 Department of Computer Science and Technology, KCG College of Technology, Chennai, Tamil Nadu, India

3 School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, Tamil Nadu, India

4 Department of Computer Science Engineering and Information Systems, Vellore Institute of Technology, Vellore, Tamil Nadu, India

5 Department of Information Science and Technology, Anna University, Chennai, Tamil Nadu, India

Abstract: In Wireless Sensor Networks (WSNs), sensor nodes are placed to sense and collect data. Due to the energy constraint nature of WSN, optimising the energy during the data dissemination is a major concern. To solve this problem, data aggregation may be used to bring down the redundant transmission of packets in WSN. In most of the previously available techniques, security is also a major concern during data aggregation and routing process with optimized energy. Many data aggregation-based routing systems are subject to security attacks during the data transfer from sensors to source to Clustered Heads (CHs) and then to sink with data aggregation process. Moreover, the existing data aggregation-based routing protocols suffer from data redundancy with less accuracy in aggregated data. For handling such issues order to overcome these issues, an Energy Efficient Secured Clustered Particle Swarm Optimization (PSO) oriented Data Aggregation Routing Protocol (EESCPSO-DARP) that can provide efficient authentication during data aggregation-based routing is introduced in this paper. Moreover, the proposed protocol enhances the rate of the data transmission by efficient prevention of false data injection and other attacks through node authentication and data encryption. This proposed protocol minimizes the energy usage by minimizing the retransmissions by eliminating the possible redundant transmissions of data during data aggregation-based routing. Moreover, the introduced protocol minimizes both communication and computational overhead through optimal clustering and routing with PSO and provides and efficient routing system. This proposed EESCPSO-DARP protocol has been developed by using the NS3 simulator. The results of this protocol showed improved security, higher packet delivery ratio and enhanced network throughput with reduced energy and delay.

Keywords: Data Aggregation, Security, Energy Efficiency, Routing, Attacks, False data injection.

1 Introduction

Wireless Sensor Network (WSN) is made from a collection of sensors for sensing the environment to collect the data and to transfer them to sink. Due the resource constraint nature of WSN[1] [2], energy optimization in WSN is an important task. Moreover, data aggregation is a viable solution[3] for the optimization of energy usage in WSN. In data aggregation[4], sensor nodes are first grouped into clusters. Every cluster member node is allocated with an associated Cluster Head (CH) node. The CH nodes collect the sensed data from their cluster member nodes and transfer them to sink. Here, only the cluster head nodes are given authority to communicate with sink. The advantages of Data Aggregation (DA) in WSN[5] are first, the data correctness has been ensured by the CH. Secondly data aggregation minimizes the count of packets transmitted among sensor nodes including sink thereby reducing computation and transmission overhead incurred. Moreover, data aggregation reduces the redundant[6] and retransmission of data. Wireless sensor networks pave the way for a wide variety of applications including wild life habited monitoring system, e-health care, military tracking, and surveillance and earth quake monitoring system. Therefore, the nodes of WSN are autonomous and installed in unsafe place; they are subject to different network attacks by intruders during data aggregation[7]. The aggregated data are highly sensitive and can be easily modified with the malicious code and false information. For example, an intruder can access the aggregate information that is sent from CHs to sink by disrupting the link between them[8]. Then the intruder can generate a fake replication[9] of the node with the same identity. By doing so, the intruder can access the sensed data and modify the data with malicious code and add false information. Finally, the intruder can compromise the whole network. Therefore, providing security during data aggregation[10] is required to preserve the integrity. Because of the resource limited nature of WSN, provision of security on data aggregation-based routing is a difficult task. In WSN, maximum amount of energy is spent on communication[11] and computation process. To maximize the life times of the nodes, the amount of computation and communication overhead should be minimized in WSN. Therefore, some energy optimized secured Data Aggregation scheme[24] must be considered to safe guard the network from various attacks which are caused by the intruders. The secure routing algorithms must either detect the occurrences of attacks earlier or prevent them through effective authentication.

Authentication is used in information and network security for proving the assertion that the user or node in a computer network is validated for their identity before they participate in the communication. Kerberos is one of the computer-network authentication protocols and it works on the basis of issuing and verifying tickets before allowing the nodes of a computer network for communication[64]. Kerberos was built using symmetric-key encryption and it uses one trust oriented third-party coordinator for ticket generation, authentication and coordination. Some versions of Kerberos use public-key encryption also in its authentication procedure. Among the various security mechanisms including intrusion detection and prevention, access control, firewalls, encryption and decryption mechanisms and key management schemes with node authentication are the important security mechanisms that can prevent the attackers before entering into the networking systems for carrying out the attacks.

Particle swarm optimization (PSO) was introduced for making optimal search using nature-inspired meta-heuristics[52][53]. It is a simple approach to solve the optimization problem by searching for an optimal solution in the state space pertaining to the solution. Moreover, PSO provides optimal solutions and it uses a flock of birds for performing the mathematical modelling. Mathematically, the PSO algorithm uses an objective function and a set of constraint-based rules having no derivatives for computing the maxima and minima values. Unlike the Machine Learning (ML) oriented classification algorithms such as Support Vector Machines, the PSO algorithm does not use the gradients and hence it has the capability of solving a variety of optimization problems including the problems having multimodal as well as the problems with non-convex nature. Many researchers used PSO and its extensions for network routing, security and optimization[62][63].

The PSO algorithm begins its search for solutions using a collection of intelligent agents, called as the particles that are distributed randomly throughout a given search space. Here, an assumed initial velocity is considered as an input to the search-based optimization algorithm which is determined by heuristics. In the PSO algorithm, one fitness function for computing their fitness value of an individual particle is set initially based on its current position. The search-based optimization problem to be solved using PSO in this work computes the best position for making next move. This position is used to minimise the fitness function value by setting the objective function to compute the minimum possible value. This algorithm works iteratively by assessing the fitness values of particles on each of the iterations. This algorithm updates the velocity of moving particles considered in the problem for every iteration count and it finally determines the next best location for making the movement. Here, the particle's next velocity is obtained by using its present velocity, current location (position) of the particle relative to its local best (l-best) and global best (g-best) locations. The l-best and g-best values are applied in the velocity update process. The algorithm is stopped either using the iterations count prescribed or when the l-best and g-best values are giving the same best location values subsequently and the trend is repeated till the converge criteria is met.

Clustering forms groups in intelligent data analysis. Among the different clustering techniques, k-means clustering is common clustering algorithm used in most applications. In WSN, nodes are clustered to design CH oriented routing for reducing energy consumption. Among the different clustering algorithms used in CH involved routing, Fuzzy Based Unequal Clustering (FBUC) algorithm proposed by Logambigai et.al.,[56] models cluster-based routing problem using an optimization problem and reduces the energy utilization in WSN. Ruby et.al.,[55] developed an optimal routing strategy for energy efficiency in routing in a type of WSN. Some other approaches used for clustering of nodes include the Dominant Set Clustering algorithm discussed by Pavan et.al.,[57] , the gravitational clustering approach[11][59], Hybrid and Energy-Efficient, Distributed clustering[58] and Low Energy based Adaptive Clustering Hierarchy (LEACH)[60][61] are the important works found in the literature.

In this research, an Energy-Efficient Secured Clustered and Data Aggregation Routing Protocol (EESC-DARP) is developed. Moreover, PSO optimization is added here optimizing clustering and secured routing in response to all of the foregoing observations made on clustering, CH based data aggregation and routing with node authentication for enhancing the security. This proposed Energy Efficient Secured Clustered Particle Swarm Optimization (PSO) oriented Data Aggregation Routing Protocol (EESCPSO-DARP) provides efficient authentication during data aggregation-based routing is introduced in this paper. This technique offers not only energy-efficient secured data aggregation with PSO optimization, but also is offering a robust defence against various network assaults through authentication and data encryption. Here, the sensors are put initially in the sensing field randomly. The sensors are clustered by the application of k-means clustering algorithm. Each node of clusters is authenticated using the authentication procedures proposed in this paper. For each cluster, the node having higher energy, shorter distance from other sensors, lower mobility and authenticated fully are designated as CHs. These clusters are optimized periodically using PSO algorithm which considers all the parameters including mobility for re-clustering. The data received from member nodes are aggregated by CHs. The route discovery procedure finds the shortest routes through CHs to sink and it is optimized using PSO. Later on, based on their energy levels, the cluster heads are rotated periodically and authenticated for forming new routes by selecting new cluster heads satisfying the selection criteria. The main uses of the proposed protocol are enhanced security, improved packet delivery ratio (PDR) and higher network performance with lower energy consumption and delay.

The other parts of this manuscript is arranged as shown: Section 2 discusses about the existing work on secured clustered optimal DA routing in WSNs. It provides the elaborate analysis of the existing systems highlighting their advantages and limitations. Section 3, depicts the secure routing system architecture developed here. Section 4 provides detailed explanation on the EESC-DARP introduced in this article. Section 5 provides the details on implementation setup and simulation results for the proposed protocol. Section 6 provides concluding remarks about the proposed protocol and suggests few future works.

2 Related Works

Several authors have presented various methods for achieving secure DA based on clustering in WSN[12]. Here, this section discusses about some of these efforts. Isaac Sajan R and Jasper[13] introduced one Secure Routing Protocol in which Base Station (BS) is Controlling the routing analysis for distinguishing between malicious and normal entities within the network. Their protocol employed a trust-based mechanism for security to establish more secure routes to sink. The trustworthiness of nodes is assessed through four distinct trusts. This approach offers the advantage that it creates a more secure path between nodes to CHs, CHs to CHs s and finally between CHs and BS. The single point of failure that results from a broken connection between the BS and sensor nodes is one of their method's weaknesses. Kowsalya and Jeetha[14] introduced the Secure Lightweight Cryptography Data Aggregation Algorithm, designed to enable cluster-based data aggregation with a focus on strong security and minimization of energy consumption. This approach offers several benefits, including enhanced data confidentiality, reliability, security, and reduced latency. However, one limitation of this work is observed when high data rates are present in the network during data aggregation, leading to network imbalances that adversely impact network performance during this process. Ahmed Hassan et.al.,[15] proposed a system to provide robust clustering approach which can extend the life time of the nodes. All cluster nodes share the workload of the Cluster Head (CH) role in their system. To optimise the clustering process in their system, they used two algorithms: optimisation based on game theory and quantum particle swarm optimisation. Their solution reduces the heavy strain on the CH, increasing energy efficiency, and extending the lifespan of WSN nodes. Due to only being elected once, CH energy will eventually run out.

Santhosh Kumar et. al.,[10] introduced one new approach to data dissemination in WSN, by employing better clustering techniques to attain heightened security and reduced energy utilization. Their system offered many advan[tages including reduction of redundant data and efficient authentication mechanisms during the process of data dissemination. The limitations of work are the overhead to choose the alternate path from optimal path when the attacker nodes are detected in the path. Maheswari and Karthika[16] introduced a neuro-fuzzy technique for selecting Tentative Cluster Heads (CHs) within their system. The Tentative CHs play a pivotal role in identifying the optimal CHs by utilizing the deer hunting optimization (DHO) algorithm, thereby optimizing the clusters. However, one limitation of their approach is that the uneven clustering it generates can result in energy imbalances among nodes, ultimately leading to a decline in network performance during data aggregation.

Aram Mosavifrada and Hamid Barati[17] came up with an energy aware clustered based routing protocol that can provide better energy optimization thereby increasing the lifespan of the nodes in WSN. Their proposed two-level routing algorithm based on inter and intra clustering operations. The limitations of their approach are data from the lower cluster layers cannot be transmitted to the BS when link of the higher cluster layer fails. Anupkumar and his colleagues[18] introduced the Intra Clustering Data Aggregation (ICA) algorithm, which focuses on establishing an efficient path from source nodes to Cluster Head (CH) nodes for effective data aggregation. Their proposed system offers several benefits, including the reduction of redundancy and the optimization of energy utilization. The limitations are requirement of high bandwidth and high delay occurs in the network due to increased data rate which occurs in aggregated node. Moreover, their proposed system does not consider security in their design.

Selvi et.al.,[11] proposed clustered based gravitational routing algorithm to find best solution for effective clustering and routing. Their proposed gravitational routing algorithm consists of two phase's namely gravitational clustering and CH routing method. In gravitational based clustering method, the Clustering is done by force of attraction and selection of CH is done by intelligent fuzzy rules. In gravitational based routing, routing is carried out by considering the velocity and position of CH. Their approach has certain limitations. Firstly, the fuzzy rule-based Cluster Head (CH) selection introduces overhead into the decision-making process. Additionally, their system does not take into account clustering reliability and security during the routing process. In contrast, Deebak and Fadi Al-Turjman[19] proposed a hybrid secured Routing Protocol (RP) that employs the symmetric key approach in encryption. To mitigate the impact of malicious activity, guard nodes are strategically placed in the network during the routing process. However, it's worth noting that their approach may consume more energy when the distance between the BS and sensors is substantial.

Ahmed Saidi et.al.,[20] proposed one CH election technique with strong security and misbehaviour identification method using the trust in the network. Their proposed system combines the clustering, and identifies and eliminates the anonymous nodes in the system. In their system, CH is chosen based on the node trust and uses the local clustering algorithm. An advantage of this system lies in its ability to establish trust relationships among sensor nodes, encompassing various forms of trusts. However, when every node in the network verifies trust scores, it results in a communication overhead. In a related context, Revanesh et.al.,[21] introduced a Secure Corona-based Zone Clustering and Routing model designed for distributed WSNs. Their proposed system works based on the network partition to reduce the energy consumption, Packet loss rate, provide high security by verification process. The limitations of their system are the inner corona which results in the redundancy of the packet in the rural area.

Yesodha et.al.,[12] proposed one model for secure routing of data in WSN. Their protocol employs the Elliptic Curve Cryptography for security and Ant Colony Optimization for the routing process and to secure the data during the communication process. Their algorithm increased the performance by reliable communication, delay identification and energy rate. The limitations of their work are overhead occurred during encryption of data. Zhang Y et.al.,[22] introduced an energy aware algorithm that relies on weighted election probabilities as its foundation. Heterogeneous nodes are selected in their model based on computing, energy and link which provides longer stability region for the suitable weight based for the nodes that has increased the energy optimization. The limitations of their approach are different initial energy of nodes which will cause the imbalance in the energy consumption.

Mehetre et.al.,[23] presented a routing method focused on security and trust within Wireless Sensor Networks (WSN). Their approach incorporates a two-way security process aimed at identifying malicious nodes. They employ a dual assurance scheme, selecting nodes and providing data packet security through two distinct methods. The initial method involves Selective Forwarding-based packet validation. The second method applies Elliptic Curve Cryptography (ECC) based packet security thereby finding out the paths which are trusted and secured. The limitations of their approach are the computational and communication overhead during the two-step verification process which is carried out by each and every node.

Ahmed Saidi et.al.,[25] underscored the efficacy of trust in mitigating issues on detection of malicious nodes in WSNs. Through innovative approaches like a secure CH election algorithm and a robust misbehaviour detection method, their research work showcased the practicality of utilizing trust metrics for tasks such as CH selection and node behaviour assessment. Their proposed strategies effectively weeded out compromised nodes and maintained network integrity, even in cases of compromised CHs. Their simulation results validated their scheme's ability to prevent malicious CHs and to detect misbehaviour with high accuracy. Their study not only contributes to the field but also highlights the vital role of trust management in enhancing WSN security. Ahmed Abdulhadi Jasim et.al.,[26] tackled the security and energy challenges present in WSNs through the introduction of the Secured End-to-End DA protocol for data aggregation. In contrast to earlier methods that neglected authentication, it significantly bolstered security by incorporating the use of secret key-generated random values and timestamps. Their protocol adeptly identifies and thwarts attacks through secure node authentication, data fragmentation, and encryption measures. Simulation results demonstrated its superiority in terms of malicious node detection, energy efficiency, and delay compared to existing protocols. Overall, it presented a promising solution to the security and energy trade-off in WSNs.

Osama et.al.,[27] addressed the security, efficiency, and energy-related issues within WSNs through the introduction of the FlexCrypt scheme. FlexCrypt offered dynamic clustering, adaptive encryption parameters, and efficient key management. Through simulation, their scheme was demonstrated to have remarkable improvements in reduced power, delay, better encryption and network lifetime compared to other cryptographic methods. Their comprehensive approach enhanced WSN performance while effectively countering diverse attacks, making FlexCrypt a promising solution for the complex demands of WSNs. Wei Fang et.al.,[28] presented Cluster-based Secure DA (CSDA), an inventive and energy-efficient secure DA scheme designed for wireless sensor networks. Through the utilization of cluster privacy preservation and dynamic fragment adjustment, CSDA provided better DA accuracy, safeguarding privacy, and enhancing communication efficiency when compared to existing approaches. This marks a significant step towards addressing the critical issue of privacy within WSN applications. Haseebet.al.,[29] provided an overview of a protocol called Light-weight Structure based DA routing protocol. This protocol was devised to tackle the challenges arising from the integration of the Internet of Things (IoT) into WSNs. Through the utilization of cluster-based decomposition and optimized routing, their protocol improved both energy efficiency and data security in the face of potential malicious threats. Their simulation results indicated substantial enhancements when compared to existing methods, encompassing reduced Energy Consumption (EC), extended Network Life Time (NLT), decreased latency, and improved packet delivery reliability. This novel protocol presents a promising advancement for the future of secure and efficient IoT networks. However, the work can be extended with authentication techniques to enhance the security further. Hu et.al.,[30] presented an Efficient DA scheme designed for predictive vehicle maintenance. This scheme incorporates super increasing sequences and better encryption to guarantee data privacy and robust protection against a range of potential attacks. Additionally, the scheme guaranteed data integrity and authenticity through shared secret keys and lightweight authentication. Both security analysis and performance evaluations confirmed that ESDC's capability to meet privacy, integrity, and efficiency requirements, making it a promising advancement over existing approaches.

Wu et.al.,[31] introduced the Secure and Efficient Multifunctional Data Aggregation (SEMDA) solution tailored for Edge-Enhanced IoT systems. SEMDA harnessed lightweight cryptographic methods to achieve resilient and precise data aggregation, eliminating the requirement for a Trusted Authority. Additionally, their scheme was extended to include support for differential privacy, effectively addressing privacy concerns. Security analysis provided by them confirmed SEMDA's ability to ensure confidentiality, privacy, integrity, and authentication. Additionally, SEMDA stands out for its efficient computation and communication, as demonstrated by them through both theoretical analysis and practical evaluations. In essence, SEMDA offered an innovative approach that strikes a balance between security, efficiency, and functionality in IoT data aggregation. One limitation of this work is the need for cryptographic encryption which provides overhead in computation. Alghamdi et.al.,[32] underscored the significance of attaining energy efficiency in WSNs through the implementation of a clustering approach. Their focus is on extending network lifespan and increasing packet delivery rates. Their proposed hierarchical clustering method involves two phases: uniform node distribution within clusters and CH selection with DA using linear programming. Their ultimate goal is to minimize EC, enhance NLT, and improve overall performance by reducing congestion and increasing packet delivery efficiency within the WSN. However, the security aspects must also be improved for enhancing the reliability of communication.

Dorsala et.al.,[33] innovatively extended privacy-preserving aggregation for mobile crowd sensing. By introducing a smart contract model on a public Block chain network, their model tackles challenges related to aggregator reliability and fair payments for data contributors. Through practical implementation and analysis on the Ethereum Blockchain, their study showcased the effectiveness of their approach in ensuring secure and equitable data aggregation. Their model can be extended with a cluster-based RP for effective data delivery. Khan et.al.,[34] addressed the critical concerns surrounding data privacy and security in the context of Smart Grids (SGs). Their research made significant contributions to the field by introducing a new DA scheme. This scheme not only enhanced data privacy through improved Shamir's secret key scheme and Paillier homomorphic encryption but also provided fault tolerance and safeguarded against various attacks including False Data Injection (FDI). Thorough security analysis, the authors validated their scheme's effectiveness in preserving data privacy, source authentication, and overall security. Moreover, their paper offered compelling evidence of their proposed scheme's efficiency through comprehensive performance evaluations, positioning it as a viable and superior solution compared to existing State-Of-The-Art (SOTA) programs. However, the work must address secure data delivery as well.

Sindhuja et.al.,[35] introduced a multi-objective CH based RP, which aimed to ensure secure data aggregation within Wireless Sensor Networks. This method utilized self-attention-based routing, a multi-objective approach to cluster head selection, and African vulture optimization for path optimization. As a result, their approach achieved substantial improvements in energy efficiency and the overall longevity of the network. Experimental results demonstrated its superiority over existing methods, achieving lower delays, improved packet delivery ratios, and reduced packet drops. The approach holds great promise for advancing secure and energy-conscious data aggregation in WSNs. However, the attacks such as FDI attacks must also be considered to enhance the security further.

Regueiro et.al.,[36] advocated for a paradigm shift from centralized data control to a decentralized model empowered by Blockchain and Homomorphic Encryption (HE). Their proposed protocol leverages Blockchain's transparency and HE's data confidentiality to create a secure and private framework for data aggregation. The synergistic potential of their technologies is highlighted through theoretical exploration, practical applications, an implementation strategy, and a performance analysis. Their solution offered a promising pathway to address the growing concerns around data breaches and privacy infringement. This work can be enhanced with better node authentication scheme for improving the security more. Othman S.B et.al.,[37] presented an authenticated DA scheme, offering a pioneering solution to address challenges in healthcare IoT. Their approach effectively minimized both energy consumption and communication overhead. Their approach safe guard sensitive healthcare data while improving security features, making it a promising avenue for secure and energy-efficient DA in IoT-enabled healthcare applications. Shen X et.al.,[38] presented a DA protocol designed to safeguard privacy within dynamic groups in the context of fog computing. By addressing the shortcomings of prior methods, their proposed scheme leveraged encryption, aggregation, and decryption algorithms to ensure secure and efficient data processing. In their model, terminal device collusion is thwarted, and bandwidth is conserved through ciphertext aggregation. Their protocol's versatility accommodated arbitrary aggregation functions while maintaining data privacy, making it a valuable addition to the fog computing paradigm. Their work pioneered a secured DA protocol for WSN. Ravi G et.al.,[39] introduced the Cluster Based and Reliable DA (CRDA) scheme for IoT networks. By efficiently eliminating data redundancies through clustering, their scheme effectively conserves energy without compromising reliability. The use of specialized algorithms, the authors optimized the cluster formation and trust computation. They integrated their model with a Re-formative and optimal learning -based deep Neural Network that ensured dependable data routing. Through rigorous simulations and comparisons, their proposed approach’s efficacy is established, highlighting its contribution to achieving energy-efficient and reliable IoT data aggregation.

Gao et.al.,[40] addressed the privacy concerns of centralized data utilization for training machine learning models, the Private Aggregation of Teacher Ensembles (PATE) framework emerged to leverage distributed teacher models' knowledge. However, PATE falls short in safeguarding individual label predictions, exposing privacy risks. In their publication, they introduced an innovative protocol that effectively leverages distributed knowledge while simultaneously ensuring robust privacy protection for label predictions. IT incorporated lightweight cryptography and differential privacy techniques to effectively safeguard data privacy while maintaining accuracy levels comparable to plaintext baselines. Furthermore, it demonstrated substantial computational and communication performance improvements over existing methods, highlighting its potential as a superior approach in distributed learning. However, the distributed model requires more energy consumption than the centralized models. Lu S et.al.,[41] addressed privacy concerns in federated learning through the Top-k Sparse Secured Aggregation protocol. Through the substitution of Rand-k scanty and the optimization of communication overhead via client grouping, their protocol achieved a substantial reduction in both communication and training time when compared related work. Anitha et.al.,[42] introduced an encryption scheme as a robust strategy aimed at enhancing the longevity and Energy Efficiency (EE) of WSNs. Through the optimization of cluster formation, CH selection, and the application of RSA cryptography for securing data transmission, their approach demonstrated superior performance relative to existing algorithms. They represented a significant advancement in bolstering the security and reliability of WSNs for various applications. Their work can be extended with node authentication scheme to enhance the security further. Liu X Liu X et.al.,[43] emphasized the pivotal role played by WSNs in Industrial Internet of Things (IIoT), with a particular focus on the vital aspects of security and efficiency. They introduced the WSN-based IIoT Model (WIM), which featured a mobile sink, presenting an innovative approach. Their model demonstrated the capability for real-time and precise data acquisition. Their integrated model ensured data security without compromising network efficiency, even when the sink's movement was random. Simulation results provided by them underscored the effectiveness of their proposed model and algorithms, showcased enhancements in WSN performance in terms of accuracy, effectiveness, and reduced delay. However, CH based routing can be used to reduce the EC in WSN.

Lin H et.al.,[44] summarized, the synergy between Sixth generation (6G) networks and network-in-box (NIB) presented a revolutionary potential for diverse industrial applications. Their integration offered enhanced fault tolerance, reduced backhaul traffic, and promising applications. They addressed the vital concern of data aggregation security, and their article proposed a blockchain-based secured distributed DA approach. By incorporating an improved blockchain design, they ensured DA performance while safeguarding privacy through task and receiver segmentation. In the context of a WSN, it is essential to consider both energy efficiency and security simultaneously. Shim K A et.al.,[45] summarized that Wireless Sensor Networks (WSNs) comprising distributed sensor nodes can offer immense potential for diverse applications. However, their battery-constrained nature and energy-intensive data transmission pose challenged for prolonged network life. To address this, the authors focused on energy-efficient data transmission over processing emerge as a crucial strategy to extend WSN longevity. This must be enhanced with security aspects for enhancing reliable data delivery.

Xue K et.al.,[46] addressed the challenge of secure DA in the smart grid. The existing solutions often burden smart meters or require a trusted authority, neglecting user-side efficiency. The scheme they put forward provided an adaptable data aggregation method that prioritized privacy preservation and efficiency, all without the need for a trusted authority and capable of accommodating evolving user dynamics. The authors' security and performance analyses validated the model's effectiveness in maintaining robust security features while simultaneously optimizing the overheads. In the context of a WSN, it's crucial to also take into account energy efficiency as another critical factor.

Rezaeibagha F et.al.,[47] summarized that the rapid growth of IoT has led to applications like Wireless Body Sensor Networks (WBSNs) in healthcare. Security concerns surround data collected by these networks, with encryption often seen as a solution, albeit with computational limitations. The existing secure IoT schemes lack comprehensive data analysis in healthcare. Their research paper presented an effective and secure solution for managing DA in IoT based WSN. The innovative cryptographic accumulator, which employed authenticated additive homomorphic encryption, enabled both confidential data collection and encrypted analysis. Security analysis and performance evaluations provided by authors validated their scheme's efficacy and highlight its potential for secure data analysis in IoT wireless body sensors. In addition, node authentication may help to improve the security further.

Jasim A et.al.,[48] explained that the Wireless Sensor Networks (WSNs) serve as critical information-gathering infrastructures, and while secure data aggregation is a focus, authenticating the process while conserving energy remains challenging. They added that prior research has limitations, such as sharing security keys, neglecting Message Authentication Code (MAC) server authentication, and leaving networks vulnerable to malicious activities. To tackle these concerns, their paper extended the SDAACA protocol by introducing the Secured EE and DA (SEEDA) protocol. SEEDA enhanced authentication through randomized values and timestamps, verified by the base station. Their protocol incorporated node authentication, encryption, and access control to effectively thwart potential attacks. Additionally, employing node clustering for routing in WSN can result in energy savings.

Zhang J et.al.,[49] presented a Privacy-Preserving (PP) health DA scheme for IoT wearable devices. By ensuring data confidentiality and recipient anonymity through cipher-text transmission, the scheme effectively prevented leakage and maintains privacy. Compared to existing methods, it's both lightweight and efficient, showcased its potential for enhancing privacy and security in healthcare data aggregation. Their model can be enhanced with authentication and attacks detection for enhancing the security with data aggregation. Rezvani M et.al.,[50] outlined a technique for data aggregation from sensor nodes within WSNs. They noted that data aggregation is frequently simplified due to constrained computational resources, making them susceptible to potential compromise attacks. They emphasized the critical importance of ensuring the trustworthiness of both data and sensor nodes to uphold WSN security. As low-power processors continue to advance, they foresee future aggregator nodes enabling more sophisticated data aggregation methods, thereby reducing vulnerability. Iterative filtering algorithms offer promising results by aggregating data and assessing source trustworthiness through weight factors. However, their study revealed that existing iterative filtering algorithms remain vulnerable to novel collusion attacks. To counter this, the paper proposed an enhanced approach that provides initial approximations, rendering the algorithms both collusion-resistant and more accurate, while also accelerating convergence. However, it is necessary to include the cluster-based routing process to preserve the energy in WSN.

Despite the abundance of techniques documented in the literature, a significant portion of existing models neglects to incorporate clustering and cluster optimization. As a result, this paper introduces a novel secured routing protocol (SRP) based on clustering and data aggregation. This SRP improves security, packet delivery rates, and mitigates both delay and energy consumption.

3 Energy Efficient Secured based Data Aggregation Protocol

The main aim of Secured DA system[25] is for providing improved security with reduced data retransmissions. Moreover, SRP provides[26] efficient hop by hop authentication which ensures the confidentiality and data integrity. The architecture of the Secure Routing System (SRS) developed in this work for DA, authentication, clustering, CH selection and CH based routing is shown in Figure-1. It consists of 10 components namely sensors, gateway, data collection module, DA module, clustering module, decision manager, PSO optimization module, authentication module, secured aggregation-based routing module and BS. The sensors are deployed initially in sensing field randomly. These nodes can sense the environment to capture related data. The Data Gathering Module (DGM) collects the data from the sensors and sends them to the Cluster Head (CH) nodes for performing DA. The DA module applies the data aggregation procedure proposed in this work and aggregates the data pertaining to each cluster. The clustering module is responsible for cluster formation, CH selection and cluster maintenance. It uses the PSO algorithm for cluster optimization. The Decision Manager (DM) controls all the activities of the secure routing system. The PSO optimization module optimizes the number of clusters, cluster members and the routing path. The authentication module performs the node authentication before every communication. The secured aggregation-based routing module performs the route discovery, route optimization using PSO and performs the data routing. All the data are collected finally by BS.

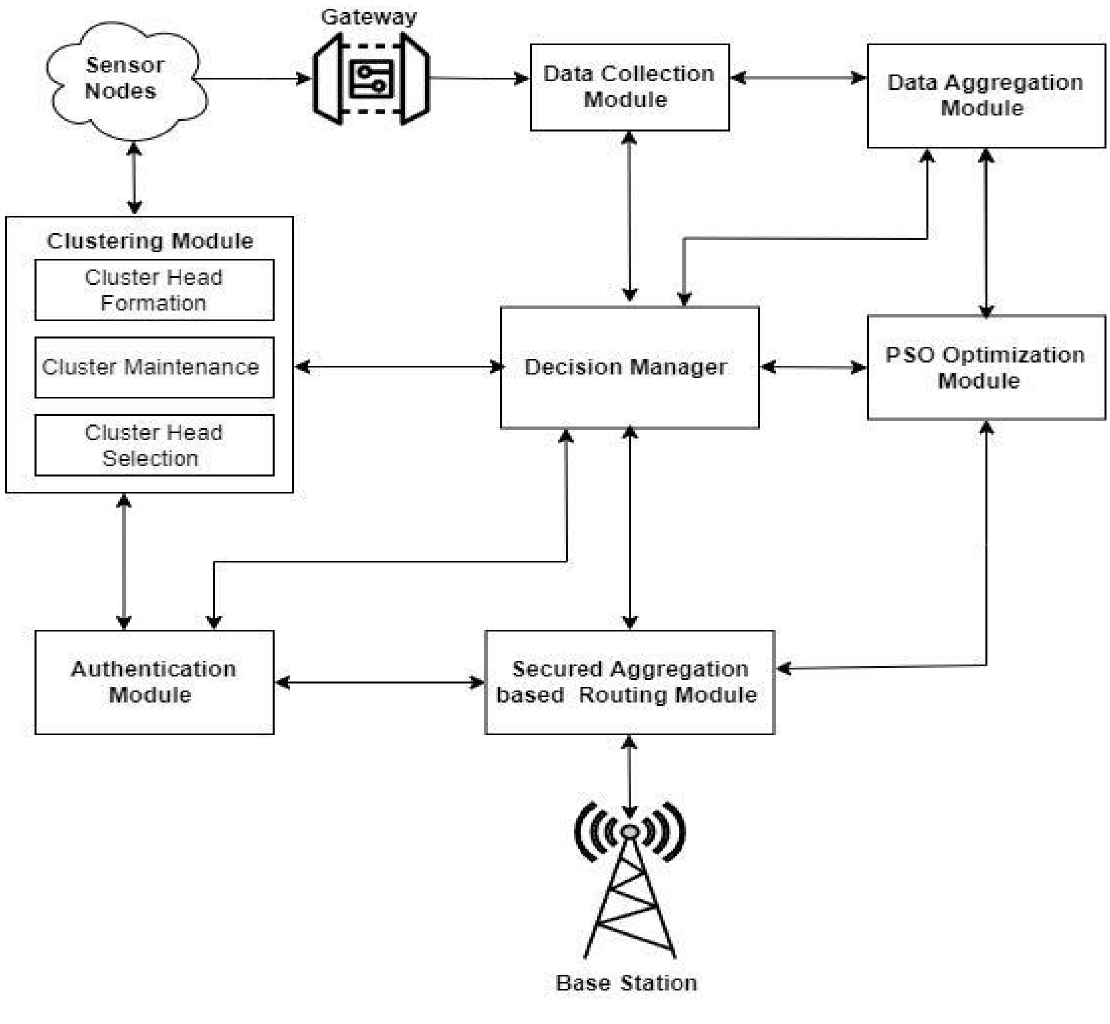

Figure. 1. Architecture of the Proposed System

Energy efficient secure data aggregation protocol operates through five phases categorized as system initialization and key generation phase, Intelligent network clustering phase, Intelligent routing phase, Aggregated data exchange phase and finally aggregated data verification phase. The creation of the public key and the private key are required for the encryption and decryption processes, is the primary goal of the system initialization and key generation phase. The next step is intelligent clustering phase where the cluster heads are originally chosen based on the distance between nodes, their degree of centrality, and their residual energy. The cluster heads are coupled with the interested nodes to create optimally unequal clusters based on the results of the cluster head election. The next step is intelligent routing phase. In this phase, the optimal routes are established with in the clusters to provide energy efficient data aggregation. Further step involves aggregated data transmission phase with which by using the optimal path, all the member nodes in the cluster transmit the data to the cluster head nodes in the secured manner.

The last step is aggregated data receiving phase. The appropriate cluster heads in this phase confirm the sensed data sent by the cluster member nodes. If the verification of aggregated data is successful then the corresponding cluster head sends the aggregated data to the Base Station else, the corresponding cluster heads will discard the aggregated data from the network.

3.1 System Initialization and key generation phase

The proposed system protocol involves the key management procedure utilizing a distributed key management mechanism. The inclusion of all network entities during the key generation process is the distributed key management mechanism's main benefit. The base station (BS) of the proposed system generates a Partial Public Key (PPLK) and a Partial Private Key (PPK), which are then transmitted through a secure channel to the associated cluster heads. Then, Cluster Heads generate the own PPK and PPLK and concatenates with the partial public key and private key generated by the BS. Finally, the member nodes in the respective clusters generate their own private key and public key. The final private key is generated by concatenating the PPK of BS, PPK of CH and PPK of member node in the cluster. The final public key is generated by concatenating the PPLKs of BS, CH and every member node in the cluster.

3.2 Optimal network Clustering Phase using PSO

The PSO algorithm begins with a collection of intelligent agents, known as the particles which are distributed at random throughout the search space. Moreover, an assumed initial velocity is given as input to the algorithm which is determined by chance. In this algorithm, a particle's fitness function is established based on its current position. The optimization problem considered in PSO is trying to find the best position for the next move, i.e., the possible position that will minimise the fitness function value. Now, the algorithm works iteratively to assess the fitness values of each particle, and it revises the velocity of the moving particles, and finally it determines the new location for movement. The particle's next velocity is calculated using its present velocity, its current position in relation to its local best and global best positions.

The PSO algorithm can perform effective intrusion detection by applying optimization of positions namely private best solution (pbest), which can be considered as the most optimal number of attributes and efficient routing path. The PSO members use the search space optimisation based on their own flying experiences to find out the importance of attributes. Moreover, the particles gather information from other particles and their environment with the respect to the formation of the clusters, in the selection of CHs. The possible attacks that can occur in the route are detected and it is used in the routing path selection. The best fitness value was achieved in this research work by firing rules. Moreover, rules are fired in this model for finding the communication activities and the contributions of member nodes within a cluster which enhances the accuracy of classification by finding the most contributing features. All the particles that are relevant and present in a cluster are referred to as the cbest particles and they are representing the attributes selected based on the behaviour of cluster members and CHs that are participating in the network communication. The cbest value is considered in this work to model the node mobility.

The PSO algorithm performs optimization of clusters and the routes for data delivery in this work. The PSO algorithm uses a number of nodes, clusters and routes which are considered as having P particles. The notation X^i (t) is used in this work for representing the position of i^{th}particle during the t^{th} iteration. Moreover, this position is expressed in this work for representing the node locations, CH locations using coordinates $X^i (t) = (x^i(t), y^i(t))$ and the paths from node I to node J are expressed using two such coordinates. In addition to their geographical locations called positions, each particle is assumed to move with a velocity denoted by the expression $Vi(t) = (v^i_x(t), v^i_y(t))$. When the particles move to a new location, the next iteration is started and hence the positions of all the moving particles will be updated using the formula given in equation (7) shown below:

$$X^i(t+1) = X^i(t) + V^i(t+1) \tag{7}$$

The new locations computed using velocities can also be represented using equation (8) and (9).

$$x^i(t+1) = x^i(t) + v^i_x(t+1) \tag{8}$$

$$y^i(t+1) = y^i(t) + v^i_y(t+1) \tag{9}$$

Moreover, the velocities are updated by applying the formula shown in Equation (10).

$$v^i(t+1) = xv^i(t) + c_1 r_1(pbest^i - x^i(t)) + c_2 r_2(gbest - x^i(t)) \quad (10)$$

Here, r_1 and $r_2$are representing the randomly generated whose values are lying between 0 and the constants w, c_1, and $c_{2.}$ These constants will serve as parameters within the PSO algorithm. Moreover, the symbol pbesti is used to denote the position at which the particle "i" has achieved its best position based on the value of f(X) throughout the exploration of the particle. Moreover, the symbol gbest is used to represent the best position which is collectively discovered by all the particles that are present within the swarm.

As both the symbols namely pbest^i and X^i (t) are representing the position vectors, the evaluation of the expression (pbest^i- $x^i(t)$)is performed using vector subtraction. By implementing this subtraction into the initial velocity V^i (t) will guide the particle to move towards its pbest^i position. In the same way, the difference operation given by the expression (gbest- X^i (t)), will make the particle to move toward the gbest position.

Here, the parameter w is used to indicate the inertia weight constant, whose value will lie between 0 and 1. This parameter is playing the pivotal role in the decision-making process for deciding the velocity and position. Moreover, the parameters c_1, and $c_2$are called as the cognitive and social coefficients which are also constants. They are useful for fine tuning the overall search process. In each iteration, both pbest^i. and gbest positions are continuously updated for representing the best positions that are discovered up to the given point.

Various clusters are formed from the network's nodes during the optimal network clustering phase. Each cluster in the network is made up of its corresponding member nodes and Cluster Heads (CHs)[27]. The CHs' primary duties include gathering sensed data from member nodes and carrying out data validation and verification. Additionally, CHs will securely send the aggregated data to BS. The network's nodes choose the CHs based on their remaining energy, their proximity to one another, and their degree of connectedness. The CHs are chosen by the member nodes for a certain period of time, after which they are chosen again when their residual energy reaches the threshold range[28]. Algorithm 4 provides the optimized clustering algorithm.

3.3. Optimal route discovery phase with PSO optimization

An ideal path is built between the respective member nodes and the CHs during the optimal route discovery phase in order to convey the sensed data from the installed environment. In the proposed system, the Base Station maintains N number of source-based routes from the corresponding member nodes to the CHs in order to maintain route reliability and fault tolerance. To compute the best route the BS, consider nodes residual energy and hop distance between corresponding member node and CHs and based on these two parameters the optimal routes are established. BS computes the hop count and current residual energy of nodes and broadcasts it to all the member of the node for the corresponding clusters. Algorithm 5 gives the steps which are involved in optimal route calculation phase.

3.4 Secured Data aggregation phase

The proposed protocol's secured data aggregation phase comes after the optimal routing phase is finished. In the phase of secured data aggregation, the suggested system offers two-way authentication. The first method of giving authentication is from cluster nodes to the associated cluster heads, and the second method is from cluster nodes to the base station. Algorithm 6 provides the steps in secured date aggregation phase.

We perform the node authentication by using a Co-ordinator (C) at the base station. The Sender (S), Intermediate Nodes (IN) and Receiver (R) must authenticate them by giving a request to the Base Station Authenticator (BSA). The request must contain the nodes MAC address, IP address, user ID, cluster ID (Cl-ID), Time Stamp (TS) and Initial Key (IK). For this purpose, the base station maintains a table consisting of the MAC addresses, IP addresses, and Initial Keys of all the nodes. Upon receiving the request from the nodes, the co-ordinator sends a new key by appending some new information to the initial key. In addition, it provides a nonce which must be sent along with the new key for authentication. The authentication must be performed by all the participating nodes for every transmission session. In this way, all the intermediate nodes also must get the authentication completed by them before they participate in the communication. The following Algorithm-8 shows the details of the proposed Energy Efficient Secured Clustering as well as Data Aggregation Routing Protocol named EESC-DARP.

4. Implementation setup and Simulation results

The suggested data aggregation scheme has been implemented by utilizing Network simulator (NS3). For the simulation of the system 1000*1000 M^{2}network area considered for the simulation. The initial energy of the nodes is considered as 100J. The 1000 sensor nodes are considered for the simulation of the proposed system. The combined size of the packet is 4065 bits. The routing protocol used by the proposed system is LEACH. The proposed system uses random way point mobility model. For encryption and decryption purpose, the SHA 512 algorithm is used. The number of rounds in this simulation is considered as 50. Performance indicators, such as Packet Delivery Ratio (PDR), delay analysis, EC analysis, NLT analysis, and FDI attack detection analysis, are used to evaluate the proposed system.

Figure 2 shows that PDR comparison between the proposed EESC-DARP and the related works by Wei Fang et.al.,[28], Ahmed Abdulhadi Jasim et.al.,[26], and Ahmed Saidi et.al.,[25].

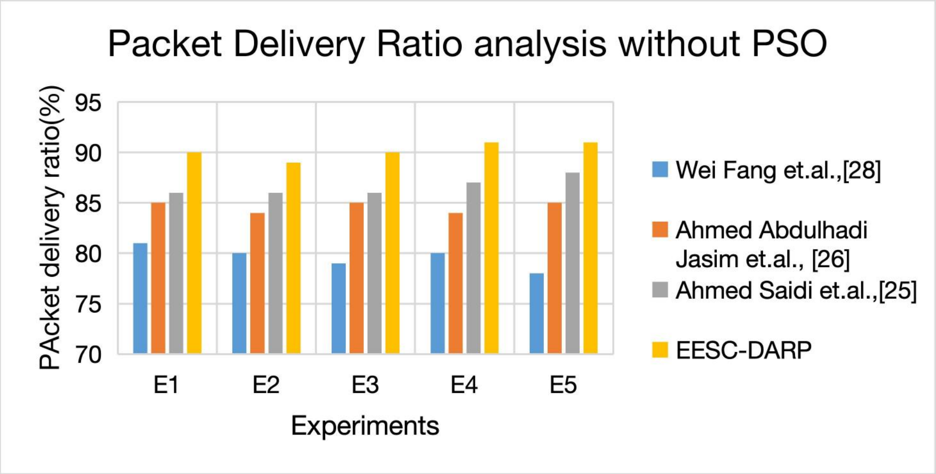

Figure 2. Packet delivery ratio analysis without PSO

Figure 2 explicates that the proposed EESC-DARP data aggregation routing scheme has improved the PDR when it is brought into comparison against the previously available protocols by Wei Fang et.al.,[28], Ahmed Abdulhadi Jasim et.al.,[26], and Ahmed Saidi et.al.,[25]. The improvement in PDR is because the proposed system discovers optimal route with clustering and transmits the packets securely during data aggregation. Moreover, the proposed system eliminates the redundancy of data packets during DA. Therefore, the system has improved PDR.

Figure 3 shows the PDR comparison between the proposed system with PSO optimization called EESCPSO-DARP and the related works by Wei Fang et.al.,[28], Ahmed Abdulhadi Jasim et.al.,[26], and Ahmed Saidi et.al.,[25].

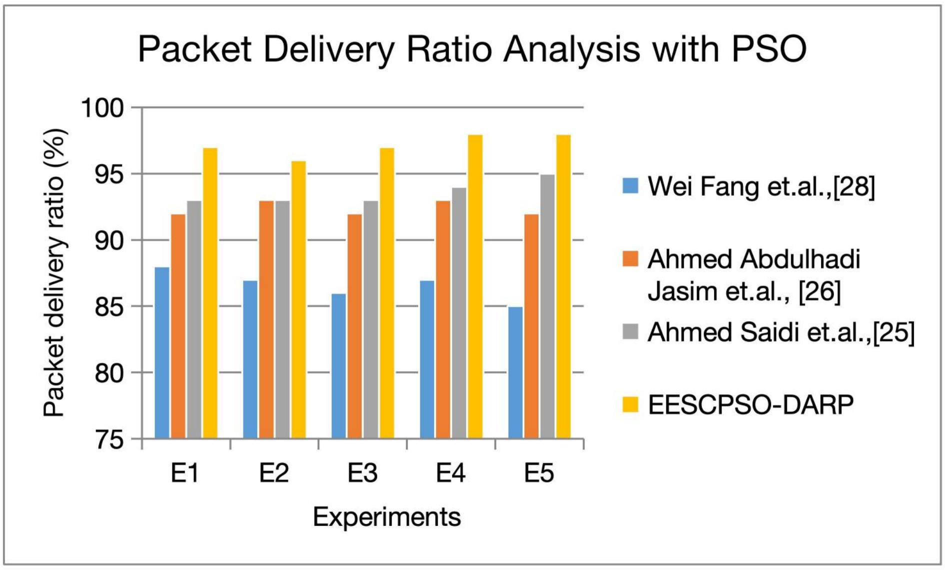

Figure 3. Packet delivery ratio analysis of routing with PSO

From Figure 3, it is shown that EESCPSO-DARP with PSO and data aggregation routing scheme has improved the PDR when it is compared with the previously available protocols by Wei Fang et.al.,[28], Ahmed Abdulhadi Jasim et.al.,[26], and Ahmed Saidi et.al.,[25].The improvement in PDR in this EESCPSO-DARP is because it discovers optimal route using PSO optimization and transmits the packets securely using authentication with data aggregation. Moreover, the proposed EESCPSO-DARP eliminates the redundancy of data packets transmitted using data aggregation. Therefore, the PSO based optimized system has improved PDR when compared to other systems and this system without PSO.

Figure 4 shows that Delay Analysis comparison between the proposed EESC-DARP and the related works by Wei Fang et.al.,[28], Ahmed Abdulhadi Jasim et.al.,[26], and Ahmed Saidi et.al.,[25].

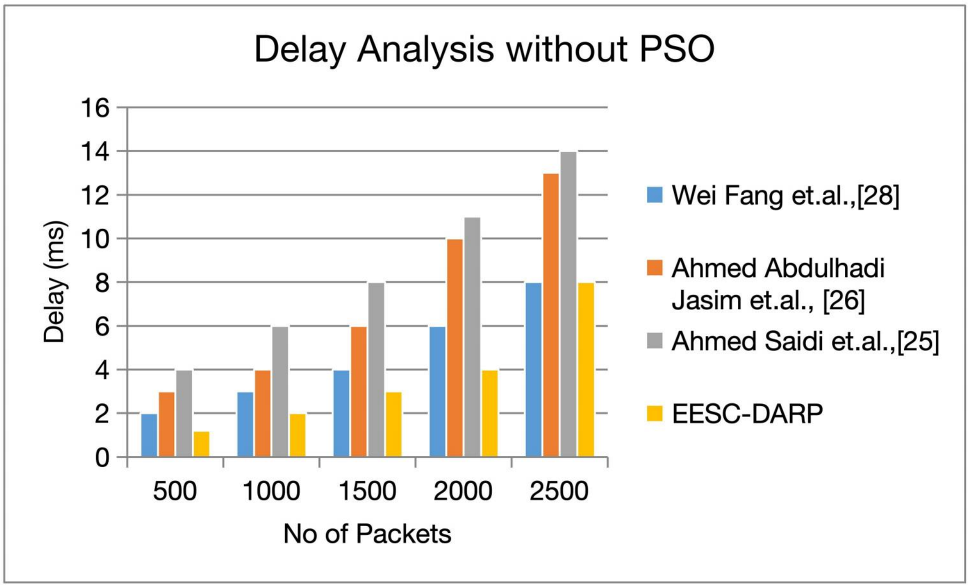

Figure 4. Delay analysis without PSO

From the figure 4, it is inferred that EESC-DARP achieves less delay when compared against the previously available protocols by Wei Fang et.al.,[28], Ahmed Abdulhadi Jasim et.al.,[26], and Ahmed Saidi et.al.,[25]. The improvement in the delay is because that the proposed system uses better route discovery through CHs and considers the different source-based routes dynamically by considering the network changes. Due to that, when one route fails also other route will take over and transmit the packets more efficiency with minimal delay. Therefore, the system has improved delay analysis when it is brought into comparison against the previously available protocols by Wei Fang et.al.,[28], Ahmed Abdulhadi Jasim et.al.,[26], and Ahmed Saidi et.al.,[25].

Figure 5 shows the delay comparison analysis between the proposed protocol namely EESCPSO-DARP with PSO and the previously available protocols by Wei Fang et.al.,[28], Ahmed Abdulhadi Jasim et.al.,[26], and Ahmed Saidi et.al.,[25].

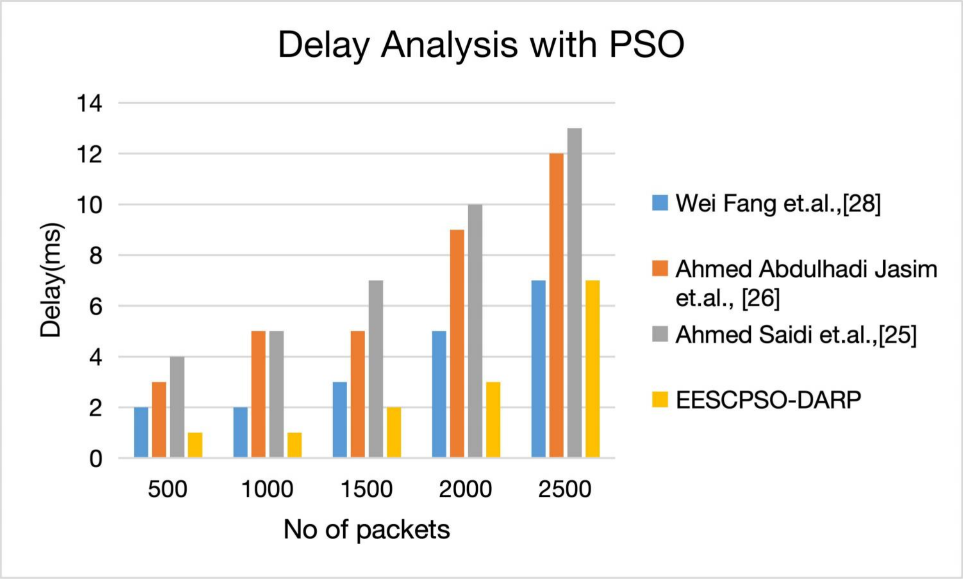

Figure 5. Delay analysis with PSO

From the figure 5, it is inferred that the proposed system namely EESCPSO-DARP achieves minimum delay when compared against the previously available protocols by Wei Fang et.al.,[28], Ahmed Abdulhadi Jasim et.al.,[26], and Ahmed Saidi et.al.,[25]. The improvement in the delay in EESCPSO-DARP is due to the fact that proposed system discovers the different source-based routes dynamically by considering the network changes and uses PSO in cluster and route optimization along with data aggregation. Due to that, when one route fails also other route will take over and transmit the packets more efficiency with minimal delay. Therefore, the system has improved delay analysis when it is brought into comparison against the previously available protocols.

Figure 6 shows that EC Analysis comparison between the proposed EESC-DARP and the related by Wei Fang et.al.,[28], Ahmed Abdulhadi Jasim et.al.,[26], and Ahmed Saidi et.al.,[25].

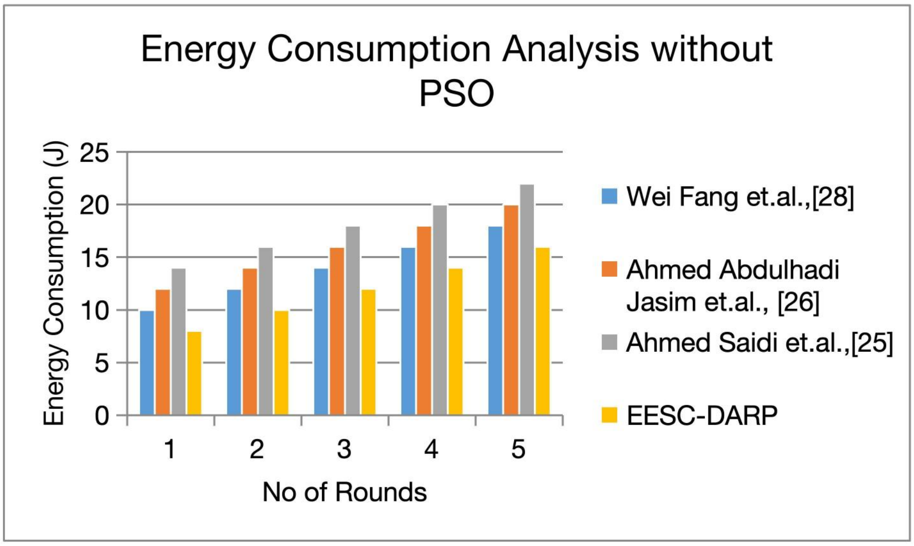

Figure 6. Energy Consumption Analysis without PSO

The figure 6 explicates that the proposed EESC-DARP system has reduced its EC rate when it is brought into comparison against the previously available protocols by Wei Fang et.al.,[28], Ahmed Abdulhadi Jasim et.al.,[26], and Ahmed Saidi et.al.,[25]. The proposed system employs the optional nodes and discovers the best route and transmits the data to other nodes via secured route. Furthermore, the system decreases the redundancy and retransmission of data during data aggregation and node authentication. Therefore, the system has optimized its energy consumption rate when it is brought into comparison against the previously available protocols.

Figure 7 shows the Energy Consumption Analysis between EESCPSO-DARP related systems by comparing it with the previously available protocols by Wei Fang et.al.,[28], Ahmed Abdulhadi Jasim et.al.,[26], and Ahmed Saidi et.al.,[25].

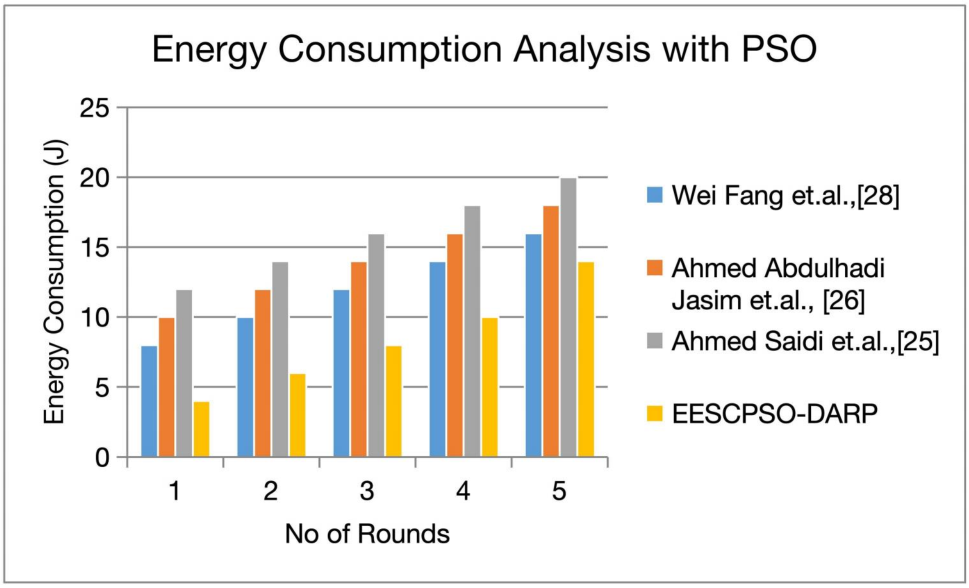

Figure 7. Energy Consumption Analysis with PSO

Figure 7 explains that the EESCPSO-DARP system has improved its energy consumption rate when it is brought into comparison against the previously available protocols by Wei Fang et.al.,[28], Ahmed Abdulhadi Jasim et.al.,[26], and Ahmed Saidi et.al.,[25]. The proposed EESCPSO-DARP reduced the energy consumption by employing PSO and uses the optional nodes and discovers the best route and transmits the data to other nodes via secured route. Furthermore, the system decreases the redundancy and retransmission of data during data aggregation using PSO. Therefore, the system has reduced its energy consumption rate when it is brought into comparison against the previously available protocols by Wei Fang et.al.,[28], Ahmed Abdulhadi Jasim et.al.,[26], and Ahmed Saidi et.al.,[25].

Figure 8 shows the Network Life time analysis comparison between the proposed EESC-DARP and the related by Wei Fang et.al.,[28], Ahmed Abdulhadi Jasim et.al.,[26], and Ahmed Saidi et.al.,[25].

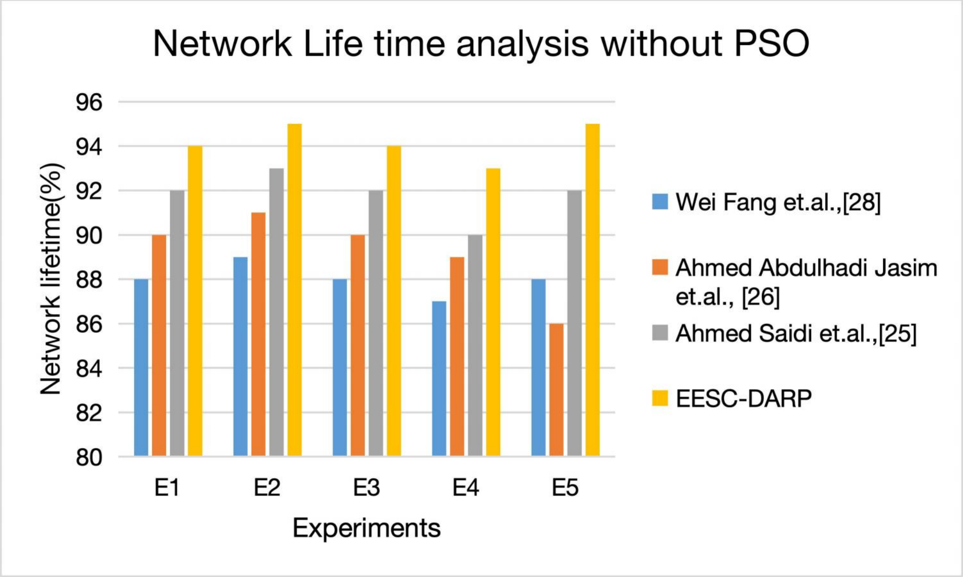

Figure 8. Network life time analysis without PSO

The Figure 8. explicates that our proposed protocol called EESC-DARP has reduced its EC rate when it is brought into comparison against the previously available protocols by Wei Fang et.al.,[28], Ahmed Abdulhadi Jasim et.al.,[26], and Ahmed Saidi et.al.,[25]. The proposed system employed clustering rules and discovered the best route through CHs and transmitted the data to other nodes via secured routing path using authentication. Hence, the proposed system called EESC-DARP has reduced the redundancy and retransmission of data during data aggregation. Therefore, the system has improved the overall network life time.

Figure 9 shows the Network Life time analysis between the proposed EESCPSO-DARP by comparing it with the previously available protocols by Wei Fang et.al.,[28], Ahmed Abdulhadi Jasim et.al.,[26], and Ahmed Saidi et.al.,[25].

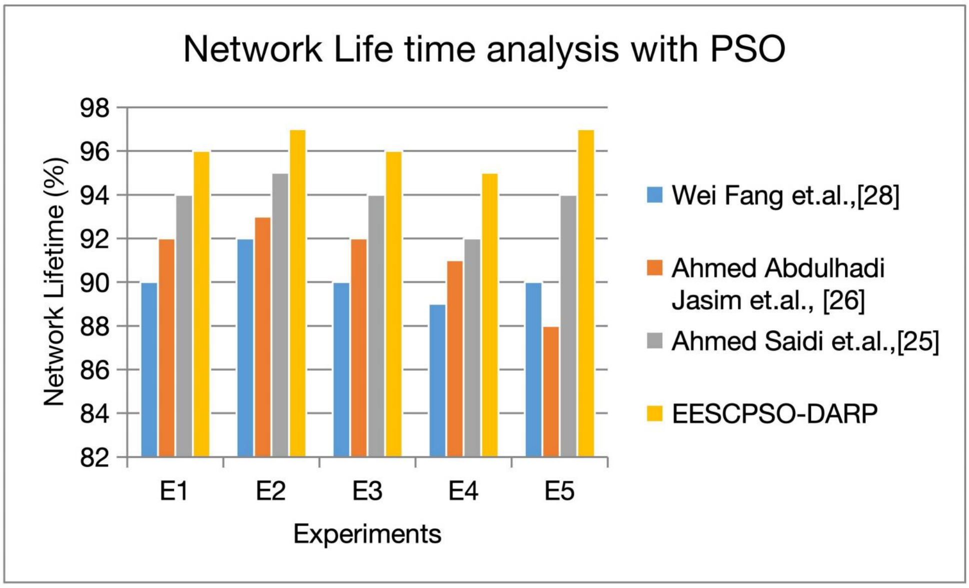

Figure 9. Network life time analysis with PSO

The Figure 9. explicates that the proposed EESCPSO-DARP has improved the NLT when it is brought into comparison against the previously available protocols by Wei Fang et.al.,[28], Ahmed Abdulhadi Jasim et.al.,[26], and Ahmed Saidi et.al.,[25]. The proposed system employed PSO in clustering and discovered the best route with PSO optimization, data aggregation and node authentication and transmitted the data to other nodes via secured routing path. Moreover, the proposed system reduces the redundancy and retransmission of data during data aggregation. Therefore, the system has improved network life time.

Figure 10 shows the False data injection attack analysis comparison between the proposed EESC-DARP and the related by Wei Fang et.al.,[28], Ahmed Abdulhadi Jasim et.al.,[26], and Ahmed Saidi et.al.,[25].

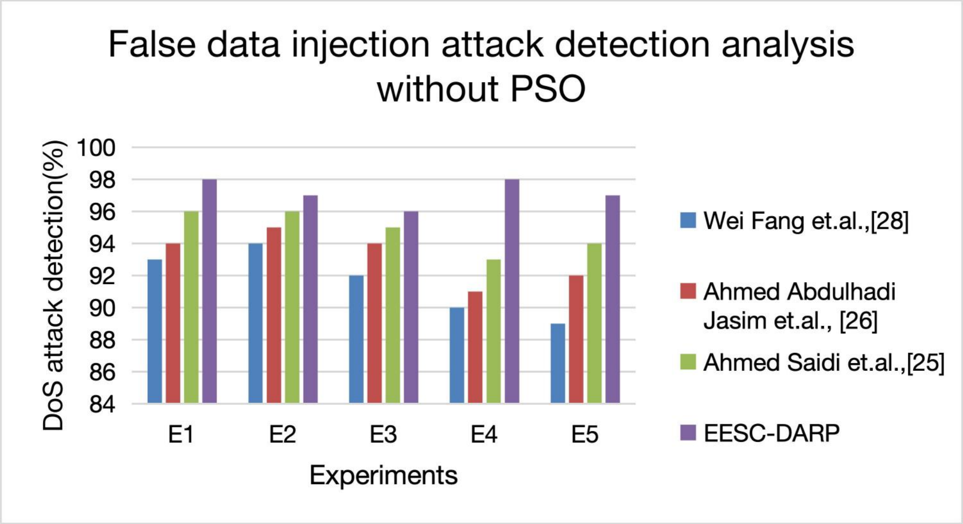

Figure 10. False data injection attack analysis without PSO

Figure 10 shows that the proposed system reduced the false data attack injection when compared to the works by Wei Fang et.al.,[28], Ahmed Abdulhadi Jasim et.al.,[26], and Ahmed Saidi et.al.,[25]. The reason behind the result is that the proposed system employed PSO in clustering and discovered the best routes with PSO optimization and CH selection and usage and hence transmits the data to other nodes via secured routing path through better authentication.

Figure 11 shows the False data injection attack analysis comparison between the proposed EESCPSO-DARP and the existing systems by comparing it with the previously available protocols by Wei Fang et.al.,[28], Ahmed Abdulhadi Jasim et.al.,[26], and Ahmed Saidi et.al.,[25].

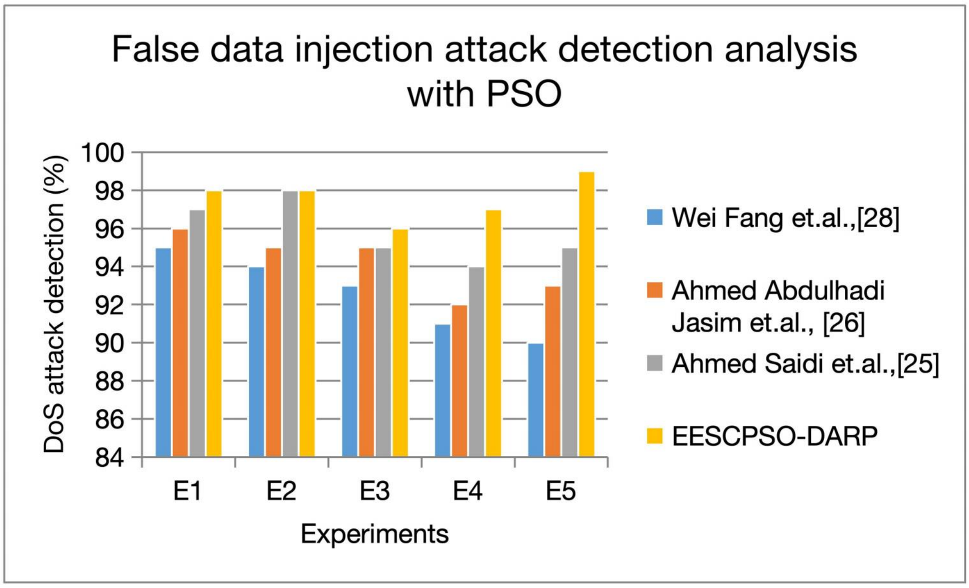

Figure 11. False data injection attack analysis with PSO

From Figure 11, it is clear that the proposed EESCPSO-DARP reduced the false data attack injection by detecting and preventing them using rules. The proposed system employed PSO, data aggregation and clustering to discover the best route and transmitted the data to sink node via secured routing path. Hence, the proposed EESCPSO-DARP increased the security in routing when it is compared with the existing works proposed by Wei Fang et.al.,[28], Ahmed Abdulhadi Jasim et.al.,[26], and Ahmed Saidi et.al.,[25]. Table 1 depicts the complexity analysis of the EESC-DARP with the chosen benchmarks for secured data aggregation in WSN.

Works/ Complexity	Time Complexity	Space Complexity	Crypt Analysis Complexity
Wei Fang et.al.,[28]	$O(n^3)$	$O(n^2)$	Polynomial Time
Ahmed Abdulhadi Jasim et.al., [26]	$O(n^2)$	$O(n^3)$	Polynomial Time
Ahmed Saidi et.al.,[25]	$O(n^2)$	$O(n^3)$	Polynomial Time
Proposed	$O(n \log n)$	$O(n^2)$	Discrete logarithmic

Table 1: Space and Time Complexity

Table 1 clearly shows that the proposed EESC-DARP provides less space and time complexity when compared with its counterparts thereby achieving security and efficient data transmission. The proposed protocol minimizes the redundancy of transmitted data and thereby enhances the lifespan of the nodes. The proposed protocol utilizes distributed key management method where the key generation responsibilities are shared among the BS, the CH nodes and member nodes in the cluster. By doing so, the computational complexity of the proposed protocol is minimized when it is brought into comparison against the previously available protocols. The system employs optimal routes discover technique between the nodes to CH and CH to the BS in an effective manner. By doing so, the communication overhead of the protocol is better and also has improved time complexity and space complexity when it is brought into comparison against the previously available protocols. Furthermore, crypt analysis of the system is difficult since it needs to resolve the logarithm problem.

5. Conclusion and future work

In this work, energy efficient and secured data aggregation scheme and an authentication scheme have been introduced in order to increase the security of the routing system and to make it more efficient. The proposed secure routing system uses the distributed key management method and discovers the optimal route using PSO, clustering, data aggregation and authentication of nodes including the starting node and end node. Moreover, the proposed protocol employed better authentication protocol which provided two-way authentications for the source-based routes during the data aggregation. Hence, the proposed protocol provides enhanced security and identifies rogue or intruder nodes through data aggregation. The proposed protocol has been implemented using NS3 simulator. As a result of the simulation the system has improved its performance in terms of PDR, NLT, delay, false data injection and malicious attack identification accuracy when it is brought into comparison against the previously available protocols. The future direction considered for the proposed work is to develop a secure routing protocol for data aggregation for the nodes with mobility.

References

[1] Jin Y, Kwak K S, and Yoo S J, 2020, “A novel energy supply strategy for stable sensor data delivery in wireless sensor networks” ,*IEEE Systems. Journal.*, vol. 14, no. 3, pp. 3418_3429.

[2] Cengiz K and Dag T, 2018, “Energy aware multi-hop routing protocol for WSNs”, IEEE Access, vol. 6, pp. 26222633.

[3] Das S.K and Tripathi S, 2018 ``Intelligent energy-aware efficient routing for MANET," Wireless Networks., vol. 24, no. 4, pp. 1159.

[4] Sasirekha S and Swamynathan S, 2017, ``Cluster-chain mobile agent routing algorithm for efficient data aggregation in wireless sensor network," Journal of Communication. Networks., vol. 19, no. 4, pp. 392-401.

[5] Haseeb K, Islam N, Saba T, Rehman A, and Mehmood Z, 2020, ``LSDAR: A light-weight structure-based data aggregation routing protocol with secure Internet of Things integrated next-generation sensor networks," Sustain. Cities Soc., vol. 54, pp. 1-9.

[6] Thangaramya K, Kulothungan K, Logambigai R, Selvi M, Ganapathy S, and Kannan A, 2019, ``Energy aware cluster and neuro-fuzzy based routing algorithm for wireless sensor networks in IoT," Computer Networks., vol. 151, pp. 211-223.

[7] Lee J S and Teng C L, 2017, ``An enhanced hierarchical clustering approach for mobile sensor networks using fuzzy inference systems," IEEE Internet Things J., vol. 4, no. 4, pp. 1095-1103.

[8] El Alami H and Najid A, 2019, ``ECH: An enhanced clustering hierarchy approach to maximize lifetime of wireless sensor networks," IEEE Access, vol. 7, pp. 107142-107153.

[9] Rajasoundaran S, Kumar SVN, Selvi M, Ganapathy S, Rakesh R, Kannan A, 2021,” Machine learning based volatile block chain construction for secure routing in decentralized military sensor networks”, Wireless Networks, vol 27 (7), pp. 4513-4534.

[10] Santhosh Kumar SVN, Yogesh Palanichamy, Selvi M, Sannasi Ganapathy, Arputharaj Kannan, Sankar Pariserum Perumal, 2021,” Energy efficient secured K means based unequal fuzzy clustering algorithm for efficient reprogramming in wireless sensor networks”, wireless networks, vol 27, pp. 3873-3894.

[11] Munuswamy Selvi, SVN Santhosh Kumar, Sannasi Ganapathy, AyyasamyAyyanar, Harichandran Khanna Nehemiah, Arputharaj Kannan, 2021,” energy efficient clustered gravitational and fuzzy based routing algorithm in WSNs”. Wireless Personal Communications, vol 116 (1).

[12] Yesodha, K., Krishnamurthy, M., Thangaramya, K. and Kannan, A., 2024. Elliptic curve encryption-based energy-efficient secured ACO routing protocol for wireless sensor networks. The Journal of Supercomputing, Vol. 80, pp. 18866–18899.

[13] Jasper J, 2021, “A secure routing scheme to mitigate attack in wireless ad hoc sensor network”, Computers & Security: Elsevier, vol.103, pp:102197.

[14] Kowsalya R, Jeetha BR, 2021, “Cluster based data-aggregation using lightweight cryptographic algorithm for wireless sensor networks”, Materials Today: Proceedings: Elsevier.

[15] Hassan A, Anter A, Kayed M, 2021, “A robust clustering approach for extending the lifetime of wireless sensor networks in an optimized manner with a novel fitness function”, Sustainable Computing: Informatics and Systems: Elsevier, vol.30, pp:100482.

[16] Maheswari M, Karthika R A, 2021, “A Novel QoS Based Secure Unequal Clustering Protocol with Intrusion Detection System in Wireless Sensor Networks”, Wireless Personal Communications: Springer, vol.118(2), pp:1535-57.

[17] Mosavifard A, Barati H. A, 2020, “An energy-aware clustering and two-level routing method in wireless sensor networks”, Computing: Springer vol.102(7), pp:1653-71

[18] Bongale AM, Nirmala CR, Bongale AM, 2020, “Energy efficient intra cluster data aggregation technique for wireless sensor network”, International Journal of Information Technology: Springer. Vol. 27, pp.1-9.

[19] Deebak BD, Al-Turjman F, 2020, “A hybrid secure routing and monitoring mechanism in IoT-based wireless sensor networks”, Ad Hoc Networks: Elsevier, vol. 97, pp:102022.

[20] Saidi A, Benahmed K, Seddiki N, 2020, “Secure cluster head election algorithm and misbehaviour detection approach based on trust management technique for clustered wireless sensor networks”, Ad Hoc Networks: Elsevier, vol.106, pp:102215.

[21] Revanesh M, Sridhar V, Acken JM, 2020, “Secure Coronas Based Zone Clustering and Routing Model for Distributed Wireless Sensor Networks”, Wireless Personal Communications: Springer, vol. 112(3), pp:1829-57.

[22] Zhang, Y., Zhang, X., Ning, S., Gao, J., & Liu, Y. 2019, “Energy-efficient multilevel heterogeneous routing protocol for wireless sensor networks”, IEEE Access, 7, pp.55873-55884.

[23] Mehetre DC, Roslin SE, Wagh SJ, 2019, “Detection and prevention of black hole and selective forwarding attack in clustered WSN with Active Trust”, Cluster Computing: Springer. Vol.22(1), pp:1313-28.

[24] Hongjuan Li, Kai Lin, Keqiu Li, 2011,” Energy-efficient and high-accuracy secure data aggregation in wireless sensor networks”, computer communications, vol.34, pp. 591-597.

[25] Ahmed, Saidi, Khelifa Benahmed, and Nouredine Seddiki. "Secure cluster head election algorithm and misbehaviour detection approach based on trust management technique for clustered wireless sensor networks." Ad Hoc Networks, vol.106, 2020 pp:102215.

[26] Ahmed Abdulhadi, Jasim, Mohd Yamani Idna Bin Idris, Saadial Razalli Bin Azzuhri, Noor Riyadh Issa, Noorzaily Bin Mohamed Noor, Jagadeesh Kakarla, and Iraj Sadegh Amiri. "Secure and energy-efficient data aggregation method based on an access control model." IEEE Access, vol.7, 2019, pp:164327-164343.

[27] Osama A. Khashan a,, Rami Ahmad Nour M. Khafajah, 2021, “An automated lightweight encryption scheme for secure and energy-efficient communication in wireless sensor networks”, ad hoc networks, vol 115.

[28] Wei Fang, XueZhi Wen, Jiang Xu, JieZhong Zhu, 2019, “CSDA: a novel cluster-based secure data aggregation scheme for WSNs, “Cluster Computing, vol. 22, pp. 5233- 5244.

[29] Haseeb, Khalid, Naveed Islam, Tanzila Saba, Amjad Rehman, and Zahid Mehmood, 2020, "LSDAR: A light-weight structure-based data aggregation routing protocol with secure internet of things integrated next-generation sensor networks." *Sustainable Cities and Society* 54, 101995.

[30] Hu, Peng, Xixi Chu, LaishuiLv, Kaizhong Zuo, Tianjiao Ni, Taochun Wang, and Zhangyi Shen. 2023, "An efficient and secure data collection scheme for predictive maintenance of vehicles." *Ad Hoc Networks* vol.146, pp.103157.

[31] Wu, Qiyu, Fucai Zhou, Jian Xu, Qiang Wang, and Da Feng, 2022, "Secure and efficient multifunctional data aggregation without trusted authority in edge-enhanced IoT." *Journal of Information Security and Applications* vol.69, pp.103270.

[32] Alghamdi, Wael Y, 2023, "Designing A Secure and Long-Lived WSN for Data Collection." *Procedia Computer Science* 220 pp. 187-194.

[33] Dorsala, Mallikarjun Reddy, V. N. Sastry, and Sudhakar Chapram, 2022, "Fair payments for privacy-preserving aggregation of mobile crowdsensing data." *Journal of King Saud University-Computer and Information Sciences* 34, no. 8,pp.5478-5492.

[34] Khan, H.M., Khan, A., Jabeen, F., Anjum, A. and Jeon, G., 2021. Fog-enabled secure multiparty computation-based aggregation scheme in smart grid. *Computers & Electrical Engineering*, *94*, p.107358.

[35] Sindhuja, M., Vidhya, S., Jayasri, B.S. and Shajin, F.H., 2023. Multi-objective cluster head using self-attention based progressive generative adversarial network for secured data aggregation. *Ad Hoc Networks*, *140*, p.103037.

[36] Regueiro, C., Seco, I., de Diego, S., Lage, O. and Etxebarria, L., 2021. Privacy-enhancing distributed protocol for data aggregation based on blockchain and homomorphic encryption. *Information Processing & Management*, *58*(6), p.102745.

[37] Othman, S.B., Almalki, F.A., Chakraborty, C. and Sakli, H., 2022. Privacy-preserving aware data aggregation for IoT-based healthcare with green computing technologies. *Computers and Electrical Engineering*, *101*, p.108025.

[38] Shen, X., Zhu, L., Xu, C., Sharif, K. and Lu, R., 2020. A privacy-preserving data aggregation scheme for dynamic groups in fog computing. *Information Sciences*, *514*, pp.118-130.

[39] Ravi, G., Das, M.S. and Karmakonda, K., 2023. Reliable cluster-based data aggregation scheme for IoT network using hybrid deep learning techniques. *Measurement: Sensors*, *27*, p.100744.

[40] Gao, Y., Li, Q., Zheng, Y., Wang, G., Wei, J. and Su, M., 2022. SEDML: Securely and efficiently harnessing distributed knowledge in machine learning. *Computers & Security*, *121*, p.102857.

[41] Lu, S., Li, R., Liu, W., Guan, C. and Yang, X., 2023. Top-k sparsification with secure aggregation for privacy-preserving federated learning. *Computers & Security*, *124*, p.102993.

[42] Anitha, S., Saravanan, S. and Chandrasekar, A., 2023. Trust management based multidimensional secure cluster with RSA cryptography algorithm in WSN for secure data transmission. *Measurement: Sensors*, p.100889.

[43] Liu, X., Yu, J., Yu, K., Wang, G. and Feng, X., 2022. Trust secure data aggregation in WSN-based IIoT with single mobile sink. *Ad Hoc Networks*, *136*, p.102956.

[44] Lin, H., Garg, S., Hu, J., Kaddoum, G., Peng, M. and Hossain, M.S., 2020. A blockchain-based secure data aggregation strategy using sixth generation enabled network-in-box for industrial applications. *IEEE Transactions on Industrial Informatics*, *17*(10), pp.7204-7212.

[45] Shim, K.A. and Park, C.M., 2014. A secure data aggregation scheme based on appropriate cryptographic primitives in heterogeneous wireless sensor networks. *IEEE transactions on parallel and distributed systems*, *26*(8), pp.2128-2139.

[46] Xue, K., Zhu, B., Yang, Q., Wei, D.S. and Guizani, M., 2019. An efficient and robust data aggregation scheme without a trusted authority for smart grid. *IEEE Internet of Things Journal*, *7*(3), pp.1949-1959.

[47] Rezaeibagha, F., Mu, Y., Huang, K. and Chen, L., 2020. Secure and efficient data aggregation for IoT monitoring systems. *IEEE Internet of Things Journal*, *8*(10), pp.8056-8063.

[48] Jasim, A.A., Idris, M.Y.I.B., Azzuhri, S.R.B., Issa, N.R., Noor, N.B.M., Kakarla, J. and Amiri, I.S., 2019. Secure and energy-efficient data aggregation method based on an access control model. *IEEE Access*, *7*, pp.164327-164343.

[49] Zhang, J. and Dong, C., 2022. Secure and lightweight data aggregation scheme for anonymous multi-receivers in WBAN. *IEEE Transactions on Network Science and Engineering*, *10*(1), pp.81-91.

[50] Rezvani, M., Ignjatovic, A., Bertino, E. and Jha, S., 2014. Secure data aggregation technique for wireless sensor networks in the presence of collusion attacks. *IEEE transactions on Dependable and Secure Computing*, *12*(1), pp.98-110.

Annex

Algorithm 1 – Creation of RSA based PPK and PPLK by the BS

```
Begin
Step 1. Abstractly select two relatively prime numbers P1, Q1 from the key pool K such that $P1 \neq Q1$.
Step 2. Calculate N = (P1 x    Q1)
Step 3. Calculate R = LCM ((P1-1), (Q1-1) // using Euler's Phi function
Step 4. Choose the random integers a,b,c and h $\in$ G // where G is the cyclic group with generator G
Step 5. Calculate G1 = (aP1. bQ1) mod N
Step 6. Compute H1 = (cQ1. hQ2) mod N
Step 6. Compute R1 = (G1(hN) ) mod Ø (N)
Step 7. Compute F1 = (R1GN) mod N
Step 8. PPK (BS (PR (PBS))) = {R1,H1}                    (1)
Step 9. PPLK (BS (PU(PBS)))    =    {G1,F1}              (2)
Step.10 Return
```

The base station created the partial public and private key which can be depicted by the equation (1) and equation (2). These (PR (PBS)) and (PU(PBS)) are transmitted to the corresponding cluster heads via secured channel.

Algorithm 2. Creation of PPLK and PPK generated by Cluster Heads

```
Step 1. Abstractly select two relatively prime integers C1, D1, G2 $\in$ G // where G is the cyclic group with generator G
Step 2. Compute B1 = (C1G1. D1G2) Mod P1
Step 3. Compute X1 = F1(C1.G2) Mod N
Step 3. Compute Y1 = (X1F1.D1G2) Mod N
Step 4. Compute Z1 = (Y1X1). (C1F1) mod N
Step 5. Return Partial Private Key of CH (PR (PCH)) = {Y1, Z1}
Step 6. The Final Private key of CH (PR (PCH)) = partial private key of BS || partial private key of CH
Step 7. PPK( CH (PR (PCH)) )= {R1,H1Y1,Z1}               (3)
Step 8. Return PPLK ( CH (PU (PCH))) = {B1, X1}
Step 9. The final public key of CH (PU (PCH)) =      PPLK (BS) || PBLK (CH)
Step 10.    Return PPLK ( CH (PU (PCH))) = {X1, B1, G1, F1}        (4)
```

Equation (3) and Equation (4) denotes the partial private and partial public key generated by CH nodes. The generated (PR (PCH)) and (PU (PCH)) are sent to corresponding member nodes via secure channel.

Algorithm 3. Algorithm to generate PPK and PPLK by member nodes

```
Step-1: Read node details
Step-2: For all member nodes in a cluster [1 to N] Do Begin
Step-3:    Choose two random relative prime numbers P1, Q1 $\in$ G
// where G is the cyclic group with generator G
Step-4: Compute N = P1*Q1
Step-5: Choose random integers S1, K1, R1 by using cyclic generator G
Step-6: Compute P1 = (S1P1. K1Q1 ) Mod N
Step-7: Compute Q1 = Q1P1 . R1S1) mod N
Step-8: Compute E1 = (Q1R1 . P1Q1) Mod N
Step-9: Compute S1 = (E1Q1. Q1P1) Mod N
Step -10: Return PPK( MN (PR (Pmn))) = {P1, Q1}
Step -11: The final Private key of MN (PR (Pmn)) =      PPK(CH ) || PPK ( MN)
```

```
Step-12: Total private key of MN (PR (Pmn)) = {P1, Q1, R1, H1Y1, Z1}                    (5)
Step-13: Return PPLK(MN (PU (Pmn)) ) = {E1, S1}
Step-14: The final public key of MN (Pu (Pmn)) =     PPLK( CH) || PPLK(MN)
Step-15: Total     public of MN (PU (Pmn)) = {E1, S1, X1, B1, G1, F1}                     (6)
```

The members of the clusters generate the total private key depicted by using Equation (5) and (6). The obtained total public key and private key helps for encryption and decryption of aggregated data from member nodes in clusters to the CHs and from corresponding clusters Heads to the BS for an efficient secured communication.

Algorithm 4: Algorithm for optimized clustering of nodes

```
Begin
Step 1:
Step 2: Initialize DV = 0 // where DV is the Decision Value
Step 3:         For the nodes N[i] with I =1 to N    Do
Step 4:    Begin
Step 5: Compute the average residual energy of the nodes
//Where, REnis the total residual energy of node n, Enis the initial energy of node n and ESn is dissipated energy of the node n//.
Step 6: Calculate the Distance    // Where, d = Distance between the nodes to the cluster heads.
Step 7: Compute (4)
//DCn is the degree of connectivity between the CH and member nodes, Cn is the nodes connectivity and nm are the quantity of members constitute the network //
Step 8: BS computes the weightage factor WF for,d,    by using the equation (11)

                              //The Weightage factors    are assigned by the BS which depends upon the tropology changes and underlining network conditions
Step 9: Call PSO and Fuzzy rules to check and optimize the clustering process in the network
Step 10:        If// When Decision Value is greater than the Value DV, the node N is made as the cluster head
Step 11:    Then CH=N
Step 12:    // When Decision Value DVn is equal to the Value DV, alternate cluster head is chosen from the nodes in the network
Step 13: End
Step 14:        Fori=1 to JDo
Step 15: Begin
Step 16:    // where Th is the threshold value for the residual energy of the node
Step 17:        Then add    to    //nth node in the network is added to the cluster j
Step 18:                End
Step 19:              Return (CH, CHMN, BS) // where CH is the Cluster Head, CHMN is the Cluster head member nodes and BS is the Base Station.
Step 20: End
```

Algorithm 5: Optimal route discovery phase r

```
Step 1: For all the member nodes in a corresponding clusters N = 1 to NDo //Where N is the        amount of member nodes that are present in the relevant Cluster.
Step 2: For all the Cluster Head nodes present in the network j = 1 to k Do
Step 3: For all source-based route R[i] between MN and corresponding CH[J] // where mn are the nodes that make up the relevant Cluster
Step 4: For all the member nodes and CHs in a corresponding clusters N[i] to CH[j] do
Step 5: Compute BS (REmn, Hop_distance [MN to CH[j]] // where REmnis the residual energy of the member node in the corresponding cluster.
Step 6:            Begin
Step 7: For the source base route R[i] = 1 to k Do
Step 8: Begin
Step 9:    Make node N[i] as source S and CH[j] as the corresponding cluster head
Step 10: If Distance (Ni[Si],CHj[Di])==Low and residual _Energy(N[i],path])==High
Step 11: Then Priority (Route[i,j,path])== High
Step 12:      If Distance (Ni[Si],CHj[Di])==Medium and residual _Energy(N[i],path])==High
Step 13:            Then Priority (Route[i,j,path])== High
Step 14:              IFDistance(Ni[Si],CHj[Di])==High    and residual _Energy(N[i],path])==High
Step 15:           ThenPriority(Route[i,j,path])==Medium
Step 16:        If Distance (Ni[Si],CHj[Di])==High and residual _Energy(N[i],path])==Medium
Step 17:                        Then Priority(Route[i,j,path]) == Medium
Step 18:        If Distance (Ni[Si],CHj[Di])==High and residual _Energy(N[i],path])==Low
Step 19:           Then Priority(Route[i,j,path])== Low
Step 20:       If Priority (Route[i,j,path])== High
Step 21:      Select the source base route which has high priority followed by medium priority and low priority
Step-22: Apply PSO and find the fitness of route.
Step 23:        If fittest route found then Return
                                Else
                          Update Velocity
Step 24:        End
```

Algorithm 6. Secured data aggregation phase

```
Step 1: For all nodes i present in the cluster n
Step 2: Do
The cluster nodes i encrypt the data with the public key by using the formula $E= M(e1)*M(q1)* M(r1)$and sent it to the corresponding CH via best possible route. Where E is the encrypted message (Cipher text), M is the plain text and e1, q1, r1 are the generated public keys
The corresponding CHs first validate the authenticity of data by decrypting with its private key by using the formula $m = C (1/e1+q1+r1)$ where M is actual message (Plain text) and C is the cipher text.
Step 3: If decrypting of data is successful Then
        3 (a). Data packets are accessed by CH
        Else
3 (b).    Packets are discarded by the Base Station
End IF
End For
Step 4: For all the Corresponding CHs of the respective clusters do the following
4 (a). Check for redundant data which have been sent by the respective CHs in the cluster.
4(b).      If there exits the redundant data then
4(c).    CHs apply average function to minimize the redundancy of data.
End IF
End For
Step 5: For all the Corresponding CHs of the respective clusters do
```

```
5(a). The respective CHs encrypt the data with its private key and sign them and transmit the data to BS via optimal route
5 (b). The BS verifies the information transmitted by each cluster head.
5 (c). If validation is successful then
5 (d). The data packets delivered by the various cluster leaders are accepted by BS.
Else
5 (e). BS will discard the data packets and mark the respective CHs and its corresponding cluster nodes as malicious nodes and will not involve them in routing process.
End IF
END for
Step 6: Return
```

Algorithm 7 Authentication

```
Input: Node Details
Output: Authenticated / Not Authenticated
Step-1: Read Node Details
Step-2: Perform Sender Authentication
Step-3: Return Result (Sender Authentication)
Step-3 :    IF Sender Authenticated then
                                  Perform Receiver Authentication
Step-4: Return Result (Receiver Authentication)
Step:5 : IF (Sender Authenticated and Receiver Authenticated)
Step-6: Label Nodes as Trusted Nodes
Step-7: Issue (Communication_Token)
Sender Authentication:
        S to C: MACA (S) || IP-Addr(S) || Cl_ID(S) || IK(S) || TS(S)
C to S: IK (S) || NK (S) || Cl-ID(S) || NONCE (S) || TS(S)
S to C: IK (S) || NK (S) || NONCE (S) || TS (S)
C to S: TS (S) || OK (S) || TS (C)
Here, TS (S) and TS (C) indicates the Times Stamps provided by the sender and Co-ordinator respectively.
Receiver Authentication:
        S to R: MACA (S) || IP-Addr(S) || ID (S) || Cl-ID(S) || TS(S)
        R to C: MACA (R) || IP-Addr(R) || IK(R) || Cl-ID(S) || TS(R)
C to R: IK (R) || NK (R) || NONCE (R) || Cl-ID(S) || TS(C)
R to C: IK (R) || NK (R) || NONCE (R) || TS (R) || Cl-ID(R)
C to R: TS (R) || OK (R) || TS (C)    || Cl-ID(S) || TS(C)
Here, TS (R) indicates the Times Stamp provide by the receiver.
```

Algorithm 8:   EES-DARP

```
Input: Node Details
Output: Secured Routing Paths and Data Delivery at sink
Step 1: Read the Node details
Step 2: For every Node perform Node authentication by calling Algorithm – 7 (Authentication Algorithm)
Step 3: Form clustering of Nodes by calling algorithm 4
Step 4:    Fuzzy rules and optimize the clusters
Step 5: Select cluster heads
Step 6: Call algorithms 1, 2 & 3 for generating private and public keys for the nodes
Step 7:    Perform optimal route discovery by calling algorithm 5
Step 8: Perform Local Data Aggregation by calling algorithm 6
Step 9:    Apply Algorithm 6 for Global Data Aggregation
Step 10: Send data packets with aggregation through authenticated cluster heads
Step 11: Check energy levels of nodes
Step 12: If energy levels of cluster heads are less than any of the member nodes, call clustering again
Step 13: Perform route discovery using new cluster heads
Step 14: Perform the routing of data with aggregation through new cluster heads-based routes
Step 15:    Repeat steps 11 to 14 until the last node in each cluster dies
Step 16: Return
Step 17: End
```

The following Algorithm shows the details of the proposed Energy Efficient Secured Particle Swarm Optimization (PSO) oriented Clustering as well as Data Aggregation Routing Protocol named EESCPSO-DARP.

Algorithm 9:   EESCPSO-DARP

```
Input: Node Details, PSO Functions, Termination Conditions
Output: Secured and Optimized Routing Paths and Data Delivery at sink
Step 1: Read the Node details, Fitness Function and Constraints
Step 2: For every Node perform Node authentication by calling Algorithm – 7 (Authentication Algorithm)
Step 3: Form clustering of Nodes by calling algorithm 4
Step-4: Select CH nodes based on Centroid nodes, Energy and Trust to have CH1, CH2, ….CHn.
Step-4: Use    PSO and optimize clusters
            While termination condition is not satisfied do begin
              For each particle i (CH of cluster i) do
              4a. Select one member    node    and     with distance, energies and trusts
4b. Let the position of CH(i) be (x1, y1) and the position of member node    Mem(i) be     (x2,y2)
              4b. Apply    Distance Formula
                    $DIST(CH(i), MEM(i)) = Sqrt( (x1-x2)2 + (y1-y2)2$
               4c. Find the cluster centroids and set the velocity
               4d. Calculate l-best, g-best and fitness function values
               4d. Evaluate Fitness Function Values
               4e. If node Mem(i) is fit, add node Mem(i) to CH(i).
               4f. Update Velocity using l-best and g-best values
                4g. Update the cluster centroids
                          End
Step 5:    Apply PSO and Fuzzy rules and check the optimized the clusters
Step 6: Select cluster heads using Energy, Keys, Distance and Trust of Nodes
Step 7: Call algorithms 1, 2 & 3 for generating private and public keys for the nodes
Step 8:    Perform optimal route discovery by calling algorithm 5
Step 9: Perform Local Data Aggregation by calling algorithm 6
Step 10:    Apply Algorithm 6 for Global Data Aggregation
Step-11: Perform Route Discovery through CHs
Step-12: Apply PSO and optimize routes using l-best and g-best values.
Step 13: Send data packets with aggregation through authenticated CHs
```

Step 14: Check energy levels of nodes

Step 15: If energy levels of cluster heads are less than any of the member nodes, call clustering again

Step 16: Perform route discovery using new cluster heads and optimize the route using PSO

Step 17: Perform the routing of data with aggregation through new cluster heads-based routes

Step 18: Repeat steps 11 to 14 until the last node in each cluster dies

Step 19: Return

Step 20: End