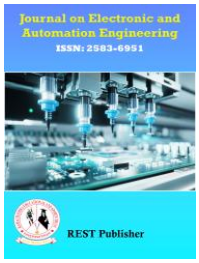
Journal on Electronic and Automation Engineering

Vol: 2(4), December 2023

REST Publisher; ISSN: 2583-6951 (Online)

Website: https://restpublisher.com/journals/jeae/

DOI: https://doi.org/10.46632/jeae/2/4/5



Cryptography Encryption of Security in Wireless Sensor Network

[*]K. Gowsic, N. Karthigavani, K. Jayasri, S. Yuvaraj

Mahendra Engineering College, Namakkal, Tamil Nadu, India.

[*]Corresponding author Email: gowsick@mahendra.info

Abstract: *For past two decade, Wireless Sensor Networks (WSNs) have emerged with the result of the low-cost availability, undersized range, and easy-to-install sensors. WSN technologies transmit real-time sensor data from specified monitoring environment in a backend to process as well as analysis. Because of the ubiquity of wireless communication channels, security and management problems have emerged as hot concepts in WSN systems. This research proposed an Improved Elliptic Key Cryptography (IEKC) based security method. Data encryption as well as decryption is achieved through IKEC. The fundamental method feature is about the source code of node's contain private keys that secure various keys in non-volatile memory. The Chicken Swarm Optimization (CSO) algorithm has highly efficient in intelligence optimization system that performs well when handling global optimization Positions (GOPs). The CSO algorithm has executes badly in complexness GOPs due to various errors, causing the iteration to rapidly descend into a local minimum. The provided approach protects against replay, Sybil attacks and DoS. Cluster chiefs have been selected by Improved CSO (ICSO), and nodes are ordered based on network sizes. Based on the simulating results, this mechanism of security efficiently opposes various attacks with lesser assets and considerably improves the network's resilience for capturing node. Experiment result indicates the suggested paradigm is efficient in terms of packet delivery Ratio (PDR), and throughput.*

Keywords: *Elliptic curve cryptography, Wireless Sensor Network, Improved Chicken Swarm Optimization, security, data encryption.*

1. INTRODUCTION

WSNs have sparked widespread interest for use in a variety of settings includes military, health, industrial and agriculture monitoring. At present, healthcare systems have made significant WSN technology utilization. When the sensors can communicating wirelessly with each other, the recognized health data from the sector around it has sent to the sink is treated either by a single hop when the sink falls under the same node's range or through multiple hops once it sink is outside the range [1]. The data routing mechanism in the WSN is also crucial for reducing the burden on sensor sources. Due to the medium, every hacker may access the network as well as collect medical data [2]. Passive and active are two kinds of attacks in which data exchange among the parties with no alteration or false data injection due to eavesdropping hackers in the network is said to be passive attack. In contrast, active attack is represented as malicious attack conduction before retransmission of nodes to the network destruction purpose or grabbing health data by eavesdropping hackers [3, 4]. For communicating crucial data in this network, it must maintain the data as secure as feasible while also preventing unauthorized individuals from supplying false data to sensors. Cryptography is utilized to alleviate certain aspects of the health network's security issues by offering trust as well as authentication. Sensors require restricted resources for energy, memory and processing [5]. As a result, typical cryptographic algorithms are unsuitable for WSN due to the increased connection, memory, and processor requirements. Finally, when creating and executing a key management strategy, it's vital to take into account the limited resources offered by these devices [6-8]. Energy and security are critical components of this network architecture which is owing to unique sensor node features unlike traditional local network devices, are restricted

by battery life as well as resource capacity such as bandwidth, storage and elaboration. As an outcome, improved Medium Access Control (MAC) protocols which take into account the restrictions of each particular sensor over network are necessary [9, 10]. WSNs are an extensive application variety and sensor networks get more complicated in their security becomes increasingly crucial. The major security risks branches from the sensor's location in remote regions and its geographic spread. Unfortunately, standard safety procedures are ineffective for sensors since they introduce significant overload. A number of researchers are conducted researchers on effective security techniques which consider into account of resource as well as memory imposed by WSNs [11]. Chickens are a unique species of poultry ani mal due to their social behavior, and they often coordinate with its food identifying activities over groups [12]. In a chicken flock, three types of individuals are Roosters, chicks and hens. There is a distinct champing hierarchy in the group based on different champing capacities [13]. Since hens in the hierarchy have lower foraging ability in comparison to roosters, individuals search after it, whereas chicks do exactly the same since they have poorer foraging capabilities.

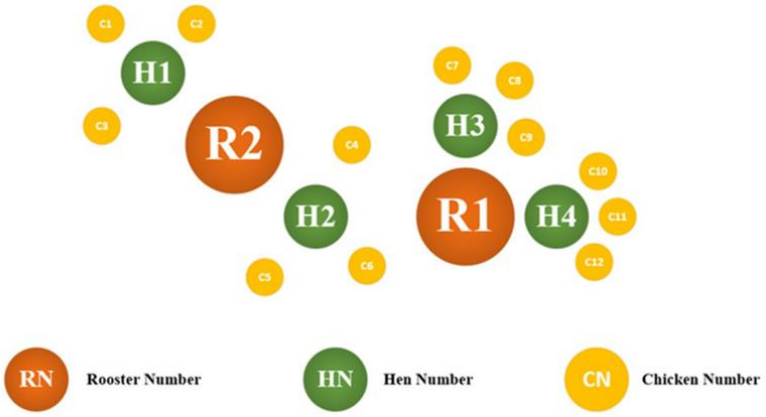


FIGURE 1. Basic structure of chicken population

Figure 1 illustrates the chickens structures population with the rooster at the center whereas the hens placed around the rooster, as well as the chicks placed around the hen. Finally, the different natural pattern for mutual learning are identified and that competing among individuals of similar species, like hens and hens, roosters and roosters, or among population of other species namely hens and chicks, over the foraging process [15]. The method's developers had been inspired through fact that the learning relationship with contest corresponds in the self-organizing group intelligence growth as well as motivated to consider this intelligent CSO technique. Sensor networks like any communication systems require fundamental security services for protecting both data as well as assets from probable threats. Sensors network require light encryption in ensuring a high security level. All sensors ought to maintain a balance among performance, cost, and safety as well as achieving all three goals at once is extremely challenging. In some cases, developers forfeit security by implementing cost-effective solutions that lack sufficient processes, such as key distributions. A WSN necessitates more adaptable ways for transferring keys within the network and can be done through two different cryptography types are: 1. Classical cryptography: It relies on the working principle of symmetric and asymmetric cryptography. 2. Advanced cryptography: It relies only on the working principle of ECC that is highly efficient in resource usage than other methods which will use public key concept. WSNs need transfer data with safe manner to a central node via transmission with multi-hop, ensuring data security as well as integrity. In WSN, several attacks and threats includes data loss, interruptions in communication, service reduce speed resulted to delays, and DoS [16, 17]. Thus, the research concentrated on these three major properties of security is integrity, authentication and confidentiality. Researchers offer many countermeasures, including intrusion prevention and detection, as well as cryptographic techniques. The research work flow is as follows in which section 2 illustrates the current cryptography method working with respect to security in data transmission and improve the less latency in WSN. Session 3 describe the proposed IEKC using ICSO algorithm and session 4 provides evaluation of proposed IEKC method and discusses the improvement in low latency in data transmission over WSN. Finally, the section 5 provides the conclusion about improvement of data transmission with improved security.

2. LITERATURE REVIEW

This section examines important management strategies as well as determines their issues as well as drawbacks about WSN security and privacy. Alakananda Tripathy et al. have introduced a novel strategy called Hybrid Encryption Technique (HET), which assesses the effectiveness of two-key as well as single-key encryption in securing sensor network data. The HET approach ensures data security by preserving security primitive objects like authentication, secrecy, and integrity. This approach requires a short period to decrypt and encrypt, and no energy usage data is accessible [18]. L. Sachin et al. have proposed a novel hybrid encoding technique integrates asymmetric as well as symmetric algorithms for offering high security level while minimizing key management cost [19]. Anwar and Maha have proposed a lightweight hybrid cryptographic technique for WSNs. The initial procedure Diffie-Hellman has secures the key exchange procedure and the subsequent modified cryptography algorithms like AES and Playfair have utilized for securing data in AMPC's proposed solution for boosting WSN security. Although it is secure currently, the consumption of power is quite significant. LSA gets limited rounds, each with its unique key in enhancing security. CSO was introduced by Meng in which characterize as intelligent optimization method that prepares the parameter modification procedure based on the flock's behavior. The technique reproduces behavior of chicken population and segregating parameter variables towards 3 groups namely rooster, chicks and hens that configures the parameter with transformation process of self organization in term of the chicken flock's rigid foraging hierarchy [21]. It incorporates the challenges faced in optimization process. The results are comparable with the way flocks of hens forage. During its inception, the CSO algorithm has sparked an array of attention, and multiple academics have researched it from different points of view. B.Nagarajan has proposed an approach from the perspective of integrated algorithm named the Markov chain theory-based CSO has worldwide convergence [22]. Saif et al. have included the actual techniques with benefits of several benchmark measures for optimization issues to evaluate and contrast the advantages and disadvantages of the CSO technique and other intelligent optimization techniques. Experts proceed to perform simulations to assess the technique solution with rapidity as well as precision that outperforms the differentiating evolution, bat, and particle swarm techniques with respect to endurance and resilience [23]. Z.Wang et al. have improved the CSO technique and applied it to actual events engineering problems and even giving proof as well as analysis. Based on investigating disadvantages of blindly, that adherent to the hen’s parameters in the chicken fock is easily drifting towards local optimal strategies. Thus, the research devised a better CSO approach based on Gaussian migration approach [24]. Y.Yu used the CSO algorithm for acquiring features, and tests comparing it with different algorithms for optimization suggested the flock optimization strategy provides benefits of rapid speed as well as excellent accuracy in feature extraction in applications [25]. The precision and speed of optimization issue solutions are becoming increasingly important over the past decade because of engineering applications like WSN, data mining, robotics engineering, feature extraction, power consumption, etc. Several researchers have developed a variety of new scenarios as well as execution methodologies in CSO algorithm as a result of continuous innovation. As a result, the evaluation research discussed in this study has focuses on the implementation of the ICSO technique as IEKC in specific domains, as well as the generating an improved security in WSNs.

3. RESEARCH METHODOLOGY

The framework now includes security criteria for WSN and the research concentrate primary in providing reliable data for decision-making while simultaneously offering for secure communication identification participants as well as data transmission.

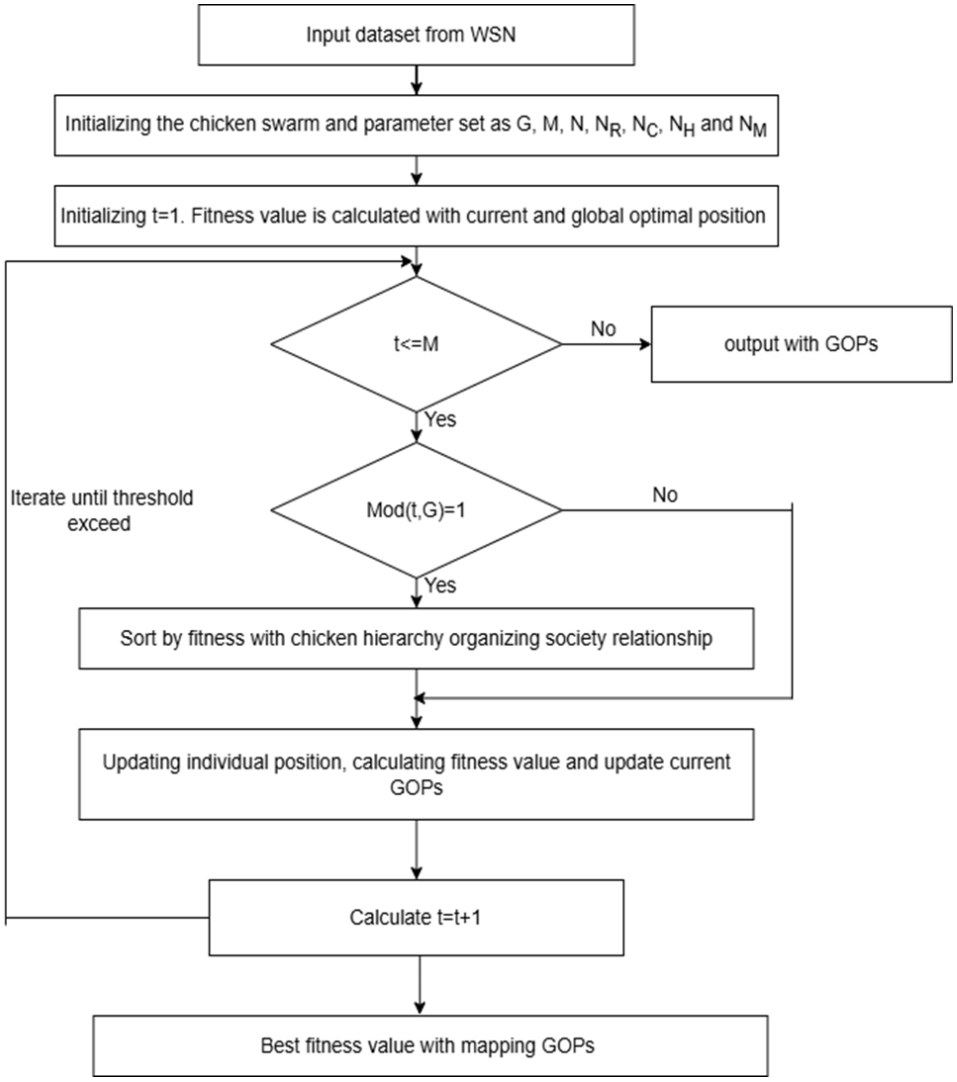


FIGURE 2. Proposed architecture of ICSO algorithm for securing WSN

In the context of WSN attacks, the concept employs cryptography, digital signatures, and public-key infrastructure (PKI) for ensuring security. Highly sensitive data is made to encrypt can the intended recipient alone is able to read it. The method uses symmetric cryptography to perform both secret key creation as well as message encryption. A public key infrastructure issues digital certificates and uses asymmetric encryption to safeguard the key. The design uses technique of digital envelope in encrypting messages as well as private keys. It ensuring only the recipient who was intended may access the message's data. The proposed paradigm involves selecting cluster heads (CH) according to ICSO, nodes with respect to size of the network, as well as data encryption as well as data decryption employing IKEC. Figure 2 illustrates the proposed method architecture. The suggested architecture has two main components with secured data architecture and preliminary network setup incorporates cluster management. Initial phase with a fundamental routing architecture is configured such that every node is capable of maintaining monitors in its neighbor with particular internal database. Thus, the study focused on implementing a mobile CH system that is both effective and successful with respect to improvement of network security in WSN.

ICSO working principle: CSO is a medically influenced meta-heuristic optimization method that replicates both the hierarchical architecture of CSO and its individual behavior. CSO hierarchies are separated into numerous groups, each of which includes chicks, roosters and hens. Hierarchical order of CSO have essential for social interactions with

swarms is stronger chicken's gets dominated in the less powerful chickens within the flock. The guidelines followed have accumulated with chicken's behaviors are: 1) There are numerous groups within the chicken flocks. Each group comprises a dominating rooster which is supported by several hens and chicks. 2) The hierarchies of the swarm are represented by chicken fitness values whereas the chicks have the lowest fitness values, while roosters operate as a learder for each group that have the highest fitness values. The hens might represent the opposing faction. 3) Strong pattern of a swarm is considered for the mother-child bond, as well as the dominant relationship stays unchanged. Only in (G) time steps do such statuses improved.

Improved chicken swarm algorithm

When the whole flock searches for food in a chaotic atmosphere, the "Levy flight" search strategies consists of short-ranged deep local searches as well as occasional longer distance walks that may assist in enhancing search efficiency as well as improve disturbance, allowing the chickens for distributing more evenly. The CSO technique prioritizes hens, since they play a vital part in the flock as a whole. Based on this concept, the ICSO technique incorporates the search technique of Levy flight towards the hen's location updating formulae that prevents iterations from reaching a local minimum as well as improves the ICSO algorithm's global search capabilities.

ICSO algorithm

- Step 1: Initializing chicken swarm as well as set parameters N、NR、NH、Nc、Nm、G and M
- Step 2: Fitness value of each chicken has measure and boosts the location of recent and global optimal by considering t=1.
- Step 3: When mod (t, G)=1, any chickens are sorted in ascending order with respect to the fitness values, the Nc chickens is located in front of each cluster that perform as roosters and each roosters represent a group. The last Nc chickens is defined as chicks, the remaining chicken located in the middle are hens.
- Step 4: The hens select a group to dwell in at random and it is represented as the mother-child bond among the hens as well as chicks.
- Step 5: Position of all rooster, chick and hen is updated as per equation 2.
- Step 6: Each chicken fitness value gets recalculated and get updated by the optimal location of both current and global for all chicken.
- Step 7: If the iteration terminating condition has been satisfied the output of global optimal location and end the iteration else set t=t+1 also return to Step 3 and step 4.

Data security using IKEC

The collected CH data get encrypted and send it to sink. IEKC involves both data encryption and decryption in which distinct keys have been utilized for encrypting specific communications.

Key Generations

Generating both public as well as private keys are critical to a model and the network communication get encrypt by sender recipient's public key, as well as get decrypted using recipient with its private key. Let X and y are two communication nodes and each choose their two random numbers as m1, n1>p -1 , and m2, n2> p-1 correspondingly. The creator point of cyclic group with elliptic curve Ep (x,y) have designed.

ECC Encryptions

While examining the code table X and y have created, if x desires for sending message 'M', all letters have been assigning with code to the points using the lexicographic elliptic curve order.

ECC Decryptions

During transmission about cipher texts, Y converts towards points on elliptic curve EP $(a,)$ as well as determines point Z characters. Y decodes message employing Y's possess private keysβ2. Subtracting gets converted in contributions by multiply y coordinates using -1. Such operations can be acceptable by employing points summation have been

utilized for identifying mirror image points with the x-axis.

4. RESULT AND DISCUSSION

This section displays the results of the experiments of the NS2 implementations used in the present study. These involve throughput, end to end delay and PDR. According to this experimental research, the average of ten simulation results with a count of 25 nodes interval. The performance metrics of simulation for various cryptograpy with proposed IEKC with ICSO. The most critical parts of securing data transmission in WSN for the entire network are exposed for attacking. Security is a critical consideration to several WSNs usage. An effective method has a shorter "key generation time," meaning refers to time required in finishing the key expansion process. The proposed IEKC with ICSO is evaluated using WSN QoS as PDR, throughput and end to end delay whereas this suggested method is compared with existing Improved Bat Optimization Algorithm (IBOA) and Improved Whale Optimization Algorithm (IWOA).

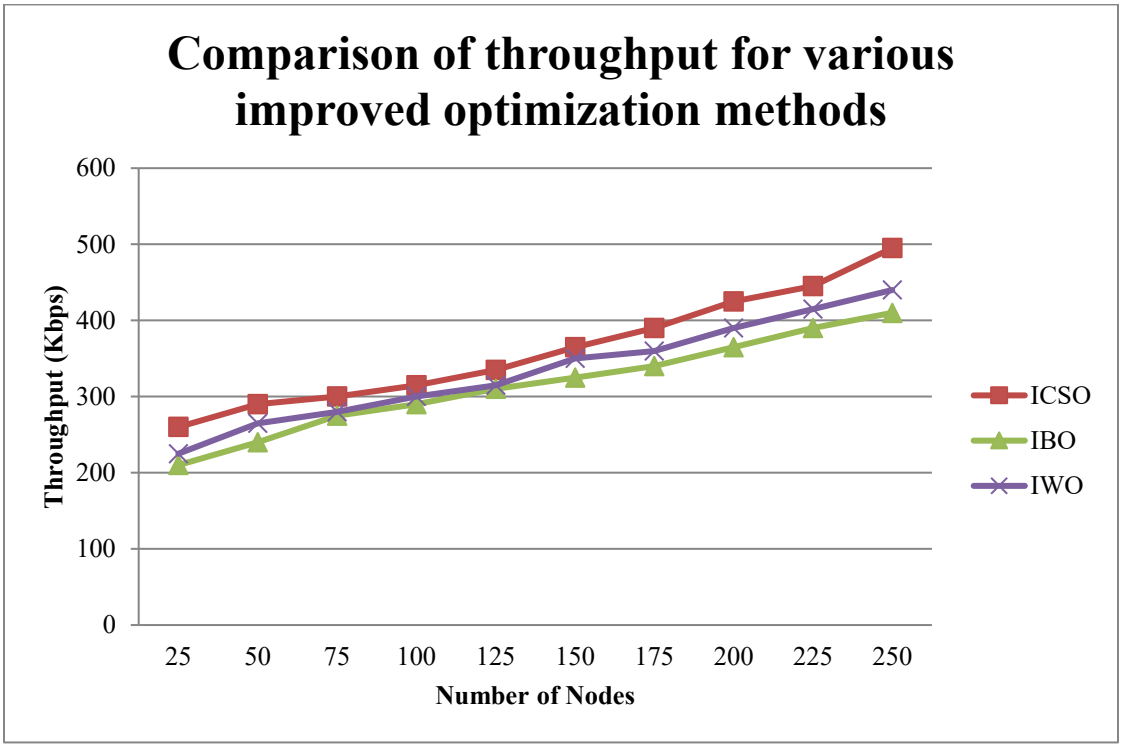


FIGURE 3. Comparison of throughput for various improved optimization methods

Figure 2 have compared the proposed IEKC-ICSO method with the existing IBO and IWO algorithms with respect to throughput performance metrics. The throughput value gets increased as the node increases whereas the node ranges from 25 to 250 with the interval of 25 nodes. The experimental results have determined that the proposed IEKC-ICSO method has a higher throughput of 495 Kbps at 250 nodes, whereas the IBO and IWO method have corresponding throughputs of 410 Kbps and 440 Kbps.

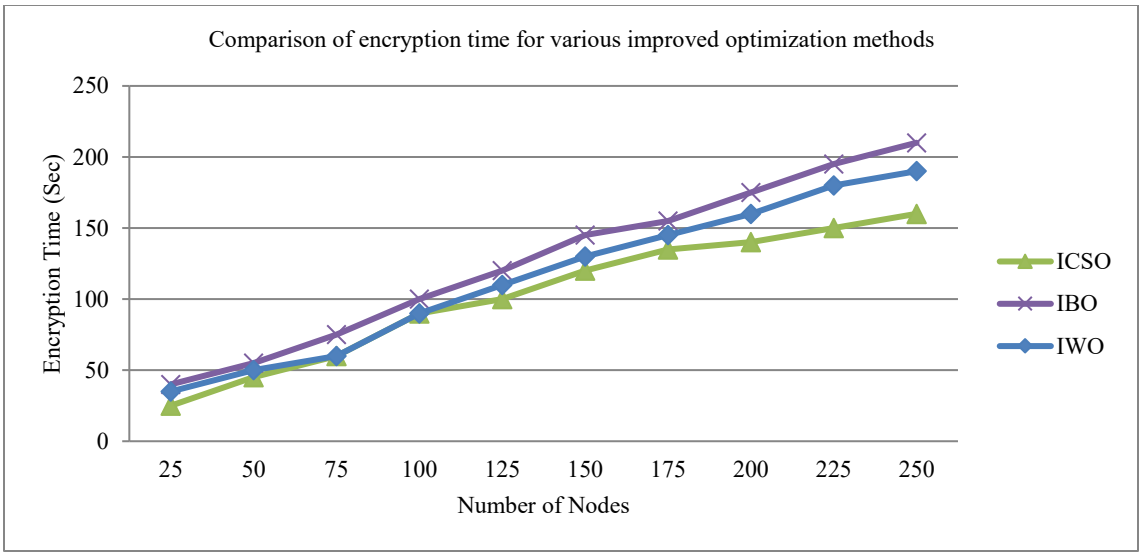


FIGURE 4. Comparison of throughput for various improved optimization methods

Figure 3 have compared the proposed IEKC-ICSO with the existing IBO and IWO algorithms with respect to encryption time metrics. The encryption time gets increased as the node increases whereas the node ranges from 25 to 250 with the interval of 25 nodes but the time consumed from proposed method and existing methods have been compared. The results determined that encryption time consumed by IEKC-ICSO is lesser as 160Sec at 250 nodes whereas the IBO and IWO method have corresponding encryption time as 210 Sec and 190 sec.

Figure 4 have compared the proposed IEKC-ICSO with the existing IBO and IWO algorithms with respect to PDR metrics. The PDR gets increased as the node increases whereas the node ranges from 25 to 250 with the interval of 25 nodes but the PDR from proposed method and existing methods have been compared. The results determined that PDR consumed by IEKC-ICSO is higher as 0.90 at 250 nodes whereas the IBO and IWO method have corresponding PDR as 0.55 and 0.8.

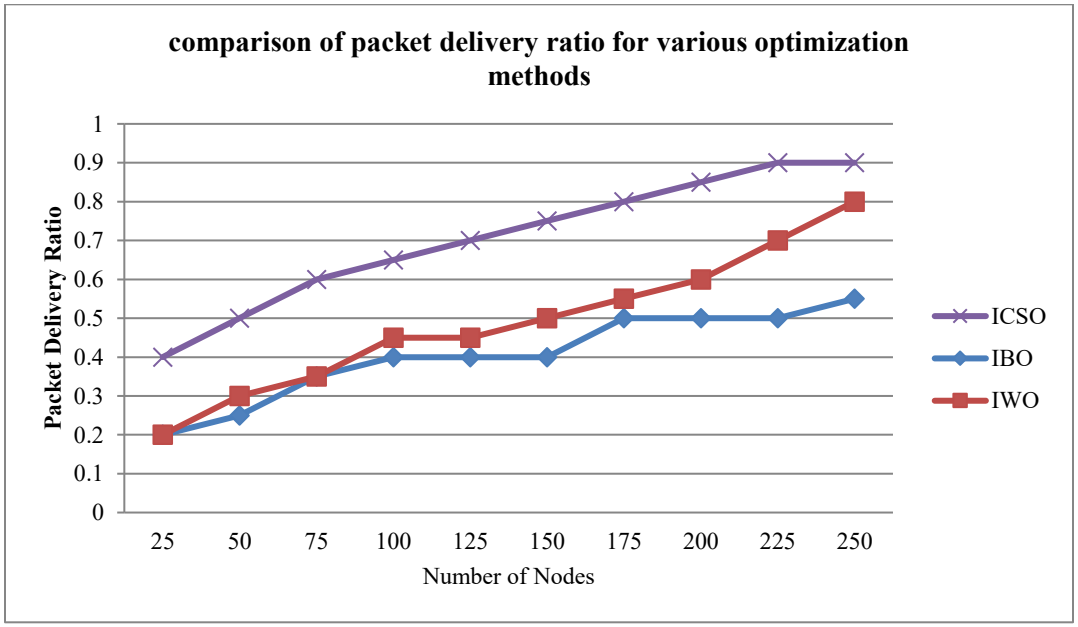


FIGURE 5. Comparison of PDR for various improved optimization methods

5. CONCLUSION

This research combines better cryptographic techniques for significant purposes including monitoring and controlling using WSN security features that are regarded essential. When employing a low-powered sensor for transmitting essential data reliably on time, reliable and secure communication is necessary. The goal of the research is to improve security in WSNs. Hence, this present study classifies nodes based on network size and the choosing of cluster chiefs by ICSO whereas the data encryption and decryption is accomplished using IEKC-ICSO algorithm. As the result, the finding of performance metrics as QoS metrics is determined and compared with certain recent improved optimization algorithms such as IBO and IWO. The evaluated results have determined that IEKC-ICSO algorithm has high throughput with better PDR and less encryption time consumption as 495Kbps, 160 Sec and 0.9 at 250 nodes respectively. It is comparatively better than other existing algorithms such as IBO and IWO algorithms.

REFERENCES

[1]. Huanan, Z.; Suping, X.; Jiannan, W. Security and application of wireless sensor network. Procedia Comput. Sci. **2021**, 183, 486–492.

[2]. Al-Zubaidie, M.; Zhang, Z.; Zhang, J. REISCH: Incorporating lightweight and reliable algorithms into healthcare applications of WSNs. Appl. Sci. 2020, 10, 2007.

[3]. Banerjee, A.; De, S.K.; Majumder, K.; Das, V.; Giri, D.; Shaw, R.N.; Ghosh, A. Construction of effective wireless sensor network for smart communication using modified ant colony optimization technique. In Advanced Computing and Intelligent Technologies; Springer: Singapore, 2022; pp. 269–278.

[4]. Khalaf, O.I.; Romero, C.A.T.; Hassan, S.; Iqbal, M.T. Mitigating hotspot issues in heterogeneous wireless sensor networks. J. Sens. 2022, 2022, 7909472.

[5]. Majid, M.; Habib, S.; Javed, A.R.; Rizwan, M.; Srivastava, G.; Gadekallu, T.R.; Lin, J.C.W. Applications of wireless sensor networks and internet of things frameworks in the industry revolution 4.0: A systematic literature review. Sensors 2022, 22, 2087.

[6]. 9. Al-Zubaidie, M. Implication of lightweight and robust hash function to support key exchange in health sensor networks. Symmetry 2023, 15, 152.

[7]. Lee, C.-C. Security and privacy in wireless sensor networks: Advances and challenges. Sensors 2020, 20, 744.

[8]. 12. Barati, H. A hierarchical key management method for wireless sensor networks. Microprocess. Microsyst. 2022, 90, 04489.

[9]. Afroz, F.; Braun, R. Energy-efficient MAC protocols for wireless sensor networks: A survey. Int. J. Sens. Netw. 2020, 32, 150–173.

[10]. 6. Samara, G. Wireless Sensor Network MAC Energy-efficiency Protocols: A Survey. In Proceedings of the 2020 21st International Arab Conference on Information Technology (ACIT), Giza, Egypt, 28–30 November 2020; pp. 1–5.

[11]. Olakanmi, O.O.; Dada, A. Wireless sensor networks (WSNs): Security and privacy issues and solutions. In Wireless Mesh Networks-Security, Architectures and Protocols; IntechOpen: London, UK, 2020; p. 13.

[12]. Yan C, Xiao J, Chen D et al (2021) Feed restriction induced changes in behavior, corticosterone, and microbial programming in slow-and fast-growing chicken breeds. Animals 11(1):141

[13]. Carvalho C, de Oliveira C, Miotto Galli G, de Oliveira Telesca Camargo N, Pereira M, Stefanello T, Melchior R, Andretta I (2022) Behavior of domestic chickens –insights from a narrative review. Journal of Agroveterinary Sciences 21:360–369

[14]. Basha AJ, Aswini S, Aarthini S, Nam Y, Abouhawwash M (2023) Genetic-chicken swarm algorithm for minimizing energy in wireless sensor network. Computer Systems Science & Engineering 44(2)

[15]. Jonsson A, Vahlne JE (2023) Complexity ofering opportunity: Mutual learning between Zhejiang Geely Holding Group and Volvo Cars in the post-acquisition process. Global Strategy Journal 13(3):700–731

[16]. Azzedin, F.; Albinali, H. Security in Internet of Things: RPL Attacks Taxonomy. In Proceedings of the 5th International Conference on Future Networks & Distributed Systems, Dubai, United Arab Emirates, 15–16 December 2021; pp. 820–825.

[17]. 9. Khanam, S.; Ahmedy, I.B.; Idris, M.Y.I.; Jaward, M.H.; Sabri, A.Q.B.M. A survey of security challenges, attacks taxonomy and advanced countermeasures in the internet of things. IEEE Access 2020, 8, 219709–219743.

[18]. [42] Alakananda Tripathy et al., “Hybrid Cryptography for Data Security in Wireless Sensor Network,” Data Engineering and Intelligent Computing. Advances in Intelligent Systems and Computing, V. Bhateja, S. C.

Satapathy, C. M. TraviesoGonzález, V. N. M. Aradhya, Eds., Springer, Singapore, vol. 1407, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[19]. [43] L. Sachin, S. Bhushan, and Surender, "Hybrid Encryption Algorithm to Detect Clone Node Attack in Wireless Sensor Network," Proceedings of the International Conference on Innovative Computing & Communications, pp. 1-6, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[20]. [44] Md. Navid Bin Anwar, and Maherin Mizan Maha, "AMPC: A Lightweight Hybrid Cryptographic Algorithm for Wireless Sensor Networks," International Journal of Innovative Science and Research Technology, vol. 5, no. 6, pp. 1142-1146, 2020.

[21]. Ishikawa A, Sakaguchi M, Nagano AJ et al (2020) Genetic architecture of innate fear behavior in chickens. Behav Genet 50:411–422

[22]. Nagarajan B, SVN SK (2023) A poisson hidden markov model and fuzzy based chicken swarm optimization algorithm for efcient fault node detection in wireless sensor network. 1:1–12

[23]. Saif MAN, Niranjan SK, Murshed BAH et al (2023) CSO-ILB: chicken swarm optimized inter-cloud load balancer for elastic containerized multi-cloud environment. J Supercomput 79(1):1111–1155

[24]. Wang Z, Zhang W, Guo Y et al (2023) A multi-objective chicken swarm optimization algorithm based on dual external archive with various elites. Appl Soft Comput 133:109920

[25]. Yu Y, Rashidi M, Samali B et al (2022) Crack detection of concrete structures using deep convolutional neural networks optimized by enhanced chicken swarm algorithm. Struct Health Monit 21(5):2244–2263.