International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2022/212557 Volume 9, Issue 3, May – June (2022)

RESEARCH ARTICLE

Hybrid Simulated Annealing with Lion Swarm Optimization Algorithm with Modified Elliptic Curve Cryptography for Secured Data Transmission Over Wireless Sensor Networks (WSN)

S. Silambarasan
Department of Computer Science, Periyar University, Salem, Tamil Nadu, India
silambus82@gmail.com

M. Savitha Devi
Department of Computer Science, Periyar University Constituent College of Arts and Science, Harur, Dharmapuri, Tamil Nadu, India
savithasanma@gmail.com

Received: 27 April 2022 / Revised: 14 May 2022 / Accepted: 30 May 2022 / Published: 28 June 2022

Abstract – The security of data processing has become an important factor in the present scenario due to the rapid growth of the internet. Especially, Wireless Sensor Networks (WSNs) face complicated challenges in their vulnerable corrupted sensor nodes. In the earlier work, Enhanced Lion Swarm Optimization Algorithm and Centralized Authentications (ELSOA-CAs) scheme has been proposed for achieving ideal, quicker, and energy efficient data transmissions. But, in the earlier work, a congestion-aware multipath routing mechanism is not considered. Moreover, for the bigger file, the security is not still strong. This security issue is addressed in the proposed work by using Hybrid Simulated Annealing with Lion Swarm Optimization and Centralized Authentication (HSALSO-CA) mechanisms. In the proposed technical work, optimum, quicker, and energy-efficient data transmission is highlighted to guarantee that the decision-making regarding tomato crops is achieved with accuracy. In this research work, multipath routing is presented to ensure that the data transmission is accelerated. In this work, rapid multipath routing is formulated by choosing the best forwarder nodes that meet limitations such as delay and energy. Optimal Forwarder Node Selection employing Hybrid Simulated Annealing with Lion Swarm Optimization Algorithm (HSALSOA) is used. The Simulated Annealing algorithm is hybridized as it emphasizes optimal local and global search capability for the bigger network. Secured data transmission employing Modified Elliptic Curve Cryptographies (MECCs) algorithm guarantees increased security for congestion-sensitive multipath routing mechanisms. It is proven from the simulation outcomes that the proposed ELSOA-CA model yields superior performance in terms of enhanced throughputs, elongated network lives with reduced utilization of energies, and delays in contrast to available techniques.

Index Terms – Aggregation, Security, Lion Swarm Optimization, Forwarder Nodes, Centralized Authentication, Secured Data Transmission.

1. INTRODUCTION

When motes of WSNs deployed in distant accesses deliver sensor inputs to users, WSNs confront serious authentication and security challenges. Various concerns and risks can be addressed depending on protocol levels. WSNs are made up of a large number of SNs that sense, gather, and distribute data in places where traditional networks are ineffective due to environmental and/or strategic factors [1]. They serve crucial roles in a wide range of applications including military surveillance and monitoring forest fire. They can also be used for monitoring building security shortly. These installed SNs can monitor very large areas where operational circumstances are hostile or difficult. Since, these kinds of networks exist in distant locations and are left unattended, protecting them against threats like node acquisitions, physical tampers, and threats including eavesdropping and DOSs (denial of services) becomes imperative.

In WSNs, the primary concerns include authentication and Security, involving motes in the network responsible for sending the sensor inputs to the user positioned remotely. Depending on the level of the protocol, the different challenges and risks are dealt with. There are several security concerns identical in both WSNs and wireless ad-hoc networks, and these form the basic dissimilarities between the architecture and objectives of the two kinds of networks [1].

RESEARCH ARTICLE

Even though the cost incurred in WSNs s is less, their computational complexity hinders them to be directly applied in the current highly robust conventional wireless security mechanisms [2].

Conventional security standards of the wireless network are undesirable for sensor networks due to huge requirements of memory, energy, and high computational complexity [3]. One major problem of WSNs is that their SNs (sensor nodes) are not supervised when situated in hazardous environments assed to limited energies, and undefined network architectures, making them vulnerable to numerous types of assaults including eavesdropping, compromised mote attacks, and traffic analyses, etc [4]. Quite diverse from the Internet, dispersed and energy-constrained WSNs have the frequent task of performing collaborative monitoring or managing one or more events in WSNs [5]. Before transmissions to data sinks that control SNs and collect their data, pre-processing or aggregations of event information at intermediary SNs is possible and even mandatory in certain cases [6]. Since conventional transport layers are not developed with no attention paid to these novel features of WSNs, better transport protocols are required [7]. Transport layers of WSNs perform two important functions namely information deliveries and control of congestions [8]. In cases of packet losses in multi-hop WSNs where few or entire packets are lost can be easily identified and lost data can be restored using suitable techniques when WSNs are robust [9]. Reliability is necessary when data is crucial for WSNs applications.

Congestions occur when SNs send their data to sinks creating traffic loads that networks struggle to handle [10]. If congestion occurs in WSN, nodes begin dropping the packets or the packet delay considerably goes above the needs of applications. Packet dropping happening often is a waste of energy and acts against any endeavor for gaining reliability. Excessive packet delay might result in data invalidity which is gathered by sensors [11].

Hence, in these devices, their constrained energy, limited processing power, less bandwidth, and communication capacity constitute the big setbacks on the processing strength and memory accessible for security depending on the executions. A vast variety of security approaches have been introduced to improve energy efficiency during the design of enhanced security protocols. It is understood that symmetric cryptography can be preferred for applications, which cannot address the computational complexity, which is a huge issue and is considered a problem identification of the research work. Therefore, the research goal is to develop effective cryptographic algorithms that are implemented optimally in terms of energy dissipation and computational complexity, and are pivotal in increasing the battery lifespan of SNs.

In this work, cache resources are allocated to diverse data flows based on their needs, and reliability and congestion-aware data transfers are achieved. Data flows occurring in WSNs generate erratic resource allocations while monitoring those helps in better management. This is accomplished in this work by computing priority levels of multiple data flows and allocating large chunks of cache resources to data flows with the highest priority levels.

The technical work is organized as given. In this section, the need for addressing the congestion and reliability focus when carrying out the data transmission in the WSNs is studied in detail. Section 2 analyzes the different research approaches, which are presented to attain congestion-free, robust data transmission. Section 3 discusses the proposed research approach in detail with the appropriate diagrams and examples. Section 4 discusses the proposed research approach's performance examination based on the numerical evaluation. Lastly in section 5, the research study's conclusion is studied depending on the achieved findings.

2. RELATED WORKS

Rosset et al [12] introduced a new bio-inspired routing protocol called CB-RACO (Community-Based Routing with Ant Colony Optimization protocol) that combined meta-heuristic ACOs (Ant Colony Optimizations) with computationally inexpensive and distributed community detection methodologies LPs (Label Propagations). WSN communities are created by CB-RACO that reduces energy usage imbalance by routing the information within groups using swarm intelligence. Consequently, CB-RACO requires less memory and experiences less overhead concerning deployment and maintenance of routing paths.

Bhatia et al [13] introduced TRM-MAC, a TDMA-based reliable multicast MAC technology aimed toward WSNs. TRM-MAC protocol featured parametric components that could be used to trade off reliability and delay performances based on the application's demands. The TRM-MAC protocol was investigated for latencies and reliabilities of performances with various PLRs (packet loss rates) and contrasted with other findings.

Mohanty et al [14] developed the protocol ESDADs (Energy Efficient Structure-Free Data Aggregation and Deliveries), which aided in aggregating repeated data of intermediate nodes. Their recommended protocol computed packet waiting times at intermediary nodes in a reasonable manner, allowing data aggregations to be accomplished efficiently throughout routing paths. Sensitive data packets were broadcast to aggregation points. The proposed ESDADs protocol developed cost functions for structure-independent next-hop node selections and information aggregations near sources.

Faheem et al [15] recommended a new Energy Efficient and Reliable Data Gathering Routing Protocol for WSN-based smart grid applications. To achieve energy efficiencies and robust information aggregations from SGs (Smart Grids) in

RESEARCH ARTICLE

WSNs, the proposed solution employed software-oriented centralised controllers and many mobile sinks were the results of elaborate simulation carried out via EstiNet 9.0 revealed that the proposed approach performed better than available mechanisms and attained its specifies objectives for event-based applications in SGs.

Elappila et al [16] proposed survivable path routes in congested and interference sensitive energy efficient routing for WSNs. Their protocol was intended for networks with heavy traffic because as several sources tried to deliver their packets to the same destinations at the same time, typical scenarios of IoTs (Internet of Things) related to remote medical monitoring. In choosing next hop nodes, the approach used conditions i.e. functions made up of link's signals to interferences and noise ratios, element of path's survival, and congestion levels at next hop nodes.

Sharma et al [17] proposed a robust congestion-based approach that resulted in bi-directional dependability and rate modifications based on congestion controls. Their scheme used TOPSIS's (Technique for Order of Preference by Similarity to Ideal Solutions) for data transmissions as they select alternates i.e. least distances from optimal ones and greatest distances from negative ideal solutions. The degrees of congestion were determined based on ratios between average packet service times and average packet inter-arrival times were used.

Vinitha et al. [18] investigated energy issues of WSNs with their proposed Taylor C-SSAs (Taylor based Cat Salp Swarm Algorithms) where modified C-SSA were used with Taylor series. Their approach involved electing CHs (Cluster Heads) and data broadcasts at two levels for achieving multi-hop routing. For efficient information broadcasts, their scheme selected energy-efficient CHs based on LEACH protocol and SNs transmitted information over CHs that forwarded it to BSs (Base Stations) over selected best hops.

Devi et al [19] suggested cluster-based Data Aggregations for Latencies and Packet Loss Reductions. The study constructed Aggregation Trees and Slot Schedules in their proposed mechanisms. CHs used compressive aggregations to collect information from SNs while BSs constructed aggregate trees using MSTs (Minimum Spanning Trees). PLRs and latencies were taken into consideration while focusing on and allocating timeslots to S|Ns having collected information from them. The approach prevented unwanted rebroadcasts and waits that were found to be advantageous in improving WSN's network performances.

Rekha & Gupta (2021) [20] presented a secure confirmation and key organization approach based on ECCs (Elliptic Curve Cryptographies) which were used for ensuring WSN's transmission of information and images. Their scheme was found to be safe, reliable, and appropriate for developing sensor-based IoTs and applications. The protocol was capable of defending the networks against hello flood, DOSs (Denial-of-Services), man-in-the-middle, and other attacks or security threats including mutual authentications, confidentialities, data integrities, perfect forward secrecies, and fair key agreements. Their proposed protocol was confirmed as safe against known threats in AVISPA simulations. Also, their performance evaluation proved the excellence of the proposed work when compared to other available approaches.

Qazi et al (2021) [21] primarily targeted security issues of WSNs by their unique authentications and data encryptions approach for communications between SNs. Their proposed scheme not only provided security for these communications but also accumulated memory spaces on nodes with the help of ECDSAs (Elliptic Curve Digital Signatures) cryptographic schemes in their key generations using times, counts of hello messages, and packet sizes. Additionally, their use of ASCWs (Algorithm for Wireless Secure Communications) allowed key managements with acceptable key lengths, thus assisting secure communications of nodes and efficient security of WSNs. Their ASCWs based authentications also reduced risk costs and security risks in comparison. Their creation of physical test beds using equipment and sensor motes were used for benchmarks for comparisons in terms of key generation times, counts of hello messages sent, and data packet sizes where findings demonstrated the appropriateness of ASCWs and implied that the new solution is used for safeguarding data on nodes during the WSN's connections.

Secure Data Communication and Enhance Sensor Reliability (SDER) based on ECCs were proposed by authors of [22]. ECC's Weierstrass functions tested the dependability of SNs while cryptography based on ECCs was used for network data security. The results of the study's simulation showed that the suggested SDER decreased both PLRs and network latencies.

Arya et al. [23] defined ideal conditions for routing. The work considered the best circumstances for bandwidth consumption where their predictions of bandwidths were enhanced by the use of ACOs for saving electricity. Their scheme demonstrated the use of energy-conscious routing protocols that can calculate energy utilization of WSNs from bandwidths without the use of optimizations. ACOs calculated optimum bandwidths for routing paths and energy consumption. Bit error rates were used to assess network performances where the study's findings indicated that optimizations based on ACOs provided practical and efficient routing strategies that increased the lifespan of WSNs.

The study in [24] described revolutionary LSDARs (light-weight structure-based Data Aggregation Routes) protocol for IoTs enables Networks that enhanced energy routing performances while protecting data at SNs against malicious attacks. The scheme divided networks into distinct clusters with varied radii to prevent energy gaps near BSs. This was

RESEARCH ARTICLE

followed by the creation of efficient and loop-free routes using A-star heuristics. Moreover, data security was provided by employing a mathematically unbreakable OTPs (one-time pads) encryption mechanism which safeguarded end-to-end communications and specifically from hostile SNs. Their simulation outcomes showed significant improvements when compared to other methods in terms of energy consumption, network lifespan, end-end delays, and PDRs (packet drop ratios).

ELSOA-CAs scheme was proposed for achieving ideal, quicker, and energy efficient data transmissions [25]. But, in the earlier work, the congestion-aware multipath routing mechanism is not considered. Moreover, for the bigger file, the security is not still strong. This is addressed in the proposed work by using HSALSO-CA (Hybrid Simulated Annealing with Lion Swarm Optimization and Centralized Authentication) mechanisms. In the proposed technical work, optimum, quicker, and energy-efficient data transmission is highlighted to guarantee that the decision-making regarding tomato crops is achieved with accuracy.

3. SECURED AND RELIABLE DATA TRANSMISSION IN WSN

In the proposed research work, the focus is on optimum, quicker, and energy efficient data transmission that guarantees the decision-making on tomato crops with accuracy. In this research work, multipath routing is presented for making sure that the data transmission speed is high. In this, rapid multipath routing is ensured by choosing the optimum forwarder nodes that face limitations in energies and packet deliveries. Hence, this work employing the suggested HSALSOA selects Optimal Forwarding Nodes. The Simulated Annealing algorithm is a hybridized one as it achieves optimum local and global search potential for the bigger network. Data transmission with better security is ensured by utilizing the modified ECC algorithm that improves the security of congestion-aware multipath routing mechanism. The framework of the discussed work is illustrated in the following figure 1.

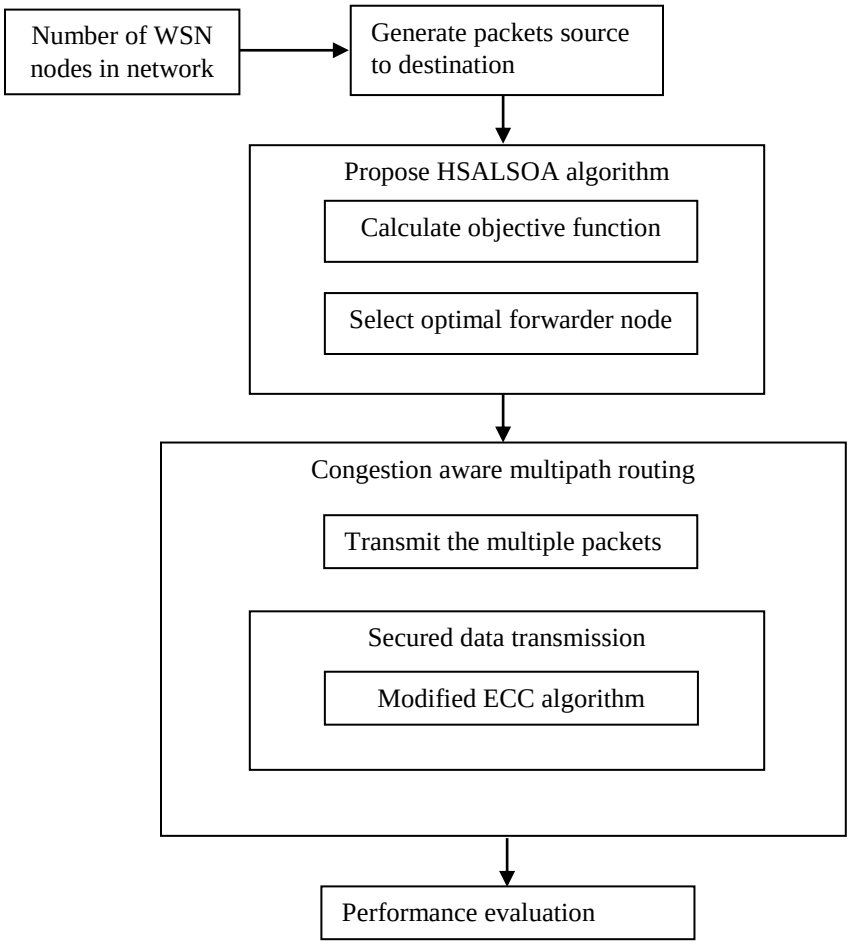

Figure 1 Architecture of Secured Data Transmission System

RESEARCH ARTICLE

3.1. System Model

WSNs used in this work consist of N number of SNs, used for sensing, observation, and acquisition of data. Every node in a particular network is stationery and power regulated. Entire WSN nodes help in the regular execution of sensing tasks with consistent data broadcast to BS that deals with nodes inside/external its range. Nodes could act as Cluster Head or simple sensor nodes [26] [27]. The proposed architecture of the network is depicted in Figure 2.

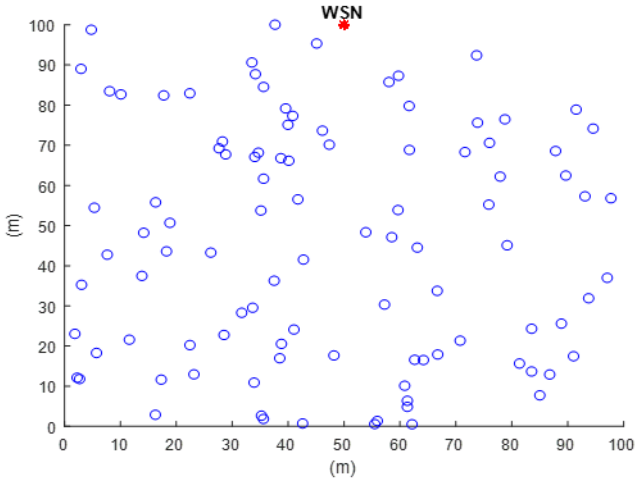

Figure 2 Network Formation

3.1.1. Energy Model

The proposed model helps in the energy analysis of nodes. Supposing that every node includes starting energy, E_i, then energy is exhausted once node i, responses or sends a broadcast to other node j [28]. Power depleted during broadcast is P_T when P_R indicates the power consumption of iwhen getting the data unit from j. Also presuming that the energy of a sink node is unconstrained and the node is on constant movement till completion of network lifespan (from beginning till dead), then goal of optimization is about achieving optimality in routing mechanisms and CH elections that improve network lifespan. Linear programming models increase the network lifespan [29] [30]. Power consumption during the transmission of L bits for distance D_t is given in Equation (1) and (2), where P_{amp} indicates the power consumed.

$$P_T = \begin{cases} P_{cons} * L * P_{amp} * D_t^2 if D_t < D_0 \\ P_{cons} * L * P_{amp} * D_t^2 if D_t \geq D_0 \end{cases} \quad (1)$$

$$P_R = P_{cons} * L \quad (2)$$

Where P_T refers to the power dissipation when transmitting the packets

L stands for bits

P_{amp} indicates power amplification

D_t signifies the distance among nodes

D_0 refers to the threshold distance

P_R indicates the power consumption during the receipt of the packets

The power dissipation is considerably decreased in the node further if it is made sure the data transmission and shortest routing path is achieved with efficiency.

3.1.2. Mobility Model

The model is intended for Internet of Things nodes existing in a system. This depends on device place, speed and how well it is connected. Let n_1 and n_2 refer to the IoT nodes at locations (u_1, v_1) and (u_2, v_2), correspondingly. Presuming that the nodes move to a new position (u_1', v_1') and (u_2', v_2') for a correlation, then the Euclidean distance between them can be defined in eqn (3)

$$d(0) = |u_1 - u_2|^2 + |v_1 - v_2|^2 \quad (3)$$

WSNs based IoT node distances at time l and their location is measured through eqn (4)

$$d(l) = |u_1' - u_2'|^2 + |v_1' - v_2'|^2 \quad (4)$$

Where (u_1', v_1') and (u_2', v_2') indicate the new locations of n_1 and n_2.

3.1.3. Objective Model

Here, objective model considers energy, and WSNs network delay. HSALSOA method is proposed to choose optimal of the forwarder nodes, yielding ideal results for flexible network. Next, CA system is used for multipath data broadcast over WSNs network. Expressions used for computing the delay, hop count, energy and lifespan can be defined in eqn (5).

$$delay(d) = \frac{\sum_{i=1}^{n}(T_{ri} - T_{si})}{n} \quad (5)$$

Where, T_{ri} – ith packet receipt time ,T_{si} - ith packet sending time, n – number of total packets

The energy is calculated using eqn (6)

$$Energy\ (e) = [(2 * pi - 1)(e_t + e_r)d \quad (6)$$

Where, pi - data packet, e_t - packet i's transmission energy, e_r - receiving packet i's energy, d - distance among source and destination node.

Objective model O_M is obtained through eqn (7):

$$O_M = n(M_e * L_d) \quad (7)$$

here N – total nodes with optimal energy and delay

M_e- Minimum energy utilization node

RESEARCH ARTICLE

L_d- Less delay

It is also utilized for choosing the numerous optimal forwarder node selection and multipath routing using HSALSOA mechanism.

3.2. Optimal Forwarder Node Selection using HSALSOA

The Suggested HSALSOA method chooses optimal forwarder nodes for rapid network broadcasts. Elections of forwarding nodes are quite complicated. A set of neighbors exists for source nodes and forwarding nodes where the latter are selected by considering their physical distances from BSs, remaining energy levels, and quality of networks. Depending on broadcast distances/ranges, sound propagation speeds, residual energies, packet collision preventions, and prevention of redundancies in broadcasts, the forwarded data packets remain in forwarder nodes for specified amounts of time. Based on the aforementioned factors, the best forwarding nodes are ones that hold packets for shorter periods. In case nodes discover overheard packets, then these packets are discarded while other packets are retained in buffers till they are forwarded. Measures taken into account for forwarder node selections have direct influences on the performance of routing protocols whereas residual energy metrics help create balances in node energies. Link qualities are primary measures as they affect the energy usage of SNs and PDRs. Measuring depths are useful in decreasing energy dissipations since the sink's beacon transmissions are used to compute local depths and physical distances. As a result, multiple parameters for energy efficacy and resilience of forwarder nodes need to be considered in the selection procedures of forwarder nodes. SNs other than selected forwarder nodes store data packets and when their holding times expire, they relay and do not spy. Hence, shortest path selections are an elementary challenge as they impact transmissions and lifespans of networks based on energy levels [31]. It is natural to choose SNs with minimized depths compared to senders so that broadcasts and elections of forwarder nodes are limited. This work has introduced HSALSOA for optimum forwarder node selection. The Simulated Annealing algorithm is hybridized as it encompasses ideal local and global search capability for the bigger network.

3.2.1. LSOs (Lion Swarm Optimizations)

LSOs are bio-influenced metaheuristic algorithms for optimization problems. It was proposed in 2009 at Cambridge University [32]. LSOs rely on the natural split of labor amongst lion kings, lionesses, and lion cubs among lions pack have been put forward recently. The primary concept of LSOs is explained in Algorithm 1 [33]. At first, the method performs random initialization of the location of lions in search space, and the location having optimal fitness value is fixed as the lion king's location. Next, multiple lions are selected to be the hunting lions (also known as a lioness) and coordinate with one another for hunting. If the prey is better compared to the lion king's prey, then the location of the prey would be taken by the lion king. So, cubs go behind the lioness so that they can study to hunt or eat close to the lion king, and would be sent out of the herd when they become adults. For survival, the lions which are sent out will attempt to get nearer to the optimal place that they have in memory. At first, as per labor division and cooperation, lions retain looking repetitively to obtain optimum data of objective function.

Steps of LSO algorithm:

Step 1: Initialize the position of every lion x_i, n, T, D, a_1, a_2 and β.

Step 2: (1) compute the fitness value of every single lion and the value of nLeader

(2) Order the positions of lions based on their fitness value

(3) Find the lion king, lionesses and lion cubs. Record $P_{best}$and $G_{best}$and select $P_{bestc}$and P_{bestm}.

(4) Generate random number γ using normal distribution N (0,1). Compute α_f and α_c.

Step 3: Update the position of lion king

Step 4: Update the position of lionesses

Step 5: Generate random number q and γ through U $(0,1)$ and N $(0,1)$. Update the position of lion cubs.

(1) If q ≤ 1/3, update the position of lion cubs

(2) If 1/3 < q < 2/3, update the position of lion cubs

(3) If 2/3 ≤ q ≤ 1, update the position of lion cubs

Step 6: (1) Compute the fitness values in accordance with the position of lion, and update pbest ,gbest, Pbestc and Pbestm.

(2) verify if the algorithm meets the stop criterion.

(3) If the termination condition is attained, move to Step 8; else, move to Step 7.

Step 7: order is resorted for every constant number of iteration (nearly 10 times) to decide the position of the lion king, the lionesses and the lion cubs, and go to Step 3.

Step 8: Output the location of Gbest to be best solution of optimization problem, terminate the iteration process.

Algorithm 1 LSOs

3.2.2. Simulated Annealing

Simulated Annealing (SA) is one of the most predominant metaheuristic algorithms that have the capability of global

RESEARCH ARTICLE

optimizations [34]. SAs are trajectory based, arbitrary search strategies that mimic annealing processes that occur when metals are frozen too for crystals with the minimum usage of energies and achieving larger crystal sizes and thus minimizing limitations of metallic structures. The annealing procedure consists of careful temperature control and cooling rate, frequently known as the annealing schedule. SAs are used with success in different fields.

The method begins with the primary result and gets a close response for that result, and if there is no improvement in the objective function, it is taken with a probability p. here ΔE refers to the difference between the objective function of the present response and the neighbor's response, T indicates temperature. At every temperature, multiple iterations are run, then the temperature is reduced gradually. In the initial stages, the temperature is maintained very high to improve the probability of getting worse responses.

The slow temperature reduction in last steps leads to possibilities of getting worse replies to reduce and therefore, method gets converged to best response. This method averts being restricted into local optimized locations resulting in movements towards reduced energies. The solution levels of x with fitness obtained using function f(x) based on its neighbours x', N(x). The differences amongst objective functions of levels are given in eqn (8):

$$\Delta = f(x) - f(x') \quad (8)$$

X' can be computed with the equation (9) below:

$$P_s = \exp\left(-\frac{\Delta}{T}\right) \quad (9)$$

Next, the probability of admitting a arbitrary value $r \in (0,1)$ is then contrasted and x' becomes acceptable if P>r. T refers to temperature that the cooling plan controls. But, simulated annealing method consists of other factors like primary temperatures, varying temperatures, and cooling plans. The fundamental construction of SA method is provided Algorithm 2.

- Choose a starting solution x
- REPEAT
- Form the solution x' in neighborhood of x_0
- Compute Δ, probability using Equation. (8)
- Determine the new solution by P_s
- Remember optimal solution got till now
- Decrease the temperature
- UNTIL criteria are satisfied

Algorithm 2 Construction of SA Method

3.2.3. Hybrid Lion Swarm Optimization Using Simulated Annealing

This work introduces a novel approach to solving optimization problems. The proposed approach is a hybrid form of lion swarm optimization and a simulated annealing algorithm. Lion swarm optimization is population-driven. These algorithms exhibit a significant capability in global search, even though they are found to be not very strong in local searches. As mentioned in the earlier segment, the simulated annealing method consists of a procedure for neighbor search.

The procedure achieves an improved local search ability for the proposed technique; however, it executes strong global searches. Fusions of these methods help in global explorations search spaces with lion swarm methods and locally employing simulated annealing technique, thus exploiting benefits of both algorithms.

The proposed technique includes the generation of n primary population of the lion is initially done and the position of each lion is calculated. Then, every lion goes in the direction of the lion with maximum attraction. This work's produced solutions use simulated annealing approaches for local searches where its form can be generalized in Algorithm 3.

1. Starting initialization of lion swarm algorithm factors like total primary population N_{Pop}, total maximum replications, and coefficients of attraction.

2. Starting Initialization of simulated annealing process variables, such as total repetitions and main temperature (T).

3. Creation of N_{Pop} lion (primary solution).

4. For every pair of lion (solutions) utilize subsequent steps:

4.1. When fitness of lion i is greater than lion j (or when fitness function i is comparably good than fitness function j), lion i travels towards lion j as per following eqn (10):

$$\Delta x_i = \beta_0 e^{-\gamma r_{ij}^2}\left(x_j^t - x_i^t\right) + \alpha\varepsilon_i \quad (10)$$

4.2. Modify the position based on the distance.

4.3. For every obtained solution x:

4.3.1. Get x neighbours.

4.3.2. when its energy is reduced $\Delta E < 0$, take solution, else admit it if $exp\ (-\Delta E/T)$

4.3.3. If the balance is not attained, temperature has to be reduced and move to step 4.3.1.

4.4. When the termination criterion of the method is not satisfied, go to step 4.

Algorithm 3 Simulated Annealing Approaches

RESEARCH ARTICLE

3.3. Secured Routing Using Modified Elliptic Curve Cryptography

When data transmissions are monitored during assaults, two metrics get measured namely delays and Packet Loss Ratios (PLRs). These variables determine if users meet their requirements of Quality of Services (QoSs). PLRs are defined as proportions of total dropped packets during flows to overall total packets of similar flows. Delays and PLRs are superior measures for assessments, specifically in the case of malicious user flows as the networks would face excessive delays. The aforementioned attacks can significantly impact QoSs including delays, throughputs, Packet Delivery Ration (PDRs), jitters, and energies.

ECC hybrid signcryption cryptographic approaches which create public/private encryption keys are used for recoveries after attacks. ECCs performs better than other encryption technique in terms of limited key lengths, stronger security, constrained memory spaces, enhanced speeds, computational costs, and forwarding privacies. Approaches of ECCs generate optimal private/public keys.

Hash padding, results of digital signatures are used in signcryption techniques. Hash padded data are then applied to encrypted hash functions with certificates received from digital signatures i.e. digitally signed. This implies authentication of data amongst neighbors. Subsequently, signed data packet are encrypted using CBCs (Cipher block chains) where plaintext blocksand earlier blocks of ciphertexts go through XOR operations prior to their encryptions. In this manner, every block of ciphertext relies on entire plaintext blocks that are handled till that point. For making every message distinct, an initialization vector has to be utilized in starting block. CBCs have remained a prominent method of analysis. The messages need to be padded in multiples of cypher block sizes, and only sequential encryptions are possible (they cannot be parallelized). One way of handling this obstacle is by using ciphertext stealing. Single bit variations in plaintexts or initialization vectors impact the following ciphertext blocks. IV, or starting variables are blocks of bits used by different modes to make encryptions random and hence offer separate ciphertexts even when comparable plaintexts are encrypted several times without requiring time-consuming re-keying procedures. The ultimate goal is to create the best signcryption possible, based on KEMs (Key Encapsulation Mechanisms) and DEMs (Data Encapsulation Mechanisms). KEMs are implemented using KDFs (Key Derivation Functions) and secure pseudo random number generation techniques [34]. KEMs transfer secret symmetric keys where extra keys are required to share secret keys for different cryptographic purposes like encryptions and integrity protections. KDFs are used to extract secret keys from other keys or known information using safe pseudo-random value methods where pseudo-random number generations and KDFs are separate in KDFs. In traditional signcryption systems, DEMs are applied on basis of AES encryptions whereas in this suggested approach, AES methods are substituted with optimal ECCs.

Algorithm 4 shows how ECCs produce private and public encryption keys in signcryptions. ECCs increasing data security and ensure that keys generated are reliable. The functions in ECCs are specified in Prime and Binary fields where suitable fields with a finite big number of points are chosen for cryptography. The prime field procedure involves choosing prime integers and generating elliptic curves with points spanning from 0 to Z.

- Order the transmission of full data packets throughout a timed session.
- Use a digital signature (static) as the Initialization Vector for the XOR operation on plain text.
- To get Cipher Texts symmetric key encryptions are used along with CBCs.

  Cipher_texts1=CBCs

  (Plain_texts1⊕Digial_signature_no)

- To perform XOR on subsequent packets, Cipher texts from the first packet are used.

  Cipher_texts2=CBCs (Plain_texts2⊕Cipher_texts1)

- The procedures are iterated for all of session's packets.

  Cipher_textsi= CBCs (Plain_textsi⊕Cipher_textsi-1)

- Symmetric keys are padded with data packets during iterations.
- Data padded with keys are encrypted using Asymmetric Key Cryptography procedures of ECC's
- KEMs and D|E|Ms are used on data packets

Algorithm 4 ECC Based Signcryption Method

4. RESULTS AND DISCUSSION

Table 1 Simulation Factors

Factor	Values
Number of Nodes	100
Size of Area	1100 X 1100 m
Mac	802.11
Radio Range	250m
Simulation Time	60 sec
Packet Size	80 bytes

RESEARCH ARTICLE

The experiments on HSALSO-CA are carried out and its comparison analysis is performed with other techniques in this section. The techniques taken for assessments are ACOs (Ant Colony Optimizations), LSDAR (Light Weight Structure-based Data Aggregation Routing), ELSOA-CAs and suggested HSALSO-CA and the simulation is performed employing the NS-2 simulator. The measures taken for contrasts are E2E delay, throughput, energy dissipation, network lifetime. Simulation factors considered are mentioned in Table 1.

4.1. Performance Assessment

4.1.1. End to End Delays

These are the average times that packets consume while being transferred from sources to destinations in networks and based on Equation (11).

$$End - to - end\ delay = \frac{\sum_{i=1}^{n}(t_{ri} - t_{si})}{n} \quad (11)$$

Where t_{ri} – ith packet delivery time, t_{si} – time when ith packet was sent, n – number of packets.

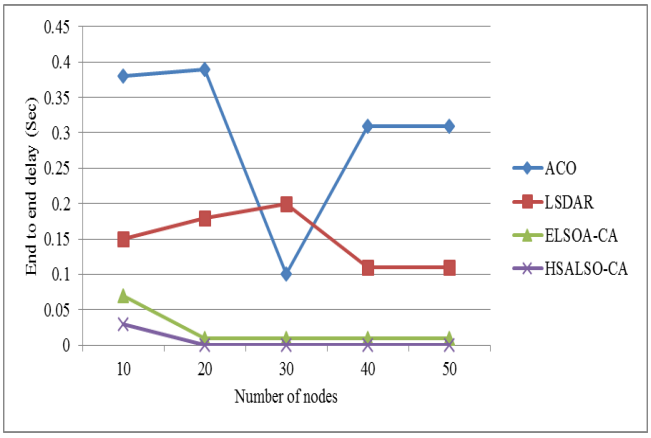

Figure 3 E2E Delay Comparison

Figure 3 shows comparative evaluations in terms of end-to-end delays where nodes form the x-axis while their corresponding delay values are plotted on the y-axis. Compared techniques include ACO, LSDAR, ELSOA-CAs, and the proposed HSALSO-CA algorithm which yields reduced E2E delays. Therefore, the proposed HSALSO-CA method chooses the best forwarder nodes by their HSALSO fitness values.

4.1.2. Throughputs

These are data packets sent against packets received effectively in networks and computed using Equation (12).

$$Throughputs = total\ number\ of\ packets\ sent\ /time \quad (12)$$

Figure 4 depicts comparison evaluations in terms of throughput performance of ACOs, LSDAR, ELSOA-CAs, and the suggested HSALSO-CA algorithm where nodes form the x-axis while their corresponding throughputs are y-axis values. The suggested method of this work yields increased throughputs amongst the strategies studied for comparison. As a result, the proposed HSALSO-CA system selects the optimal forwarder nodes based on HSALSO fitness values.

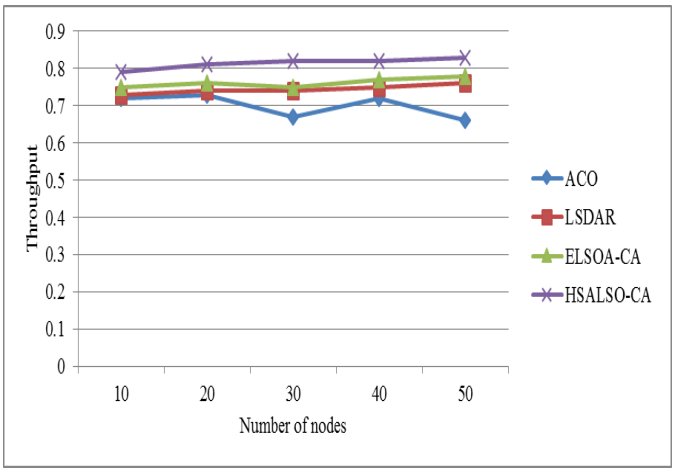

Figure 4 Comparison of Throughput

4.1.3. Energy Consumptions

This parameter implies average energies required by networks for transmissions of packets to SNs within a specified time frame and given as Equation (13)

$$Energy\ (e) = [(2 * pi - 1)(e_t + e_r)d \quad (13)$$

Where pi - data packet, e_t - packet i's source energy, e_r - energy needed for the receipt of packet i, d - distance among source and destination nodes.

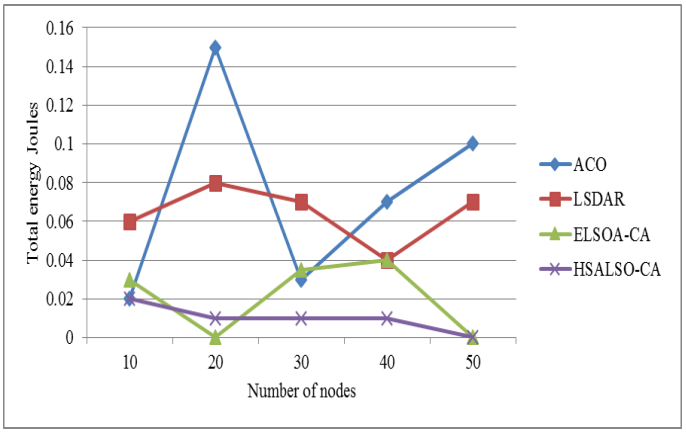

Figure 5 Energy Consumption Comparison

Figure 5 shows the comparative analysis concerning energy utilization performance, where nodes form the x-axis while their corresponding energy utilization is y-axis values.

RESEARCH ARTICLE

Compared techniques comprises of ACO, LSDAR, ELSOA-CAs, and the proposed algorithm HSALSO-CA dissipating less energy. Therefore, the proposed HSALSO-CA system helps in choosing the best of the forwarder nodes on the basis of HSALSO fitness data.

4.1.4. Network Lifespans

The life spans of networks can be computed using Equation (14)

$$Lifetime\ \mathbb{E}[L] = \frac{\varepsilon_0 - \mathbb{E}[E_w]}{P + \lambda \mathbb{E}[E_r]} \qquad (14)$$

Where P represents network's constant power consumptions and a continuous value, ε_0 represents sum of non-rechargeable initial energy, λ stands for average reporting rates of sensors, $\mathbb{E}[E_w]$ implies the expected energy wastages or non-utilized energies till the death of a network and $\mathbb{E}[E_r]$ –reported energy consumption of nodes.

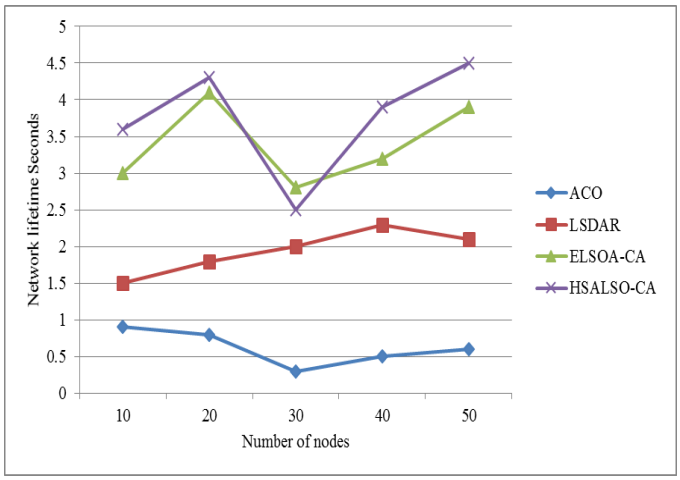

Figure 6 Network Lifetime

Figure 6 depicts a comparison analysis concerning the performance of network lifetime, where nodes form the x-axis while their corresponding network's life spans are y-axis values. The methods used in comparisons include ACOs, LSDAR, ELSOA-CAs, and proposed HSALSO-CA which yields an increase in network lifetime. Therefore, the proposed HSALSO-CA selects the best of the forwarder nodes by HSALSO fitness values.

4.1.5. PDR

PDR indicates the proportion of total lost packets to overall sent packetscan be expressed in eqn (15)

$$\text{Packet loss ratio} = \frac{N^{tx} - N^{rx}}{N^{tx}} \times 100\% \qquad (15)$$

Where N^{tx} - transmitted packets, N^{rx} - received packets. This evaluation was carried out through the extraction of all real-time packet sizes, which are sent and obtained.

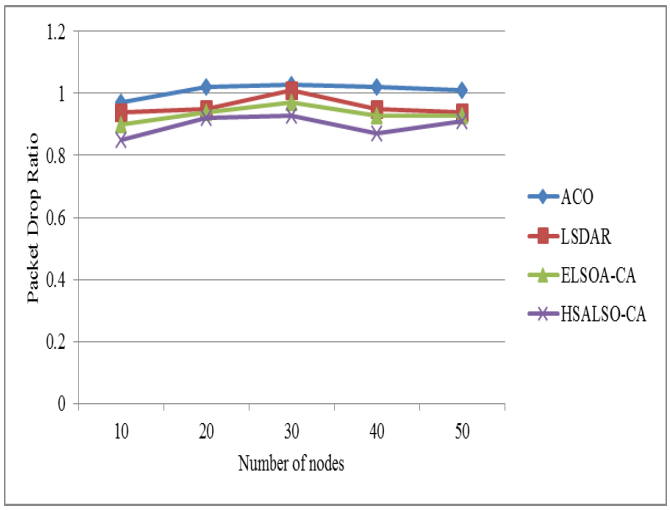

Figure 7 Packet Drop Ratio

Figure 7 shows the comparison evaluation concerning PDR performance, where nodes form the x-axis while their corresponding PDRs are y-axis values. Techniques taken for comparison include ACO, LSDAR, ELSOA-CAs, and the proposed HSALSO-CA algorithm which reveals reduced PDR. This way, the proposed HSALSO-CA system chooses the best forwarder nodes based on HSALSO fitness values.

5. CONCLUSION

In the proposed technical work, the focus is on optimum, rapid, and energy-efficient data broadcasting such that decisions on tomato crops are made with accuracy. In this research work, multipath routing is proposed for guaranteeing that the data transmission is faster. In this, rapid multipath routing is made sure by choosing the optimal forwarder nodes that handle limitations in delays and energies. Hence, optimal Forwarding Node selections are employed using the proposed HSALSOA scheme. The Simulated Annealing algorithm is hybridized as it encompasses both optimal local and global search capability for the bigger network. Secured data transmission employing modified ECC algorithm guarantees increased security for congestion-aware multipath routing mechanisms. In comparison to existing methodologies, simulation results demonstrate that the proposed ELSOA-CAs model delivers superior performance in terms of throughputs, network longevities, reduced energy usage, and end-to-end delays.

REFERENCE

[1] Orhan, O. (2016). Energy neutral and low power wireless communications (Doctoral dissertation, Polytechnic Institute of New York University).
[2] Li, J., Liu, W., Wang, T., Song, H., Li, X., Liu, F., & Liu, A. (2019). Battery-friendly relay selection scheme for prolonging the lifetimes of sensor nodes in the Internet of Things. IEEE Access, 7, 33180-33201.
[3] Wang, C., He, Y., Yu, F. R., Chen, Q., & Tang, L. (2017). Integration of networking, caching, and computing in wireless systems: A survey,

RESEARCH ARTICLE

some research issues, and challenges. IEEE Communications Surveys & Tutorials, 20(1), 7-38.
[4] Shaf, A., Ali, T., Draz, U., & Yasin, S. (2018). Energy Based Performance analysis of AODV Routing Protocol under TCP and UDP Environments. EAI Endorsed Transactions on Energy Web, 5(17).
[5] Yang, L., Zhu, H., Kang, K., Luo, X., Qian, H., & Yang, Y. (2018, April). Distributed censoring with energy constraint in wireless sensor networks. In 2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) (pp. 6428-6432). IEEE.
[6] Randhawa, S., & Jain, S. (2017). Data aggregation in wireless sensor networks: Previous research, current status and future directions. Wireless Personal Communications, 97(3), 3355-3425.
[7] Tomić, I., & McCann, J. A. (2017). A survey of potential security issues in existing wireless sensor network protocols. IEEE Internet of Things Journal, 4(6), 1910-1923.
[8] Kharb, K., Sharma, B., & Trilok, C. A. (2016). Reliable and congestion control protocols for wireless sensor networks. International Journal of Engineering and Technology Innovation, 6(1), 68.
[9] Anand, N., Varma, S., Sharma, G., &Vidalis, S. (2018). Enhanced reliable reactive routing (ER3) protocol for multimedia applications in 3D wireless sensor networks. Multimedia Tools and Applications, 77(13), 16927-16946.
[10] Kumaravel, K., &Anusuya, N. (2018). A SURVEY ON CONGESTION CONTROL SYSTEM IN WIRELESS SENSOR NETWORKS. International Journal for Research in Science Engineering & Technology, 5(9), 7-11.
[11] Harish, V. S. K. V., & Kumar, A. (2016). A review on modeling and simulation of building energy systems. Renewable and sustainable energy reviews, 56, 1272-1292.
[12] Rosset, V., Paulo, M. A., Cespedes, J. G., & Nascimento, M. C. (2017). Enhancing the reliability on data delivery and energy efficiency by combining swarm intelligence and community detection in large-scale WSNs. Expert Systems with Applications, 78, 89-102.
[13] Bhatia, A., &Hansdah, R. C. (2016). TRM-MAC: A TDMA-based reliable multicast MAC protocol for WSNs with flexibility to trade-off between latency and reliability. Computer Networks, 104, 79-93.
[14] Mohanty, P., & Kabat, M. R. (2016). Energy efficient structure-free data aggregation and delivery in WSN. Egyptian Informatics Journal, 17(3), 273-284.
[15] Faheem, M., Butt, R. A., Raza, B., Ashraf, M. W., Ngadi, M. A., &Gungor, V. C. (2019). Energy efficient and reliable data gathering using internet of software-defined mobile sinks for WSNs-based smart grid applications. Computer Standards & Interfaces, 66, 103341.
[16] Elappila, M., Chinara, S., &Parhi, D. R. (2018). Survivable path routing in WSN for IoT applications. Pervasive and Mobile Computing, 43, 49-63.
[17] Sharma, B., Srivastava, G., & Lin, J. C. W. (2020). A bidirectional congestion control transport protocol for the internet of drones. Computer Communications, 153, 102-116.
[18] Vinitha, A., & Rukmini, M. S. S. (2019). Secure and energy aware multi-hop routing protocol in WSN using Taylor-based hybrid optimization algorithm. Journal of King Saud University-Computer and Information Sciences.
[19] Devi, V. S., Ravi, T., & Priya, S. B. (2020). Cluster Based Data Aggregation Scheme for Latency and Packet Loss Reduction in WSN. Computer Communications, 149, 36-43.
[20] Rekha, & Gupta, Rajeev. (2021). Elliptic Curve Cryptography based Secure Image Transmission in Clustered Wireless Sensor Networks. International Journal of Computer Networks and Applications. 8. 67. 10.22247/ijcna/2021/207983.
[21] Qazi, R., Qureshi, K. N., Bashir, F., Islam, N. U., Iqbal, S., & Arshad, A. (2021). Security protocol using elliptic curve cryptography algorithm for wireless sensor networks. Journal of Ambient Intelligence and Humanized Computing, 12(1), 547-566.
[22] Uma Maheswari P, Ganeshbabu TR, P.Subramaninan, Elliptic Curve Cryptography based Secure Data Communication and Enhance sensor Reliability in Wireless Sensor Network, International Journal of Recent Technology and Engineering (IJRTE), 8(5), 2020.
[23] Rajeev Arya and S.C. Sharma, "Energy Optimization of Energy Aware Routing Protocol and Bandwidth Assessment for Wireless Sensor Network", International Journal of System Assurance Engineering and Management, 9(3), pp. 612-619, 2018.
[24] Haseeb, K., Islam, N., Saba, T., Rehman, A., & Mehmood, Z. (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.
[25] Silambarasan, S., & Devi, M. S. (2021). Enhanced Lion Swarm Optimization Algorithm With Centralized Authentication Approach for Secured Data Transmission Over WSN. ICTACT Journal on Communication Technology, 12(3), 2471-2479.
[26] W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks," IEEE Transactions on Wireless Communications, vol. 1, no. 4, pp. 660–670, 2002.
[27] D. Kumar, T. C. Aseri, and R. B. Patel, "EEHC: energy efficient heterogeneous clustered scheme for wireless sensor networks," Computer Communications, vol. 32, no. 4, pp. 662–667, 2009.
[28] Lee, H.; Wicke, M.; Kusy, B.; Gnawali, O.; Guibas, L. Data Stashing: Energy-Efficient Information Delivery to Mobile Sinks through Trajectory Prediction. Proceedings of the 9th ACM/IEEE International Conference on Information Processing in Sensor Networks, Stockholm, Sweden, 12–16 April 2010; pp. 291–302.
[29] Tian, K.; Zhang, B.; Huang, K.; Ma, J. Data Gathering Protocols for Wireless Sensor Networks with Mobile Sinks. Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM 2010), Miami, FA, USA,, 6–10 December 2010; pp. 1–6.
[30] Kusy, B.; Lee, H.; Wicke, M.; Milosavljevic, N.; Guibas, L. Predictive QoS Routing to Mobile Sinks in wireless sensor networks. Proceedings of the IEEE International Conference on Information Processing in Sensor Networks (IPSN, 2009), San Francisco, CA, USA, 13–16 April 2009; pp. 109–120.
[31] Wang, M.; Heidari, A.A.; Chen, M.; Chen, H.; Zhao, X.; Cai, X. Exploratory differential ant lion-based optimization. Expert Syst. Appl. 2020, 159, 113548.
[32] Pierezan, J.; Coelho, L.d.S.; Mariani, V.C.; Goudos, S.K.; Boursianis, A.D.; Kantartzis, N.V.; Antonopoulos, C.S.; Nikolaidis, S. Multiobjective Ant Lion Approaches Applied to Electromagnetic Device Optimization. Technologies 2021,
[33] E. Aarts, J. Korst, and W. Michiels, "Simulated annealing," in Search Methodologies: Introductory Tutorials in Optimization and Decision Support Techniques, K Burke and G. Kendall, Eds., pp. 91–120, Springer US, Boston, Mass, USA, 2nd edition, 2014.
[34] Nishanth, R. B., Ramakrishnan, B., & Selvi, M. (2015). Improved signcryption algorithm for information security in networks. International Journal of Computer Networks and Applications (IJCNA), 2(3), 151-157.

Authors

Silambarasan S received the BCA (2004) from Periyar University, Salem, MCA (2008) from Anna University and M.Phil (2014) in Computer Science from the Vinayaka Missions University, Salem. He joined the Department of Computer Science and Applications at Don Bosco College, Dharmapuri in 2009, as an Assistant Professor. His research interests include Data Mining, Big Data, and Network Security.

RESEARCH ARTICLE

Dr. M. Savitha Devi completed her Ph.D in Mother Teresa Women's University, Kodaikanal. She done her M.C.A and M.Philfrom Periyar University, Salem, and studied her PGM.Sc Computer Science in Vysya College, Salem where she got University 11th rank in the year 2003. She completed her under graduate course in Government Arts College, Salem-8. She began her carrier as Assistant Professor in Computer Science in AVS College, Salem in 2003 and taught for 4 years and then joined in Don Bosco College, Dharmapuri and continued her teaching profession for 9 years as a Faculty, Head of the Department, Research Co-Ordinator, IQAC Co-Ordinator, Academic Council Member, Class Quality Cell Co-Ordinator as well as member in various committees. She also attended Faculty Development Programmes on "Total Quality Management" organised by CHRIST University, Bangalore and "Role of IQAC Towards Quality Assurance in Autonomous Colleges" organised by Sacred Heart College, Thirupattur. She has received a Best Co-Ordinator award by ARK Techno Solutions, IIT Chennai, chief faculty 2015 ROBOKART.com. She has completed a "Virtual Course for Teachers of Higher Education in International Distant Education Unit of DBI of Higher Education – Brazil" on Oct' 2009 to Apr'2010. She was a Board of Studies member for B.Sc Digital Print Media in Periyar University, Salem for 7 years. She acted as an External Expert Committee Member in MGR College, Hosur on 2013 for Visual Communication Course. On July 2017, she joined as an Assistant Professor and Head in Computer Science, Government Arts and Science College, Harur - 636903, Dharmapuri District, TamilNadu and continuing her admirable job in the 18th year.

How to cite this article:

S. Silambarasan, M. Savitha Devi, "Hybrid Simulated Annealing with Lion Swarm Optimization Algorithm with Modified Elliptic Curve Cryptography for Secured Data Transmission Over Wireless Sensor Networks (WSN)", International Journal of Computer Networks and Applications (IJCNA), 9(3), PP: 316-327, 2022, DOI: 10.22247/ijcna/2022/212557.