EAI Endorsed Transactions
on Internet of Things
Research Article EAI.EU

Preventing Double Spending Attacks through Crow Search Algorithm to Enhance E-Voting System Security

S. Muthulakshmi[1,*] and A. Kannammal[2]

[1] KPR Institute of Engineering and Technology, Coimbatore, India
[2] Coimbatore Institute of Technology, Coimbatore, India

Abstract

Electronic voting system is the process of polling votes and counting votes. In most of the countries voting may now be done electronically, there are still several difficulties involved, including the expense of paper, how ballots are organized, the possibility of varying results when tallying the votes, and others. Duplicate votes pose a significant concern as they can be fraudulently cast by individuals. To focus on this issue,Distributed Ledger Technology (DLT) is employed to enhance the voting procedure in a secured manner. A directed acyclic graph is used by the Internet of Things Application (IOTA), a promising distributed ledger system. Faster transaction confirmation, high scalability and zero transaction fees are achieved via the Directed Acyclic Graph structure. In both IOTA tangle and blockchain technology, the public cast duplicate votes. The unauthorized user can create duplicate votes in the blockchain as well as IOTA tangle. This can be focused in this proposed method. The double spending problem can be solved by using Crow Search Algorithm (CSA). This Optimization problem produces an improved result for resolving double spending in e-voting systems.

Keywords: Internet of Things Application, Tangle, Directed Acyclic Graph, Crow Search Algorithm, E- Voting System, Double Spending Attack

Received on 01 December 2023, accepted on 19 February 2024, published on 26 February 2024

doi: 10.4108/eetiot.5208

*Corresponding author. Email: muthunjanu@gmail.com

1. Introduction

Voting is essential to enable people to elect the right leader for their country. Most of the places the conventional voting process doesn't produce correct result due to lack of security. The alternative method of conventional process is e-voting system which can be implemented through a mobile app and electronic voting machine. However, it does not necessarily provide a better solution.

Few research can be done by using Blockchain technology. In a blockchain, transactions are recorded in blocks, which progressively accumulate more transactions over time. As these blocks reach their capacity or a predefined time interval, they become finalized. After a block is finished, it is appended to the blockchain in a sequential and chronological fashion, forming an unbroken and unchangeable sequence of blocks. Implementing E-voting systems using blockchain technology introduces several challenges, including scalability concerns due to increased transaction volume, heightened energy consumption resulting from resource-intensive consensus mechanisms, potential security vulnerabilities, and the high costs associated with miners participating in the network [1]. IOTA is a decentralized ledger developed with a specific focus on supporting the Internet of Things (IoT) ecosystem. IOTA employs a Directed Acyclic Graph (DAG) data structure named the Tangle, in contrast to the use of traditional blockchains.

The Tangle allows for the direct inclusion of transactions into the ledger without the need for blocks, and each transaction must approve two previous transactions, forming a mesh-like structure. IOTA does not rely on miners but instead requires participants to

validate two previous transactions when submitting a new one, making it more decentralized and eliminating the need for transaction fees [2]. IOTA's Tangle offers potential advantages in terms of scalability, energy efficiency, and suitability for IoT applications. In this proposed System, the implementation of distributed ledger technology can address the lack of security effectively [3-4].

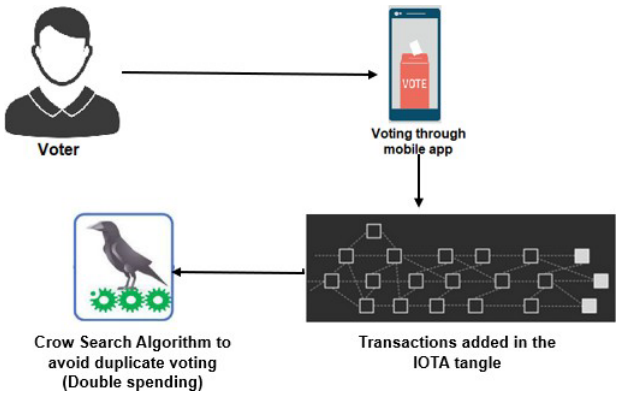

Figure 1. System Architecture diagram

In Figure 1, the overview of the proposed system is discussed. Initially, the voter possesses an Aadhar card number and a voter ID. These two identifications are linked together alongwith their mobile number. When the voter enters the mobile app, they have to verify themselves using their fingerprint, voter ID, and Aadhar number. After successful verification, the mobile app displays the list of candidates running in the election. The voter selects their preferred candidate, and the choice is recorded. Subsequently, the selection is added to the database for vote counting.
The contribution of the paper:

- The decentralized e-voting system uses a DAG that follows the fundamental properties of the voting system.
- Crow search optimization focuses on producing a better result for double spending attack in the voting procedure.

2. Literature Survey

Haseeb et.al [5] introduced the Secure and Energy-aware Heuristic-based Routing (SEHR) method, aiming to optimize routing in IoT-Wireless Sensor Networks (WSN) while effectively countering malicious attackers. The SEHR algorithm utilized a heuristic function that incorporated factors like hop count to the base station, link integrity, and remaining energy within the network. To ensure data security in the IoT-WSN, implemented counter mode encryption. The studies emphasized essential factors, such as route maintenance, energy consumption, and secure communication, to achieve reliable communication. In 2016, Alireza Askarzade H et al. introduced the CSA, which is a contemporary optimization technique. It draws inspiration from the activities of crows, where they store food and later retrieve it as needed. Since its inception, CSA has gained widespread popularity and various optimization problems in diverse fields, including chemical engineering [6], feature selection [7], medical sciences [8], and image processing [9].

Ikram Ullah's et al. [10] comprises various types of attacks faced by IOTA and analyzes the depth of the security vulnerabilities using the Common Vulnerability Scoring System. The vulnerabilities are categorized based on their feasibility and impact by this scoring method. In the literature survey conducted in Pericle Perazzo [11], the authors discussed routing attacks in the context of IOTA on the internet. Three distinct attacks have been identified that a malicious Autonomous System can execute against IOTA. These attacks are as follows: freezing the address, denial of consensus in both targeted and general form. The consequences of these attacks include potential financial losses, the disruption of consensus mechanisms for specific victim nodes, and even the disturbance of consensus throughout the entire IOTA cryptocurrency network.

The study conducted by Rani et al. [12] focuses on investigating the constraints faced by smart cities and analyzing their computational workload and storage resources. In this research, the authors propose a novel approach that combines software defined networking to detect network attacks and blockchain technology for data transmission. The smart cities model they construct establishes a secure framework for the IoT. Chen's et al. study [13] centers on double spending attacks within the DAG structure. The attackers create an illegal tangle, which is then integrated into the network to appear legitimate, enabling them to execute double spending attacks within the tangle network. The study explores the security threshold and its influence on the resilience of the tangle, evaluating the likelihood of potential vulnerabilities. By manipulating key parameters in the security threshold, IOTA can proficiently detect fraudulent tangle branches, thereby mitigating the risk of double-spending attacks.

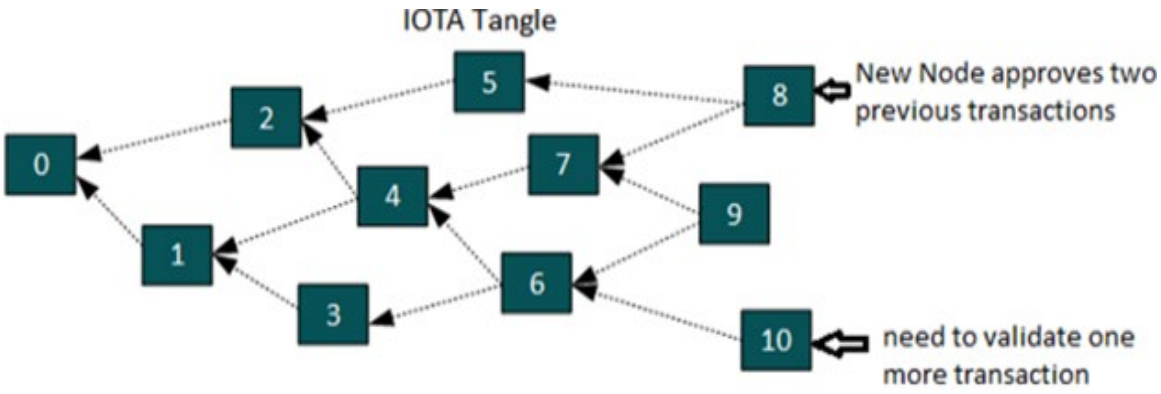

Figure 2. IOTA

3. Concepts of Internet of Things Application

IOTA focuses on the IOT ecosystem, supporting various applications such as supply chain management, driverless vehicles, smart cities, trading and more. It enables a machine-to- machine communication, fees less transaction while achieving high scalability. DAG used in the IOTA distributed ledger technology. IOTA's distributed ledger technology utilizes a DAG known as the Tangle to organize transactions in a unique manner. The Tangle allows participants in the network to transact value or data efficiently and securely. When a new participant creates its own transaction, it must validate whether two previous transactions, created by other participants are valid or not in the network. More approving transactions result in an increased security level. The previous two transactions can be chosen by the participants based on tip selection consensus mechanism.

In the figure 2; shows the illustration of IOTA tangle in the network with a total of 11 nodes are participating in the IOTA network. Each node verifies 2 or more transactions in the network. In figure 2, Node 3, 4, 7 are approved by at least two transactions. Node 5, 10 have only been approved by one transaction and need to approve one transaction to complete the procedure.

4. Proposed System

4.1. Crow Search Algorithm

The implementation of the metaheuristic optimization algorithm was inspired by intelligent crow behavior. The CSA imitates how search the food crow independently, communicating with other crows and then shares the food they find, which increases their effectiveness at foraging [14-17]. The CSA used to find optimal solution for complex mathematical functions or parameter optimization in various engineering applications.

Local Search

Crows conduct a search around its position form their current position by making a small adjustment to the positions of individual crow. This search operation finds its local neighbourhoods in a better solution. This process allows the algorithm to focus on regions that are likely to contain local optima, where a higher-quality solution can be found within a limited region of the search space. This local search enhances its exploration and exploitation capabilities of the crucial component. The local search is typically performed using heuristic rules or operators that guide the movement of each crow. These rules are designed to balance exploration and exploitation. In Figure 3 shows the exploration involves searching a broader area of the solution space to discover diverse solutions, while exploitation involves refining the search to focus on promising regions and converge to better solutions. Neighbourhood search, gradient search, greedy improvement and perturbation are techniques to perform local search in the CSA.

Global Search

The global search mechanism involves the sharing of information among individual crows (candidate solutions) to promote exploration of different regions in the solution space. This collective information exchange helps in escaping local optima and allows the algorithm to search for potentially better solutions in a broader and more diverse manner. In figure 4 shows the exploitation of CSA.

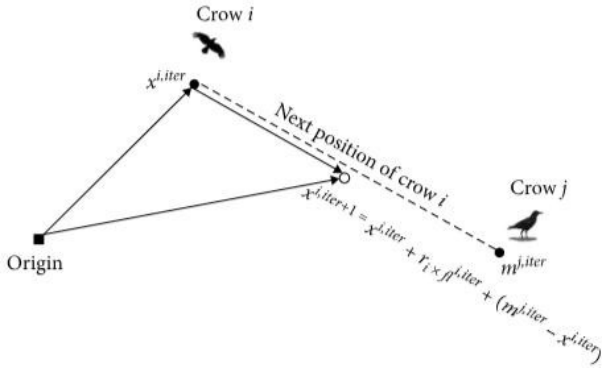

Figure 3. Exploration of CSA

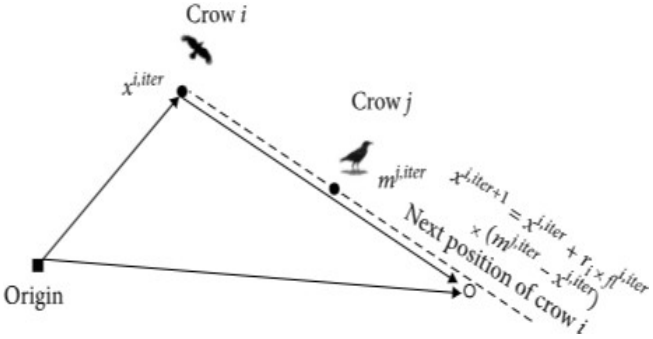

Figure 4. Exploitation of CSA

The essential stages of the CSA [18] are delineated as follows:

Step 1: Initialize Crow Size (N), position of crow (pos), Maximum iteration number (MAX itr), and Probability of Awareness (AP), Step size Flight (fl), Initial memory (m).

Step 2: setting up the memory matrix and individual crows. Crows are produced in the n- dimensional search space on each row $x_i = x_{i1}, x_{i2}, x_{i3}, \ldots\ldots x_{in}$ that provides a workable solution to a problem.

Step 3: Determine the fitness calculation for every individual crow

Step 4: Two things might happen if a crow declares that it wants to steal from another crow:

Step 4.1: Crow i does not directly monitor the movements of crow j, the one following it. Instead, crow i locates the food that crow j has hidden and adjusts its position, accordingly, as described in equation (1)

$$x^{t+1} = x_i^t + rand_i * fl_i^t * (m_i^t - q_i^t) \quad (1)$$

Step 4.2: Compute the fitness of crow i using its updated position and adjust its memory accordingly according to the following process.

$$me_i^{t+1} = x_i^{t+1}, f(x_i^{t+1}) \quad (2)$$

Where,

$f(x_i^{t+1})$ - denotes fitness calculation

Step 5: Iterate steps 2-3 for each crow until the termination conditions are met.

4.2. Double Spending attack

An individual seeking to use the same token for multiple transactions can be identified as engaging in a double spending attack [19]. This type of attack is very crucial concern for any distributed ledger technology. Initially the attacker sends an amount of IOTA token to a recipient. At the time of processing, the attacker creates another transaction with the same IOTA token and this time sends them to a different recipient. These two conflicting transactions are not immediately detected by the network nodes and validators. Initially, the first transaction appears to be legitimate and is validated. However, if the attacker dedicates additional time and computational resources, they can attempt to ensure that the second conflicting transaction gets confirmed instead of the first one. By successfully executing this process, the attacker effectively performs a double spend of the same tokens, undermining the integrity and reliability of the IOTA network.

4.3. Avoiding Double Spending attack by CSA

Initially, the CSA algorithm applies local search and global search techniques to identify nodes within the IOTA network. During the searching process, the algorithm consumes IOTA tokens. The IOTA network consists of numerous nodes forming a peer-to-peer network. Information about IOTA tokens is sent to all participating nodes in the network, and each node stores this information. In the event that an attacker creates a new transaction using the same token; the participating nodes in the network should be able to identify this attempt. Consequently, they will reject the fraudulent transaction, preventing it from being confirmed [21].

In the e-voting process, this CSA was implemented. When the initial token is created and added to the network, the voter generates its own token to vote. This token information will be maintained in the distributed ledger. If a voter attempts to create the same token with different identification with same mobile number, the CSA can monitor this activity and share the information with other nodes in the network. As a result, the conflicting token created by the voter cannot be approved by other nodes in the network. This helps in preventing a double spending attack and ensures the integrity and reliability of the e-voting system.

5. Experiment and Result Analysis

During the testing process to achieve optimal results with the CSA, several parameters need to be determined. These parameters include the size of the flock, iterations number, and probability of awareness. In this particular experiment, the flock size is the parameter being tested. In order to assess its impact on the algorithm's

effectiveness, numerous testing scenarios are executed using a spectrum of values starting from 100 and extending up to 500. Each test configuration is run autonomously in 20 iterations to ensure robust statistical significance. The other parameters, namely the number of iterations (500), length of flight (2), and probability of awareness (0.1), are set to constant values throughout the testing process. These constants provide a controlled environment for evaluating the impact of the changing the size of the flock on the mean fitness value. In Figure 5, displays the results of the flock size test. The values shown on the graph represent the mean fitness value obtained from the 20 independent tests for each tested flock size. This graph serves as a visualization of how the mean fitness value varies as the size of the flock is adjusted. By conducting this comprehensive testing process and analyzing the results, researchers can determine the optimal size of the flock to use with the CSA algorithm for the specific problem or optimization task at hand. The insights gained from these experiments will aid in selecting appropriate parameter values to achieve the best performance of the CSA.

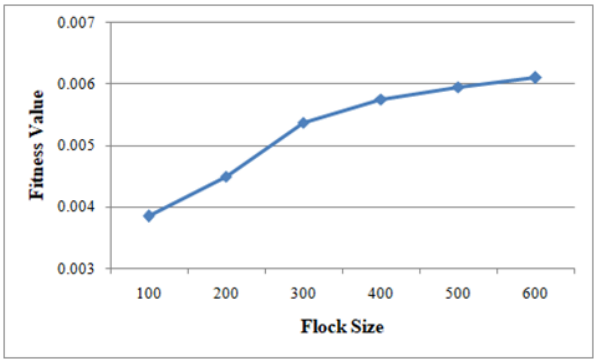

Figure 5. Flock size result

As depicted in Figure 6, it is clear that augmenting the number of iterations leads to higher average fitness values. Larger iterations allow search agents more time to improve the obtained solutions, leading to better results. However, this also implies increased computational time. Notably, the mean fitness value stabilizes when the number of iterations exceeds 250. This suggests that beyond 250 iterations, the fitness values remain nearly constant. As a result, the optimal number of iterations appears to be 250, as increasing it further does not significantly improve the fitness values, while incurring additional computational overhead.

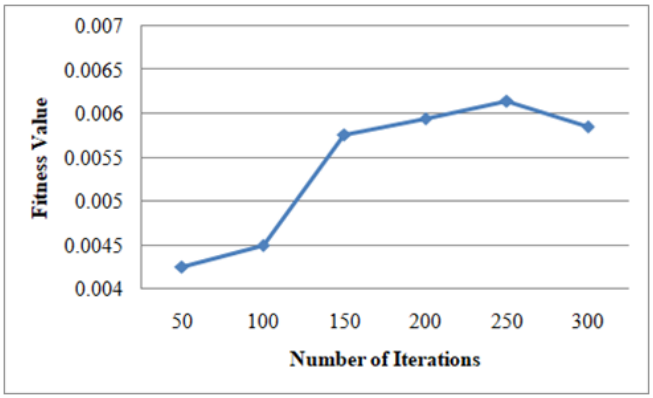

Figure 6. Maximum numbers of iterations testing result

The awareness probability is assessed across various test scenarios, using values ranging from 0.1 to 0.5, and repeating each scenario 20 times for reliable results. The chosen parameters, such as a flock size of 300, 250 iterations, and a flight length of 2.5, are based on previous experiments. A low awareness probability tends to focus the algorithm on local search around the current best solution, while a high awareness probability encourages global exploration. Achieving the right balance between exploration and exploitation is essential for a successful process. Figure 7 demonstrates that an awareness probability of 0.1 results in the highest mean fitness value, indicating its significance as the optimal value for generating quality solutions.

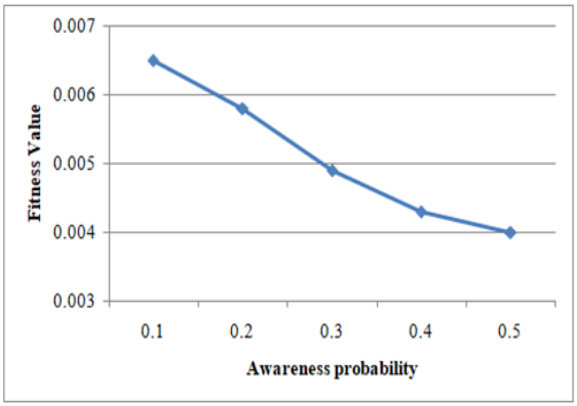

Figure 7. Test result of awareness probability

6. Conclusion and Future Enhancement

The CSA and the IOTA platform were used to make the voting process robust, trustworthy, and resistant to malicious attacks or manipulation. The proposed method effectively addressed the issue of double spending attacks in the e-voting application. To ensure voter authorization, multiple identification methods such as Aadhar card, voter ID, and mobile number were employed. Once the

verification process was completed successfully, the voter was given an IOTA token that was added to the network. The IOTA token had been created only once with all proofs. If a voter attempted to vote again using the same token, the CSA came into play. The CSA algorithm efficiently identified the duplicate token address by comparing it with the addresses of all other nodes that had participated in the IOTA tangle network. This ensured that each voter was issued a distinct and verifiable IOTA token, and any attempt to duplicate or reuse the same token for voting purposes was immediately identified through the built-in proofs and verification mechanisms. As a result, the system maintained a high level of security, ensuring that each voter could only use their assigned token to cast a single vote in the e-voting application.

The proposed method primarily addressed the issues of double-spending attacks within the tangle. However, it is crucial to consider other potential threats, such as the parasite chain attack, where an attacker creates a parallel chain with greater computational power to disrupt the main tangle. Additionally, the splitting attack involves intentionally dividing the network into partitions, isolating nodes and causing conflicts. Furthermore, the Sybil attack poses a risk as it enables an attacker to create multiple fake identities, granting them control over a substantial portion of the network. To ensure the overall security and integrity of the system, it is essential to address and mitigate these various types of attacks.

References

[1] Vladucu MV, Dong Z, Medina J, Rojas-Cessa R. E-Voting Meets Blockchain: A Survey. IEEE Access. 2023;11:23293–308.

[2] Muthulakshmi.S, Kannammal.A. Security Enhancements Based on Optimal Lightweight Blockchain Model for Data Sharing in Wireless IoT Networks. AHSWN.2023;.55: 233-256.

[3] Conti M, Kumar G, Nerurkar P, Saha R, Vigneri L. A survey on security challenges and solutions in the IOTA. Journal of Network and Computer Applications 2022;203:103383.

[4] Chen Y, Tang X, Yao R, Bie R. Security Analysis of A Parasite Chain Attack in IOTA Based on Repeated Game. Procedia Computer Science 2022;202:83–8.

[5] Haseeb K, Almustafa KM, Jan Z, Saba T, Tariq U. Secure and Energy-Aware Heuristic Routing Protocol for Wireless Sensor Network. IEEE Access 2020;8:163962–74.

[6] He J, Peng Z, Zhang L, Zuo L, Cui D, Li Q. Enhanced crow search algorithm with multi-stage search integration for global optimization problems. Soft Computing 2023;27:14877–907.

[7] Han X, Xu Q, Yue L, Dong Y, Xie G, Xu X. An Improved Crow Search Algorithm Based on Spiral Search Mechanism for Solving Numerical and Engineering Optimization Problems. IEEE Access 2020:1–1.

[8] Cullen A, Ferraro P, King C, Shorten R. Distributed Ledger Technology for IoT: Parasite Chain Attacks. IEEE. 2020; 7: 7112-71227112-7122.

[9] Cheng Q, Huang H, Chen M. A Novel Crow Search Algorithm Based on Improved Flower Pollination. Mathematical Problems in Engineering 2021;2021:1–26.

[10] Algamal ZY, Abdallh GY. A QSAR classification model of skin sensitization potential based on improving binary crow search algorithm. Electronic Journal of Applied Statistical Analysis. 2020; 13: 86-95.

[11] Anter AM, Hassenian AE, Oliva D. An improved fast fuzzy c-means using crow search optimization algorithm for crop identification in agricultural. Expert Systems with Applications 2019;118:340–54.

[12] Fred L, Kumar S, Padmanaban P, Gulyas B, Kumar H. A Fuzzy-crow search optimization for medical image segmentation. Applications of Hybrid Metaheuristic Algorithms for Image Processing. Springer. 2020. 890:413-439.

[13] Upadhyay P, Chhabra JK. Kapur's entropy based optimal multilevel image segmentation using Crow Search Algorithm. Applied Soft Computing 2020;97:105522.

[14] Muthulakshmi S, Kannammal A, Padma Priya M, Pramila V, Shobiadevi G. Improvising micro transactions using IOTA tangle on smart refrigerator applications. International Journal of Health Sciences 2022:4955–65.

[15] Chen Y, Guo Y, Wang M, Xu E, Xie H, Bie R. Securing IOTA Blockchain Against Tangle Vulnerability by Using Large Deviation Theory. IEEE Internet of Things Journal 2023;11:1952–65.

[16] Ullah I, de Roode G, Meratnia N, Havinga P. Threat Modeling—How to Visualize Attacks on IOTA? Sensors 2021;21:1834.

[17] Aruchamy P, Gnanaselvi S, Sowndarya D, Naveenkumar P. An artificial intelligence approach for energy-aware intrusion detection and secure routing in internet of things-enabled wireless sensor networks. Concurrency and Computation: Practice and Experience 2023;35.

[18] Vazhuthi PPI, Prasanth A, Manikandan SP, Sowndarya KKD. A hybrid ANFIS reptile optimization algorithm for energy-efficient inter-cluster routing in internet of things-enabled wireless sensor networks. Peer-to-Peer Networking and Applications 2023;16:1049–68.

[19] Askarzadeh A. A novel metaheuristic method for solving constrained engineering optimization problems: Crow search algorithm. Computers & Structures 2016;169:1–12.

[20] Cortés-Caicedo B, Avellaneda-Gómez LS, Montoya OD, Alvarado-Barrios L, Álvarez-Arroyo C. An Improved Crow Search Algorithm Applied to the Phase Swapping Problem in Asymmetric Distribution Systems. Symmetry 2021;13:1329.

[21] Perazzo P, Arena A, Dini G. An Analysis of Routing Attacks against IOTA Cryptocurrency. IEEE International Conference on Blockchain. 2020. 517-524.

[22] Houssein EH, Helmy BE-D, Elngar AA, Abdelminaam DS, Shaban H. An Improved Tunicate Swarm Algorithm for Global Optimization and Image Segmentation. IEEE Access 2021;9:56066–92.