Received: February 16, 2023. Revised: March 16, 2023. 280

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Compound Metric Assisted Trust Aware Routing for Internet of Things through Firefly Algorithm

Mohammad Osman[1]* Kaleem Fatima[2] P. Naveen Kumar[1]

[1]*Department of Electronics and Communication Engineering, Osmania University, Hyderabad, Telangana, India.*
[2]*Muffakham Jah College of Engineering & Technology, Department of Electronics and Communication Engineering, Hyderabad, Telangana, India.*
* Corresponding author's Email: adnan.aspect@gmail.com

Abstract: Security and privacy are the major concerns in the internet of things (IoT) which are uncertain and unpredictable. Trust aware routing is one of the recent and effective strategies which ensure better resilience for IoT nodes from different security threats. Towards such concern, this paper proposes a new strategy called independent onlooker withstanding trust aware routing (IOWTAR) for IoT. IOWTAR introduced a new compound trust metric by combining three individual metrics namely independent trust, onlooker trust, and withstanding trust (a combination of resilient trust and immovability trust). Independent trust and onlooker trust are assessed based on direct and indirect experiences of nodes about their neighbor nodes. Withstanding trust is assessed based on the stability and resilience of nodes towards dynamic topological changes and network failures respectively. Further, this work adapted the Firefly algorithm (FFA) to optimize the weights of individual trusts and establishes a secure path. Simulation experiments carried out over the proposed method had shown its superiority in terms of packet delivery ratio, delay, and throughput. The proposed method has gained an average improvement in the throughput is of 23.71%, 20.18%, 17.27%, and 2.88% from PSO, GSA, WOA, and CBBMOR-TSM-IOT methods respectively.

Keywords: Internet of things, Trust awareness, Independent trust, Onlooker trust, Withstanding trust, Compound metric.

1. Introduction

In the current technology, the Internet has major significance through which the end-to-end devices can communicate in a hassle-free manner. Due to such significance, the internet of things (IoT) has emerged as an interesting paradigm that can connect a billion devices with heterogeneous characteristics. Hence, the IoT has gained widespread applicability in different fields like micro-electromechanical systems (MEMS), smart automation, wireless sensor networks (WSNs), Embedded systems, etc. The basic theme of IoT was established in the 80s, popularized in the 90s, and accelerated in the 20s [1-3]. At present, the IoT is involved in every field and plays a very important role in the lives of human beings, for example in infrastructure management, smart transportation, smart health care systems, home and building automation, and environmental monitoring [4]. From the Federal trade commission (FTC) report, it was reported that the total number of IoT devices are already crossed the total number of working people in their corresponding working stations [5, 6]. It is predicted that the total number of IoT devices will become approximately 29.42 billion by the end of the year 2030. Thus, IoT can be stated as a Global connector that forms a virtual network with non-traditional computing devices. But, connecting such devices through the internet brings so many challenges like security, resource scarcity, mobility, interoperability, scalability, etc.

Among these challenges, security and privacy concerns are deemed as major hurdles facing by IoT. Since the devices connected to IoT are heterogeneous in nature, the potential security risks are totally uncertain and unpredictable in nature. For instance, a

compromised IoT device may influence some other devices in the network to get compromised. Further, depending on the nature of compromising, the compromised nodes may lead to several problems like leaking personal information, misuse of resources and authorized credentials, etc. Hence, to protect the IoT network from all these constraints, there is a need for a complete security provision strategy which is the main motivation of this paper. Over the past few years, several researchers and academicians are seriously developing several secure strategies to ensure a risk-free communication in IoT. trust aware routing (TAR) [7, 8] is one of the current and effective security provision strategies. In TAR, each node assesses the trustworthiness of all of its neighbor nodes and selects the next hop node. In such a process, an objective function is defined through several trust metrics and computes the trust of nodes. The next hop node is selected which has more trustworthiness. However, from past studies, it was found that the metrics used to trust computation are not adequate and also limited in number. The inadequate and limited Metris won't provide resilience against a larger number of attacks.

Hence, this paper proposes a new TAR-assisted routing mechanism that considers multiple and adequate trust metrics. The proposed method considers totally 3 types of trust metrics viz.; Independent trust, onlooker trust, and withstanding trust. Independent trust is assessed based on the direct past experiences between nodes. Onlooker trust is assessed with the help of neighbor nodes and Withstanding trust is assessed based on the Resilience and Immovability of nodes in the network. Finally, a compound routing metric is formulated by integrating these three metrics and the most trustworthy node is selected as a next hop forwarding node.

The remainder of this paper is structured in the following manner; the literature survey details are explored in the 2nd section. The particulars of the proposed TAR based on compound routing metrics are explored in 3rd section. The details of the experimental analysis are explored in the 4th section and the 5th section provides the conclusions.

2. Literature survey

TAR has gained a significant research interest in IoT networks as it helps in the establishment of a stable and secure path for communication between IoT devices. TAR is employed to ensure the security of nodes, especially for a larger node count where the centralized administrator is not capable to handle or when the communicating media among the nodes is navigating network media. compared to traditional cryptography algorithms the TAR is more effective and dynamic in nature. Furthermore, TAR is also capable of continuously monitoring the node's behavior in the network thereby it can assess the trustworthiness and can determine the trustworthy nodes to collaborate with. Different TAR methods have been developed earlier to provide trustworthy communication between nodes of IoT networks.

D. Chen et al. [9] propose a "trust and reputation model (TRM)" by considering the packet forwarding ratio, energy consumed, and PDR for trust assessment. Further, they employed fuzzy set theory to accomplish the TRM model. As there exist only few trustworthy nodes in IoT network, considering them for every time data transmission results in a quick depletion that effect on the lifetime of network.

P. K. Reddy, R. S. Babu [10] proposed an "optimal Secure and Energy Aware Protocol (OSEAP)". Initially, they clustered the entire network with Fuzzy C-Means algorithm and then adapted for cluster head selection through an "Improved bacterial foraging optimization (IBFO) [14]" algorithm. IBFO is also applied for the selection of optimal keys in their method under group key distribution. But, FCM is not an appropriate method for clustering because in FCM, IoT devices are grouped with the help of the impact but in the original, the IoT nodes have to get grouped based on distance from other IoT nodes in the network. Moreover, the IBFO consequences to huge computational complexity in the process of route discovery if a sender node has information to send.

Focusing on the detection of DoS attack in the "message queuing telemetry transport (MQTT)" [11], A. P. Haripriya and K. Kulothungan [12] developed an IDS model based on fuzzy logic and it is named as Secure-MQTT. Unlike the conventional dense rule of fuzzy logic, this approach accomplished a lightweight fuzzy logic that generates the rules dynamically.

P. Muthukannanand and R. Thirukkumaran [13] proposed a "trust aware access control system using fuzzy logic (TAACS-FL)" for IoT networks. Here, first, the trust evaluation is done based on three metrics such as "successful forward ratio (SFR)", "data integrity (DI)" and "energy consumption rate (ECR)". Next, the overall trust is measured with the help of "fuzzy engine trust (FET)" and depending on the measured values, the access control is designated. S. Gali, and V. Nidumolu [15] adapted multi-context trust aware routing for IoT networks (MCTAR-IOT) by considering three metrics such as communication trust, energy trust, and hop count. For long-distance secure path selection mostly they concentrated on

hop-count metric but weight optimization is not done. As a a next contribution, the same authors such as Sowmya and venkatram [16] proposed a new optimization algorithm based routing in IoT and named it as chaotic Bumble bees mating optimization routing based trust sense model (CBBMOR-TSM) for IoT networks. Direct and indirect trusts are used to measure total trust. Different Metaheuristic algorithms are applied for the optimization of weights of corresponding trust and declared that heuristic Bumble bee mating optimization (HBBMO) [17] has shown the best performance. As the number of nodes increases the number of malicious nodes also increases due to poor trust evaluation.

Mabodi, K., et al. [18] aimed at the identification of grayhole attacks in which the compromised nodes make the packets not to reach the destination node. They used the traditional "Adhoc On-demand distance vector (AODV)" protocol and employed it under "multi-level trust intelligent secure system (MTISS)". This approach employed the cryptographic authentication mechanism under four phases such as trust verification of a node, routes testing, discovery of gray hole attacks, and elimination of malicious attacks. However, the proposed method consumes more energy when the number of nodes increases and it impacts the trust verification of a node.

N. Djedjig, et al. [19] applied game theory concept to model the metric based RPL trustworthiness scheme for the provision of security in a Resource-constrained RPL IoT network. Wang et al. [20] proposed an intelligent trust evaluation mechanism for Mobile edge computing devices in Industrial IoT. The trust assessment is carried out based on the data gathered by sensor nodes and the communication scenario that happened between them. S. M. Muzammal et al. [21] proposed SMTrust, a mobility based secure routing protocol which majorly considered the mobility of nodes in the trust assessment. SMTrust is mainly aimed at the detection of RPL Rank and Blackhole Attacks in both static and mobile environments. They have not considered the interaction between the nodes while measuring trust.

Ragesh and Kumar [22] aimed at the detection of signal processing attacks in IoT and proposed a trust based secure routing mechanism to identify them. They determined a secure path based on a technique developed by combining "fuzzy and particle swarm optimization (F-PSO)". Then "learning with errors over rings (R-LWE)" algorithm is employed to encrypt the data. Trustworthiness is measured only based on the trust value. Considering energy and security as prime aspects, S. M. Mujeeb et al. [23] proposed an "energy harvesting trust aware routing algorithm (EHTARA)". For the determination of the best path, a cost metric is introduced by combining trust, distance, and energy. Further, they proposed the big data classification at the destination through exponential bat algorithm [24] based deep belief networks (DBN) [25]. Non-uniform weights are considered to measure the cost metric to determine the best path.

Shalini Subramani, M. Selvi [26] proposed "intelligent intrusion detection system for detecting intruders in IoT based wireless sensor networks". For this purpose, they proposed rule and multi-objective PSO based feature selection algorithm. Rajesh Kumar Dhanaraj et al. [27] proposed "simulated annealing black-hole attack detection (SABD) based enhanced gravitational search algorithm (EGSA)" to enhance the security of packet delivery in WSNs. They concentrated on the detection of block-hole (BH) attacks by clustering the entire network into few clusters which have similar residual energy. Initially, BH nodes are identified and EGSA-SABD is applied to quarantine the attacked nodes. The proposed method's attack detection accuracy rate is decreased when the number of BH nodes increases.

Regonda Nagaraju et al. [28] proposed an attack prevention and detection system for IoT networks. They developed cybersecurity warning system for both regular and abnormal congestion in the network. Further, grey wolf optimization and whale optimization algorithms are used to detect the attack prevention system. The loss and delay incurred in this system are more.

3. Proposed method

3.1 Overview

Here in the current s section, we explore the complete details of proposed trust aware routing mechanism. The proposed mechanism established a secure route between IoT nodes through a compound metric that consists of three individual trusts. They are namely independent trust, onlooker trust ad withstanding trust. Since the proposed method adapted multi-hop routing, each node checks the trustworthiness of its neighbor nodes and chooses one node as a final node that has more trustworthiness. In the compound trust metrics, depending on the scenario, the weights are adjusted for three trust metrics and based on the values, the node selection is done. The complete details of the proposed mechanism are explored here;

3.2 Network model

The network model consists of *N* number of IoT nodes and one sink node. The nodes are deployed randomly in the network of size *MXN*, where *M* denotes the network's length and *N* denotes network's width. All nodes are assumed as static nodes and they are location-aware nodes. Further, assumed the characteristics such as energy status, and trust values of all nodes are similar in nature. The energy of sink node is considered as infinite and the energy mode of each node is dynamically adjusted according to the distance. Each node collects past data such as working history, opinions of other nodes, and earlier decisions from its neighbor nodes. Moreover, nodes are able to serve as intermediate forwarders for more than one route. Further, the range of communication of each node is anticipated as constant and let it is denoted with *R*. Each node collects the opinions of other nodes and prepares trust list. The trust list consists of three trust-related factors such as independent trust (IT), onlooker trust (OT), and withstanding trust (WT).

3.3 Independent trust

Independent trust (IT) is measured based on previous interactions, observations, and experiences. IT is the trust of a node regarding another node and it can be evaluated by considering direct and past experiences [29]. Initially, all nodes in the network interact with each other and after that, each node gathers opinions from its neighbor nodes. Like this, the Independent trust is evaluated by gathering past or earlier opinions obtained based on the communication interactions that happened. IT is assessed only upon the occurrence of at least one communication interaction between nodes.

Independent trust is very close to the behavior of human beings. In this regard, a person can acquire the opinion of another person if he/she has at least one interaction in the past with another person. However, there would be a problem if there is not at least one previous interaction. At this instance, Independent trust is evaluated by accumulating the opinions of nodes that are in resemble with the target node. Consider an instance in which the source node wants to assess the trustworthiness of a stranger node that doesn't have any past communication history with the source node. At this case, the source node asks for the opinions of neighbor nodes those are following the resemblance characteristics of the stranger node. In such a way, the source node can create an initial level of trust about stranger node and if it is within the limit, then the source node starts communicating with the corresponding stranger node.

Consider two nodes n_i and n_j in the network which are directly connected and the node n_j interacted *S* times in the past with node n_i. In each interaction, the node n_i creates an opinion about the node n_j based on the direct communication between them. Let that opinion is $O_s(n_j)$ and the range of $O_s(n_j)$ is in between 0 and 1 i.e. $O_s(n_j) \in [0,1]$. Further, assume that the node n_i collects *T* number of malicious opinions about the node n_j. Assume there exists L number of nodes that have resemblance features with node n_j and they have past communication experience with node n_j. In this case, they use previously collected opinions to know the behavior of node n_j. These *L* number of opinions are taken into account to assess the initial trust of node n_j by node n_i. Let the opinion of node n_l about the behaviour of node n_j is denoted as $O_l(n_j) \forall l \in L$. Therefore, Independent trust is measured as

$$I_T(n_i, n_j) = \begin{cases} x \times \frac{\sum_{l=1}^{L} O_l(n_j)}{L}, & if\ S = 0 \\ y \times \frac{\sum_{s=1}^{S} O_s(n_j)}{S}, & if\ S \neq 0 \end{cases} \quad (1)$$

Where, $I_T(n_i, n_j)$ represents the Independent trust between the nodes n_i and n_j, $O_l(n_j)$ represents the opinion of node n_l about the behaviour of n_j, $O_s(n_j)$ represents the opinion of node n_i about the behaviour of n_j at s^{th} interaction, x represents influence factor, and y represents the monitoring factor.

From Eq.(1), it can be seen that the IT is assessed under two modes, they are; non-interactive mode ($S \neq 0$) and interactive mode ($S = 0$). In the former mode, the $S \neq 0$ indicates there is no past communication history between nodes and in such case, the IT is an accumulated value of opinions of resemblance nodes of target node n_j. Next, the Second condition comes into existence once direct communication is established between n_i and n_j. At s^{th} communication interaction, the IT is assessed based on the opinions noticed at 1 to *S-1* interactions. Among S number of opinions, few opinions are considered as malicious opinions where node n_i may give malicious opinions about node n_j. Hence, we need to monitor the maliciousness behaviour by considering the monitoring factor y and it is obtained as

$$y = \left(\frac{S-T}{S}\right)^{\left(\frac{1}{S-T}\right)} \quad (2)$$

Where, S & T indicates the count of total opinions and malicious opinions respectively. The monitoring factor monitors the malicious behavior during the communication process between nodes. IT values diminishes when the malicious opinions count is more. It replicates human behavior i.e. the continuous interaction between human beings improves the strength of the relationship. But if any interaction went wrong then the strength of the relationship reduces.

3.4 Onlooker trust (OT)

OT is obtained with the help of observations and previous experiences of neighbour nodes. In this trust, the node can take the opinions of its neighbour nodes when there is no direct connection between the source and next-hop node. Generally, in IoT, the nodes are not directly connected. At this instance, the source node takes the critical reviews of other nodes for next-hop trustable node selection. Like this, the next-hop node selection is done by taking the opinions of third-party nodes such as trustworthy neighbour nodes when the source and next-hop nodes are not directly connected. In addition to this, the Onlooker trust is measured based on the level of connectivity between them. The level of connectivity between the source node and its most trustable next-hop node as well as next-hop node to the destination node shows the strength of the relationship. Therefore, the trust threshold is considered for the selection of most trustable neighbour nodes.

Let's consider two nodes n_i and n_j, which are not directly connected each other and consider k^{th} neighbour node of node n_i is n_i^k, where n_i^k maintains the direct connection between the nodes n_i and n_j. The node n_i^k collects the individual opinions about the node n_j and let $O\left(n_i^k, n_j\right)$ be the opinion of the node n_i^k about the node n_j and $O\left(n_i, n_i^k\right)$ be the opinion of the node n_i about n_i^k. Hence, the Onlooker trust is measured as,

$$O_T\left(n_i, n_j\right) = \frac{\sum_{k=1}^{K}\left(O\left(n_i, n_i^k\right) \times O\left(n_i^k, n_j\right)\right)}{\sum_{k=1}^{K} O\left(n_i, n_i^k\right)} \quad (3)$$

s.t.

$$O\left(n_i, n_i^k\right) \geq O_T^T \quad (4)$$

Where, $O_T\left(n_i, n_j\right)$ is the OT between the nodes n_i and n_j, O_T^T is the threshold of Onlooker trust. Eq. (4) determines the trustworthy node from the set of neighbour nodes based on O_T^T. If the opinion between the nodes n_i and n_i^k is greater than the trust threshold value then the corresponding node is selected as most trustworthy next-hop neighbour node. Further, Eq. (3) is used to measure the O_T^T trust, initially using Eq. (4) the next-hop trustable neighbour node is selected and then all the opinions are cumulated based on weighted average technique. The onlooker trust has less computational complexity and low risk due to the selection of most trustable next-hop neighbour node. Figure.1 shows an example demonstration of the evaluation of Onlooker trust.

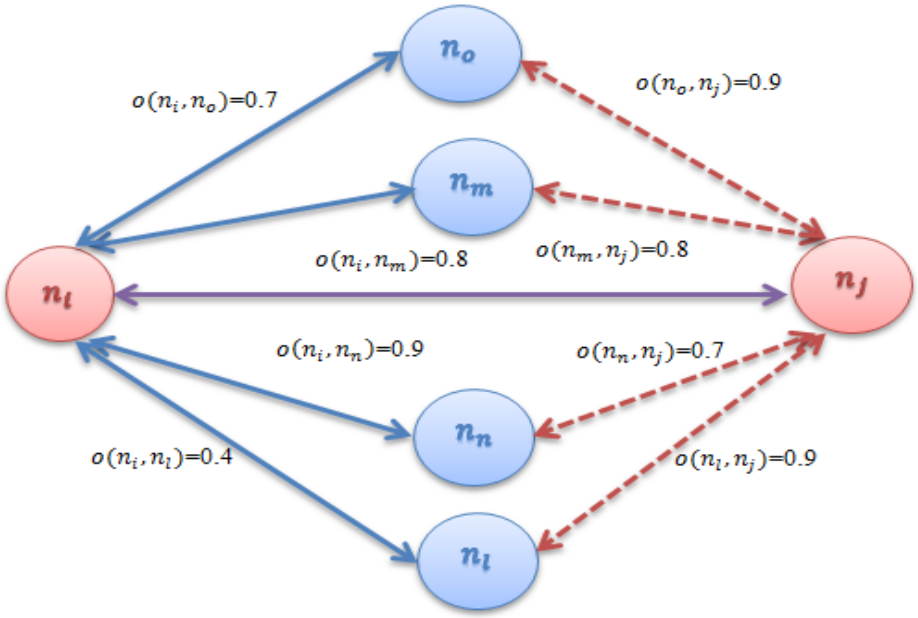
3.5 Withstanding trust (WT)

Withstanding trust is obtained based on the withstanding capacity of an IoT node and it signifies the withstanding capability of a node to the external failures in network. Two sub-trusts are considered to evaluate the Withstanding trust; they are Resilient Trust and Immovability Trust. Resilient trust is measured by observing the node failures due to some technical causes and Immovability trust is measured based on the mobility of nodes in the network. The following subsection explores the details of two sub-trusts.

3.5.1. Resilient trust

The nodes in the IoT networks are smaller sized devices that are extremely sensitive to operational settings including electrical surges, breakages, and damages etc. The nodes cannot perform well when there is any node breakage and it disturbs the basic operations of the sensor device such as sense, process, and communication. Even if all these sensor nodes are quickly recovered, they could not function effectively as before the breakdown. Moreover, the tiny devices recovery time is very small due to its less complex circuitry. Furthermore, there is an alternate solution to recover the node from damages is to replace the damaged circuit. But even though the damaged circuit is replaced, few nodes may not resume to its normal operation. A node which faces frequent damages can reduce the reliability. Therefore, the resilient trust is evaluated by taking these considerations into account.

For this purpose, we considered three rates; they are success rate, failure rate, and healing rate. The success rate is defined as the ratio of all the successfully completed occurrences by the target node to the all occurrences which are given by source node. If the target node remains active for a given task until it is completed, then the task is treated as success and success rate is obtained by such tasks accumulation. As success rate is high then the



$$O_T(n_i, n_j) = \frac{(0.7 \times 0.9) + (0.8 \times 0.8) + (0.9 \times 0.7)}{(0.7 + 0.8 + 0.9)} = 0.7916$$

Figure. 1 Onlooker trust computation

resilient trust is also high. Further, the failure rate counts the total failed occurrences from the total occurrences. Finally, healing rate counts the total number of occurrences which are recovered from the damages. A node which maintains high success rate and healing rate, low failure rate is considered as more resilient node and that type of nodes are preferably chosen for communication. Resilient trust is measured based on the past experiences which are taken from the list of interactions where the heavy data is not communicated. For two nodes n_i and n_j, let the success rate is denoted as $R_s(n_j)$, the failure rate is denoted as $R_f(n_j)$ and healing rate is denoted as $R_h(n_j)$. Therefore, the robust trust is measured as

$$R_T(n_i, n_j) = \left(R_s(n_j)\right)^{\left(1-R_f(n_j)\right)} \times \left(R_h(n_j)\right)^{R_f(n_j)} \quad (5)$$

Where, $R_T(n_i, n_j)$ is the resilient trust between the nodes n_i and n_j and it ranges from 0 to 1, where 0 indicates the node n_j have less resilience, and 1 indicates high resilience. The resilient trust is measured using Eq. (5) and it selects one node as a final node among all nodes which has larger resilient trust.

3.5.2. Immovability Trust

Dynamic changes in the network topology consequences to dynamic node movements i.e. the nodes may join or leave the network dynamically. Dynamic changes in the network topology are due to several reasons, for example deployment of additional nodes, energy depletion, minor movements due to external causes, resource constraints etc. These variations affect the behavior of nodes in the network. Therefore, we have taken all these considerations into account to analyze the node's immovability. A larger immovable node can achieve better trust because it improves the network lifetime. Here, we considered the life cycle of a node because it provides the information regarding leaving and joining times of a node. The complete life cycle of a node is modeled based on 2 time instances, they are; operating and surviving times. Surviving time is the time interval where the node can stay at the same position (neither joining nor leaving) or for its entire life cycle. Next, the operating time is the time interval where the node presents in the operating state. In the operating state, each sensor node can sense, process, and communicate. In general, higher operating time indicates less immovability of a node. Therefore, the immovability trust is defined as the fraction of operating time to the surviving time. Let's assume n_i

and n_j, operating time is T_o and surviving time is T_s. $|T_o|$ and $|T_s|$ are operating and surviving time intervals of node n_j. Next, consider node n_j was communicated S times with node n_j, the immovability trust is evaluated as,

$$M_T(n_i, n_j) = \begin{cases} \frac{|T_o|}{|T_s|}, \ if\ S = 0 \\ \gamma \times \frac{|T_o|}{|T_s|}, \ if\ S \neq 0 \end{cases} \quad (6)$$

Where, $M_T(n_i, n_j)$ is the Immovability trust between the nodes n_i and n_j, γ is the penalizing parameter and it is measured based on the number of interactions happened between the nodes n_i and n_j. γ is derived mathematically as,

$$\gamma = \delta^{\left(1-\frac{1}{S+1}\right)} \quad (7)$$

Where, δ is an arbitrary constant and $\delta \in [0, 1]$, and S is the total interactions happened between the two nodes n_i and n_j. The parameter γ become high when there are frequent departures of a node from the network. For a node, the frequent leavings from the network make it unreliable and consequences to less immovability trust. Hence, it is not considered to forward the data. Further, the computational complexity of immovability trust is not considerable because the length of the time intervals is recorded by the nodes.

Based on the Resilient and Immovability trusts, the final Withstanding trust is evaluated as follows;

$$W_T(n_i, n_j) = \frac{1}{2} \times \left[w_1 \times R_T(n_i, n_j) + w_2 \times M_T(n_i, n_j)\right] \quad (8)$$

Where, $W_T(n_i, n_j)$ is the proportional trust between the nodes n_i and n_j, w_1 is the weight of resilient trust, and w_2 is the weight of immovability trust. The withstanding trust is an average of resilient trust and immovability trust and the source nodes selects one node as a next-hop trustable node which has highest withstanding trust among the available neighbour nodes.

3.6 Compound trust and optimization

Independent trust ($I_T(n_i, n_j)$), Onlooker trust ($O_T(n_i, n_j)$), and Withstanding trust ($W_T(n_i, n_j)$) are integrated to formulate the compound trust. The compound trust mathematically expressed as

$$C_T(n_i, n_j) = \frac{1}{3}\left[(w_1 \times I_T(n_i, n_j)) + \left(w_2 \times O_T(n_i, n_j)\right) + (w_3 \times W_T(n_i, n_j))\right] \quad (9)$$

Where, $C_T(n_i, n_j)$ is the compound trust w_1, w_2, and w_3 are the weights corresponding to Independent, Onlooker and Withstanding trusts respectively. The values for the weights w_1, w_2, and w_3 are adjusted in such a way that $w_1 + w_2 + w_3 = 1$. Here, we assumed equal values for three weights to maintain equal importance for every trust. Here the weights are optimized through Firefly Algorithm [30]. Since the manual optimization of weights constitutes huge computational time, we adapted for a simple and efficient nature inspired algorithm called as Firefly algorithm.

Consider a route between the source (S_n) and destination (D_n) with intermediate nodes are $n_1, n_2, \ldots\ldots, n_z$. Therefore, the overall trust of a route is evaluated as

$$O_{RT}(S_n, D_n) = \frac{1}{route\ length}\left[C_T(S_n, n_1) + \sum_{z=1}^{Z}\left(C_T(n_{z-1}, n_z)\right) + C_T(n_z, D_n)\right] \quad (10)$$

4. Experimental analysis

Here, we explore the complete details of simulation experiments carried out over the developed method. For simulation purpose, we referred MATLAB tool and the network creation is done in a random fashion. Once the network s created with random locations of nodes, they are assigned to specific characteristics like energy, range of transmission, data transmission rate etc. A first, we explain the particulars of simulation setup and then the particulars of performance metrics. Further, we incorporate the comparative analysis between proposed and existing methods.

4.1 Simulation setup

For experimental validation of our method, we used MATLAB tool and created a Random network with several nodes distributed in an area of 1000×1000. All the nodes are assumed to be stationary and immovable. For each node, the range of communication is fixed and it is determined based on the network area. To realize the randomization concept, the positions of nodes are changed in every simulation randomly. Moreover, the selection of source and destination node pairs is also chosen randomly. Since the proposed approach majorly

Table. 1 Simulation parameters

Parameter	Value
Node count	30-50
Area of network	1000×1000
Data Transmission Rate	20 Packets per sec
Packet Size	512 Bytes
Range of communication of each node	10% of Network area
Deployment of Nodes	Random
Malicious nature	5-25% of total nodes
Trust Threshold	0.6
Weights range	[0, 1]
Number of Interactions (P)	100-1000

dependent on the communication interactions incurred between nodes, we varied it from 100-1000 to analyze their impact. Next, the malicious concept is realized by introducing the abnormal behavior at some nodes and applied the proposed method to identify them. Here, the malicious node count is varied with total nodes present in the network. For instance, if the network is assumed to have 200 nodes and malicious nodes are 20%, then the malicious node count is 40. In such way, the malicious nodes are varied as 5%, 10%, 15%, 20% and 25%. The detailed configuration of simulation parameters are shown in Table.1.

4.2 Performance Metrics

Packet Delivery Ratio (PDR): It is defined as the ratio of total number of packets received a destination node and total numbers of packets sent by source node. Consider $P_r(s,d)$ be the total number of packets received at destination and $P_t(s,d)$ be the total number of packets transmitted by source nodes, the PDR is measured as

$$PDR = \frac{P_r(s,d)}{P_t(s,d)} \tag{11}$$

The expression in Eq.(1) is determined only for on source and destination node however, in our final results analysis, we consider multiple source and destination node pairs. The larger value of PDR signifies better performance and vice versa.

Packet Loss Ratio (PLR): It is defined as the ratio of total number of packets lost during transmission from source node to destination node and total numbers of packets sent by source node. Consider $P_l(s,d)$ be the total number of packets lost and $P_t(s,d)$ be the total number of packets transmitted by source nodes, the PLR is measured as

$$PLR = \frac{P_l(s,d)}{P_t(s,d)} \tag{12}$$

The smaller value of PLR signifies better performance and vice versa.

Throughput: It is defined as the ratio of total number of packets received at the destination node and the total time taken to receive. Through signifies the quality of data after receiving at destination. The lesser value of throughout signifies that all the packets are not received within the stipulated time. Mathematically, the throughput is measure as

$$Throughput = \frac{\text{Total Number of packets received (in Kilobits)}}{\text{Time ellapsed (in Sec)}} \tag{13}$$

End-to-End Delay: It is defined as the time elapsed to transmit the complete packets by source node to destination node. Higher delay indicates worst performance and lower delay indicates best performance. The delay is related to throughput, follows an inverse relation.

4.3 Results

At the simulation time, the total number of interactions is varied from 100-1000 and the malicious node cunt is varied in terms of percentage of total nodes present in the network. At each simulation, we have considered different source and destination nodes and after receiving the data at destination node, we measured the performance through different metrics. Further, to check the efficiency of proposed approach, we compared it with several existing methods such as TRM-IOT [9], OSEAP-IOT [10], MCTAR-IOT [15] and CBBMOR-TSM-IOT [16]. The observations are shown in the following figures.

Fig. 2 shows the average trust value (AV) of different types of nodes in the network, they are malicious nodes and trustworthy or normal nodes. The ATV of malicious nodes is noticed in the range of 0.4 to 0.5 while the ATV of normal nodes is noticed as 0.75 to 0.8. As there is much difference between the trust values of normal and malicious nodes, the detection becomes efficient. Since there exists three types of trust metrics, the average trust value is varies in a range but not fixed to a static value.

Fig. 3 demonstrates the performance effectives of proposed mechanism in terms of PDR at different malicious node count. As the number of malicious nodes increases in the network, they won't cooperate to other nodes to forward the data. In such case, the packets won't get forwarded and the results PDR

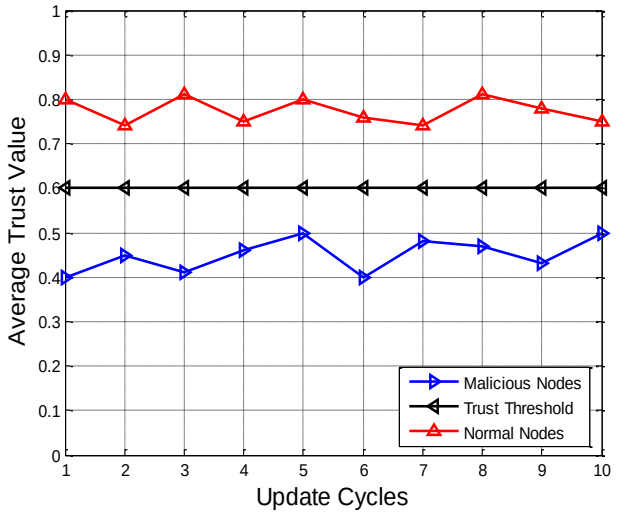


Figure. 2 Average trust value for different types of nodes

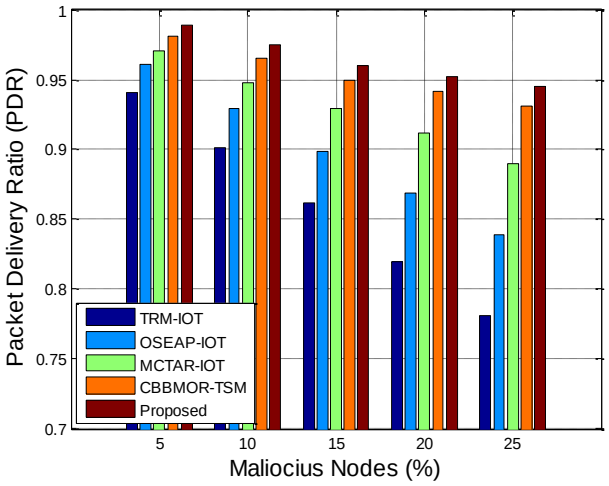


Figure. 3 Packet delivery ratio at different malicious node count

become less. This illusion can be observed at the 25% malicious node count where the proposed approach has obtained only 93.50% PDR. Even though it is less, compared with several existing methods, it is high because the proposed trust sensing method referred three trust metrics which has different contexts. As the number of reference metrics increases, the nodes will gain more knowledge and can easily identify the malicious nodes. Especially, the proposed method evaluated the trust in direct and indirect fashions which can assist the node in an appropriate selection of trustworthy nodes. Since the earlier methods would not concentrate on such kind of trust assessment, they gained less PDR. Moreover, they have not concentrated on multi attribute based trust sensing in IoT. For example CBBMOR-TSM has considered only direct and indirect trusts and MCTAR-IOT didn't consider the withstanding trusts

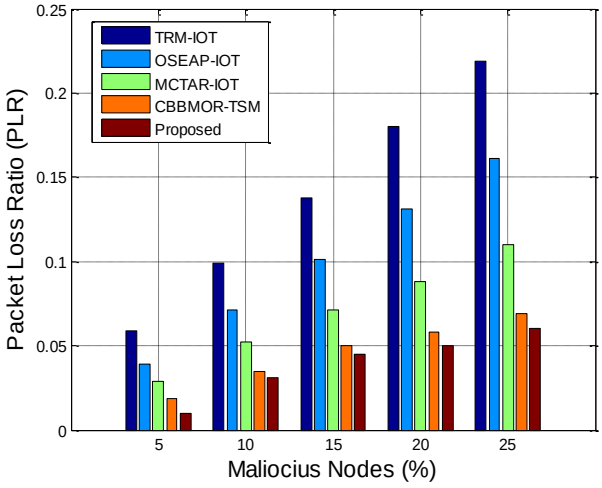


Figure.4 Packet loss ratio at different malicious node count

which are very important in the analysis of node's forwarding capacity. Approximately, the proposed method gained an average PDR of 0.9686 while the existing methods have gained 0.9436, 0.9200, 0.8990 and 0.8772 by CBBMOR-TSM, MCTAR-IOT, OSEAP-IOT and TRM-IOT respectively. Next, the PLR has an inverse relation with PDR, as the number of packets lost is more; the number of packets delivered is less. The loss of packets is more for a larger number of malicious nodes count, as shown in Fig. 4. As the proposed method has higher PDR, the PLR is less and it is approximately observed as 0.0312. For existing methods, the average PLR is observed as 0.0576, 0.0810, 0.1014 and 0.238 for CBBMOR-TSM, MCTAR-IOT, OSEAP-IOT and TRM-IOT respectively.

As the malicious node count increases in the network, the End-to-End delay increases. Because, the compromised nodes won't notify to their preceding nodes about their packet forwarding behavior. In such case, the pre-hop node waits until the TTL time and sends the same packet again. This process induces an additional delay and it becomes more for a larger malicious node count. The End-to-End delay behavior of proposed approach and existing methods for varying malicious node count is shown in Fig. 5. From the results, we can understand that the proposed approach obtained less delay because its process of trustworthiness evaluation is effective than the existing methods.

The past methods' didn't provide a quick alternative node in the case of node and route failures. Hence, they experienced more delay. Especially no method has focused on the Withstanding trust which is very important because it assures a stable and fault tolerant node. Based on the results, the average End-

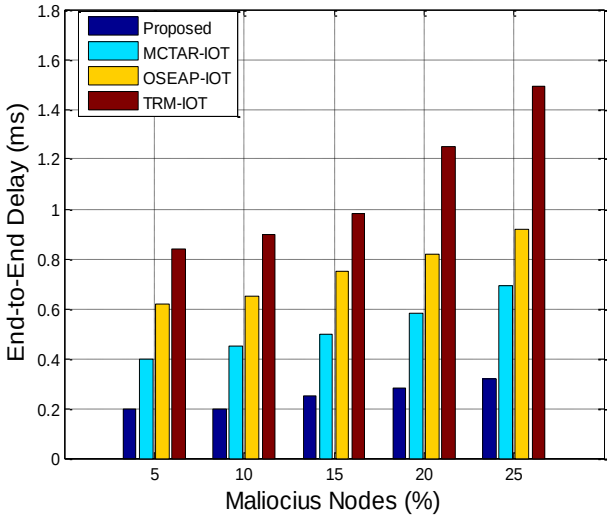


Figure. 5 End-to-End delay (ms) at different malicious node count

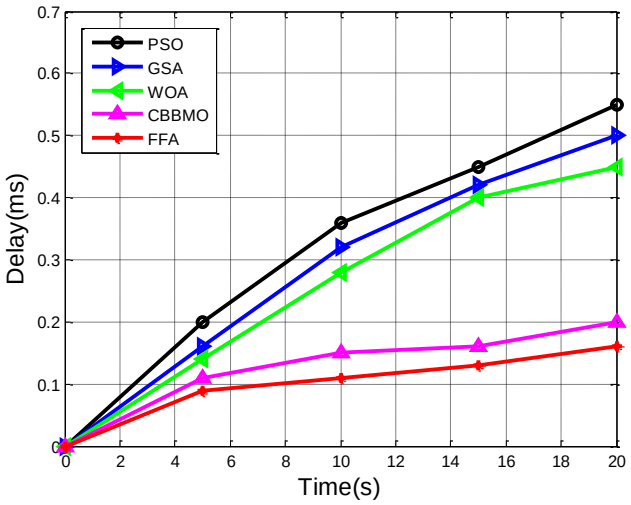


Figure. 6 Delay (ms) comparison between different Metaheuristic algorithms

to-End delay gained by proposed method is observed as 0.2500 ms while the existing methods has gained 0.5240 ms, 0.7520 ms and 1.0920 ms by MCTAR-IOT, OSEAP-IOT and TRM-IOT respectively.

Metaheuristic algorithms have significant role in the process of optimization of weights associated with different parameters. Even though a vast research has been carried out over metaheuristic algorithms for optimization of network related parameters, they were not concentrated on the proper selection.

Some authors employed computationally complex algorithms and some applied simple algorithms. In such situation, the selection of Metaheuristic algorithm becomes complex. Hence, we conduct a simulation study through different Metaheuristic algorithms including “particle swarm

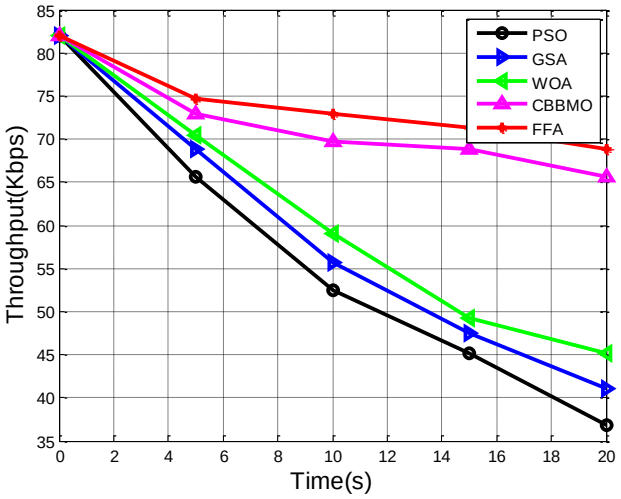


Figure. 7 Throughput (kbps) comparison between different Metaheuristic algorithms

optimization (PSO)” [26], “gravitational search optimization (GSA)” [27], “whale optimization algorithm (WOA)” [28], “chaotic bumble bee mating optimization (CBBMO)” [16] and “firefly algorithm (FFA)”. Among these algorithms, we found the better performance at FFA which ensured a less delay than the remaining algorithms. The delay and throughput analysis of different metaheuristic algorithms is shown in Fig. 6 and Fig. 7 respectively. From the results, the FFA is observed to have less delay and high throughput. Since the delay has an inverse relation with throughput, we analyzed these two performance metrics. With simple calculations, the FFA algorithm provided optimal weights for the three trust metrics and helped in the trustworthy node selection. This kind of selection lessens the delay and increases the throughput. In the case of PSO, GSA, GWO and CBBMO, the optimization process takes more time thereby induces an additional delay which indirectly shows impact n delay and throughout. On an average, the delay incurred due to FFA is observed as 0.0980 ms, while PSO, GSA, WOA and CBBMOR-TSM-IOT has induced a delay of 0.3120ms, 0.2800ms, 0.2540ms and 0.1240ms respectively. Similarly, on an average, the through gained due to FFA is observed as 73.9480 Kbps, while PSO, GSA, WOA and CBBMOR-TSM-IOT has induced a delay of 56.4160 Kbps, 59.0240 Kbps, 61.1720 Kbps and 71.8160 Kbps respectively.

5. Conclusion

In this paper, we aimed at an establishment of secure and efficient path and proposed a new TAR mechanism based on three different trust attributes namely independent trust, onlooker trust, and withstanding trust. The independent trust is a result of direct experience of a node with its neighbour

nodes. Next, the onlooker trust is an indirect trust which considers the opinions of common neighbour nodes. Finally, Withstanding trust ensures the node's resilience and stability. The resilience trust explores the fault tolerance of a node for different failures and damages those generally occur in network. The larger immovability ensures that the node is more stable which indirectly signifies that the node stays for more time. The consideration of these many trust metrics provides secure and efficient communication between nodes in IoT and helps in the determination of the most reliable path for every node. Finally, simulation experiments conducted over the IOWTAR-IOT explore the superiority in terms of Delay, Packet Delivery, and Throughput.

Conflicts of interest

The authors declare that there is no conflict of interest.

Author contributions

Mohammad Osman (Author 1) contributed towards the conceptualization, methodology design and experimental investigation. Kaleem Fatima (Author 2) Contributed towards Validation and Verification. P. Naveen Kumar (Author 3) Contributed towards proof reading and corrections.

References

[1] K. Ashton, "That Internet of Things", *RFID Journal*, Vol.22, No.6, pp. 97-114, 2009.

[2] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A Survey", *Computer Networks*, Vol. 54, No. 15, pp. 2787-2805, 2010.

[3] D. Giusto, A. Lera, G. Morabito, and L. Atzori, "The Internet of Things: 20th Tyrrhenian Workshop on Digital Communications", *eBook*, Springer, New York City, NY, USA, 2010.

[4] Y. Kawamoto, H. Nishiyama, M. Fadlullah and N. Kato, "Effective Data Collection Via Satellite- Routed Sensor System (SRSS) to Realize Global- Scaled Internet of Things", *IEEE Sensors Journal*, Vol. 13, No. 10, pp. 3645-3654, 2013.

[5] D. Miorandi, S. Sicari, F. D. Pellegrini, and I. Chlamtac, "Internet of things: vision, applications and research challenges", *AdHoc Networks*, Vol. 10, No. 7, pp. 1497–1516, 2012.

[6] R. Roman, P. Najera, and J. Lopez, "Securing the internet of things", *Computer*, Vol. 44, No. 9, pp. 51–58, 2011.

[7] Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on trust management for Internet of Things", *Journal of Network and Computer Applications*, Vol. 42, No. 6, pp. 120-134, 2014.

[8] S. Sankar, S. Ramasubbareddy, R. L. Kumar, and M. A. Jayanthi, "Trust-Aware Routing Framework for Internet of Things", *International Journal of Knowledge and Systems Science*, Vol. 12, No. 1, pp. 48-59, 2021.

[9] D. Chen, G. Chang, D. Sun, J. Li, J. Jia, and X. Wang, "TRM-IoT: A trust management model based on fuzzy reputation for internet of things", *Computer Science and Information Systems*, Vol. 8, No. 4, pp. 1207-1228, 2011.

[10] P. K. Reddy and R. S. Babu, "An Evolutionary Secure Energy Efficient Routing Protocol in Internet of Things", *International Journal of Intelligent Engineering and Systems*, Vol. 10, No. 3, pp. 337-346, 2017.

[11] R. A. Light, "Mosquitto: server and client implementation of the MQTT protocol", *J. Open Source Softw*, Vol. 2, No. 13, pp. 265-266, 2017.

[12] A. P. Haripriya and K. Kulothunga, "Secure-MQTT: an efficient fuzzy logic-based approach to detect DoS attack in MQTT protocol for internet of things", *EURASIP Journal on Wireless Communications and Networking*, Vol. 90, pp. 1-15, 2019.

[13] R. Thirukkumaran and P. Muthukannan, "TAACS-FL: trust aware access control system using fuzzy logic for internet of things", *International Journal of Internet Technology and Secured Transactions*, Vol. 9, No. 1/2, pp. 201-220, 2019.

[14] B. Niu, J. Liu, Y. Bi, T. Xie, and L. Tan, "Improved Bacterial Foraging Optimization Algorithm with Information Communication Mechanism", In: *Proc. of 10th International Conf. on Computational Intelligence and Security*, Kunming, China, pp. 47-51, 2014.

[15] G. Sowmya and N. Venkatram, "Multi-context trust aware routing for internet of things", *Int. J. Intell. Eng. Syst.*, Vol. 12, No. 1, pp. 189–200, 2018.

[16] G. Sowmya and N. Venkatram, "An intelligent trust sensing scheme with Metaheuristic based secure routing protocol for Internet of Things", *Cluster Comput*, Vol. 25, pp. 1779–1789, 2022.

[17] N. Singh and R. Tirole, "Bumble Bees Mating Optimization Algorithm for Economic Load Dispatch with Pollution", In: *Proc. of International Conference on Advanced Computation and Telecommunication (ICACAT)*, Bhopal, India, pp.1-6, 2018.

[18] K. Mabodi, M. Yusefi, S. Zandiyan, L. Irankhah, and R. Fotohi, "Multi-level trust-based intelligence schema for securing of internet of

things (IoT) against security threats using cryptographic authentication", *J. Supercomput.*, Vol. 76, pp. 7081–7106, 2020.
[19] N. Djedjig, D. Tandjaoui, F. Medjek, and I. Romdhani, "Trust-aware and cooperative routing protocol for IoT security", *J. Inf. Secur.Appl.*, Vol. 52, p.102467, 2020.
[20] T. Wang, H. Luo, W. Jia, A. Liu, and M. Xie, "MTES: An intelligent trust evaluation scheme in sensor-cloud-enabled industrial internet of things", *IEEE Trans. Ind. Inf.*, Vol. 16, No. 3, pp. 2054–2062, 2020.
[21] S. M. Muzammal, R. K. Murugesan, N. Z. Jhanjhi, M. S. Hossain, and A. Yassine, "Trust and Mobility-Based Protocol for Secure Routing in Internet of Things", *Sensors*, Vol. 22, No. 16, p. 6215, 2022.
[22] G. K. Ragesh and A. Kumar, "Trust based Secure Routing and message delivery protocol for signal processing attacks in Io applications", *J Supercomput*., Vol. 79, pp. 2882-2909, 2023.
[23] S. M. Mujeeb, R. P. Sam, and K. Madhavi, "Trust and energy aware routing algorithm for Internet of Things networks", *International Journal of Numerical Modelling*, Vol. 34, No. 4, pp. e2858, 2021.
[24] X. S. Wang, "A New Metaheuristic Bat-Inspired Algorithm, in: Nature Inspired Cooperative Strategies for Optimization (NISCO 2010)", *Studies in Computational Intelligence*., Vol. 284, pp. 65–74, 2010.
[25] G. E. Hinton, S. Osindero, Y. W. Teh, "A fast learning algorithm for deep belief nets", *Neural Computation.*, Vol. 18, No. 7, pp. 1527–54, 2006.
[26] S. Subramani and M. Selvi, "Multi-objective PSO based feature selection for intrusion detection in IoT based wireless sensor networks", *Optik*, Vol. 273, pp. 1-10, 2023.
[27] R. K. Dhanaraj, R. H. Jhaveri, L. Krishnasamy, G. Srivastava, and P. K. R. Maddikunta, "Black-Hole Attack Mitigation in Medical Sensor Networks Using the Enhanced Gravitational Search Algorithm", *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, Vol. 29, No. 2, pp. 297–315, Dec. 2021.
[28] R. Nagaraju, J. T. Pentang, S. Abdufattokhov, R. F. CosioBorda, N. Mageswari, G. Uganya, "Attack prevention in IoT through hybrid optimization mechanism and deep learning framework", *Measurement: Sensors*, Vol. 24, pp. 1-10, 2022.
[29] A. R. Alfarez and S. Hailes, "Supporting trust in virtual communities", In: *Proc. of the 33rd Annual Hawaii International Conference on System Sciences*, Maui, HI, USA, p. 9, 2000.
[30] Lones, and A. Michael, "Metaheuristics in Nature-Inspired Algorithms", In: *Prof of GECCO '14*, pp. 1419–1422, 2014.