IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 21 June 2023, accepted 21 July 2023, date of publication 24 July 2023, date of current version 2 August 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3298559

RESEARCH ARTICLE

Elephant Herding Robustness Evolution Algorithm With Multi-Clan Co-Evolution Against Cyber Attacks for Scale-Free Internet of Things in Smart Cities

TALHA NAEEM QURESHI[1], ZAHOOR ALI KHAN[2], NADEEM JAVAID[1], (Senior Member, IEEE), ABDULAZIZ ALDEGHEISHEM[3], MUHAMMAD BABAR RASHEED[4], (Senior Member, IEEE), AND NABIL ALRAJEH[5]

[1]Department of Computer Science, COMSATS University Islamabad, Islamabad 44000, Pakistan
[2]Department of Computer Information Science, Higher Colleges of Technology, Fujairah, United Arab Emirates
[3]Department of Urban Planning, College of Architecture and Planning, King Saud University, Riyadh 11574, Saudi Arabia
[4]Department of Electronics and Robotics Engineering, University of Gloucestershire, GL50 2RH Cheltenham, U.K.
[5]Department of Biomedical Technology, College of Applied Medical Sciences, King Saud University, Riyadh 11633, Saudi Arabia

Corresponding author: Nadeem Javaid (nadeemjavaidqau@gmail.com)

This work was supported by King Saud University, Riyadh, Saudi Arabia, through the Researchers Supporting Project under Grant RSP2023R295.

ABSTRACT A large number of sensors are deployed for performing various tasks in the smart cities. The sensors are connected with each other through the Internet that leads to the emergence of Internet of Things (IoT). As the time passes, the number of deployed sensors is exponentially increasing. Not only this, the enhancement of sensors has also laid the base of automation. However, the increased number of sensors make the IoT networks more complex and scaled. Due to the increasing size and complexity, IoT networks of scale-free nature are found highly prone to attacks. In order to maintain the functionality of crucial applications, it is mandatory to increase the robustness of IoT networks. Additionally, it has been found that scale-free networks are resistant to random attacks. However, they are highly vulnerable to intentional, malicious, deliberate, targeted and cyber attacks where nodes are destroyed based on preference. Moreover, sensors of IoT network have limited communication, processing and energy resources. Hence, they cannot bear the load of computationally extensive robustness algorithms. A communication model is proposed in this paper to save the sensors from computational overhead of robustness algorithms by migrating the computational load to back-end high power processing clusters. Elephant Herding Robustness Evolution (EHRE) algorithm is proposed based on an enhanced communication model. In the proposed work, 6 phases of operations are used: initialization, sorting, clan updating, clan separating,selection and formation, and filtration. These process collectively increase the robustness of the scale-free IoT networks. EHRE is compared with well-known previous algorithms and is proven to be robust with a remarkable lead in performance. Moreover, EHRE is capable to achieve global optimum results in less number of iterations. EHRE achieves 95% efficiency after 60 iterations and 99% efficiency after 70 iterations. Moreover, EHRE performs 58.77% better than Enhanced Differential Evolution (EDE) algorithm, 65.22% better than Genetic Algorithm (GA), 86.35% better than Simulating Annealing (SA) and 94.77% better than Hill climbing Algorithm (HA).

INDEX TERMS Elephant herding robustness evolution, Internet of Things, scale-free networks, malicious attacks, targeted attacks, topology robustness, smart cities.

NOMENCLATURE

IoT	Internet of Things.
EHRE	Elephant Herding Robustness Evolution.
EDE	Enhanced Differential Evolution.

The associate editor coordinating the review of this manuscript and approving it for publication was Alessio Giorgetti.

GA	Genetic Algorithm.
SA	Simulating Annealing.
HA	Hill climbing Algorithm.
BA	Barabasi Albert.
EABA	Energy Aware Barabasi Albert.
GPS	Global Positioning System.
SAN	Storage Area Network.

I. INTRODUCTION

The modern era is the era of automation where everything is getting automated. Internet was formed with the main thought to connect people and devices. Devices are becoming smarter with every passing day along with exponential expansion. The devices are coming together and connecting with each other using the Internet, referred to as Internet of Things (IoT). IoT is a favorite field for researchers and scientists in the recent decade. These devices will expand and will acquire even more space than humans in the near future. It is estimated that these devices will cross even twenty nine billion in the year 2030 [1], [2]. The rapid expansion of IoT is due to low cost sensors that are smart enough to sense multiple attributes at the same time. This expansion of sensors has laid the foundation for automation in multiple fields and making multiple tasks very easy [3], [4]. The IoT is an integration of multiple disciplines, including fifth generation (5G) ultra-dense cellular networks, heterogeneous ad hoc networks, hybrid mobile networks, wireless sensor networks, and so on. The IoT has a broad range of applications in smart cities [3], [5], [6], [7], [8], [9]. Typically, it deploys a large number of networking nodes within a certain area, and these nodes communicate with each other to collect data and provide reference for smart cities in various fields like industry, agriculture, security, transportation, smart home, health care, etc. Meanwhile, these are producing a vast amount and different types of data. Therefore, how to improve the robustness of IoT against node failure of smart cities has become an essential issue in recent years. With the evolution of technology, automation has exponentially increased in almost all fields to speed up the processes and to decrease human errors. IoT helps in automation through sensors. In health care, vital information of patients is proactively monitored through smart watches, Holter monitor and other health care sensors. They all are combined to form a health care IoT network. Industrial processes are revolutionized through IoT and are managed through sensor based IoT networks. In transportation, congestion control and early warning traffic systems work on IoT based sensors. Robustness of IoT network is important as its unavailability can result in life threatening results due to dependence of critical data that is served through IoT. A novel algorithm, Elephant Herding Robustness Evolution (EHRE), is proposed to enhance the robustness of IoT network. It is inspired by the herding behavior of elephants and designed to solve complex problems. It is a very powerful algorithm that works on a swarm-based search approach. As per the best of our knowledge, it is the first attempt to map elephant herding behavior over IoT networks and to enhance robustness of IoT networks through this design. It has multiple evolutionary characteristics that were not present in classical heuristic algorithms including fast convergence and ability to obtain global optimum results.

Majorly, there are two network models for IoT, i.e., scale-free and small world. Scale-free models are normally used to model homogeneous networks while small world models are used for heterogeneous networks. Due to the fact that IoT sensors share the same communication ranges, bandwidths, and processing power, IoT is considered to be scale-free in nature [3], [4], [9]. We have adopted scale-free model for IoT network of smart cities. In scale-free networks, nodes form edges based on the power-law distribution due to which there are fewer high degree nodes as compared to low degree nodes. While scale-free networks are highly immune to random attacks, they are extremely vulnerable to targeted, malicious, intentional, high-level, and cyber attacks [3], [4], [9], [10], [11], [12], [13]. When high degree nodes are specifically targeted in scale-free networks, they tend to fragment quickly after a few attacks. As a result, the network is paralyzed [10], [11], [12], [13]. To ensure smooth operations of the smart cities and reliability of extremely crucial IoT applications, resilience of the scale-free IoT networks against malicious, targeted, intentional, and cyber attacks is of key importance.

Main contributions

The main contributions are as follows.

- Sensor nodes in IoT network have limited processing and communication resources due to which they cannot have a large number of neighbors and long-distance links. Scale-free topology with preferential attachment property is formulated through sensor's dense deployment. Distance of links and overloading of neighbors are controlled through $Sensor_{range}$ and $Neighbor_{threshold}$ respectively.
- A novel algorithm, EHRE, is proposed to obtain global optimum results in very less time. Hence, the energy, processing and communication resources of IoT sensors are saved.
- The proposed algorithm keeps the degree distribution of sensors unchanged during all operations. Hence, additional resources are not required for communication links and energy is optimized.
- System model for IoT network of smart cities is designed that transfers the processing overhead of structural topology robustness algorithm from IoT sensors to the big data server cluster. Hence, energy and resources of sensors are saved.

Smart cities are powered by numerous Artificial Intelligence (AI) and Machine Learning (ML) based applications that are dependent on IoT sensors for data gathering and decision making. In smart traffic control systems of smart cities based on IoT, early detection, prediction and congestion control of traffic are ensured through AI assistance [15].

Traffic data that can assist in prevention of accidents and congestion control is highly prone to intelligent targeted cyber attacks that can result in life threatening losses in the form of road accidents [15]. EHRE can effectively prevent targeted cyber attacks by converging the topology towards an enhanced and robust structure. IoT is the pivot of smart cities. IoT systems of military and government are targeted by political hackers and criminals to gain information [15]. These IoT systems can be protected by the formation of a topology that is robust against targeted cyber attacks.

The rest of the paper is organized as follows. Section II describes the literature review of already proposed topology robustness strategies for IoT networks and allied issues. Section III describes the system model for optimized and future IoT network based smart cities. Section IV represents the preliminaries. Section V describes the mapping of EHRE on IoT networks. Section VI shows the simulation details and results. Section 8 concludes the paper.

II. RELATED WORK

Numerous networks including IoT and wireless networks are analyzed by the researchers and found to be scale-free. The behavior of nodes during edge generation in scale-free networks is defined by a power-law distribution. Scale-free networks were studied by A. L. Barabasi and R. Albert, who then presented a model they called the BA model [14] to generate topologies with power law distribution, where the edges formed by the nodes in the generated network strictly follow the power-law distribution. Besides, the topologies generated by BA model are not compatible with the IoT and wireless networks. In IoT and wireless networks, sensor nodes have limited energy resources along with limited communication capabilities as most of the sensors are battery-powered. When sensor nodes are forced to make communication links over large distances, they will quickly deplete their energy and will die after a short time span.

Herrmann et al. suggest using the Hill climbing Algorithm (HA) [16] to improve the resilience of scale-free networks. By altering the topology to resemble an onion, HA improves the robustness of scale-free networks. The edges are picked and swapped at random to operate. HA has a low computational efficiency as a result of the random selection and edge swapping.

P. Buesser et al. suggest Simulating Annealing (SA) [17] to improve the stability of scale-free networks. Although SA relies on the randomization phenomena, it also takes into account inferior configurations when edges are randomly swapped.

Y. Jian et al. propose Energy Aware BA (EABA) model [18] for scale-free networks. Ranges and energy consumption are varied by tuning the variables in EABA that results in communication overhead due to parallel operations of energy balancing and data transmission adjustment. EABA is unable to handle IoT and wireless networks because it does not take into account the constrained communication range of IoT sensor nodes. It is inefficient at computing and gets stuck in local optimum conditions.

A model to improve the robustness of scale-free networks is put forth by Rong et al. in [19]. The suggested model works by categorizing the network's edges into different groups and is based on edge classification. Due to the model's disregard for the sensor nodes' resource constraints, it is not suitable to IoT and wireless networks. In IoT, nodes cannot have high communication range due to limited energy, processing and communication capabilities. Moreover, only a single type of edge swap mechanism is considered in the proposed model, which restricts the model to achieve high robustness and global optimum results.

A memetic algorithm is proposed by Zhou and Liu [20] to enhance the robustness of scale-free networks. The algorithm is based on multi-channel operations along with considering the degree distribution of nodes. Multi-channel operation leads to high complexity and computational overhead that results in quick depletion of node's energy. Moreover, it does not consider the limitation of communication radius for IoT nodes due to which it cannot be applied to IoT network to enhance topology robustness.

A multi-objective approach is put out by Zhou and Liu [21] to improve the resilience of scale-free networks. The suggested algorithm evaluates networks under various forms of attacks. Evaluation also takes into account scenarios from the real world. The suggested algorithm cannot be applied to the IoT because it fails to cater to the resource constraints of the IoT devices.

The greedy approach was proposed by Qiu et al. [22] for enhancing the robustness of IoT networks. The proposed solution works on greedy approach and improves the robustness of the topology by adding additional links. The addition of links results in huge financial impact and requires extra resources, which are practically not feasible in a large scale network. Additional links also change the edge density of the existing network along with degree distribution.

Qiu et al. [9] propose a Genetic Algorithm (GA) based solution for improving robustness of scale-free networks. The proposed solution is unable to perform deep search in solution space for global optimum results. As a result, the robustness is not enhanced to the maximum level. Besides, the fixed probabilities for crossover and mutation operators are used that restrict the solution from getting global optimum results along with the lack of maintaining diversity. The proposed solution has a slow convergence rate.

ROSE [23] is proposed by T. Qiu et al. for enhancing robustness of scale-free networks. It works by converting topology into onion-like structure through two major operations. ROSE uses the first node as a reference for converting topology into onion-like structure in degree difference operation. However, in most scale-free networks, the first node is not the highest degree node. Due to which ROSE failed to convert the topology into a perfect onion-like structure because of wrong selection. Moreover, the robustness of the topology is not fully enhanced by ROSE.

The scale-free networks' robustness can be improved with ROCKS, according to Qiu et al. [24]. ROCKS cannot discover the solution space's hidden advantages since it employs fixed crossover and mutation probability. This prevents the global optimum solution from being reached. Furthermore, ROCKS is unable to do a thorough search in the solution space. It also has a modest convergence rate.

Detection of malicious data flows and anomaly is of critical importance in IoT network according to Shafiq et al. [25]. Undesired and unauthorized data traffic should be blocked in IoT networks to ensure data security and improve robustness of IoT network. An algorithm based on improved feature selection approach named CorrAUC is proposed to detect malicious traffic in IoT networks. Malicious traffic and unauthorized data flows in IoT networks can be effectively controlled through machine learning according to Shafiq et al. [26]. However, these machine learning based techniques can misclassify many traffic flows in IoT networks due to wrong feature selection. To resolve this issue, effective feature selection is applied followed by CorrACC. Shafiq et al. [27] worked on identification of cyber attacks in IoT based smart cities. These attacks can cause significant damage to the infrastructure and human life. Hence, improving the robustness of IoT based smart cities is critically important. Shafiq et al. [28] put an effort to highlight literature review of sustainable smart cities, data mining, machine learning and feature selection to classify data flows in IoT networks. When machine learning techniques are applied, then datasets and features gain essential importance. Shafiq et al. [28] put an effort to highlight literature review of sustainable smart cities, data mining, machine learning and feature selection to classify data flows in IoT networks. When machine learning techniques are applied, then datasets and features gain essential importance.

III. ROBUST AND EFFICIENT SCALE-FREE IOT MODEL FOR SMART CITIES

In this section, we have proposed a modeling strategy for a scale-free IoT network. We have further evaluated the scale-free nature of our proposed IoT network based on complex network theory. The system model proposed for scale-free IoT based smart cities, shown in figure 1, is motivated from [3], [4], and [9]. Multiple networks come together and forms the IoT network. The communication in IoT networks is majorly done via a wireless medium. Besides, many sensors have limited communication and processing capabilities along with energy constraints. The mentioned limitations have the following effects on the network.

- Sensor nodes cannot make arbitrarily long communication links with other nodes due to limited communication range, which is being controlled by parameter $Sensor_{range}$.
- The number of edges or links each node can form is limited due to the above mentioned constraints. Moreover, the number of links each node can form is controlled by parameter $Neighbor_{threshold}$. After reaching the threshold value, sensors are not allowed to form additional links.

Due to the limited communication capability, sensor nodes cannot make communication links with a sufficient number of neighbors due to which preferential attachment attribute of the BA model is not fully implementable. To overcome this, we have deployed a dense IoT network. To achieve dense topology, each sensor node should be in the communication range with atleast 50% of the sensors and the communication range of senor nodes should be large enough to cover a desired number of sensors in the network. If nodes' communication radii are not appreciably great, high degree nodes will be dispersed around the network, which will cause network fragmentation. Significant research on dense network topologies is now being done [3], [4], [29], [30] due to the rapid developments made in the field of sensor manufacturing. Dense network topologies will be common in the future as the costs of sensors are decreasing day by day. Moreover, ranges of sensors can be enhanced to an optimum level with minimum cost. It leads to the dense deployment of sensors and now sensors can be found everywhere including homes, transportation, roadsides, commercial buildings, shopping malls and hospitals to support a variety of multiple services under the umbrella of IoT based smart cities. As a whole sum, dense deployments are adopted more often in the current era. We have considered the following aspects for creation of IoT networks with scale-free nature in the smart cities.

- Communication links are non simultaneously added between nodes. The new incoming node will establish links with the existing nodes in the network. Here, non simultaneously means, at the same instance, the new link is not established by a pair of nodes.
- New incoming node prefers to establish link with the existing nodes in the communication range that are controlled by parameter $Sensor_{range}$ based on their degree. It is desirable to select high degree nodes as neighbors. The phenomena is based on the Roulette approach, which uses newly arriving nodes to create links.
- By connecting with the other nodes already in the network, new entering nodes become neighbors. It is known as the node's local world. Higher degree nodes use consume energy. Hence, having high probability to die down quickly. It may lead the network to get fragmented. Besides, $Neighbor_{threshold}$ is used to restrict a node from establishing links more than the desired limit. This value limits the total number of neighbors that each node can have. The weight of adjacent nodes within its range is calculated each time a new node joins a network, denoted as $Sensor_{range}$, using the equation given below. The newly joined node N_i prefers to establish neighborhood relation with nodes in

$Sensor_{range}$ having high value of $N_{we(i)}$ as per equation 1.

$$N_{we(i)} = D_i / \sum_{j=1}^{n_{nei}} D_j, \tag{1}$$

where the number of nodes in the newly joined node's $Sensor_{range}$ is denoted by the symbol n_{nei}. Node i's degree is denoted by the symbol D_i. The proposed architecture, as depicted in Figure 1, is formed with the aim to relief the sensors from computational overhead of advanced optimization algorithms. The suggested model takes into account the limited processing and communication resources of IoT sensors. Traditional models are based on intercommunication of sensor nodes as per protocols defined by algorithms, which increases the computational load on sensors and leads to high energy consumption. The proposed architecture collects the topology information from the sensors and performs all the processing in the data center. The proposed EHRE algorithm has multiple evolutionary characteristics including fast convergence and ability to obtain global optimum results in very less time due to reliance on swarm based search methods. These capabilities also make the algorithm to save energy and computational resources. These characteristics were not present in traditional heuristic algorithms.

- **Smart cities cloud:** All IoT segments, i.e., smart homes, smart industry, smart agriculture, health care and smart transportation, in our suggested model are mostly based on sensors, as seen in Figure 1. To the cloud of the smart cities, all the sensors broadcast their positions, application-specific data, and neighbor information. The smart cities cloud acts as an aggregation hub where all the data is received from multiple IoT networks and aggregated. The aggregated data is forwarded to big data server cluster through the sink node.
- **Sink node**: Sink node is an intermediate communication hub between the IoT network and back-end data processing facility. It supports two-way data communication and sends all the information received from smart cities cloud to back-end data storage. The sink node acts as an intermediate communication hub between smart cities' cloud and the big data server cluster. The sink node is responsible for sending the locations and neighbors of sensor nodes to the big data server cluster and it will also intimate sensor nodes to form edges according to directions of the central processor.
- **Big data server cluster**: It is a data processing facility of smart cities where all the information regarding sensors including location and neighbors is processed. Whenever a new node enters any IoT segment, it calculates its location through the Global Positioning System (GPS) module that is an embedded part of every sensor and sends it to the big data server cluster. The location and neighbors' information of each sensor node resides in the big data server cluster and is provided to all the stakeholders when required. The location and neighbor information are automatically updated by the big data server cluster after a specific interval of time and after the occurrence of a change in the topology.
- **Storage Area Network (SAN)**: SAN is a data storage facility that stores huge quantity of data for longer periods. With the passage of time, data of IoT sensors will increase due to scalability and increase in number of applications. The increase in data demands for excessive big data server cluster resources. It is because SAN is connected to the big data server cluster to keep records of all topology changes and provide previous history of sensor locations and neighbors' information. Whenever changes are observed in topologies due to the addition or deletion of the sensor node, location of sensors and connected neighbors are updated in the big data server cluster and the previous information of the topology is transferred to SAN.
- **Central processor**: The central processor is regarded as the brain of the entire network. It acts as a decision maker that ensures topology robustness by swapping the edges of sensor nodes. Topology robustness is optimized by extracting current locations and neighbor information of all sensor nodes from the big data server cluster. The central processor forms an adjacency matrix of the whole topology based on extracted locations and neighbors' information. The robustness of current topology is calculated through extracted adjacency matrix based on Schneider R. An elephant is formed after the conversion of the adjacency matrix. Multiple clans are formed by the central processor with each clan having a fixed number of elephants. The proposed EHRE algorithm is used by the central processor to optimize the current topology of IoT networks. Sensors reform their links with the neighboring sensors according to optimized topology as per directions received from central processor. Once an optimized topology is formed, it is updated in the big data server cluster. In IoT networks, most of the sensors are powered by batteries, and have limited communication and computational resources. If computationally extensive algorithms are processed by sensor nodes, then they will quickly deplete their energy reservoir. One major goal of our proposed system model is to ensure that sensors are not affected by the complexity of the proposed solution. Sensors must send their location and neighbors' information to big data server cluster for ensuring robustness. All the computational calculations are performed by a central processor. Central processor has no limitation of computational resources as it can be upgraded by adding additional resources as per requirements.

Real world industry is going through the era of optimization that aims to minimize the requirement of people through automation. It has enhanced the production capacity along with speeding up the processes with minimum errors. IoT has played a pivotal role in enabling automation capability of real-world industry where machines are monitored and managed by IoT based interconnected devices. The

real-world industry processes are now highly dependent on these interconnected IoT devices for proper working [31]. Any interruption in communication due to targeted cyber attacks will hinder the performance of the industrial automation systems resulting in huge financial loss. The proposed EHRE algorithm ensures the robustness of IoT network, saves the industrial automation systems from hindrances and avoids financial loss. The level of response has become truly proactive through IoT based interconnected devices, i.e., smart watches, health care sensors, etc. These devices are capable of collecting clinical data along with vital information of patients. In remote areas, these IoT based health care devices communicate and send patients' data to health care centers, which enables the doctors to monitor the patients living in remote areas where advanced health care facilities are not available [32]. Hence, it can save precious human lives. Besides, any distribution in IoT network of health care devices due to cyber attack may cause life threatening losses. To address this, EHRE is proposed that optimizes the topology of IoT networks and enhances their resilience against malicious cyber attacks.

IV. PRELIMINARIES

Topology robustness matrices Schneider R and R_{link} are used to evaluate the proposed robustness solution. EHRE is swarm based novel heuristic algorithm having multiple strengths including maintaining diversity in solution space through clans, fast convergence and ability to attain global optimum results. EHRE rapidly converge the solution to optimum solution by eliminating weak individuals. EHRE is mapped over scale-free networks for enhancing topology robustness through 6 phases of operations.

A. TOPOLOGY ROBUSTNESS MATRICES FOR SCALE-FREE IoT NETWORKS

The main indicator of how well a network resists attacks is its robustness. As the IoT is mostly made up of wireless battery-powered nodes, nodes and edges in the network may be destroyed as a result of intentional and malicious cyber attacks, as the result of a disaster. The nodes and edges may also be destroyed due to nodes running out of charge. As a result of attacks, communication nodes or links are destroyed that lead to separate the network and IoT network is fragmented, and time critical information is blocked and cannot be exchanged between the stakeholders. Strength of network to sustain such failures or attacks is termed as robustness. IoT network is responsible to host critical applications, i.e., smart health care, smart transportation, smart industry and smart agriculture, which are the major parts of the automated smart cities. Any disruption in these applications can result in unbearable loss. Hence, enhanced robustness of IoT network is the prime requirement. These attacks on IoT networks are characterized as random and Intentional or malicious or targeted attacks. In random attacks, nodes or edges are destroyed randomly without any preference. In scale-free networks, majority of the nodes are having low degree. Hence, more often low degree nodes are destroyed by random attack. Destruction of low degree nodes are having very minimal impact on network. Scale-free networks are by nature robust against random attacks.

In malicious or targeted cyber attacks, nodes or edges are attacked based on some preference, i.e., edge density. Malicious cyber attacks are also termed deliberate, intentional, targeted or high degree attacks. These attacks often prioritize network nodes based on the number of edges they have, while high degree nodes are eliminated one at a time. These attacks quickly fragment the network by very few attacks and the entire network is collapsed as a result. Hence, these attacks have high importance in terms of network robustness and cause worst damage to network structure.

From perspective of black hat cyber attack, attack of all types caused by black hat attacker are divided in two categories, i.e., random and intentional. Scale-free network is by nature robust against random attacks due to having large number of low degree nodes. During the intentional attack by black hat attacker, proposed EHRE algorithm is used to optimize the topology against intentional attacks regardless of their occurrence via any means.

For decades, researchers have evaluated IoT networks and found them to be scale-free in nature [3], [4]. Node's edge distribution follows the power-law distribution in the scale-free networks. The robustness against the random attacks is via this inherit property. Contrarily, against the malicious or targeted cyber attacks, the vulnerability is manifolds. So, to evaluate the robustness of EHRE for IoT networks, we have used deliberate, intentional, targeted and malicious cyber attacks. We obtained the degree of nodes through neighbor information residing in big data server cluster. Then, we sorted the nodes and edges on the basis of their importance in the networks. Besides, the nodes are selected for attacks on the basis of their degrees.

Schneider [9], [33] proposed a robustness metric R for evaluating the network based on percolation theory. High degree adaptive attack strategy is the basis of Schneider R. It is based on an iterative mechanism. It first calculates the highest degree node in each step and then removes it until the entire network is fragmented. Schneider R calculates the largest connected sub graph in the network after each malicious or targeted cyber attack. It is a well known metric used for estimating the capacity of the network to withstand deliberate, targeted, intentional and malicious cyber attacks. Schneider R is calculated using equation 2.

$$R = \frac{1}{N} \sum_{i=1}^{N} MaxSubGraph(i), \tag{2}$$

where the accumulated number of network nodes is given by N while $MaxSubGraph$ shows the number of nodes in the largest component of the network after ith cycle of attack. Range of Schneider R is between 0 to 0.5, where 0.5 refers to full mesh network. $\frac{1}{N}$ is a normalization factor, which is used for the comparison of networks having different number of

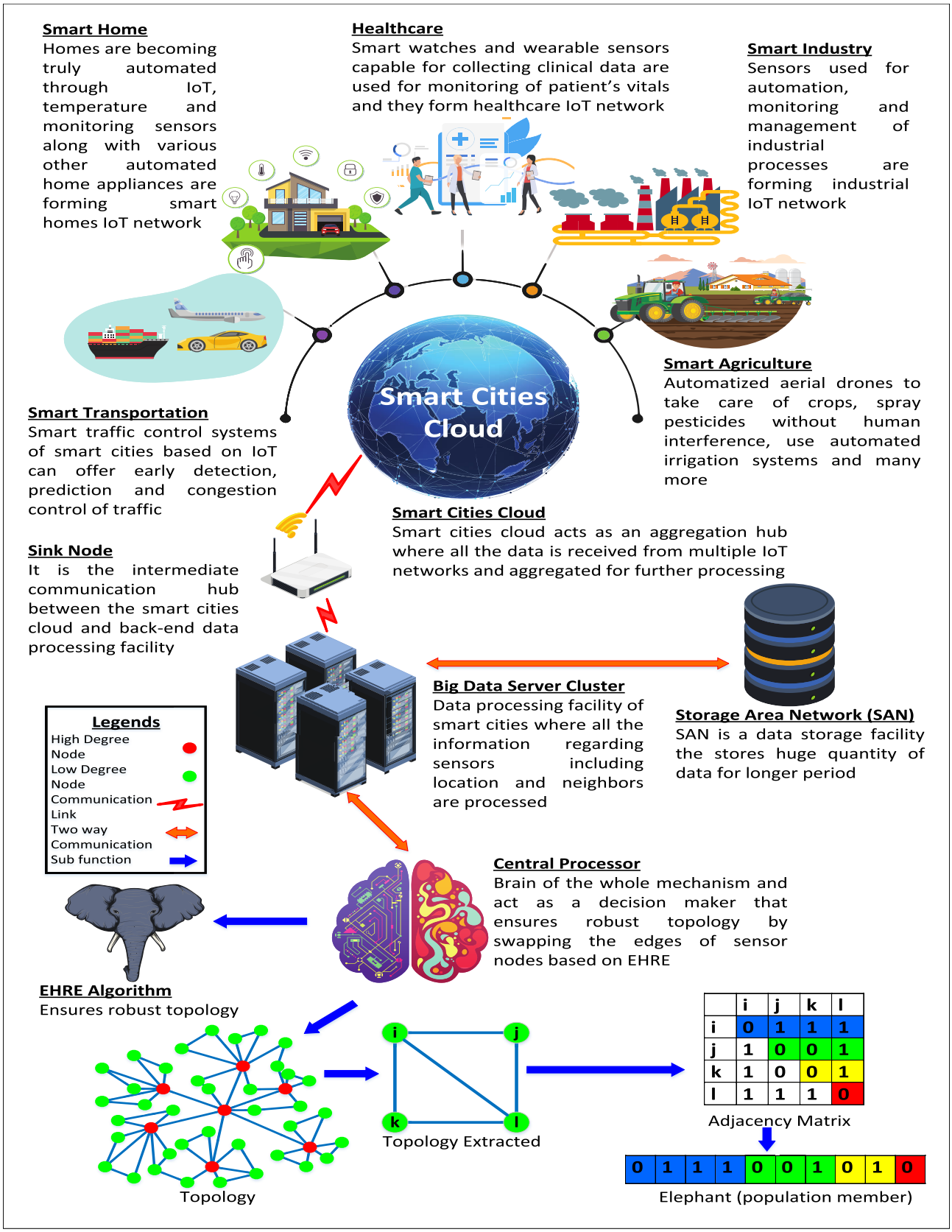


FIGURE 1. Proposed IoT system model for smart cities.

nodes. Besides, high value of Schneider R refers to increased robustness of the network against malicious, targeted, high degree and deliberate cyber attacks.

Schneider R is based on high degree adaptive attack performed on the nodes. The same concept is extended to edges of the network by Zeng and Liu [21], [34] as per equation 3.

$$R_{link} = \frac{1}{L} \sum_{j=1}^{L} MaxSubGraph(j), \tag{3}$$

where R_{link} refers to the link robustness, L is the total number of communication links or edges in the network. *MaxSubGraph* shows the maximum numbers of nodes in the largest connected sub graph after *jth* cycle of attack. $\frac{1}{L}$ is the normalization factor that enables the comparison of different works having different number of edges or links. EHRE is a multi-objective algorithm wherein we have used both Schneider R and R_{link} for evaluating its performance.

B. EHRE ALGORITHM

Modern meta heuristic algorithms cannot provide the exact results. However, desirable optimum solutions can be achieved in a reasonable time. Multiple meta heuristic algorithms are proposed for solving complex problems. Swarm based meta heuristic algorithms are widely applied to multiple problems and desirable results are achieved due to their varied strengths, i.e., fast convergence and achieving global optimum results. EHRE is a type of heuristic algorithm that is based on swarm based meta heuristic search methods [35], [36], [37], [38]. It is designed for solving complex optimization problems. EHRE is influenced by the elephant's herding behavior [35], [36], [37], [38]. It has many multiple evolutionary characteristics that are mostly not present in the conventional heuristic algorithms that include rapid convergence rate, converging capability towards global optimum results by exploring hidden strengths of population space and maintaining population diversity through multiple clans. Elephants live in different clans under the leadership of a matriarch. Male elephants leave their clans as they grow up. The behavior of elephants is modeled into the following two operators.

- **Clan Updating Operator**: The matriarch governs all elephants and acts as the fittest elephant. The position of each elephant *j* in the clan *ci* is influenced by the position of the matriarch x_{best} as per equation 4 [35]:

$$x_{new,ci,j} = x_{ci,j} + \alpha(x_{best,ci} - x_{ci,j})r, \tag{4}$$

  where, $x_{new,ci,j}$ shows the new updated position of elephant *j* in the clan *ci* while $x_{ci,j}$ is the previous position of the elephant. $x_{best,ci}$ is the position of the matriarch. α is the parameter that controls the influence of matriarch on elephants and its value lies between 0 and 1. r ϵ [0,1] is a random number that is based on uniform distribution. Matriarch is the fittest elephant in each clan and its value is updated through equation 5 [35].

$$x_{best,ci} = \beta(x_{center,ci}). \tag{5}$$

  β parameter controls the influence of $x_{center,ci}$ on $x_{best,ci}$ and its value lies between 0 and 1. $x_{center,ci}$ will be calculated as per equation 6 [35].

$$x_{center,ci} = \frac{1}{n_{ci}} \sum_{j=1}^{n_{ci}} x(ci, j). \tag{6}$$

  n_{ci} shows the number of elephants in each clan. Through clan updating operator, all the elephants will evolve and improve their fitness due to the influence of a matriarch as it is having the highest fitness value.
- **Clan Separating Operator**: After reaching puberty, male elephants leave their clans [35]. The process of leaving the clan is modeled into a clan separating operator and it will further enhance the efficiency of the algorithm. Through this operator, weak elephants will be replaced by optimum individuals to save other elephants from their effects during the process of evolution. The worst elephant with the lowest fitness value will be replaced as per equation 7 [35]:

$$x_{worst,ci} = x_{min} + (x_{max} - x_{min} + 1)rand. \tag{7}$$

  x_{max} and x_{min} are the upper and lower bound positions of elephants in the clan. *rand* is the scaling factor based on uniform distribution and its value lies between 0 and 1.

V. UNFOLDING EHRE ALGORITHM OVER SCALE-FREE IOT NETWORKS

Multiple phases for mapping EHRE algorithm over scale-free IoT networks are discussed in this section.

A. INITIALIZATION PHASE

By converting the entire network into an adjacency matrix, as shown in figure 2, the robustness of the scale-free network can be increased by EHRE. A binary-coded matrix called the adjacency matrix contains data on all of the connections between nodes. Figure 2 shows the adjacency matrix for nodes i, j, k and l. Adjacency matrix stores binary value 1 when there is a link between nodes and 0 if there is no communication link. To further improve the computational efficiency along with memory, the adjacency matrix is converted into an elephant, as shown in figure 2. The elephant contains all the required information regarding links and nodes, same as the adjacency matrix.

Multiple clans *ci* are used by EHRE, as shown in figure 3. Multiple clans ensure the prevention of premature convergence along with attaining population diversity. The number of clans is controlled through parameter $Clan_{scale}$ during the evolution process of EHRE. We have taken the value of $Clan_{scale}$ as 5 for our algorithm. Each clan has a fixed number of elephants x that are controlled by n_{ci}. We have fixed n_{ci} equal to 32 to prevent premature convergence for

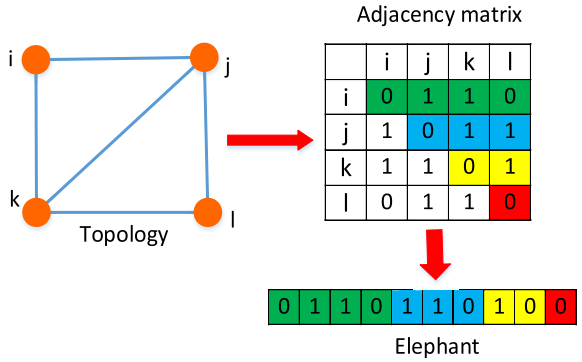


FIGURE 2. Adjacency matrix for EHRE.

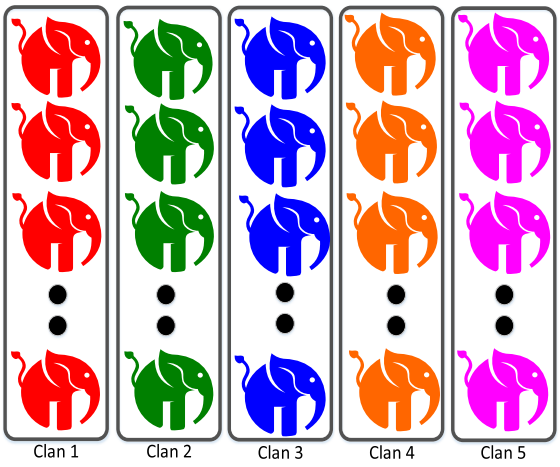


FIGURE 3. Clan based multiple population.

our EHRE algorithm, as shown in figure 3. Each elephant is donated by $x_{ci,j}$ where ci is the clan to which the elephant belongs to and j is the position of the elephant in the clan. $x_{ci,j}$ is a graph of vertices V and edges E, given by equation 8.

$$x_{ci,j} = G(V, E). \tag{8}$$

Where $V = \{1, 2, 3, \ldots, N\}$ and $E = \{e_{ij} | i, j \in Vand\ i \neq j\}$.

B. SORTING PHASE

The sorting phase is the preliminary phase for the remaining operations. It prepares all the clans for further phases of optimization.

- **Step 1**: Schneider R metric is based on node attacks while R_{link} metric is governed by link based attacks over the network. In this phase, Schneider R and R_{link} are calculated for all the elephants belonging to the multiple clans, as per equations 9 and 10.

$$R_{clans} = R\{c_1, c_2, c_3, \ldots, c_n\}. \tag{9}$$

$$Rlink_{clans} = R\{c_1, c_2, c_3, \ldots, c_n\}. \tag{10}$$

- **Step 2**: After calculating the Schneider R and R_{link}, all the elephants in each clan are sorted accordingly.

C. CLAN UPDATING OPERATOR PHASE

The clan updating operator phase converges the elephant x_i towards matriarch x_{best}, as it is the fittest elephant of the clan. It recombines the fitness of elephants with the matriarch for all clans c_i.

- **Step 1**: In the start of the phase, the fittest elephant x_i is selected form R_{clans} and $Rlink_{clans}$. Both R_{clans} and $Rlink_{clans}$ are already calculated in the sorting phase. Matriarch with the maximum value of fitness function is found using equations 11 and 12.

$$x_{best} = Max(R_{clans}). \tag{11}$$

$$x_{best} = Max(Rlink_{clans}). \tag{12}$$

  In the case, where we are taking node robustness R as the fitness function, R_{clans} will be used to calculate matriarch x_{best} and when considering link robustness R_{link}, then $Rlink_{clans}$ will be used for the calculation of the matriarch.
- **Step 2**: For all clans, each elephant $x_{ci,j}$ will be updated according to the position of x_{best} in each iteration as per equation 4.
- **Step 3**: We will calculate the exclusive edges of $x_{best,ci}$ and $x_{ci,j}$. Exclusive edges of $x_{best,ci}$ are established into $x_{ci,j}$ and the final topology is represented by $x_{new,ci,j}$. However, the degrees of nodes remain the same after the creation of exclusive edges.
- **Step 3**: We will update all elephants $x_{ci,j}$ in the clan. Matriarch $x_{best,ci}$ will be calculated again for all the clans.

1) EXCLUSIVE EDGE EXCHANGE OPERATION

Exclusive edges are linkages that only appear in one elephant topology and not in any other. In figure 4, there are two candidate elephant topologies, i.e., elephant 1 in figure 4(a) and elephant 2 in figure 4(b). Exclusive edge e_{ab} exists only in topology of elephant 1, whereas, exclusive edge e_{cd} exists only in topology of elephant 2, as shown by blue color in figures 4(a) and 4(b). Now we will explain process of implementing exclusive edge e_{cd} into topology of elephant 1. Finally, after the completion of exclusive edge exchange operation, elephant 1 will disconnect existing edges in order to generate edge e_{cd} along with keeping the degree distribution of each node unchanged. In order to generate edge e_{cd} in the topology of elephant 1, we will select candidate nodes e and f from neighbors of node d that are not having any existing connection with node c, as shown by the green color in figure 4(c). Now we calculate the distance of candidate nodes from the node c, as shown by the green colored dotted lines in figure 4(d). Node f is the node nearest to node c and has no existing edge with node c, as shown in figure 4(e). Now, node c will search for its neighbor nodes having no existing edge with node f along with being nearest to node f. Node g as shown by the blue color in figure 4(f) is the nearest node to node f from neighbors of node c. Nodes c and g will disconnect the existing edge along with nodes d and f, as shown by green dotted lines in figure 4(f). Nodes c and d will form a new edge along with node g and f as shown in figure 4(f). After the exclusive edge exchange operation, edge e_{cd} that was the exclusive edge from elephant

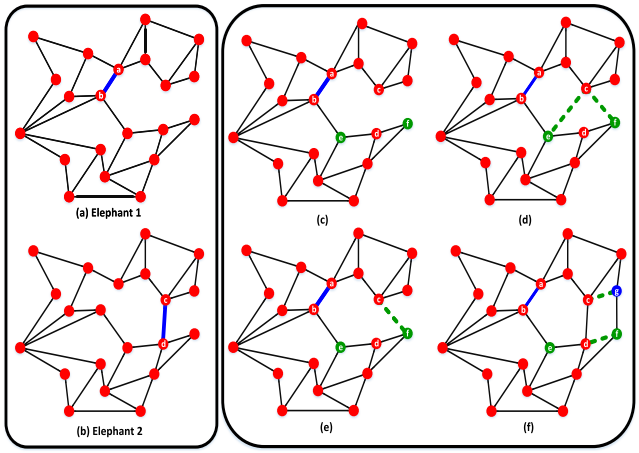


FIGURE 4. Exclusive edge exchange operation.

2 is formed by elephant 1's topology. The degrees of nodes c, d, g and f are still the same after the completion of operation.

Algorithm 1 Clan Updating Operator Phase

Input: [Clans c_i, Elephants of all clans $x_{ci,j}$ and Matriarch of all clans $x_{best,ci}$]
for Fittest elephant x_i is selected form R_{clans} and $Rlink_{clans}$ **do**
  $x_{best,ci}$ based of the fitness function R and R_{link}
end for
Find exclusive edges of $x_{best,ci}$ for all clans c_i **then**
for All clans c_i **do**
  Find exclusive edges of $x_{ci,j}$
  Exclusive edges of $x_{best,ci}$ are established into $x_{ci,j}$
  Final topology after operation is termed as $x_{new,ci,j}$
  Calculate fitness function R and R_{link} for final topology $x_{new,ci,j}$
  if fitness function for $x_{new,ci,j} > x_{ci,j}$ **then**
    $x_{new,ci,j} = x_{ci,j}$
  end if
end for
for Fittest elephant x_i is selected from all clans x_{ci} **do**
  Update matriarch $x_{best,ci}$ based of fitness function R and R_{link} for all clans c_i
end for

D. CLAN SEPARATING OPERATOR PHASE

The clan separating phase enhances the fitness of all clans c_i by replacing the elephants with poor fitness with the optimum elephant. The elephant $x_{worst,ci}$ with the worst fitness will be calculated as per equation 7.

- **Step 1**: Calculate the $x_{worst,ci}$ from each clan along with x_{max}, x_{min} and $x_{min}+1$ that are the first, last and second last elephants, respectively, of the same clan.
- **Step 2**: Calculate the exclusive edges of x_{max}, x_{min} and $x_{min}+1$ for each clan.
- **Step 3**: Establish exclusive edges of x_{max} into $x_{min}+1$ to get the resultant topology graph G'. Establish exclusive edges of x_{min} in graph G' to get the final topology graph G''.
- **Step 4**: Calculate fitness function for the final topology G''. If the robustness is enhanced, then replace it with $x_{worst,ci}$ for each clan.

Algorithm 2 Clan Separating Operator Phase

Input: [Clans c_i and Elephants of all clans $x_{ci,j}$]
for Worst elephant x_i is selected from all clans x_{ci} **do**
  $x_{worst,ci}$ based on the fitness function R and R_{link}
end for
Find exclusive edges of top most elephant $x_{max,ci}$ for all clans c_i**then**
Find exclusive edges of last elephant $x_{min,ci}$ for all clans c_i**then**
Find exclusive edges of second last elephant $x_{min,ci}+1$ for all clans c_i**then**
for All clans c_i **do**
  Establish exclusive edges of x_{max} into $x_{min}+1$
  Get resultant topology graph G'
  Establish exclusive edges of x_{min} in graph G' to get the final topology graph G''
  Calculate fitness function R and R_{link} for final topology G''
  if fitness function for $G'' > x_{ci,j}$ **then**
    $x_{worst,ci} = G''$
  end if
end for

E. SELECTION AND FORMATION OPTIMIZATION PHASE

The onion-like structure is proven to be robust against malicious, targeted, international, high degree and cyber attacks [10], [11], [12], [13]. By transforming topology into an onion-like structure, the selection and formation optimization step increases topology's robustness. The same degree nodes are joined together to form rings, in accordance with the idea of an onion-like structure. As we come towards the center of onion-like structure, the degree of nodes, connected in ring formation, start to increase and as we move towards the outer layer of the structure, the degree of nodes start to decrease. Hence, nodes of the same degrees are connected in each ring. Selection and formation phase works on the phenomena to encourage nodes of the same degrees to connect with each other. Hence, encouraged nodes have minimum degree difference between them to satisfy the criteria of onion-like structure.

- **Step 1**: It will select two independent edges from the topology of the best optimum elephant that is matriarch x_{best}. All the nodes of the independent edges are within the communication radius of each other.

Term independent edges means that nodes belonging to each edge will not have any other edge or link with the nodes of other edge. Nodes i and j belong to the first independent edge. Whereas, nodes k and l belong to the second independent edge. Degrees of nodes i, j, k and l will be d_i, d_j, d_k and d_l, respectively. Their difference of degrees will be calculated as per equations 13, 14 and 15.

$$Diff_0 = |d_i - d_j| + |d_k - d_l| \quad (13)$$

$$Diff_1 = |d_i - d_k| + |d_j - d_l| \quad (14)$$

$$Diff_2 = |d_i - d_l| + |d_j - d_k| \quad (15)$$

- **Step 2**: We will calculate the $Diff_{min}$ as per equation 16. It will provide us with the most optimum swap combination that will result in minimum degree difference between the connecting nodes. Hence, it will result in converging the topology towards an enhanced onion-like structure.

$$Diff_{min} = min(Diff_0, Diff_1, Diff_2) \quad (16)$$

Algorithm 3 Selection and Formation Optimization Phase

Input: [Matriarch $x_{best,ci}$, Clans c_i and Elephants of all clans $x_{ci,j}$]
for All clans c_i **do**
  Select two independent edges from matriarch x_{best}
  Find degrees of nodes belonging to edges d_i, d_j, d_k and d_l
  Calculate $Diff_0$, $Diff_1$, $Diff_2$ and $Diff_{min}$ using equations 13-16.
end for
if $Diff_{min} = Diff_0$ **then**
  Topology remains unchanged
end if
if $Diff_{min} = Diff_1$ **then**
  Remove edges e_{ij}, e_{kl} **and** Add edges e_{ik}, e_{jl} to get the topology G'
  Calculate fitness function R and R_{link} for the final topology G'
  if fitness function for $G' > x_{best,ci}$ **then**
    $x_{best,ci} = G'$
  end if
end if
if $Diff_{min} = Diff_2$ **then**
  Remove edges e_{ij}, e_{kl} **and** Add edges e_{il}, e_{jk} to get the topology G'
  Calculate fitness function R and R_{link} for the final topology G'
  if fitness function for $G' > x_{best,ci}$ **then**
    $x_{best,ci} = G'$
  end if
end if

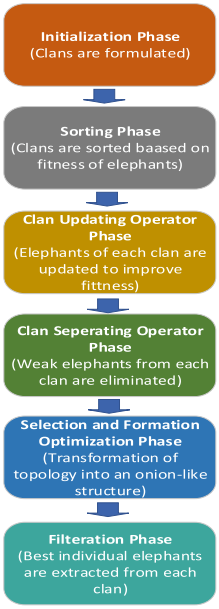


FIGURE 5. Block diagram - unfolding EHRE algorithm over scale-free IoT networks.

F. FILTRATION PHASE

The filtration phase filters the best individual elephants that are matriarch x_{best} of all clans and save them from further altering. Hence, globally optimized solutions are not disturbed and are maintained in a separate space.

- **Step 1**: Calculate the fitness function for each matriarch x_{best} of all clans c_i.
- **Step 2**: Compare the matriarchs of all clans for getting the maximum fitness function that is robustness as per equation 17.

$$x_{fil-best} = max(x_{best,c1}, x_{best,c2}, \ldots, x_{best,cn},) \quad (17)$$

Block diagram is illustrated for all operations as per figure 5.

VI. SIMULATIONS AND RESULTS

The big data server of the smart cities receives information from all of the IoT sensor nodes installed there, including the location coordinates determined by GPS and the specifics of their neighbors. If the users request it for additional processing, it will give them access to the stored data. We have simulated the IoT network in MATLAB based on location coordinates of the sensor nodes extracted through the big data server. It is observed by S. Prendeville *et al.* [39] that modern cities will become efficient and economical by implementing a circular disc shape design. To make our network smarter and more economical, we have implemented the topology in a circular disc shape design. The size of our simulated network is controlled through $Field_{perimeter}$, which deals with the diameter of the topology. We have fixed the diameter to 500 meter as depicted in figure 5. Sensor nodes in IoT networks have constraint of communication range due to which preferential attachment property of the BA model suffers [23]. To resolve the issue of preferential attachment,

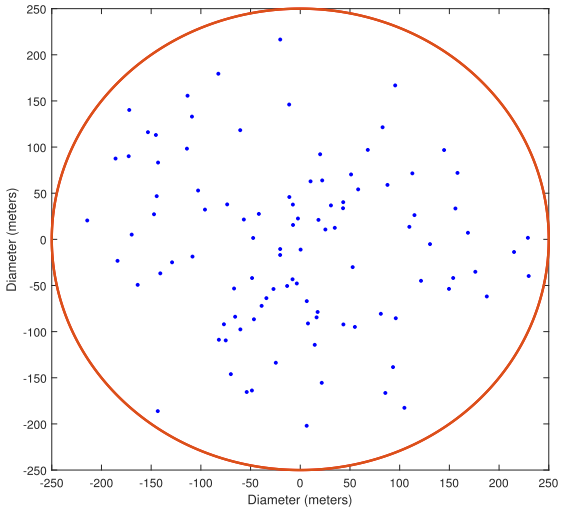


FIGURE 6. Nodes' deployment in a circular disc shape topology.

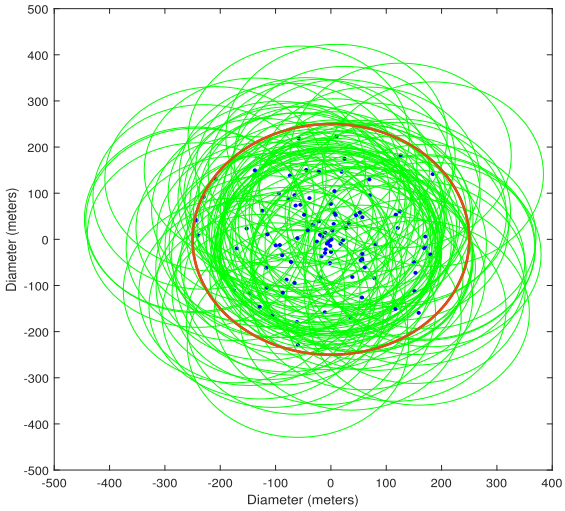


FIGURE 7. Nodes forming neighbors in 200 meters range.

the dense sensor network topology is used [23]. Parameter $Sensor_{range}$ controls the communication radius of the sensors. We fixed the communication radius to 200 meters, so that each sensor should have sufficient neighbors to form a dense IoT network, as shown in figure 6. Besides, the sensor nodes cannot have an arbitrarily large number of neighbors due to the limited processing and communication capabilities. Parameter $Neighbor_{threshold}$ is defined to restrict the maximum number of links each IoT sensor node can form in the network. After reaching the threshold defined by $Neighbor_{threshold}$, IoT sensor node is not allowed to form any further link. Many heuristic based optimization solutions are proposed that suffer from premature convergence due to lack of global search capability and population diversity [40], [41]. Diversity during evolution process is achieved through multiple clans that are controlled by parameter $Clan_{scale}$. We have fixed the number of clans to 5 for simulations. Parameter n_{ci} controls the number of elephants in each clan. Moreover, we have considered the value of n_{ci} as 32 for all clans. A large number of simulations are performed in order to fix the values of $Clan_{scale}$ and n_{ci} for our proposed scheme. All results are averaged for Run_{avg} times, where $Run_{avg} \geq 25$.

A. PERFORMANCE OF THE EHRE ALGORITHM AGAINST SCHNEIDER R

IoT networks are widely spread on large scale due to having extensive utilization in numerous applications and being part of cyber space. Malicious or targeted or intentional attacks occur on IoT network as a result of hacking attempt sourced via cyber channel. We have simulated network of 100 nodes for observing the performance of our proposed EHRE algorithm. We have evaluated the EHRE for 100 iterations against node robustness metric Schneider R. Besides, the simulation results for 25 independent runs are averaged. The performance of EHRE is demonstrated by the blue colored line in figure 8 and is presented in table 1. Most of the conventional heuristic algorithms suffer from premature convergence due to the deficiency of global search capability that is caused due to loss of population diversity during evolution process. Population diversity is maintained by EHRE through multiple clans. EHRE simultaneously co-evolves multiple clans through its 6 phase operation mechanism. This phenomenon leads EHRE to converge rapidly towards global optimum results. Hence, rapid convergence behavior is observed, as shown in figure 8 and table 1. Optimal individuals are mixed during evolution process of traditional heuristic algorithms. Hence, optimal individuals are lost and evolution process is not fully benefited. It leads to slowing down the evolution process. Hence, slow convergence is observed in most of the traditional heuristic algorithms. The clan separation and filtration phases of EHRE are designed to cope with the loss of optimal individuals and to save the algorithm from slow convergence. The former phase of EHRE replaces the weakest elephant from each clan with a suitable elephant that is obtained after the specific evolution mechanism during each cycle. While the latter phase of EHRE filters out and saves the optimal elephants from each clan. Hence, optimum elephants are not mixed and lost during the evolution process. EHRE achieved approximately 95% efficiency after 60 iterations and 99% efficiency after 70 iterations in comparison to the value of Schneider R achieved after 100 iterations, given in table 1. It validates the fast convergence capability of EHRE.

EHRE also converges the topology very effectively into onion-like structure through its selection and formation optimization phase. It works on the phenomenon that perfect onion-like structure is powered by rings of interconnected nodes having similar degree. It selects two independent edges from optimal elephant. In order to minimize the degree difference between the nodes, it switches the edges in every conceivable way. Figure 8's simulation output demonstrates how well EHRE works to improve the scale-free IoT networks' resistance to high-intensity attacks.

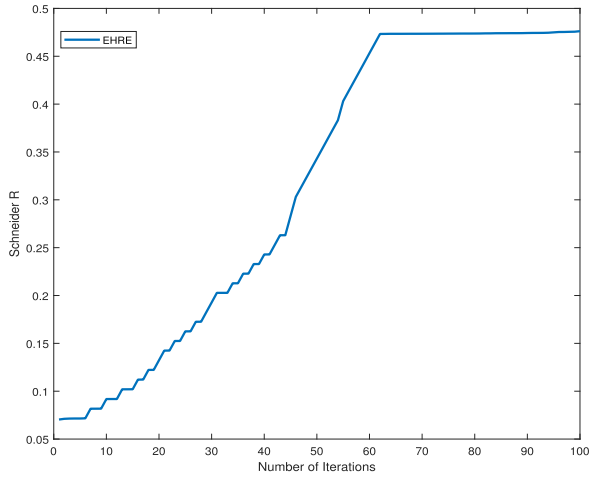


FIGURE 8. Performance of the EHRE algorithm against schneider R.

TABLE 1. Performance of the EHRE agorithm against schneider R.

Iteration	Schneider R
10	0.09180198
20	0.132356436
30	0.192673267
40	0.242891089
50	0.343069307
60	0.453267327
70	0.473524752
80	0.473762376
90	0.47429703
100	0.476217822

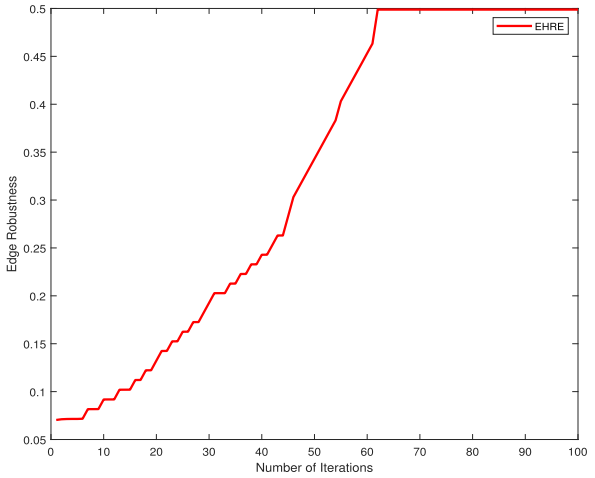


FIGURE 9. Performance of the EHRE algorithm against edge robustness.

TABLE 2. Performance of the EHRE algorithm against edge robustness.

Iteration	Edge Robustness
10	0.09180198
20	0.132356436
30	0.192673267
40	0.242891089
50	0.343069307
60	0.453267327
70	0.498807337
80	0.49880926
90	0.498810509
100	0.498815093

B. PERFORMANCE OF THE EHRE ALGORITHM AGAINST EDGE ROBUSTNESS

In this subsection, performance of EHRE is observed for 100 iterations against edge robustness metric. The network of 100 nodes is used for observing the performance of EHRE. Edge robustness metric is based on link based attacks. It measures the fraction of nodes present in the largest connected cluster of nodes after removing links, based on priority, in each cycle. EHRE performs equally well against link based attacks, as shown by the red colored line in figure 9 and given in table 2. Results in figure 9 and table 2 are average of 25 independent simulations. EHRE performs well against link based attacks due to its rapid convergence ability towards the global optimum solution that is attained because of EHRE's ability to co-evolve multiple clans simultaneously through 6 phases of operations. The clan updating phase of EHRE co-evolves multiple clans on the basis of edge robustness. During the evolution process, individual elephants that are robust against edge attacks are searched and used in further phases of operations.

The clan separating phase eliminates the weak individual elephants that are not capable to cope with edge attacks and replace them with suitable individual elephants obtained by certain criteria. Hence, a rapid convergence is observed during the evolution process of EHRE. EHRE attained 90% efficiency after 60 iterations and 99% efficiency after 70 iterations in comparison to 100 iterations against edge robustness. The simulation results presented in figure 9 demonstrate that EHRE is robust against edge attacks.

C. PERFORMANCE OF THE EHRE ALGORITHM AGAINST EXISTING ALGORITHMS

The performance comparison of EHRE with the existing heuristic algorithms i.e., EDE, GA, SA and HA, is provided herein this subsection. A network of 100 nodes is considered for performance comparison of above mentioned algorithms. The performance of all algorithms is tested for 100 iterations. Independent 25 runs for all algorithms are averaged to demonstrate results in figure 9 and table 3. The blue colored line shows EHRE, green colored line shows EDE, magenta colored line shows GA, black colored line shows SA and mustard colored line shows HA. EHRE performs better than EDE, GA, SA and HA. Considering the performance of EHRE after 100 iterations, EHRE performs 58.77% better than EDE, 65.22% better than GA, 86.35% better than SA and 94.77% better than HA. It is also pertinent to highlight that the convergence rate of EHRE is greatest of all algorithms. EHRE has achieved 95% of the results after 60 iterations, which is a remarkable improvement in comparison to other algorithms. The fast convergence capability of EHRE in comparison

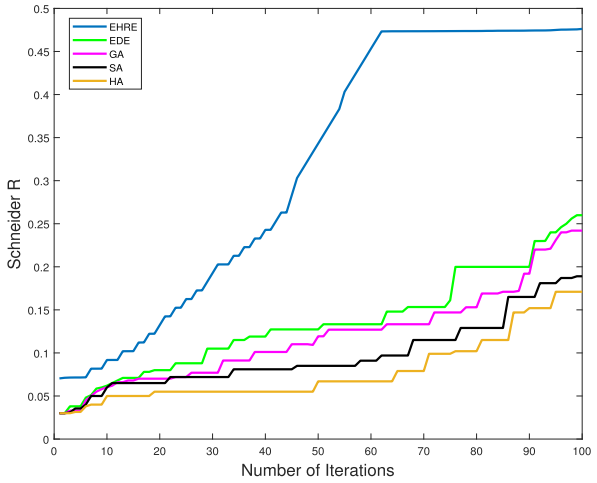


FIGURE 10. Performance of the EHRE algorithm against existing algorithms.

to EDE, GA, SA and HA is due to its enhanced ability to maintain population diversity, which is not present in most conventional heuristic algorithms. Enhanced population diversity in EHRE is maintained due to parallel evolution of multiple clans through 6 phases of operations. Starting with the initialization phase of EHRE, 5 clans are created with population size of 32 elephants in each clan. Multiple clans create diversity in the search space. Hence, fast EHRE converges rapidly by improving value of Schneider R. EHRE also saves optimal individuals and prevents them from mixing into the whole population. Besides, EHRE converges more rapidly because of the exploration of the hidden strengths of all clans and binding them together through its 6 phases of operations. In most conventional heuristic algorithms, optimal individuals are lost due to mixing with the rest of the population. The rapid and remarkable improvement in EHRE gives better results as compared to EDE, GA, SA and HA. EDE and GA lack in performing diverse extensive searching and exploring the solution space to find global optimum results in comparison to EHRE. Besides, the searching speed of EDE and GA is also limited as the solution space is increased to create population diversity due to which EDE and GA show low performance in comparison to EHRE. The performance of HA is the least of all algorithms. HA works by selecting random edges and then swapping them together in each iteration due to which HA is not capable to search global optimum results from whole solution space due to randomization phenomenon and stucks in local optima. On the other hand, SA is also based on the randomization phenomenon. It also randomly selects the edges and swap them together along with considering the inferior configurations based on probability. As a result, it has better performance in comparison to HA. However, its performance is still low as compared to EHRE, EDE and GA. Even after considering inferior variables, SA gets stuck into local optima and is unable to give improved Schneider R result.

TABLE 3. Performance of the EHRE algorithm against existing algorithms.

Algorithm	Schneider R
EHRE	0.476217822
EDE	0.2599
GA	0.2420
SA	0.1890
HA	0.1700

D. PERFORMANCE OF THE EHRE ALGORITHM AGAINST EXISTING ALGORITHMS WITH VARIED NODE DENSITIES

By altering node densities, we compared EHRE with EDE, GA, SA, and HA in this subsection. At each step, the increase of 50 is done in the node density, and the nodes lie in the range starting from 100 nodes and ending at 300 nodes. Figure 10 and Table 4 show the average results of 25 separate runs for each algorithm. In figure 10, the blue colored line depicts the performance of EHRE for networks of different node densities while performance of EDE, GA, SA and HA is shown by green, magenta, black and mustard colored lines, respectively. HA shows the worst performance of all. It is due to HA's random selection and swapping of edges, which leads the model to stuck in local optima. From table 4, it is obvious that the performance of HA decreases as the node density increases. HA's performance decreases by 15.8% as the node densities increases from 100 to 300. SA, on the other hand, shows marginal better performance than HA. SA is also based on the randomization phenomenon. Though, it considers some inferior configurations due to which it performs better than HA. However, it cannot escape from local optima due to randomization. Both HA and SA show low performance due to lack of ability to explore the solution space for finding global optimum results. SA shows 9.01% performance loss as the number of nodes increases from 100 to 300. Besides, both EDE and GA perform better than SA and HA. However, they have lower performance as compared to EHRE. Both EDE and GA cannot perform diverse extensive searching. Hence, both lack in exploration of solution space to dig out the global optimum results. The issue of exploration is even more engraved as we increase the size of solution space by increasing node densities. As a result, the increase of 50 in the node densities, ranging from 100 to 300, causes the performance of EDE, GA, SA, and HA to decline, as shown in table 6. EHRE performs the best of all algorithms for all node densities. It gives relatively low performance degradation, i.e., 3.22%, as node densities increase from 100 to 300. When node density is increased to 150, EHRE performs 57.87%, 64.44%, 85.78% and 94.46% better than EDE, GA, SA and HA, respectively. When node density is further increased to 200, EHRE performs 57.77%, 64.67%, 86.14% and 94.58% better than EDE, GA, SA and HA, respectively. In the next step, node density is increased to 250 nodes for performance analysis. EHRE performs 58.60%, 64.40%, 90.69% and 100% better than EDE, GA, SA and HA, respectively. Finally, all algorithms are tested for 300 nodes. EHRE performs 57.88%, 67.30%, 91% and 104.25% better than EDE, GA,

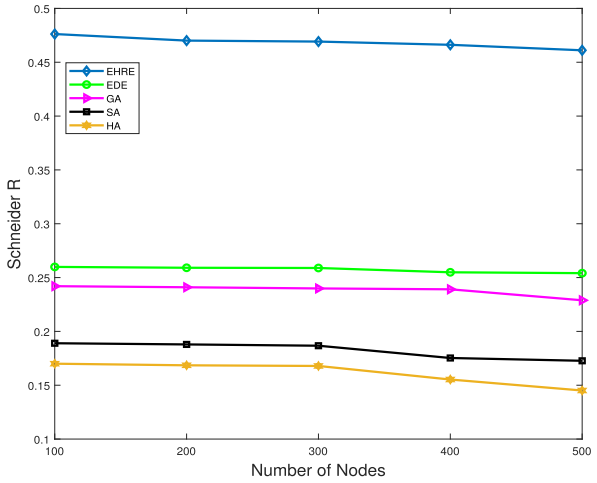


FIGURE 11. Performance of the EHRE algorithm against existing algorithms with varied node densities.

TABLE 4. Performance of the EHRE algorithm against existing algorithms with varied node densities.

Algorithm	100 Nodes	150 Nodes	200 Nodes	250 Nodes	300 Nodes
EHRE	0.4762	0.4701	0.4692	0.4662	0.4611
EDE	0.2599	0.2591	0.2589	0.2549	0.2541
GA	0.2420	0.2410	0.2399	0.2391	0.2289
SA	0.1890	0.1879	0.1867	0.1753	0.1727
HA	0.1700	0.1685	0.1679	0.1553	0.1451

SA and HA. EHRE performs better than other algorithms in all scenarios due to the enhanced capability of maintaining population diversity through multiple clans. It also has deep searching capability to find hidden strengths of solution space through 6 phases of operations and finding global optimum results, which lack in the traditional heuristic algorithms. EHRE ensures prevention of optimal population individual elephants from getting lost and mixing during evolution process. EHRE also updates the weak population individual elephants based on specific criteria during each cycle of evolution and filters out the optimal elephants. It leads EHRE to outperform all other algorithms under all scenarios having varied node densities.

VII. CONCLUSION

An important field of research that is covered in this paper is making the topologies of scale-free IoT networks highly robust for the smart cities. The vulnerability of the scale-free IoT networks against malicious, intentional, targeted and cyber attacks is mitigated through the proposed EHRE algorithm. A communication model is presented that migrates the processing overhead from IoT sensors having limited energy, processing and communication capabilities to back-end high power processing clusters. Hence, save the IoT sensors from processing and communication overhead. Proposed EHRE algorithm enhances the robustness of scale-free IoT network of smart cities through 6 phase operations against node and link based attacks. Moreover, EHRE is compared with the existing well-known algorithms, i.e., EDE, GA, HA and SA. EHRE is proven to enhance the robustness with a remarkable margin as compares to the existing algorithms. Besides, EHRE has built-in multiple strengths that are not present in the conventional heuristic algorithms, i.e., rapid convergence rate, converging capability towards global optimum results by exploring hidden strengths of population space and maintaining population diversity through multiple clans. EHRE is also tested for scalability by increasing the network size from 100 nodes to 500 nodes. EHRE proved its fast convergence capability by achieving approximately 95% efficiency after 60 iterations and 99% efficiency after 70 iterations. Considering the performance of EHRE after 100 iterations, EHRE performs 58.77% better than EDE, 65.22% better than GA, 86.35% better than SA and 94.77% better than HA. In addition, latency can be a possible trade-off between the processing overload and the time required to get instructions from the big data server cluster of smart cities. This issue is intended to be addressed in the future. Moreover, as EHRE is based on 6 phases of operations that may require excessive processing resources, so complexity of solution may be kept in consideration in future research. Along with that, machine learning models will be used as they are quite useful in many problem solving scenarios.

REFERENCES

[1] L. S. Vailshery. Number of IoT connected devices worldwide 2019–2021, with forecasts to 2030. Statista. Accessed: Mar. 3, 2023. [Online]. Available: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/

[2] S. E. Collier, "The emerging enernet: Convergence of the smart grid with the Internet of Things," in *Proc. IEEE Rural Electr. Power Conf.*, Asheville, NC, USA, Apr. 2015, pp. 65–68, doi: 10.1109/REPC.2015.24.

[3] T. N. Qureshi, N. Javaid, A. Almogren, Z. Abubaker, H. Almajed, and I. Mohiuddin, "Attack resistance-based topology robustness of scale-free Internet of Things for smart cities," *Int. J. Web Grid Services*, vol. 17, no. 4, pp. 343–370, 2021.

[4] T. N. Qureshi, N. Javaid, A. Almogren, A. U. Khan, H. Almajed, and I. Mohiuddin, "An adaptive enhanced differential evolution strategies for topology robustness in Internet of Things," *Int. J. Web Grid Services*, vol. 18, no. 1, pp. 1–33, 2022.

[5] C.-W. Tsai, H.-H. Cho, T. K. Shih, J.-S. Pan, and J. J. P. C. Rodrigues, "Metaheuristics for the deployment of 5G," *IEEE Wireless Commun.*, vol. 22, no. 6, pp. 40–46, Dec. 2015, doi: 10.1109/MWC.2015.7368823.

[6] G. Han, L. Liu, S. Chan, R. Yu, and Y. Yang, "HySense: A hybrid mobile crowdsensing framework for sensing opportunities compensation under dynamic coverage constraint," *IEEE Commun. Mag.*, vol. 55, no. 3, pp. 93–99, Mar. 2017, doi: 10.1109/MCOM.2017.1600658CM.

[7] N. Javaid, A. Sher, H. Nasir, and N. Guizani, "Intelligence in IoT-based 5G networks: Opportunities and challenges," *IEEE Commun. Mag.*, vol. 56, no. 10, pp. 94–100, Oct. 2018, doi: 10.1109/MCOM.2018.1800036.

[8] K. Adhinugraha, W. Rahayu, T. Hara, and D. Taniar, "On Internet-of-Things (IoT) gateway coverage expansion," *Future Gener. Comput. Syst.*, vol. 107, pp. 578–587, Jun. 2020.

[9] T. Qiu, J. Liu, W. Si, M. Han, H. Ning, and M. Atiquzzaman, "A data-driven robustness algorithm for the Internet of Things in smart cities," *IEEE Commun. Mag.*, vol. 55, no. 12, pp. 18–23, Dec. 2017, doi: 10.1109/MCOM.2017.1700247.

[10] S. M. Abbas, N. Javaid, A. T. Azar, U. Qasim, Z. A. Khan, and S. Aslam, "Towards enhancing the robustness of scale-free IoT networks by an intelligent rewiring mechanism," *Sensors*, vol. 22, no. 7, p. 2658, Mar. 2022, doi: 10.3390/s22072658.

[11] S. A. Changazi, A. D. Bakhshi, M. Yousaf, M. H. Islam, S. M. Mohsin, S. S. Band, A. Alsufyani, and S. Bourouis, "GA-based geometrically optimized topology robustness to improve ambient intelligence for future Internet of Things," *Comput. Commun.*, vol. 193, pp. 109–117, Sep. 2022, doi: 10.1016/j.comcom.2022.06.030.

[12] M. A. Khan and N. Javaid, "Computationally efficient topology optimization of scale-free IoT networks," *Comput. Commun.*, vol. 185, pp. 1–12, Mar. 2022, doi: 10.1016/j.comcom.2021.12.013.

[13] G. Keerthana, P. Anandan, and N. Nandhagopal, "Enhancing the robustness and security against various attacks in a scale: Free network," *Wireless Pers. Commun.*, vol. 117, no. 4, pp. 3029–3050, Apr. 2020, doi: 10.1007/s11277-020-07356-5.

[14] A.-L. Barabási and R. Albert, "Emergence of scaling in random networks," *Science*, vol. 286, no. 5439, pp. 509–512, Oct. 1999, doi: 10.1126/science.286.5439.509.

[15] J.-P.-A. Yaacoub, H. N. Noura, O. Salman, and A. Chehab, "Ethical hacking for IoT: Security issues, challenges, solutions and recommendations," *Internet Things Cyber-Phys. Syst.*, vol. 3, pp. 280–308, 2023.

[16] H. J. Herrmann, C. M. Schneider, A. A. Moreira, J. S. Andrade Jr., and S. Havlin, "Onion-like network topology enhances robustness against malicious attacks," *J. Stat. Mech., Theory Exp.*, vol. 2011, no. 01, Jan. 2011, Art. no. P01027, doi: 10.1088/1742-5468/2011/01/p01027.

[17] P. Buesser, F. Daolio, and M. Tomassini, "Optimizing the robustness of scale-free networks with simulated annealing," in *Adaptive and Natural Computing Algorithms*. 2011, pp. 167–176, doi: 10.1007/978-3-642-20267-4_18.

[18] Y. Jian, E. Liu, Y. Wang, Z. Zhang, and C. Lin, "Scale-free model for wireless sensor networks," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Shanghai, China, Apr. 2013, pp. 2329–2332, doi: 10.1109/WCNC.2013.6554924.

[19] L. Rong and J. Liu, "A heuristic algorithm for enhancing the robustness of scale-free networks based on edge classification," *Phys. A, Stat. Mech. Appl.*, vol. 503, pp. 503–515, Aug. 2018, doi: 10.1016/j.physa.2018.02.173.

[20] M. Zhou and J. Liu, "A memetic algorithm for enhancing the robustness of scale-free networks against malicious attacks," *Phys. A, Stat. Mech. Appl.*, vol. 410, pp. 131–143, Sep. 2014, doi: 10.1016/j.physa.2014.05.002.

[21] M. Zhou and J. Liu, "A two-phase multiobjective evolutionary algorithm for enhancing the robustness of scale-free networks against multiple malicious attacks," *IEEE Trans. Cybern.*, vol. 47, no. 2, pp. 539–552, Feb. 2017, doi: 10.1109/TCYB.2016.2520477.

[22] T. Qiu, D. Luo, F. Xia, N. Deonauth, W. Si, and A. Tolba, "A greedy model with small world for improving the robustness of heterogeneous Internet of Things," *Comput. Netw.*, vol. 101, pp. 127–143, Jun. 2016, doi: 10.1016/j.comnet.2015.12.019.

[23] T. Qiu, A. Zhao, F. Xia, W. Si, and D. O. Wu, "ROSE: Robustness strategy for scale-free wireless sensor networks," *IEEE/ACM Trans. Netw.*, vol. 25, no. 5, pp. 2944–2959, Oct. 2017, doi: 10.1109/TNET.2017.2713530.

[24] T. Qiu, J. Liu, W. Si, and D. O. Wu, "Robustness optimization scheme with multi-population co-evolution for scale-free wireless sensor networks," *IEEE/ACM Trans. Netw.*, vol. 27, no. 3, pp. 1028–1042, Jun. 2019, doi: 10.1109/TNET.2019.2907243.

[25] M. Shafiq, Z. Tian, A. K. Bashir, X. Du, and M. Guizani, "CorrAUC: A malicious bot-IoT traffic detection method in IoT network using machine-learning techniques," *IEEE Internet Things J.*, vol. 8, no. 5, pp. 3242–3254, Mar. 2021, doi: 10.1109/JIOT.2020.3002255.

[26] M. Shafiq, Z. Tian, A. K. Bashir, X. Du, and M. Guizani, "IoT malicious traffic identification using wrapper-based feature selection mechanisms," *Comput. Secur.*, vol. 94, Jul. 2020, Art. no. 101863.

[27] M. Shafiq, Z. Tian, Y. Sun, X. Du, and M. Guizani, "Selection of effective machine learning algorithm and bot-IoT attacks traffic identification for Internet of Things in smart city," *Future Gener. Comput. Syst.*, vol. 107, pp. 433–442, Jun. 2020.

[28] M. Shafiq, Z. Tian, A. K. Bashir, A. Jolfaei, and X. Yu, "Data mining and machine learning methods for sustainable smart cities traffic classification: A survey," *Sustain. Cities Soc.*, vol. 60, Sep. 2020, Art. no. 102177.

[29] W. P. Tay, J. N. Tsitsiklis, and M. Z. Win, "On the impact of node failures and unreliable communications in dense sensor networks," *IEEE Trans. Signal Process.*, vol. 56, no. 6, pp. 2535–2546, Jun. 2008, doi: 10.1109/TSP.2007.914343.

[30] M. Hefeeda and M. Bagheri, "Randomized k-coverage algorithms for dense sensor networks," in *Proc. 26th IEEE Int. Conf. Comput. Commun. (IEEE INFOCOM)*, Anchorage, AK, USA, May 2007, pp. 2376–2380, doi: 10.1109/INFCOM.2007.284.

[31] *The Role of IoT in Industrial Automation*. Accessed: Jun. 10, 2023. [Online]. Available: https://www.hitachivantara.com/en-hk/insights/faq/what-is-the-role-of-iot-in-industrial-automation.html

[32] B. Pradhan, S. Bhattacharyya, and K. Pal, "IoT-based applications in healthcare devices," *J. Healthcare Eng.*, vol. 2021, Mar. 2021, Art. no. 6632599.

[33] C. M. Schneider, A. A. Moreira, J. S. Andrade, S. Havlin, and H. J. Herrmann, "Mitigation of malicious attacks on networks," *Proc. Nat. Acad. Sci. USA*, vol. 108, no. 10, pp. 3838–3841, Mar. 2011, doi: 10.1073/pnas.1009440108.

[34] A. Zeng and W. Liu, "Enhancing network robustness against malicious attacks," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 85, no. 6, Jun. 2012, Art. no. 066130, doi: 10.1103/physreve.85.066130.

[35] G.-G. Wang, S. Deb, and L. D. S. Coelho, "Elephant herding optimization," in *Proc. 3rd Int. Symp. Comput. Bus. Intell. (ISCBI)*, Bali, Indonesia, Dec. 2015, pp. 1–5, doi: 10.1109/ISCBI.2015.8.

[36] W. Li and G.-G. Wang, "Elephant herding optimization using dynamic topology and biogeography-based optimization based on learning for numerical optimization," *Eng. Comput.*, vol. 38, no. S2, pp. 1585–1613, Feb. 2021, doi: 10.1007/s00366-021-01293-y.

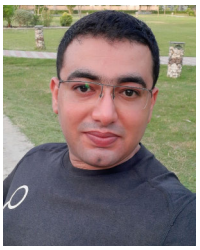
[37] J. Li, H. Lei, A. H. Alavi, and G.-G. Wang, "Elephant herding optimization: Variants, hybrids, and applications," *Mathematics*, vol. 8, no. 9, p. 1415, Aug. 2020, doi: 10.3390/math8091415.

[38] Y. Duan, C. Liu, S. Li, X. Guo, and C. Yang, "Gradient-based elephant herding optimization for cluster analysis," *Appl. Intell.*, vol. 52, no. 10, pp. 11606–11637, Jan. 2022, doi: 10.1007/s10489-021-03020-y.

[39] S. Prendeville, E. Cherim, and N. Bocken, "Circular cities: Mapping six cities in transition," *Environ. Innov. Societal Transitions*, vol. 26, pp. 171–194, Mar. 2018, doi: 10.1016/j.eist.2017.03.002.

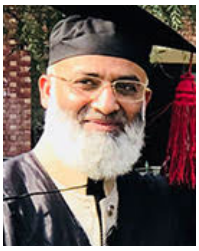
[40] T. Qiu, Z. Lu, K. Li, G. Xue, and D. O. Wu, "An adaptive robustness evolution algorithm with self-competition for scale-free Internet of Things," in *Proc. IEEE Conf. Comput. Commun. (IEEE INFOCOM)*, Toronto, ON, Canada, Jul. 2020, pp. 2106–2115, doi: 10.1109/INFOCOM41043.2020.9155426.

[41] N. Chen, T. Qiu, Z. Lu, and D. O. Wu, "An adaptive robustness evolution algorithm with self-competition and its 3D deployment for Internet of Things," *IEEE/ACM Trans. Netw.*, vol. 30, no. 1, pp. 368–381, Feb. 2022, doi: 10.1109/TNET.2021.3113916.



TALHA NAEEM QURESHI received the bachelor's degree in computer engineering from COMSATS University Islamabad Wah Campus, and the M.S. degree in electrical engineering from the Communications over Sensors (ComSens) research laboratory, Department of Computer Science, COMSATS University Islamabad, Islamabad Campus under the supervision of Prof. Dr. Nadeem Javaid. He is currently pursuing the Ph.D. degree in computer science under the supervision of Prof. Dr. Nadeem Javaid. He has ten international conference proceedings and three international journal publications. His research interests include the Internet of Things, wireless sensor networks, and energy management in smart grids.

ZAHOOR ALI KHAN is currently the Division Chair of the Computer Information Science (CIS) Division and the Applied Media Division, Higher Colleges of Technology, United Arab Emirates. He has more than 19 years of research and development experience. His current research interests include e-health pervasive wireless applications, theoretical and practical applications of WSNs, smart grids, and the IoT. He is an editorial board member of several prestigious journals. He is a Senior Member of IAENG. His several conference papers have received the Best Paper Award from BWCCA 2012, IEEE ITT 2017, and EIDWT-2019. He also serves as a regular reviewer/organizer for numerous reputed journals, conferences, and workshops.



NADEEM JAVAID (Senior Member, IEEE) received the bachelor's degree in computer science and physics from Gomal University, Dera Ismail Khan, Pakistan, in 1995, the master's degree in electronics from Quaid-i-Azam University, Islamabad, Pakistan, in 1999, and the Ph.D. degree from the University of Paris-Est, France, in 2010. He has Teaching and Research Experience of 25 years. He has worked as a Visiting Professor at the University of Technology Sydney, Australia. He is currently a Tenured Professor and the Founding Director of the Communications Over Sensors (ComSens) Research Laboratory, Department of Computer Science, COMSATS University Islamabad, Islamabad Campus. He has supervised 187 master's and 30 Ph.D. theses. He has authored over 950 papers in technical journals and international conferences. His research interests include energy optimization in smart/microgrids and wireless sensor networks using data analytics and blockchain. He was a recipient of the Best University Teacher Award (BUTA'16) from the Higher Education Commission (HEC) of Pakistan, in 2016, and the Research Productivity Award (RPA'17) from the Pakistan Council for Science and Technology (PCST), in 2017. He is an Editor of Sustainable Cities and Society journal. He has also worked as an Associate Editor of IEEE Access Journal.

ABDULAZIZ ALDEGHEISHEM received the Ph.D. degree in urban planning and spatial information from the University of Illinois at Urbana–Champaign, USA. He was the Head of the Department of Urban Planning, in 2012. He was an adviser to several government agencies and supervised many projects and specialized studies. He is currently the Dean of the College of Architecture and Planning, King Saud University, and a Professor with the Department of Urban Planning. He is also an Adviser with the Vision Realization Office (VRO), King Saud University, and the Supervisor of the Traffic Safety Technologies Chair. His research interests include spatial information in urban planning and management, also he focuses on areas related to city planning, spatial management, and smart city technologies.

MUHAMMAD BABAR RASHEED (Senior Member, IEEE) received the master's and Ph.D. degrees from COMSATS University, Islamabad, in 2013 and 2017, respectively. He was a GET-COFUND Marie Curie Fellow with Universidad de Alcal' (UAH), Spain. Previously, he was an Associate Professor and an Assistant Professor with the Department of Electronics and Electrical Systems, The University of Lahore, Pakistan. He obtained postdoctoral fellowships from Durham University, U.K., and King Abdulaziz University (KAU), Saudi Arabia, in 2019 and 2020, respectively. He is currently a Lecturer with the University of Gloucestershire, U.K. He has authored over 40 peer-reviewed papers in well-reputed journals and conference proceedings and supervised/supervising more than ten students in their final year projects and theses. His research interests include LP, NLP, heuristic optimizations, machine learning, smart grids, electric vehicles, and demand response. He is an active Reviewer of many esteemed journals and conferences, including IEEE Transactions, IEEE Access, IEEE Transactions on Industry Applications, *Applied Energy*, and *Energies*.

NABIL ALRAJEH received the Ph.D. degree in biomedical informatics engineering from Vanderbilt University, USA. Currently, he is a Professor of Health Informatics at King Saud University. He worked as a Senior Advisor for the Ministry of Higher Education, his role was implementing development programs including educational affairs, strategic planning, and research and innovation. He served as a member of the boards of trustees for five private universities in Saudi Arabia. His research interests include E-health Applications, Hospital Information Systems, Telemedicine, Healthcare applications of smart cities, and Wireless Sensor Networks.