Computationally Efficient Topology Optimization of Scale-Free IoT Networks

Muhammad Awais Khan[a], Nadeem Javaid[b,c,*]

[a]Department of Electrical and Computer Engineering, COMSATS University Islamabad, Islamabad 44000, Pakistan,
[b]Department of Computer Science, COMSATS University Islamabad, Islamabad 44000, Pakistan,
[c]School of Computer Science, University of Technology Sydney, Ultimo, NSW, 2007, Australia.

ARTICLE INFO

Keywords:
Betweenness Centrality
Closeness Centrality
Heat Map Centrality
Malicious Attacks
Scale-Free IoT Networks

ABSTRACT

The malicious attacks in the scale-free Internet of Things (IoT) networks create a serious threat for the functionality of nodes. During the malicious attacks, the removal of high degree nodes greatly affects the connectivity of the remaining nodes in the networks. Therefore, ensuring the maximum connectivity among the nodes is an important part of the topology optimization. A good scale-free network has the ability to maintain the functionality of the nodes even if some of them are removed from the network. Thus, designing a robust network to support the nodes' functionality is the aim of topology optimization in the scale-free networks. Moreover, the computational complexity of an optimization process increases the cost of the network. Therefore, in this paper, the main objective is to reduce the computational cost of the network with the aim of constructing a robust network topology. Thus, four solutions are presented to reduce the computational cost of the network. First, a Smart Edge Swap Mechanism (SESM) is proposed to overcome the excessive randomness of the standard Random Edge Swap Mechanism (RESM). Second, a threshold based node removal method is introduced to reduce the operation of the edge swap mechanism when an objective function converges at a point. Third, multiple attacks are performed in the network to find the correlation between the measures, which are degree, betweenness and closeness centralities. Fourth, based on the third solution, a Heat Map Centrality (HMC) is used that finds the set of most important nodes from the network. The HMC damages the network by utilizing the information of two positively correlated measures. It helps to provide a good attack strategy for robust optimization. The simulation results demonstrate the efficacy of the proposed SESM mechanism. It outperforms the existing RESM mechanism by almost 4% better network robustness and 10% less number of swaps. Moreover, 64% removal of nodes helps to reduce the computational cost of the network.

1. Introduction

The Internet of Things (IoT) has become an essential technology nowadays. Its integration with the Wireless Sensor Networks (WSNs) provides good support to the research community. The IoT-WSNs have various applications including intelligent transportation [1], smart environmental monitoring [2], smart cities, etc. An important characteristic of the IoT-WSNs is that they are operational even in hostile environments [3]. The IoT-WSNs consist of sensor nodes connected with the Internet to perform their functions without any human interaction. The activities of the sensor nodes help the researchers to explore the behavior of many real-world networks.

A lot of researchers have put their efforts to study the properties of different IoT-WSNs [4], [5]. Among these networks, the complex networks have high importance over other networks due to their dense nature. These networks have two classic network models, namely, a small-world network model [6] and a scale-free network model [7]. The small-world networks have a high clustering coefficient and a low average distance. They are generally used for modeling the topology in heterogeneous networks [8]. On the other hand, the scale-free networks are generally used for modeling the topology in homogenous networks [9] due to similar bandwidth and transmission range.

An important property of the scale-free networks is that most of the nodes in the networks are low degree nodes while few nodes have a high degree. Therefore, the scale-free networks become more vulnerable to malicious attacks by removing the most important nodes from the networks. Such attacks split the networks into multiple independent graphs [10] and paralyze them with time. A network is robust if it has the ability to withstand against node or link removal from the network. Therefore, a robust topology designing is a common application in the scale-free networks. The common measure for evaluating the robustness of the network is proposed by Schneider *et al.* [11] that considers removing the nodes one by one until the entire network becomes paralyzed. The network robustness R is calculated by analyzing the connectivity of the nodes in the network, and it is used in a number of research papers including [11, 12, 13, 14].

In the scale-free networks, the nodes which act as hubs are considered as the most important nodes and the removal of these nodes creates a serious threat to the network's connectivity. Due to the node removal, the connections of the remaining nodes are deeply affected, which reduces the network performance. The connectivity of the nodes is important to maintain network's functionality. Therefore, the goal is to propose a network, which maintains high robustness against the node removal. Addition or deletion of links

*Corresponding author
awaixmuhammad051@gmail.com (M.A. Khan);
nadeemjavaidqau@gmail.com (N. Javaid)
ORCID(s):

Table 1
List of Abbreviations and Mathematical Symbols

Notation	Description
AI	Artificial Intelligence
BA	Barabasi Albert
CI	Cumulative Influence
DDLP	Deep Deterministic Learning Policy
GA	Genetic Algorithm
HMC	Heat Map Centrality
HC	Hill Climbing
MA	Multi Agent
ML	Machine Learning
RESM	Random Edge Swap Mechanism
SESM	Smart Edge Swap Mechanism
A	Adjacency Matrix
$ANNF$	Average Node's Neighbor Farness
CC	Closeness Centrality
r	Assortativity
m	Edge Density
G	Graph
MCS	Maximal Connected Subgraphs
N	Number of Nodes
NF	Node's Farness
NNF	Node's Neighbor Farness
α	Power Law Exponent
R	Robustness
s	Shortest Path

between the nodes increases the network robustness, however, it also increases the computational cost of the network by increasing the nodes' degree distribution. Therefore, an edge swap mechanism is adopted to reduce the cost. The edge swap mechanism increases the network robustness by keeping the nodes' degree distribution unchanged. A similar edge swap mechanism is introduced using Hill Climbing (HC) algorithm [11], where edge swap is performed by selecting two random independent edges from the network for the construction of an optimized scale-free topology. The edge swap mechanism adopted by ROSE [13] uses the degree difference and angle sum operations to increase the network robustness. However, the random selection of edges in HC and ROSE increases the number of redundant operations and computational cost of the network. Furthermore, there are some other factors as well that increase the computational cost of the network. Among them is the convergence of an objective function after its limit is achieved and obtaining similar results after further optimization. For topology optimization case, performing unnecessary edge swaps does not provide an optimized scale-free topology, except it increases the cost of the optimization process. Also, the removal of nodes based on degree and betweenness in [14] shows success because of a strong positive correlation between them. However, the betweenness centrality has high computational cost [15]. Moreover, making the network robust against different types of malicious attacks is a complex problem in the scale-free networks and the attacker removes the nodes based on their importance like degree, betweenness, closeness, etc.

To find the hub nodes from the networks, some other measures [16, 17, 18, 19] are also proposed. However, these measures are designed for large-scale networks whereas, our proposed model is a small-scale network. If these measures are considered in the proposed model, their efficacy in finding the hub nodes will be compromised due to the following reasons.

1. The Cumulative Influence (CI) index [16] only provides the local information of nodes [17]. It effectively evaluates the nodes' importance for large-scale networks. However, for small-scale networks, the global information is also required to judge the nodes' importance [15]. Therefore, CI index cannot effectively find the hub nodes in small-scale networks. Besides, the degree centrality measure used in our work also provides the local information of nodes. However, the measure is computationally efficient and adopted by our base schemes, i.e., HC and ROSE. On the other hand, the closeness and betweenness centralities are global measures that provide the impact of a node on all the other nodes in the network. Thus, they are optimal measures to evaluate nodes' importance for small-scale networks.
2. The belief propagation [17] and explosive immunization [18] methods evaluate the nodes' importance effectively. However, both methods are computationally complex, resource constrained and are not suitable for the proposed network, where resource constrained nodes are used. On the other hand, the degree, betweenness and closeness measures used in proposed model require simple calculations. Thus, they are suitable for our network.
3. The CoreHD [19] is a computationally efficient index for evaluating the nodes' importance in a core-based network. However, our proposed model is not based on cores. The construction of a core-based network requires a complete change of the proposed network topology, which is not suitable in this case.
4. The measures used for the evaluation of nodes' importance in [20] are designed for multiplex networks and have high computational cost. Whereas, our proposed model is a single resource constrained network. If these measures are used for finding the hub nodes from the network, it will increase the computational cost of the network. Thus, these measures are not suitable for our proposed model. The degree, closeness and betweenness centrality measures used in the proposed model use less computational cost to evaluate the node's importance. Thus, they are suitable for our model.

1.1. Contributions

In this paper, we address the aforementioned problems in the scale-free networks and present our model to solve them with less computational cost. It is important to note that in this work, it is found that the high computational cost of the network is due to the excessive use of random edge swaps. Therefore, it is necessary to validate the effectiveness of the proposed model with less number of swaps to achieve high network robustness. Moreover, in this paper, the term robustness, $\boldsymbol{R}$, and network robustness are used alternatively. Also, scale-free networks and scale-free IoT-WSNs are alternate terms used in this paper. Our contributions in this work are summarized as follows.

1. Aiming to overcome the randomness of edge swap, a Smart Edge Swap Mechanism (SESM) is proposed to evaluate the network robustness against the malicious attacks. The proposed SESM is used to optimize the network robustness of HC and ROSE. The SESM integrated models are known as HC-Smart and ROSE-Smart, respectively.
2. A threshold based node removal method is introduced to reduce the computational complexity of the network. It tackles the problem of performing unnecessary topology optimization when a convergence is achieved.
3. For the construction of a robust scale-free topology, three important measures are considered, which are named as degree, betweenness and closeness. The Pearson correlation coefficient is used to find two strong positively correlated measures that can be used simultaneously.
4. Considering that multiple attacks can occur on the network, the scale-free topologies are optimized using a centrality measure named as Heat Map Centrality (HMC).

1.2. Organization

The organization of this paper is as follows. In Section 2, we discuss related work. The scale-free network modeling is discussed in Section 3. The topology optimization using the proposed solutions is performed in Section 4 and their performances are evaluated in Section 5. The paper ends with the conclusion and future work in Section 6.

2. Related Work

This section provides the literature review of different papers and categorizes them based on their work.

2.1. Construction of a Robust Topology using an Edge Swap Mechanism

In the scale-free networks, an attacker removes the high degree nodes that maintain the stability of the networks [12, 13] and the addition of new edges in the network is a good choice to overcome the loss caused due to the malicious attacks. However, the addition of edges increases the cost of the network. Therefore, the authors optimize the network robustness through an edge swap mechanism by performing malicious attacks on the nodes. However, the degree of a node is not the only parameter to measure its importance and the attacker can use other important parameters like betweenness, closeness, etc., to attack the nodes. The work in [14] is based on a fault-tolerant model, which shows high network robustness against random node failure and low robustness against the malicious attacks. Moreover, the authors in [21] highlight the importance of the scale-free networks and find that constructing a robust network topology against the malicious attacks is a significant challenge in the optimization problem. However, both aforementioned models perform edge swap to increase the network robustness of the scale-free networks. However, they require a complete knowledge of the scale-free network topology to perform edge swap. In [22], the authors analyze the threats of malicious attacks on an Artificial Intelligence (AI) community and inform that many algorithms involving Machine Learning (ML) are fragile against malicious attacks. However, these algorithms do not ensure a reliable and robust scale-free topology. Thus, the authors introduce a model, which performs different rewiring mechanisms to increase the network robustness. Still the link addition and deletion increase the network's cost and change the degree distribution of the nodes.

2.2. Construction of a Robust Topology using Evolutionary Mechanism

In [23], the authors find that the addition of the links increases the cost of the network. The conventional Genetic Algorithm (GA) is a good example of an evolutionary algorithm that optimizes the network robustness. However, the premature convergence in GA reduces the exploration capability and lowers the performance of the network against the malicious attacks [24]. Therefore, the authors use Multi-Population Genetic Algorithm (MPGA) to increase the network robustness. However, both GA based schemes increase the computational complexity of the network. Moreover, a similar issue is raised in [25], where the authors state that improving the robustness of the scale-free network against the malicious attacks is a complex problem. Therefore, the authors propose a model, which shows high robustness against the malicious attacks. However, it increases the network's computational complexity because it involves different measures to adjust the crossover and mutation rate adaptively. The authors in [26] address the malicious attacks on a Multi Agent (MA) network. However, the research focuses only on constructing a robust MA network without considering its deployment cost. Furthermore, the network robustness of the proposed scheme is only compared with the Barabasi Albert (BA) model [7]. The existing literature studies in [27] prove that it is necessary to involve both cooperation and robustness in constructing a robust network. However, the studies are only limited to undirected network. Therefore, a model is proposed to increase the network robustness for a directed network. However, it increases the computational complexity of the network. The authors in [28] reveal that node attacks and link attacks are negatively correlated. Therefore, multi-objective optimization is a better choice in this case. However, the computational costs for calculating the robustness of node and link attacks are different due to more number of links in the network as compared to nodes. Furthermore, the optimization of network robustness in the proposed scheme is performed for large area networks and is still an open challenge to minimize the computational cost for large-scale networks. Another attack strategy is introduced in [29], which measures the impact of the intentional attacks and analyze that they are harmful to the stability of the network. Therefore, the authors perform single objective optimization to increase the network robustness. However, the optimization strategies only deal with optimizing the robustness against the attacks. Also, considering only the degree information of the nodes in case of an attack is not the right choice as several nodes in the network have similar degrees, and choosing one node from multiple nodes involves randomness.

2.3. Construction of a Robust Topology using Machine Learning Techniques

The authors in [30] use an edge swap mechanism on randomly selected independent edges. However, the random edge swap mechanism increases the computational cost of the network because it performs large number of redundant operations. Thus, the proposed mechanism increases the network robustness through a deep learning mechanism. However, the optimal value of R is not successfully achieved because of insufficient model training and the solution converges towards the local optima. According to [31], the scale-free networks show vulnerability to malicious attacks. Thus, designing a robust mechanism against the attacks is challenging. The previous optimization strategies have optimized the network topology by maintaining the network's connectivity, however, the strategies increase the computational cost of the network. Due to the increasing demand for IoT devices, increasing the network robustness against malicious attacks is one of the challenging issues in the scale-free networks [32], which needs to be tackled. Thus, the proposed mechanism performs optimization using a Deep Deterministic Learning Policy (DDLP) method to increase the network robustness. However, it increases the computational complexity of the network.

2.4. Construction of a Robust Topology using the Cost of the Network

According to [33], most of the attack strategies remove all nodes in a specific order. However, the attack cost is involved in removing the nodes in a specific order. The proposed scheme provides a way to damage the network with little cost. However, considering both high degree and low degree node attacks simultaneously, damage the scale-free property of the network. Furthermore, removing a high degree nodes from the network costs more than removing a low degree node. Therefore, controlling the network robustness by considering the cost of the attacks is a major problem in a network [34]. Moreover, according to [35], the degree distribution of the nodes during the attack process is dynamic as it changes for each attack. However, both proposed models fail to consider ways to optimize the network robustness after the node removal.

2.5. Construction of a Robust Topology using Different Network Structures

The majority of the research studies in [36] test the network robustness against the random node removal, however, in general, the attacker tries to attack the most critical nodes in the network. Besides, the proposed model aims to reduce the cost of an interdependent directed network. The complicated structure of the directed network becomes an easier choice for the numerical simulations. However, the structure is not suitable for practical scenarios due to high computational cost. Based on the analysis of [37], measuring the network robustness against node and link removal is an open issue in the complex networks. The former measures for calculating the network robustness are natural connectivity, controllability robustness, etc. The measures are based on edge and node's connectivity, size of the largest connected component, etc. However, the measures have failed to express the network's capability in preserving the connectivity of the network. Therefore, a genetic based model is proposed to increase the network robustness by protecting the links in the network. However, due to premature convergence of GA, the proposed model does not provide optimal results. Moreover, due to the growing demand of the complex networks according to [38], there is also a concern of security issues related to these networks. Therefore, the authors focus on attacking the links in a single network. However, many networks are coupled with each other, and removing a link from a network brings great damage to other network as well. Thus, several core based attacks are performed to increase the network robustness against the links removal. Moreover, according to [39], the link addition strategy increases the cost of the network and changes the degree distribution of the nodes in the network. To keep the nodes' degree distribution unchanged and reduce the cost of the network, the edge swap mechanism is designed. However, the random edge swap mechanism increases the computational complexity of the network and performs many redundant operations during the optimization process.

2.6. Construction of a Robust Topology using Different Parameters

According to [40], the assortativity r and the power law exponent α are important factors in the scale-free networks, which help to create a strong interaction between the nodes. The value of r close to 1 tends to make a strong interaction between the nodes of similar degree. However, there is no evidence where the proposed model highlights the correlation between R and these measures. Moreover, in the proposed work, the improvement in robustness against the malicious attacks is satisfactory. However, in terms of random attacks, the proposed model fails to provide optimal results. Furthermore, the optimization of the network is important for the construction of a robust network. However, the authors do not perform optimization in the proposed work. The previous literature studies discussed in [41] reduce the cascading failure by considering the capacity of the nodes. However, they fail to analyze its effect on network recovery. The proposed research is helpful for the network with a fixed environment. However, its performance can be complicated in a dynamic environment. According to [42], the degree to degree correlation is an important factor for enhancing the robustness of the network. However, the Newman's research reveals that the enhancement of degree to degree correlation is limited to a certain degree threshold under malicious attacks. The addition of edges in the proposed work improves the network robustness, however, this process increases the cost of the network. Moreover, the addition of edges alters the degree distribution of the nodes, thus, damages the scale-free property of the network.

Based on the literature, we analyze that the computational complexity of the optimization process is very important in the scale-free networks. It is because, due to a large number of redundant operations in the previous edge swap mechanisms, the convergence operation slows down. From the previously discussed literatures, we can say that the authors do not focus on minimizing the number of redundant operations in the networks, which is the main operation for the evaluation of network robustness. It is therefore necessary to reduce the number of redundant operations for the construction of a robust scale-free topology. Furthermore, the convergence of an operation after a threshold and the integration of different attack strategies with the proposed SESM mechanism help to provide a computationally efficient robust network topology, which can outperform HC and ROSE.

3. Scale-Free Network Modeling

In this section, we discuss the construction of a scale-free network, its robustness measure and the independent selection of edges from the network.

3.1. Construction of a Scale-Free Network

The authors consider a BA model [7] that utilizes the information of the initially deployed nodes to construct a scale-free network topology. The preferential attachment property of the BA model allows the newly added nodes to make connections with the high degree nodes in the network. However, due to the limited transmission range, the newly joined nodes have limited neighbors in their communication range. Also, it is important for the nodes in the network to have sufficient neighbors in their communication range due to the growing demand of dense network topologies in the future. The ROSE emphasizes the importance of the dense WSNs and takes into account the communication range of nodes in the network. The communication range in ROSE allows the nodes to connect with 50% of the nodes in the network, making it a dense scale-free network. Moreover, the ROSE analyzes that for limited transmission range, the division of a network into multiple clusters is a good choice to develop a robust network. Therefore, the following aspects of ROSE are considered in the proposed model for the construction of the scale-free network.

1. The preferential attachment property of a node is limited to its nodes, which are within its communication range.
2. Considering the limited resources of the nodes in IoT-WSNs, their maximum degree is limited to a certain threshold.
3. The high degree nodes must be located in the center of the network.

3.2. Network Robustness Measure

In the scale-free networks, the attacker can attack the nodes as well as the links to destroy the connectivity of the nodes in the network. Generally, the attacks can be random or malicious. The random attacks remove random nodes while the malicious attacks remove the most important nodes from the network. In the scale-free networks, we use malicious attacks, which remove the high degree nodes and damage the connectivity of the network. Initially, the degrees of nodes are calculated and the node with the highest degree is removed. Also, the edges connected with the node are also removed. Then, the degree of the nodes is recalculated and the highest degree node is removed again. The process is repeated many times until all nodes are removed from the network.

For calculating the network robustness, a metric R proposed by Schneider *et al.* [11] is used based on percolation theory. When a node is removed from the network, the graph is divided into multiple subgraphs. The connectivity of the nodes is checked and the subgraph where the nodes are maximally connected is considered for the evaluation of R. We take the mathematical equation from [13] for evaluating the robustness, which provides the information of the nodes in the maximal connected subgraphs after removing nth nodes from the network. The equation for evaluating the robustness in [11] also provides the number of nodes information in the maximal connected subgraphs, however, it considers the fraction of nodes, which needs to be removed in order to disconnect the entire network. Both are similar in terms that they both provides the information of the network connectivity after repeated removal of nodes in the network. The equation for evaluating the network robustness [13] is given as follows.

$$R = \frac{1}{N+1}\sum_{n=0}^{N-1}\frac{MCS_n}{N} \quad . \tag{1}$$

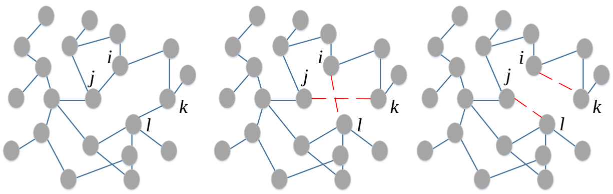
From Equation (1), N denotes the total number of nodes and MCS_n denotes the maximal connected subgraphs after nth highest degree node removal from the network [13].

3.3. Network Optimization through Selection of Independent Edges

In the scale-free networks, the optimization is performed through edge swap mechanism by selecting two independent edges from the graph $G = (V, E)$. Where, V represents the

Table 2
Limitations Identified, Proposed Solutions and Validations

Limitations Identified	Solutions Proposed	Validations Done
L1: Random selection of independent edges increases the computational cost of the network.	S1:SESM reduces the randomness through a smart selection of edges.	V1: The performance of the network is validated through R (Figure 10a and Figure 10b) and number of swaps (Figure 11a and Figure 11b).
L2: The computational cost is increased by performing unnecessary removal of nodes after the convergence is achieved.	S2: We analyze the robustness value and set a threshold for node removal to reduce the computational cost.	V2: The efficacy of the network is validated using MCS/N for node removal in the network (Figure 5).
L3: Multiple attacks can happen on the network simultaneously.	S3: Finding the two strong positively correlated measures to make the network robust against multiple attacks.	V3: The validation is provided using Pearson correlation coefficient (Figure 3), execution time (Figure 6 and Figure 7) and R (Figure 9).
L4: Finding the set of most influential nodes in the network that can damage the network in less time is a challenging task.	S4: HMC reduces the computational cost of the network by damaging the network to a greater extent.	V4: The performance parameters used for validation are R (Figure 10b) and number of swaps (Figure 11b).



(a) Initial Topology (b) Swap 01 (c) Swap 02

Figure 1: Edge Swap Mechanism

set of nodes and E represents the set of edges. The two selected edges are said to be independent if they lie within the communication range of each other and there is no extra connection between these two edges. Figure 1a shows that $e_{i,j}$ and $e_{k,l}$ are the independent edges. Figure 1b and Figure 1c show the edge swap performed on these independent edges.

The optimization of the network robustness against the malicious attacks is evaluated by swapping the independent edges in the network. The edges are swapped in such a way that the updated topology increases the network robustness against the malicious attacks. If the first swap increases the network robustness, the topology is updated. If the first swap has low robustness value, the second swap is performed and the topology is updated only if it increases the robustness. If both swaps fail to optimize the network robustness, the original topology is considered in the network.

4. Computationally Efficient Topology Optimization: Overview

This section describes our proposed topology optimization mechanism where we identify four limitations. Each limitation is associated with the optimization of the network robustness in the scale-free network, as shown in Figure 2. The limitations are denoted as L1, L2, L3 and L4, while their proposed solutions are provided using S1, S2, S3 and S4, respectively. Table 2 shows the mapping of these limitations with their proposed solutions and validations. L1 and L2 mentioned in Table 2 are associated with the limitations in the previous edge swap mechanism based on redundancy and computational cost of the network. These limitations are tackled using SESM and threshold based node removal, respectively. The validation for both these solutions is done using R, number of swaps, MCS, etc.

For L3, the issue of multiple attacks on the network is tackled using S3, where a combined attack strategy of the two strongly correlated measures is needed. In contrast, L4 is associated with finding an attack measure to damage the network's connectivity in quick time, as mentioned in Table 2. Therefore, S4 introduces a measure named as Heat Map Centrality (HMC) to overcome L4. We discuss the solution of each limitation in the given subsections.

4.1. Smart Edge Swap Mechanism

Due to the involvement of randomness in the edge swap mechanism used in HC and ROSE, many redundant operations are generated in the optimization of the network robustness. Specifically, in HC, the edge swap mechanism increases the number of redundant operations in the network because it does not mark the independent edges after their selection. Thus, these edges are selected again in the optimization process, which results in increasing the number of redundant operations in the network. In ROSE, the marking of independent edges reduces the redundancy of the network. However, the random edge swap mechanism happens on low degree edges in the network, which results in providing low robustness against the malicious attacks with the high computational cost. Therefore, a new selection criteria for independent edges is required to overcome the redundancy issue and increase the network robustness. It is known that the high degree nodes are the main target of the attacker and the

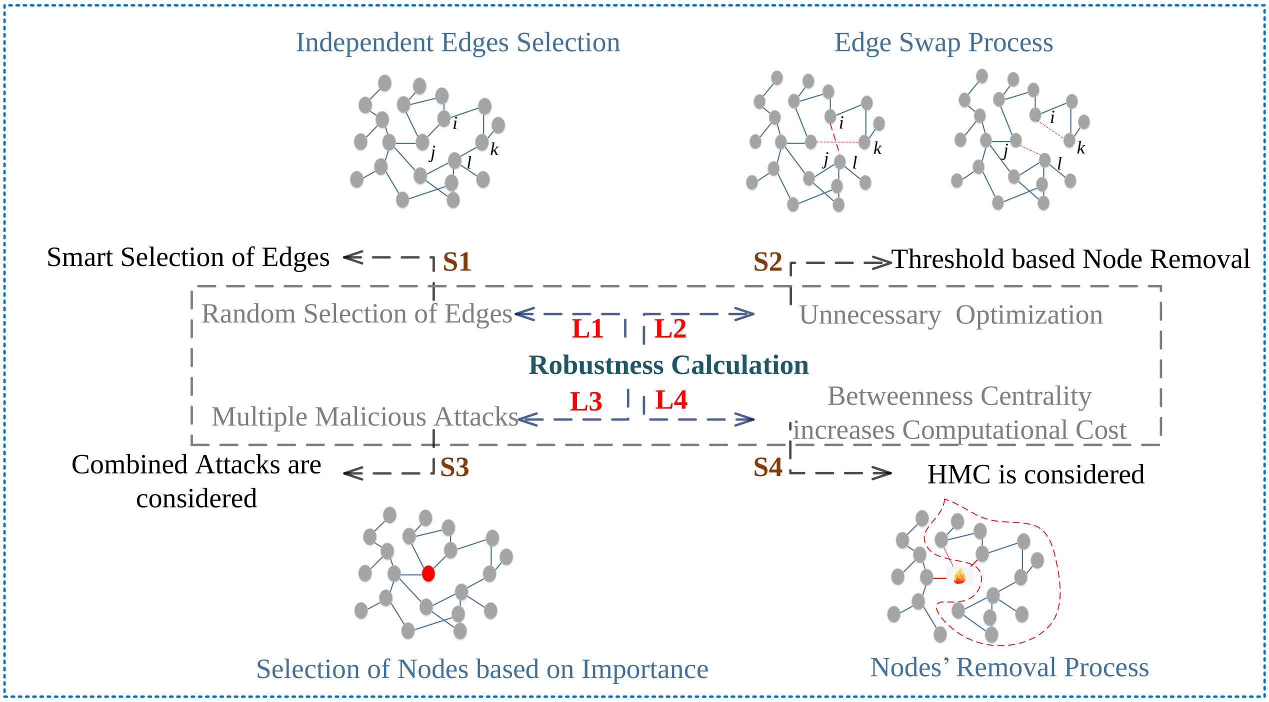

Independent Edges Selection
Edge Swap Process
i
j
k
l
Smart Selection of Edges
S1
S2
Threshold based Node Removal
Random Selection of Edges
L1
L2
Unnecessary Optimization
Robustness Calculation
Multiple Malicious Attacks
L3
L4
Betweenness Centrality increases Computational Cost
Combined Attacks are considered
S3
S4
HMC is considered
Selection of Nodes based on Importance
Nodes' Removal Process

Figure 2: Limitations Identified and their Proposed Solutions

removal of high degree nodes damages the topology of the network. Therefore, based on the information of the high degree nodes, one can protect the connectivity of the nodes by altering their connections. Furthermore, it is understood that one high degree node replaces other high degree node in the network. Thus, changes in the connections of these nodes can bring a significant improvement in the network. Besides, an onion-like structure has strong tolerance against the malicious attacks and in the structure, the high degree nodes are tightly connected with other high degree nodes. Therefore, the edge swap mechanism based on high degree nodes is a good choice to construct an onion-like structure.

For L1, as shown in Table 2, the problem of edge randomization is controlled through the selection of high degree nodes. The SESM is proposed to overcome the random selection of the independent edges in the previous Random Edge Swap Mechanism (RESM). For the initial topology, a set of high degree nodes is selected from the network. From the set, two high degree nodes are selected before performing the edge swap mechanism. The information of the neighboring nodes of these two selected nodes is extracted. The selection process of finding a node from the neighbors' set is a complex problem as each node has multiple neighbors. Therefore, to avoid this problem, a random neighbor is selected from the neighbor's set. The information of the selected neighbor is utilized for the selection of independent edges. The independence of the selected edges is checked. If they are independent, the edge swap operation is performed, else the selection process continues to try further connections to find the independent edges. The edge swap mechanism swaps the edges of the network in search for a more optimized network topology.

Algorithm 1 Smart Edge Swap Mechanism

```
1: procedure SMART EDGE SWAP MECHANISM($A$)
2:     Input: $A$, $N$, $G$
3:     for all $N \in G$ do
4:         Find a high degree node $i$ from $N$
5:         Calculate neighbors of the high degree node
6:         Pick a neighbor randomly from the neighbors of node $i$ and mark it as $j$
7:         Perform steps 3-5 again for 2nd high degree node $k$ and its neighbor $l$
8:         $Swap_{counter} = 0$
9:         if $(i, j)$ and $(k, l)$ are two independent edges from the set $E$ then
10:            Perform optimization using HC and ROSE
11:            if swap is successful then
12:                Update $A$ and $G$
13:                Calculate $R$
14:                $Swap_{counter} = Swap_{counter} + 1$
15:            end if
16:        end if
17:    end for
18: end procedure
```

Algorithm 1 describes the process of SESM. The high degree node is selected from graph G, which consists of N number of nodes (Line 4). The neighbor of the selected node is chosen and the link between them is marked (i, j) (Line 6). The steps 3-5 are followed for other high degree nodes (Line 7). The swap counter is initialized (Line 8). If the selected edges (i, j) and (k, l) are independent, the edge swap mechanism is performed. For optimization, the operation of HC and ROSE are used (Line 10). If the swap is successful and the robustness is increased, the swap counter is incremented (Line 14).

4.2. Threshold based Node Removal

Several mechanisms including HC and ROSE increase the network robustness by focusing on changing the network topology through swapping. Due to the structural complexity of the network, optimizing the network robustness using an edge swap becomes a difficult task. Moreover, there is not enough evidence to guide the network to perform limited edge swaps. Besides, it is understood that the performance of the network is greatly reduced when a specific optimization task is performed continuously without any improvement. In the optimization process, analyzing the convergence of an objective function is an important factor. It is useless to perform unnecessary optimization for an objective function after its maximum value is achieved. In the topology optimization scenario, the objective is to maximize the network robustness by swapping the edges of the topology until a single node is left in the network. However, this type of process consumes excess memory and increases the computational cost of the network. Therefore, based on these problems, a threshold based node removal method is considered as mentioned in Table 2. The method considers removing the nodes one by one until convergence is achieved. The details of the proposed solution are described below.

Consider a network whose topology is constructed using the previous BA model. The preferential attachment property of the scale-free network guides the newly added node to connect with high degree nodes in the network. These nodes are added into the network one by one until a topology of the scale-free is generated. The network robustness is calculated for initial topology by removing the nodes one by one. For node removal, we have performed several experiments and found out that almost 60-65% node removal is enough to destroy the network's connectivity. The 60-65% node removal guides us to select a threshold value for node removal, where the robustness value reaches its maximum. Therefore, the node removal is performed based on the given threshold. For each node removal, the edge swap mechanism swaps the independent edges within the given threshold. The topology that maximizes the R value is considered for the construction of a robust scale-free network

In Algorithm 2, the threshold based node removal is discussed. The high degree node is removed from graph G (Line 6). The robustness R is calculated for each node removal (Line 7). If the value of R_k is greater than the value of R_{k-1}, the node removal process is repeated again until all nodes are removed from the network. If R_k is equal to the previous value R_{k-1} for consecutive node removal steps, the threshold value is recalculated. The optimization is performed using Algorithm 1 with the node removal at the given threshold (Line 12).

Algorithm 2 Threshold based Node Removal

```
1: procedure THRESHOLD BASED NODE REMOVAL($A$)
2:     Input: $A$, $N$, $G$
3:     for all $N \in G$ do
4:         for $k = 1 : N - 1$ do
5:             Find a high degree node $i$ from $N$
6:             Remove the node $i$ and update the topology from $G$ to $G_2$
7:             Calculate $MCS$ and evaluate network robustness $R_i$
8:             if $R_k > R_{k-1}$ then
9:                 Continue the removal process
10:            else if $R_k$==$R_{k-1}$ then
11:                Calculate the value for node removal where $R_k$==$R_{k-1}$
12:                Update the threshold for node removal and perform optimization through Algorithm 1 using the selected node removal phase
13:            end if
14:        end for
15:    end for
16: end procedure
```

4.3. Optimization of Network Considering Multiple Attacks

The authors in HC and ROSE have analyzed the network robustness against high degree node removal. They consider that the degrees of the nodes can provide more influential nodes from the network. However, the research performed in [14] has termed betweenness centrality as another metric to measure the most important nodes from the network. Therefore, in [14], the authors have combined both measures to find the attack probability of nodes. Still, they have failed to provide enough evidence about the importance of both these measures in terms of computational cost. The work proposed in [15] has discussed both these measures in terms of computational cost. The authors have considered the degree of nodes as an excellent parameter to find the local information of nodes. However, choosing betweenness centrality is not the best option because it increases the computational cost of the network [15].

To determine the relationship between any two measures, the Pearson correlation coefficient is used, which is a well-known correlated measure. In our scenario, initially, three attacks named as degree, betweenness and closeness are induced. Then, based on these attacks, three robustness measures are calculated. Afterwards, the Pearson correlation coefficient between the robustness of any two centrality measures is evaluated using the following formula.

$$r = \frac{N(\sum R_{C1} R_{C2}) - (\sum R_{C1})(\sum R_{C2})}{\sqrt{[N(\sum R_{C1}^2) - (\sum R_{C1})^2][N(\sum R_{C2}^2) - (\sum R_{C2})^2]}}, \tag{2}$$

From Equation (2), R_{C1} and R_{C2} are the evaluated robustness for any two centrality measures. Figure 3 shows the correlation comparison of the three centrality measures. From Figure 3, the strong positive correlation between degree and closeness attacks shows that both these measures can be considered simultaneously in an attack to improve the robustness. The idea of finding the correlation between the measures is adopted from [23], where the authors use two strong negatively correlated measures for multi-objective optimization. The optimization of both the measures are necessary to increase the robustness. Contrary to the aforementioned case, the strong positively correlated measures are combined together to improve the robustness. The reason is that the two positively correlated measures have no conflicts at all and their optimization leads to a similar network structure. It means that a topology which shows high robustness against degree and closeness attacks (strong positively correlated measures) also shows high robustness against the betweenness attack and the combination of any two attacks. It is to be noted that we only assume degree, closeness and betweenness attacks on the network. Moreover, if these two measures are used simultaneously to derive an attack strategy, it will prove to be helpful for the optimization of network robustness.

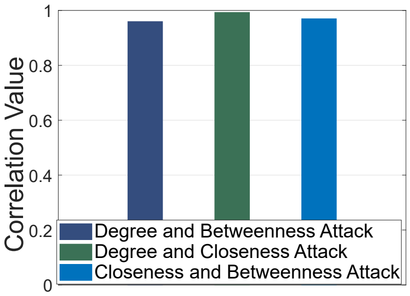


Figure 3: Pearson Correlation Bar Graph (Combined Attacks)

4.4. Heat Map Centrality

The importance of the nodes helps the attacker to damage the network to a greater extent. Finding the most important nodes from the network is challenging, as mentioned in Table 2. In ROSE, the degree of nodes is an important parameter to measure the importance of nodes from the network. Therefore, the attacker always removes high degree nodes from the network. However, if we consider the cost of removing high degree nodes from the network, the results can be costly. Furthermore, the attacker does not always consider removing the high degree nodes every time from the network. Therefore, another measure needs to be considered that can eliminate the most important nodes from the network. The study in [14] reveals that the nodes' betweenness centrality is another important parameter that measures the flow of information between the nodes in the network. As a result, the authors combine the betweenness centrality and degree to measure the importance of nodes in the network. However, the computational complexity for calculating the betweenness centrality is high for complex networks [15]. Furthermore, the betweenness centrality takes into account the shortest path calculation using the global information of all the nodes in the network. Therefore, the computational cost of the network is relatively high in this case.

The closeness centrality [15] is another important metric that measures the importance of nodes through calculating the sum of information of the shortest path between a particular node and all other nodes in the network. In terms of time complexity, closeness centrality has less computational time because it does not need to calculate the number of shortest paths that pass through particular nodes, which is required for the betweenness centrality. In this work, we use a node's importance metric HMC [15] that has a strong capability to damage the network. It uses the local and global information of the nodes in the network. The global information of the nodes is calculated using the farness of each node in the network. This farness is based on closeness centrality information. On the other hand, the local information of the nodes is evaluated using the degree's farness of each node. The node with small farness is considered the most important node in the network as most of the information is passed through the node. Therefore, the attacker attacks the nodes one by one with the small HMC_{value}. The steps for calculating HMC_{value} [15] for each node are given as under.

Step 1:
Calculate the Closeness Centrality (CC) of a node i using the shortest path s as shown in Equation (3):

$$CC(i) = \frac{1}{\sum_{j=1}^{N} s(i,j)} \quad . \tag{3}$$

Step 2:
Calculate Node's Farness (NF_i) using CC obtained from Equation (3):

$$NF_i = \frac{1}{CC(i)} \quad . \tag{4}$$

Step 3:
Calculate Node's Neighbor Farness (NNF), which utilizes the information of the adjacency matrix A and NF_i through Equation (4):

$$NNF_i = A * NF_i \quad . \tag{5}$$

Step 4:
Calculate Average Farness of Node's Neighbors ($ANNF_i$) utilizing the information of NNF_i in Equation (5) and degree of node i:

$$ANNF_i = \frac{NNF_i}{degree_i} \quad . \tag{6}$$

Step 5:
Calculate HMC_{value} using the difference of NF_i and $ANNF_i$ obtained from Equation (4) and Equation (6), respectively:

$$HMC_{value} = NF_i - ANNF_i \quad . \tag{7}$$

Algorithm 3 Nodes' Importance Measure

```
Input: $N, G$
Output: $A, R, MCS$
procedure HMC
    for all $N \in G$ do
        Evaluate CC of all nodes using (2)
        Calculate $NF_i$ using (3)
        Calculate $NNF_i$ using (4)
        Evaluate $ANNF_i$ using (5)
        Use (6) to calculate $HMC_{value}$
        Find a node $i$ with minimum $HMC_{value}$ from topology $G$
        Remove the node $i$ and update the topology from $G$ to $G_2$
        Calculate $MCS$ and evaluate network robustness $R$
    end for
end procedure
```

5. Simulation Results and Discussion

In this section, we compare the performance of our proposed solutions with the existing algorithms, namely HC and ROSE. A sensor field of 500x500 m^2 is considered and the transmission range of nodes is set to 200 m. The nodes are randomly deployed in the network . The number of nodes before the start of the network is set to 3. The newly added nodes then join the network one by one based on the preferential attachment. The newly added nodes make connections with $m = 2$ nodes. Due to the limited resources of sensor nodes, the maximum degree limit for the nodes is initially set to 25 for 100 nodes. The degree threshold increases to 30 when the number of nodes increases to 150 and so on. The simulations are performed on MATLAB, which is installed on Dell Latitude E6520 5th Generation system with 4GB RAM. The simulations are performed 50 times and the results are averaged across 20 independent runs.

5.1. Power Law Distribution

The degree distribution of the nodes in the scale-free network follows the power law distribution. Therefore, it is necessary to show that the degree of the nodes in the proposed network is distributed according to the power law. Figure 4 shows the power law distribution of the proposed network with $N = 100$ and $m = 2$. $P(d)$ denotes the probability of the nodes having degree d. The results show that the degree of the nodes is distributed according to the power law. It is clear that the probability of high degree nodes in the network is less than low degree nodes. Therefore, the proposed model has a scale-free network topology.

The degree distribution of the nodes in the scale-free network follows the power law distribution. Therefore, it is necessary to show that the degrees of nodes in the proposed network are distributed according to the power law. Figure 4 shows the power law distribution of the proposed network with $N = 100$ and $m = 2$. $P(d)$ denotes the probability of the nodes having degree d. The results show that the degrees of the nodes are distributed according to the power law. It is clear that the probability of high degree nodes in the network is less than low degree nodes. Therefore, the proposed model has a scale-free network topology.

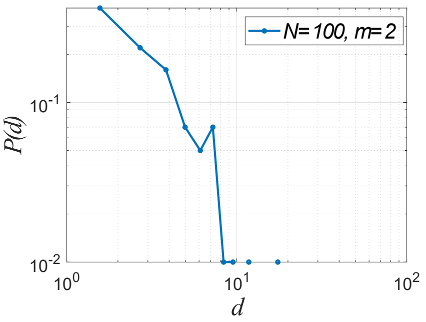


Figure 4: Power Law Distribution

5.2. Measuring the Extent of Damage Caused by Each Attack

To measure the extent of damage, we use the ratio of maximum connected nodes in a subgraph and the total number of nodes in the network (MCS/N). Figure 5 shows the connectivity of the nodes after the high degree nodes are removed from the network. It shows the extent of damage caused by each attack when all nodes are removed from the network. When 30 nodes are removed from the network, the betweenness attack initially causes more damage to the network as it performs efficiently when the solution space is large. However, when the number of removed nodes increases, the effect of the betweenness attack reduces. In that case, the closeness attack performs better in terms of damaging the network at a greater extent. From nodes the 50-90, the closeness attack causes more damage to the network as compared to the degree and betweenness attack. The closeness attack has a very strong positive correlation with degree attack. Therefore, it has more probability to provide more important nodes in the network. Also, its execution time is less as compared to the betweenness attack. Thus, it helps to reduce the complexity of the network by fragmenting it at a quick time compared to the betweenness attack.

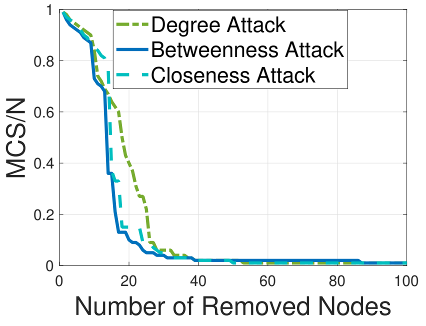


Figure 5: Extent of Damage

5.3. Execution Time of Different Attacks

The convergence of a certain objective function is directly related to the execution time of the algorithm designed for optimization. The high execution time results in providing less optimal results and vise versa. Figure 6 shows the execution time of each attack strategy in removing the nodes from the network. It is shown that the betweenness attack has less execution time when the number of removed nodes is less than 55 because the betweenness attack utilizes the number of paths information in the network. Also, the betweenness attack finds the nodes' importance based on the number of paths a node is a part of. As a result of the large number of links, the performance of the betweenness attack is improved. The number of paths reduces when the nodes are removed from the network, which results in removing the number of links. Therefore, the performance of the betweenness attack reduces when the number of removed nodes exceeds to 55, which in turn increases the time complexity of the network. On the other hand, the closeness attack has a greater execution time when the number of removed nodes is greater than 55. It is because the closeness attack has low performance to decide the importance of the nodes when a high number of links are present in the network. However, when the number of removed nodes exceeds 55, its execution time reduces and has closed intact with the degree attack. On average, it takes less time to execute than the betweenness attack, making it the better choice for use with the degree attack for single optimization. In Figure 7, multiple attacks are performed to evaluate the execution time of the network using degree, closeness and betweenness attacks. The result shows that the degree and closeness attack has less time consumption as compared to degree and betweenness attack. The performance of the degree and betweenness attack is better when few number of nodes are removed from the network. However, the difference between both combined attacks gradually decreases from 30 onwards and after the removed nodes reaches 60, the performance of the degree and closeness attack starts getting better and better. This shows that when more nodes are removed from the network, its effectiveness is increased. Therefore, the degree and closeness measures are used in the same attack as compared to the degree and betweenness or closeness and betweenness measures.

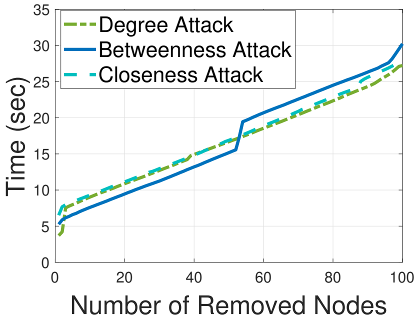


Figure 6: Execution Time (Single)

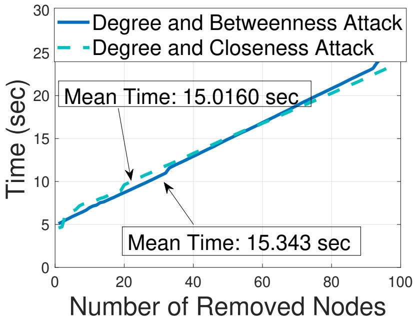


Figure 7: Execution Time (Combined)

5.4. Convergence of Robustness using the Degree Attack

An optimization process generates better results when the computational complexity of the network is decreased by reducing the number of nodes removed after the convergence is achieved. Figure 8 shows the convergence of R using the degree attack. The robustness in Figure 8 is evaluated by considering the node removal from initial network topology. It is observed that the convergence decreases when more nodes are removed from the network. Because robustness is directly linked with the connectivity of the nodes. Thus, removing more nodes lowers the connectivity of the network, which in turns reduces the robustness. It is evident that after removing 64 nodes, the convergence of the network remains constant. It means that the network is converged at a point. Therefore, removing only 64 nodes out of 100 reduces the computational complexity of the network. Moreover, the optimization of the network is directly related to the computational complexity of an objective function. Thus, when the computational complexity is reduced, better robustness value is achieved. Therefore, when the threshold value is set for node removal, the reduction of unnecessary swaps helps to develop a robust scale-free network.

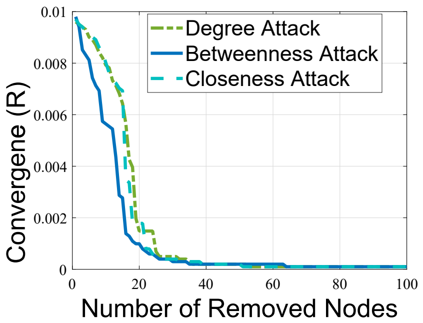


Figure 8: Convergence of Initial Network Topology

5.5. Initial Robustness Evaluation considering Multiple Attacks

Figure 9 shows the initial robustness evaluation considering combined attacks. The robustness is evaluated from the initial network topology by removing the nodes one by one. For each node removal, the robustness is evaluated through MCS. It is evident that the initial robustness of the degree and closeness attack is high as compared to the degree and betweenness attack. The total initial robustness for the degree and betweenness attack is 0.1425, while for the degree and closeness attack, it is 0.1438. The high value of robustness for the degree and closeness attack shows that both measures are strongly positive correlated with each other and they can be used simultaneously to damage the network at a greater portion. Moreover, both these measures have relatively less execution time and computational cost. Thus, when they are performed together, their average execution time is reduced. On the other hand, the execution time difference of the degree and betweenness attack is large. Also, the total damage caused by the betweenness attack is less as compared to the closeness attack. Therefore, the robustness of the the degree and betweenness attack is low. Hence, considering the degree and closeness attack for single objective optimization is a better choice to make a robust network topology.

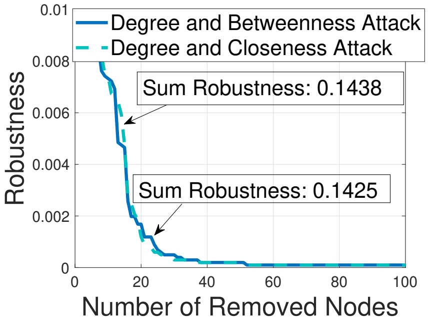


Figure 9: Robustness of Initial Network Topology

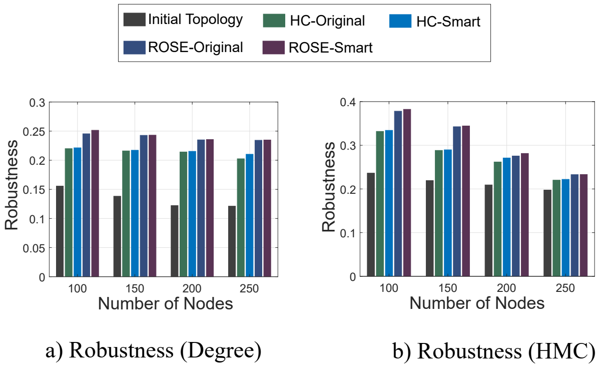
5.6. Robustness Analysis using Degree Attack and HMC Attack

The robustness of the network using the proposed SESM is evaluated for the degree attack and HMC attack with different node density. The performance of the proposed topology is compared with the initial topology, HC and ROSE. In HC and ROSE, the RESM is replaced with SESM and are named as HC-Smart and ROSE-Smart. Their performances are compared with HC-Original and ROSE-Original.

Figure 10a shows the robustness analysis of the proposed SESM using the degree attack on nodes. It is observed that the proposed HC-Smart and ROSE-Smart have achieved high robustness as compared to initial topology, HC-Original and ROSE-Original. This is due to the selection of high degree edges for swap that reduces the number of redundant operations of the previous RESM in HC and ROSE. SESM utilizes the information of high degree nodes to find more robust solutions in the network. Due to the predefined criteria for the selection of the independent edges, there is no chance of redundant operations in the network. Therefore, this mechanism gives a more optimized robustness value. For HC, the difference between HC-Original and HC-Smart is clearly seen for high node density. The high node density increases the number of edges as well as the number of redundant operations in the network. Thus, the improvement of HC-Smart at high density shows reduction of redundant operations in the network. For ROSE, the difference between ROSE-Original and ROSE-Smart is high when the number of nodes is 100. SESM shows better efficacy in reducing the number of redundant operations to increase the robustness. However, this difference decreases when the number of nodes is increased, which shows that both ROSE-Original and ROSE-Smart provide high robustness value. Still the effectiveness of ROSE-Smart is judged by the number of swaps in the network.

Both HC-Smart and ROSE-Smart perform better in constructing a robust scale-free network by utilizing high degree nodes' information. As high degree nodes are the important part of the network, the edge swap between high degree nodes plays a key role in constructing an onion-like topology. Moreover, HC-Smart and ROSE-Smart have shown better robustness for high network density, proving the efficacy of the SESM for the the degree attack. However, the decreasing trend of the robustness with the increasing network density is due to the high removal of nodes, which slows down the convergence operation.

From Figure 10b, it is seen that our proposed HC-Smart and ROSE-Smart achieve high robustness as compared to HC-Original and ROSE-Original. The SESM is performed using the HMC attack for node removal. Furthermore, the robustness value for HMC attack is high as compared to the degree attack because the optimization of the network using HMC attack is performed using both degree and closeness information of nodes. Thus, its robustness value is high as compared to the degree attack. A good centrality measure provides a way to protect the most important nodes in the network. Therefore, protecting these important nodes in the network overcomes the damage caused due to node removal. Moreover, both degree and closeness have less execution time, which is already shown in Figure 7. Therefore, the optimization using both measures gives better robustness value as it happens in quick time.



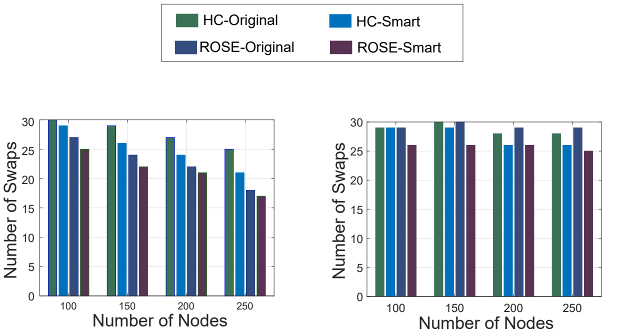
a) Robustness (Degree)

b) Robustness (HMC)

Figure 10: Robustness Analysis

5.7. Swap Cost using Degree Attack and HMC Attack

The computational complexity of the network is evaluated through the number of swaps in the network. The average results are taken for 10-20 independent runs. Figure 11a shows the number of swaps performed in the optimization process for finding a robust network topology. The performance of the proposed HC-Smart and ROSE-Smart is compared with HC-Original and ROSE-Original for both degree attack and HMC attack. It is seen that SESM reduces the computational complexity of the optimization process by reducing the number of swaps in the network. It is clear from the results shown in Figure 11a and Figure 11b that the convergence operation of the optimization process is inversely related to the number of swaps in the network. The high number of swaps slows down the convergence process. Because the algorithm has to evaluate the network robustness for all possible swaps in the network. In HC-Original and ROSE-Original, the RESM affects the performance of the network by reducing the network robustness. Because the RESM has excess memory consumption due to many redundant operations and it is not feasible to optimize robustness at a low computational cost. Moreover, it is seen that the difference between HC-Smart and HC-Original is more significant as compared to ROSE-Smart and ROSE-Original. This is due to the absence of marking the selected independent edges in HC, which increases the number of redundant operations in the network. ROSE performs edge swap by keeping the independent edges selected during the edge swap process. Therefore, it reduces the number of redundant operations. However, the random selection of independent edges continues to perform unnecessary optimization in search for a robust network topology. On the other hand, the SESM is used to overcome redundant operations. The result shows that HC-Smart and ROSE-Smart achieve great success in optimizing the robustness with a low number of swaps.

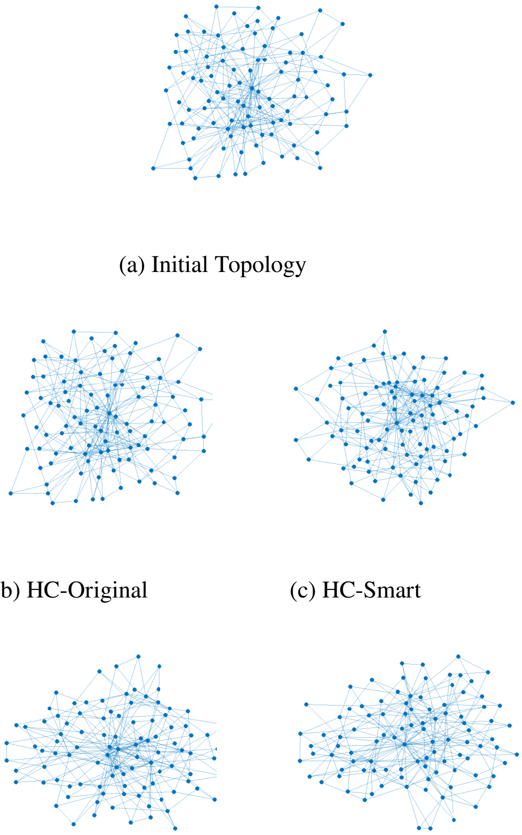


a) Number of Swaps (Degree)   b) Number of Swaps (HMC)

Figure 11: Number of Swaps

5.8. Topology Comparison

A perfect onion-like topology shows better robustness against the degree attack. Therefore, it is necessary for an optimized topology to have a perfect onion-like structure. From Figure 12, the network topology is visualized through a graph during the removal of high degree nodes. The results show that both HC-Smart and ROSE-Smart have constructed a better onion-like topology as compared to initial topology (Figure 12a), HC-Original (Figure 12b) and ROSE-Original (Figure 12d). Therefore, the optimization based on the SESM in Figure 12c and Figure 12d show better robustness against the degree attack through the construction of a robust network topology. Moreover, most of the nodes in the optimized network topologies are low degree nodes, which proves that our proposed SESM mechanism has maintained the property of the scale-free network.



(a) Initial Topology

(b) HC-Original   (c) HC-Smart

(d) ROSE-Original   (e) ROSE-Smart

Figure 12: Scale-Free Topology Comparison for $N = 100$ and $m = 2$ (Degree Attack

6. Conclusion and Future Work

Considering that the selection of random independent edges increases the computational complexity of the network; SESM is introduced to increase the network robustness. The proposed mechanism utilizes the information of high degree nodes to find independent edges in the network. The computational complexity is minimized through the reduction of the number of swaps in the network. The removal of important nodes from the network after the convergence is achieved further reduces the computational complexity of the network. Besides, HMC attack helps to damage the network quickly. Moreover, it optimizes the convergence speed of the network.

The degree distribution of the nodes in the proposed mechanism follows the power law distribution and constructs a better onion-like topology without changing the degree distribution of nodes. The performance of the proposed mechanism is optimized using HC and ROSE. The results show the efficacy of the proposed edge swap mechanism when compared with the original edge swap mechanism in HC and ROSE. With fewer swaps and a better onion-like topology, the proposed HC-Smart and ROSE-Smart improve the network robustness. For multiple attack scenarios, the degree and closeness attack shows high network robustness when the nodes are removed from the network. Therefore, selecting these two attacks is a good choice for network optimization. Thus, the HMC attack is designed to optimize the network robustness using both degree and closeness centrality.

For future work, we will test the efficacy of our proposed SESM for link removal as well. Moreover, an optimized topology will be constructed by analyzing the convergence of the robustness with respect to the number of nodes. The threshold based node removal method will aid in the development of a more robust network with a high node density. In addition, the solutions proposed in this paper will be tested on synthetic networks as well.

References

[1] Azpilicueta, L., Iturri, P.L., Aguirre, E., Astrain, J.J., Villadangos, J., Zubiri, C. and Falcone, F., 2015. Characterization of wireless channel impact on wireless sensor network performance in public transportation buses. IEEE Transactions on Intelligent Transportation Systems, 16(6), pp.3280-3293.

[2] Hodge, V.J., O'Keefe, S., Weeks, M. and Moulds, A., 2014. Wireless sensor networks for condition monitoring in the railway industry: A survey. IEEE Transactions on intelligent transportation systems, 16(3), pp.1088-1106.

[3] Wang, T., Zhou, J., Huang, M., Bhuiyan, M.Z.A., Liu, A., Xu, W. and Xie, M., 2018. Fog-based storage technology to fight with cyber threat. Future Generation Computer Systems, 83, pp.208-218.

[4] Yan, P., Choudhury, S., Al-Turjman, F. and Al-Oqily, I., 2020. An energy-efficient topology control algorithm for optimizing the lifetime of wireless ad-hoc IoT networks in 5G and B5G. Computer Communications, 159, pp.83-96.

[5] Priya, J.S., Saravanan, K. and Sathyabama, A.R., 2020. Optimized evolutionary algorithm and supervised ACO mechanism to mitigate attacks and improve performance of adhoc network. Computer Communications, 154, pp.551-558.

[6] Watts, D.J. and Strogatz, S.H., 1998. Collective dynamics of 'small-world'networks. nature, 393(6684), pp.440-442.

[7] Barabási, A.L. and Albert, R., 1999. Emergence of scaling in random networks. science, 286(5439), pp.509-512.

[8] Singh, S. and Andrews, J.G., 2013. Joint resource partitioning and offloading in heterogeneous cellular networks. IEEE Transactions on Wireless Communications, 13(2), pp.888-901.

[9] Jeon, S.W., Devroye, N., Vu, M., Chung, S.Y. and Tarokh, V., 2011. Cognitive networks achieve throughput scaling of a homogeneous network. IEEE Transactions on Information Theory, 57(8), pp.5103-5115.

[10] Holme, P., Kim, B.J., Yoon, C.N. and Han, S.K., 2002. Attack vulnerability of complex networks. Physical review E, 65(5), p.056109.

[11] Herrmann, H.J., Schneider, C.M., Moreira, A.A., Andrade Jr, J.S. and Havlin, S., 2011. Onion-like network topology enhances robustness against malicious attacks. Journal of Statistical Mechanics: Theory and Experiment, 2011(01), p.P01027.

[12] Buesser, P., Daolio, F. and Tomassini, M., 2011, April. Optimizing the robustness of scale-free networks with simulated annealing. In International conference on adaptive and natural computing algorithms (pp. 167-176). Springer, Berlin, Heidelberg.

[13] Qiu, T., Zhao, A., Xia, F., Si, W. and Wu, D.O., 2017. ROSE: Robustness strategy for scale-free wireless sensor networks. IEEE/ACM Transactions on Networking, 25(5), pp.2944-2959.

[14] Hu, S. and Li, G., 2020. TMSE: A topology modification strategy to enhance the robustness of scale-free wireless sensor networks. Computer Communications, 157, pp.53-63.

[15] Durón, C., 2020. Heatmap centrality: A new measure to identify super-spreader nodes in scale-free networks. Plos one, 15(7), p.e0235690.

[16] Morone, F. and Makse, H.A., 2015. Influence maximization in complex networks through optimal percolation. Nature, 524(7563), pp.65-68.

[17] Mugisha, S. and Zhou, H.J., 2016. Identifying optimal targets of network attack by belief propagation. Physical Review E, 94(1), p.012305.

[18] Clusella, P., Grassberger, P., Pérez-Reche, F.J. and Politi, A., 2016. Immunization and targeted destruction of networks using explosive percolation. Physical review letters, 117(20), p.208301.

[19] Zdeborová, L., Zhang, P. and Zhou, H.J., 2016. Fast and simple decycling and dismantling of networks. Scientific reports, 6(1), pp.1-6.

[20] Zhao, D., Wang, L., Xu, S., Liu, G., Han, X. and Li, S., 2017. Vital layer nodes of multiplex networks for immunization and attack. Chaos, Solitons & Fractals, 105, pp.169-175.

[21] Khan, M.A., Javaid, N., Javaid, S., Khalid, A., Nasser, N. and Imran, M., 2020, June. A novel cooperative link selection mechanism for enhancing the robustness in scale-free IoT networks. In 2020 International Wireless Communications and Mobile Computing (IWCMC) (pp. 2222-2227). IEEE.

[22] Xuan, Q., Shan, Y., Wang, J., Ruan, Z. and Chen, G., 2020. Adversarial Attacks to Scale-Free Networks: Testing the Robustness of Physical Criteria. arXiv preprint arXiv:2002.01249.

[23] Zhou, M. and Liu, J., 2016. A two-phase multiobjective evolutionary algorithm for enhancing the robustness of scale-free networks against multiple malicious attacks. IEEE transactions on cybernetics, 47(2), pp.539-552.

[24] Qiu, T., Liu, J., Si, W., Han, M., Ning, H. and Atiquzzaman, M., 2017. A data-driven robustness algorithm for the internet of things in smart cities. IEEE Communications Magazine, 55(12), pp.18-23.

[25] Qiu, T., Lu, Z., Li, K., Xue, G. and Wu, D.O., 2020, July. An Adaptive Robustness Evolution Algorithm with Self-Competition for Scale-Free Internet of Things. In IEEE INFOCOM 2020-IEEE Conference on Computer Communications (pp. 2106-2115). IEEE.

[26] Deng, Z., Xu, J., Song, Q., Hu, B., Wu, T. and Huang, P., 2020. Robustness of multi-agent formation based on natural connectivity. Applied Mathematics and Computation, 366, p.124636.

[27] Wang, S. and Liu, J., 2017. A multi-objective evolutionary algorithm for promoting the emergence of cooperation and controllable robustness on directed networks. IEEE Transactions on Network Science and Engineering, 5(2), pp.92-100.

[28] Wang, S., Liu, J. and Jin, Y., 2021. A Computationally Efficient Evolutionary Algorithm for Multi-Objective Network Robustness Optimization. IEEE Transactions on Evolutionary Computation.

[29] Wang, S. and Liu, J., 2019. Designing comprehensively robust networks against intentional attacks and cascading failures. Information Sciences, 478, pp.125-140.

[30] Sohn, I., 2019. A robust complex network generation method based on neural networks. Physica A: Statistical Mechanics and its Applications, 523, pp.593-601.

[31] Chen, N., Qiu, T., Zhou, X., Li, K. and Atiquzzaman, M., 2019. An intelligent robust networking mechanism for the Internet of Things. IEEE Communications Magazine, 57(11), pp.91-95.

[32] Chen, N., Qiu, T., Mu, C., Han, M. and Zhou, P., 2020. Deep

Actor–Critic Learning-Based Robustness Enhancement of Internet of Things. IEEE Internet of Things Journal, 7(7), pp.6191-6200.

[33] Yang, Z. and Liu, J., 2018. A memetic algorithm for determining the nodal attacks with minimum cost on complex networks. Physica A: Statistical Mechanics and its Applications, 503, pp.1041-1053.

[34] Wang, C. and Xia, Y., 2020. Robustness of Complex Networks Considering Attack Cost. IEEE Access, 8, pp.172398-172404.

[35] Jiang, Z.Y., Zeng, Y., Liu, Z.H. and Ma, J.F., 2019. Identifying critical nodes' group in complex networks. Physica A: Statistical Mechanics and its Applications, 514, pp.121-132.

[36] Cui, P., Zhu, P., Wang, K., Xun, P. and Xia, Z., 2018. Enhancing robustness of interdependent network by adding connectivity and dependence links. Physica A: Statistical Mechanics and its Applications, 497, pp.185-197.

[37] Pizzuti, C. and Socievole, A., 2018, December. A genetic algorithm for enhancing the robustness of complex networks through link protection. In International Conference on Complex Networks and their Applications (pp. 807-819). Springer, Cham.

[38] Sun, S., Liu, X., Wang, L. and Xia, C., 2020. New Link Attack Strategies of Complex Networks Based on k-Core Decomposition. IEEE Transactions on Circuits and Systems II: Express Briefs, 67(12), pp.3157-3161.

[39] Mozafari, M. and Khansari, M., 2019. Improving the robustness of scale-free networks by maintaining community structure. Journal of Complex Networks, 7(6), pp.838-864.

[40] Wang, S. and Liu, J., 2016. Robustness of single and interdependent scale-free interaction networks with various parameters. Physica A: Statistical Mechanics and its Applications, 460, pp.139-151.

[41] Xu, S., Xia, Y. and Ouyang, M., 2020. Effect of resource allocation to the recovery of scale-free networks during cascading failures. Physica A: Statistical Mechanics and its Applications, 540, p.123157.

[42] Chujyo, M. and Hayashi, Y., 2021. A loop enhancement strategy for network robustness. Applied Network Science, 6(1), pp.1-13.