Hindawi
Security and Communication Networks
Volume 2021, Article ID 4539540, 12 pages
https://doi.org/10.1155/2021/4539540

Research Article

On Improving the Robustness of MEC with Big Data Analysis for Mobile Video Communication

Jianming Zhao ,[1,2,3] Peng Zeng ,[1,2,3] Yingjun Liu ,[4] and Tianyu Wang[1,2,3]

[1]*State Key Laboratory of Robotics, Shenyang Institute of Automation, Chinese Academy of Sciences, Shenyang 110016, China*
[2]*Key Laboratory of Networked Control Systems, Chinese Academy of Sciences, Shenyang 110016, China*
[3]*Institutes for Robotics and Intelligent Manufacturing, Chinese Academy of Sciences, Shenyang 110169, China*
[4]*Industry Development and Promotion Center,*
Ministry of Industry and Information Technology of the People's Republic of China, Beijing 100846, China

Correspondence should be addressed to Peng Zeng; zp@sia.cn

Received 13 April 2021; Revised 18 May 2021; Accepted 8 June 2021; Published 7 July 2021

Academic Editor: Kai Wang

Mobile video communication and Internet of Things are playing a more and more important role in our daily life. Mobile Edge Computing (MEC), as the essential network architecture for the Internet, can significantly improve the quality of video streaming applications. The mobile devices transferring video flow are often exposed to hostile environment, where they would be damaged by different attackers. Accordingly, Mobile Edge Computing Network is often vulnerable under disruptions, against either natural disasters or human intentional attacks. Therefore, research on secure hub location in MEC, which could obviously enhance the robustness of the network, is highly invaluable. At present, most of the attacks encountered by edge nodes in MEC in the IoT are random attacks or random failures. According to network science, scale-free networks are more robust than the other types of network under the random failures. In this paper, an optimization algorithm is proposed to reorganize the structure of the network according to the amount of information transmitted between edge nodes. BA networks are more robust under random attacks, while WS networks behave better under human intentional attacks. Therefore, we change the structure of the network accordingly, when the attack type is different. Besides, in the MEC networks for mobile video communication, the capacity of each device and the size of the video data influence the structure significantly. The algorithm sufficiently takes the capability of edge nodes and the amount of the information between them into consideration. In robustness test, we set the number of network nodes to be 200 and 500 and increase the attack scale from 0% to 100% to observe the behaviours of the size of the giant component and the robustness calculated for each attack method. Evaluation results show that the proposed algorithm can significantly improve the robustness of the MEC networks and has good potential to be applied in real-world MEC systems.

1. Introduction

MEC is defined as providing IT service environment and cloud computing capability at the edge of mobile network [1–9]. In the view of the service providers, the network is actually divided into three parts: wireless access network, mobile core network, and application network. Among them, the wireless access network is composed of base stations, which are responsible for the access of mobile terminals [10–12]. The mobile core network is composed of a bunch of high-performance routers and servers, which are responsible for connecting the wireless base station to the external network [13–15]. The application network is where all kinds of application servers work, in fact, all kinds of data centres, servers, and even PCs [16, 17]. The server providers are basically only in charge of the wireless access network and the mobile core network. The application network is usually in the hands of OTT. These three kinds of networks transfer data alternately between the user terminal and the application server to meet the various Internet needs of users. However, with the emergence of various new types of services, such as AR/VR, connected cars, and so on, this traditional network structure is gradually overburdened [18–21]. Therefore, the emergence of MEC, that is, network services “sink” to the wireless access network side closer to users, brings about three benefits: (1) The transmission delay perceived by users is significantly reduced; (2) network congestion is controlled remarkably; and (3) more network information and network congestion control functions can be opened to developers.

There are many service scenarios for MEC. In the white paper “Mobile Edge Computing-A Key Technology towards 5G” of ETSI [22], the following typical scenarios are listed:

(1) *Augmented Reality (AR)*. Augmented reality (AR) is a technology that uses additional information generated by computer to enhance or expand the real-world scene that users see. The MEC server caches the AR audio and video content that needs to be pushed. Based on the location technology and geographic location information, it corresponds to the way of one by one. According to the application request initiated by the terminal, MEC server judges the application content through deep packet analysis, determines to push AR content combined with location information, and sends it to the user. On the one hand, MEC solution reduces content delay and improves user experience through content localization; on the other hand, it greatly enhances the application effect and value of AR based on location.

(2) *Intelligent Video Acceleration*. On the Internet, media and file transfer is usually in the form of stream or HTTP download based on TCP protocol. The change of channel environment, terminal access, and departure will lead to the change of link capacity. TCP may not be able to quickly adapt to the rapid changes of Ran, so using MEC for video acceleration can solve this kind of problem.

(3) *Connected Cars*. MEC servers can be deployed on LTE base stations along the road, receiving and analyzing local information from on-board applications and road sensors, so as to transmit some emergency information to other vehicles in the region.

(4) *Convergence Gateway of Internet of Things*. IOT devices are usually resource constrained in terms of processor and memory capacity, so it is necessary to use aggregation gateway to aggregate all kinds of IOT device information, which can reduce the response time of analysis and processing.

During the process of transferring video flow, mobile devices could be easily attacked, which would seriously influence the function of the whole systems. In this paper, in order to improve the robustness of MEC network for mobile video communication, we proposed a novel method for hub location to generate a more robust structure of the network. The MEC networks discussed in this paper include the edges nodes for edge computation and the information transferred between the nodes. To optimize the structure of the network, we use an optimization algorithm to overall consider the capability of edge nodes and the amount of the information. The main contributions of this work are summarized as follows:

(1) We address the problem of improving the robustness of MEC networks. We can show that MEC networks with different structures perform significantly uniquely under the same attacks.

(2) We propose a well-tuned optimization algorithm to improve the robustness of MEC networks.

The rest of this paper is organized as follows. Section 2 provides the definition of the robustness of the MEC network, and the relationship between the robustness and the structure. In Section 3, we present the optimization algorithm, which can improve the robustness of the MEC networks. Section 4 shows the performance of our algorithm, we evaluate the robustness of each generated network under different kinds of attacks, and the relative size of the giant component and the robustness under different attacks are reported in this part. Finally, conclusions are given in Section 5.

2. Background

2.1. Definition of Network Robustness. In this paper, we discuss the problem of improving the robustness of an MEC network. Connectivity is one of the most popular characteristics of network structure and function, and the size of giant component in the network is used to evaluate the connectivity. Therefore, the robustness could be evaluated by the size of the giant component after attacks. The same network shows different robustness under different attacks. In paper [23], the robustness of a network under certain attacks is defined as follows:

$$R = \frac{1}{|N|} \sum_{Q=1}^{N} GC\mathrm{size}(Q), \qquad (1)$$

where $|N|$ is the number of nodes in the network, Q is the attack on the network, and $GC\mathrm{size}(Q)$ means the size of the giant component under the attack of Q. Figure 1 shows the effect of two different attacks on the same example network. Figure 1(a) is the example network, and Figures 1(b-c) are under two different attacks of one node in the network. As we can see, the attack in the middle subfigure results in the size of the network of only one node, and the attack in the right subfigure leads to the size of the network of four nodes. This reflects the fact that the same network will show different robustness under different attacks of the same scale. In MEC networks, the size of the giant component means the subset of the network, where the information could reach each edge node. The parameter “R” displays the accumulated influence of the attacks on the MEC network, in terms of the giant component. As known by intuition, the area with the function of information transportation can effectively evaluate the robustness of the MEC network. In the basis of the analysis, the parameter R would be used for the evaluation of our method to improve the robustness of the MEC

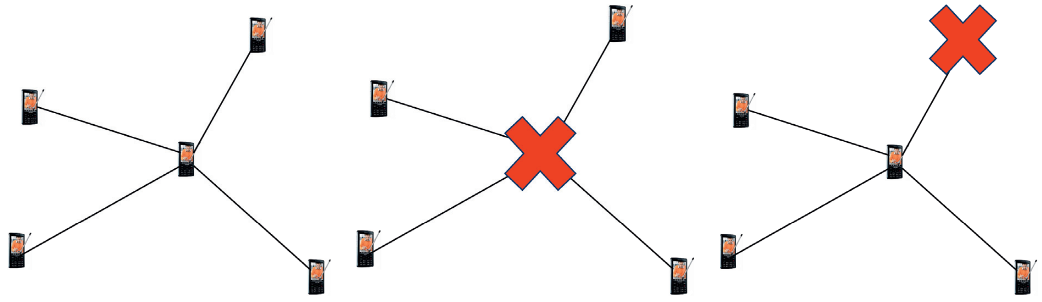


Figure 1: Different attacks on an example network. The example network and two situations with different attacks on the network.

networks. Therefore, designing a robust network according to the potential attacks is an important work.

2.2. Popular Attack Method. In MEC networks for mobile video communication, the mobile edge nodes are exposed to an open environment, which could cause random damages to the nodes [24]. Therefore, the first attack method mentioned here is random attack, in which the nodes would be damaged randomly.

One of the simplest metrics in complex network theory is the degree. The degree of a node $i\,(\mathrm{deg}_i)$ is the number of the node i's links and is defined in terms of the adjacency matrix A as [25]

$$\mathrm{deg}_i = \sum_{j\in N} a_{ij}. \tag{2}$$

The adjacency matrix storage structure uses a one-dimensional array to store the edge information for each vertex, so that all the points together represent the adjacency relationship between the vertices in the graph with a matrix. A matrix is actually a two-dimensional array. As a method to attack networks, degree-based methods first attack nodes with larger degree. In real MEC networks, the edge nodes with larger degree are often connected to more other nodes, which reflect the importance of the nodes to some degree. The degree-based methods are significantly efficient even for very large-scale networks.

Betweenness is another very popular network metric. The information exchange between two nodes that are not directly adjacent depends on the nodes on the path connecting these two nodes. The betweenness of a node can describe the importance in terms of exchanging information, and the betweenness of node i is defined as [26, 27]

$$b_i = \sum_{x,y\in N, x\neq y} \frac{n_{xy}(i)}{n_{xy}}, \tag{3}$$

where n_{xy} means the number of the shortest paths between node x and y and $n_{xy}(i)$ is the number of the shortest paths between node x and y through node i. Similarly to degree-based methods, in betweenness-based methods, the nodes with larger betweenness are attacked first. The ones with larger betweenness would be more important for information transforming in real MEC networks. Betweenness-based methods are used more frequently in real-world applications, since they could often identify more important nodes than degree-based methods.

Based on the attack methods above, we evaluate the methods on a small example network with only thirteen nodes. Figure 2 shows the networks under different attacks with two nodes. As we can see, after the optimal attack on the example network, the size of the giant component would be 5; the size of the giant component under degree-based method is 7; and the size of the giant component under betweenness-based method is 7. To sum up, it can be seen that different attack methods lead to different effectiveness of the attack. Therefore, we will evaluate the networks designed in our paper under different attack methods.

3. Proposed Algorithm

Given the vulnerability of the MEC network under attacks, we proposed to improve the robustness of MEC for mobile video communication with big data. Since the mobile devices need to send and receive video data, the capacity of each device and the size of the video data should be taken into consideration in the algorithm. Generally, the structure and function of MEC network should be related to two aspects: the video flow transferred in the network and the type of attacks that the network is facing with.

In this paper, we define the MEC network to be $G(E, V)$, where E means the mobile device nodes in the network and V means the links in the network. If there is a link between two nodes, this means there is a video flow transferring between them. The attacks used in the paper are also classified into two aspects: random attack and human intentional attacks. When the MEC network is under random attack, the mobile devices will break down randomly, maybe due to hardware damage or being out of power. When it comes to human intentional attacks, the attackers would aim at some important nodes, which would influence the network function and structure seriously. We use some popular intentional attack methods here to test the effectiveness of our algorithm. However, different network structure could show different robustness under the same type of attacks, and the same network could behave differently under different types of attacks. Therefore, in this paper, the structure of the MEC network can adapt to the change of attack types at any time. Firstly, two typical kinds of complex networks

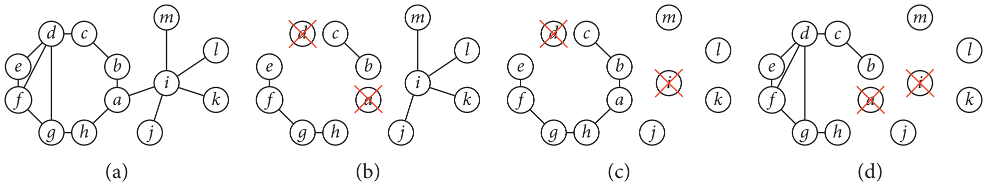


Figure 2: The effectiveness of different attack methods. (a) Original network. (b) Optical method (5). (c) Degree-based method (7). (d) Betweenness-based method (7).

with different structure would be introduced for the use of our algorithm.

(1) *BA Scale-Free Network* [28, 29]. In this model, the construction of BA networks consists of two steps:

(1) Starting with a connected network with m_0 nodes, a new node is generated in the network each time, which would build $m(m \leq m_0)$ links with the existing nodes

(2) When a new node is selecting an existing node to build a link, the probability of its connection with node i is $p_i = k_i / \sum_j k_j$

After time t, the above steps will generate a network with $N = t + m_0$ nodes. In this paper, we set the parameters $N = 200$ and $N = 500$, m is 2 or 3 or 4, which means the scale of the MEC network.

(2) *WS Small-World Network* [30]. In this model, the construction of WS networks also consists of two steps:

(1) Starting from a regular network: consider a network with N nodes, which are surrounded by a ring, in which each node is connected to its left and right $k/2$ nodes.

(2) Rewiring randomly: each link in the network is randomly rewired with probability p, that is, one endpoint of the link remains unchanged, and the other endpoint is taken as a randomly selected node in the network. It stipulates that any two different nodes can only have one link at most, and each node cannot have a link connected to itself.

In the WS network model, it is a regular network when $p = 0$, and it is a random network when $p = 1$. The characteristic of the network could be controlled through the variety of parameter p.

According to the knowledge of network science, BA networks are more robust under random attacks, while WS networks behave better under human intentional attacks. Therefore, we should change the structure of the network accordingly, when the attack types is different. Besides, in the MEC networks for mobile video communication, the capacity of each device and the size of the video data influence the structure significantly. When the capacity of a node is used up, there could be no more video data it can deal with.

We show the process of our algorithm in Figure 3 and the pseudocode of our algorithm in Algorithm 1. Our algorithm consists of three building blocks: (1) collect information of nodes and attacks, (2) generate networks, and (3) test the effectiveness of the network. Each step is discussed in detail as follows:

Block 1: Collect Information of Nodes and Attacks. First, collect the information of the nodes' capacity and the video flow, since this information would directly influence the structure and function of the networks. Then, as discussed before, since the robustness of the same network under different types of attacks is unique, the types of the attack need to be analyzed before constructing the network.

Block 2: Generate Networks. In network science, BA networks and WS networks are two typical kinds of networks, and they behave differently under the same attacks. Therefore, we decide to generate BA or WS networks according to the information of the MEC. When generating the networks, the capacity and the video flow need to be concerned. This means that if one node total is beyond its capacity, it will not be connected with new nodes.

Block 3: Test the Effectiveness of the Network. After generating networks, we need to use popular methods to attack them and to see if the robustness is good enough. If not, we would improve the parameter in the process of generating networks.

4. Results and Discussion

In this section, we evaluate the effectiveness of our algorithms on some artificial MEC networks with 200 nodes ($n = 200$) and 500 nodes ($n = 500$). Besides, the capacity of each node is 200 or 500 in this section, and the video flow to be transferred on each node varies from 1 to 4. To show the performance of our algorithm, we evaluate the robustness of each generated network under different kinds of attacks. The relative size of the giant component and the robustness under different attacks are also reported in this part.

4.1. Random Network Generation. In this section, we would generate the MEC networks for mobile video communication under different types of attacks. As introduced above, different types of networks behaves unique under different types of attacks: the BA network is more robust under random attacks, and the WS network behaves better under intentional attacks.

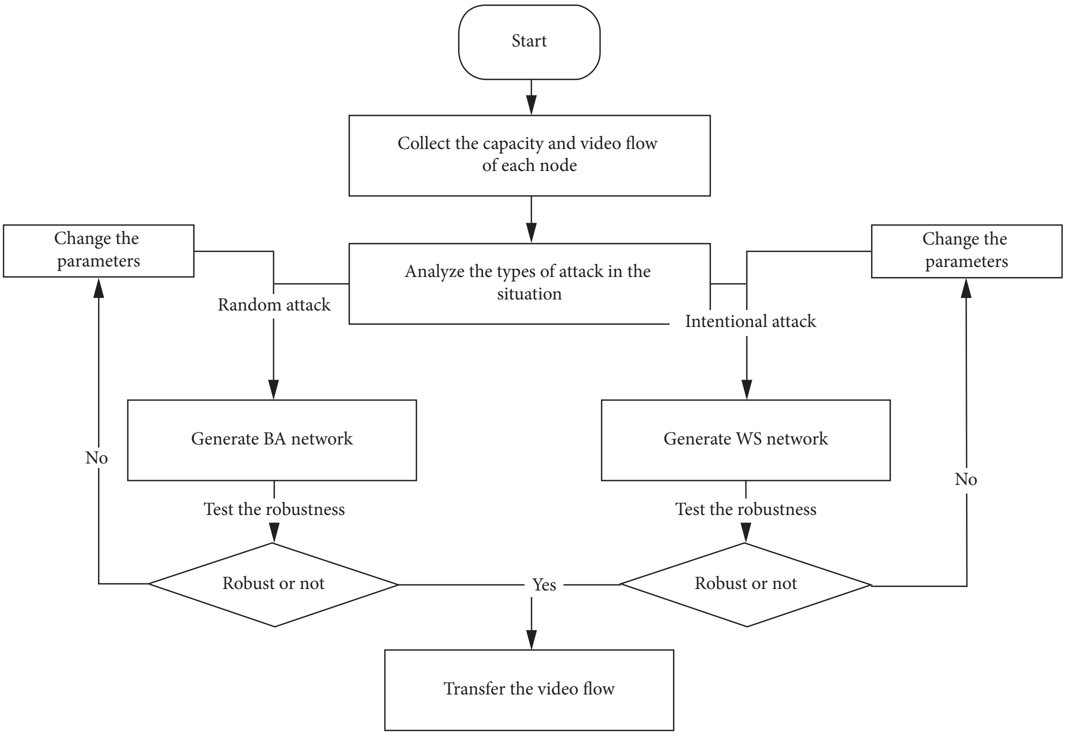


Figure 3: The process of our algorithm.

```
Robust MEC algorithm;
Collect the capacity and video flow of each node;
Analysis the types of attacks in the situation of mobile video communication;
while the robustness of the networks is not good enough
  Change the parameter of generating network method
  if the attacks are random attacks then:
    Generate BA networks
    for each node do
      if sum of neighbours' video flow is larger than the node's capacity then
      regenerate the network
  else if the attacks are intentional attacks then:
    Generate WS networks
    for each node do
      if sum of neighbours' video flow is larger than the node's capacity then
        regenerate the network
  Test the robustness under different attacks.
Return the generated networks.
```

Algorithm 1: The robust MEC algorithm.

4.1.1. Random Attacks. Firstly, for random attacks, we would use our algorithm to generate BA networks. In this paper, we set the number of nodes in the network to be 200 and 500, and the parameter m to be 2, 3, and 4. Table 1 and Figure 4 show the details of the generated networks.

Table 1 displays basic statistics for the three BA networks generated with our algorithm. In Table 1, "ave. deg" and "ave. betw" mean the average degree and average betweenness of all nodes, respectively; ASPL stands for the average of the distance between all node pairs in the networks; CC represents the clustering coefficient of the networks, which can show the degree of nodes being in the same cluster; the nodes in the same community usually have the same characteristics. As we can see from the table, though the numbers of the nodes in each network are the same, the structures of these networks are rather diverse. With the

Table 1: Basic statistics for the BA networks used in our study.

Metrics	200BA (2)	200BA (3)	200BA (4)
Node number	200	200	200
Link number	400	600	800
Ave. deg	3.95	5.9	7.83
Ave. betw	0.012	0.0097	0.0082
ASPL	3.38	2.91	2.61
CC	0.10	0.07	0.12
Community	12	10	10
Metrics	500BA (2)	500BA (3)	500BA (4)
Node number	500	500	500
Link number	1000	1500	2000
Ave. deg	3.984	5.964	7.936
Ave. betw	0.0058	0.0044	0.0039
ASPL	3.91	3.18	2.93
CC	0.048	0.058	0.067
Community	16	13	11

Ave. deg means average degree; ave. betw is average betweenness; ASPL stands for the average shortest path length; and CC represents clustering coefficient.

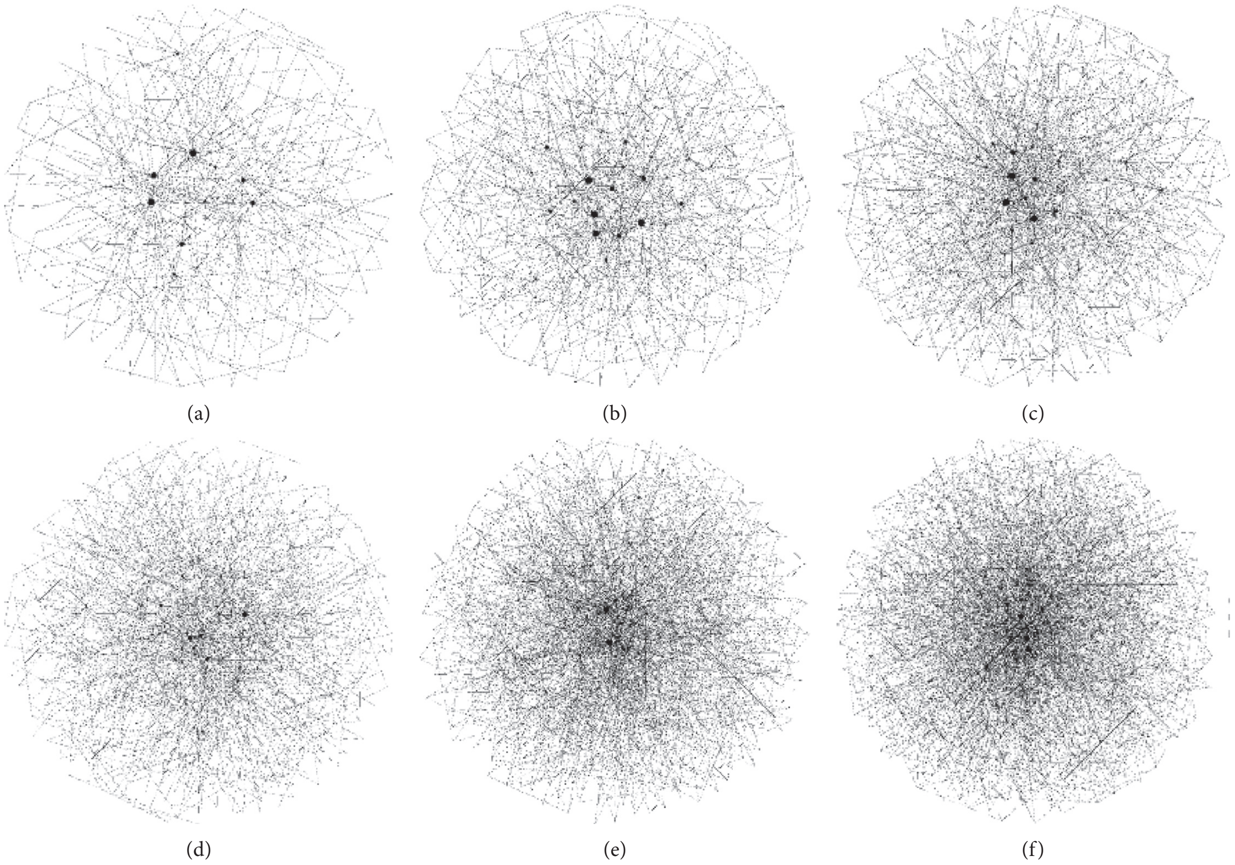


Figure 4: Structure of the BA networks.

increase of the link number, the average betweenness and the ASPL would be smaller. The community structure is detected by Louvain method in this paper.

Figure 4 visualizes the six BA networks, where the size of a node is proportional to its degree. The hub nodes are obvious in the network. As seen from the figure, the parameter in the algorithm can significantly influence the structure of the network.

4.1.2. Intentional Attacks. For intentional attacks, our algorithm would generate a series of WS networks. In WS network model, there are three parameters: number of nodes, initial number of each node's neighbours, and probability of each node rewiring. In order to evaluate the effectiveness of our algorithm in experiment with different parameters, we set the number of nodes to be 200 and 500, initial number of each node's neighbours to be 4, and probability of each node rewiring to be 20%, 30%, and 40%.

Table 2 shows basic statistics for the three WS networks generated with our algorithm. As we can see from the table, though the numbers of the nodes in each network are the same, with the increase of the rewiring probability, the average betweenness and the ASPL would be smaller. The difference of WS networks is less than BA networks.

Figure 5 visualizes the six WS networks, where the size of a node is proportional to its degree. The structure of these three WS networks looks similar, and there is no obvious hub node.

4.2. Robustness Test. To test the robustness of the networks, we will attack the networks with different attack methods. The attack methods used in this paper is random attack, degree-based attack, and betweenness-based attack. Specially, for the random attack, we attack the network randomly for ten times and choose the one with the best effectiveness. For intentional attacks, we attack the networks with two most popular methods: degree-based and betweenness-based methods.

Figure 6 and Table 3 report the size of the giant component and the robustness for the six BA networks. In the evaluation process, we increase the attack scale from 0% to 100% to observe the behaviours of the size of the giant component and the robustness calculated for each attack method.

In Figure 6, as we can see, on the whole ranges from 0% to 100% of the whole network, the generated MEC networks (BA networks) are more robust under random attacks. At the beginning of the attacks, the intentional attack methods (degree-based and betweenness-based methods) can rapidly influence the structure of the networks. For example, for BA (2) network, the size of the giant component is nearly 0 when 17% nodes are attacked, while the random attacks could hardly influence the structure of the network. Through comparing the effectiveness on different BA networks, it can be concluded that as the parameter of BA network increases, the networks would show better robustness.

Table 2: Basic statistics for the WS networks used in our study.

Metrics	200WS (0.2)	200WS (0.3)	200WS (0.4)
Node number	200	200	200
Link number	800	800	800
Ave. deg	3.99	3.99	3.99
Ave. betw	0.021	0.018	0.017
ASPL	5.09	4.47	4.28
CC	0.28	0.13	0.12
Metrics	500WS (0.2)	500WS (0.3)	500WS (0.4)
Node number	500	500	500
Link number	2000	2000	2000
Ave. deg	3.99	3.99	3.99
Ave. betw	0.011	0.0090	0.0083
ASPL	6.24	5.47	5.16
CC	0.26	0.18	0.10
Community	22	19	20

Ave. deg means average degree; ave. betw is average betweenness; ASPL stands for the average shortest path length; and CC represents clustering coefficient.

When it comes to Table 3, the robustness of generated MEC networks (BA networks) against random attacks and two intentional attacks is shown. In all generated networks, the robustness against random attacks is the largest while that against degree-based attacks is the smallest. It should be noticed that since hub nodes are the most important characteristics of BA networks, the hub-attack method (degree-based attack) is the most effective.

Figure 7 and Table 4 report the size of the giant component and the robustness for the six WS networks. In the evaluation process, we also increase the attack scale from 0% to 100% to observe the behaviours of the size of the giant component and the robustness calculated for each attack method.

For Figure 7, when the attack range is smaller than 30%, there is no obvious difference between random and intentional attacks, which reflects the fact that the generated MEC networks are relatively robust under intentional attacks. Comparing with Figure 6, WS networks show better robustness than BA networks, since these WS networks have more links than most of BA networks.

In Table 4, similarly to the results on BA networks, the WS networks are more robust under random networks. However, it should be noticed that the difference between random attacks and intentional attacks is rather small. This means that the MEC networks (WS networks) generated for intentional attacks show good robustness against intentional networks. Compared with BA4, which contains the same number of nodes and links, WS networks' robustness has been improved a lot. WS40 network's robustness is nearly 21.1% larger than BA networks. The results show that our algorithm could generate robust MEC networks for mobile video communication under both random attacks and intentional attacks.

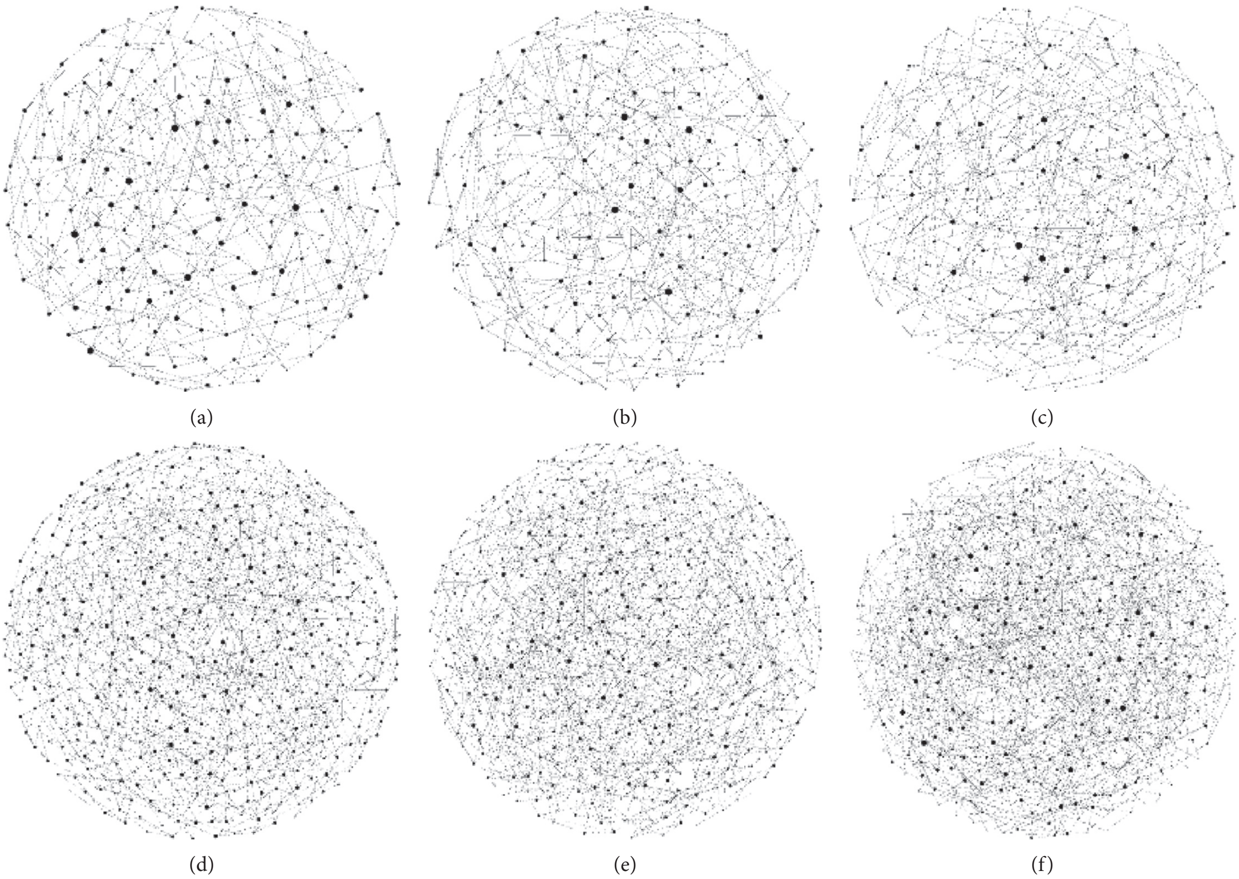


Figure 5: Structure of the WS networks.

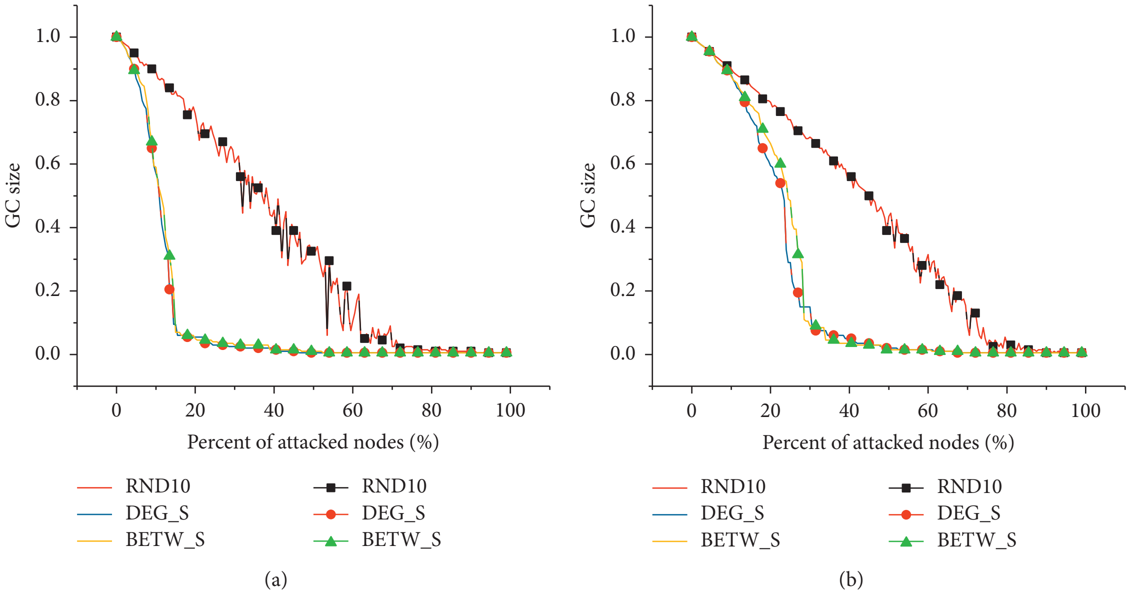
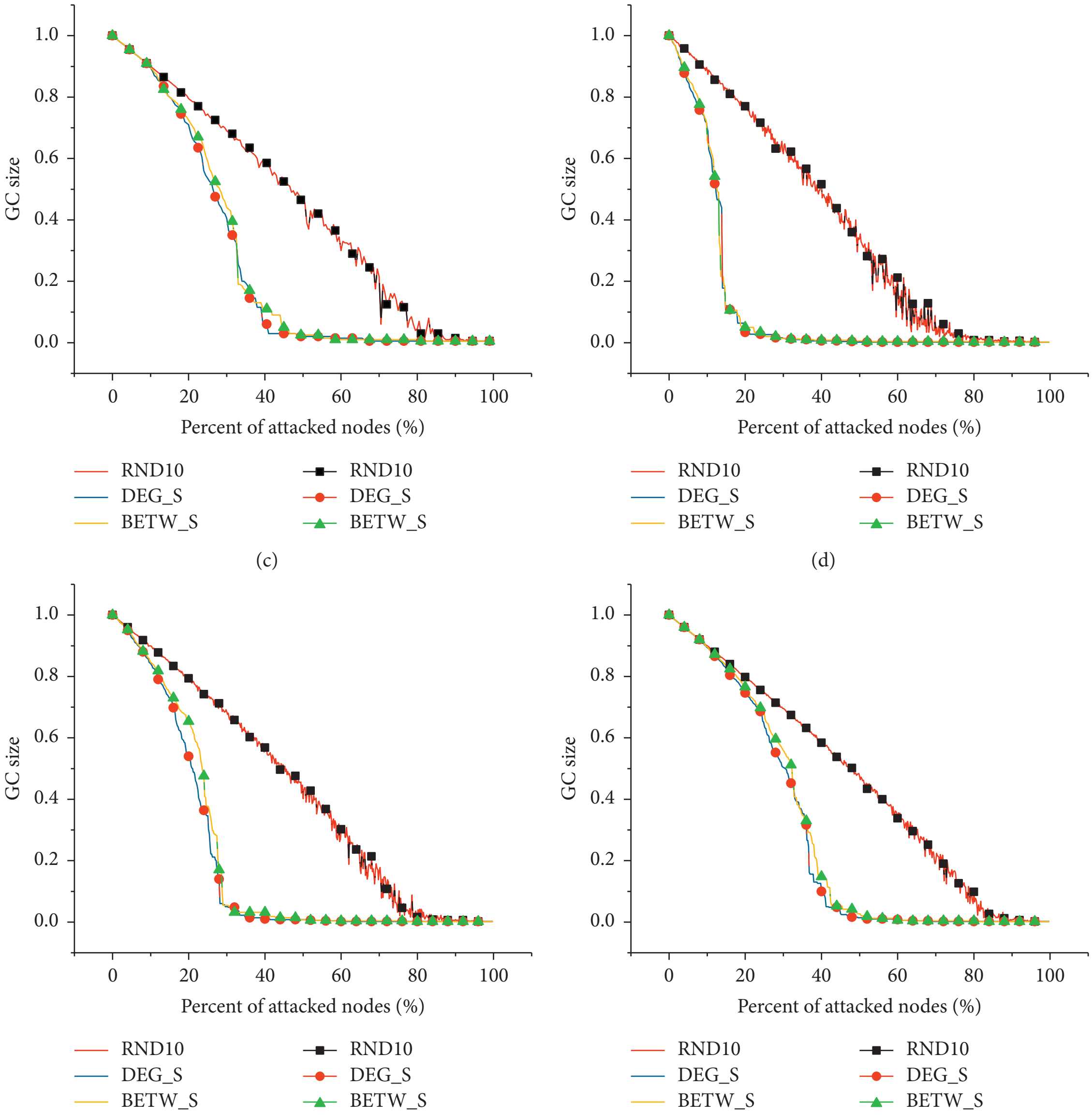


Figure 6: Continued.



(c)

(d)

(e)

(f)

Figure 6: Results of the BA networks.

Table 3: Robustness of BA networks under different attacks.

Method	200BA2	200BA3	200BA4
RND	0.367	0.431	0.454
Deg	0.116	0.219	0.261
Betw	0.122	0.230	0.270
Method	500BA2	500BA3	500BA4
RND	0.383	0.433	0.460
Deg	0.118	0.198	0.279
Betw	0.120	0.214	0.291

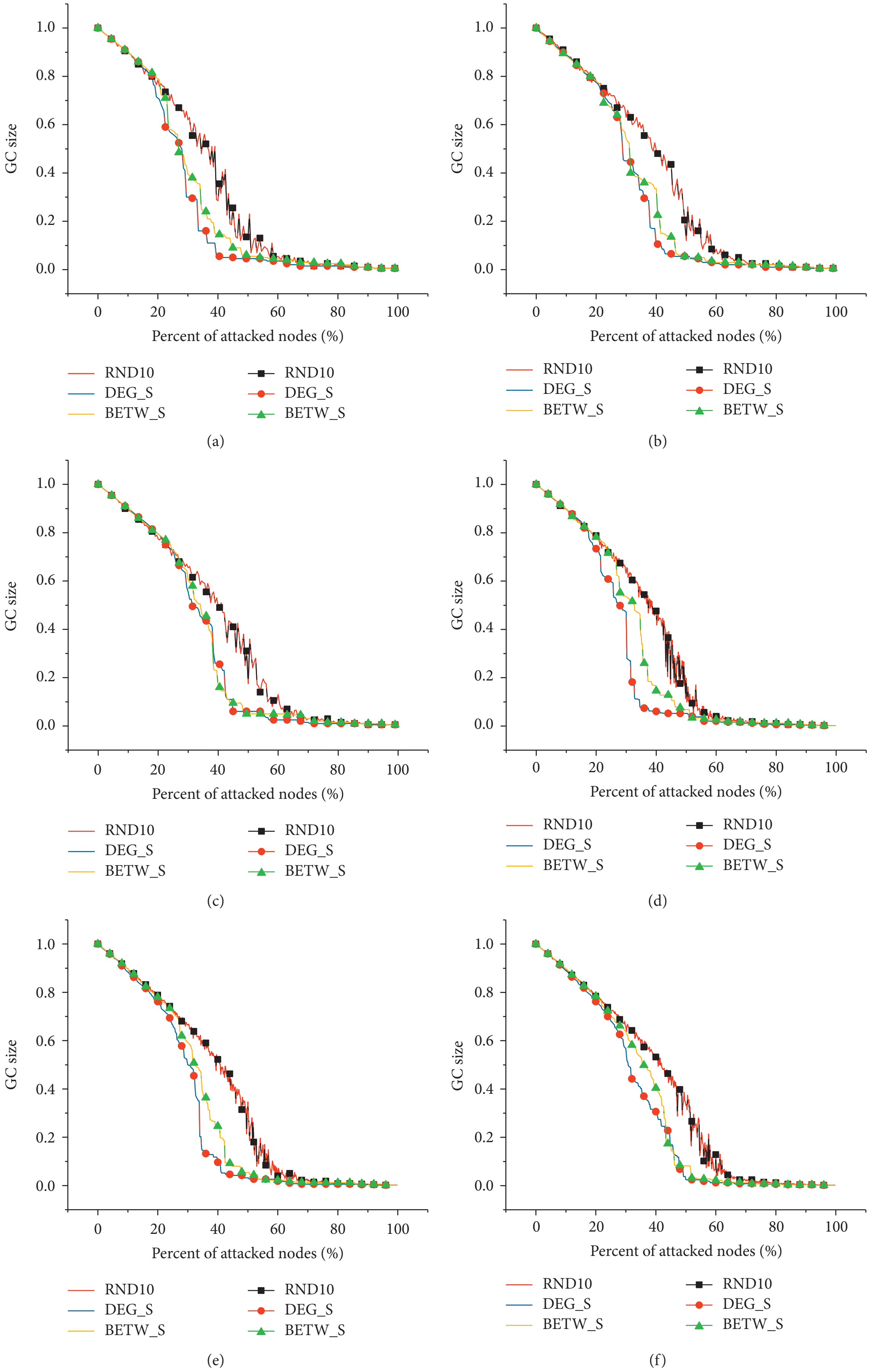


FIGURE 7: Results of the WS networks.

Table 4: Robustness of WS networks under different attacks.

Method	200WS20	200WS30	200WS40
RND	0.343	0.372	0.378
Deg	0.268	0.294	0.316
Betw	0.292	0.310	0.322
Method	500WS20	500WS30	500WS40
RND	0.350	0.372	0.383
Deg	0.261	0.278	0.308
Betw	0.302	0.308	0.329

5. Conclusions

In this paper, we designed an MEC network generating algorithm for mobile video communication to improve the security and robustness. After evaluation on artificial networks, our algorithm could significantly improve the robustness of the networks under either type of attacks (random attacks or human intentional attacks). Our algorithm provides a view to improving the security of mobile video communication and robustness of MEC networks.

In future work, our algorithm can also be improved in the following ways:

(1) Design an algorithm for more types of attacks. For the current algorithm, we only concern on two types of attacks: random or intentional. However, in real-world MEC systems, the attacks may be a mixture of the two types. Therefore, it is necessary to make the algorithm applicable for more situations.

(2) Collect real-world data. In this paper, we evaluate our algorithm on some artificial networks, and it shows effectiveness. However, in order to prove that our algorithm can be applied to real-world MEC networks, it is necessary to collect some real-world data for experiments.

Data Availability

In this manuscript, the data used to support the findings of this study are simulation data and generated by the NetworkX library in Python. Actually, we have sketched the basic technological process in this manuscript, but some contents and specific parameters of this process may be not completely open details. Therefore, if other researchers want to verify the results, replicate the analysis, or conduct secondary analyses, the corresponding author or first author can be contacted. The requests for the data will be considered by them after a confidentiality agreement.

Conflicts of Interest

The authors declare that they have no conflicts of interest regarding the publication of this paper.

Acknowledgments

This study was supported by the National Key R&D Program of China: "Key Technologies for Information Security of Measurement and Control Equipment" (Grant no. 2018YFB2004200) and the 2020 Industrial Internet Innovation and Development Project: "MEC Network Security Protection Technology and Product."

References

[1] S. Wang, X. Zhang, Y. Zhang, and L. Wang, "A survey on mobile edge networks: convergence of computing, caching and communications," *IEEE Access*, vol. 99, p. 1, 2017.

[2] H. Hu, H. Shan, C. Wang et al., "Video surveillance on mobile edge networks-A reinforcement-learning-based approach," *IEEE Internet of Things Journal*, vol. 7, no. 6, pp. 4746–4760, 2020.

[3] K. Peng, C. Victor, M. Leung, X. Xu, L. Zheng, and J. Wang, "A survey on mobile edge computing: focusing on service adoption and provision," *Wireless Communications and Mobile Computing*, vol. 2018, Article ID 8267838, 16 pages, 2018.

[4] X. Zhang, W. Wu, S. Yang, and X. Wang, "Falcon: a blockchain-based edge service migration framework in MEC," *Mobile Information Systems*, vol. 2020, Article ID 8820507, 17 pages, 2020.

[5] M. Wan, J. Li, Y. Liu, J. Zhao, and J. Wang, "Characteristic insights on industrial cyber security and popular defense mechanisms," *China Communications*, vol. 18, no. 1, pp. 130–150, 2021.

[6] Y. Gong and Y. Mo, "Qualitative analysis of commercial services in MEC as phased-mission systems," *Security and Communication Networks*, vol. 2020, Article ID 8823952, 11 pages, 2020.

[7] M. Cui, Y. Fei, and Y. Liu, "A survey on secure deployment of mobile services in edge computing," *Security and Communication Networks*, vol. 2021, Article ID 8846239, 8 pages, 2021.

[8] Q. Cao, Q. Wu, B. Liu, S. Zhang, and Y. Zhang, "An optimization method for mobile edge service migration in cyberphysical power system," *Wireless Communications and Mobile Computing*, vol. 2021, Article ID 6610654, 12 pages, 2021.

[9] Y. Mao, C. You, J. Zhang, and K. Huang, "A survey on mobile edge computing: the communication perspective," *IEEE Communications Surveys & Tutorials*, vol. 99, p. 1, 2017.

[10] H. Kim, M. Bae, W. Lee, and H. Kim, "Adaptive decision of wireless access network for higher user satisfaction," *Wireless Communications and Mobile Computing*, vol. 2018, Article ID 3427238, 19 pages, 2018.

[11] J. Huang, V. Subramanian, R. Agrawal, and R. Berry, "Joint scheduling and resource allocation in uplink OFDM systems for broadband wireless access networks," *IEEE Journal on Selected Areas in Communications*, vol. 27, no. 2, pp. 226–234, 2009.

[12] D. Tipper, T. Dahlberg, H. Shin, and C. Charnsripinyo, "Providing fault tolerance in wireless access networks," *IEEE Communications Magazine*, vol. 40, no. 1, pp. 58–64, 2002.

[13] A. D. Zayas, B. G. García, and P. Merino, "An end-to-end automation framework for mobile network testbeds," *Mobile Information Systems*, vol. 2019, Article ID 2563917, 8 pages, 2019.

[14] J. He and W. Song, "Smart routing: fine-grained stall management of video streams in mobile core networks," *Computer Networks*, vol. 85, pp. 51–62, 2015.

[15] S. Racz, M. Telek, and G. Fodor, "Call level performance analysis of 3rd generation mobile core networks," in

Proceedings of the IEEE International Conference on Communications, IEEE, Glasgow, Scotland, 2007.

[16] T. Szyrkowiec, A. Autenrieth, and W. Kellerer, “Optical network models and their application to software-defined network management,” *International Journal of Optics*, vol. 2017, Article ID 5150219, 9 pages, 2017.

[17] E. Lakiotakis, C. Liaskos, and X. Dimitropoulos, “Application-network collaboration using SDN for ultra-low delay tele-orchestras,” in *Proceedings of the 2017 IEEE Symposium on Computers and Communications (ISCC)*, IEEE, Heraklion, Greece, July 2017.

[18] B. Priya, R. Sri, A. Nimmagadda, and K. Garudkar, “Mobile edge communication an overview of MEC in 5G,” in *Proceedings of the 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS)*, pp. 271–276, IEEE, Coimbatore, India, March 2019.

[19] T. X. Tran, A. Hajisami, P. Pandey, and D. Pompili, “Collaborative mobile edge computing in 5G networks: new paradigms, scenarios, and challenges,” *IEEE Communications Magazine*, vol. 55, no. 4, pp. 54–61, 2017.

[20] Y. Yu, “Mobile edge computing towards 5G: vision, recent progress, and open challenges,” *China Communications*, vol. 13, no. Supplement2, pp. 89–99, 2016.

[21] E. Garcia-Palacios, “Mobile edge computing towards 5G: vision, recent progress, and open challenges,” *China Communications*, vol. 13, no. Supplement2, pp. 89–99, 2016.

[22] ETSI, *Mobile Edge Computing-A Key Technology Towards 5G*, Vol. 11, ETSI White Pap, Sophia Antipolis, France, 2015.

[23] C. M. Schneider, A. A. Moreira, J. S. Andrade, S. Havlin, and H. J. Herrmann, “Mitigation of malicious attacks on networks,” *Proceedings of the National Academy of Sciences*, vol. 108, no. 10, pp. 3838–3841, 2011.

[24] Q. Li, S. Meng, S. Zhang, J. Hou, and L. Qi, “Complex attack linkage decision-making in edge computing networks,” *IEEE Access*, vol. 7, no. 99, pp. 12058–12072, 2019.

[25] T. Opsahl, F. Agneessens, and J. Skvoretz, “Node centrality in weighted networks: generalizing degree and shortest paths,” *Social Networks*, vol. 32, no. 3, pp. 245–251, 2010.

[26] P. Holme, B. J. Kim, C. N. Yoon, and S. K Han, “Attack vulnerability of complex networks,” *Physical review. E, Statistical, nonlinear, and soft matter physics*, vol. 65, no. 5, Article ID 056109, 2002.

[27] D. Ding, J. Cao, Overview of network security of cyber-physical systems,” *Information and Control*, vol. 48, no. 5, pp. 513–521,527, 2019.

[28] Y.-y. Zhu, W. Li, and X. Cai, “Opinion evolution on a BA scaling network,” *Physica A: Statistical Mechanics and Its Applications*, vol. 392, no. 24, pp. 6596–6602, 2013.

[29] R. Yin, F. Zhang, Y. Xu, L. Liu, and X. Li, “A security routing algorithm against selective forwarding attacks in scale-free networks,” *Procedia Computer Science*, vol. 174, pp. 543–548, 2020.

[30] V. Latora and M. Marchiori, “Efficient behavior of small-world networks,” *Physical Review Letters*, vol. 87, no. 19, Article ID 198701, 2001.