A Flow Attack Strategy based on Critical Links for Cyber-attack

Jiming Qi,Jiazheng Zhang,Qingxia Liu,Bang Wang
School of Electronic Information and Communications
Huazhong University of Science and Technology(HUST), Wuhan, China, 430074
Email:{qijiming, jiazhengzhang, liuqingxia, wangbang}@hust.edu.cn

***Abstract*—Whether it be congestion control in cities or massive access in the Internet, these dynamic behaviors can be abstracted as flow demand between origin-destination node pairs (OD pairs) in the network. Links in complex systems are with notable heterogeneity, which means the volume of flow varies greatly, resulting in some critical links being more likely to congest under the flow attack, reducing the service capability of the system, and even causing network collapses. To explore how flow dynamics influences the network functionality and stability under congestion, we propose a link-based flow attack strategy that significantly degrades the service capability between OD pairs. In this approach, we first extract the routing paths and score the vulnerability of links between OD pairs, then an attack flow allocation rule based on critical links is designed to efficiently attack the target flow between OD pairs. Experiments on real-world networks show that the proposed strategy can quickly identify critical links and accurately attack the target flow. Besides, the proposed method provides positive and unique insights for defense strategy and network topology optimization.**

***Index Terms*—demand-serving network, critical link, network flow, attack strategy, routing strategy**

I. Introduction

Diverse real-world infrastructures such as transportation, communication, and power grids can be modeled as complex networks for analysis [1]. Whether it be the vehicles' mobility demand in transportation systems or the users' access requirements on the Internet, these dynamic behaviors can be regarded as the flow demand between OD pairs in the network. The primary purpose of many infrastructure networks is to best serve this flow demand. We refer to networks with such behavioral characteristics as "demand-serving networks [2]".

With the frequency of international cyber security incidents, great attention has been paid to the stability of crucial infrastructure systems. Generally, links in a complex system are with notable heterogeneity, which contains the various volume of flow. The uneven flow distribution causes some links more prone to congestion [3] under the influence of internal drivers or external attacks, resulting in packet loss, delay increase, and so on. The flow service capacity between specific OD pairs will be significantly reduced and even lead to cascading failures of the system. When the demand-serving networks fail to satisfy the real-world flow demand, typical examples include the regional power outage in the power grids, the congestion, or even paralysis in the transportation system.

Critical links are the edges that play a decisive role in network function, also known as bottleneck links. Locating and protecting the critical links in the network is of great significance in network robustness and survivability. On the one hand, from the perspective of attackers, the analysis of the critical links is essential for flow attack strategy design. On the other hand, from the perspective of defenders, the performance of the demand-serving can be improved by widening the flow bandwidth of critical links. How to design an effective algorithm to identify key network elements (nodes or links) [4], [5] has attracted a large number of scholars to study it in recent years. It is generally believed that the more important a node (link) is to the network structure, the stronger its ability to propagate. For example, in the human-contact disease network, preventing contact between infected people and their neighbors plays an important role in the control of infectious diseases, so the neighborhood-based centrality index is often chosen to measure the importance of elements.

Link failure in a complex system will bring pervasive phenomena such as various forms of congestion (e.g., traffic jams in transportation or packet congestion in communication networks), which reduce the efficiency of flow transfer in a continuous manner rather than the breakdown of the whole network. Although many methods have been proposed from different aspects to identify critical elements in networks, the relevant work is almost based on the topological characteristics of network elements in the network, without considering the flow demand and other factors. To fill the gaps in the above research fields, we propose a link-based flow attack strategy which focuses on the short-board effect and resource allocation. The goal is to maximize the loss of demand flow (target flow) between the given OD pair in the network. Experimental results on real-world networks validate our proposed method, which quickly identifies critical links and accurately attacks the target flow. Besides, the proposed method provides positive and unique insights for defense strategy and network topology optimization.

The rest of the paper is organized as follows: In Section 2, we review the most related work about the ranking algorithms of network elements' importance in complex networks. In

2324-9013/22/$31.00 ©2022 IEEE
DOI 10.1109/TrustCom56396.2022.00126

Section 3, we introduce the foundation of the research and propose our method to attack the target flow on the network. In Section 4, we verify the feasibility of the proposed method by designing some contrast experiments in real networks. Finally, Section 5 summarizes the paper with some discussions. The main contributions of this paper include proposing a link scoring mechanism, designing a critical link mining algorithm, and an attack flow allocation strategy.

II. Related Work

Network element importance metrics involve assessing their impact on the whole system. Many methods from different perspectives have been proposed to recognize vital network elements. The common measurement methods can be divided into three types: structure information-based [6]–[10], iterative refinement-based [11], and network percolation-based [2], [12].

Structural information-based metrics rely on the network structure to define the importance of elements, including global structure-based methods such as closeness and betweenness, local structure-based methods like degree centrality, and other measurement metrics based on mixed (local and global) structure information.

Iterative refinement-based metrics not only consider the number of neighboring nodes but also the importance of its neighbors, which iteratively computes node importance until convergence. Representative algorithms are classical PageRank algorithm and eigenvector.

Network percolation-based methods [13]–[17] describe the dynamics of the giant connectivity component in the network as the network elements are gradually attacked and failed, leading a phase transition of the network robustness. Li, et al. [12] constructed the urban traffic function network based on percolation theory, and identified bottleneck sections of the traffic network by studying the change characteristics of the local connectivity components of the network near the percolation phase change point. Hamedmoghadam, et al. [2] proposed a method to identify the bottleneck sections of the traffic network considering the flow demand, which takes the flow demand into account in the percolation process, and the key links obtained by simulation experiments are closer to the bottleneck sections in the real network.

III. Method

A. Problem definition

In this section, we formally define the problem of critical link-based flow attacking. With known routing strategy, packet loss strategy and flow distribution, critical link-based flow attacking problem is to maximize the loss of the target flow between the OD pair by distributing the attack flow in routing paths under fixed cost of attack flow.

B. Notations

Complex networks are often mathematically abstracted by graphical models. In this paper, we take an unweighted and undirected network $\mathscr{G}(\mathscr{V},\mathscr{E})$ with $N=|\mathscr{V}|$ nodes and $M=|\mathscr{E}|$ edges into consideration. The properties of the links in the original network include link capacity c_i and existing flow e_i. For the entire network, we use S,s_i,A,a_i to represent the total target flow transmitted between OD pairs,the flow flowing through l_i,the total attack flow and the flow allocated to l_i respectively.

TABLE I
Parameter Symbols and Descriptions

Parametric	Parametric Description
$\mathscr{G}$	original network
$\mathscr{V}$	set of nodes
N	number of nodes,$N=\|\mathscr{V}\|$
$\mathscr{E}$	set of edges
M	number of edges,$M=\|\mathscr{E}\|$
$\mathscr{P}_{OD}$	set of routing paths between OD pairs
p_m	the m-th path in $\mathscr{P}_{OD}$
L_{p_m}	length of p_m
C_{p_m}	cost of p_m
W_{p_m}	weight of p_m
$\mathscr{L}$	set of all links in the network
l_i	the i-th link in $\mathscr{L}$
c_i	capacity of l_i
e_i	the existing flow in l_i
r_i	the remaining bandwidth of l_i
S	total target flow between OD pairs
s_i	the target flow flowing through l_i
A	total attack flow
a_i	attack flow allocated to l_i
$\mathscr{L}_T$	set of target links
L_{T_j}	the j-th link in $\mathscr{L}_T$

C. Routing strategy

The investigation into routing strategies is to simulate real networks better. Traditional routing protocols take a single-path routing approach to transmission; that is, from the origin node to the destination node, all packets are forwarded through a single path, with other links in a backup or invalid state. In single-path transmission, we can quickly locate critical links by using attributes such as link capacity and maximum bearer flow. Extended to the more general situation, we introduce some multipath transmission-based load-balanced routing strategies [18]–[24] for analysis, which are more commonly used in practice.

ECMP (Equal Cost Multipath Routing): If there is more than one routing path with the same cost to the same destination, flow can be equally shared and forwarded through different paths. We assume that the cost of the path is directly related to the length of the path, and the longer the path the higher the cost. Therefore, we choose the set of shortest paths as the transmission paths under the ECMP routing strategy.

WCMP (Weighted Cost Multipath Routing) [24]: WCMP is an improved routing strategy based on ECMP, which no longer divides flow equally among the set of shortest paths, but distributes it based on the weight of the paths.

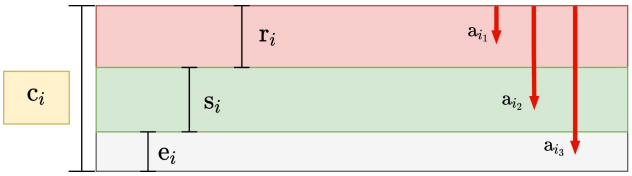


Fig. 1. Congestion control strategy

D. Congestion control strategy

When multiple flow packets compete for the same link, the link becomes congested, and the queue overflows and will drop packets. A brief summary is that the demand for aggregate bandwidth exceeds the available capacity of the link. Current congestion control strategies [25]–[28] include DF(drop-front), DL(drop-last), DO (drop-oldest), DY(drop-youngest) and so on. In this paper, the congestion control strategy is set as follows: when a link is attacked by flow, the remaining capacity space r_i of the link is first filled (the red piece in Fig.1), and then the target flow s_i in the link is dropped (the green piece in Fig.1), then the loss in the link is recorded as

$$\text{loss}_i = \begin{cases} 0, 0 \le a_i \le r_i \\ a_i - r_i, r_i \le a_i \le c_i - e_i, r_i = c_i - e_i - s_i \\ s_i, c_i - e_i \le a_i \end{cases} \quad (1)$$

The three-segment values a_{i_1},a_{i_2},a_{i_3} correspond to the three situations in Fig.1. In addition, the interaction of flow between the preceding and following links in the same path needs to be considered. The loss of target flow in the preceding link will cause a corresponding reduction of target flow in the following link.

E. Evaluation index

The effectiveness of the flow attack strategy is measured by the percentage of target flow lost during transmission from the origin node to the destination node, and the larger the percentage of loss, the better the performance of the attack strategy. Set the attack strategy performance metric K as

$$K = \sum_{i=1}^{n} \text{loss}_i / S \quad (2)$$

Where n is size of $\mathscr{L}$, $loss_i$ is the amount of target flow lost in l_i, and S is the total target flow.

F. SCL Algorithm

In this paper, we proposed a flow attack strategy based on critical links, SCL (Set of Critical Links). The strategy consists of three modules, namely the link criticality scoring module, the target link location module, and the attack flow allocation module.

As shown in Fig.2, the total target flow S between OD pairs (1,8) is 4, and the total attack flow $A = 8$. The values marked on the links in the figure are the link capacities. All the above

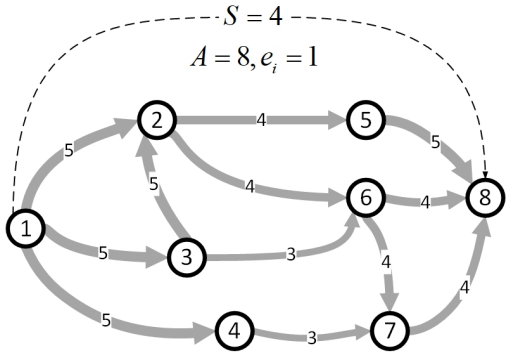


Fig. 2. Network Topology

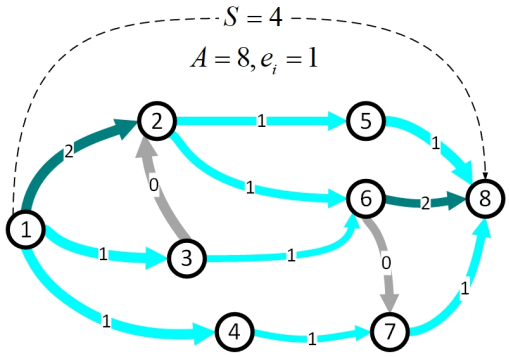


Fig. 3. Distribution of target flow

units are Gbps.According to the ECMP routing strategy, there are four equivalent shortest paths between origin node 1 and destination node 8, which are $1 \to 2 \to 5 \to 8$,$1 \to 2 \to 6 \to 8$,$1 \to 3 \to 6 \to 8$,$1 \to 4 \to 7 \to 8$. Therefore, the total target flow S is equally divided among the four equivalent shortest paths. Since l_{12} is the shared link of path $1 \to 2 \to 5 \to 8$and $1 \to 2 \to 6 \to 8$, and l_{68} is the shared link of path $1 \to 2 \to 6 \to 8$ and $1 \to 3 \to 6 \to 8$, the target flow in both links is equal to 2. However, l_{32} and l_{67} do not belong to any transmission path, so $s_{32} = 0, s_{67} = 0$. The target flow in other links is 1. As shown in Fig.3, the values marked on the links are the target flow.

Step 1: link criticality scoring module.The score of a link indicates how difficult it is to attack the target flow on the link, and is closely related to the capacity of the link and the target flow within it. Links with low capacity are relatively fragile and prone to congestion. The smaller the target flow in the link, the less impact the attack will have on the performance of the demand-servicing network. Furthermore, if the target flow in the link is 0, no matter how large the attack flow is, the effect of the attack will not be achieved. Therefore, set the score of the link l_i as

$$\text{score}_i = (A - r_i) * (s_i / c_i) \quad (3)$$

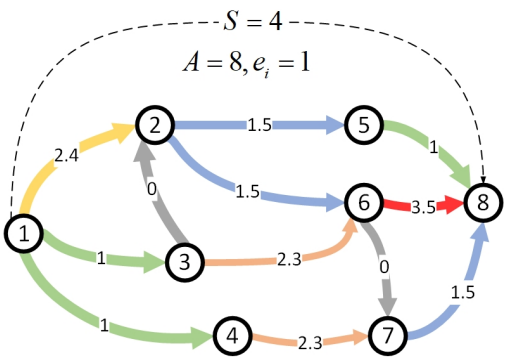


Fig. 4. Criticality score of links

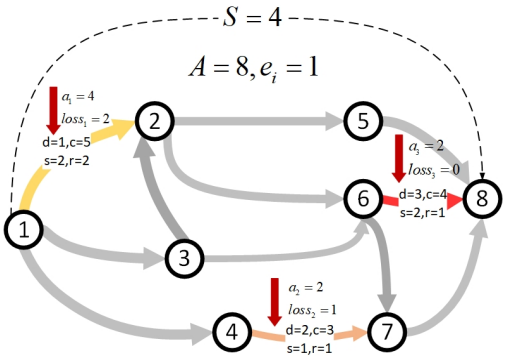


Fig. 5. Attack flow allocation

Where A is the total attack flow, and c_i,r_i,s_i represent the capacity of the l_i, the remaining space of l_i, and the target flow in l_i .

The score of each link can be calculated according to (3), which is marked in Fig.4. In path $1 \rightarrow 2 \rightarrow 5 \rightarrow 8$, although the capacity of l_{25} is less than l_{12}, the score is lower than that of l_{12}. Therefore, we can obtain that it is not the smaller the capacity that makes the link more vulnerable, but also the amount of target flow in the link. Since the target flow in l_{32} and l_{67} is 0, both links are scored as 0. Attacks on these two links will have no impact on the network's demand service capacity.

Step 2: target link location module. Select the link with the highest score in each transmission path based on the short board effect to obtain the set of target links. The highest rated link in each transmission path is marked with a black dashed line in Fig.4,$1 \rightarrow 2 \rightarrow 5 \rightarrow 8\,(l_{12})$, $1 \rightarrow 2 \rightarrow 6 \rightarrow 8\,(l_{68})$, $1 \rightarrow 3 \rightarrow 6 \rightarrow 8\,(l_{68})$,$1 \rightarrow 4 \rightarrow 7 \rightarrow 8\,(l_{47})$. As ECMP and WCMP are both intersecting multipath routing strategies, shared links can exist between different transport paths. If the shared links between different transmission paths are the critical links of the respective paths, the scores will be cumulative. Relevance: If a link is a shared critical link, in other words, it has the highest score among multiple transmission paths, it should also be more critical in the overall network.

Step 3: attack flow allocation module. We first calculate the distance of the links in $\mathscr{L}_T$ from the origin node and then prioritize attacking the links that are close to the source node. If the current attack flow cannot cause damage to the target flow on the link, the next link will be attacked. Based on the set of target links, the attack flow allocation scheme and the attack strategy performance metric K can be calculated.

As shown in Fig.5, the distance between the links in $\mathscr{L}_T$ and the origin node can be calculated, prioritizing the attack on the link l_{12} with a distance of 1 from the origin node, the attack flow $a_1 = 4$ allocated, resulting in a loss of flow $loss_1 = 2$. The attack is then carried out on l_{47} with a distance of 2, with an allocated attack flow $a_2 = 2$, resulting in a loss of target flow $loss_2 = 1$. The last attack will be carried out on l_{12} at a distance of 3,because the target flow flowing through paths $1 \rightarrow 2 \rightarrow 5 \rightarrow 8$ and $1 \rightarrow 2 \rightarrow 6 \rightarrow 8$ was lost during the previous attack, and the target flow flowing through the link was only the target flow in path $1 \rightarrow 6 \rightarrow 5 \rightarrow 8$, and the attack flow was allocated $s_{68} = 1$, without causing any loss of target flow. Finally, according to (2), the attack strategy performance metric can be calculated $K = 0.75$.

Algorithm 1: Set of Critical Links Algorithm

input : $\mathcal{G}$,c_i,e_i,S,A, routing strategy, origin and destination node.
output: K.

Compute all routing paths between the OD node pair according to the routing strategy, get $\mathscr{P}_{OD}$;
Score all links according to (3);
Find the highest rated link in each routing path, get $\mathscr{L}_T$;
Calculate and rank the links in $\mathscr{L}_T$ by their distance from the origin node;
for L_{T_j} in $\mathscr{L}_T$,j from 1 to len($\mathscr{L}_T$):
    If $A > 0$ and $S > 0$:
        Calculate a_j and $loss_j$;
        Update$A$ and S;
    else:
        break;
Calculate K by (2).

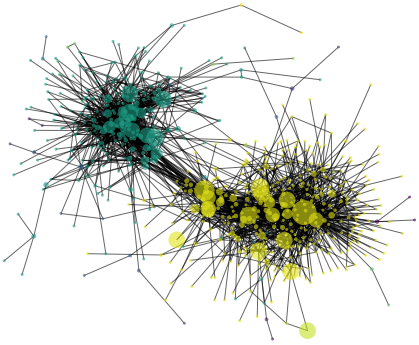
IV. Experiments

A. Experimental settings

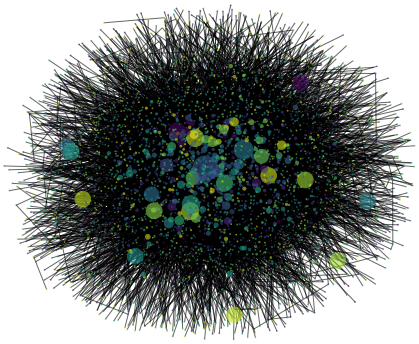
In this section, we evaluate the effectiveness of our method against state-of-the-art strategies on three benchmarks: the EU educational research network (geant, N=27), the US politician blog network (web-polblogs, N=643), and US Environmental Protection Agency associated website (web-EPA, N=4772) [29]. Detailed statistics of each network are summarized in Table II,where N,M,$< k >$,C,D,P represent the node number, the edge number, the average degree, the clustering coefficient, the diameter and the average path length of networks,

respectively. We randomly generate link capacity and existing flow information on real-world datasets in which the flow information is missing. All the experiments were conducted on an 8-core workstation with the following configurations: Intel Xeon E5-2620, 64GB of RAM and a Nvidia TITAN V GPU with 12GB memory.

(a) geant



(b) web-polblogs



(c) web-EPA

Fig. 6. Experimental networks

B. Baseline

To demonstrate the effectiveness of our proposed method among flow attack strategies, we compare five following heuristic methods which is designed relying on priori knowledge [30]:

SCL-s: The difference with the SCL is the attack flow is allocated proportional to the score of the selected target links.

SCL-d: SCL-d considers the case that target flow in the subsequent link will be reduced accordingly when the preceding link is attacked. It can be observed that links closer to the source node are more critical and vice versa. SCL-d sets a decay factor β so that the distant links with lower scores. Formally, the scoring rule is modified to

$$\text{score}_i = (A - r_i) * (s_i/c_i) * \beta^{d_i} \tag{4}$$

ES: It traverse the combination of all target links (containing the target flow) to obtain the best attack strategy under average allocation of attack flow.

RS-a: RS-a randomly select the same number of target links as the SCL and average allocate of attack flow.

RS-s: RS-s randomly select the same number of target links as the SCL and assign the attack flow proportional to the score of the selected target links.

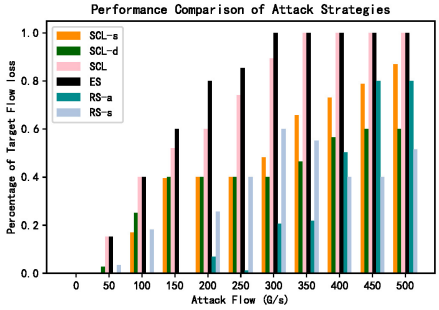
TABLE II
STATISTICAL PROPERTIES OF REAL-WORLD NETWORKS

Network	N	M	$< k >$	C	D	P
geant	27	41	3.037	0.096	6	3.009
web-polblogs	643	2280	7.092	0.232	10	3.828
web-EPA	4772	8909	3.734	0.064	10	4.184

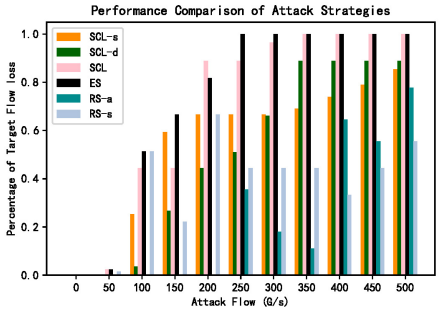
C. Experimental results

Experiment 1: Performance of different attack methods under different cost of attack flow. To simulate the state of flow information in route network, we introduce the ECMP routing strategy and congestion control strategy as described in the previous section. Note that capacities of links are randomly selected from [120,140,160,180] (Gbps) and volume of existing flow is randomly generated from [1-50] (Gbps), and we set the demand service flow is 100 (Gbps) and the total cost of attack flow from 50 to 500 (Gbps) at 50 intervals. We evaluate all the baselines on the three real-world networks. In the geant network, node 14 and 20 is chosen as OD pair with 5 equivalent paths and the length of which is 5 hops. In the web-polblogs network, we select node 224 and 300 as OD pair with 9 equivalent paths and path length of 5 hops. In the web-EPA, the length of 38 equivalent paths between OD pair (8,68) is 5 hops. Fig.7 presents the experimental results.

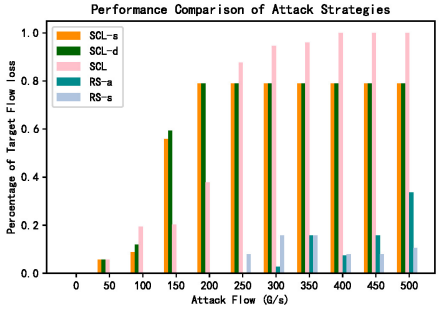
In Fig.7, the ES (pink) achieve better performance overall, i.e. ES has strong attack capabilities causing more target flow loss, the second best one is SCL, in some cases very close to the close-to-optimal state-of-the-art as ES, and much better than other methods. Besides, SCL-a and SCL-s perform similar, while RS-a and RS-s perform poorly in most cases because of the randomness of attacking links.



(a) comparison of attack strategy performance on geant



(b) comparison of attack strategy performance on web-polblogs

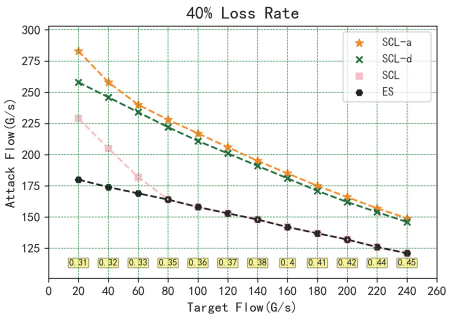


(c) comparison of attack strategy performance on web-EPA

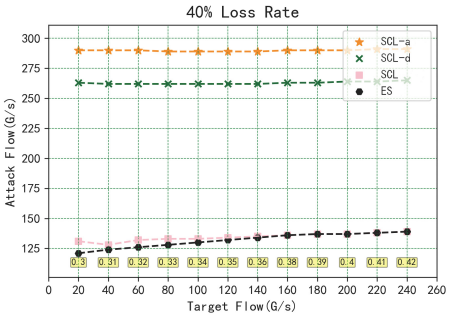
Fig. 7. Comparison of attack strategy performance

Although ES performs excellently on most of real-world networks, the complexity of the algorithm is too high and it no longer works in web-EPA. Specifically, the complexity of ES is not directly related to the size of the network, but rather to the set of links through which the target flow flows, which depends on the choice of routing paths. In the web-EPA, there are 38 equivalent routing paths and the lengths of paths are all 5 hops, which far exceeds the 5 equivalent paths in the geant network and the 9 equivalent paths in the web-polblogs network. Comparing the performance of SCL on above three benchmark, it can be seen that all the target flow is invalid when the attack flow = 350 Gbps in geant and web-polblogs, while it needs 400 Gbps in the web-EPA.

Experiment 2(a): Performance of different attack methods



(a) experimental results on genat network



(b) experimental results on web-polblogs network

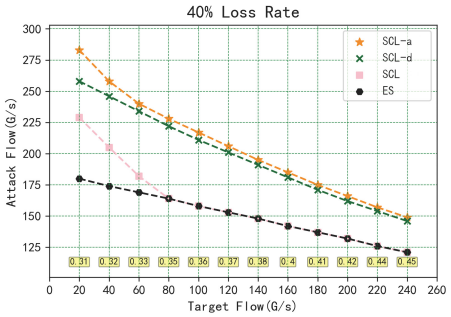
Fig. 8. Experimental results under different volume of target flow

under different volume of target flow. The experiment settings are the same as in Experiment 1 (excluding web-EPA network), we set the target flow ranging from 20 to 240 (Gbps) at 20 intervals, and the goal is to cause 40% loss of target flow.

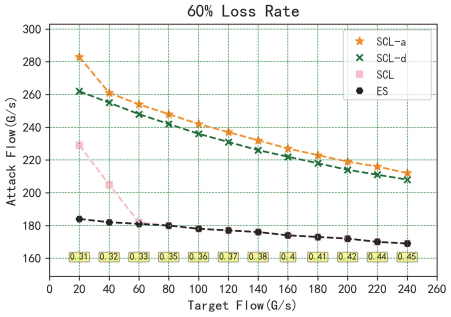
As can be seen in Fig.8, as link saturation increases (Yellow x-axis sub-coordinate, $\left(\sum_{i=1}^{N} s_i + \sum_{i=1}^{N} e_i\right) / \sum_{i=1}^{N} c_i$), the volume of attack flow required decreases progressively for the goal that makes the target flow lose 40% and more. That is, link saturation is proportional to the vulnerability of the target flow. Comparing the different attack strategies under same attack goal, ES achieves the best performance and requires less attack flow, our proposed SCL is the second best one, and SCL-a performs slightly better than the SCL-d algorithm in all three networks.

Experiment 2(b): Performance of different attack methods under different goal. Fig.9 compares the performance of different attack goal for the same three real-world networks. As the requirements of the attack goal increase, the more attack flow is required. In Fig.9(c), SCL outperforms ES in some cases since ES allocates attack flow on target links equally rather than adaptive distribution of flow, which implies that ES algorithm has limitations in some scenarios.

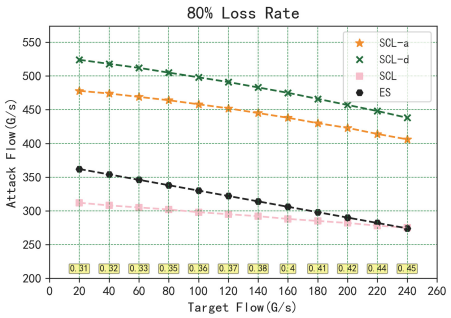
Experiment 3: Performance of different attack methods under different routing strategies. We keep the same setting with Experiment 1, the target flow is fixed at 100 Gbps. To



(a) target set at 40%

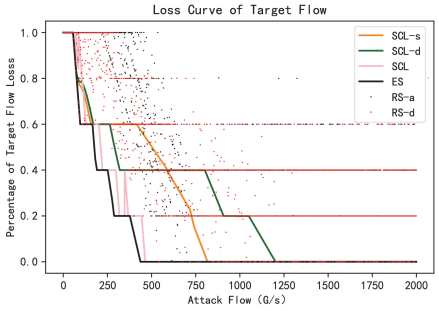


(b) target set at 60%

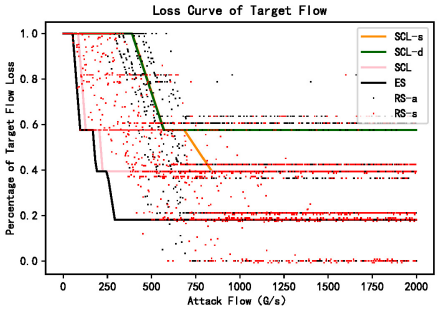


(c) target set at 80%

Fig. 9. Experimental results under different attack targets



(a) experimental results under ECMP routing Strategy



(b) experimental results under WCMP routing Strategy

Fig. 10. Experimental results under different routing strategies

TABLE III
COMPREHENSIVE PERFORMANCE INDICATORS OF ATTACK STRATEGIES UNDER DIFFERENT ROUTING STRATEGIES

Algorithm	ECMP	WCMP
SCL − s	426	1132
SCL − d	496	1356
SCL	238	691
ES	202	486

further understand the impact of different routing strategies on effectiveness of attack methods, We use the area under the curve with the x and y axis as a measure of the performance. As shown in Table III, the smaller the value, the better the performance of the flow attack strategy. Comparing the performance of different methods under ECMP and WCMP routing strategies, it is observed that these attack methods is more effective under ECMP routing. Alternatively, the system has stronger resistance under WCMP routing.

V. CONCLUSION AND DISCUSSION

To investigate how flow in a demand-servicing network affects the operational state of the network by causing congestion, this paper proposes a high-scoring link aggregation algorithm to quantify the impact of links on the overall demand service capability of the network, which is based on link scoring to identify critical links and assign attack flow.

The experimental results show that the flow attack strategy based on critical links proposed in this paper can quickly locate critical links and accurately attack the target flow, which is of great significance for the research on problems such as learning the dynamic change process of the network and selecting the optimal defense strategy for different attack strategies. In the future, problems such as flow attack strategies for multiple OD pairs can be considered.

REFERENCES

[1] G. S. Z and L. Z. M, *The basic theory of complex network*. Science Press, 2012.

[2] H. Hamedmoghadam, M. Jalili, H. L. Vu, and L. Stone, "Percolation of heterogeneous flows uncovers the bottlenecks of infrastructure networks," *Nature communications*, vol. 12, no. 1, pp. 1–10, 2021.

[3] J. Zhu, X. Jiang, Y. Yu, G. Jin, H. Chen, X. Li, and L. Qu, "An efficient priority-driven congestion control algorithm for data center networks," *China Communications*, vol. 17, no. 6, pp. 37–50, 2020.

[4] R. X. L and L. L. Y, "A survey of sorting methods for important nodes in the network," *Chinese Science Bulletin*, vol. 59, no. 13, pp. 1175–1197, 1 2014.

[5] L. Q. X and W. B, "Network resilience and recovery mechanism: A review," *Cyber Security*, vol. 6, no. 4, pp. 44–59, 2021.

[6] F. Chung and L. Lu, "Connected components in random graphs with given expected degree sequences," *Annals of combinatorics*, vol. 6, no. 2, pp. 125–145, 2002.

[7] D. Chen, L. Lü, M.-S. Shang, Y.-C. Zhang, and T. Zhou, "Identifying influential nodes in complex networks," *Physica a: Statistical mechanics and its applications*, vol. 391, no. 4, pp. 1777–1787, 2012.

[8] L. C. Freeman, "Centrality in social networks conceptual clarification," *Social networks*, vol. 1, no. 3, pp. 215–239, 1978.

[9] M. E. Newman, "A measure of betweenness centrality based on random walks," *Social networks*, vol. 27, no. 1, pp. 39–54, 2005.

[10] E. Estrada, D. J. Higham, and N. Hatano, "Communicability betweenness in complex networks," *Physica A: Statistical Mechanics and its Applications*, vol. 388, no. 5, pp. 764–774, 2009.

[11] J. M. Kleinberg, "Authoritative sources in a hyperlinked environment," *Journal of the ACM (JACM)*, vol. 46, no. 5, pp. 604–632, 1999.

[12] D. Li, B. Fu, Y. Wang, G. Lu, Y. Berezin, H. E. Stanley, and S. Havlin, "Percolation transition in dynamical traffic network with evolving critical bottlenecks," *Proceedings of the National Academy of Sciences*, vol. 112, no. 3, pp. 669–672, 2015.

[13] A. A. Saberi, "Recent advances in percolation theory and its applications," *Physics Reports*, vol. 578, pp. 1–32, 2015.

[14] O. Artime and M. De Domenico, "Percolation on feature-enriched interconnected systems," *Nature communications*, vol. 12, no. 1, pp. 1–12, 2021.

[15] L. Hébert-Dufresne and A. Allard, "Smeared phase transitions in percolation on real complex networks," *Physical Review Research*, vol. 1, no. 1, p. 013009, 2019.

[16] X. Yuan, Y. Dai, H. E. Stanley, and S. Havlin, "k-core percolation on complex networks: Comparing random, localized, and targeted attacks," *Physical Review E*, vol. 93, no. 6, p. 062302, 2016.

[17] S. R. Broadbent and J. M. Hammersley, "Percolation processes: I. crystals and mazes," in *Mathematical proceedings of the Cambridge philosophical society*, vol. 53, no. 3. Cambridge University Press, 1957, pp. 629–641.

[18] C. J. F. Q. L. Y. XU Xiao, GU Lingli, "An intelligent cooperative algorithm for multi-path routing and subflow allocation," *Computer Engineering*, vol. 47, no. 9, p. 136, 2021.

[19] R. Dewanto, R. Munadi, and R. M. Negara, "Improved load balancing on software defined network-based equal cost multipath routing in data center network," *Jurnal Infotel*, vol. 10, no. 3, pp. 157–162, 2018.

[20] Y. Zhang, M. Roughan, N. Duffield, and A. Greenberg, "Fast accurate computation of large-scale ip traffic matrices from link loads," *ACM SIGMETRICS Performance Evaluation Review*, vol. 31, no. 1, pp. 206–217, 2003.

[21] F. H. L. F. F. L. Zhu WANG, Qingyun YUAN, "Multipath congestion control algorithm based on link capacity," *Journal on Communications*, vol. 41, no. 5, p. 59, 2020.

[22] P. P. Lee, V. Misra, and D. Rubenstein, "Distributed algorithms for secure multipath routing in attack-resistant networks," *IEEE/ACM Transactions on Networking*, vol. 15, no. 6, pp. 1490–1501, 2007.

[23] S. Benatia, O. Smail, B. Meftah, M. Rebbah, and B. Cousin, "A reliable multipath routing protocol based on link quality and stability for manets in urban areas," *Simulation Modelling Practice and Theory*, vol. 113, p. 102397, 2021.

[24] F. Ye, S. Mandal, W. Sun, and M. Zhu, "Weighted cost multipath routing with intra-node port weights and inter-node port weights," Jan. 31 2017, uS Patent 9,559,985.

[25] J. Wang, Y. Hu, Y. Wang, and Q. Zhao, "Anomaly detection method of packet loss node location in heterogeneous hash networks," *Computer Communications*, vol. 178, pp. 201–211, 2021.

[26] Q. Wu, Q.-Y. Liu, X. Ling, and L.-J. Zhang, "The self-adaptive routing strategy to alleviate packet loss in finite buffer networks," *Journal of Statistical Mechanics: Theory and Experiment*, vol. 2021, no. 12, p. 123402, 2021.

[27] Y. Shi, J. Wang, X. Fang, Y. Huang, and S. Gu, "Robust mixed h2/h ∞ control for an uncertain wireless sensor network systems with time delay and packet loss," *International Journal of Control, Automation and Systems*, vol. 19, no. 1, pp. 88–100, 2021.

[28] S. Behal and K. Kumar, "Characterization and comparison of ddos attack tools and traffic generators: A review." *Int. J. Netw. Secur.*, vol. 19, no. 3, pp. 383–393, 2017.

[29] R. Rossi and N. Ahmed, "The network data repository with interactive graph analytics and visualization," in *Twenty-ninth AAAI conference on artificial intelligence*, 2015.

[30] H. An, Y. Na, H. Lee, and A. Perrig, "Resilience evaluation of multipath routing against network attacks and failures," *Electronics*, vol. 10, no. 11, p. 1240, 2021.