K-core-preferred Attack to the Internet: Is It More Malicious Than Degree Attack?

Jichang Zhao[1], Junjie Wu[2], Mingming Chen[1], Zhiwen Fang[1], and Ke Xu[1]

[1] State Key Laboratory of Software Development Environment, Beihang University
[2] Beijing Key Laboratory of Emergency Support Simulation Technologies for City Operations, School of Economics & Management, Beihang University

Abstract. K-core (k-shell) index is an interesting measure that describes the core and fringe nodes in a complex network. Recent studies have revealed that some high k-core value nodes may play a vital role in information diffusion. As a result, one may expect that attacking high k-core nodes preferentially can collapse the Internet easily. To our surprise, however, the experiments on two Internet AS-level topologies show that: Although a k-core-preferred attack is feasible in reality, it turns out to be less effective than a classic degree-preferred attack. Indeed, as indicated by the measure: normalized susceptibility, we need to remove 2% to 3% more nodes in a k-core-preferred attack to make the network collapsed. Further investigation on the nodes in a same shell discloses that these nodes often have degrees varied drastically, among which there are nodes with high k-core values but low degrees. These nodes cannot contribute many link deletions in an early stage of a k-core-preferred attack, and therefore make it less malicious than a degree-preferred attack.

Keywords: Robustness, K-core, AS-level Internet, Malicious Attack.

1 Introduction

The Internet has become the most important communication infrastructure in the world, especially after the explosion of online social networking sites. Tremendous research efforts have been devoted to scale-free networks, such as the AS-level Internet in the level of autonomous system [20,5,21,2]. Among them, attack survivability remains one of the core topics. People find that, while the Internet is robust to the random failure, it is fragile to malicious attacks, which are generally defined as removing important nodes or links from the networks preferentially [1]. Specifically, the simple degree-preferred attack, i.e., attacking the nodes with high degrees preferentially, is often regarded as the most probable attack type in reality. Other types of attacks, e.g., attacking the nodes with higher betweenness preferentially, may be more malicious than the degree-preferred attack, but often need the global topological information of networks and consume much more computational time [3], and thus become infeasible in practice [12].

K-core (k-shell) index is an interesting measure that categorizes the nodes in a complex network into the core nodes and the fringe ones. Recently, in their landmark paper [14], the authors found in many types of complex networks that k-core

J. Wang et al. (Eds.): WAIM 2013, LNCS 7923, pp. 717–728, 2013.

value is a more effective measure to describe the influence of a node to the propagation of information or diseases. Indeed, they disclosed a surprising fact that some nodes with high degrees play a trivial role in the information spreading process. They argued that a k-core viewpoint is more instructive; that is, those high-degree nodes actually have low k-core values and thus locate in the fringe of the network. From this aspect, one may expect that a k-core-preferred attack, i.e., attacking high k-core nodes preferentially, can collapse the Internet more easily than a degree-preferred attack. This motivates our study on the k-core-preferred attack, which to our best knowledge is among the first few studies along this line.

To this end, we performed comparative experiments for the two types of malicious attacks on two real-world AS-level Internet data sets. Six measures including both the structural and propagative ones were introduced to characterize the damages to the networks during the attacks. To our surprise, the results show that: Although a k-core-preferred attack is feasible using the traceroute tool [9,13], it is less malicious than a classic degree-preferred attack. Indeed, as indicated by the normalized susceptibility measure, we need to remove 2% to 3% more nodes in a k-core-preferred attack to make the network collapsed. Further investigation on the nodes in a same shell disclosed that these nodes often have degrees varied drastically, among which there are nodes with high k-core values but low degrees. These nodes cannot contribute sufficient link deletions in an early stage of a k-core-preferred attack, and therefore make it less malicious than a degree-preferred attack.

2 Related Work

Weak attack survivability but strong error tolerance [1] is a dilemma for the complex networks. In recent years, many researchers focus on the robustness analysis and enhancement of complex networks. For instance, Cohen et al. unveiled that the Internet is resilient to random failures [6] but fragile to the intentional attack [7]. Holme et al. proposed four different attacking strategies and found that attacks by recalculating degrees and betweenness centrality are often more harmful than attacks based on the initial network [12]. Meanwhile, as a key metric in complex networks, k-core index also attracts a lot of research interests in the scope of the Internet. For example, Carmi et al. used information on the connectivity of network shells to separate the AS-level Internet into three subcomponents [5]. Zhang et al. found that the k-core with larger k is nearly stable over time for the real AS-level Internet [21]. Zhang et al. proposed a model based on k-core decomposition to model the Internet Router-level topology [22]. In the inspirational work [14], Kitsak et al. focused on evaluating the influence of a node in the spread of information or diseases through its k-core index. They reported an unexpected finding that some hub nodes may locate in the periphery of the network.

Despite of the existed abundant researches on the network robustness and k-core index, little work has been done to unveil whether the attack based on k-core is more malicious than other types of attacks to the AS-level Internet. This indeed motivates our study in this paper.

3 Preliminaries

In this section, we first discuss the feasibility of attacking the AS-level Internet, and then revisit the measures employed to characterize the damages of networks caused by malicious attacks. Finally, the real-world data sets employed in this paper are presented.

3.1 Feasibility of Attacking an AS in the Internet

The network of AS-level Internet stands for business relationships between different *Internet Service Providers (ISP)*. The recent survey by Kevin Bulter et al. revisited several attacking methods [4]. For instance, *prefix hijacking* means an AS A can advertise a prefix from address space belonging to another AS B; then the traffic that should be routed to B would be routed to A falsely, which means AS B is deleted from the network. For another, *link cutting attack* can be manifested by either physically attacking a link or employing Denial-of-Service(DoS) attacks. In addition, there have been quite a few real-world AS-attacking cases in the history of the Internet [4]. For example, in 1997, a misconfigured router maintained by a small *ISP* in Florida injected incorrect routing information into the global Internet and claimed to have optimal connectivity to all Internet destinations. As a result, most Internet traffic was routed to this *ISP*, which overwhelmed the misconfigured router and crippled the Internet for nearly two hours [4]. To sum up, attacking an AS in the real-world Internet is indeed feasible. As a result, discussing attack survivability of the Internet in the level of AS makes physical sense.

3.2 K-Core index

The Internet can be intuitively modeled as a *graph* $G(V, E)$ at different levels, where V is the set of interfaces, routers or ASes, while E is the set of links between them. In this paper, we mainly focus on the AS-level Internet, which means a node stands for an AS and a link stands for the business relationship between its two ends. The number of links of a node is defined as its *degree* k. K-core [19] in a graph G could be defined as the maximum subgraph G^k, in which each node's degree is at least k. By recursively pruning the least connected nodes, the hierarchical structure of the network can be broken down to the highly connected central part, which is stated as the *core* of the network [10]. Then *k-core* (k-shell) index, denoted as k_s, is used to characterize how far a node is from the core of a network. A node i has k-core index k_s if it is in the k_s-core but not in the $(k_s + 1)$-core. A larger k_s indicates the node is closer to the core. K-core can be computed through the following steps [5,14]. First, remove all the nodes with degree $k = 1$. After this step, there may appear new nodes with $k = 1$. Then keep on pruning these nodes until all nodes with degree $k = 1$ are removed. k_s of the removed nodes is then set to 1. Next, we repeat the pruning process in a similar way for the nodes with degree $k = 2$ and subsequently for higher values of k until all nodes are removed. After this process, the k-core values of all the nodes can be determined.

3.3 Measures of Network Robustness

We employ four structural measures to characterize the damage of a network. The *relative size of the giant connected component* (GCC), denoted as f_{GCC}, is a generally used metric to quantify the extent to which a network is damaged. Another intuitive measure is *the number of disconnected clusters* in the network. The greater the number is, the more disconnected sub-networks are due to the attack, which indicates a more serious damage. We can normalize the number by dividing it by the size of the network, denoted as $f_{cluster}$. *Network efficiency* [16] is the only topology property we adopt in this paper, which relates strongly to global shortest paths. It is defined as

$$\Lambda = \frac{1}{N(N-1)} \sum_{i=1,j=1,i\neq j}^{N} \frac{1}{d_{ij}}, \tag{1}$$

where N is the size of the network and d_{ij} is the length of the shortest path between nodes i and j. A lower Λ means the averaged length of shortest paths in the network is longer and the network efficiency is lower. We also employ the *normalized susceptibility* [15], which is denoted as

$$\bar{S} = \frac{\sum n_s s^2}{N}, \tag{2}$$

where n_s is the number of components of size s. If there exists a phase transition in the variation of $\bar{S}$, it means that the network is already collapsed. However, the network is just shrinking if there is no phase transition during the attack.

In [8,17], the AS-level topology of the Internet was employed as the underlying network for worm spread investigation. Hence, we also adopt two propagative measures, corresponding to the Susceptible-Infected-Susceptible (SIS) model and the Susceptible-Infected-Recovered (SIR) model, respectively, to describe the damage status of an AS-level network. For the SIS model, nodes in the network are classified into two categories: the infected ones and the susceptible ones. Each susceptible node can be infected by its infected neighbors with a probability μ, meanwhile an infected one may return to the susceptible status with a probability β. As a result, we denote a SIS model as $SIS(\mu, \beta)$. As time evolves, the *fraction of the infected population* will eventually stabilize at a certain level, denoted as f_c^{SIS}. f_c^{SIS} can be used to characterize how far the disease can spread in the network, and thus reflect the damage status of the underlying network. All other things being equal, a smaller f_c^{SIS} implies a more severe damage. In the SIR model, a node in the network is in one of the three statuses: susceptible, infected and recovered. For a susceptible node, it may get infected by its infected neighbors with a probability μ, and an infected node may get recovered with a probability λ and will never be infected again. As a result, we denote the SIR model as $SIR(\mu, \lambda)$. Here, we utilize the *maximum fraction of nodes that get infected during the spreading process*, denoted as f_{max}^{SIR}, to characterize the worst situation.

Table 1. Traceroute samples

T_{id}	1	2	3	4	5
DIMES-AS	$T(1, 500)$	$T(26, 260)$	$T(53, 530)$	$T(132, 1320)$	$T(264, 2640)$
UCLA-AS	$T(1, 500)$	$T(38, 380)$	$T(76, 760)$	$T(191, 1910)$	$T(382, 3820)$
T_{id}	6	7	8	9	
DIMES-AS	$T(528, 5280)$	$T(793, 7930)$	$T(1057, 10570)$	$T(1321, 13210)$	
UCLA-AS	$T(764, 7640)$	$T(1146, 11460)$	$T(1528, 15280)$	$T(1910, 19100)$	

3.4 Real-World Network Topologies

It is hard to obtain an accurate and complete picture of the AS-level Internet. In order to make our results more reliable and convincing, we use two AS-level Internet data sets. The first one, denoted as DIMES-AS, comes from the project of DIMES[1]. DIMES-AS was released in March, 2010 with 26424 nodes and 90267 links. The second data set, denoted as UCLA-AS, was released by Internet Research Lab in UCLA[2] in November, 2010. We extract the topology only from the map file released on Nov. 23, 2010 and get a network of 38200 nodes and 140726 links.

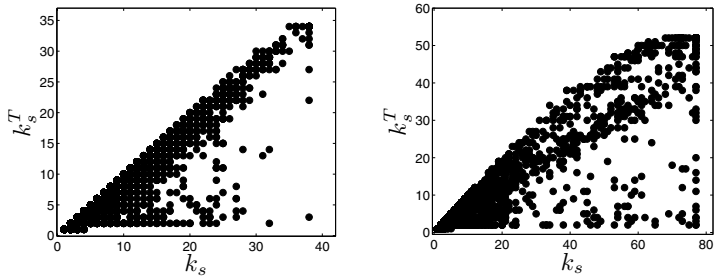
4 Modeling Attacks to the AS-Level Internet

In the section, we first give the definitions of attacks based on the degree and k-core values of network nodes, respectively. Then we demonstrate how to estimate the k-core index, which enables the k-core preferred attack to real-world networks.

4.1 Defining Attacks

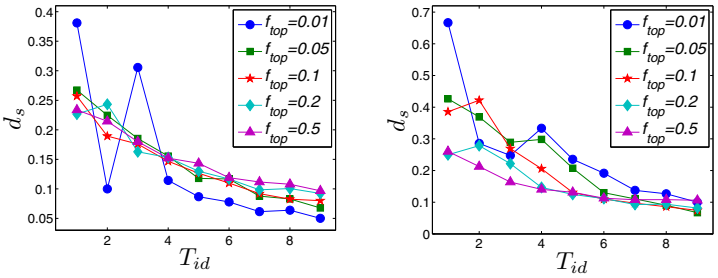
Here we focus on two kinds of malicious attacks in the AS-level Internet. One is the attack based on the node degree, called *degree-preferred attack* (DA). The other is the attack based on the k-core index, called *k-core-preferred attack* (CA). In a degree-preferred attack, we sort all the nodes in the descending order of degrees and remove from the network the ones with high degrees first. Similarly, in a k-core-preferred attack, all the nodes in the network are ranked in the decreasing order of k-core values. Nodes located in the same shell, i.e., having a same k-core value, are further sorted in the decreasing order of degrees. Then the nodes will be removed from the highest rank to the lowest rank gradually. Note that we do not recalculate the nodes' degrees or k-core values after each wave of attack, as done in [12,18].

[1] http://www.netdimes.org
[2] http://irl.cs.ucla.edu/topology/



(a) DIMES-AS with $T(528, 5280)$. (b) UCLA-AS with $T(764, 7640)$.

Fig. 1. Correlation between k_s^T and k_s



(a) DIMES-AS (b) UCLA-AS

Fig. 2. Distances between sample sequences and real sequences

4.2 Estimating the K-Core Index

Generally speaking, the k-core index of a node is robust, i.e., it can be estimated from limited information of the network. To illustrate this, we perform simulations of traceroute [11] on the two AS-level topologies.

In the simulation, we randomly choose the sources and destinations from the network. Each simulation is denoted as $T(s, d)$, where s is the number of sources and d is the number of destinations. For simplification, we let $d = 10s$ (since $d = 10$ is not sufficient to setup the experiment, we let $d = 500$ when $s = 1$), and adopt the typical assumption that a route obtained by traceroute is a shortest path between the source and the destination [9]. Each sample obtained from one pair of (s, d) is denoted as $G^{T(s,d)}$. Table 1 shows the nine samples for DIMES-AS and UCLA-AS, respectively.

We first investigate the correlation between the original k-core index and the new k-core index (denoted as k_s^T) estimated from traceroute samples. As shown in Figure 1, for DIMES-AS with $T(528, 5280)$ and UCLA-AS with $T(764, 7640)$, most of the nodes have their k-core values estimated correctly; that is, they are distributed around the line $k_s = k_s^T$.

We also validate the robustness of k-core index by checking the attack sequence. For each sample $G^{T(s,d)}$ from $T(s,d)$, we obtain the list of nodes in the descending order of k-core values, denoted as $\zeta^{T(s,d)}$. For the nodes with a same k-core value, we reorder them by their degrees. Similarly, from the original network we can get the attack sequence ζ. We then measure the distance between the two sequences $\zeta^{T(s,d)}$ and ζ. We define the distance between two rank lists r_1 and r_2 with a same length as follows:

$$d_s = \frac{\sum_{\forall i,j(i\neq j)} d_{ij}}{n(n-1)}, \tag{3}$$

where n is the length of the rank list, and

$$d_{ij} = \begin{cases} 1 \; r_1(i) > r_1(j), r_2(i) \leq r_2(j) \\ 1 \; r_1(i) < r_1(j), r_2(i) \geq r_2(j) \\ 1 \; r_1(i) = r_1(j), r_2(i) \neq r_2(j) \\ 0 \text{ otherwise} \end{cases}, \tag{4}$$

in which $r_1(i)$ ($r_2(i)$) stands for the rank of i in r_1 (r_2). Therefore, a lower d_s indicates the greater similarity between r_1 and r_2. We select top f_{top} nodes from $\zeta^{T(d,s)}$ as r_1, and select the same nodes from ζ to compose r_2. As shown in Figure 2, for both the `DIMES-AS` and `UCLA-AS` networks, as the number of sources increases, d_s decreases rapidly. For example, in `DIMES-AS`, the sequence from $T(528, 5280)$ is very similar to the real sequence with $d_s < 0.1$. For `UCLA-AS`, the sample $T(764, 7640)$ also captures most of the real sequence information.

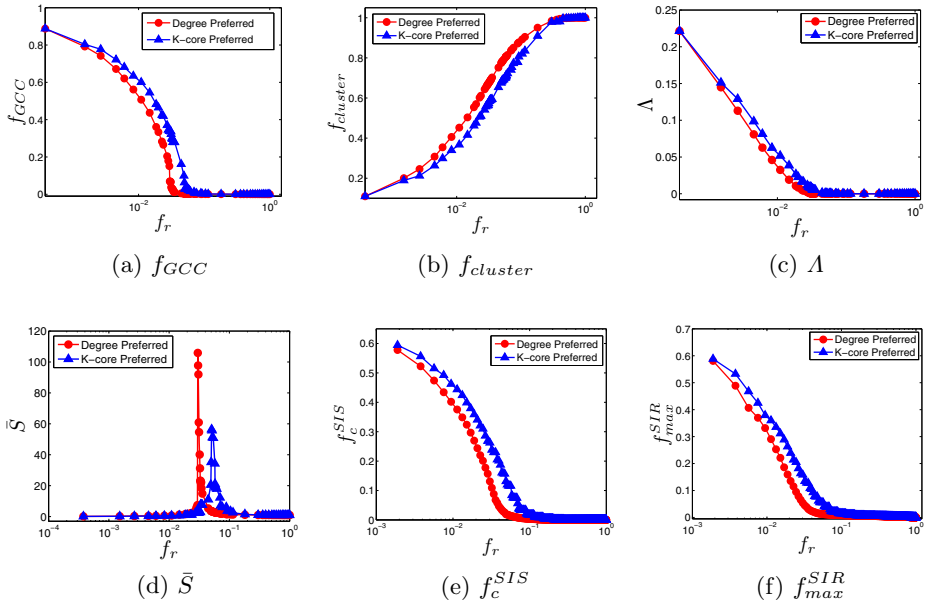
In summary, for the real-world AS-level Internet, the task of estimating the k-core value of an AS, or obtaining the attack sequence based on k-core index, is not that difficult. For `DIMES-AS`, the attackers only need to collect IP addresses from 528 (i.e., 2%) ASes to perform traceroute, and therefore is feasible in reality. For `UCLA-AS`, they may need to collect more IP addresses, say from 764 (i.e., 2%) ASes — but still feasible.

5 Empirical Study

In this section, we perform malicious attacks on real-world AS-level networks, and compare the results using the above-mentioned six measures. Some explanations will then be given to highlight the characteristic of a k-core attack.

5.1 Emperimental Results

Here, we consider the degree-preferred attack and k-core-preferred attack. We denote the fraction of removed nodes as f_r. For the four structural measures, we first perform one round of attack and then calculate the measure values. For the two propagation measures, we first conduct one wave of attack and then simulate the SIS or SIR model on the networks for 100 times, and return the average f_c^{SIS} or f_{max}^{SIR} value. Note that we let $\mu = 1.0$ and $\beta = 0.3$ for the SIS model, and $\mu = 1.0$ and $\lambda = 0.3$ for the SIR model.



(a) f_{GCC} (b) $f_{cluster}$ (c) Λ

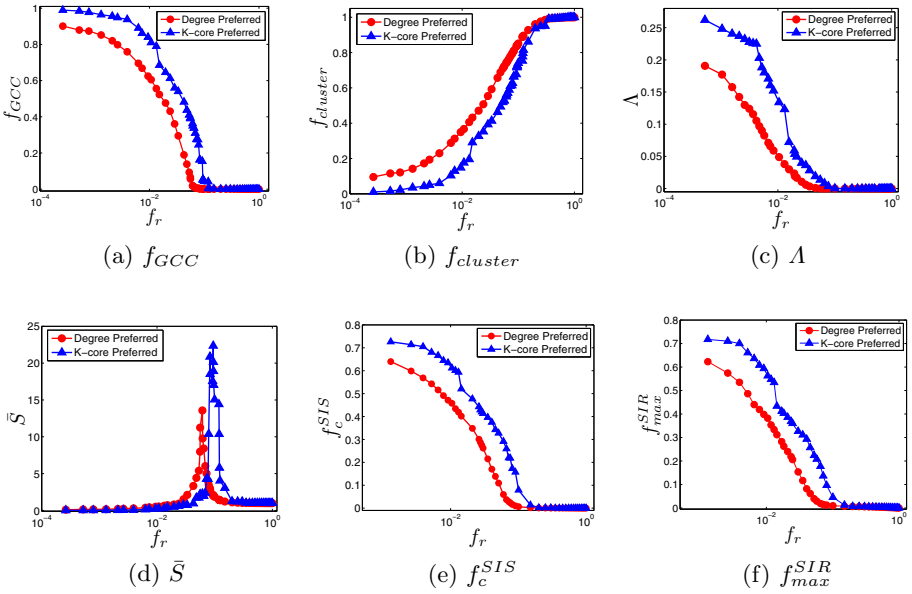
(d) $\bar{S}$ (e) f_c^{SIS} (f) f_{max}^{SIR}

Fig. 3. Comparison of two attacks to `DIMES-AS`

Figures 3 and 4 show the results. As can be seen, to our surprise, we find that the k-core-preferred attack (CA) is less malicious to the AS-level Internet than the degree-preferred attack (DA). We take the `DIMES-AS` network for illustration. As shown in Figure 3a, as f_r increases, f_{GCC} decreases more slowly for CA. This means that after removing the same amount of nodes, the network damaged by CA contains a larger GCC. Meanwhile, $f_{cluster}$ increases more quickly for DA, which implies that DA is more likely to break the network into pieces. As to Λ, it decreases less steeply for CA as f_r grows. That is to say, compared with DA, CA will not degrade the network efficiency rapidly. Finally, regarding to $\bar{S}$, the critical points of f_r at which a phase transition occurs are different for CA and DA. Specifically, the critical point for CA is 0.051, a value much larger than 0.029, the critical point for DA. This implies that DA can result in an earlier collapse of the network. Indeed, additional 528 ASes need to be attacked for CA to collapse DIMES-AS, and this number rises to 1146 in UCLA-AS.

The propagation measures also validate the less maliciousness of k-core-preferred attack. As can be seen in Figure 3e, for the model $SIS(1.0, 0.3)$, f_c^{SIS} decreases more slowly for CA, which means that the information or disease will spread wider in the network bearing CA rather than DA. A similar trend can be found for f_{max}^{SIR} in Figure 3f with the $SIR(1.0, 0.3)$ model. Note that we have tried different configurations of μ, β and λ for the SIS and SIR models, and always obtained results similar to the ones in Figure 3e and Figure 3f.

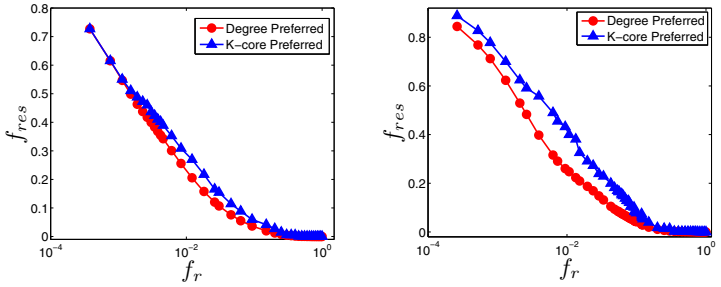
All the six measures indicate a same result for the `UCLA-AS` network in Figure 4; that is, the k-core-preferred attack is less malicious than the degree-preferred attack. Nevertheless, it is still noteworthy that the measure differences between



(a) f_{GCC} (b) $f_{cluster}$ (c) Λ

(d) $\bar{S}$ (e) f_c^{SIS} (f) f_{max}^{SIR}

Fig. 4. Comparison of two attacks to `UCLA-AS`



(a) `DIMES-AS` (b) `UCLA-AS`

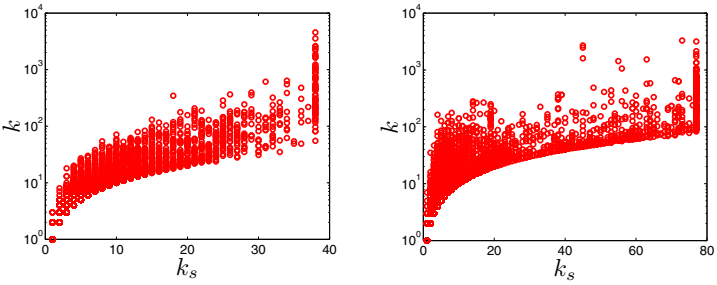
Fig. 5. The fraction of residual links

CA and DA are greater for the `UCLA-AS` network. For instance, as shown in Figure 4d, the critical points for CA and DA are 0.095 and 0.061 respectively, which lead to a gap larger than the one in the `DIMES-AS` network.

In summary, although being influential for information diffusion [14], the concept of k-core seems not that important for malicious attacks. In particular, the k-core-preferred attack is less malicious than the simple degree-preferred attack to the AS-level Internet.

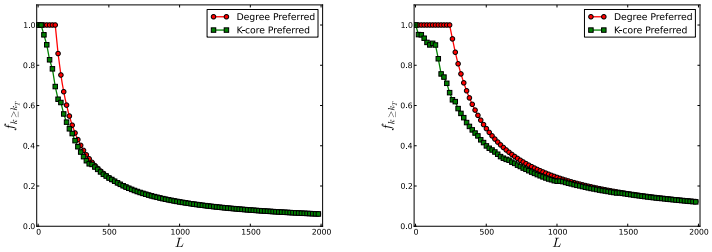
5.2 Explanations and Discussions

Here, we try to explain the above finding by exploring the relationship between the degree and k-core of a node.



(a) DIMES-AS (b) UCLA-AS

Fig. 6. Comparison of degrees in the same shell



(a) DIMES-AS, $k_T = 20\langle k \rangle$ (b) UCLA-AS, $k_T = 20\langle k \rangle$

Fig. 7. Comparison of $f_{k \geq k_T}$

The essence of attacks based on node removals is to delete the links connected to those nodes. We define the fraction of residual links in the network as f_{res} and observe how it varies as f_r increases. As shown in Figure 5, the fraction of residual edges for the k-core-preferred attack is clearly larger than the one for the degree-preferred attack. This implies that the k-core-preferred attack leads to much less link deletions.

Let us take a closer look at the nodes with a same k-core value. As shown in Figure 6, for nodes in the same shell, their degrees vary dramatically. As a result, compared with the degree-preferred attack, the k-core-preferred attack tends to delete less links from the nodes that have higher k-core values but lower degrees. To further illustrate this, we compare the attack sequences of CA and DA. We choose the first L nodes from the sequences and examine the fraction of nodes with degrees no less than a threshold k_T, denoted as $f_{k \geq k_T}$. As shown in Figure 7, compared with the degree-preferred attack, $f_{k \geq k_T}$ is obviously less for the k-core-preferred attack, especially at the early stage when $50 < L < 300$ for DIMES-AS or $50 < L < 1000$ for UCLA-AS. It should also be noted that the gap of $f_{k \geq k_T}$ is greater in UCLA-AS, which could also explain the more evident differences between the two attacking strategies in Figure 3 and Figure 4.

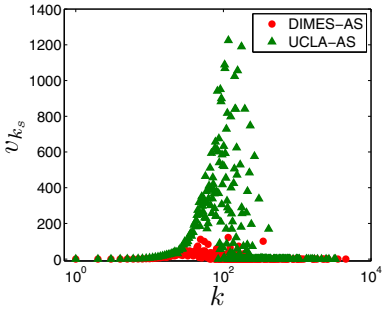


Fig. 8. Variance of k-core for nodes with a same degree

Moreover, to understand why the gap between the two different attacks is more obvious in `UCLA-AS`, we examine the variance of k-core for nodes with a same degree. Figure 8 shows the result. As can be seen, the variance in `UCLA-AS` is much higher than the variance in `DIMES-AS`, especially when $50 < k < 200$. This implies that the attack sequences for DA and CA are more inconsistent in `UCLA-AS`, which eventually leads to significantly different attack effects.

In summary, the reason for the k-core-preferred attack being less malicious is that the nodes with high k-core values may own low degrees, and thus lead to less link deletions in the early stage of the attack.

6 Conclusion

The Internet plays a vital role in modern communications. However, as a typical instance of scale-free networks, it is fragile to the malicious attacks. In this paper, we proposed *k-core-preferred attack*, a malicious attack for nodes with higher k-core values, and compared it with the classic degree-preferred attack. Extensive experiments on two AS-level Internet topologies using six measures demonstrate that: (1) The k-core-preferred attack is feasible in real-world scenarios; (2) The k-core-preferred attack is less malicious than the degree-preferred attack; (3) The nodes in a same shell may have drastically different degrees, which degrades the efficiency of a k-core-preferred attack.

Acknowledgements. This work was partially supported by the fund of the State Key Laboratory of Software Development Environment under Grant SKLSDE-2011ZX-02, the Research Fund for the Doctoral Program of Higher Education of China under Grant 20111102110019, and the National 863 Program under Grant 2012AA011005. Jichang Zhao thanks the China Scholarship Council (CSC) for its support. Junjie Wu was supported in part by National Natural Science Foundation of China under Grants 71171007 and 70901002, by the Foundation for the Author of National Excellent Doctoral Dissertation of PR China under Grant 201189, and by the Program for New Century Excellent Talents in University under Grant NCET-11-0778.

References

1. Albert, R., Jeong, H., Barabási, A.L.: Error and attack tolerance of complex networks. Nature 406(6794), 378–382 (2000)
2. Boguñá, M., Papadopoulos, F., Krioukov, D.: Sustaining the internet with hyperbolic mapping. Nature Communications 1(62) (2010)
3. Brandes, U.: A faster algorithm for betweenness centrality. Journal of Mathematical Sociology 25, 163–177 (2001)
4. Butler, K., Farley, T., McDaniel, P., Rexford, J.: A survey of bgp security issues and solutions. Proceedings of the IEEE 98, 100–122 (2010)
5. Carmi, S., Havlin, S., Kirkpatrick, S., Shavitt, Y., Shir, E.: A model of internet topology using k-shell decomposition. PNAS 104(27), 11150–11154 (2007)
6. Cohen, R., Erez, K., Ben-Avraham, D., Havlin, S.: Resilience of the internet to random breakdowns. Phys. Rev. Lett. 85(21), 4626–4628 (2000)
7. Cohen, R., Erez, K., Ben-Avraham, D., Havlin, S.: Breakdown of the internet under intentional attack. Phys. Rev. Lett. 86(16), 3682–3685 (2001)
8. Cowie, J., Ogielski, A.T., Premore, B.J., Yuan, Y.: Internet worms and global routing instabilities. In: Proc. SPIE, vol. 4868 (2002)
9. Donnet, B., Friedman, T.: Internet topology discovery: a survey. IEEE Communications Surveys and Tutorials 9(4), 2–15 (2007)
10. Dorogovtsev, S.N., Goltsev, A.V., Mendes, J.F.F.: k-core organization of complex networks. Phys. Rev. Lett. 96, 040601 (2006)
11. Guillaume, J.L., Latapy, M., Magoni, D.: Relevance of massively distributed explorations of the internet topology: Qualitative results. Computer Networks 50, 3197–3224 (2006)
12. Holme, P., Kim, B.J., Yoon, C.N., Han, S.K.: Attack vulnerability of complex networks. Phys. Rev. E 65(5), 056109 (2002)
13. Huffaker, B., Plummer, D., Moore, D., Claffy, K.C.: Topology discovery by active probing. In: SAINT-W 2002, pp. 90–96 (2002)
14. Kitsak, M., Gallos, L.K., Havlin, S., Liljeros, F., Muchnik, L., Stanley, H.E., Makse, H.A.: Identification of influential spreaders in complex networks. Nature Physics 6, 888–893 (2010)
15. Kumpula, J.M., Onnela, J.P., Saramäki, J., Kaski, K., Kertész, J.: Emergence of communities in weighted networks. Phys. Rev. Lett. 99(22), 228701 (2007)
16. Latora, V., Marchiori, M.: Efficient behavior of small-world networks. Phys. Rev. Lett. 87(19), 198701 (2001)
17. Liljenstam, M., Yuan, Y., Premore, B.J., Nicol, D.M.: A mixed abstraction level simulation model of large-scale internet worm infestations. In: MASCOTS 2002, pp. 109–116 (2002)
18. Schneider, C.M., Moreira, A.A., Andrade Jr., J.S., Havlin, S., Herrmann, H.J.: Mitigation of malicious attacks on networks. PNAS 108(10), 3838–3841 (2011)
19. Seidman, S.B.: Network structure and minum degree. Social Networks 5, 269–287 (1983)
20. Shakkottai, S., Fomenkov, M., Koga, R., Krioukov, D., Claffy, K.: Evolution of the internet as-level ecosystem. European Physical Journal B 74, 271–278 (2006)
21. Zhang, G.Q., Zhang, G.Q., Yang, Q.F., Cheng, S.Q., Zhou, T.: Evolution of the internet and its cores. New J. Phys. 10(12), 123027 (2008)
22. Zhang, J., Zhao, H., Xu, J., Liu, Z.: Characterizing and modeling the internet router-level topology - the hierarchical features and hir model. Comput. Commun. 33, 2001–2011 (2010)