Physica A 482 (2017) 713–727

Contents lists available at ScienceDirect

Physica A

journal homepage: www.elsevier.com/locate/physa

# Robustness of non-interdependent and interdependent networks against dependent and adaptive attacks

Adam Tyra [a], Jingtao Li [b,c], Yilun Shang [a,d], Shuo Jiang [b], Yanjun Zhao [b], Shouhuai Xu [a,*]

[a] Department of Computer Science, University of Texas at San Antonio, TX 78249, USA

[b] Software School, Fudan University, Shanghai 200433, China

[c] Shanghai Key Laboratory of Intelligent Information Processing, Fudan University, Shanghai 200433, China

[d] School of Mathematical Sciences, Tongji University, Shanghai 200092, China

## HIGHLIGHTS

- The Achilles' Heel phenomenon is **not** valid for dependent attacks.
- Powerful attack strategies (e.g., targeted attacks and dependent attacks, dependent attacks and adaptive attacks) are **not** compatible.
- The attacker cannot take advantage of the different kinds of powerful attacks at the same time.

## ARTICLE INFO

*Article history:*
Received 2 January 2016
Received in revised form 28 March 2017
Available online 29 April 2017

*Keywords:*
Complex networks
Robustness
Percolation
Random attacks
Dependent attacks
Adaptive attacks
Cyber security

## ABSTRACT

Robustness of complex networks has been extensively studied via the notion of site percolation, which typically models *independent* and *non-adaptive* attacks (or disruptions). However, real-life attacks are often *dependent* and/or *adaptive*. This motivates us to characterize the robustness of complex networks, including non-interdependent and interdependent ones, against dependent and adaptive attacks. For this purpose, dependent attacks are accommodated by $L$-hop percolation where the nodes within some $L$-hop ($L \geq 0$) distance of a chosen node are all deleted during one attack (with $L = 0$ degenerating to site percolation). Whereas, adaptive attacks are launched by attackers who can make node-selection decisions based on the network state in the beginning of each attack. The resulting characterization enriches the body of knowledge with new insights, such as: (i) the Achilles' Heel phenomenon is only valid for independent attacks, but not for dependent attacks; (ii) powerful attack strategies (e.g., targeted attacks and dependent attacks, dependent attacks and adaptive attacks) are not compatible and cannot help the attacker when used collectively. Our results shed some light on the design of robust complex networks.



## 1. Introduction

Characterizing robustness of complex networks against attacks (or disruptions) has been extensively studied for both non-interdependent networks (see, e.g., [1–16]) and interdependent networks (see, e.g., [17–28]). However, most studies focused on *independent* and *non-adaptive* attacks that can be accommodated by the standard site percolation [29], perhaps because its simplicity enables analytic treatments. However, real-life attacks are often *dependent* and/or *adaptive*.

* Corresponding author.
*E-mail address:* shouhuai.xu@utsa.edu (S. Xu).

http://dx.doi.org/10.1016/j.physa.2017.04.078
0378-4371/

Dependent attacks cause the deletion of multiple nodes during one attack (i.e., an atomic deletion iteration). The notion of $L$-hop percolation [30,31] models the following dependent attacks: At each iteration, both a chosen node and its neighbors *within* $L$-hop distances are all deleted, where $L = 0$ degenerates to the standard site percolation. Two examples of real-life dependent attacks are the following. In the context of cyber defense against peer-to-peer botnets, which are networks of infected or compromised computers that are controlled by some entities called botmasters [32–36], the defender can eliminate all of the bots that are within some $L$-hop distance of a given bot (i.e., an infected computer under the control of a botmaster). This is realistic because, for example, the bots within $L$-hop distance are located in the same cyber jurisdiction/administration domain [30] (e.g., belonging to the same enterprise network). In the context of transportation networks, the attacker may be able to destroy multiple nodes or sites within some $L$-hop distance of a chosen node. Finally, it should be noted that a related attack strategy has been analytically addressed in [8], where the attacker attempts to destroy the neighborhood of a node.

Adaptive attacks allow the attacker to choose nodes in an adaptive fashion, namely that the selection of the next node for deletion will be based on the current (rather than the initial) state of the network. Adaptive attacks have been used to characterize the effectiveness of social networks based protection of sensitive data [37]. Adaptive attacks have been also used to identify more robust structures with respect to the average of giant component factions, where "average" is on all possible node deletions (i.e., the results obtained after deleting 1, 2, . . . nodes) [38]. This measurement disregards the shape of the curve, which represents fractions of giant components as nodes are deleted; whereas, the shape information is explicitly considered in the present paper. Adaptive attacks are realistic because attackers are often intelligent, but are extremely challenging to treat analytically (the only analytic treatment of adaptive attacks we are aware is [39], which is however in a different problem setting). It is imperative to understand and characterize the robustness of complex networks under adaptive attacks because these attacks represent, in a sense, the worst case scenario, where the attacker attempts to cause the most catastrophic damage by taking advantage of the real-time global state of the network. This is because the attacker, who knows the current global state of the complex network, can always choose to delete the nodes that can cause the most damage. It is therefore plausible to hypothesize that an attacker can cause more damages by launching dependent and adaptive attacks when compared with launching dependent attacks or adaptive attacks separately. Understanding this powerful attack strategy can guide, for example, the design of robust complex network against a spectrum of sophisticated attack strategies.

It is worthwhile to clarify the relationship between adaptive and/or dependent attacks and cascading failures (see, for example, [40–42]). On one hand, cascades are triggered by local failures, but the consequence is non-local and therefore can be more disruptive than dependent attacks. For example, cascading failures can cause catastrophic damages to infrastructures [40,41] and can lead to first-order transition in both non-interdependent networks [41] and interdependent networks [42]. On the other hand, adaptive attacks allow the attacker to choose and delete nodes according to the *present* global state of a complex network throughout the entire attack process. This concept of "present global state" does not have a counterpart in the setting of cascading failures, because the attacker only has the freedom to cause failures to an initial set of nodes (i.e., upon the determination of the set of nodes that fail at the beginning of a cascading process, the nodes that will fail during the cascading process are determined according to the load on the complex network, rather than according to any further input from the attacker.) Although the two classes of attacks are different, it is an interesting future work to investigate whether there is a natural "fusion" of these two classes of attacks or not.

The present paper makes two contributions. First, we propose specifying attacks against (non-interdependent and interdependent) complex networks via the dependence aspect ("how nodes are deleted during each attack iteration") and the adaptiveness aspect ("how nodes are selected at each attack iteration"). This two-dimension specification leads to clear definitions of attacks against complex networks. Second, we characterize the robustness of non-interdependent networks against 10 kinds of attacks, which are combinations of the two-dimensional *node-deletion* and *node-selection* strategies mentioned above. In the study of interdependent networks, we consider 6 kinds of attacks (because the other combinations have no physical meanings). We find that the behavior of complex networks under dependent and adaptive attacks can be very different from its counterpart behavior under independent and non-adaptive attacks. We highlight some of the findings as follows: (i) The Achilles' Heel phenomenon is only valid for independent attacks, but not for dependent attacks. (ii) Powerful attack strategies (e.g., targeted attacks and dependent attacks, dependent attacks and adaptive attacks) are not compatible and cannot help the attacker when used collectively. This insight can guide the design of robust complex networks because it says that the designer and defender can disregard certain attacks that may appear to be devastating at a first glance (e.g., combinations of dependent and adaptive attacks). (iii) Robustness of interdependent networks is dominated by the upper-level network, from which nodes are actively selected for deletion. (iv) When the upper-level network has a power-law degree distribution, the interdependence structure has little impact on the overall robustness.

## 2. Methodology

We characterize robustness of complex networks via the *fraction of the giant component* (which reflects the percolation threshold) and the *mean size of small components* in the node deletion process. This approach has been widely used in the literature (e.g., [3,14,38,43]). We note that another approach is to characterize the existence/non-existence of thresholds (e.g., [17,18,21,44]), which will be reflected in Section 4.1 for interdependent networks.

We consider two *node-deletion* strategies, namely $L = 0$ for independent attacks and $L > 0$ for dependent attacks. Moreover, we consider the following five *node-selection* strategies.