



Effects of Node Protections against Intentional Attack in Complex Communication Networks

Shi Xiao, Gaoxi Xiao

School of EEE

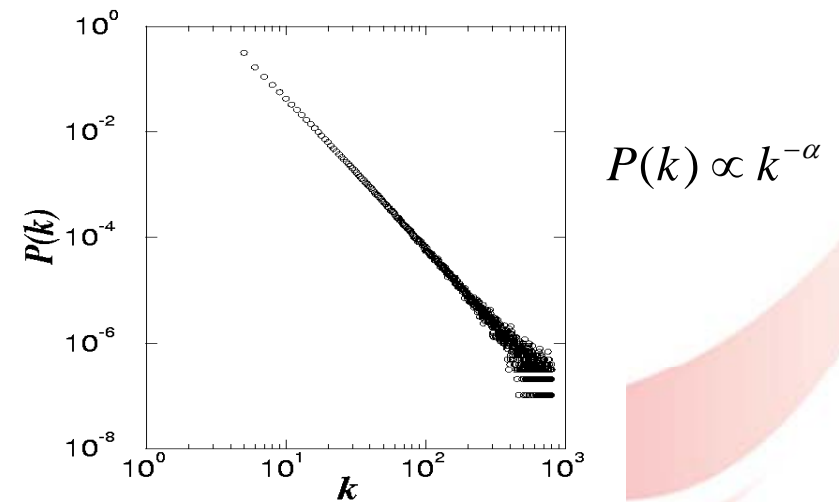
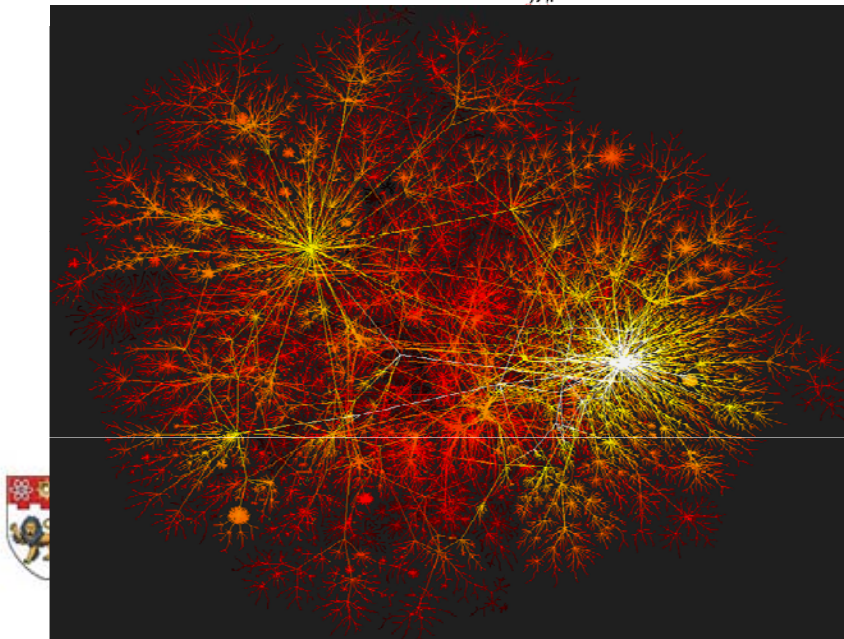
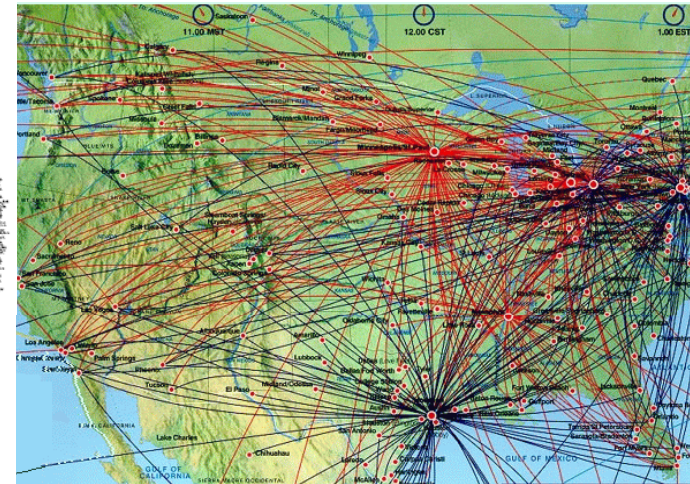
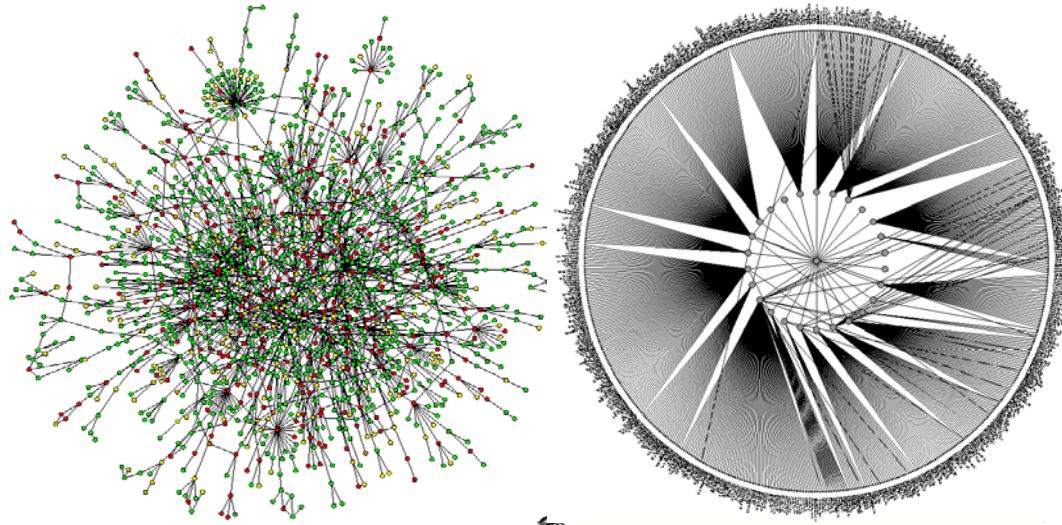
Nanyang Technological University

Singapore

Outline

- **Introduction of background**
 - **Complex networks**
 - **Intentional attacks**
- **Node protection schemes**
- **Simulations on random network models**
- **Simulations on real-life network models**
- **Conclusion**

Complex networks



Some common features of scale-free networks

For example:

- **Tolerance against failure**
 - **Fragile under intentional attack** (even when the attacker has only “local information” in the neighborhood region of the compromised nodes)
 - **Small in diameter (small world)**
 - **Extremely easy for infectious agents to spread out**
- etc. etc.

Node protection schemes to be evaluated

We evaluate a few typical node protection schemes to achieve some benchmark/insights into the effectiveness of protecting high-degree nodes in scale-free networks

- Protect the **single highest-degree** node
- Protect **a few highest-degree** nodes
- The high-degree nodes are all taken down yet some **medium-degree nodes** are protected

Theoretical analysis

Mean-field analysis in random network to analyze the fraction of nodes that needs to be removed in order to eliminate any giant component, i.e., when $\langle k^2 \rangle / \langle k \rangle \leq 2$ (details skipped)

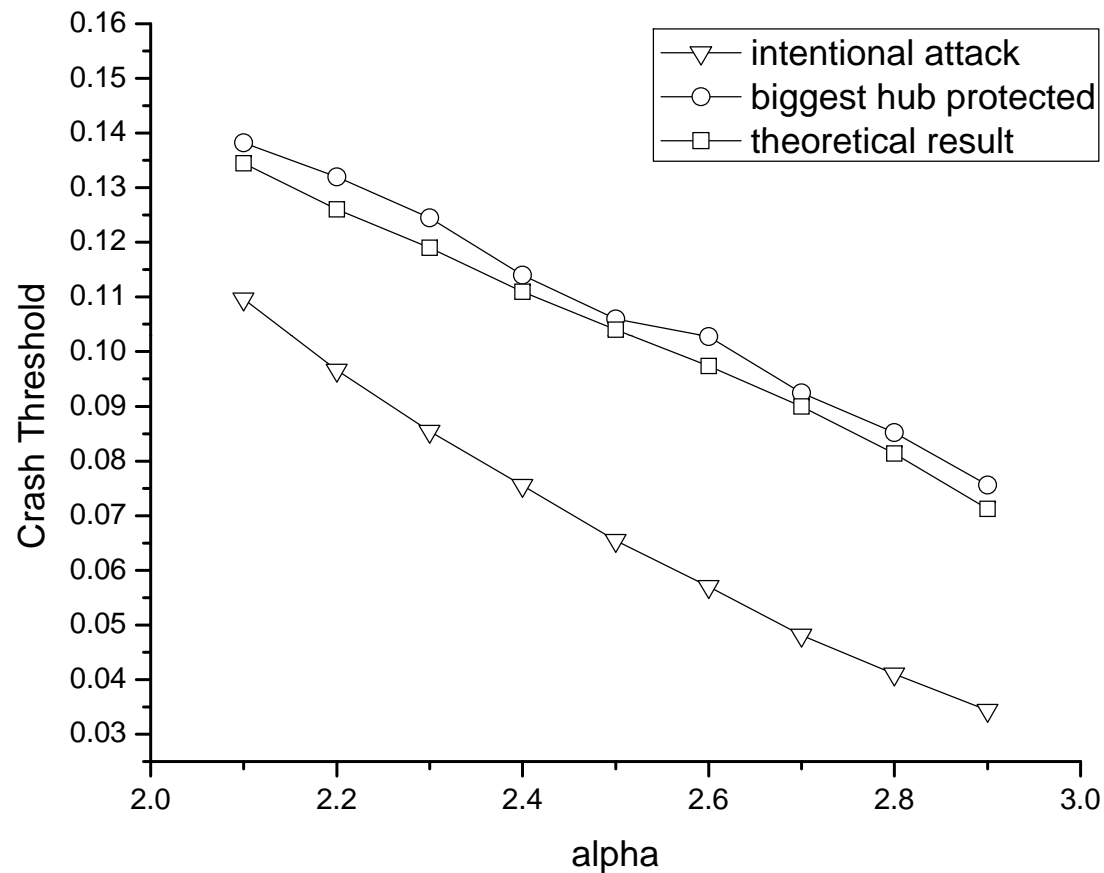
Settings for random network-based simulations

- **10,000-node random scale-free networks**
 - Exponent value (i.e., the α in $P(k) \propto k^{-\alpha}$) varies between 2 and 3.
 - For the case with multiple protected hubs, let N_0 , the number of protected hubs, vary from 1 to 5.
 - For the medium-size node protection scheme, let the top 1% of the biggest hubs be removed and after that, 10% and 50% of the next 1% of largest-degree nodes be protected.

Evaluation metrics

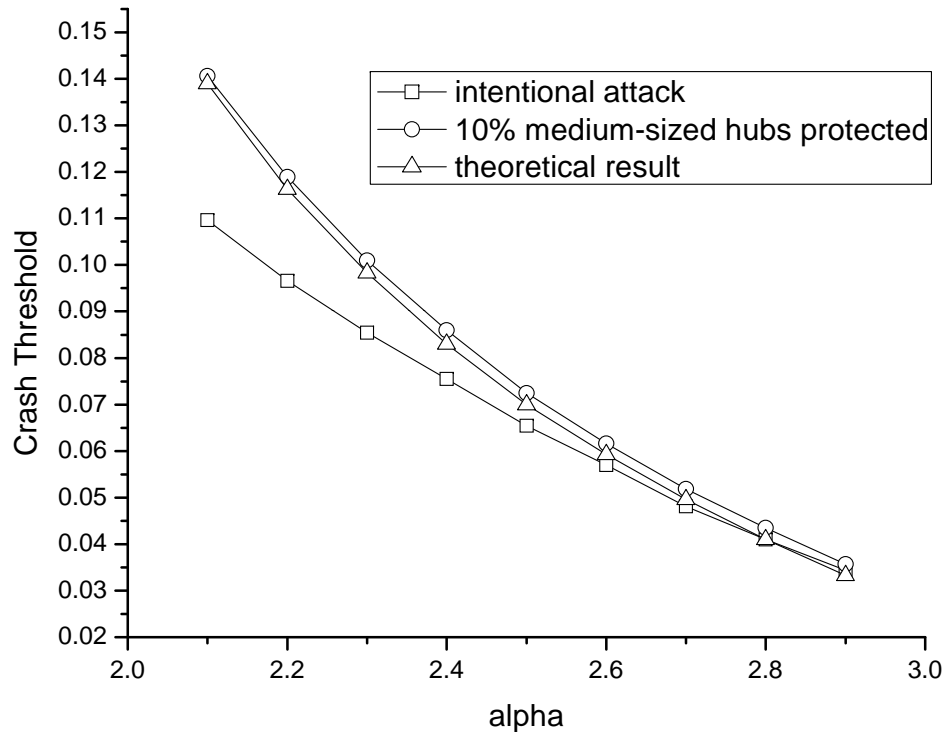
- **Crash threshold:** fraction of nodes to be removed to achieve $\langle k^2 \rangle / \langle k \rangle \leq 2$
- **Cluster diameter:** average hop length of the shortest path between every pair of source-destination nodes in the largest connected component.

Simulation results: single hub protection

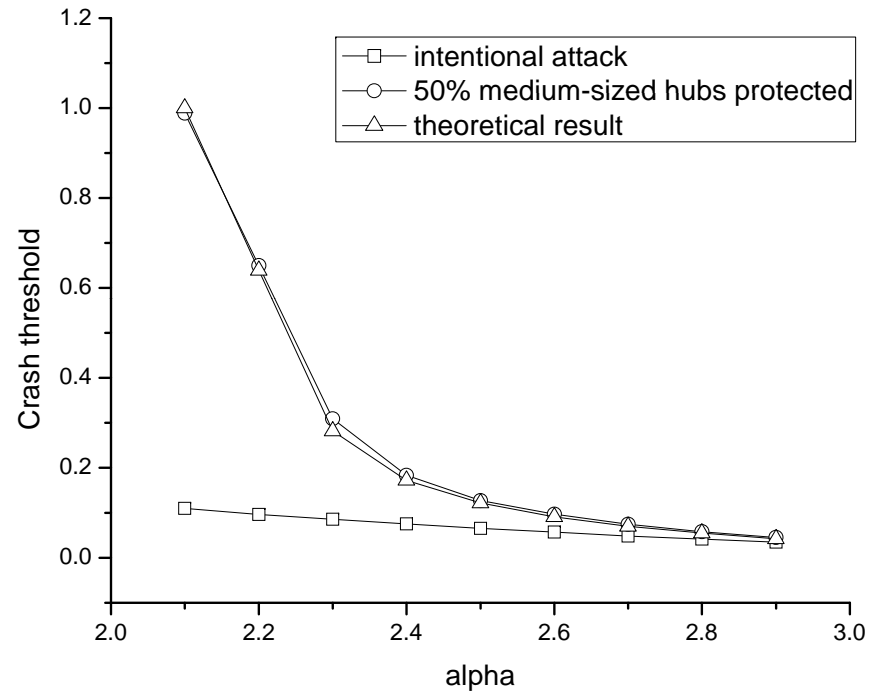


Protecting four of five biggest hubs will be enough to keep the network almost never being crashed.

Simulation results: protecting medium-sized nodes



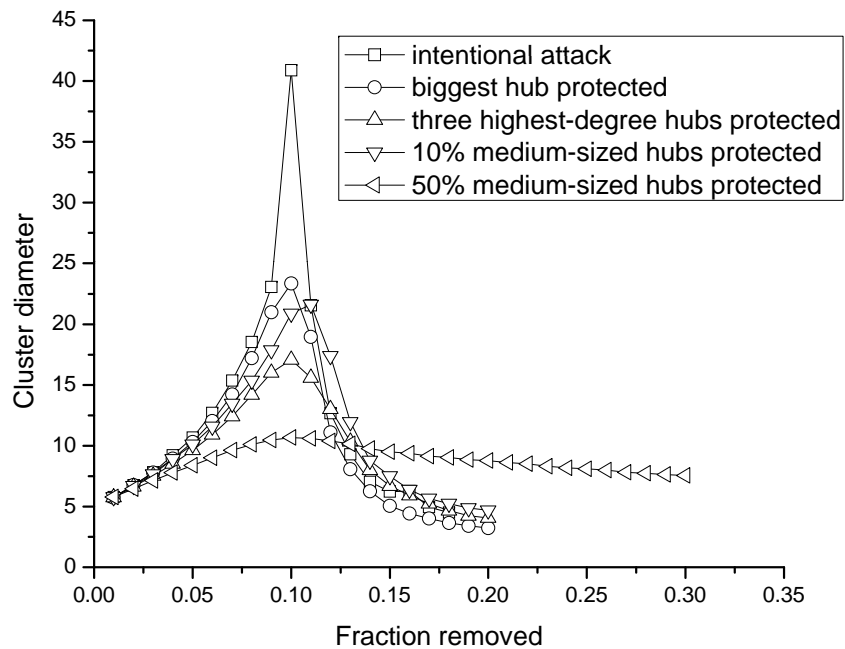
10% medium-sized nodes protected



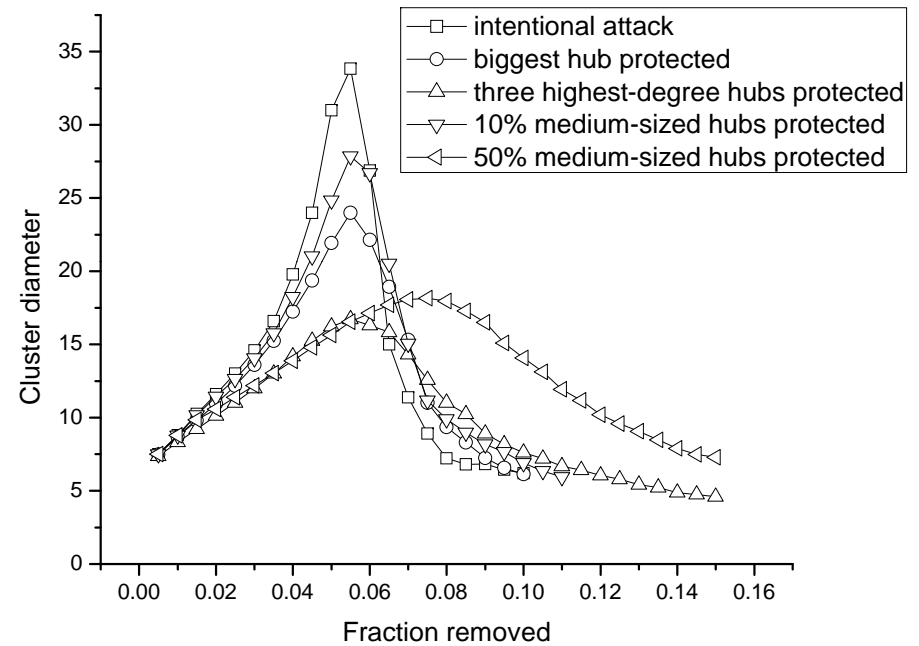
50% medium-sized nodes protected

For $\alpha=2.1$, the protected nodes have their degrees varying from 27 to 45, while for $\alpha=2.9$, it varies from 7 to 12

Simulation results: cluster diameter (1)



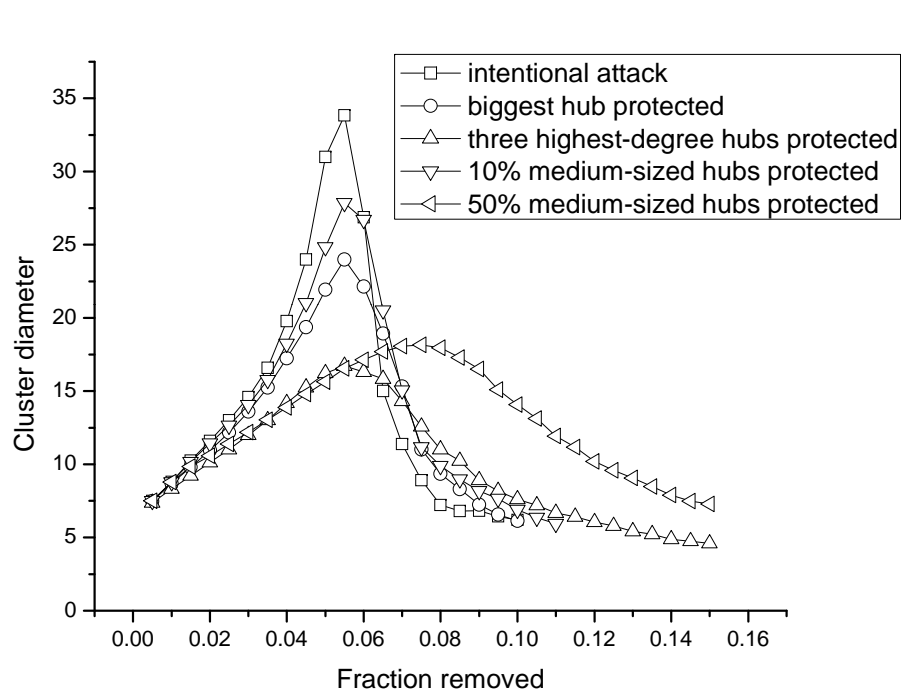
Alpha=2.1



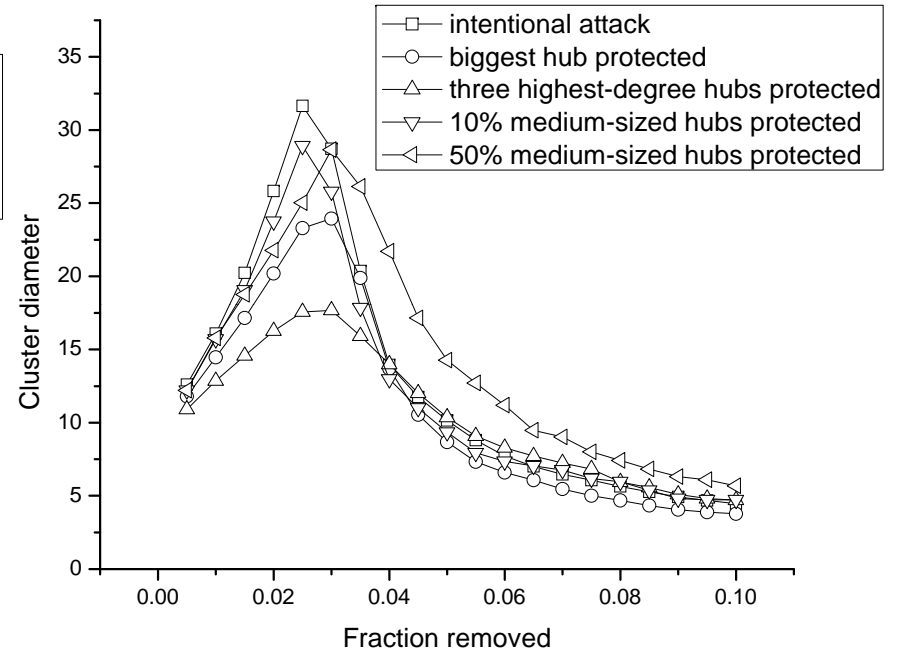
Alpha=2.5

For network with small value of alpha, it is better to protect medium-sized nodes. For network with large alpha, it becomes better to protect a few big hubs.

Simulation results: cluster diameter (2)



Alpha=2.5



Alpha=2.9

The trend becomes more obvious when we compare the cases where $\alpha=2.5$ and 2.9 respectively.

Simulations in real-life networksL simulation settings

Network models

- AS-level Internet model measured by Applied Network Research (NLNR) project in 2000, which contains 6,470 nodes and 12,566 links.
- Router-level Internet model measured by CAIDA, which contains 192,244 nodes and 609,066 links.

We measure:

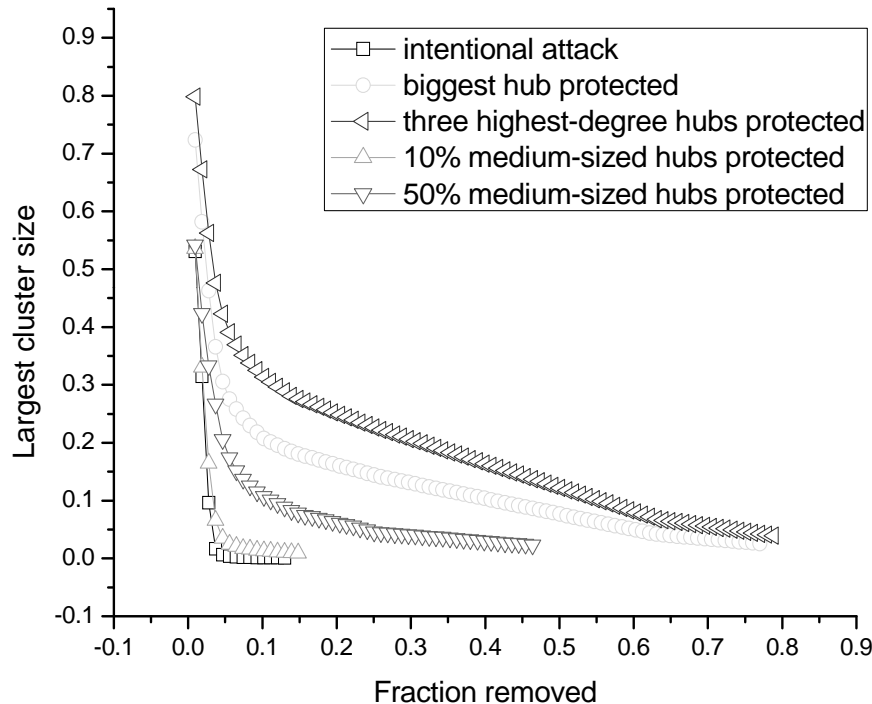
- **Largest cluster size:** number of nodes in the largest connected component versus the number of nodes in the original network.
- **Cluster diameter**

Simulations in real-life networksL

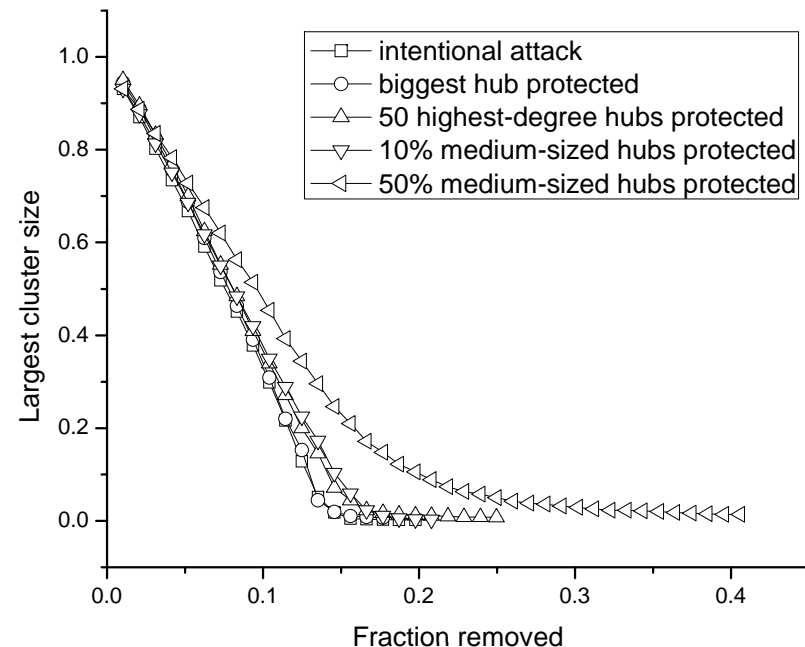
Protection schemes

- Only the biggest hub is protected
- A few highest-degree hubs are protected. Specifically, we let the top 3 hubs be protected in AS-level model and top 50 nodes be protected in router-level model.
- The medium-sized node protection:
 - In the router-level model, we let the top 1% of the biggest hubs be removed and after that, 10% and 50% of the next 1% highest-degree nodes are protected.
 - In the AS-level model, we let the top 0.5% of biggest hubs be removed and after that, 10% and 50% of the next 1% highest-degree nodes are protected. Protected nodes have degrees varying 26 to 61 in AS-level model, and 38 to 55 in router-level model.

Simulation results: largest cluster size



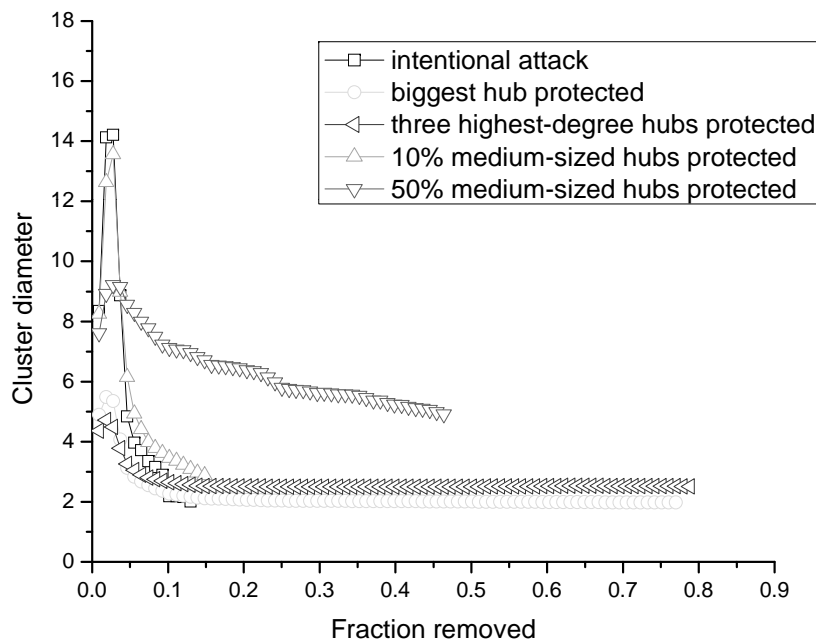
AS-level model



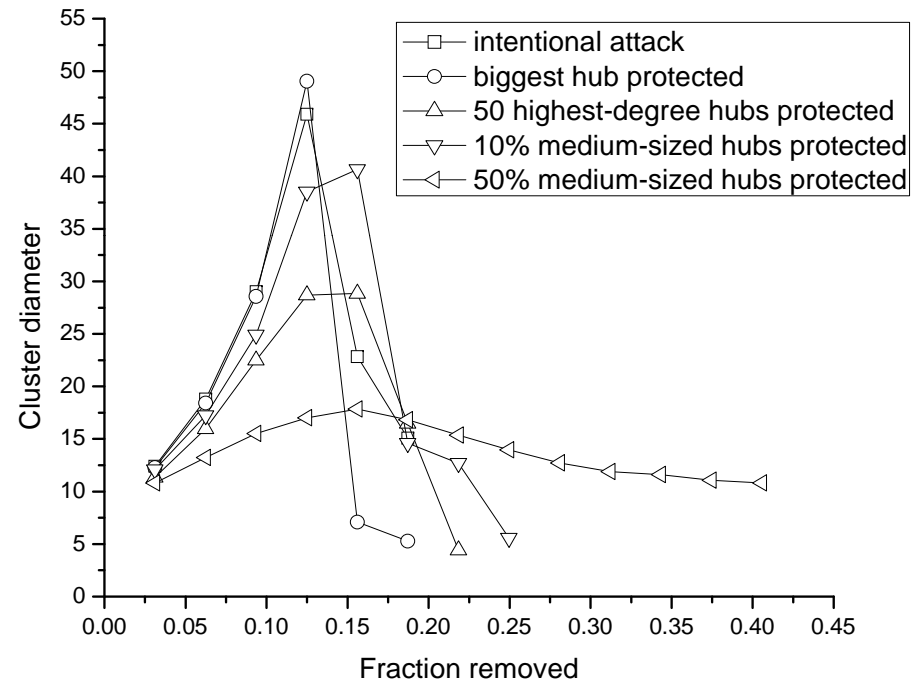
Router-level model

Highest nodal degree: 1458 in AS model, 1071 in router-level model
Combined top hub degrees: 2899 and 23,696
Combined medium-node degrees: 2696 and 91,901, respectively.

Simulation results: cluster diameter



AS-level model



Router-level model

Again, hub protection is more effective in AS-level model, while medium-sized node protection is more effective in router-level model.

Conclusions

- Overall speaking protecting a limited set of high or medium-degree nodes help enhance network robustness significantly.
- Different schemes perform differently in different networks.
 - It is more effective to protect a few big hubs in networks with big hubs or large exponent values
 - It may be more effective to protect a relatively larger number of medium-degree nodes in networks with moderate-size hubs or small exponent values.
- Rule of thumb: protecting more links when it is possible. When protecting roughly the same number of links, protecting higher-degree nodes usually helps.

Other results and future work

- Even when we cannot perfectly protect all the links connected to the high- or medium-degree nodes, an “**imperfect protection**” still helps enhance network robustness against intentional attack significantly.
- For epidemic spreading in complex networks: the conclusion is that imperfect protection does not easily prevent an outbreak from happening but will significantly lower the infection size

What we do not know

- Best protection (say, subject to a cost constraint) for a given nonrandom network.
- Best protection in interconnected and inter-dependent systems, etc.

Thank you!