On the Effectiveness of Sybil Defenses based on Online Social Networks

David Koll
University of Göttingen
Germany
koll@cs.uni-goettingen.de

Jun Li
University of Oregon
USA
lijun@cs.uoregon.edu

Joshua Stein
University of Oregon
USA
jgs@cs.uoregon.edu

Xiaoming Fu
University of Göttingen
Germany
fu@cs.uni-goettingen.de

I. INTRODUCTION

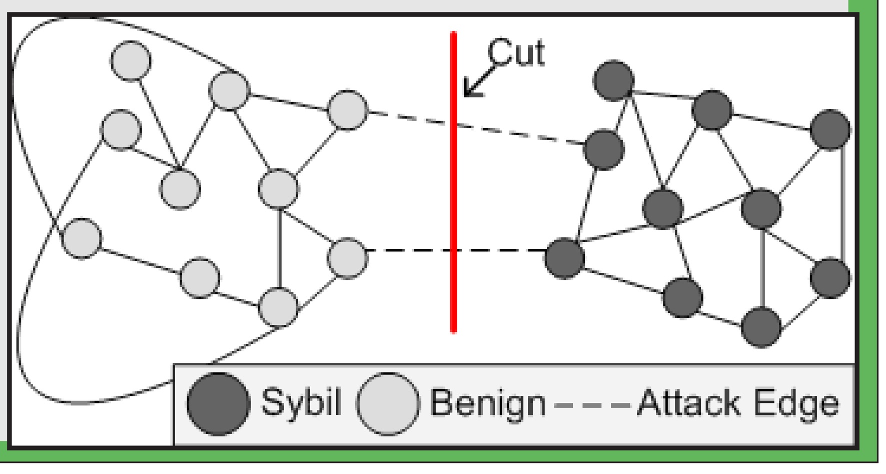
» One way of defend against Sybil Attacks: use Online Social Networks (OSNs)

» Assupmption: Sybils have difficulties to establish links to honest nodes (attack edges), which results in a minimal cut in the OSN graph

» State-of-the-Art:

» Detect Sybils by their position in graph (Sybil Detection)

» Limit influence of Sybils' (Sybil Tolerance)



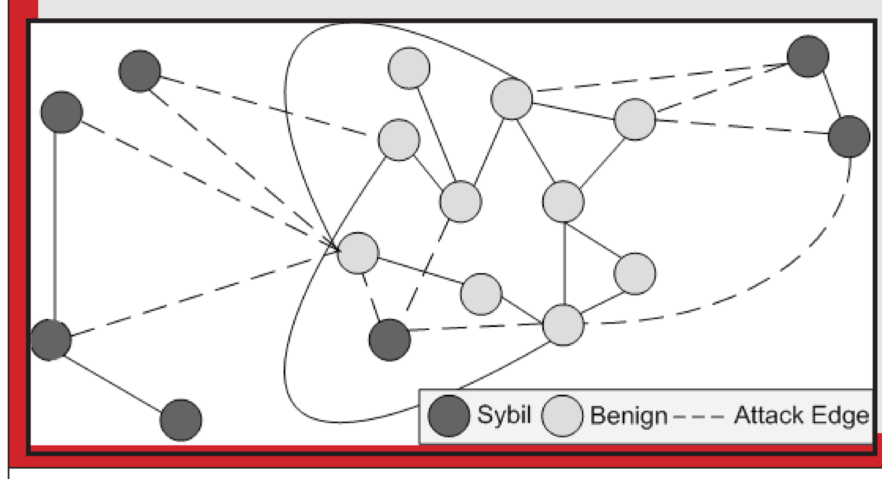
II. TROUBLING OBSERVATIONS

» Recent observations suggest that...

» Up to 90% of requests by Sybils are accepted by honest users

» A Sybil can passively gain hundreds of attack edges per day

» Sybils do not interconnect with each other as suggested, but rather with honest nodes (ratio 1/4 : 3/4)



» Our work:

» Revisit State-of-the-Art, analyze and evaluate the performance under new assumption

III. SYBIL DEFENSES UNDER PRESSURE

» Sybil Detection (SD) approaches:

» Exploit the low reachability of Sybils from a trusted node

» Primary method: random walk (exception: GateKeeper [4])

» Decision (YES/NO for admission):

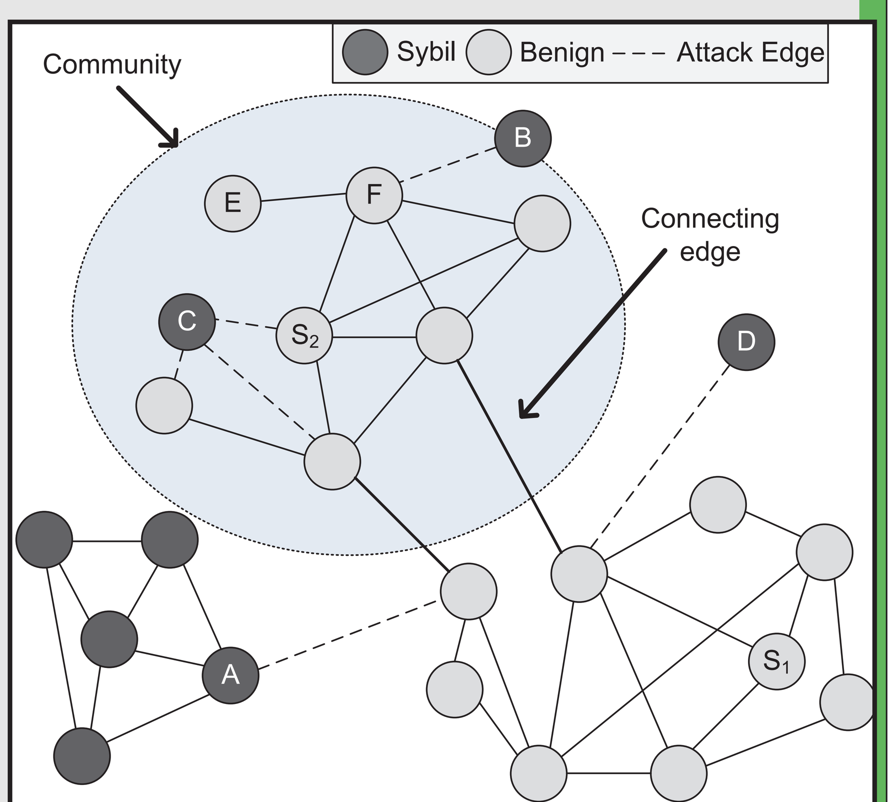
» Do walks intersect with a verifier? [1,2]

» Landing probability of random walk [3,4]

» Number of tickets obtained [5]

» New assumption:

» Unable to distinguish?



» Sybil Tolerance (ST) approaches

» Limit influence of Sybils

» Less universal than SD

» Primary method: credit networks

» Decision (YES/NO for specific application):

» Path in OSN graph from source to destination with credit?

» Send message [6]/collect vote [7] on path ; block otherwise

» New assumption:

» Increases spam and risk of honest user blocking

IV. EVALUATION

» SD approaches - Example SybilRank [3]:

» If a Sybil node can obtain two randomly placed attack edges, it will rank better than 30% of honest nodes

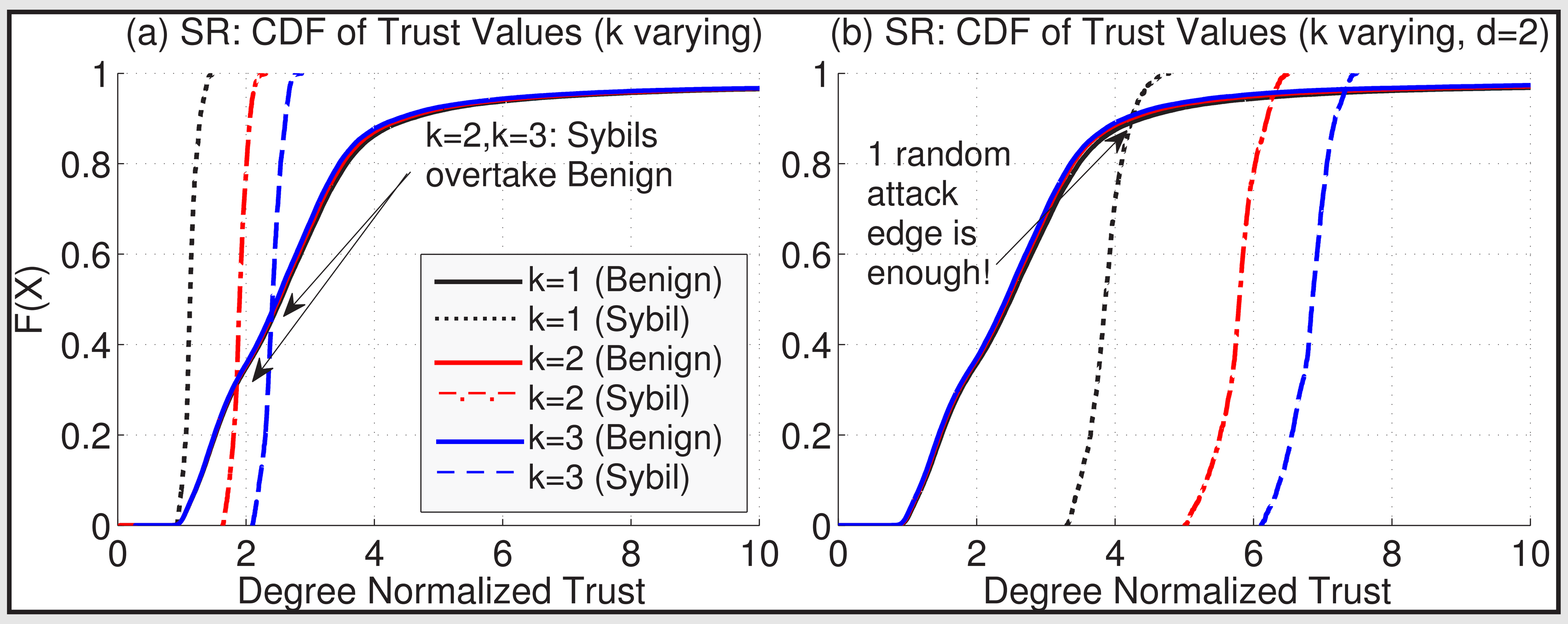
» Exclusion of all Sybils -> exclusion of 30% of honest nodes

» Reduce Sybil's distance to the trust seed -> one randomly placed edge is enough

» Exclusion of all Sybils -> exclusion of 85% of honest nodes

» All other SD approaches have the same issues.

» Best performance: Slightly modified SybilLimit breaks at k=5

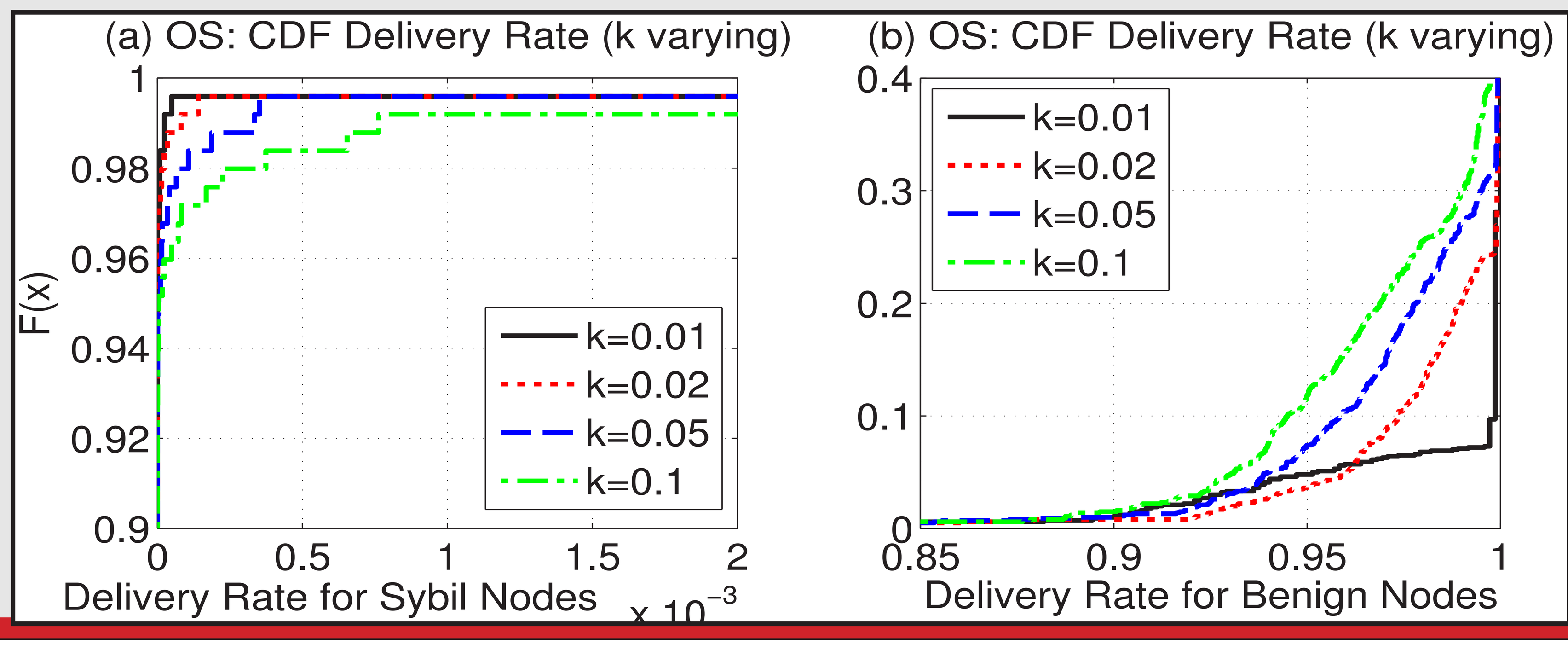


» ST approaches - Example Ostra [5]:

» Spam mitigation works well

» But: number of blocked edges increases

» Similar for SumUp and: Sybils can cycle through attack edges



V. CONCLUSION & DISCUSSION

» A handful of attack edges is sufficient to confuse SD approaches

» Goes along with theoretical guarantees from SD approaches (O(log n) admitted Sybils per attack edge)

» But: Sybils have shown to average about 150 attack edges

» In ST approaches, issues are more specific:

» Blocked messages, cycling through attack edges

» Purely structural approaches are not a good choice

» Enrich the links with meta data to distinguish honest links from attack edges in future approach

REFERENCES:

[1] H. YU, M. KAMINSKY, P. B. GIBBONS, AND A. D. FLAXMAN, "SybilGuard: Defending Against Sybil Attacks via Social Networks", IEEE/ACM Transactions on Networking 16 (2008)

[2] H. YU, P.B. GIBBONS, M. KAMINSKY, AND F. XIAO, "SybilLimit: a near-optimal Social Network Defense against Sybil Attacks", IEEE/ACM Transactions on Networking 18 (2010)

[3] Q. CAO, M. SIRIVIANOS, X. YANG, AND T. PREGUEIRO, "Aiding the Detection of Fake Accounts in Large Scale Social Online Services", NSDI'12 (2012)

[4] G. DANEZIS, AND P. MITTAL, "SybilInfer: Detecting Sybil Nodes using Social Networks", NDSS'09 (2009)

[5] N. TRAN, J. LI, L. SUBRAMANIAN, AND S. CHOW, "Optimal Sybil-resilient Node Admission Control", INFOCOM'11 (2011)

[6] A. MISLOVE, A. POST, P. DRUSCHEL,AND K. P. GUMMADI, "Ostra: Leveraging Trust to Thwart Unwanted Communication," NSDI'08 (2008)

[7] N. TRAN, B. MIN, J. LI, AND L. SUBRAMANIAN, "Sybil-resilient Online Content Voting," NSDI'09 (2009).