# Measuring Vulnerability of Complex Networks by Simulating DDoS Attacks

Igor Mishkovski, Dimitar Trajanov, Sonja Filiposka

# Measuring Vulnerability of Complex Networks by Simulating DDoS Attacks

Igor Mishkovski, Sonja Filiposka, Dimitar Trajanov and Ljupco Kocarev, *Member, IEEE*

*Abstract* — **In this paper we assess the vulnerability of different generic complex networks by measuring the throughput for networks with different load in presence of Distributed Denial-of-Service (DDoS) attacks. DDoS attacks are simulated by choosing a number of bot nodes using several measures, such as: random, degree centrality, eigenvector centrality, betweenness centrality and *k*-medoids clustering algorithm. In order to obtain some information about the vulnerability of the three different complex networks (random, small-world and scale-free) we analyze the useful throughput of these networks in the presence of DDoS attack by the bot nodes.**

*Keywords* — **Complex networks, DDoS attacks, Network Utility Maximization, Vulnerability.**

## I. Introduction

IN today's everyday life we are surrounded with complex systems. These complex systems can be represented as networks with a certain number of nodes joined together by edges. Commonly cited examples include social networks, technological networks, information networks, biological networks, communication networks, neural networks, ecological networks and other either naturally occurring or man-made occurring networks. The topology of these complex networks is one aspect that might help understand in details the surrounding complex systems and its exploration started with the graph theory introduced by Erdős and Rényi [1]. Erdős and Rényi introduced random models in order to model the real complex systems and to capture some of the main characteristics of the real complex systems. However, these models could not give a clear picture of the topology of complex systems and there was an increasing need of new more realistic models. Watts and Strogatz found out that many real world networks exhibit what is called the small-world property, i.e. most vertices can be reached from the others through a small number of edges, like in social networks. After the introduction of the Watts and Strogatz's model, Barabási and Albert showed that the structure and the dynamics of the network are strongly affected by nodes with a great number of connections [2]. It was found that many real complex networks have a power-law distribution of a node's degree and by that they are in fact scale-free networks. Additionally, many of the systems are strongly clustered with a big number of short paths between the nodes, i.e. they obey the small world property.

Recently, the primary interest in complex networks is the flow properties of the transport entities. In the complex systems there are many types of flows, such as: traffic flows, information flows, energy flows, chemical flows, idea flows, etc. In particular, the most interesting aspect is how the networks structure affects the flow properties, like traffic congestion [3]. In addition to this, many researchers have studied how attacks or failures of nodes affect the traffic performance in the network [4]. This is a present problem in the real-world networks like the power grids, the Internet, telephone networks and transportation networks. In [5] authors study the robustness to random and intentional node attacks. In this study when a node is attacked, the flows which go through the node have to reconfigure their paths which may affect the loads on the other nodes and may start a sequence of overload failures. Their results show that scale-free networks are highly robust to random node failures but fragile to intentional node attacks, while the random graphs are robust under both node attacks. In their results, the flow rates are assumed to be fixed even after the reconfiguration of flow paths.. In [6] authors analyze the total throughput of ad hoc networks with different network interaction models at communication level. Their results show that the full-mesh network has highest throughput, while scale-free and star networks show lowest throughput.

The rest of the paper is organized as follows. In Section 2 we present the way we consider DDoS attacks in the network, while in Section 3 we present the network utility maximization problem with its constraints and utility function. Afterwards, in Section 4 we give the description of the various strategies for intentional node and edge attacks. Simulation results and analysis are given in Section 5 and Section 6 concludes this paper.

## II. DDoS Attacks

The primary goal of DDoS attacks is to take down certain sites by bandwidth or server extortion caused by the excessive traffic thrown at the target. These kind of attacks scale from small and targeted attacks to large attacks from thousand of bots, affecting not only the target victim, but also the infrastructure of the service provider. Today, we witness a great sophistication and bigger magnitude of these kind of attacks. For more information about DDoS based attacks refer to [15-22].

In this paper we are assessing the vulnerability of complex networks based on optimal flow measurements

Igor Mishkovski, DELEN, Politecnico di Torino, Turin, Italy (e-mail: igor.mishkovski@polito.it).

Sonja Filiposka, Faculty of Electrotechnics and Information Technology, Skopje, Macedonia (e-mail: filipos@feit.ukim.edu.mk).

Dimitar Trajanov, Faculty of Electrotechnics and Information Technology, Skopje, Macedonia (e-mail: mite@feit.ukim.edu.mk).

Ljupco Kocarev, Macedonian Academy of Sciences and Arts, Skopje, Macedonia (email: lkocarev@manu.edu.mk).

under DDoS attacks. We are using three models of complex networks as underlying networks: random, small-world, scale-free. On these models we calculate the optimal bandwidth allocation solution for a given flow scenario. We use different flow scenarios, ranging from scenario where there are only 10% of the available flows in the network to scenario where there 50% of the available flows. Then we introduce bot nodes which aim is to generate DDoS traffic. We change the percentage of bot nodes from 1% to 30%. The bot nodes generate DDoS traffic to all the nodes in the network and they are chosen using random, degree, betweenness and k-medoids strategy. The vulnerability of a given network in a given scenario is calculated by finding the percentage of DDoS traffic in the optimal bandwidth allocation solution for a given flow scenario, i.e. the higher the percentage of DDoS traffic, the network is more susceptible to DDoS attacks.

Therefore, the main goal of this work is to measure and analyze the vulnerability of different complex networks by simulating DDoS attacks and by choosing the nodes which will perform the attacks using different strategies.

## III. Network Utility Maximization Problem - NUM

Consider a network with m edges, labeled 1, . . . ,*m*, and *n* flows, labeled 1, . . . , *n*. Each flow has an associated nonnegative flow rate $f_j$; each edge or link has an associated positive capacity $c_i$. Each flow passes over a fixed set of links (its route); the total traffic $t_i$ on link *i* is the sum of the flow rates over all flows that pass through link *i*. The flow routes are described by a routing matrix $R \in R^{m x n}$, defined as:

$$R_{ij} = \begin{cases} 1 & \text{flow } j \text{ passes through link } i \\ 0 & \text{otherwise.} \end{cases} \qquad (1)$$

Thus, the vector of link traffic, $t \in R^m$, is given by *t* = *Rf*. The link capacity constraint can be expressed as $Rf \le c$.

The aim of transmitting a flow of packets from their source to the destination is to get some benefit from the information transmission. Thus, it is natural to set a utility function $U_j$ for flow *j*, and assume that $U_i$ is related to its rate $f_j$. In this work as a utility function we use a function which provides proportional fairness among the end users:

$$U(f_j) = \log f_j \qquad (2)$$

This function is strictly concave, because the second derivative is negative. From the concavity of the utility function it follows that the optimal rates $\{\hat{f}_j\}$ satisfy the following condition:

$$\sum_j \frac{f_j - \hat{f}_j}{\hat{f}_j} \le 0, \qquad (3)$$

This means that if rate of one transmitter rises, the rate of another transmitter will drop, and the drop will be proportionally larger than the rise. This property is known as the law of diminishing returns.

In order to maximize the utility we have to solve the following convex problem:

$$\begin{aligned} &\text{maximize } \textstyle\sum_{j=1}^{n} \log f_j \\ &\text{subject to } Rf \le c, \end{aligned} \qquad (4)$$

with variable *f*, and the implicit constraint $f \ge 0$.

Some comments about the NUM problem are given in the text below.

An unfair resource allocation is also possible, in which the goal is to maximize the overall throughput without any consideration about the fairness among the end users. If this is the case, then the unfair utility function would be:

$$U(f_j) = f_j \qquad (5)$$

Additionally some reformulations and relaxations can be used by which the NUM problem can be decomposed both horizontally and vertically, and can be solved in distributed manner as in [15] and [16]. These decompositions are not needed for our analysis, because we are interested in overall network performance, so we solve the problem in a centralized manner.

In order to represent the performance of the complex network we use the maximum end-to-end throughput (*MT*) as performance indicator. *MT* is the total amount of bits received by all nodes per second and is measured in Mega bits per second (Mbps):

$$MT = \sum_{j \in n} f_j \qquad (6)$$

## IV. Attack Strategies

In order to assess the vulnerability of the network we have to simulate the DDoS attacks by choosing the bot nodes which will generate DDoS traffic. We choose the bot nodes using 5 strategies.

The first and the simplest one is to choose the nodes at **random**.

Another strategy is to choose the nodes by their **degree (DEG)**. Degree centrality is a measure which is based on the idea that more important nodes (edges) are more active, that is, they have more neighbors in the graph [17], [18]. It may be used for finding the core nodes (or edges) of a certain community.

**Betweenness centrality (BTWN)** is a measure of the importance of a node in a network, and is calculated as the fraction of shortest paths between node pairs that pass through the node. Betweenness is, in some sense, a measure of the influence a node has over the flow of information through the network. Let *G* be a graph given with set of nodes *V* and set of edges *E*. Let *s* and *t* be nodes of the graph. $\sigma_{st}$ is the number of paths that pass from *s* to *t*. Let $\sigma_{st}(v)$ be the number of shortest paths that pass through the node *v*. The central betweenness of node *v* is:

$$C(v) = \sum_{s \ne v \ne t \in V} \frac{\sigma_{st}(v)}{\sigma_{st}} \qquad (7)$$

With **eigenvector centrality (pagerank) – PR** we can find out the importance of nodes according to the adjacent matrix of a connected graph [19], [20]. It assigns relative scores to all nodes in the network based on the principle that connections to high-scored nodes contribute more to the score of a node than connections to low-scored nodes.

The last strategy is the **k-medoids clustering algorithm**

[21], which is a simple algorithm and it is a discrete version of the well known *k*-means clustering algorithm [22]. The algorithm requires that the value of *k* is known in advance (in our case it is the number of bot nodes). It uses some measure to represent the distance between a pair of instances. The procedure is as follows: (1) randomly select *k* bot nodes to serve as "seeds" for the *k* clusters; (2) assign the remaining nodes to the cluster of the nearest seed; (3) calculate the medoid of each cluster using local closeness centrality and selecting the node with the greatest closeness score; and 4) repeat steps 2 and 3 using the medoids as seeds until the clusters stabilize.

## V. Simulation And Results

For our simulations we are using the above mentioned network models, where each network generator generates 5 samples of the 4 network models. Each sample has $n$=100 nodes and average node degree around 6 as it is found common in many networks. First, we choose the bot nodes in the network (the number of bot nodes *b* ranges from 1 to 30). The bot nodes are chosen using random, degree (DEG), betweenness (BTWN), pagerank (PR) and k-medoids strategy. After defining the bot nodes we generate DDoS flows $f_j^{BN}$ from every bot node to any other node in the network. The flow rate $f_j^{BN}$ is generated randomly and it is between 0 and 1. Second, from the remaining nodes (*n-b*) we define the number of useful flows, which is either 10% (low load) or 50% (higher load) of the total available flow in the network and each O-D (Origin – Destination) pair is generated randomly from the *n-b* nodes. The flow rate $f_j$ is also generated randomly and it is between 0 and 1. The capacity $c_i$ of all links in the networks is equal to 1.

In order to solve our network utility maximization problem defined with (4) we are using the CVX implementation in Matlab [23].

The simulation starts with calculating the maximum end-to-end throughput *MT* (6) for the given network. After this we calculate the effective maximum end-to-end throughput $MT_{eff}$, without the flows from the bot nodes as:

$$MT_{eff} = \sum_{j\in(n-b)} f_j \tag{8}$$

The fraction of DDoS traffic in the network $F_{DoS}$ is calculated as:

$$F_{DoS} = 1 - MT_{eff} / MT \tag{9}$$

Higher value for $F_{DoS}$ means that there is more DDoS traffic in the network, i.e. the network is more vulnerable to DDoS attacks.

In the next part we will show and analyze some of the interesting results we have obtained in our simulations.

Fig. 1 shows that the best strategy for a DDoS attacker when the topology of the network is scale-free and the load is low (around 10%) is to choose the bot nodes according to the BTWN strategy. For instance, if 30% of the nodes are bot nodes then the effectiveness of the network is reduced by 82%. Similar results have been obtained for the DEG and PR strategy. The k-medoids strategy is in between these strategies based on centrality and the case when we are choosing the bot nodes by random.

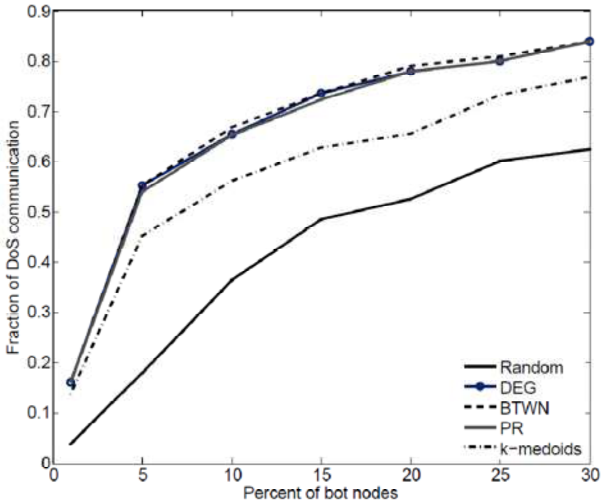

Fig. 1. Fraction of DDoS communication for the scale-free network when the load in the network is 10%.

When the network has heavier load, around 50%, the difference between the centrality strategies (DEG, BTWN, PR), k-medoids and the random strategy is not so obvious (see Fig. 2). Still, the centrality strategies are more suitable for a DDoS attacker, but sometimes maybe it's better and easier for the attacker to choose the bot nodes at random. We would like to stress that the results shown in Fig. 2 coincide with the results obtained for the other two types of networks: random and small-world. That is, no matter the network configuration for higher loads in the network the strategy for choosing bot nodes does not greatly affect the outcome.

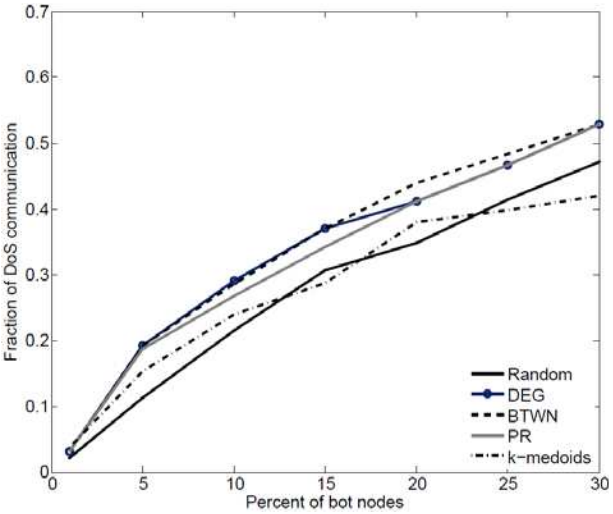

Fig. 2. Fraction of DDoS communication for the scale-free network when the load in the network is 50%.

The BTWN strategy, as expected, shows the biggest degradation for a scale-free network (see Fig. 3). It finds the hub in the network and sets them as bot nodes. For instance, if the load in the network is 10%, this strategy shows degradation of 82%, for the small-world and the random network around 70%.

The PR strategy, also gives the biggest degradation for the scale-free network, then for random and the lowest degradation is for the small-world topology. We believe that the small-world topology is more resistant to the PR strategy, because PR fails to find the center nodes in the clusters and to set them as bot nodes.

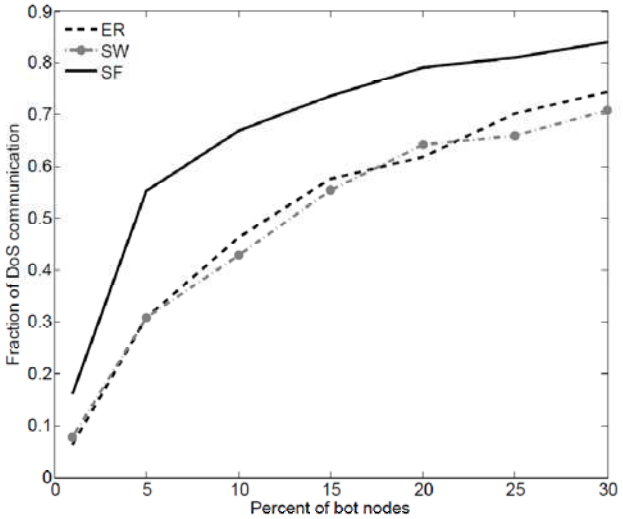

Fig. 3. Fraction of DDoS communication when choosing the bot nodes using betweenness. The traffic load is 10%.

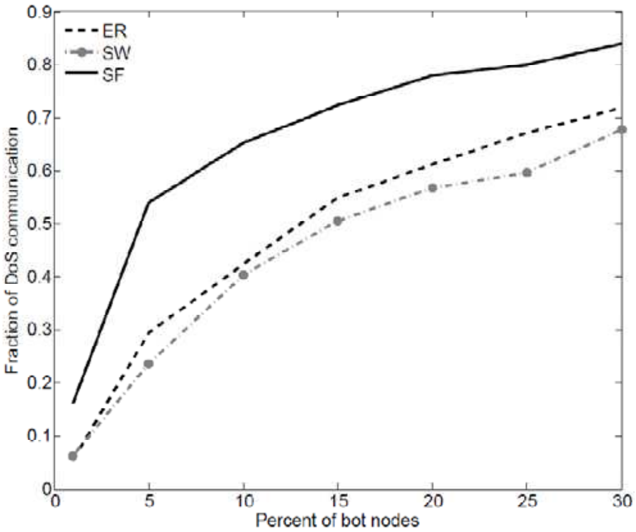

Fig. 4. Fraction of DDoS communication when choosing the bot nodes using pagerank. The traffic load is 10%.

## VI. Conclusion

This brief has studied vulnerability of complex networks by simulating DDoS attacks. DDoS attacks are simulated by choosing bot nodes that will generate DDoS traffic. The bot nodes are chosen using several strategies, such as: random, degree, betweenness, pagerank and k-medoids. The simulations are done on: random, small-world and scale-free topology. The vulnerability of a given network in a given scenario is measured calculating the percentage of DDoS traffic in the network.

For the scale-free network with low load (around 10%) we obtained that the best strategy for a DDoS attacker is to choose the bot nodes according to the BTWN strategy. The fraction of the DDoS traffic, when the percentage of the bot nodes in this scenario is 30, is 82%. The situation changes when there is heavier load in the network (50%), then for an attacker it is maybe more effective to choose the bot nodes by random.

The BTWN and the PR strategy, as expected, show the biggest degradation for a scale-free network. It finds the hub in the network and sets them as bot nodes. We find out that the small-world topology is more resistant to the PR strategy, since this strategy fails to find the center nodes in the clusters and to set them as bot nodes, while favoring to attack the inter-cluster links.

As a future work instead of static routing we want to use dynamic routing with load balancing, which takes into account the current flow in the edges. Another improvement would be, instead of using constant and equal capacity of the links we could use some function that will depend on the initial load of the link.

## References

[1] P. Erdős, A. Rényi: On the evolution of random graphs, Publ. Math. Inst. Hung. Acad. Sci. 5 (1960) 17–61

[2] A.-L. Barabási, R. Albert: Emergence of scaling in random networks, Science 286, Oct 1999, pp. 509–512

[3] R. Guimera, A. Diaz-Guilera, F. Vega-Radondo, A. Cabrales, A. Arenas: Optimal network topologies for local search with congestion, Phys. Rev. Lett. 89 (2002) 248701–248704

[4] S. Boccaletti, V. Latora, Y. Moreno, M. Chavez, and D.-U. Hwang: Complex networks: Structure and dynamics, Phys. Rep., vol. 424, pp. 175–308, 2006

[5] A. E. Motter and Y.-C. Lai: Cascade-based attacks on complex networks, Phys. Rev. E, vol. 66, p. 065102(R), 2002

[6] M. Mirchev, S. Filiposka, N. Trajkovski, D. Trajanov: Network utility maximization in ad hoc networks with different communication patterns, ETAI 2009, Ohrid, Macedonia (2009)

[7] Hang Chau, Network Security – Defense Against DoS/DDoS Attacks.

[8] Wesley M. Eddy, Verizon Federal, “Defenses Against TCP SYN Flooding Attack”, The Internet Protocol Journal, 9, No. 4, December 2006.

[9] F. Lau, S. H. et al., “Distributed Denial of Service Attacks,” 2000 IEEE Int. Conf. on Systems, Man, and Cybernetics, Nashville, TN, October 2000.

[10] B. Saha and A, Gairola, “Botnet: An overview,” CERT-In WhitePaperCIWP-2005-05, 2005.

[11] E. Cooke, F. Jahanian, and D. McPherson, “The Zombie Roundup: Understanding, Detecting and Disrupting Botnets”, In Proceedings of the Steps to Reducing Unwanted Traffic on the Internet (SRUTI 2005 Workshop), Cambridge, MA, July 2005.

[12] CERT Coordination Center, “Denial of Service Attacks,” http://www.cert.org/homeusers/ddos.html.

[13] Stephen M. Specht, Ruby B. Lee, “Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures”, Proceedings of the 17th ICPDCP, pp. 543-550, September 2004.

[14] S. Singh and M. Gyanchandani: “Analysis of Botnet Behavior using Queuing Theory”, IJCSC, Vol. 1, No. 2, July-December 2010, pp. 239-241

[15] F.P. Kelly, A.K. Maulloo, and D.K.H. Tan: Rate control in communication networks: shadow prices, propor¬tional fairness and stability, J. Optical Research Society, Vol. 49, Mar 1998, pp. 237–252

[16] S. Kunniyur and R. Srikant: End-to-end congestion control schemes: Utility functions, random losses and ECN marks, IEEE/ACM Transactions on networking, Vol. 11(5), Oct 2003, pp. 689-702

[17] L. Freeman: Centrality in social networks: Conceptual clarification, Social Networks, vol. 1, no. 3, pp. 215–239, 1979

[18] J. Nieminen: On the centrality in a graph, Scandinavian Journal of Psychology, vol. 15, no. 1, pp. 332–336, 1974

[19] P. Bonacich: Factoring and weighting approaches to status scores and clique identification, Journal of Mathematical Sociology, vol. 2, no. 1, pp. 113–120, 1972

[20] P. Larry, B. Sergey, R. Motwani et al.: The PageRank citation ranking: Bringing order to the web, Online: http://citeseer. nj. nec.com/page98pagerank. html [04.06. 2003], 1998

[21] Kaufman, L., Rousseeuw, P.: Finding groups in data: An introduction to cluster analysis. Applied Probability and Statistics, Wiley, New York (1990)

[22] MacQueen, J.: Some methods for classification and analysis of multivariate observations. In Proc. of the 5th Berkeley Symposium on Mathematical Statistics and Probability, 1, 281--297 (1967)

[23] CVX: Matlab Software for Disciplined Convex Programming. Available: http://www.standofd.edu/~boyd/cvx