

Key words — Communication system traffic, traffic modeling, anonymous peer-to-peer networks.

Igor MARGASIŃSKI^{*}, Michał PIÓRO^{*,†}

ON TRAFFIC PERFORMANCE MEASURES FOR ANONYMOUS P2P NETWORKS

The modeling of anonymous systems is mostly aimed at the evaluation of the level of provided anonymity. However, the utility of anonymity solutions depends not only on their security, but also on necessary traffic overheads. In this paper, we have proposed an empirical, traffic performance model for anonymous P2P networks. We based our research on a well known information entropy measurement model for an estimate of secure configuration of anonymous forwarding path lengths. Then, we proposed a simulation-based methodology for an evaluation of latency and dynamics of the selected configurations. As an example we used the classical system called CROWDS. We evaluate traffic performance of CROWDS and show that the empirical analysis of the system has been analogous to results obtained analytically for representative boundary conditions.

1. INTRODUCTION

The anonymous P2P networks are the vital domain among the ever increasing variety of anonymous communications solutions. The P2P network architecture is extremely promising for an implementation of effective anonymous techniques since the distributed P2Ps eliminate the presence of trusted third party—privacy trustee. Concerning anonymity, we know a lot about robustness of anonymity systems and particular P2P solutions (e.g., [2], [3], [8], [14]). A mature information theoretic model for the evaluation of anonymity systems ([4], [10]) already is in use. Still, while the research in the field of anonymous systems measuring is mainly focused on the evaluation of the level of provided anonymity, the modeling of traffic performance of anonymization methods is in our opinion neglected. Yet, the utility of a particular anonymous system results not only from its robustness against attackers and traffic analysis but also its necessary traffic overheads. Roughly speaking, the first question is: “how much anonymity do I get?” and the second, on which we focused our attention in this paper, is: “how much does it cost?” A research in this field was recently introduced in [13] and [5]. These works however, are devoted to the specific system (TOR [7]) and the presented measures in [5] are based on the gathered system’s statistics. Still, we have to learn more about the traffic performance’s “costs” and its modeling for anonymous networks. In [6] we introduced and used a model for the traffic performance analysis of the new anonymous P2P system (called P2PRIV) and to compare the system with the CROWDS [9]. This paper presents a detailed description of this model.

In 2002, two papers authored by Diaz *et al.* [4] and Serjantov *et al.* [10] simultaneously and independently introduced a new methodology for anonymity measurement based on Shannon’s

^{*} Institute of Telecommunications, Warsaw University of Technology

[†] Department of Electro and Information Technology, Lund University

information theory. The information entropy proposed by Shannon [11] describes the uncertainty associated with a random variable. It can be applied to anonymity quantification by assignment of probability of being an initiator of a specified action in the system to its particular users. Certainly, the sum of all these probabilities should equal 1. Then, based on the information provided by a system (shown by the system to an adversary) it is possible to measure the uncertainty of finding a real initiator. Let X be a discrete random variable, and

$$p_i = \Pr(X = i) \quad (1)$$

where i corresponds to the number of a particular subject/node/user of the analyzed system. For each user from the set of all system users N , the adversary can assign probability of being the initiator p_i . Then the entropy H will be described by

$$H = -\sum_{i=1}^N p_i \log_2(p_i) . \quad (2)$$

In Equation (2), a base-2 logarithm was used. Therefore the unit of the expressed entropy is a *bit*. This measure discloses a number of bits required for an adversary to explicitly point out the initiator. The adaptation of information theory seems to be a proper method for anonymity quantification as the uncertainty of the observer increases proportionally with H . The anonymity corresponds intuitively to a blending into the crowd of other similar subjects. Entropy measurement, as a quantification of a disorder of a structure of a system, gives a description of this phenomenon and an analytical instrument to measure how particular subjects of the system are distinguishable among the whole population of subjects. To enable the comparison between heterogeneous anonymity systems, a normalization of entropy was proposed by Diaz *et al.* [4]. Let H_{\max} be the maximum entropy for a current number of system users. Entropy reaches the maximum value when all possible users are equiprobable

$$H_{\max} = \log_2(N) , \quad (3)$$

where N is the number of users. Then the normalized entropy – degree of anonymity is

$$d = \frac{H}{H_{\max}} = -\frac{\sum_{i=1}^N p_i \log_2(p_i)}{\log_2(N)} , \quad (4)$$

where p_i is the probability assigned to i subject, describing how likely this subject is perceived by the adversary as the initiator. This metric (4) describes the uncertainty of the system observer (the adversary) in finding the initiator of a specific action (for example sending a request for a specific content) and takes values from [0,1]. The minimum degree of anonymity depends on the purpose of anonymous system. However, in [4] acceptable normalized entropy was restricted to values higher or equal to $d_{\min} = 0.8$.

In this paper we revised this model of anonymity systems in order to achieve the P2P environment usability and to reflect the practical capabilities of a P2P adversary. In effect, we provide methodology allowing finding a secure configuration of anonymous P2Ps (Section 2). In Section 3 we provide an empirical model of anonymous P2P traffic, capable of evaluating the traffic cost of selected secure configurations of anonymous P2P network. We focus our research on latency and dynamics measures. Latency constitutes a crucial factor for anonymous P2P traffic performance, since the basic common mechanism used to achieve network anonymization is traffic forwarding by a set of middleman nodes. Additionally, we concentrate our research on dynamics measures. Robustness against dynamically changing conditions, such as peers/content migration and traffic bursts introduced by publication of new data, demonstrates the suitability of particular networks anonymization techniques to P2P overlays. Finally, we conclude the paper and discuss a future work in Section 4.

2. ESTIMATION OF SECURE FORWARDING PATH LENGTHS

We will apply the entropy measurement model to quantify anonymity of the CROWDS system. The CROWDS can be used as an example of an attacked system, because it combines anonymity and performance with simplicity and reputability ([12], [15]). The adversary, who foists colluding nodes to the network, can assign probabilities of being the initiator to particular network nodes. Based on [9] and [4] the probability assigned to a predecessor of the first colluding node from the forwarding path is

$$p_{c+1} = 1 - p_f \frac{N - C - 1}{N} . \quad (5)$$

The rest of nodes will have assigned equal probabilities since the adversary has no additional information about them. All colluding nodes should not be considered,

$$p_i = \frac{p_f}{N} . \quad (6)$$

According to (2), the entropy of the system will be described by

$$H_{paCROWDS} = \frac{N - p_f(N - C - 1)}{N} \log_2 \left(\frac{N}{N - p_f(N - C - 1)} \right) + \frac{p_f}{N} (N - C - 1) \log_2 \left(\frac{N}{p_f} \right) . \quad (7)$$

The CROWDS maximum entropy is reached when all honest nodes are equiprobably recognized by the adversary as the initiator

$$H_{\max CROWDS} = \log_2(N - C) , \quad (8)$$

then the normalized entropy equals

$$d_{paCROWDS} = \frac{H_{paCROWDS}}{H_{\max CROWDS}} \quad (9)$$

$$d_{paCROWDS} = \frac{(N - p_f(N - C - 1)) \log_2 \left(\frac{N}{N - p_f(N - C - 1)} \right) + p_f(N - C - 1) \log_2 \left(\frac{N}{p_f} \right)}{N \log_2(N - C)} . \quad (10)$$

2.1. HOW LONG FORWARDING PATHS CAN DEGRADATE ANONYMITY

In the model proposed by [4] and [10] it is assumed that the adversary has yet colluding nodes among network nodes, which actively anonymize specified request (for example nodes from the forwarding random walk path of CROWDS system). Practically, the scenario may be different, and what is more, the probability that the adversary can find this group of nodes (referred to as an “active set”) also determines the quality of the system anonymization.

The scenario described above should be called an adaptive attack, because it is assumed that the adversary is capable of adopting an area of its observation to the scope of activity of system users. It is important to also consider a more general case, where the adversary cannot be certain of a successive collaboration of proper active set. This uncertainty

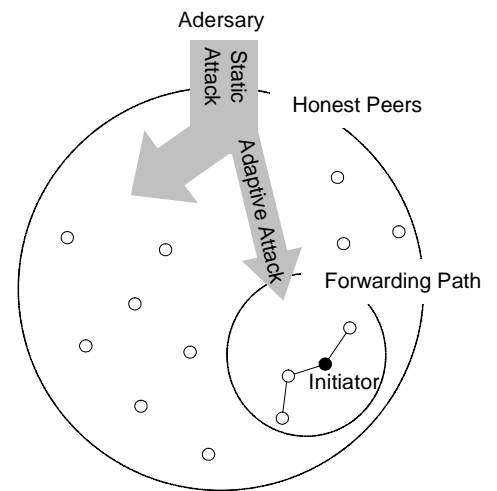


Fig. 1. Range of observation for static and the adaptive attacks.

should be quantified as well. For example, in the CROWDS system an increase of p_f parameter can easily increase the system active sets. However, if the active set is too numerous, even for large networks, collaboration of active nodes is simple – highly probable. Notice that when the adversary has no collaborating nodes among the active set then all the nodes of the system are equalprobable and the uncertainty of the adversary is maximized. The need for considering the impact of the observer uncertainty in finding proper active nodes was noticed in [4] and a weight mean formula was proposed to compute final d . This seems to be an intuitive attitude. However, the same results can be achieved by using a conditional entropy formula. In [1] a conditional entropy was proposed to describe the generalized scenario of the observation. The conditional entropy describes the entropy of a random variable X under condition of elimination of the entropy of other random variable Y . The conditional entropy expresses then the uncertainty associated with one aspect when the other aspect is certain.

This attack will be referred to as a static attack, as in this scenario the adversary “injects” colluding nodes in a static manner and cannot dynamically predict (adapt, like in previous scenario referred to as adaptive attack) which random nodes will actively anonymize the specified request. Let us return to the CROWDS example. A probability that none of the collaborating nodes can become a member of the random walk forwarding path is

$$p_r = \frac{N-C}{N} (1-p_f) \sum_{i=0}^{\infty} \left(\frac{N-C}{N} p_f \right)^i = 1 - \frac{C}{N - p_f(N-C)}, \quad (11)$$

then entropy for passive-static attacks equals

$$H_{psCROWDS} = -\frac{C}{N - p_f(N-C)} \frac{N - p_f(N-C-1)}{N} \log_2 \left(\frac{N - p_f(N-C-1)}{N} \right) + \left(1 - \frac{C}{N - p_f(N-C)} \right) p_f \frac{N-C-1}{N} \log_2 \left(\frac{p_f}{N} \left(1 - \frac{C}{N - p_f(N-C)} \right) \right), \quad (12)$$

and the normalized entropy is

$$d_{psCROWDS} = \frac{H_{psCROWDS}}{H_{maxCROWDS}} \quad (13)$$

$$d_{psCROWDS} = -\frac{C}{N - p_f(N-C)} \frac{N - p_f(N-C-1)}{N \log_2(N-C)} \log_2 \left(\frac{N - p_f(N-C-1)}{N} \right) + \left(1 - \frac{C}{N - p_f(N-C)} \right) p_f \frac{N-C-1}{N \log_2(N-C)} \log_2 \left(\frac{p_f}{N} \left(1 - \frac{C}{N - p_f(N-C)} \right) \right). \quad (14)$$

We will analyze how p_f configuration impacts the entropy of the CROWDS system for both attack scenarios. It is important to remember that p_f value directly affects the forwarding path length – the number of network nodes actively involved in the anonymization process. Figure 2a and Figure 2b show the entropy of CROWDS in the full spectrum of available p_f configuration. We use maximum entropy $H_{maxCROWDS}$ (8) as a reference. First we analyzed three variants of network collaboration level (i) $C = 10\%$ – scenario usually considered in the state of the art; (ii) $C = 5\%$ – more realistic collaboration level for large and public access overlays; and (iii) $C = 20\%$ – scenario for small overlays. The next results, Figure 2c and Figure 3d, present the CROWDS entropy as a function of the number of collaborating nodes C , finally including the global collaboration.

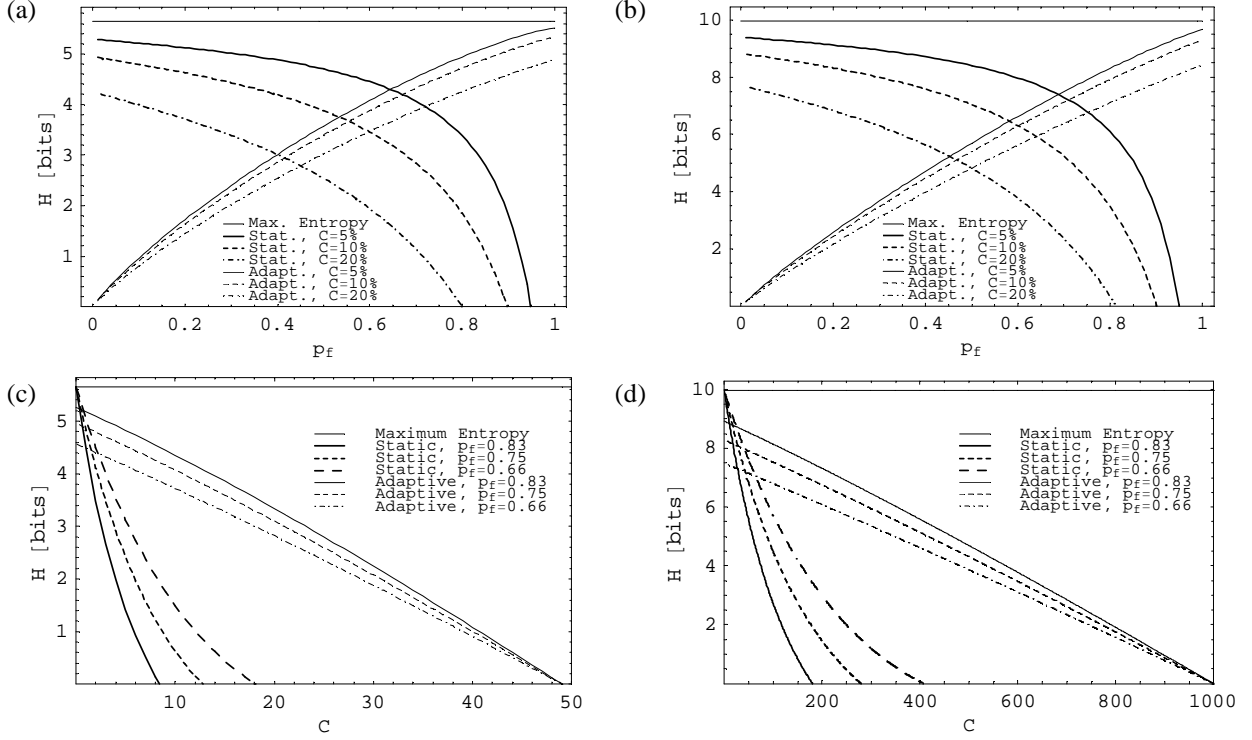


Fig. 2. Entropy of CROWDS, static and adaptive attacks; $N = 50$ (a), (b); $N = 100$ (c), (d).

The results for the two considered attack scenarios are substantially opposite. In the adaptive scenario low entropy, close to zero, is obtained for low p_f values, and high, close to maximum, entropy is achieved for large p_f . In the static scenario, the dependency is quite different and the best results are achieved for the lowest p_f values. As p_f grows, the entropy grows logarithmically smaller. In a small network this decrease (static attack) of entropy is slightly faster in contrast to the adaptive scenario where, in the small network, the decrease of the entropy is slower than for large overlays. This analysis shows that a set of nodes actively involved in the anonymization process should not be too numerous. Longer cascades not only impose larger traffic overheads, but can also make it easier for the adversary to become a member of the forwarding path. Especially in small networks the security of particular systems can be effectively compromised. In small networks, nodes from a forwarding path constitute a significant part of all network nodes. It should be reminded that the analyzed CROWDS system does not include mixing or asymmetric encryptions techniques for traffic analysis protection.

The results show that the secure configuration of forwarding path lengths should be adjusted to the size of the CROWDS overlay network. Taking into account large overlays, more typical for public P2P networks and a collaboration level C lower or equaled to 5%, the p_f configuration of CROWDS should be no lower than roughly 0.6 and no higher than about 0.8. Lower values than 0.6 expose the originator of a particular request against the adaptive adversary. Values higher than 0.8 compromise him to the static attacker. Then the mean forwarding path length of network random walk P equals

$$P = \sum_{i=2}^{\infty} i p_f^{i-2} (1-p_f) = \frac{p_f - 2}{p_f - 1}. \quad (15)$$

We can emphasize minimum and maximum secure mean path lengths of CROWDS:

$$P_{\min CROWDS} = 4 (p_f = 0.66), P_{\max CROWDS} = 6 (p_f = 0.83). \quad (16)$$

Forwarding paths shorter than $P_{\min CROWDS}$ cannot provide sufficient “crowd” of nodes, which actively anonymize the initiator. If the adversary is yet among this set of nodes there should be additional 2 other honest nodes. On the other hand, the forwarding paths longer than 6 nodes ($P_{\max CROWDS}$) becomes too easy to enter, because the size of the “crowd” provided by nodes passively anonymizing the active set becomes insufficient. Table 1 contains the summary of the results represented as a degree of anonymity obtained for promising values of p_f parameter.

Table 1. Degree of anonymity for CROWDS, static and adaptive attacks.

p_f	$C = 5\%$			$C = 10\%$			$C = 20\%$		
	0.66	0.75	0.83	0.66	0.75	0.83	0.66	0.75	0.83
Static attack	0.69	<u>0.63</u>	0.58	0.51	0.41	0.32	0.25	0.11	0.0099
Adaptive attack	0.69	<u>0.78</u>	0.82	0.66	0.74	0.79	0.59	0.67	0.71

Our analysis confirmed that the optimum configuration for a realistic level of CROWDS collaboration is about $p_f = 0.75$ (recommended by the system authors). Concerning the collaboration level of $C = 5\%$, the degree of anonymity for CROWDS become close to d_{\min} .

As one can expect, the entropy largely depends on the number of colluding nodes. What is more, we can observe a significant impact of static observation on the anonymity of the CROWDS system. CROWDS entropy is significantly lower for static attacks than for adaptive scenarios. Still, both static and adaptive variants of attacks are vital to the anonymity analysis as they correspond to different aspects of the system’s anonymity. The static scenario shows more realistic capabilities of the adversary and constitutes a critical point of view on the expansion of the system active sets. However, a more pessimistic attack – adaptive observation – is possible. Even though this scenario happens comparatively rarely, it is important to analyze its consequences.

3. AN EMPIRICAL MODEL OF ANONYMOUS P2P TRAFFIC

For the purpose of the complicated dynamic conditions analysis, we have created a peer-to-peer traffic simulation environment. Each peer of the simulated network retrieves the same algorithm suitable to a simulated protocol (for example Jondo of CROWDS). The simulator traces tasks for each symmetric peer independently. The peers can collect a specified content and can randomly leave the overlay – depriving other users of the content copies. Figure 3 shows an outline of the simulator architecture.

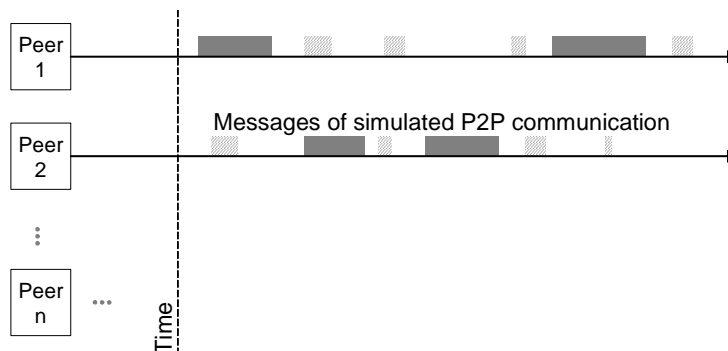


Fig. 3. Architecture of P2P traffic simulator.

The simulator allows setting-up of the following parameters of an overlay traffic:

- mean request arrival rate (λ) – intensity of requests for a content;
- mean download time between two neighbor peers (μ^{-1}) – resultant of a link throughput and an amount of sent data;
- mean request arrival rate for a specified content (λ_{Dc}) – intensity of requests for a specified (for example newly published) content;
- mean migration rate (λ_{Dm}) – intensity of users’ leaving and arriving in the overlay network (“churn”).

We use Poisson distribution to model a request arrival process. We simulated the CROWDS random walk algorithm to verify the simulation model.

3.1. LATENCY

Let average link throughput between peers be $B = 512$ kb/s and average file size of the shared content $V = 32$ MB. To analyze systems latency quoted as a mean download time we have computed series of simulation with 30 realizations each starting from the maximum request arrival rate per each node

$$\lambda_{\max} = \frac{\mu_{\min}}{P} = 0.0005[s^{-1}]. \quad (17)$$

where P is a mean random walk path length (15) and a μ_{\min}^{-1} denotes download time between two directly connected nodes (referred in the rest of the work as FTP for simplification),

$$\mu_{\min} = \frac{B}{V} = 0.002[s^{-1}]. \quad (18)$$

Figure 4 shows 95% confidence intervals and 25% to 75% quantiles (marked as boxes) surrounding the mean values of DT for the CROWDS system as the function of parameter λ^{-1} . In the analysis we have assumed CROWDS configuration which is accurate with recommendation of the CROWDS authors and with our analysis: $p_f = 0.75$. It means that the mean number of overlay nodes forwarding a single request equals 5 (15).

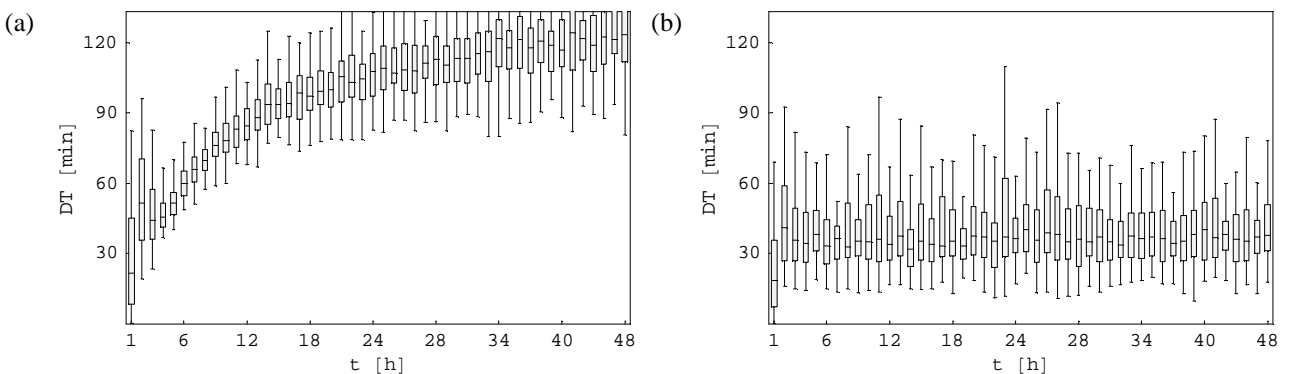


Fig. 4. Mean download time for CROWDS random walk in a period of two days after start of network operation, $N = 100$; maximum request arrival rate (a) and low request arrival rate (b).

Our first remark is that the simulated CROWDS random walk overlay works on the brink of stability for a analytical maximum request arrival rate. Simulations results for a lower request arrival rate showed the stable operation of the overlay.

Secondly, for a low arrival rate we can observe download time much above half an hour. The mean DT of a single file, measured in a period of two days of the system operation, equals 38.82 minutes. The analytically obtained mean time of a file transfer between neighbor nodes equals $\mu_{\min}^{-1} = 8.33$ minutes. In the CROWDS random walk each file is sent through a cascade of nodes. In the configuration of $p_f = 0.75$ the mean number of links in the cascade between source and destination peers equals 4. The simulation results show that DT for the CROWDS random walk is about 4.6 times longer than a FTP DT for a single link.

We repeated our simulation for $P_{\min CROWDS}$ and $P_{\max CROWDS}$ forwarding path lengths. Figure 5 shows results of CROWDS latency in a range of request arrival rate starting from the maximum traffic intensity. We can observe that as P grows, DT grows linearly higher. Addition of one node to the forwarding path results in an addition of μ_{\min} value to the final DT.

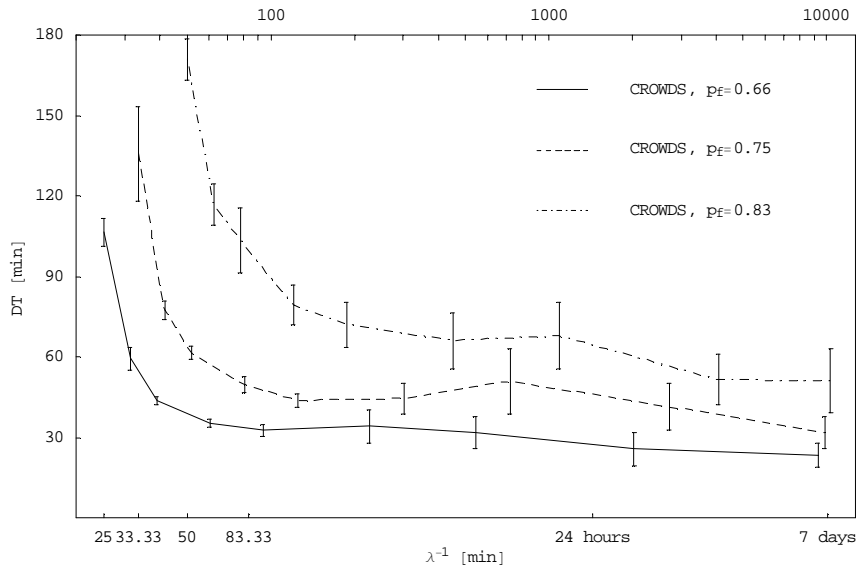


Fig. 5. Latency for CROWDS.

3.2. DYNAMICS

Next we will apply the simulation model to consider the mean DT characteristics under dynamically changing network traffic conditions. We will analyze system behavior starting from a new file publication. We analyze the scenario where the new and popular content is just shared by one of the overlay nodes. Additionally, we take into account the common practice of some users to connect to the overlay only for the purpose of a particular content download and to leave the network just after its successful delivery. Let D be the part of all requests which corresponds to the new file. We will take into account “selfish” users’ behavior where simultaneously D percent of copies leaves the overlay network for each request. In this manner we have joined two parameters of the simulation which describe the popularity of a selected content and the migration of overlay users (λ_{Dc} and λ_{Dm}).

Figure 6 shows 95% confidence intervals and 25% to 75% quantiles (marked as boxes) surrounding the mean values of DT. We simulated the overlay under dynamically changing traffic conditions D . The first presented results (Figure 6a) were obtained for dynamics $D = 20\%$. We can observe that mean download time is slightly longer after a new content publications and returns to an initial level after about 5 hours. The further increase of dynamics to the value of $D = 30\%$ (presented on Figure 6b) caused an instability of the system – DT increases in the analyzed period

of 36 hours. However, this scenario is highly pessimistic as about $\frac{1}{3}$ of all user requests in the overlay network are directed towards the same, new content.

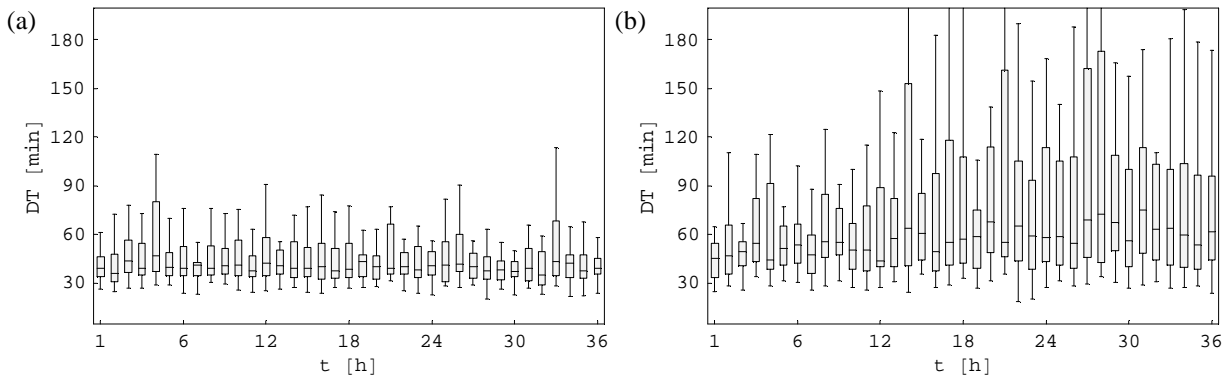


Fig. 6. Reaction of CROWDS to the new content publication, $N = 100$, low request arrival rate, (a) $D = 20\%$, (b) $D = 30\%$.

4. CONCLUSIONS

In this paper, we have proposed an empirical model for an evaluation of traffic performance of anonymous P2P networks. We used an information entropy measurement model ([4], [10]) for estimation of secure configuration of anonymous forwarding path lengths and proposed methodology for evaluation of latency and dynamics of the selected configurations. As an example of an evaluated system we used the classical solution called CROWDS.

The information theoretic model ([4], [10]) of system's anonymity has been revised in order to achieve the P2P environment usability and to reflect the practical capabilities of a P2P adversary. We analyzed the widely described in the state of the art literature, adaptive observation scenario, and also considered more realistic static attacks. Static attacks create awareness of boundless extension of forwarding path lengths. The long paths can impose not only larger traffic overheads, but can also make it easier for the adversary to become a member of set of nodes actively involved in the anonymization process. We have found that both static and adaptive attacks are vital to the anonymity analysis, as they correspond to different aspects of system protection. The static scenario shows more realistic capabilities of the adversary and it exemplifies a critical point of view on the expansion of forwarding paths. However, a more pessimistic attack – an adaptive observation – is possible. This scenario shows the effectiveness of the system's anonymity protection among network nodes actively involved in hiding on an initiator.

We have observed that latency of CROWDS is roughly a multiplication of the direct download time between two neighboring nodes and the forwarding path length. The observation of system's behavior under dynamically changing conditions shows that a stable operation of network random walk from CROWDS can be retained for dynamics lower or equal to 20%.

We have found that the empirical analysis of the network random walk algorithm (taken from CROWDS) is analogous to theoretical values, under boundary conditions. The analytical calculations included: available capacity (traffic intensity of the maximum request arrival rate) and the mean download time for a low-loaded network (low request arrival rate). For the analytically obtained maximum request arrival rate, we have observed that the simulated system works on the brink of stability. For a low traffic intensity the mean download time provided by the simulated system is slightly higher than the analytically obtained results that do not deal with delays introduced by network nodes.

Our future work will include a more detailed analysis of the impact imposed by various anonymous techniques on their traffic performance. An interesting goal is the consideration of overlay dynamics with simultaneous migration of many content resources. The traffic performance analysis, presented in this paper, has covered the following two elements: (i) the evaluation of the latency in the stable operation of simulated overlays; and (ii) the measures of the latency after the publication of a new file – we have considered a series of copying and removing of the single content resource. The future analysis should include modeling of anonymous traffic where many new files are copied and removed in the overlay network simultaneously. Additionally, this research can be based on a sociological analysis of users' habits, as this study can bring the simulation model closer to real networks. The next important direction of the future work is carrying out analytical traffic performance models for anonymous systems.

REFERENCES

- [1] N. Borisov: *Anonymous Routing in Structured Peer-to-Peer Overlays*. PhD Thesis, UC Berkeley, 2005.
- [2] R. Dingledine, M. J. Freedman, and D. Molnar, "The free haven project: Distributed anonymous storage service," in *H. Federrath, editor, Designing Privacy Enhancing Technologies: Workshop on Design Issues in Anonymity and Unobservability*. Springer-Verlag, LNCS 2009, July 2000.
- [3] M. J. Freedman and R. Morris, "Tarzan: A peer-to-peer anonymizing network layer," in *9th ACM Conference on Computer and Communications Security*, Washington, DC, November 2002.
- [4] C. Diaz, S. Seys, J. Claessens and B. Preneel, "Towards measuring anonymity," in *Roger Dingledine and Paul Syverson, editors, Proceedings of the Privacy Enhancing Technologies Workshop*. Springer-Verlag, LNCS 2482, April 2002.
- [5] K. Loesing, W. Sandmann, C. Wilms, and G. Wirtz, "Performance Measurements and Statistics of Tor Hidden Services," in *Proceedings of the 2008 International Symposium on Applications and the Internet (SAINT)*, Turku, Finland, July 2008.
- [6] I. Margasiński and M. Pióro, "A Concept of an Anonymous Direct P2P Distribution Overlay System," in *Proceedings of the 22nd IEEE International Conference on Advanced Information Networking and Applications (AINA2008)*, ISSN 1550-445X, ISBN 978-0-7695-3095-6, pp. 590-597, Ginowan, Okinawa, Japan, March 2008.
- [7] D. N. Mathewson and P. Syverson, "Tor: The second generation onion router," in *Proceedings of the 13th USENIX Security Symposium*, August 2004.
- [8] M. Rennhard and B. Plattner, "Introducing MorphMix: Peer-to-Peer based Anonymous Internet Usage with Collusion Detection," in *Proceedings of the Workshop on Privacy in the Electronic Society (WPES 2002)*, Washington, DC, USA, November 2002.
- [9] M. K. Reiter, A. D. Rubin, "Crowds: Anonymity for web transactions," *ACM Transactions on Information and System Security*, 1(1), June 1998.
- [10] A. Serjantov and G. Danezis, "Towards an information theoretic metric for anonymity," in *Roger Dingledine and Paul Syverson, editors, Proceedings of the Privacy Enhancing Technologies Workshop*, San Diego, CA, April 2002. Springer-Verlag, LNCS 2482.
- [11] C. E. Shannon, *A Mathematical Theory Of Communication*, the Bell System Technical Journal, Vol. 27, pp. 379–423 and pp. 623–656, 1948.
- [12] V. Shmatikov, "Probabilistic analysis of anonymity," in *Proceedings of the Computer Security Foundations workshop (CSFW-15 2002)*, pages 119-128, Cape Breton, Nova Scotia, Canada, 24-26 June 2002. IEEE Computer Society.
- [13] R. Snader and N. Borisov, "A Tune-up for Tor: Improving Security and Performance in the Tor Network," in *Proceedings of the Network and Distributed Security Symposium – NDSS '08*, February 2008.
- [14] P. Tabriz and N. Borisov, "Breaking the collusion detection mechanism of MorphMix," in *Proceedings of the Privacy Enhancing Technologies Workshop (PET)*, June 2006.
- [15] M. Wright, M. Adler, B. N. Levine, and C. Shields, "An analysis of the degradation of anonymous protocols," in *Proceedings of the Network and Distributed Security Symposium (NDSS'02)*, San Diego, California, 6-8 February 2002.