The Power of Memory in Randomized Broadcasting*

Robert Elsässer[†] Thomas Sauerwald[‡]

Abstract

In this paper we analyze the runtime and number of message transmissions generated by simple randomized broadcasting algorithms in random-like networks, and show that an apparently minor change in the ability of the nodes implies an exponential decrease in the average communication overhead produced by these algorithms at an arbitrary node.

A natural randomized broadcasting protocol, called *random phone call model*, has been introduced by Karp et al. [20]. In this model it is assumed that in each time step, every node of G calls a neighbor, chosen uniformly at random, and establishes a communication channel with this neighbor. Any node u is then allowed to send/receive messages to/from all nodes which have established communication channels with u in the current time step. Karp et al. showed that some piece of information r, placed initially on one of the nodes of a *complete graph* of size n, can be spread with probability $1 - n^{-\Omega(1)}$ to all nodes of this graph within $O(\log n)$ time steps, by using $O(n \log\log n)$ transmissions related to r. Furthermore, they proved that this result is asymptotically optimal among all address-oblivious broadcasting algorithms. In a recent paper [9], we analyzed the random phone call model in traditional random graphs $G_{n,p}$ with $p > \log^2 n/n$, and showed that any address-oblivious broadcasting algorithm requires with high probability $\Omega(\log n)$ time steps and $\Omega(n(\log\log n + \log n/\log(pn)))$ message transmissions to inform all nodes of such a graph. In this paper we consider two simple modifications of the random phone call model, and show that in both cases the number of total message transmissions can be reduced significantly (up to almost a logarithmic factor). In the first case, we allow each node of a random graph $G_{n,p}$ with $p > \log^\delta n/n$, where δ is a properly chosen constant, to call in every time step *four different neighbors*, chosen uniformly at random, and we prove that the number of message transmissions decreases to $O(n \log\log n)$. This can be viewed as a "power of multiple choices" type theorem for randomized broadcasting. Then we show that if in the random phone call model the nodes are provided with a little memory, i.e., they are able to remember the addresses of the nodes chosen in the most recent three time steps, then the communication overhead decreases substantially, too. Finally, we prove the optimality of our results.

The algorithms presented in this paper can cope with restricted communication failures, only require rough estimates of the number of nodes, and are robust against slight topological changes. In addition, our results can be extended to the generalized random graph model of [6].

*This work was partially supported by the German Research Foundation (DFG) Research Training Group GK-693 of the Paderborn Institute for Scientific Computation and by the Integrated Project IST-15964 "Algorithmic Principles for Building Efficient Overlay Networks" of the European Union.

[†]University of Paderborn, 33102 Paderborn, Germany

[‡]Paderborn Institute for Scientific Computation (PaSCO-GK), 33098 Paderborn, Germany

1 Introduction

1.1 Models and Motivation Information dissemination in large networks has various fields of application in distributed computing. Consider for example the maintenance of replicated databases in name servers in a large corporate network [8]. There are updates injected at various nodes, and these updates must be propagated to all the nodes in the network. In order to let all copies of the database converge to the same content, efficient broadcasting algorithms have to be developed.

There is an enormous amount of experimental and theoretical study of (deterministic and randomized) broadcasting in various models and on different networks. In this paper we only concentrate on randomized broadcasting algorithms, and study their runtime and communication overhead. As an example, consider the so-called *push model* [8]: In a graph $G = (V, E)$ we place at some time t a piece of information r on one of the nodes. Then, in each succeeding time step, any *informed* vertex forwards a copy of r to a neighbor selected independently and uniformly at random.

The advantage of randomized broadcasting is its inherent robustness against failures and dynamical changes compared to deterministic schemes that either need substantially more time [15] or can tolerate only a relatively small number of faults [22]. Our intention is to develop time efficient randomized broadcasting algorithms which have the following properties:

- They can successfully handle restricted communication failures in the network.
- They work well if size or topology of the network change slightly while the algorithm is executed.
- The number of message transmissions they produce is asymptotically minimal.

Clearly, the effects of node failures or dynamical changes in the size of the network do not really affect the efficiency of the push model. Concerning the communication overhead, it is known that the push model requires $\Omega(n \log n)$ message transmissions (cf. [20, 9]).

In order to reduce the communication overhead, Demers et al. introduced the idea of so called *pull transmissions*, i.e. any (informed or uninformed) node is allowed to call a randomly chosen neighbor, and information is sent from the called to the calling node [8]. This kind of transmission only makes sense if new or updated messages occur frequently in the network so that almost every node has to place a random call in each round anyway. In this model it may happen that some nodes transmit messages to several neighbors within one step, however, the number of transmissions within one step is still bounded by the number of nodes in the graph. It was observed in complete graphs of size n that if a constant fraction of the nodes is informed, then with probability $1 - n^{-\Omega(1)}$ all nodes of the graph become informed within $O(\log \log n)$ additional steps [8, 20]. Thus, $O(n \log \log n)$ transmissions are enough in such graphs, if the distribution of the information is stopped at the right time.

In this paper we are particularly interested in randomized broadcasting algorithms on random-like graphs. Apart from being of wide theoretical interest, random graphs received a lot of attention in the context of peer-to-peer (P2P) networks recently. P2P networks are emerging as a significant platform for providing distributed services such as search, content integration and administration. An important feature of such networks is their dynamically changing topology generated by peers which continuously enter and leave the system. Thus, overlay networks for P2P systems must exhibit good topological properties (i.e., connectivity, low diameter, low degree, etc.), should support efficient data management and information dissemination algorithms, and have to be highly fault tolerant.

The idea of using random networks for P2P systems appears in e.g. the Gnutella network [17] and JXTA of Sun Microsystems [3]. Several research groups have recently designed a variety of random-like networks for P2P systems (e.g. WARP of [19]), and there is a considerable amount of work dealing with the generation and maintenance of random regular graphs (with up to logarithmic degree) (e.g. [7, 12, 21, 23]).

1.2 Related Work Most papers dealing with randomized broadcasting analyze the runtime of the push algorithm in different graph classes. Frieze and Grimmett showed that, with probability $1 - o(1)$, it is possible to broadcast a message in a complete graph of size n in time $\log_2(n) + \ln(n) + o(\log n)$ [14]. Later, Pittel improved this bound to $\log_2(n) + \ln(n) + O(1)$ [26]. In [13], Feige et al. determined asymptotically optimal upper bounds for the runtime of this algorithm in random graphs of at least logarithmic density, bounded degree graphs, and Hypercubes. Furthermore, they also derived upper bounds on the runtime of the push algorithm in general graphs and analyzed the fault tolerance of randomized broadcasting in complete graphs.

Karp et al. [20] considered the runtime and number of message transmissions generated by randomized broadcasting in complete graphs. They introduced the so called random phone call model by combining push and pull, and presented a termination mechanism, which reduces the number of total transmissions to $O(n \log \log n)$, with high probability[1], in complete graphs of size n. It has also been shown that this result is asymptotically optimal among these kind of algorithms. They also considered communication failures and analyzed the performance of the algorithm in the case when the random connections established in each time step follow an arbitrary probability distribution.

In the random phone call model of [20] any node is allowed to send/receive messages to/from each neighbor which has established a communication channel with this node in the current time step. Then, even if a node does not know anything about the existence of any messages that are to be transmitted to all nodes in the network, it still establishes communication channels with neighbors to exchange messages. Therefore, this model (as well as our model presented in this paper) only makes sense, if new or updated messages occur frequently in the network so that every node has to transmit some messages in each step anyway. Then, the cost of establishing communication amortizes over all transmissions, and we are allowed to consider the number of transmissions of one single message only [20]. However, in some application it might happen that only a few pieces of information are generated in one step, and then the cost of establishing communication could exceed the total cost for transmissions. Thus, we assume in this paper that new pieces of information are frequently generated by almost every node, however, we only focus on the distribution and lifetime of a single information.

As described in the previous section, our goal is to improve the efficiency of randomized broadcasting in random-like graphs. The theory of random graphs was founded by Erdős and Rényi [10, 11]. They considered the elements in a probability space consisting of graphs of a particular type. The simplest such probability space consists of all graphs with n vertices and m edges, and each such graph $G_{n,m}$ is assigned the same probability. Another random graph model has been introduced by Gilbert in [16], in which a graph ${G_p}^2$ of size n is constructed by letting two pairs of vertices be connected independently with probability p. A generalization of

[1]When we write "with high probability" or "w.h.p.", we mean with probability at least $1 - 1/n^{\Omega(1)}$.

[2]Due to simplicity reasons, in this paper we always write G_p instead of $G_{n,p}$.

this model to random graphs with arbitrary degree distribution can be found in e.g. [6]. In this paper we mainly concentrate on the G_p model, however our results also hold for the other classes of random graphs mentioned before.

In [9], we considered the random phone call model in random graphs G_p with $p > \log^{\delta} n/n$, where $\delta > 2$ is a constant. We presented an algorithm, which broadcasts a piece of information r to all nodes of the graph within $O(\log n)$ time steps and by using $O(n \max\{\log\log n, \log n/\log(pn)\})$ transmissions of r, with probability $1 - 1/n^{\Omega(1)}$. Furthermore, we proved that this algorithm has optimal runtime and communication overhead among all address-oblivious algorithms (which work within the limits of the random phone call model).

1.3 Our Results In this paper we introduce the following modifications of the random phone call model:

- **Model I:** Let a piece of information r be initially placed on one of the nodes of a graph $G = (V, E)$. Then, in each succeeding time step, every node of G chooses *four different neighbors*, uniformly at random, and establishes communication channels with these neighbors.

- **Model II:** Let a piece of information r be placed initially on one of the nodes of a graph $G = (V, E)$. Then, in each succeeding time step t any node u of G chooses a neighbor, uniformly at random *from the set of neighbors not chosen by u in time steps* $t - [(t-1) \mod 4], \ldots, t-1$ (whenever $t - [(t-1) \mod 4] \leq t-1$), i.e., it avoids the nodes chosen in the $[(t-1) \mod 4]$ most recent time steps, and establishes a communication channel with this neighbor.

In both models, every node is allowed to send/receive messages to/from all nodes which have established communication channels with u in the current step. We assume in both cases that any node has a proper estimate of n.

We show that if $p > \log^{\delta} n/n$, where δ is some properly chosen constant, then there is an algorithm in both Models (I and II), which broadcasts any information r, placed initially on one of the nodes of a random graph G_p, to all nodes of the graph within $O(\log n)$ time steps, by producing only $O(n \log\log n)$ transmissions, w.h.p. Furthermore, we show the optimality of our results.

Please note that our main theorem w.r.t. Model I is a "power of two choices" type result (cf. [25]), and might have applications in different fields of computer science beyond randomized broadcasting. The main result concerning Model II implies that if we empower the nodes with the ability to remember in each step t the addresses of the neighbors chosen in time steps $t-3, t-2,$ and $t-1$, then the number of total message transmissions may decrease by almost a logarithmic factor.

Our analysis consists of two main parts. In the first part we consider the case when the number of uninformed nodes is larger than $n/\sqrt[4]{d}$, while in the second part we focus on the case when the number of uninformed nodes is smaller than $n/\sqrt[4]{d}$. In the first part we may use similar techniques to [20, 9]. However, in the second part we cannot apply the same methods. Thus, in order to handle the second case we have to derive new combinatorial results w.r.t. the structure of random graphs, and by applying probabilistic techniques we then integrate these results into the dynamical behavior of randomized broadcasting.

We give now a brief description about the relationship between the number of different choices and the number of message transmissions produced by the algorithm. If any node is only allowed to choose *one single neighbor*, uniformly at random, then we need $\Omega(n \log n/\log d)$ message transmissions to inform all nodes in G_p, w.h.p. [9]. The main idea behind this lower bound result is that if only one neighbor is chosen in each step, then two adjacent nodes can repeatedly select each other as communication partners, and remain uninformed for $\Omega(\log n/\log d)$ steps after $n/2$ nodes have been informed. In light of this fact, one would expect that some mechanism, which excludes the possibility that in a very small subset of nodes each node places only calls to nodes of this subset for $\omega(\log\log n)$ steps, is able to overcome this bottleneck and achieves the communication bound obtained in complete graphs. If the nodes are allowed to choose *two different neighbors* in each step, then with probability $1 - o(1)$ there does not exist such a subset of nodes, and a mechanism with the properties described above is implemented. However, a careful adaption of our proofs to this case would imply that with probability $1 - o(1)$ the number of transmissions is still $\Theta(n\sqrt{\log n/\log d})$, and this contradicts the expectation formulated before. On the other hand, if we allow the nodes to choose *three different neighbors*, then we do obtain the desired $O(n \log\log n)$ bound. Since the analysis of this case would be very complex and hard to read, we concentrate in this paper on the *power of four choices*.

The results of this paper can also be extended to the case $p \geq \delta' \log n/n$, where δ' is a large constant, and to the general random graph model of [6], if $d_{\min} \geq \delta' \log n$. However, the proofs for these cases would require elaborate case analysis which is omitted in this paper due to space limitations.

2 Randomized Broadcasting on G_p

We begin our analysis with Model I. We show that there is an efficient algorithm with respect to both, runtime and message complexity, which broadcasts a message to all nodes of a random graph G_p, where $p > \log^{\delta} n/n$ for some proper constant $\delta > 3$. Then, we state a relationship between Model I and Model II, and construct an efficient algorithm for Model II. We conclude the section by proving the optimality of our algorithm.

Analysis of Model I: In this section we analyze the behavior of a randomized broadcasting algorithm which is based on Model I introduced in the previous section. Hereby we assume that all nodes have access to a global clock, and they work in a synchronous environment. Due to the definition of the model, a node may transmit/receive messages to/from several neighbors within one step, however, the number of total messages in one step is still asymptotically bounded by the number of vertices.

We consider the model described above on random graphs G_p of size n and average degree $d = pn$. Note that for our choice of p the graph G_p is connected with high probability [2]. We assume in this section that every node has an estimation of n (within a constant factor), and present an algorithm which is able, w.h.p, to broadcast an information r to all nodes of G_p within $O(\log n)$ time steps, whereby the number of transmissions related to r is bounded by $O(n \log \log n)$.

As mentioned in the introduction, we assume that new pieces of information occur frequently in the network so that almost every node places a call in each time step anyway. However, we only focus here on the distribution and lifetime of a single information. The algorithm we describe in the following paragraphs consists of several time steps. In each time step, whenever a communication channel is established between two nodes, each one of them has to decide whether to transmit the specific information to the other node, without knowing if the vertex at the other end of the edge has already received some specific information prior to this step. The size of information exchanged in any way is not limited and the exchange of one piece of information between two neighbors is counted as a single transmission.

Let r denote the information we consider and assume w.l.o.g. that r is placed on one of the nodes at time 0. In each succeeding time step, any node which decides to transmit r, also sends the age of r (cf. algorithm below). At the beginning, we initialize at each node u the integer $age = 0$, which is used to denote the age of r, and a counter $ctr = 0$. During the execution of the algorithm, each node can be in one of the states U (uninformed), A (active), G (going down), or S (sleeping). At the beginning, the node on which r has initially been placed is in state A. All other nodes are in state U. Now, in each step t any node $u \in V$ executes the following procedure:

---

1. Choose 4 different neighbors, uniformly at random, and call these nodes to establish communication channels with them. Furthermore, establish communication channels with all nodes which call u.
2. If u is in state A or G, then send to all nodes which have established a communication channel with u the message (r, age).
3. Receive messages from all neighbors which established a communication channel with u. Let these messages be denoted by (r, age_1), ..., (r, age_k) (if any). Then, close all communication channels.
4. Perform the following local computations:
   - 4.1. If u is in state U and receives r, then switch state of u to A, and set age to age_1.
   - 4.2. If u is in state A and $age \geq \log_9 n$, then switch state of u to G.
   - 4.3. If u is in state G, then increment ctr by 1. If additionally $ctr = \lceil \alpha \log \log n \rceil$ for some large constant α, then switch state of u to S.
   - 4.4. If u is in state A/G, then increment age by 1.

Figure 1: The Algorithm for Model I performed by some node u in time step t. Observe that $age_1 = age_2 = \ldots = age_k$, since these ages are all associated with r.

Please note that in this algorithm, the nodes are aware of a proper estimate of n (within a constant factor). In the rest of this section we analyze the behavior of the algorithm presented above. First, we state a combinatorial result needed for the main analysis.

For some $u, v \in V$ let $A_{u,v}$ denote the event that u and v are connected by an edge, and let $A_{u,v,l}$ denote the event that u and v share an edge **and** u calls v in time step l (according to Model I described above). In the next "deconditioning lemma", we deal with the distribution of the neighbors of a node u in a graph G_p, after it has chosen $4t$ neighbors, uniformly at random, in $t = O(\log n)$ consecutive time steps. In particular, we show that the probability of u being connected with some node v, not chosen within these t time steps, is not substantially modified after $O(\log n)$ time steps.

LEMMA 2.1. *Let $V = \{v_1, \ldots, v_n\}$ be a set of n nodes and let every pair of nodes v_i, v_j be connected with probability p, independently, where $p \geq \log^{\delta} n/n$ for some constant $\delta > 3$. If $t = O(\log n)$, $u, v \in V$, and $A(U_0, U_1, U_2) = \bigwedge_{\substack{0<l\leq t \\ (v_i,v_j,l)\in U_0}} A_{v_i,v_j,l} \bigwedge_{(v_{i'},v_{j'})\in U_1} A_{v_{i'},v_{j'}} \bigwedge_{(v_{i''},v_{j''})\in U_2} \overline{A_{(v_{i''},v_{j''})}}$, then we have*

$$\Pr\left[(u,v) \in E \mid A(U_0,U_1,U_2)\right] = p(1 \pm O(t/d)),$$

for any $U_0 \subset V \times V \times \{0, \ldots, t\}$ and $U_1, U_2 \subset V \times V$ satisfying the following properties:

- *$|U_0 \cap \{(v_i, v_j, l) \mid v_j \in V \setminus \{v_i\}\}| = 4$ for any $v_i \in V$ and $l \in \{0, \ldots, t\}$, (i.e, every node chooses 4 different neighbors in each step),*
- *$|U_1 \cap \{(u, u') \mid u' \in V \setminus \{u\}\}| = \Omega(d)$ and $|U_1 \cap \{(v, v') \mid v' \in V \setminus \{v\}\}| = \Omega(d)$, (i.e., u and v have $\Omega(d)$ neighbors, each),*
- *$(u, v) \notin U_1 \cup U_2$, and $(u, v, l), (v, u, l) \notin U_0$ for any $l \leq t$, (i.e., nothing is known about the existence of an edge between u and v).*

The proof of this lemma is similar to the proof of Lemma 1 in [9], and is omitted due to space limitations.

This lemma implies that even if the occurrence of the edges are not really independent after $t = O(\log n)$ steps, in certain cases (as in the lemmas below) we still can apply some known results which normally require independency (like the Chernoff bounds [4, 18]), since $\Pr[(u,v) \in E \mid A(U_0,U_1,U_2)]$ is properly approximated by $p(1 \pm O(t/d))$.

Now we are ready to analyze the algorithm presented at the beginning of this section. Let A_d denote the event that each node of G_p has $\Omega(d)$ neighbors. In our proofs we will often use the fact that $\Pr[A_d] = 1 - o(1/n^2)$ for this choice of p [2]. Let $I(t)$ denote the set of informed nodes at time t. The set of uninformed nodes is denoted by $H(t) = V \setminus I(t)$.

Our analysis consists of two main parts. In the first part, we show that within $\log_9 n + O(\log\log n)$ time steps the number of uninformed nodes becomes smaller than $n/\sqrt[4]{d}$, and the number of message transmissions is bounded by $O(n \log\log n)$. Since we use here similar techniques to [20, 9], the proof of this part is omitted due to space limitations. The second part of the analysis handles the case when $|H(t)| \leq n/\sqrt[4]{d}$. In this part it is essential to use the combinatorial power of four neighbor choices, and the techniques of [20, 9] are not applicable here. Since this part of the analysis is crucial for our main result, the corresponding lemmas and proofs are included in the paper.

In our proofs, *age* and t are considered to be the same at any informed node, since we assumed that r is placed on one of the nodes at time 0. We know that the algorithm has the claimed performance if $p = n^{\Omega(1/\log\log n)}/n$ [9], even in the unmodified random phone call model. Hence, we assume here that $p \in [\log^{\delta} n/n, n^{O(1/\log\log n)}/n]$. First we consider the simple case in which $|H(t)| \geq n/\sqrt[4]{d}$, and state the following lemma.

LEMMA 2.2. *Let the algorithm presented at the beginning of this section be executed on the graph G_p of size n, where $p > \log^{\delta} n/n$ and α is a properly chosen (large) constant. If $t = \log_9 n + \frac{\alpha}{2}\log\log n$, then $|H(t)| \leq n/\sqrt[4]{d}$ and the number of transmissions after t time steps is bounded by $O(n \log\log n)$. Additionally, if $t = \log_9 n + \frac{3\alpha}{8}\log\log n$, we have $|H(t)| \geq n/\sqrt[4]{d}$.*

The proof of this lemma is omitted due to space limitations. In the rest of this section we consider the case $|H(t)| \leq n/\sqrt[4]{d}$. Before we start with the analysis, we first derive some combinatorial results w.r.t. $H(t)$. For some t, define $G(t) = (H(t), E(t))$ with $E(t) = \{(v, w) \mid (v, w) \in E \text{ and } v, w \in H(t)\}$. Let $k_t = |H(t)|$ and let $v_1, \ldots, v_{k_t}$ represent the nodes of $H(t)$. Furthermore, let the probability space $\mathcal{G}(d_1, \ldots, d_{k_t})$ consist of all (simple) graphs of size k_t, in which v_i has degree d_i, $i \in \{1, \ldots, k_t\}$ (for a fixed ordering of the nodes), and assign each graph from this probability space the same probability. In order to analyze the graphs of $\mathcal{G}(d_1, \ldots, d_{k_t})$, we use the so called configuration model (also known as pairing model) [2, 27].

LEMMA 2.3. *For some $k > \log^q n$ let $G \in \mathcal{G}(d_1, \ldots, d_k)$, where q is a large constant, and let $d_i \in \{1, \ldots, O(\log n)\}$ for any $i \in \{1, \ldots, k\}$. If S is an arbitrary subset of the nodes of G of size $O(k/x)$, where $x \geq \log^4 k$, then, with probability $1 - o(n^{-2})$ there is a set $X \subset S$ of size $|X| = \Omega(|S|/(x \log^{O(1)} n) - \log^{q-1} n)$ such that any node of X has at least one neighbor in S. Moreover any such X has $O(|S| \log n/x + \log^{q-1} n)$ vertices, and any set Y in which each node has at least 4 neighbors in S has $O(|S|(\log^{O(1)} n/x)^4 + \log^{q-1} n)$ vertices, with probability $1 - o(n^{-2})$.*

Proof. Let $V = \{v_1, \ldots, v_k\}$, and let $V' = \{(v_i, j) \mid v_i \in V \text{ and } 1 \leq j \leq d_i\}$. Let the probability space $\mathcal{G}'$ consist of all 1-regular graphs with set of nodes V', in which any such graph is assigned the same probability. Let $G' = (V', E')$ be a graph from the probability space $\mathcal{G}'$ (notice that E' consists of a perfect matching formed by the nodes of V'). Then, G' *corresponds* to some graph $G = (V, E)$ iff for any $((v_i, j), (v_{i'}, j')) \in E'$ we have $(v_i, v_{i'}) \in E$ and for any $(v_i, v_{i'}) \in E$ there exist $j \in \{1,\ldots,d_i\}$ and $j' \in \{1,\ldots,d_{j'}\}$ such that $((v_i,j),(v_{i'},j')) \in E'$.

It is known that for any $G \in \mathcal{G}(d_1,\ldots,d_k)$ there are $d_1! \cdot \ldots \cdot d_k!$ different graphs G' in $\mathcal{G}'$ corresponding to G [24]. For any such G' it holds that if two nodes $(v_i,j),(v_{i'},j') \in V'$ are connected, then for any $l \in \{1,\ldots,d_i\} \setminus \{j\}$ and $l' \in \{1,\ldots,d_{i'}\} \setminus \{j'\}$ we have $((v_i,l),(v_{i'},l')) \notin E'$. On the other hand, if in a graph $G' \in \mathcal{G}'$ there are some j,j',l,l' with $j \neq l$ and $j' \neq l'$ such that $((v_i,j),(v_{i'},j')),((v_i,l),(v_{i'},l')) \in E'$, then G' does not correspond to any graph $G \in \mathcal{G}(d_1,\ldots,d_k)$.

Now we concentrate on the class $\mathcal{G}'$, and analyze the distribution of the edges in a graph $G' \in \mathcal{G}'$. Let S be a subset of $\{v_1,\ldots,v_k\}$ and let $N(v_i,j)$ denote the set of neighbors of (v_i,j) in G'. Let us consider the edges incident to the nodes of the subset $S' = \{(v_i,j) \in V' \mid v_i \in S \text{ and } 1 \leq j \leq d_i\}$. Assume w.l.o.g. that $S = \{v_1,\ldots,v_{|S|}\}$, and let G' be the graph generated by the following procedure: At time 0 let $G'_0 = (V',\emptyset)$. In time interval $[i-1,i]$ consider node v_i, and in substep $i-1+j/d_i$ if $N(v_i,j) = \emptyset$, then choose in substep $i-1+j/d_i$ a node $(v_{i'},j') \neq (v_i,j)$ with $N(v_{i'},j') = \emptyset$, uniformly at random, and set $E' = E' \cup \{((v_i,j),(v_{i'},j'))\}$. Define $G'_t = (V',E')$ as the random graph, which is obtained by this algorithm at time t. Obviously, this procedure generates any $G' \in \mathcal{G}'$ with the same probability.

Let X_{in} be the random variable which denotes the number of edges between the nodes of S' in G'. Let $X_{i-1+j/d_i} = \mathbf{E}[X_{in} \mid G'_{i-1+j/d_i}]$. Now it is easy to verify that the martingale condition holds, i.e., $\mathbf{E}[X_{i-1+j/d_i} \mid X_0,\ldots,X_{i-1+(j-1)/d_i}] = X_{i-1+(j-1)/d_i}$, if $j > 0$. Similarly, it also holds that $\mathbf{E}[X_i \mid X_0,\ldots,X_{i-1+(d_i-1)/d_i}] = X_{i-1+(d_i-1)/d_i}$. Hence, $X_0,\ldots,X_{|S|}$ is a Martingale (similar to a vertex- or edge exposure Martingale [1]). Now, $|X_{i-1+j/d_i} - X_{i-1+(j-1)/d_i}| = 0$, if the node (v_i,j) is already connected to a node $(v_{i'},j')$ with $i' < i$, or $i' = i$ and $j' < j$. If (v_i,j) is connected to a node of $V' \setminus S'$, then $|X_{i-1+j/d_i} - X_{i-1+(j-1)/d_i}| = O(|S'|/|V'|)$, and if (v_i,j) is connected to a node $(v_{i'},j')$ with $i' > i$ or $i' = i$ and $j' > j$, then $|X_{i-1+j/d_i} - X_{i-1+(j-1)/d_i}| \leq 1$. Since a node (v_i,j) is connected to some $(v_{i'},j') \in S' \setminus G'_{i-1+(j-1)/d_i}$ with probability $O(|S'|/|V'|)$, we have $\mathrm{Var}[X_{i-1+j/d_i} \mid G'_{i-1+(j-1)/d_i}] = O(|S'|/|V'|)$. Applying now an Azuma-Hoeffding type inequality [5] and using $X_0 = |S'|(|S'|-1)/2(|V'|-1)$ we obtain that $\Pr[|X_{|S|} - X_0| \geq \sqrt{X_0}\log^2 n]$ is at most

$$\begin{aligned}
& 2e^{-\frac{X_0 \log^4 n}{O(|S'|^2/|V'| + \sqrt{X_0}\log^2 n)}} \\
\leq \quad & 2e^{-\Omega(\frac{|S'|^2 \log^4 n/|V'|}{|S'|^2/|V'| + |S'|\log^2 n/\sqrt{|V'|}})} \\
\leq \quad & 2e^{-\omega(\log^3 n)},
\end{aligned}$$

whenever $|S'|^2/|V'| = \omega(\log^2 n)$. Then, the inequality above implies that there are $|S'|(|S'|-1)/2(|V'|-1) \pm O(\sqrt{|S'|^2/|V'|} \cdot \log^2 n)$ inner edges in S', with probability $1 - e^{-\omega(\log^3 n)}$. A corresponding upper bound on the number of vertices of S having at least four neighbors in S' can be derived by applying some case analysis w.r.t. to the cardinality of the sets S' and V'.

It is known that $\mathcal{G}'$ contains $|\mathcal{G}'|/e^{O(\log^2 n)}$ graphs which correspond to some graph $G \in \mathcal{G}(d_1,\ldots,d_k)$ [24]. On the other hand, in an arbitrary graph $G' \in \mathcal{G}'$ there are $|S'|(|S'|-1)/2(|V'|-1) \pm O(\sqrt{|S'|^2/|V'|} \cdot \log^2 n)$ inner edges in some S', with probability $1 - e^{-\omega(\log^3 n)}$. Summarizing, the number of inner edges in an arbitrary set of nodes S' of a graph $G' \in \mathcal{G}'$, which corresponds to some graph $G \in \mathcal{G}(d_1,\ldots,d_k)$, is $|S'|(|S'|-1)/2(|V'|-1) \pm O(\sqrt{|S'|^2/|V'|} \cdot \log^2 n)$, with probability $1 - e^{-\omega(\log^3 n)}$. We consider now a graph $G \in \mathcal{G}(d_1,\ldots,d_k)$. Since $|S| = O(|S'|)$ and $|V| = \Omega(|V'|/\log n)$, we conclude that in an arbitrary subset $S \subset V$ with $|S| = O(|V|/\log^4 k)$ there are at most $O(|S|^2 \log n/|V| + \log^{q-1} n)$ inner edges, with probability $1 - e^{-\omega(\log^3 n)}$, provided that q is large enough. If now X denotes the set of nodes being incident to these inner edges we obtain the second claim of the lemma. The upper bound for the subset of nodes which have four neighbors in S is obtained in a similar way. The results above also imply that there is a subset of S, which has $\Omega(|S|^2/(|V|\log^{O(1)} n) - \log^{q-1} n)$ neighbors in S, with probability $1 - e^{-\omega(\log^3 n)}$, whenever q is large enough. □

A similar lemma can also be stated for the case $d_1,\ldots,d_k = \Theta(f)$ for some $f = \Omega(\log n)$.

Lemma 2.4. *For some $k > \log^q n$ let $G \in \mathcal{G}(d_1,\ldots,d_k)$, where q is a large constant, and $d_i = \Theta(f)$ for any $i \in \{1,\ldots,k\}$, where $f = \Omega(\log n)$. Now, if S is an arbitrary subset of the nodes of G of size $O(k/x)$, where $x \geq \log^4 k$, then, with probability $1 - o(n^{-2})$ there is a set $X \subset S$ of size $|X| = \Omega(|S|f/x - \log^{q-1} n)$ such that any node of X has at least one neighbor in S. Moreover any such X has $O(|S|f/x + \log^{q-1} n)$ vertices, and any set Y in which each node has at least 4 neighbors in S has at most $O(|S|(f/x)^4 + \log^{q-1} n)$ vertices, with probability $1 - o(n^{-2})$.*

The proof of this lemma is similar to the proof of Lemma 2.3 and is omitted due to space limitations.

Now we consider the distribution of the edges in the set $H(t)$.

Lemma 2.5. *Let G_p be a random graph on the set $V = \{v_1,\ldots,v_n\}$ of nodes with $p > \log^\delta n/n$, and let* *the algorithm described at the beginning of this section be executed for this graph. Furthermore, let $A(t,S,G_I)$ denote the event $(G(t) \in \mathcal{G}(d_1,\dots d_{k_t})) \wedge (H(t) = S) \wedge (G_p \setminus G(t) = G_I)$, where S is a subset of V, $G_I = (V, E_I)$ is a fixed graph with $E_I \cap (S \times S) = \emptyset$, and $G_p \setminus G(t) = (V, E \setminus E(t))$. If $\Pr[A(t,S,G_I] \neq 0$, then for any fixed $G(d_1,d_2,\dots,d_{k_t}) \in \mathcal{G}(d_1,\dots,d_{k_t})$*

$$\Pr[G(t) = G(d_1,d_2,\dots,d_{k_t}) \mid A(t,S,G_I)]$$

equals $1/|\mathcal{G}(d_1,\dots,d_{k_t})|$.

Proof. We know that any fixed random graph $G_p = (V,E)$ with n vertices and exactly m edges occurs with probability $p^m(1-p)^{n(n-1)/2-m}$, whenever $m \leq n(n-1)/2$.

We assume w.l.o.g. that the vertices $v_1,\dots,v_n \in V$ are ordered so that $v_1,\dots,v_{k_t} \in S$, and call an edge $(v_i,v_r) \in E$ the jth edge of v_i, if there are exactly $j-1$ edges $(v_i,v_k) \in E$ with $k < r$. Let $A(v_i,j,l)$ denote the event that node v_i chooses its jth neighbor in step $l \leq t$, and let $A(t) = \wedge_{(v_i,j,l)\in U} A(v_i,j,l)$, where $U \subset V \times \{1,\dots,n\} \times \{1,\dots,t\}$ such that $|U \cap \{(v_i,j,l) \mid 1 \leq j \leq |N(v_i)|\}| = 4$ for any $v_i \in V$ and $l \leq t$. Then, we show that $\Pr[G(t) = G' \mid (G_p \setminus G(t) = G_I) \wedge (G(t) \in \mathcal{G}(d_1,\dots,d_{k_t})) \wedge (H(t) = S) \wedge A(t)]$ is the same for any fixed G', whenever $\Pr[G_p \setminus G(t) = G_I \wedge G(t) \in \mathcal{G}(d_1,\dots,d_{k_t}) \wedge A(t)] \neq 0$.

We know that

$$\begin{aligned}
P_t &= \Pr[G(t) = G' \mid (G_p \setminus G(t) = G_I) \wedge \\
&\quad (G(t) \in \mathcal{G}(d_1,\dots,d_{k_t})) \wedge (H(t) = S) \wedge A(t)] \\
&= \Pr[(G(t) = G') \wedge (G_p \setminus G(t) = G_I) \wedge \\
&\quad (G(t) \in \mathcal{G}(d_1,\dots,d_{k_t})) \wedge (H(t) = S) \wedge A(t)] \cdot \\
&\quad (\Pr[(G_p \setminus G(t) = G_I) \wedge (G(t) \in \mathcal{G}(d_1,\dots,d_{k_t})) \\
&\quad \wedge (H(t) = S) \wedge A(t)])^{-1} \\
&= \Pr[(G_S = G') \wedge (G_p \setminus G_S = G_I) \wedge \\
&\quad (G(t) \in \mathcal{G}(d_1,\dots,d_{k_t})) \wedge (H(t) = S) \wedge A(t)] \cdot \\
&\quad (\Pr[(G_p \setminus G_S = G_I) \wedge (G_S \in \mathcal{G}(d_1,\dots,d_{k_t})) \\
&\quad \wedge (H(t) = S) \wedge A(t)])^{-1},
\end{aligned}$$

where G_S denotes the subgraph induced by the vertices of S. Now we show that if $(G_S = G') \wedge (G_p \setminus G_S = G_I) \wedge A(t)$ leads to $H(t) = S$, then for any $G'' \in \mathcal{G}(d_1,\dots,d_{k_t})$ the event $(G_S = G'') \wedge (G_p \setminus G_S = G_I) \wedge A(t)$ leads to $H(t) = S$, too. To show this, we prove by induction that $H(i)$ is the same in both $G' \cup G_I$ and $G'' \cup G_I$ for any $i \leq t$. For $i = 0$ the assumption is trivially fulfilled. Now assume that the claim holds for $i-1$. If now a node v in the graph $G_I \cup G'$ becomes informed in step i, then there must be some event $A(u,j,i)$ or $A(v,j',i)$ such that the jth edge of $u \in I(i-1)$ is adjacent to v, or the j'th edge of v is adjacent to a node $u' \in I(i-1)$. In both cases the corresponding event implies that v in $G_I \cup G''$ becomes informed as well, since both edges (jth edge of u and j'th edge of v) are contained in G_I. On the other hand, if a node v of $G_I \cup G'$ is in $H(i)$, then for all events $A(u,j,i)$, for which the jth edge of u is adjacent to v, it holds that $u \in H(i-1)$. Similarly, for $A(v,j',i)$ we conclude that the j'th edge of v is adjacent to some node $u' \in H(i-1)$. If now $u' \in V \setminus S$, then the j'th edge of v is still adjacent to u' in $G_I \cup G''$, and v cannot be informed. If the j'th edge of v is adjacent to some $u' \in S$ in $G_I \cup G'$, then v has less than $d_v - j'$ neighbors in $V \setminus S$, and the j'th edge of v in $G_I \cup G''$ will be in G''. Hence, the claim holds.

Now assume $(G_S = G') \wedge (G_p \setminus G_S = G_I) \wedge (G_S \in \mathcal{G}(d_1,\dots,d_{k_t})) \wedge A(t)$ leads to $H(t) = S$. Then,

$$\begin{aligned}
P_t &= \Pr[(G_S = G') \wedge (G_p \setminus G_S = G_I) \wedge \\
&\quad (G_S \in \mathcal{G}(d_1,\dots,d_{k_t})) \wedge A(t)] \cdot \\
&\quad (\Pr[(G_p \setminus G_S = G_I) \wedge \\
&\quad (G_S \in \mathcal{G}(d_1,\dots,d_{k_t})) \wedge A(t)])^{-1} \\
&= \Pr[(G_S = G') \wedge (G_p \setminus G_S = G_I)] \Pr[A(t)] \cdot \\
&\quad (\Pr[(G_p \setminus G_S = G_I) \wedge \\
&\quad (G_S \in \mathcal{G}(d_1,\dots,d_{k_t}))] \Pr[A(t)])^{-1} \\
&= \frac{1}{|\mathcal{G}(d_1,\dots,d_{k_t})|},
\end{aligned}$$

which is independent of G' and $A(t)$. Thus, the lemma holds. □

In the next lemma we analyze the subset $H(t+1)$ of $H(t)$ given some properties of $H(t)$. In fact we prove that the set $H(t+1)$ does not depend on the distribution of the edges which have both endpoints in $H(t)$.

Lemma 2.6. *Let $G_p = (V,E)$ be a random graph with $p > \log^\delta n/n$, and let the algorithm described at the beginning of this section be executed for this graph. Furthermore, let $A'(t,S',G_I)$ denote the event $(G_p \setminus G(t) = G_I) \wedge (G(t) = G') \wedge (H(t) = S')$ Then, for any t with $|H(t)| \geq \log^q n$, where q is a large constant, and $S \subseteq H(t)$, the conditional probability*

$$\Pr[H(t+1) = S \mid A'(t,S',G_I)]$$

is the same for any $G' \in \mathcal{G}(d_1,\dots,d_{k_t})$, whenever $\Pr[(G_p \setminus G(t) = G_I) \wedge (G(t) = G') \wedge (H(t) = S')] \neq 0$. *Here S' is a fixed set of nodes, and G_I is a graph of size n.*

Again, the proof of this lemma is omitted due to space limitations.

Now we are ready to analyze the case $|H(t)| \leq n/\sqrt[4]{d}$.

LEMMA 2.7. *Let $|H(t)| \in [\log^q n, n/\sqrt[4]{d}]$ be the number of uninformed nodes in G_p at some time $t = O(\log n)$, where q is a large constant, and let the algorithm described at the beginning of this section be executed on G_p. If all informed nodes are in state A or G with $ctr \leq 3\alpha \log\log n/4$, then $|H(t + c\log\log n)| \leq \log^q n$, w.h.p., provided that α and c are large enough.*

Proof. If $A(d_1, \ldots, d_{k_t})$ denotes the event that $v_i \in H(t)$ has degree d_i for any $i \in \{1, \ldots, k_t\}$, then Lemma 2.5 implies that

$$\Pr[G(t) = G(d_1, \ldots, d_{k_t}) \mid A(d_1, \ldots, d_{k_t})]$$

equals $1/|\mathcal{G}(d_1, \ldots, d_{k_t})|$ for any $G(d_1, \ldots, d_{k_t}) \in \mathcal{G}(d_1, \ldots, d_{k_t})$.

Now we concentrate on $H(t_0)$, where t_0 denotes the first time step in which $|H(t_0)| \leq n/\sqrt[4]{d}$. Combining Lemma 2.1 with the Chernoff bounds [4, 18], we conclude that any node of $H(t_0)$ has, with probability $1 - o(1/n^2)$, at most $p|H(t_0)|(1 + o(1)) = O(\sqrt[4]{d^3})$ uninformed neighbors. We assume for simplicity that $|H(t_0)| \in [\omega(n \log n/d), o(n/\sqrt[4]{d \log n})]$. Since each node of $H(t_0)$ has $p|H(t_0)|(1 \pm o(1))$ neighbors in $H(t_0)$, with probability $1 - o(1/n^2)$, a node remains uninformed with conditional probability $(p|H(t_0)|(1 \pm o(1))/d)^4 = (|H(t_0)|(1 \pm o(1))/n)^4$, given that every node has $d(1 \pm o(1))$ neighbors in G_p and $p|H(t_0)|(1 \pm o(1))$ neighbors in $H(t_0)$. Since each of these two events occurs with probability $1 - o(n^{-2})$, we neglect the cases in which one of these events does not occur. Then, $|H(t_0 + 1)| = \Theta((H(t_0)/n)^4)|H(t_0)|$, w.h.p., and since we assumed that $|H(t_0)| = o(n/(\sqrt[4]{d \log n}))$, we have $|H(t_0 + 1)| = o(n/d)$, w.h.p.

Next we focus on $H(t_0 + 2)$. Let $d_1, \ldots, d_{k_{t_0}}$ denote the degree sequence occurring in $H(t_0)$. Then $\Pr[G(t_0) = G(d_1, \ldots, d_{k_{t_0}})] = 1/|\mathcal{G}(d_1, \ldots, d_{k_{t_0}})|$ for any $G(d_1, \ldots, d_{k_{t_0}})$, and $d_i = \Theta(p|H(t_0)|)$ for any i, with probability $1 - o(1/n^2)$. Again, we ignore the cases in which $d_i \neq \Theta(p|H(t_0)|)$ for some i.

Due to Lemma 2.6, the set of nodes informed in step $t_0 + 1$ is independent of the distribution of the edges inside $H(t_0)$. Then, applying Lemma 2.4 with $k = |H(t_0)|$, $S = H(t_0 + 1)$, and $f = p|H(t_0)|$, we conclude that there are at most $\Theta\left(\left(\frac{|H(t_0+1)|}{|H(t_0)|} \cdot p|H(t_0)|\right)^4\right) \cdot |H(t_0 + 1)|$ nodes in $H(t_0 + 1)$ which have at least 4 neighbors in $H(t_0 + 1)$, w.h.p. All other uninformed nodes become informed in step $t_0 + 2$. Due to Lemma 2.1, every node of $H(t_0 + 1)$ has $O(\log n)$ neighbors in $H(t_0 + 1)$, with probability $1 - o(1/n^2)$. Therefore, a fraction of $1 - O(\log^4 n/d^4)$ of the uninformed nodes which have more than 3 neighbors in $H(t_0 + 1)$ become informed in step $t_0 + 2$, w.h.p. This implies that

$$\begin{aligned} |H(t_0 + 2)| &\leq \Theta\left(\left(\frac{|H(t_0 + 1)|}{|H(t_0)|} \cdot p|H(t_0)|\right)^4\right) \cdot \\ &\qquad |H(t_0 + 1)| \cdot O\left(\frac{\log^4 n}{d^4}\right) \\ &\leq O\left(|H(t_0 + 1)|^4 \frac{\log^4 n}{n^4}\right) \cdot |H(t_0 + 1)|, \end{aligned}$$

w.h.p. On the other hand, Lemma 2.4 also implies that a fraction of $\Omega\left(\frac{|H(t_0+1)|}{|H(t_0)|} \cdot p|H(t_0)|\right)$ of the nodes informed in step $t_0 + 2$ has at least one neighbor in $H(t_0 + 1)$, with probability $1 - o(1/n^2)$.

Now we show by induction that if $|H(t)|, |H(t+1)| \in [\log^q n, n/(d \log n)]$, then the following properties hold:

1. $\frac{|H(t+1)|}{|H(t)|} = O\left(\frac{|H(t)|^2}{|H(t-1)|^2}\right)$, w.h.p., and
2. $\Omega\left(\frac{|H(t)|^2}{|H(t-1)| \log^{O(1)} n}\right)$ nodes of $H(t)$ have at least one neighbor in $H(t)$, w.h.p.

We have seen above that the claim holds for $t = t_0 + 1$. Now assume that the claim holds for some $t > t_0$, and we are going to show that it also holds for $t + 1$. Again, due to Lemma 2.5 we have here $\Pr[G(t) = G(d_1, \ldots, d_{k_t})] = 1/|\mathcal{G}(d_1, \ldots, d_{k_t})|$ for any $G(d_1, \ldots, d_{k_t})$, where $d_i = O(\log n)$ for any i. Thus, the set of nodes informed in step $t + 1$ is independent of the distribution of the edges inside $H(t)$, provided that $A(d_1, \ldots, d_{k_t})$ occurs. We assumed that the claim holds for t, and hence there are $\Omega(|H(t)|^2/(|H(t-1)| \log^{O(1)} n))$ nodes in $H(t)$ with $d_i \geq 1$, with probability $1 - o(1/n^2)$. Since $d_i = O(\log n)$, we can apply Lemma 2.3 with $k = \Omega(|H(t)|^2/(|H(t-1)| \log^{O(1)} n))$ and $S = H(t+1)$, and conclude that there are $O\left(\frac{|H(t+1)| \log^{O(1)} n}{|H(t)|^2/|H(t-1)|}\right)^4 \cdot |H(t + 1)|$ nodes in $H(t + 1)$ with at least 4 neighbors in $H(t + 1)$, w.h.p. Now an uninformed node v_i with at least 4 uninformed neighbors remains uninformed with probability $O((d_i/d)^4) = O((\log n/d)^4)$. Thus, applying a Chernoff bound we obtain

$$\begin{aligned} |H(t + 2)| &= O\left(\frac{|H(t + 1)| \log^{O(1)} n}{|H(t)|^2/|H(t - 1)|}\right)^4 \cdot \\ &\qquad O\left(\frac{\log^4 n}{d^4}\right)|H(t + 1)| \\ &= O\left(\frac{|H(t + 1)|}{|H(t)|^2/|H(t - 1)|}\right)^4 \cdot \\ &\qquad \frac{\log^{O(1)} n}{d^4}|H(t + 1)| \\ &= O\left(\left(\frac{|H(t + 1)|/|H(t)|}{|H(t)|/|H(t - 1)|}\right)^4\right)|H(t + 1)|, \end{aligned}$$

w.h.p., whenever δ is large enough. Now, since $(|H(t)|/|H(t-1)|)^2 = \Omega(|H(t+1)|/|H(t)|)$, we obtain

$$\frac{|H(t+2)|}{|H(t+1)|} = O\left(\frac{|H(t+1)|^2}{|H(t)|^2}\right).$$

In order to show the second claim of the induction, we make use of the fact that $\Pr[G(t+1) = G(d_1, \ldots, d_{k_{t+1}})] = 1/|\mathcal{G}(d_1, \ldots, d_{k_{t+1}})|$ for any $G(d_1, \ldots, d_{t+1})$, where $d_i = O(\log n)$ for any i. Furthermore, there are at most $|H(t)|$ nodes in $G(t)$, and each of them has degree $O(\log n)$, w.h.p. Since any node of $H(t+1)$ has at least one uninformed neighbor before step $t+1$, we obtain by Lemma 2.3 that at least $\Omega(|H(t+1)|^2/(|H(t)| \log^{O(1)} n))$ nodes of $G(t+1)$ have a neighbor in $H(t+1)$, w.h.p.

Noting that the first property shown above induces a quadratic shrinking process, we obtain the lemma. $\square$

Lemma 2.8. *Let $|H(t)| \leq \log^q n$ be the number of uninformed nodes in G_p at time $t = O(\log n)$, and let the algorithm described at the beginning of this section be executed on G_p. If all informed nodes are in state A or G with ctr $\leq 7\alpha \log\log n/8$, then within additional $\alpha \log\log n/8$ steps all nodes in the graph will be informed, w.h.p., whenever α is large enough.*

Proof. Due to Lemma 2.1, any uninformed node has $O(\log n)$ uninformed neighbors. Therefore, a node remains uninformed after some step t with probability $O(\log^4 n/d^4)$. Using a Chernoff bound [4, 18], we obtain $|H(t+1)| = O(|H(t)| \log^4 n/d^4 + \log n)$, w.h.p., for any t with $|H(t)| \geq q \log n$.

To complete the proof, we show that with high probability there is no set of size $\leq q \log n$ in which more than 3/4th of the nodes have at least 4 inner neighbors. Let $S \subset V$ be a randomly chosen set of nodes with $|S| \leq q \log n$. If now $p_+ = p(1 + o(1))$, then this set contains more than $3|S|/2$ inner edges with probability

$$\begin{aligned} P_{3|S|/2} &= \sum_{i=3|S|/2}^{|S|^2/2} \binom{|S|^2/2}{i} p_+^i (1-p_+)^{|S|^2/2-i} \\ &\leq \left(\frac{p_+}{3/|S|}\right)^{3|S|/2} \left(\frac{1-p_+}{1-3/|S|}\right)^{|S|^2/2-3|S|/2} \\ &\leq \left(\frac{|S| n^{O(1/\log\log n)}}{3n}\right)^{3|S|/2} \left(\frac{1-o(1)}{1/n^{O(1)}}\right) \\ &= \frac{1}{n^{3|S|(1-o(1))/2}} \end{aligned}$$

(in the second inequality we used the estimates on the tail of binomial distributions [18]). On the other hand, there are less than $n^{|S|}$ sets of size $|S|$ in G_p. Applying now the Union bound, we obtain that there is no set of size $|S| \leq q \log n$ in G_p, which has more than $3|S|/2$ inner edges, w.h.p. This implies that if $|H(t)| \leq q \log n$, then $|H(t+1)| \leq 3|H(t)|/4$ for any t, w.h.p. $\square$

Lemma 2.8 ensures that all nodes become informed within $O(\log\log n)$ additional steps, w.h.p. Combining Lemmas 2.2-2.8, we obtain the following theorem.

Theorem 2.1. *Let G_p be a random graph of size n with $p > \log^\delta n/n$, and assume that a piece of information r is placed on one of the nodes at time 0. Then, the algorithm described at the beginning of this section distributes r, with high probability, to all nodes of G_p within $O(\log n)$ steps by producing only $O(n \log\log n)$ transmissions related to r.*

Using the techniques of [20, 9] we can show that the results of Theorem 2.1 are asymptotically optimal.

Analysis of Model II: For this model, we adapt the algorithm described for Model I in the following way: In Step 1. of the algorithm described in the previous section we allow any node u to choose one neighbor, uniformly at random, from the nodes not chosen by u in steps $t-[(t-1) \mod 4)], \ldots, t-1$. In Step 4.2. of the same algorithm u switches to state G if $age \geq \log_3 n$. In all other cases, the algorithm described for the Model I is executed.

Now we can state the following theorem w.r.t. to the runtime and message complexity of the algorithm.

Theorem 2.2. *Let G_p be a random graph of size n, where $p > \log^\delta n/n$. The algorithm described above broadcasts some piece of information r, placed on one of the nodes at time 0, to all nodes of G_p within $O(\log n)$ steps and by using $O(n \log\log n)$ transmissions related to r, w.h.p.*

The proofs in this part are omitted due to space limitations

Next we consider lower bounds on the runtime and number of message transmissions produced by "almost" oblivious randomized broadcasting algorithms.

Theorem 2.3. *Let G_p be a random graph with $p \geq \log^\delta n/n$ and assume that a piece of information r is placed on one of the nodes at time 0. Furthermore, we assume that in any succeeding time step t, each node u is allowed to choose one neighbor, uniformly at random from the set $N(u) \setminus S_t(u)$, where $S_t(u)$ is a subset of the neighbors chosen by u in steps $1, \ldots, t-1$, and to establish a communication channel with this neighbor. Now, even if every node is allowed to transmit r in both* *directions along an incident communication channel, any broadcasting algorithm obeying the rules above needs at least $\Theta(\log n)$ time steps, w.h.p., to spread r to all nodes of G_p. Moreover, any such time efficient broadcasting algorithm produces, with high probability, at least $\Omega(n \log\log n)$ transmissions of r.*

3 Conclusion

In this paper, we analyzed the runtime and number of message transmissions produced by simple randomized broadcasting algorithms in random-like graphs. We considered two simple modifications of the random phone call model, and showed that a minor change in the ability of the nodes implies a substantial decrease of the communication overhead generated in the network. It should be noted that the adaptive algorithms presented in [9] may also be applied to these modified models, and hence the results can be generalized to the case in which the nodes do not have any knowledge about the size or topology of the network. Additionally, the results can also be extended to the generalized random graph model introduced in [6], whenever the minimum degree is bounded by some polylogarithmic value in the number of nodes. Unfortunately, we could not generalize our results to random regular graphs of sublogarithmic degree by using the techniques of this paper. Furthermore, it would be interesting to know whether similar results can also be obtained for some well structured graphs.

References

[1] N. Alon and J. Spencer. *The Probabilistic Method*. John Wiley, 1991.

[2] B. Bollobás. *Random Graphs*. Academic Press, 1985.

[3] S.M. Botros and S.R. Waterhause. Search in jxta and other distributed networks. In *Proc. of P2P'01*, pages 30–35, 2001.

[4] H. Chernoff. A measure of asymptotic efficiency for tests of a hypothesis based on the sum of observations. *The Annals of Mathematical Statistics*, 23:493–507, 1952.

[5] F. Chung and L. Lu. Concentration inequalities and martingale inequalities — a survey. *Internet Mathematics (to appear)*.

[6] F. Chung and L. Lu. Connected components in random graphs with given expected degre sequences. *Annals of Combinatorics*, 6:125–145, 2002.

[7] C. Cooper, M. Dyer, and C. Greenhill. Sampling regular graphs and a peer-to-peer network. In *Proc. of SODA'05*, pages 980–988, 2005.

[8] A. Demers, D. Greene, C. Hauser, W. Irish, J. Larson, S. Shenker, H. Sturgis, D. Swinehart, and D. Terry. Epidemic algorithms for replicated database maintenance. In *Proc. of PODC'87*, pages 1–12, 1987.

[9] R. Elsässer. On the communication complexity of randomized broadcasting in random-like graphs. In *Proc. of SPAA'06*, pages 148–157, 2006.

[10] P. Erdős and A. Rényi. On random graphs I. *Publ. Math. Debrecen*, 6:290–297, 1959.

[11] P. Erdős and A. Rényi. On the evolution of random graphs. *Publ. Math. Inst. Hungar. Acad. Sci.*, 5:17–61, 1960.

[12] T. Feder, A. Guetz, M. Mihail, and A. Saberi. A local switch Markov chain on given degree graphs with application in connectivity of peer-to-peer networks. In *Proc. of FOCS'06*, pages 69–76, 2006.

[13] U. Feige, D. Peleg, P. Raghavan, and E. Upfal. Randomized broadcast in networks. *Random Structures and Algorithms*, 1(4):447–460, 1990.

[14] A.M. Frieze and G.R. Grimmett. The shortest-path problem for graphs with random arc-lengths. *Discrete Applied Mathematics*, 10:57–77, 1985.

[15] L. Gasieniec and A. Pelc. Adaptive broadcasting with faulty nodes. *Parallel Computing*, 22:903–912, 1996.

[16] E.N. Gilbert. Random graphs. *The Annals of Mathematical Statistics*, 30:1141–1144, 1959.

[17] Gnutella. *The gnutella protocol specification v.0.4.*

[18] T. Hagerup and C. Rüb. A guided tour of Chernoff bounds. *Information Processing Letters*, 36(6):305–308, 1990.

[19] S. Jagannathan, G. Pandurangan, and S. Srinivasan. Query protocols for highly resilient peer-to-peer networks. In *Proc. of ISCA PDCS'06*, pages 247–252, 2006.

[20] R. Karp, C. Schindelhauer, S. Shenker, and B. Vöcking. Randomized rumor spreading. In *Proc. of FOCS'00*, pages 565–574, 2000.

[21] C. Law and K.-Y. Siu. Distributed construction of random expander networks. In *Proc. of INFOCOM'03*, pages 2133–2143, 2003.

[22] T. Leighton, B. Maggs, and R. Sitamaran. On the fault tolerance of some popular bounded-degree networks. In *Proc. of FOCS'92*, pages 542–552, 1992.

[23] P. Mahlmann and C. Schindelhauer. Distributed random digraph transformations for peer-to-peer networks. In *Proc. of SPAA'06*, pages 308–317, 2006.

[24] B.D. McKay and N.C. Wormald. Asymptotic enumeration by degree sequence of graphs with degrees o(sqrt(n)). *Combinatorica*, 11:369–382, 1991.

[25] M. Mitzenmacher. *The Power of Two Choices in Randomized Load Balancing*. PhD thesis, University of California at Berkeley, 1996.

[26] B. Pittel. On spreading rumor. *SIAM Journal on Applied Mathematics*, 47(1):213–223, 1987.

[27] N.C. Wormald. Models of random regular graphs. *Surveys in Combinatorics*, 276:293–298, 1999.