Report from Dagstuhl Seminar 13042

Epidemic Algorithms and Processes: From Theory to Applications

Edited by

Benjamin Doerr[1], Robert Elsässer[2], and Pierre Fraigniaud[3]

1 **MPI für Informatik – Saarbrücken, DE**
2 **Universität Salzburg, AT,** robert.elsaesser@sbg.ac.at
3 **University Paris-Diderot, FR,** pierre.fraigniaud@liafa.univ-paris-diderot.fr

Abstract

This report documents the program and the outcomes of Dagstuhl Seminar 13042 "Epidemic Algorithms and Processes: From Theory to Applications", which took place from January 20 to 25, 2013 at Schloss Dagstuhl – Leibniz Center for Informatics. Several research topics were covered by the seminar participants, including scientists working in Theoretical Computer Science, as well as researchers from the more practical area of Computer Systems. Most of the participants presented their recent results on the topic of the seminar, as well as some challenging new directions and open problems. The presentations contained a description of the main research area for a wide audience. During the seminar, ample time was reserved for informal discussions between participants working on different topics. In our executive summary, we describe the main field of the seminar, as well as our goals in general. Then, we present the abstracts of the presentations given during the seminar.

Seminar 20.–25. January, 2013 – www.dagstuhl.de/13042
1998 ACM Subject Classification C.2.1 Network Architecture and Design – Network communications, C.2.4 Distributed Systems – Distributed applications, F.2.2 Nonnumerical Algorithms and Problems – Computations on discrete structures / Geometrical problems and computations, G.2.2 Graph Theory – Graph algorithms
Keywords and phrases Message dissemination, Epidemic spreading, Dynamic spreading processes
Digital Object Identifier 10.4230/DagRep.3.1.94
Edited in cooperation with Adrian Ogierman

1 Executive Summary

Benjamin Doerr
Robert Elsässer
Pierre Fraigniaud

The Dagstuhl seminar 13042 "Epidemic Algorithms and Processes: From Theory to Applications" took place from January 20 to 25, 2013, and the main goal of the seminar was to fertilize interaction between theory and applications in this emerging research area. Especially in the algorithmic community several fundamentally new ideas have been developed in recent years. At our Dagstuhl seminar, we explored them further, by mixing various ideas coming from experts working on different fields. Theoretical computer scientists presented their results and methods, in order to disseminate them to a wider community. Researchers from application areas presented their current findings and new challenging research directions, in order to influence (theoretical) research toward real-world applications. The interaction between the seminar participants led to ample discussions and further research collaborations between different domains.

Epidemic algorithms provide a powerful paradigm for distributed computing. Some of the most interesting application areas are the efficient dissemination of updates in replicated data-bases, as well as data dissemination in peer-to-peer systems or wireless sensor networks. By contacting random neighbors in parallel, and making them join forces, an epidemic like progress can be achieved. Furthermore, epidemic processes inherently possess a high level of simplicity and robustness, and therefore the corresponding algorithms can easily deal with the dynamically changing structure of the networks mentioned before.

Theoretical Computer Science makes these useful observations precise and provides certain performance guarantees. One of the well-known algorithms is the so called *randomized rumor spreading*, which disseminates a piece of information in a network to all nodes in a number of communication rounds. In the corresponding communication model, in each round every informed node (i.e, a node which possesses the message) passes/retrieves the information to/from a randomly chosen neighbor. Since 2008, epidemic algorithms received an increased attention by the theory community, leading to a series of new developments such as the development of new analysis techniques for e.g. the bit-complexity of random phone call algorithms, flooding protocols for dynamic graphs, or relating the performance of an epidemic algorithm to the conductance of the network. On the other side, new algorithm design principles have been introduced, which allow the nodes to remember (and avoid) a certain number of previously contacted neighbors, or the use of intentionally dependent randomized decisions. The first modification resulted in an exponential improvement in the number of message transmissions, and lead to the remarkable result that in social networks information can be spread in sublogarithmic time. The second idea gave rise to a number of high-quality papers ranging from, e.g., a theoretical analysis of the amount of randomness needed to the design of the first epidemic rumor spreading algorithm having a safe termination criterion.

One of the main goals of the seminar was to intensify the collaboration between theory and application fields on epidemic algorithms and processes. We mainly concentrated on two major applications. The first one focuses on the construction and maintenance of peer-to-peer networks in a highly dynamic scenario. Since the epidemic algorithms described above are scalable, robust against edge or node failures, and only require a small amount of message transmissions, they can successfully deal with the challenges imposed in a peer-to-peer environment.

The second focus was on the generation of personalized connections in social networks by using epidemic algorithms. Personalization is applied to fundamental processes such as dissemination, search, and navigation, in order to improve the benefits of social networking. The generated views give rise to certain clusters within the network, and the gossip algorithm for communicating profiles and broadcasting messages distinguishes then between intra-cluster and inter-cluster connections.

2 Table of Contents

3 Overview of Talks

3.1 From Caesar to Twitter: On the Elites of Social Networks

Chen Avin (Ben Gurion University – Beer Sheva, IL)

Joint work of Avin, Chen; Lotker, Zvi; Pignolet, Yvonne-Anne; Turkel, Itzik
Main reference C. Avin, Z. Lotker, Y.-A. Pignolet, I.Turkel, "From Caesar to Twitter: An Axiomatic Approach to Elites of Social Networks," arXiv:1111.3374v3 [cs.SI].
URL http://arxiv.org/abs/1111.3374v3

In many societies there is an *elite*, a relatively small group of powerful individuals that is well connected and highly influential. Since the ancient days of Julius Caesar's senate to the recent days of celebrities on Twitter, the size of the elite is a result of conflicting social forces competing to increase or decrease it. In this paper we formulate these forces as axioms and study their equilibrium and other properties of elites in social networks and complex systems.

Our findings indicate that elite properties such as a *size* of $\Theta(\sqrt{m})$ (where m is the number of edges in the network), disproportionate *influence*, *stability* and *density* are universal and should join an increasing list of common phenomenon that complex systems share such: "small world", power law degree distributions, high clustering, etc. As an approximation for the elite we study the subgraph formed by the highest degree nodes, also known as the rich-club. We analyze the structural properties of the k-rich-club of nine existing complex networks and three theoretical models systematically, where the k-rich-club is the subgraph induced by the k nodes with the highest degree in the network. In all real-life networks we observe similar elite properties for rich-clubs consisting of around $\sqrt{m}$ nodes, however, none of the theoretical models we analyzed captures all the elite properties, and thus they should be either adjusted or extended to address these findings.

3.2 Tight Bounds for Connected Dominating Set Packings, Distributed Construction, and Applications

Keren Censor-Hillel (MIT – Cambridge, US)

Joint work of Censor-Hillel, Keren; Ghaffari, Mohsen; Kuhn, Fabian

We study the connected dominating set (CDS) packing and the closely related connected domatic partition (CDS-Partition) problems. The CDS-Partition problem asks for partitioning the nodes of a graph into as many vertex-disjoint connected dominated sets as possible. CDS-Packing is the fractional relaxation of CDS-Partition, where nodes can be in several CDSs and we aim to maximize the ratio between the total number of CDSs and the maximum number of CDSs that contain any node. The size of any CDS-Packing or CDS-Partition is upper bounded by the vertex connectivity k of the graph. Our main result is an efficient distributed algorithm that constructs a CDS-Packing of size $\Omega(k/\log(n))$. We show that there are graphs on which no better CDS-Packing exists. For the CDS-Partition problem, we describe a fully-random algorithm that does not require any communication between the nodes and which constructs a CDS-Partition of size $\Omega(\sqrt(k)/\log(n))$, and we give an efficient distributed algorithm that constructs a CDS-Partition of size $\Omega(k/\log^2(n))$ if $k = \Omega(\sqrt(n))$.

As a prime application of our results, we obtain efficient distributed algorithms to construct high-throughput communication backbones for store-and-forward broadcast algorithms. In particular, the CDS-Packing algorithm allows to construct a communication backbone for store-and-forward algorithms with throughput $Omega(k/\log(n))$, which we prove to be optimal. This result also implies that the network coding advantage for simultaneously broadcasting messages – the ratio between the throughput achievable with and without network coding – is a tight $\Theta(\log n)$. As a by-product, we also get an efficient distributed algorithm for approximating the vertex connectivity of a graph, and we identify almost optimal connections between the vertex-connectivity of a graph and its resilience to remain connected in the presence of random node failures.

3.3 Fast Fault Tolerant Rumor Spreading with Minimum Message Complexity

Carola Doerr (MPI für Informatik – Saarbrücken, DE)

Joint work of Doerr, Benjamin; Doerr, Carola; Moran, Shay; Moran, Shlomo
Main reference B. Doerr, S. Moran, S. Moran, C. Winzen, "Fast Fault Tolerant Rumor Spreading with Minimum Message Complexity," arXiv:1209.6158v3 [cs.DS].
URL http://arxiv.org/abs/1209.6158v3

An approach for dissemination in complete networks different from randomized rumor spreading that naturally leads to a simple termination criterion is the *workload splitting* algorithm proposed by Gasieniec and Pelc (Parallel Computing 22:903–912, 1996).

It is based on the following simple idea: Each node, when called, receives a list of other nodes that he has to ensure being called. For the initially informed node, this list consists of all other nodes. A node with such a non-empty workload list calls one node of the list, sends the rumor to it, and also moves half of the own workload list to the new node. This easily obtains the optimal dissemination time of $\lceil \log_2 n \rceil$.

The problem with this approach is that it is not very robust against node failures. The approach taken by Gasieniec and Pelc is that a node repeats calling nodes from its list until successful, and then again splits the remaining workload into equal pieces. This may, though, lead to a dissemination time of $\lceil \log_2(n-k) \rceil + k$ when k nodes do not cooperate.

We first show that this estimate is far to pessimistic when we can assume that the failed nodes are distributed randomly. We then obtain a logarithmic dissemination time even for a constant fraction of failed nodes.

This can easily be used to obtain a good protocol also against adversarial node failure: The initial node simply starts the protocol of Gasieniec and Pelc, however, with randomly permuted node identifiers. The price for this approach is that the random permutation also has to be communicated to all nodes, increasing the maximum message size to linear. We then show how to overcome this short-coming by reducing the number of available permutations from $n!$ to polynomial, thus allowing to transmit the permutation with a logarithmic number of bits.

3.4 Epidemic Algorithms: A “Systems” Perspective

Pascal Felber (Université de Neuchâtel, CH)

Joint work of Felber, Pascal; Kermarrec, Anne-Marie; Leonini, Lorenzo; Rivière, Etienne ; Voulgaris, Spyros
Main reference P. Felber, A.-M. Kermarrec, L. Leonini, E. Rivière, S. Voulgaris, “Pulp: An adaptive gossip-based dissemination protocol for multi-source message streams,” Peer-to-Peer Networking and Applications, Vol. 5, Issue 1, pp. 74–91, 2012.
URL http://dx.doi.org/10.1007/s12083-011-0110-x

Epidemic protocols are attractive from a theoretical perspective because of their algorithmic simplicity (typically easy to model, prove correct, study). They are also attractive from a “systems” perspective because they are robust and scalable. They just work in real systems! This talk gives an overview of some classical epidemic algorithms and presents a pragmatic design for a push-pull dissemination protocol that performs efficiently in large-scale networks.

3.5 WhatsUp: a P2P instant news item recommender

Davide Frey (INRIA Bretagne Atlantique – Rennes, FR)

WhatsUp [1] is a collaborative-filtering system for disseminating news items in a large-scale dynamic setting with no central authority. It relies on three layered gossip protocols. The lowest two layers build on overlay network that clusters users with similar opinions on the news items they receive. The top-level protocol uses this overlay to disseminate news items to interested users.

The lowest layer in the architecture is a random peer sampling protocol [2]. It gossips information about other nodes in the network and provides each node with a continuously changing random sample of the network. The middle layer also gossips information about other network nodes, but it aims at clustering nodes that have similar interests. These two protocols provide the basis for BEEP, the top-layer protocol in WhatsUp’s architecture. BEEP is a heterogeneous epidemic dissemination protocol. Unlike the other two protocols, it exchanges news items. In doing so, it (1) biases the orientation of its targets towards those with similar interests, and (2) amplifies dissemination based on the level of interest in each news item.

WhatsUp outperforms various alternatives in terms of accurate and complete delivery of relevant news items while preserving the fundamental advantages of standard gossip: namely simplicity of deployment and robustness. Nonetheless, the fact that it is based on the combination of three protocols makes it difficult to analyze. The interaction among the protocols is in fact bidirectional. The top-layer dissemination protocol depends on the two overlay protocols. Yet, its dissemination choices also influence the overlay by determining what items will reach which users. An interesting direction for future research will consist in building models that will describe its behavior and provide insight in tuning its operation.

References

1 A. Boutet, D. Frey, R. Guerraoui, A. Jégou, A.-M. Kermarrec (2013). WhatsUp Decentralized Instant News Recommender. IPDPS 2013. Retrieved from http://hal.inria.fr/hal-00769291
2 M. Jelasity, S. Voulgaris, R. Guerraoui, A.-M. Kermarrec, M. van Steen. 2007. Gossip-based peer sampling. ACM Trans. Comput. Syst. 25, 3, Article 8 (August 2007).

3.6 Gossiping Efficiently in an Asynchronous World

Chryssis Georgiou (University of Cyprus, CY)

Joint work of Georgiou, Chryssis; Gilbert, Seth; Guerraoui, Rachid; Kowalski, Dariusz
Main reference C. Georgiou, S. Gilbert, R. Guerraoui, D.R. Kowalski, "Asynchronous Gossip," Journal of the ACM, Vol. 60, Issue 2, 2013.
URL http://www.cs.ucy.ac.cy/~chryssis/pubs.html

We consider the complexity of epidemic rumor spreading in an asynchronous, message-passing fault-prone distributed system. The underlining philosophy of this work is "to design for the best and hope for the best". That is, the objective is to design rumor spreading algorithms that do not rely on any information on the network's message delay or the relative processes' speeds, but be efficient when such timing bounds indeed hold.

Under this setting, we show that an adaptive adversary can significantly hamper the spreading of a rumor, while an oblivious adversary cannot. Under the latter adversarial type we devise efficient asynchronous epidemic gossip algorithms, and show that when applied as a building block, they can improve the complexity of asynchronous randomized consensus.

3.7 Tight Bounds for Rumor Spreading with Vertex Expansion

George Giakkoupis (INRIA – Rennes, FR)

Main reference G. Giakkoupis, "Tight Bounds for Rumor Spreading with Vertex Expansion," arXiv:1302.6243v1 [cs.DM].
URL http://arxiv.org/abs/1302.6243v1

We establish a bound for the classic Push-Pull rumor spreading protocol on arbitrary graphs, in terms of the vertex expansion of the graph. We show that $\mathcal{O}(\log^2(n)/\alpha)$ rounds suffice with high probability to spread a rumor from a single node to all n nodes, in any graph with vertex expansion at least alpha. This bound matches a known lower bound, and settles the question on the relationship between rumor spreading and vertex expansion asked by Chierichetti, Lattanzi, and Panconesi (SODA 2010). Further, some of the arguments used in the proof may be of independent interest, as they give new insights, for example, on how to choose a small set of nodes in which to plant the rumor initially, to guarantee fast rumor spreading.

3.8 How To Gossip (Multiple Messages)

Bernard Haeupler (MIT – Cambridge, US)

Main reference B. Haeupler, "Simple, Fast and Deterministic Gossip and Rumor Spreading," in Proc. of the 24th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA'13), pp. 705–716, SIAM, 2013.
URL http://knowledgecenter.siam.org/0236-000055/

Gossip algorithms have recently gained attention as a powerful approach for achieving robust and message efficient multicast communication. This talk presents several ideas to improve the efficiency and applicability of these algorithms.

In particular, we provide the first gossip protocol whose efficiency does not rely on expansion properties of the network but which instead performs well on any topology. We also give a novel analysis that shows that a wide variety of natural gossip processes very robustly achieve the same (or even better efficiency) without using any randomization. The existence of such protocols is somewhat surprising because conventional wisdom suggested that both robustness and the efficient information dispersion of gossip protocols stem from their use of randomness.

We also show how combining gossip protocols with network coding can drastically improve the throughput in settings where the amount of data to be multicast is much larger than what can be transmitted in one round. While the idea of using network coded gossip is not new analyzing its performance turned out to be very challenging even in the simplest setting. We introduce projection analysis, as a very simple and powerful technique for providing sharp convergence times in all settings considered in the literature. Beyond this we demonstrate how the projection analysis directly extends to highly dynamic networks.

References

1 B. Haeupler, Analyzing network coding gossip made easy, in Proc. of 43rd ACM Symposium on Theory of Computing (STOC'11), pp. 293-302, ACM, 2011. http://dx.doi.org/10.1145/1993636.1993676

2 B. Haeupler, Simple, Fast and Deterministic Gossip and Rumor Spreading, in Proc. of the 24th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA'13), pp. 705–716, SIAM, 2013. http://knowledgecenter.siam.org/0236-000055/

3.9 Local Algorithms and Large Graph Analysis

Silvio Lattanzi (Google – New York, US)

Joint work of Lattanzi, Silvio; Kiveris, Raimondas; Korula, Nitish; Mirrokni, Vahab; Alvisi, Lorenzo; Clement, Allen; Epasto, Alessandro; Panconesi, Alessandro

The analysis of very large graph is a central problem in computer science. In this talk we analyze this area of research from a practical prospective. We first describe general problems and directions arising from real world problems then we focus on developing solutions for them using local algorithms.

The first problem that we consider is a security problem in social network. In this context we show how truncated random walk techniques can be used to rescue a social network under sybil attack.

Then we consider a reconciliation problem between two social networks. In this problem we assume to have two social networks and our goal is to map the same user across them. In this setting we show that for several social network model if an initial set of mapping is available it is possible to map almost all the nodes in the network using a simple local algorithm.

3.10 Computing Radius and Diameter of Real World Huge Graphs

Andrea Marino (University of Florence, IT)

Joint work of Crescenzi, Pierluigi; Grossi, Roberto; Habib, Michel; Lanzi, Leonardo; Marino, Andrea
Main reference P. Crescenzi, R. Grossi, M. Habib, L. Lanzi, A. Marino, "On computing the diameter of real-world undirected graphs," Theoretical Computer Science, corrected proof, 2012.
URL http://dx.doi.org/10.1016/j.tcs.2012.09.018

The diameter of a graph is the maximum eccentricity among all its nodes, where the eccentricity of a node x is the distance from x to its farthest node and the distance from x to y is the number of edges contained in the shortest path from x to y.

In the context of real-world networks, the textbook method based on performing a breadth-first search from every node of the graph, requires a prohibitive cost of $\mathcal{O}(nm)$ time, where n is the number of nodes and m is the number of edges of the graph: indeed, it is not rare that a real-world graph contains several millions of nodes and several millions of edges. Even more efficient theoretical methods turn out to be too much time consuming.

We have shown a new algorithm for computing the diameter of directed (or undirected) weighted (or unweighted) graphs. Our algorithm dynamically refines a lower and upper bound of the diameter by analysing the eccentricity of the nodes in a specified "good" order. Although its worst-case complexity is $\mathcal{O}(nm)$ time, we have experimentally shown that our algorithm works in $\mathcal{O}(m)$ time in practice, requiring few breadth-first searches to complete its task.

By applying the same approach, we have shown that it is possible to compute efficiently also the radius, that is the minimum eccentricity of the nodes of a graph.

3.11 Towards Truly Distributed Matrix Computations

Gerhard Niederbrucker (Universität Wien, AT)

Joint work of Niederbrucker, Gerhard; Straková, Hana; Gansterer, Wilfried N.

Numerical linear algebra kernels are fundamental for computational science. Traditionally, algorithms for matrix computations are studied on reliable parallel systems. In contrast to that, we investigate whether or not we can provide such kernels also on unreliable decentralized distributed systems, like sensor networks or peer-to-peer systems. Moreover, future high performance computing systems are expected to be more distributed than parallel in their nature and hence, it is further expected that fault tolerance already at the algorithmic level will become a necessity.

To address the rising need for fault tolerance at the algorithmic level, we investigate the potential of gossip-based algorithms to robustly provide core computational primitives, e.g., distributed summations. While most existing gossip-based approaches are highly flexible and efficient, a single failure in the system in general immediately translates to wrong results. Concerning this issue, we present a technique which allows for deriving fault tolerant variants of a variety of known algorithms which naturally tolerate a wide range of possible system failures.

3.12 Epidemics in Urban Environments – A Virus' Tale

Adrian Ogierman (Universität Paderborn, DE)

Joint work of Ogierman, Adrian; Elsässer, Robert

We consider a dynamic epidemic process in a certain urban environment. The epidemic is spread among n agents, which move from one location to another according (mostly) to a power law distribution. If two agents meet at some spot, a possible infection may be transmitted from one agent to the other.

For the theoretical part, we analyze two different scenarios. We show that at least a small number of agents remains uninfected and the epidemic is stopped after a logarithmic number of rounds. Then, by adding some countermeasures, the epidemic is stopped after $(\log \log n)^{\mathcal{O}(1)}$ steps affecting at most a polylogarithmic number of agents.

For the experimental part, we compare our model to real world data provided by the RKI. Additionally, we empirically analyze the effects of certain countermeasures as applied in the US against the Influenza Pandemic in 1918–1919. Based on our empirical tests, we show that by utilizing the right parameters – some of them being obtained from real world observations – one can efficiently approximate the course of a disease in real world.

3.13 Rumor Spreading in Models of Social Networks

Konstantinos Panagiotou (LMU München, DE)

Joint work of Fountoulakis. Nikolaos; Panagiotou, Konstantinos; Sauerwald, Thomas
Main reference N. Fountoulakis, K. Panagiotou, T. Sauerwald, "Ultra-fast rumor spreading in social networks," in Proc. of the 23rd Annual ACM-SIAM Symp. on Discrete Algorithms (SODA '12), pp. 1642–1660, SIAM, 2012.
URL http://dl.acm.org/citation.cfm?id=2095246

We analyze the popular push-pull protocol for spreading a rumor in networks. Initially, a single node knows of a rumor. In each succeeding round, every node chooses a random neighbor, and the two nodes share the rumor if one of them is already aware of it. We present the first theoretical analysis of this protocol on random graphs that have a power law degree distribution with an arbitrary exponent $\beta > 2$.

Our main findings reveal a striking dichotomy in the performance of the protocol that depends on the exponent of the power law. More specifically, we show that if $2 < \beta < 3$, then the rumor spreads to almost all nodes in $\mathcal{O}(\log \log n)$ rounds with high probability. On the other hand, if $\beta > 3$, then $\mathcal{O}(\log n)$ rounds are necessary.

We also investigate the asynchronous version of the push-pull protocol, where the nodes do not operate in rounds, but exchange information according to a Poisson process with rate 1. Surprisingly, we are able to show that, if $2 < \beta < 3$, the rumor spreads even in constant time, which is much smaller than the typical distance of two nodes.

3.14 Rumor Spreading in Random Evolving Graphs

Francesco Pasquale (University of Rome "La Sapienza", IT)

Joint work of Clementi, Andrea; Crescenzi, Pierluigi; Doerr, Carola; Fraigniaud, Pierre; Isopi, Marco; Pasquale, Francesco; Panconesi, Alessandro; Silvestri, Riccardo
Main reference A. Clementi, P. Crescenzi, C. Doerr, P. Fraigniaud, M. Isopi, A. Panconesi, F. Pasquale, R. Silvestri, "Rumor Spreading in Random Evolving Graphs," arXiv:1302.3828v1 [cs.DM].
URL http://arxiv.org/abs/1302.3828v1

Randomized gossip is one of the most popular way of disseminating information in large scale networks. This method is appreciated for its simplicity, robustness, and efficiency. In the "Push" protocol, every informed node selects, at every time step (a.k.a. round), one of its neighboring node uniformly at random and forwards the information to this node. This protocol is known to complete information spreading in $\mathcal{O}(\log n)$ time steps with high probability (w.h.p.) in several families of n-node "static" networks. The Push protocol has also been empirically shown to perform well in practice, and, specifically, to be robust against dynamic topological changes.

We analyze the Push protocol in "dynamic" networks. We consider the "edge-Markovian" evolving graph model which captures natural temporal dependencies between the structure of the network at time t, and the one at time $t+1$. Precisely, a non-edge appears with probability p, while an existing edge dies with probability q. In order to fit with real-world traces, we mostly concentrate our study on the case where $p = \Omega(\frac{1}{n})$ and q is constant. We prove that, in this realistic scenario, the Push protocol does perform well, completing information spreading in $\mathcal{O}(\log n)$ time steps w.h.p. Note that this performance holds even when the network is, w.h.p., disconnected at every time step (e.g., when $p \ll \frac{\log n}{n}$). Our result provides the first formal argument demonstrating the robustness of the Push protocol against network changes. We also address other ranges of parameters p and q (e.g., $p + q = 1$ with arbitrary p and q, and $p = \frac{1}{n}$ with arbitrary q). Although they do not precisely fit with the measures performed on real-world traces, they can be of independent interest for other settings. The results in these cases confirm the positive impact of dynamism.

3.15 From Unstructured to Structure Epidemics: Past and Future Work

Luis Rodrigues (Technical University – Lisboa, PT)

Joint work of Rodrigues, Luis; Leitao, Joao; Ferreira, Mario; Branco, Miguel

We illustrate some of our research that aims at optimizing practical epidemic information dissemination protocols using different approaches to add structured to an otherwise unstructured dissemination process. Two approaches are illustrated: embedding trees and biasing gossip.

The embedded approach is illustrated with Thicket. One way to efficiently disseminate information in a P2P overlay is to rely on a spanning tree. However, in a tree, interior nodes support a much higher load than leaf nodes. Also, the failure of a single node can break the tree, impairing the reliability of the dissemination protocol. These problems can be addressed by using multiple trees, such that each node is interior in just a few trees and a leaf node in the remaining; the multiple trees approach allows to achieve load distribution and also to send redundant information for fault-tolerance. Thicket is a decentralized algorithm to efficiently build and maintain such multiple trees over a single unstructured overlay network.

The biasing approach is illustrated with BoundedGossip. Gossip-based protocols are very robust and are able to distribute the load uniformly among all nodes. Furthermore, gossip-protocols circumvent the oscillatory phenomena that are known to occur with other forms of reliable multicast. As a result, they are excellent candidates to support the dissemination of information in large-scale datacenters. However, in this context, topology oblivious approaches may easily saturate the switches in the highest level of the datacenter network fabric. BoundedGossip provides an adequate load distribution among the different layers of the switching fabric of the datacenter, avoiding being a source of network bottlenecks.

We also provide some brief overview of our future research directions.

This work was partially supported by FCT – Fundacao para a Ciencia e a Tecnologia under the projects PEst-OE/EEI/LA0021/2011 and HCPI under the grant PTDC/EIA-EIA/102212/2008.

References

1 M. Branco, J. Leitão, L. Rodrigues. Bounded Gossip: A Gossip Protocol for Large-Scale Datacenters. In *Proceedings of the 28th Symposium On Applied Computing (SAC 2013)*, Coimbra, Portugal. March 1013.
2 Leitão, J. Pereira and L. Rodrigues. HyParView: a membership protocol for reliable gossip-based broadcast. In *Proceedings of the 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, Edinburgh, UK, June, 2007.
3 M. Ferreira, J. Leitão, and L. Rodrigues. Thicket: A Protocol for Building and Maintaining Multiple Trees in a P2P Overlay. In *Proceedings of the 29th IEEE Symposium on Reliable Distributed Systems (SRDS)*, New Delhi, India, 31 October–3 November 2010.

3.16 Revealing Epidemic Processes: On the Detection of Peer-to-peer Botnets

Stefan Ruehrup (FZ Telekommunikation Wien, AT)

Joint work of Ruehrup, Stefan; Urbano, Pierfrancesco; Berger, Andreas; D'Alconzo, Alessandro
Main reference S. Ruehrup, P. Urbano, A. Berger, A. D'Alconzo, "Botnet detection revisited: theory and practice of finding malicious P2P networks via Internet connection graphs," 5th IEEE International Traffic Monitoring and Analysis Workshop (TMA'13), 2013.

Structured peer-to-peer networks are designed such that information can be spread fast in the network. Their communication structure often emerges from some kind of epidemic process. Since peer-to-peer networks have been used as command and control structures for botnets (networks of malicious software), it is important for network operators to reveal such structures. For this analysis, network traffic can be represented by a Traffic Dispersion Graph, which contains IP addresses as nodes and edges whenever at least one IP packet is exchanged between the respective hosts. The start point for detection is an infected host, which is trapped by a honeypot in the operator's network. Then the rest of the botnet is most likely connected to this start node.

In theory, structured peer-to-peer networks form dense communities, which can be separated from legitimate background traffic by using community detection methods such as the Louvain method. Our experiments on real DSL network traces show that traffic dispersion graphs of legitimate traffic often contain densely connected components, which makes separation from malicious peer-to-peer traffic difficult. An alternative is to target the neighborhood of known bots. The comparison of such approaches on real network traces show that a local graph search starting from known bots can reveal members of a Kademlia botnet efficiently, where a separation by high degree, betweenness or page rank alone gives non-satisfactory recall factors.

3.17 Discrete Load Balancing on Arbitrary Network Topologies

Thomas Sauerwald (MPI für Informatik – Saarbrücken, DE)

Joint work of Sauerwald, Thomas; Sun, He
Main reference T. Sauerwald, H. Sun, "Tight Bounds for Randomized Load Balancing on Arbitrary Network Topologies," in Proc. of the 53rd Annual IEEE Symp. on Foundations of Computer Science (FOCS'12), pp. 341–350, IEEE CS, 2012.
URL http://dx.doi.org/10.1109/FOCS.2012.86

We consider the problem of balancing load items (tokens) on networks. Starting with an arbitrary load distribution, we allow in each round nodes to exchange tokens with their neighbors. The goal is to obtain a distribution where all nodes have the same number of tokens. For the continuous case where tokens are arbitrarily divisible, most load balancing schemes correspond to Markov chains whose convergence is fairly well-understood in terms of their spectral gap.

However, in many applications load items cannot be divided arbitrarily often and we need to deal with the discrete case where load is composed of indivisible tokens. In this talk we investigate a natural randomized protocol and demonstrate that there is almost no difference between the discrete and continuous case. Specifically, we show that for any regular network, all nodes have the same number of tokens up to an additive constant in the same number of rounds as in the continuous case.

3.18 From Push&Pull to Pointer Push&Pull

Christian Schindelhauer (Universität Freiburg, DE)

Main reference T. Janson, P. Mahlmann, C. Schindelhauer, "A Self-Stabilizing Locality-Aware Peer-to-Peer Network Combining Random Networks, Search Trees, and DHTs," in Proc. of the 16th Int'l Conf. on Parallel and Distributed Systems (ICPADS'10), pp. 123–130, IEEE, 2010.
URL http://dx.doi.org/10.1109/ICPADS.2010.42

We revisit dynamic graph transformations for establishing low diameter, high expansion random d-regular connected graphs. After presenting some connected areas like Pointer-Jumping in PRAMs and Hot Link Assignment we present the two open questions about the Mixing Time of the Flipper operation and the Pointer- Push&Pull operation.

We survey some recent publications and conclude with the demonstration of Pointer-Push&Pull operations inside an existing Peer-to-Peer network.

3.19 Randomness-Efficient Information Spreading

He Sun (MPI für Informatik – Saarbrücken, DE)

Joint work of Sun, He; Guo, Zeyu

We study the classical rumor spreading problem, which is used to spread information in an unknown network with n nodes. We present the first push-based protocol on a complete graph G of n nodes such that, by using $\mathcal{O}(\log n \log\log n)$ random bits, every node gets informed in $\mathcal{O}(\log n)$ rounds with high probability. Both of runtime and randomness complexity are known to be almost tight. Moreover, for several graph topologies our protocols are as fast as the classical protocol and use $\tilde{O}(\log n)$ random bits in total, in contrast to $\mathcal{O}(n \log^2 n)$ random bits used in the classical rumor spreading protocol. These results together give us almost full understanding of the randomness requirement for this basic epidemic process.

3.20 Gossip Protocols for Renaming and Sorting

Philipp Woelfel (University of Calgary, CA)

Joint work of Giakkoupis, George; Woelfel, Philipp

Gossip protocols have emerged as an important communication paradigm for large networks of distributed systems, such as sensor, peer-to-peer, or mobile ad-hoc networks. In these protocols, every node contacts only a few random nodes in each round and exchanges a small amount of information with them. Such protocols are attractive because they offer reasonable performance and at the same time are simple, scalable, and fault-tolerant, and decentralized. Often, they are designed so that nodes need only little computational power and a small amount of storage space.

In this talk I describe efficient gossip-based algorithms for some fundamental distributed tasks. In every round of these protocols, each of the n nodes exchanges information of size $\mathcal{O}(\log n)$ bits with (at most) one other randomly chosen peer. We first consider the *renaming* problem, that is, to assign distinct IDs from a small name space to all nodes of the network. We propose a simple gossip protocol with logarithmic round complexity and name space $\{1, ..., (1+\epsilon)n\}$, for any fixed $\epsilon > 0$. Then we solve the *tight* renaming problem, where each node obtains a unique ID in $\{1, ..., n\}$, in $\mathcal{O}(\log^2 n)$ rounds.

Next we study the following *sorting* problem: Nodes have consecutive IDs 1 up to n, and they receive numbers as inputs. They then have to exchange those inputs so that in the end the input of rank k is located at the node with ID k. Jelasity and Kermarrec (2006) suggested a simple and natural protocol, where nodes exchange keys with peers chosen uniformly at random, but it is not hard to see that this protocol requires $\omega(n)$ rounds. We prove that the same protocol works in $\mathcal{O}(\log^2 n)$ rounds if peers are chosen according to a non-uniform power law distribution.

3.21 Flooding in Dynamic Graphs with Arbitrary Degree Sequence

Pierluigi Crescenzi (University of Florence, IT)

Joint work of Fraigniaud, Pierre; Baumann, Hervé

In this talk we address the flooding problem in dynamic graphs, where flooding is the basic mechanism in which every node becoming aware of an information at step t forwards this information to all its neighbors at all forthcoming steps $t' > t$. Dynamic graphs are modeled as a sequences of graphs $(G_0, G_1, G_2, \ldots)$ with the same node set $[n]$, such that G_t is drawn independently at random according to some random graph model $\mathcal{G}$, for every $t \geq 0$. The case of a sequence of Erdös-Renyi random graphs (i.e., $\mathcal{G} = \mathcal{G}_{n,p}$) has been extensively studied in the literature. In this talk, we consider a sequence of random graphs $(G_t)_{t\geq 0}$ where every G_t is drawn at random in $\mathcal{G}_{\mathbf{w}}$, the model of random graphs with given expected degree sequence $\mathbf{w}$. We show that our techniques developed in a previous paper, for analyzing flooding in a Markovian sequence of $\mathcal{G}_{n,p}$ graphs, is robust enough to be used also in the general case of $\mathcal{G}_{\mathbf{w}}$ whenever there is mutual independence between consecutive graphs in the sequence. In particular, in the case of power-law degree distributions with intercept α, and exponent β, we prove that flooding in a sequence of graphs drawn from $\mathcal{G}_{\alpha,\beta}$ takes a.s. $O(\log n)$ steps even if, a.s., none of the graphs in the sequence is connected, while in the case of graphs with an arbitrary degree sequence we can prove several bounds, which depend on some specific properties of the degree sequence itself. For instance, if this sequence is specially admissible, then the flooding completion time is bounded by $O(\log n(\frac{1}{\log(1+\tilde{d})} + \frac{1}{w_{\min}}))$, where $w_{\min}$ denotes the smallest value in the degree sequence, and $\tilde{d}$ is the second order average degree.

4 Open Problems

During the seminar two open problem sessions were organized, in which several participants presented open problems within the research topics of the seminar. One of these open problems is close to be solved due to a collaboration between the participants.

Participants

- Chen Avin
Ben Gurion University – Beer Sheva, IL
- Keren Censor-Hillel
MIT – Cambridge, US
- Pierluigi Crescenzi
University of Florence, IT
- Oksana Denysyuk
INESC-ID – Lisboa, PT
- Benjamin Doerr
MPI für Informatik – Saarbrücken, DE
- Carola Doerr
MPI für Informatik – Saarbrücken, DE
- Robert Elsässer
Universität Salzburg, AT
- Pascal Felber
Université de Neuchâtel, CH
- Pierre Fraigniaud
University Paris-Diderot, FR
- Davide Frey
INRIA Bretagne Atlantique – Rennes, FR
- Tobias Friedrich
Universität Jena, DE
- Chryssis Georgiou
University of Cyprus, CY
- George Giakkoupis
INRIA Bretagne Atlantique – Rennes, FR
- Bernard Haeupler
MIT, US
- Hovhannes A. Harutyunyan
Concordia Univ. – Montreal, CA
- Anna Huber
University of Durham, GB
- Amos Korman
LIAFA – Paris, FR
- Silvio Lattanzi
Google – New York, US
- Andrea Marino
University of Florence, IT
- Gerhard Niederbrucker
Universität Wien, AT
- Adrian Ogierman
Universität Paderborn, DE
- Konstantinos Panagiotou
LMU München, DE
- Alessandro Panconesi
University of Rome "La Sapienza", IT
- Francesco Pasquale
University of Rome "La Sapienza", IT
- Luis Rodrigues
Technical Univ. – Lisboa, PT
- Stefan Rührup
FZ Telekommunikation Wien, AT
- Thomas Sauerwald
MPI für Informatik – Saarbrücken, DE
- Christian Schindelhauer
Universität Freiburg, DE
- He Sun
MPI für Informatik – Saarbrücken, DE
- Philipp Woelfel
University of Calgary, CA