Decentralized Communication against Surveillance and Privacy Violation

Kalman Graffi

Abstract: The Internet is one of the main communication platforms of our society. In many countries, communication contents and patterns are surveilled aiming to identify, punish or block undesired ideas. I focus with my research on fully decentralized and secure communication platforms which cannot be surveilled or switched off, on Android-based wireless mesh networks which support local communication that do not pass through the Internet, as well as on concepts for Internet-based democracy. My contributions aim for a practical usability in form of prototypes and software provided to potential users.

ACM CCS: Networks → Network types → Overlay and other logical network structures

Keywords: Dynamic Overlay Networks, Opportunistic Networks, Scalable Internet-based Democracy.

1 Introduction

I consider freedom of speech as the most valuable achievement of mankind. If not censored, it allows people all over the world to express their feelings, their thoughts and most valuable: their knowledge. The Internet has become the predominating communication channel to exchange information and data. As technology improves, authorities increasingly feel the urge to monitor, censor or even prohibit communication via Internet as it allows information and ideologies to spread rapidly. Many countries are known for spying on the communication and data of their citizens. The publications of Edward Snowden have shown that also Western countries are affected. He showed that centrally and mainly in the USA hosted data is to be assumed to be easily readable by national agencies. Thus, communication needs to be encrypted. Further, we observe that several countries easily block the access to unliked communication platforms nation-wide, such as to Twitter in China. Thus, a communication needs to be free from any single point of failure, meaning it requires to be fully decentralized. Other countries, such as Libya early 2011 and Hong Kong in late 2014, have even switched of the Internet access in their country to suppress the freedom of speech. Thus, local communication should be preferred over communication through the Internet.

My research focus is on secure, robust and decentralized communication systems. Here, I consider autonomous agents, which independently and often selfishly interact to provide a function or service within the network they are part of. This research question I follow with my nine PhD students in three selected topic areas. International cooperations and scientific exchanges to Italy, India and the Arab world further strengthen these competencies.

1) In peer-to-peer (p2p) networks, nodes in the Internet join an overlay network and act in this as service consumer but also as provider, to host in cooperation with the other nodes interesting services. Challenges arise with regard to security, robustness and the quality of the service, as these demands should be provided purely through the interaction of the unreliable, heterogeneous and potentially malicious nodes in the overlay network. We research on adaptive and partitionable overlays, various storage concepts and distributed data structures, communication patterns and distributed, precise monitoring concepts, as well as application-specific concern. We integrate and evaluate our approaches in the p2p system simulator PeerfactSim.KOM and a prototypical p2p framework for social networks, named LibreSocial.

2) Besides the decentralized communication platforms for the Internet, we further explore decentralized mobile mesh networks in form of vehicular ad hoc networks as well as Android-based opportunistic networks, which allow spontaneous local connections to nodes close by. Challenges arise in terms of the limited time nodes have to interact. Through the mobility, communication opportunities come and go frequently and last only for a short time. We design delay-tolerant routing and

storage concepts in combination with more advances application-specific protocols and mechanisms to support the opportunistic nature of such interactions.

3) My research focus is completed with investigations of the interaction of users in large-scale online communities. In specific, we address the scalability and security of Internet-based mechanisms for deliberation, argumentation and voting. Challenges arise through the large number of potential participants, topics and arguments in democratic discussions. Our researched mechanisms allow participants to find relevant topics and to contribute to the discussion according to their time and knowledge available. Next, I describe these research fields in detail.

2 Dependable P2P Systems Engineering

Since a decade, I research on the quality and security of p2p networks with focus on the application scenario of online social networks and secure communication platforms. My research vision is to overcome the various challenges in building p2p systems and to create a fully decentralized and secure p2p framework for various application, such as social networks, with reliable and controllable service quality. While centralized architectures for today's social networks are technically mature, they bear risks for both users and providers. Users fear the misuse of their data by the provider, while the provider fears the high costs of hosting the service. Decentralized architectures, especially p2p architectures, promise to be intrinsically scalable and to address security concerns at a conceptual and general level. P2P mechanisms in literature up to now, however, do mostly address partial challenges but provide no guaranteed or controllable service quality, reliability and security for modern use cases altogether, such as for online social networks needed. Despite the strengths of the p2p technology, i.e. the scalability and the distribution of operational costs, the challenges are yet not solved sufficiently so that professional p2p applications merely exist.

One essential part of my work is the systems' engineering of a fully-decentralized p2p framework or middleware for distributed, secure, large-scale applications, such as social networks. We aim to harness the power of the end user devices, to tame the complexity of such pure p2p networks and to understand the interdependencies of various layered and interacting p2p protocols.

Here, I provided contributions in the following fields.

1. A p2p framework for online social networks, termed LibreSocial, has been created over the last years with the participation of more than 60 students, each contributing in average more than 6 months. LibreSocial has been presented in [15, 14, 9, 10] as well as on industry fairs such as CeBIT or Hannover Messe.
2. Within the kernel of the platform, essential p2p building blocks have been implemented. In [2, 18, 6, 3, 26, 16, 12], I presented overlay networks which connect the network nodes and provide essential functions such as routing and simple data storage and retrieval. In [2, 18], we optimize them for social interaction patterns, in [6, 3] for self-stabilizing which allow the correction of invalid network topologies. In [26, 16, 12], we investigate how to support quality requirements and load balancing in these networks.
3. Distributed data structures, such as lists, sets or arrays, support the needs of social applications better than simple data items. We investigate them in [20]. Further elements such as various communication concepts (unicast, multicast, publish/subscribe), security mechanisms, and application specific plugins have been further added to the p2p framework.
4. I provided mechanisms to monitor [13, 11, 24] the quality of dynamic, complex networks and presented approaches to implement autonomous control loops in these [17, 7, 21] to control and maintain the quality.
5. With regard to the security of p2p networks, I analyzed the potential threats and provided solutions to implement a distributed identity management, key infrastructure [14] as well as access controlled distributed data structures [20].
6. For the evaluation of p2p systems, I co-initiated the p2p systems simulator PeerfactSim.KOM in [23, 22] and continuously extended it in [8, 4, 5].

Challenges not only arise in the solution of individual functions for this framework, but also in the interaction of the various solutions, the overall quality management and the seamless security. All mechanisms have to balanced and integrated, and finely harmonized in order to provide an acceptable user experience.

The main aim of this attempt, which I follow with 3 PhD students, is to contribute in the field of dependable distributed systems engineering and to implement a secure, robust, reliable and appealing p2p framework for social networks. This is from my perspective of high relevance for various social interest groups, namely in the private sector, in corporate environments and also as coordination platform for political organizations, such as NGOs in oppressed countries.

3 Wireless Opportunistic Networking

Besides the strong focus on p2p technologies in my research scope, I am also very interested in the combination with mobile aspects. Here, I work with 4 PhD students in the research field of opportunistic and delay tolerant networks. Opportunistic networks are characterized by mobile nodes that wirelessly communicate to further nodes in their proximity in cases they meet by chance, i.e. opportunistically. As a connected path for routing from source to destination or from publishers to subscribers is not assumed and rarely given, nodes act in a store-carry-forward approach to transport messages and data elements. Applications for such networks are given in the interconnection of widely spread smartphones, in car-to-car networks as well as in smart sensor

networks. One of the research questions we follow is with regard to cross layer optimization in p2p and opportunistic networks. In specific, we elaborate the options on how to design and to apply decentralized data structures on mobile and delay tolerant networks. Distributed data structures that allow to store and retrieve information reliably in such mobile and unreliable environments are beneficial for the use case of vehicular networks and localized data synchronization approaches. Challenges arise through the heterogeneity of the nodes, the strong dynamics in the network and through the various types of user interaction on distributed data structures.

Reliability, quality of service and security play a vital role in opportunistic networks. How can we make sure, that through message passing, messages arrive reliably and quickly at their destination, without being dropped, modified or read by unauthorized nodes. Interesting challenges also arise with respect to the reachable quality through the heterogeneity of the user devices and the various use cases. We investigate how we can support the contact opportunities by adapting the signaling procedure in the connection phase and by researching routing protocols optimized for the most popular wireless mobile devices currently, namely Android phones.

In tight cooperation with the industry, an Android-based local data synchronization solution is researched and created which enables users to synchronize files across many devices in multihop environments without user interaction or access to the Internet. In a second step, we integrate and connect the purely decentralized, secure synchronization solution with the centralized data management of the legacy backend of the synchronization service. For Android-based opportunistic networks, we optimize in [25] the opportunistic connection between two nodes and quicken the connection setup time. In [1], we exemplary show how various applications in Android can be combined and mashed up. Finally in [19], we present our first prototype for secure, opportunistic networks based on Android systems.

4 Internet-based Democracy: Deliberation, Argumentation and Voting

In the context of the liberation of communication worldwide and the support of citizen engagement in democratic movements, we see Internet-based online participation as a key element. The Internet can connect people and can be a platform for crowd sourcing best ideas for the benefit of our societies. In ideal Internet-based democratic processes, namely the collection and evaluation of all relevant arguments and the identification and selection of a best considered approach, users are assumed to cooperate for a common good. As an example for this use case, recently approximately 700 members of the faculty for mathematics and natural sciences at the University of Düsseldorf deliberated and voted on new PhD regulations. Argumentation systems are hereby a tool that allow users to describe their ideas, arguments and facts and link these with either supporting or contradicting relations. Over time, all view points on a certain topic and proposal can be gathered and a decision can be made through voting. The implementation of this ideal faces several challenges, which are given through the scale, heterogeneity of the participants and the complexity of relevant topics on the one hand and the strict technical requirements on the other hand.

Questions arise one how to organize and display topics and arguments to allow a quick, adequate access for all participants matching their knowledge background. The scale of the discussion with potentially millions of participants and a similar number of proposals, arguments and opinions complicates a targeted access. How can users contribute with arguments, claims or facts best according to their knowledge status in a potentially very large argumentation map? How should the infrastructure for argumentation and voting be hosted to prove its security and the validity of the results?

With 2 PhD students I focus on two research questions in this field. First, we focus on the creation of a reliable and secure (decentralized) system architecture for online deliberation that is able to withstand attackers from inside and outside, who try to corrupt the process or results for various reasons. Second, we elaborate the options to access large scale argumentation maps and deliberation corpora ideally for each individual user. As the users are assumed to be very heterogeneous in terms of interest, values, time available and knowledge to contribute, thus the presentation should be filtered to best match their current interest, knowledge and time. In future, we aim to extend and apply our solutions in cooperation with our interdisciplinary partners, that allow to harness the wisdom of the crowd and to find and provide best accepted solutions in a most democratic manner.

5 Conclusions

Through the tremendous developments in networking the world grows closer. Communications over the Internet and mainly over centrally hosted communication services, such as Facebook or Twitter, are to be considered unsafe and surveilled. With my research, I aim to create an alternative p2p framework for social networks, which addresses security and controlled quality in a purely decentralized system. For mobile devices it seems beneficial to exchange data to close by nodes directly instead of using up the data plan and being easier to detect. An finally, we work on Internet-based tools for online deliberation, argumentation and voting. We believe, that even when our approaches will not be used directly, there are several groups on the world that benefit from our solutions, this idea motivates me.

Literature

[1] R. Ali and K. Graffi. SandMash: An Approach for Mashups Techniques on Smartphones. In *MobiWis '15: Proc. of the Int. Conf. on Mobile Web and Intelligent Information Systems*, pages 1–16, 2015.

[2] T. Amft, B. Guidi, K. Graffi, and L. Ricci. FRoDO: Friendly Routing over Dunbar-based Overlays. In *IEEE LCN '15: Proc. of the IEEE Int. Conf. on Local Computing Networks*, pages 1–9, 2015.

[3] M. Benter, M. Divband, S. Kniesburges, A. Koutsopoulos, and K. Graffi. Ca-Re-Chord: A Churn Resistant Self-stabilizing Chord Overlay Network. In *NetSys '13: Proc. of the Int. Conf. on Networked Systems*, 2013.

[4] M. Feldotto and K. Graffi. Comparative Evaluation of Peer-to-Peer Systems Using PeerfactSim.KOM. In *IEEE HPCS'13: Proc. of the Int. Conf. on High Performance Computing and Simulation*, 2013.

[5] M. Feldotto and K. Graffi. Systematic Evaluation of Peer-to-Peer Systems Using PeerfactSim.KOM. *Concurrency and Computation: Practice and Experience*, pages 1–27, 2015.

[6] M. Feldotto, C. Scheideler, and K. Graffi. HSkip+: A Self-Stabilizing Overlay Network for Nodes with Heterogeneous Bandwidths. In *IEEE P2P '14: Proc. of the Int. Conf. on Peer-to-Peer Computing*, pages 1–10, 2014.

[7] K. Graffi. *Monitoring and Management of Peer-to-Peer Systems*. PhD thesis, Technische Universität Darmstadt, Germany, 2010.

[8] K. Graffi. PeerfactSim.KOM: A P2P System Simulator - Experiences and Lessons Learned. In *IEEE P2P '11: Proc. of the Int. Conf. on Peer-to-Peer Computing*, 2011.

[9] K. Graffi, C. Groß, P. Mukherjee, A. Kovacevic, and R. Steinmetz. LifeSocial.KOM: A P2P-based Platform for Secure Online Social Networks. In *IEEE P2P '10: Proc. of the Int. Conf. on Peer-to-Peer Computing*, 2010.

[10] K. Graffi, C. Groß, D. Stingl, D. Hartung, A. Kovacevic, and R. Steinmetz. LifeSocial.KOM: A Secure and P2P-based Solution for Online Social Networks. In *IEEE CCNC '11: Proc. of the IEEE Consumer Communications and Networking Conf.*, 2011.

[11] K. Graffi, C. Groß, D. Stingl, H. Nguyen, A. Kovacevic, and R. Steinmetz. Towards a P2P Cloud: Reliable Resource Reservations in Unreliable P2P Systems. In *IEEE ICPADS '10: Proc. of the Int. Conf. on Parallel and Distributed Systems*, 2010.

[12] K. Graffi, A. Kovacevic, K. Wulffert, and R. Steinmetz. ECHoP2P: Emergency Call Handling over Peer-to-Peer Overlays. In *IEEE P2PNVE'07: Proc. of the Inter. Workshop on Peer-to-Peer Network Virtual Environments*, 2007.

[13] K. Graffi, A. Kovacevic, S. Xiao, and R. Steinmetz. SkyEye.KOM: An Information Management Over-Overlay for Getting the Oracle View on Structured P2P Systems. In *IEEE ICPADS '08: Proc. of the Int. Conf. on Parallel and Distributed Systems*, 2008.

[14] K. Graffi, P. Mukherjee, B. Menges, D. Hartung, A. Kovacevic, and R. Steinmetz. Practical Security in P2P-based Social Networks. In *IEEE LCN '09: Proc. of the Int. Conf. on Local Computer Networks*, 2009.

[15] K. Graffi, S. Podrajanski, P. Mukherjee, A. Kovacevic, and R. Steinmetz. A Distributed Platform for Multimedia Communities. In *IEEE ISM '08: Proc. of the Int. Symposium on Multimedia*, 2008.

[16] K. Graffi, K. Pussep, S. Kaune, A. Kovacevic, N. Liebau, and R. Steinmetz. Overlay Bandwidth Management: Scheduling and Active Queue Management of Overlay Flows. In *IEEE LCN '07: Proceedings of the International Conference on Local Computer Networks*, 2007.

[17] K. Graffi, D. Stingl, J. Rückert, and A. Kovacevic. Monitoring and Management of Structured Peer-to-Peer Systems. In *IEEE P2P '09: Proc. of the Int. Conf. on Peer-to-Peer Computing*, 2009.

[18] B. Guidi, T. Amft, A. De Salve, K. Graffi, and L. Ricci. DiDuSoNet: A P2P Architecture for Distributed Dunbar-based Social Networks. *Peer-to-Peer Networking and Applications*, pages 1–18, 2015.

[19] A. Ippisch and K. Graffi. An Android Framework for Opportunistic Wireless Mesh Networking. In *NetSys'15: Proc. of the Conf. on Net. Systems*, pages 1–2, 2015.

[20] J. Janiuk, A. Mäcker, and K. Graffi. Secure Distributed Data Structures for Peer-to-Peer-based Social Networks. In *IEEE CTS '14: Proc. of the IEEE Int. Conf. on Collaboration Technologies and Systems*, pages 1–10, 2014.

[21] T. Klerx and K. Graffi. Bootstrapping Skynet: Calibration and Autonomic Self-Control of Structured Peer-to-Peer Networks. In *IEEE P2P '13: Proc. of the Int. Conf. on Peer-to-Peer Computing*, pages 1–5, 2013.

[22] A. Kovacevic, K. Graffi, S. Kaune, C. Leng, and R. Steinmetz. Towards Benchmarking of Structured Peer-to-Peer Overlays for Network Virtual Environments. In *IEEE ICPADS '08: Proc. of the Int. Conf. on Parallel and Distributed Systems*, 2008.

[23] A. Kovacevic, S. Kaune, H. Heckel, A. Mink, K. Graffi, O. Heckmann, and R. Steinmetz. PeerfactSim.KOM - A Simulator for Large-Scale Peer-to-Peer Networks. Technical Report Tr-2006-06, TU Darmstadt, 2006.

[24] V. Rapp and K. Graffi. Continuous Gossip-based Aggregation through Dynamic Information Aging. In *IEEE ICCCN '13: Proc. of the Int. Conf. on Computer Communications and Networks*, 2013.

[25] S. Sati and K. Graffi. Adapting the Beacon Interval for Opportunistic Network Communications. In *ICACCI '15: Proc. of the Int. Conf. on Advances in Computing, Communications and Informatics*, pages 1–7, 2015.

[26] P. Wette and K. Graffi. Adding Capacity-Aware Storage Indirection to Homogeneous Distributed Hash Tables. In *NetSys '13: Proc. of the Conf. on Networked Systems*, 2013.

Jun.-Prof. Dr.-Ing. Kalman Graffi

Professor Dr.-Ing. Kalman Graffi is Junior-Professor for the "Technology of Social Networks" in the Institute of Computer Science at the Heinrich Heine University of Düsseldorf in Germany. He obtained his doctorate degree (Dr.-Ing.) from the faculty of Electrical Engineering and Information Technology at the Technische Universität Darmstadt in July 2010, and diplomas in Computer Science and Mathematics, both in 2006, at the same university. With his nine PhD students he concentrates his research on network protocols and mechanisms to support the freedom of speech and privacy around the globe. In specific he researches on a secure peer-to-peer framework for online social networks, on Android-based wireless mesh networks as well as on mechanisms for large-scale democratic argumentation and voting in the Internet. He is founding member of the "Düsseldorf Institute for Internet and Democracy". He received several awards for his work on secure and decentralized communication platforms and their impact on society. In 2014, he was elected as member in the Arab-German Young Academy of Sciences and Humanities (AGYA) and in 2015 he was elected as "Junior Fellow" of the Gesellschaft für Informatik, both for 5 years. In March 2015 he was awarded the title "Young Scientist of the Year 2014" (Nachwuchswissenschaftler des Jahres 2014) by Academics.de. Being in dialogue with political activists in the Arab word and outside, allows him to learn the requirements for secure decentralized communication platforms from first hand and to test his solutions in places where they are needed.

Address: Heinrich Heine Universität Düsseldorf, Computer Science Institute, D-40225 Düsseldorf, E-Mail: graffi@hhu.de