Computer Networks and Distributed Systems

IAM-03-011

September 03

Computer Networks and Distributed Systems

Klausurtagung of the
”Computer Networks and Distributed Systems” research group
Institute of Computer Science and Applied Mathematics
University of Bern

August 26-30
Pochtenalp, Kiental, Switzerland
http://www.iam.unibe.ch/˜rvs/events/

Abstract

The research group ”Computer Networks and Distributed Systems” of the “Institute of Computer Science and Applied Mathematics” at the University of Bern led by Prof. Dr. Torsten Braun focuses the research activities in the areas of mobile and multimedia communications as well as on distance learning and security architectures. In fall 2003, a Klausurtagung has been organized in Pochtenalp with the goal to present and intensively discuss the state of the research work performed by the research group’s Ph.D. students. External international experts working in related research areas have been invited in order to contribute to the discussions and to present their current and future research areas. Each speaker had 90 minutes time for his presentation including discussion. The overall results have been very positive. In particular, the discussions have been very intensive and productive and should be valuable for the Ph.D. students’ future work. This report summarizes the various talks from research group members and external experts.

CR Categories and Subject Descriptors: C2.1 [Computer-Communication Networks]: Network Architecture and Design; **C2.2 [Computer-Communication Networks]:** Network Protocols; **C2.5 [Computer-Communication Networks]:** Local and Wide-Area Networks; **C2.6 [Computer-Communication Networks]:** Internetworking.

General Terms: Algorithms, Design, Performance, security.

List of Presentations

1 Hybrid Simulation
Dipl. phil. nat. Matthias Scheidegger, University of Bern

2 Using Fuzzy Logic to Assist TCP error detection in Mobile Ad Hoc Networks
Dipl. phil. nat. Ruy de Oliveira, University of Bern

3 Beaconless Routing in Mobile Ad-Hoc Networks
Dipl. phil. nat. Marc Heissenbüttel, University of Bern

4 Prof. Dr. Torsten Braun: Quality-of-Service for Internet Multicast, University of Bern

5 Accounting for infrastructured WLAN with Ad-Hoc Extensions
Dipl. phil. nat. Attila Weyland, University of Bern

6 AAI Portal
Dipl. phil. nat. Marc-Alain Steinemann, University of Bern

7 Multipath Multimedia transfer in Ad-hoc Networks
Dipl. phil. nat. Marcin Michalak University of Bern

8 Verification of Telecommunications Systems - Introduction, Problems, and (Partial) Solutions
Prof. Dr. Ulrich Ultes-Nitsche, University of Fribourg

9 Inter Domain Modelling and Simulation
Dr. Florian Baumgartner, University of Bern

10 Value-Added IP Components
Prof. Dr. Georg Carle, University of Tübingen

11 Peer-to-Peer-Networks
Dr. Klaus Wehrle, University of Tübingen

12 CAHN
Dipl. phil. nat. Marc Danzeisen, University of Bern

Acknowledgements: This event has been partly supported by Stiftung zur Förderung der wissenschaftlichen Forschung an der Universität Bern (Hochschulstiftung).

Hybrid Simulation

Matthias Scheidegger

Computer network simulation has always been an important element of network planning and research. However, the most popular approach to IP network simulation—packet-based simulation—has severe scalability issues when it is used for large scenarios.

Several alternative approaches have been proposed [1] [2] [3]. Each of these approaches abstracts details of the scenario to gain efficiency. This choice of abstraction leads to different advantages and disadvantages of the approaches, making the choice of approach dependent on the scenario in question.

We propose the novel abstraction of using analytical models for network domains, inter-domain links and application traffic aggregates. This abstraction is based on the assumption that packet loss only occurs in inter-domain links, not inside domains. The rationale behind this is the ability of network operators to police ingress traffic to avoid congestion inside their networks, and the usually bigger bandwidths inside domains. While this assumption is only an approximation it should be sufficiently realistic in most cases.

A collection of analytical domain, inter-domain link and traffic aggregate models is contained and organized inside multi-domain models, which model the interactions and relations among them. For storing the topology of the underlying models two data structures are used: vertex and edge tables are useful for file storage, while a linked-graph structure is beneficial for calculations. Additionally, routing information is stored since it is required to calculate the effects of traffic load in the multi-domain model. It suffices to store sequences of inter-domain links to uniquely define a path across a multi-domain model.

In order to be able to determine the multi-domain models' packet loss and delay behavior the load distribution inside the model has to be recalculated regularly. This process yields the offered and serviced loads of all inter-domain links. Based on this, the packet forwarding probabilities and link delay distributions can be computed. The packet loss ratio of a path through the multi-domain model is then given by the complement of its cumulative forwarding probability, and its delay distribution is the same as the convolution of the discrete delay distributions of all domains and inter-domain links along the path.

We combined this analytical modeling approach with packet-based simulation, which resulted in the so-called hybrid simulation approach. There are several advantages to this: Many application and protocol models already exist for packet-based simulators and can thus be used together with analytical models. On the other hand, combining fine-grained packet-based simulation with coarse-grained analytical modeling is useful in multi-site VPN scenarios, and others. The approach we chose is to extend nodes of packet-based simulators with embedded analytical models. Every packet passing an extended node is then treated as if it did not only pass a single node but rather the whole network cloud represented by the embedded multi-domain model.

A main problem of hybrid simulation is the transition between packet-events on one hand and “bandwidth at time t” on the other. We solved this problem with so-called bandwidth estimators, which use sliding time windows to estimate the bandwidth at a certain point in time. However, choosing a good time window size is difficult as too small windows lead to overestimated burstiness, while too large windows tend to smoothen the estimation too much.

The concept of hybrid simulation has been implemented into the ns-2 simulator, and some preliminary evaluation has been done. As a first test, a single domain delay model was parameterized based on the measured delay between two endpoints at the University of Bern and the ETH Zürich, respectively. The simulator was able to very closely reproduce the delays observed in reality. A second, rather similar test replaced a nine hop ns-2 scenario with a three hop scenario, using the same source and sink nodes but replacing the seven middle ones with a domain model. The delay behavior was again similar, but the calculation times were reduced dramatically.

The domain models thus proved to be reliable in the assumed quasi-static situations. Inter-domain link models and traffic aggregate models still remain to be evaluated. Especially the inter-domain links’ effects like packet loss and dynamically changing delay characteristics are important for any non-trivial scenario. Further, multi-class traffic—which was specified in theory—should be integrated into the simulator and model in order to be able to study the effects of various QoS mechanisms. Unfortunately, obtaining measurement data from real networks proved to be hard because of the operators’ reluctance to publish any kind of data about their internal networks.

References

[1] K. M. Chandy and J. Misra, “Asynchronous distributed simulation via a sequence of parallel computations,” Communications of the ACM, vol. 11, no. 24, pp. 198-205, April 1981.

[2] A. Yan and W. B. Gong, “Fluid simulation for high speed networks with flow-based routing,” IEEE Transactions of Information Theory, pp. 1588-1599, 1999

[3] Y. Guo, W. Gong, and D. Towsley, “Time-stepped hybrid simulation (TSHS) for large scale networks,” in Proceedings of IEEE Infocom, March 2000.

A Fuzzy Logic Engine to Assist TCP Error Detection in Mobile Ad Hoc Networks

Ruy de Oliveira

Wireless mobile ad hoc networks are innovative in the sense that they do not rely on any fixed infrastructure to communicate. Since there is no centralized point of coordination, these networks are labeled self-organizing networks, where topology changes may occur quite dynamically and unpredictably.

These networks pose some tough challenges to the Transmission Control Protocol (TCP) because it was not designed to work in such highly dynamic and unpredictable environments. This makes the standard TCP performs poorly when packet losses occur by either wireless channel errors (high bit error rate) or link interruptions (due to mobility), rather than by congestion. Hence, changes are necessary to provide the TCP error detection mechanism with the actual cause of every packet loss, so that the error recovery mechanism may take dedicated actions for each case.

Existing approaches may be classified into two classes: Network oriented [1], [2] and end-to-end [3], [4]. In the former, the end nodes rely on explicit message notifications from inside the network to detect congestion or link interruptions. The main drawbacks here are high dependence on lower layer protocols to carry the messages and necessity of changes in the intermediate nodes, which may not only delay deployment but also pose security concerns since such nodes need full access to the packets header. End-to-end approaches, on the other hand, do not need any explicit cooperation of the intermediate nodes, and may be somewhat independent of lower layer protocols. These features make these approaches easier to deploy as changes are limited to the end nodes. Our approach is end-to-end based as described in the following.

The key idea of our proposal is to keep track of the TCP flow and record useful data to infer the current state of the network when packet losses are perceived. Actually, Round Trip Time (RTT) measurements are used as indicator of the internal state of the network. The rationale here is that TCP already relies on this parameter for computing its fundamental retransmission timeout (RTO) timer, and such measurements may be really valuable to reflect the condition inside the network [3], [5]. Nevertheless, RTT measurements are not trivial to be evaluated as they contain imprecision and uncertainties under certain conditions, which calls for an elaborate tool in order to extract the useful data.

Therefore, we make use of Fuzzy Logic theory [6], [7] for distinguishing between bit error and congestion induced losses, using RTT values as input variables. By using fuzzy logic, the continuous and imprecise behavior of the information can be handled without the necessity of arbitrary rigid boundaries. Besides, it has the great advantage of being processing inexpensive. This renders fuzzy logic quite suitable for evaluating RTT values where imprecision and uncertainties are effectively present and the processing requirements (at the end nodes) must be as low as possible.

In this report, we focus on our proposed fuzzy engine to distinguish between channel error and congestion induced losses, having a fixed number of hops end-to-end. However, the scheme should work smoothly for different number of hops. The exact number of hops in place can be determined by the end nodes via standard mechanisms such as the Time To Live (TTL) value in the IP header. Losses by link interruptions have to be determined differently since no packet gets through under these conditions. We briefly explain in the following the basis of our approach.

First of all, we performed a number of simulation runs, using ns-2 simulator, for qualifying the RTT pattern in ad hoc networks. We considered varying levels of both congestion and bit error rate (BER), as well as their combined effects. From these evaluations we could figure out that RTT values may reflect well the internal state of the network. In particular, we noticed that RTT mean values increase significantly with congestion and modestly with bit error. Conversely, RTT variance grows more noticeably under bit error conditions.

According to the observations above, extremely high levels of BER might be misdetected as congestion if only RTT mean are used for inference. Thus, we decided to take into consideration RTT variance as well. Additionally, as the measured values are quite dynamic and contain overlapping ranges (for congestion and bit error values), we realized that an intelligent mechanism, such as a fuzzy logic engine, should be used for carrying out the needed inferences as smooth as possible.

The proposed fuzzy engine makes inference on RTT measurements (RTT mean and variance) and gives as output the discrimination between congestion and bit error induced losses inside the network. Preliminary simulation evaluations show that this scheme may provide accurate result, but a reasonable number of RTT are required. This feature may cause our approach to be a bit slow to detect abrupt transitions in the internal state of the network. We intend to develop supporting mechanisms to improve this behavior. More elaborate fuzzy models are also planned for future work.

References

1. K. Chandran, et al. A Feedback Based Scheme For Improving TCP Performance In Ad-Hoc Wireless Networks. In *Proceedings of ICDCS '98*, IEEE, pp. 472-479, May 1997.

2. J. Liu, S. Singh. ATCP: TCP for Mobile Ad Hoc Networks. *IEEE Journal on selected areas in communications*, pp. 1300-1315, July 2001.

3.R. Oliveira, T. Braun, M. Heissenbuettel, An Edge-based Approach for Improving TCP in Wireless Mobile Ad Hoc Networks, *DASD 2003 as part of ASTC 2003*, pp. 172-177, Mar./April 2003.

4. Z. Fu, B. Greenstein; X. Meng; S. Lu. Design and Implementation of a TCP-Friendly Transport Protocol for Ad Hoc Wireless Networks. *10th IEEE Intl Conference on Network Protocols*. pp. 212-225, 2002.

5. J. Liu, I. Matta and M. Crovella. End-to-End Inference of Loss Nature in a Hybrid Wired/Wireless Environment. *WiOpt'03*, March 2003.

6.L. A. Zadeh, Fuzzy logic=computing with words. *IEEE Transactions on Fuzzy systems*,Vol. 4, No 2, pp. 104-111, 1996.

7.L. Cheng and I. Marsic, Fuzzy Reasoning for Wireless Awareness, *International Journal of Wireless Information Networks*, Vol. 8, Jan. 2001, pp. 15-26.

Beacon-Less Routing in Mobile Ad Hoc Networks

M. Heissenbüttel

A wireless mobile ad-hoc network operates without any centralized administration and does not rely on any fixed infrastructure. Instead the network is completely self-organizing and the communication is maintained on a peer-to-peer basis between the mobile hosts. If two hosts are not within transmission range, other intermediate node may act as routers and relay the packets on behalf of them. Due to the mobility of the nodes the topology of the network may change frequently and in unpredictable ways. Furthermore, devices may suddenly be switched on or off, causing new links to appear or existing links to vanish. Routing in such a dynamic environment is a difficult task and has been subject of extensive research over the past several years. A lot of routing protocols are (were) proposed within MANET working group of IETF such as AODV [1], DSR [2]. Opposed to these topology-based routing protocols which do not make use of location information, position-based protocols try to optimize the routing by making use of geographical information available at each node (GFG [3], GPSR[4], Terminodes [5]]). Every node is aware of its own position and is notified of its neighbors' positions through beacons, small packets broadcasted by the neighbors to announce their position. Additionally, a node is able to determine the location of the destination through any location management scheme (e.g. VHR [6]). This additional position-information allows improving routing significantly and, thus, increases the network scalability in terms of network size, mobility, and traffic. However, the periodical broadcast of beacons not only wastes scarce battery power, but also interferes with regular data transmission. Data packets are destroyed and need to be retransmitted, consuming even more battery power, reducing the capacity of the network, and introducing additional delay.

The impact was studied by means of simulation of the Terminodes routing and GPSR routing protocols and as well two kind of adapted versions of these two protocols. In the first adapted version, called beacon-less, no beacons are transmitted anymore. Every node has complete local neighborhood information, which is provided by the simulator at no cost of transmitting any additional packets. In the second version, called beacons-not-used, the beacons are still transmitted but the used neighbor information for routing is again provided by the simulator. Simulations with this two adapted version give a theoretical bound on the impact of beaconing on the performance and what can be achieved with an optimized beaconing strategy. (In current work, we study more sophisticated time-based, distance-based, and speed-based strategies). Results indicate that the adapted version of GPSR and the Terminodes routing are able to deliver almost 100% of the packet independent of the speed as opposed to 90-95% of the original, unmodified versions. The average end-to-end delay could be decreased by a factor in the order of 4. This shows that beaconing indeed can have really many disadvantages on the performance of the protocol.

Furthermore, we developed a position-based routing protocol, called BLR [7] (Beacon-Less Routing) which avoids to have beacons transmitted periodically and, hence, eliminating the drawbacks that come along. The algorithm performs routing in a completely distributed manner without having information about neighboring nodes. If a node wishes to send a packet, it just broadcasts the packet and every neighboring node receives it. The protocol takes care that just one of these nodes relays the packet any further. This is accomplished by introducing a small additional delay at each node depending on its position relative to the last node and the destination. The node located at the most "optimal" position introduces the fewest delay and thus transmits the packet at first. The other nodes detect this subsequent relaying and cancel their scheduled transmission. To ensure that all nodes detect the forwarding, only nodes within a certain area take part in the contention to forward the packet. In this way, BLR avoids the periodical transmission of beacons which has many advantages. Preliminary results show a superior performance of BLR over GPSR and other position-based routing protocols in terms of packet-delivery-ratio and end-to-end delay. Especially this holds in the case of high mobility in the network. (For more information about the simulation please see [8] and the links there.)

References

[1] Perkins, C., Royer, E.: Ad-Hoc On-Demand Distance Vector Routing. Proceedings of 2nd IEEE Workshop on Mobile Computing Systems and Applications (1999)

[2] D.B. Johnson, D. A. Maltz, and J. Broch, “DSR: The dynamic source routing protocol for multihop wireless ad hoc networks,” in Ad Hoc Networking, Addision-Wesley, 2001, ch. 5, pp. 139 – 172

[3] P. Bose, P. Morin, I. Stojmenovic, and J. Urrutia, “Routing with guaranteed delivery in ad hoc wireless networks”, ACM/Baltzer Wireless Networks, vol. 7, no. 6, pp. 609-616, Nov. 2001

[4] Karp, B., Kung, H.: GPSR: Greedy Perimeter Stateless Routing for Wireless Networks. Proceedings of the Sixth Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom) (2000)

[5] L. Blazevic, S. Giordano, and J.-Y. Le Boudec, “Self-organized terminode routing,” Cluster Computing Journal, vol. 5, no.2, pp. 205 – 218, Apr.2002

[6] S. Giordano and M. Hamdi, “Mobility management: The virtual home region,” EPFL Lausanne, Switzerland, Tech. Rep. SSC/1999/037, Oct. 1999

[7] M. Heissenbüttel, T. Braun, “A Novel Position-based and Beacon-less Routing Algorithm for Mobile Ad-Hoc Networks,” 3rd IEEE Workshop on Applications and Services in Wireless Networks (ASWN03), Bern, Switzerland, July 2-4, 2003

[8] http://www.iam.unibe.ch/~heissen/

Cooperation and Accounting Strategy for Hybrid Networks[1]

Attila Weyland

Hybrid networks increasingly attract interest in the research community. They appear to be a promising combination of the advantages of two worlds: the dynamics of mobile ad hoc networks and the reliability of wired networks. In this context new possibilities to deal with the weaknesses of mobile ad hoc networks become available. We think that besides the security and routing issues the cooperation among nodes is of great importance. The advantages of hybrid networks are clear, but to become widely accepted, new management and maintenance solutions are required. We propose a cooperation and accounting scheme, which takes into account the availability of a reliable network infrastructure and stimulates cooperation by making it a rewarding alternative to selfishness.

Most of the proposed cooperation schemes so far focus on pure mobile ad hoc networks. Of them most apply very restrictive control mechanisms, which are unsuitable for civilian use. We believe that in this kind of environment cooperation among nodes should be achieved by means of rewards and not penalization. And by using the available infrastructure in a hybrid network, it becomes possible to offer an architecture which corresponds with our notion. Similar approaches have been taken only recently, described in two different works.

In [1] and in [2] two charging schemes have been proposed, where cooperative nodes get rewarded. The Nuglets [3] approach enforces cooperation by making the allowance to transmit self-generated packets dependant on the number of forwarded packets. The CONFIDANT [4] approach monitors the behavior of nodes and punishes selfish nodes by means of isolation from the network.

With our scheme we make cooperation among nodes a gainful alternative to selfishness and still leaving the option for a node to not cooperate. We think that in civilian networks where each node can be seen as its own authority, leaving the choice of cooperation to the node increases the acceptance of hybrid networks.

In our scheme, we assume - similar to the Nuglet approach - the existence of a tamper resistant device, i.e. a smart card in each node. This device ensures a protected environment, where our schemes' functions can be executed safely. Additionally, we require a sufficient amount of processing power and memory on the node.

The main idea of our scheme can be summarized as follows: Every time a node wants to transmit a self-generated packet, it has to pay with *Traffic Credit(s)*. Every time a node forwards a packet it gets *Helper Credit(s)*. Traffic Credits can be obtained from gateways, Helper Credits can be traded in at gateways for Traffic

[1] An extended abstract of the presentation given during the RVS Summer School 2003 (September 1-4) held in Pochtenalp, Kiental, Switzerland

Credits. Gateways provide the interconnection between the wired networks and the mobile ad hoc networks. On the one hand, the possibility to obtain Traffic Credits from a centralized source (e.g. a provider) at any time prevents starvation of a node and on the other hand the possibility to earn Helper Credits stimulates the cooperation among nodes.

The accounting is done decentralized on the smart card, which maintains two accounts: one for helper and one for traffic credits. The node authentication is done using Crypto-based IDs as proposed in [5]. A nodes public key is bound to its address. All packets are signed with a private key before transmission and ownership can thus be validated using the packet source address without relying on a centralized security service.

When sending self-generated packet the Traffic Credit account is debited according to the number of hops until the gateway and the packet is transmitted to the next hop according to the routing table. When forwarding a packet the Helper Credit account gets credit and the packet is transmitted to the next hop according to the routing table. Our scheme coexists with ad hoc only traffic as no debit/credit is made for generating/forwarding it.

Our proposed strategy provides incentives for cooperation among nodes in hybrid networks in civilian use. Currently we investigate security protocols for our scheme as well as suitable ad hoc routing protocols. In future we will simulate our strategy using different routing protocols.

References

[1] N. B. Salem, L. Buttyán, J.-P. Hubaux, and M. Jakobsson. A Charging and Rewarding Scheme for Packet Forwarding inMulti-hop Cellular Networks. In *Proceedings of ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*. Annapolis, MD, USA, June 2003.

[2] B. Lamparter, K. Paul, and D. Westhoff. Charging support for ad hoc stub networks. *Elsevier Journal of Computer Communications*, 26(13):1504–1514, August 2003.

[3] L. Butty´an and J.-P. Hubaux. Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks. *ACM Mobile Networks & Applications*, 8(5), October 2003.

[4] S. Buchegger and J.-Y. L. Boudec. Performance Analysis of the CONFIDANT Protocol (Cooperation Of Nodes - Fairness In Dynamic Ad-hoc NeTworks). In *Proceedings of ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*. Lausanne, Switzerland, June 2002.

[5] G. Montenegro and C. Castelluccia. Statistically Unique and Cryptographically Verifiable (SUCV) Identifiers and Addresses. In *Proceedings of Network and Distributed System Security Symposium (NDSS)*. San Diego, CA, USA, February 2002.

Quality-of-Service for Internet Multicast

Torsten Braun

1 Introduction

IP multicast has still not been deployed widely in commercial Internet service provider networks and this will hardly change in the near future although many applications such as audio/video conferencing are becoming more popular. In most cases, group communication is mapped to unicast communication mechanisms. For example, multipoint control units serve as centralized mixing and distribution systems in audio/video conferencing scenarios. Applications establish unicast connections to and from the multipoint control unit to exchange audio/video data streams. Other recent approaches are based on application level multicast mechanisms. Overlay networks serve as distribution trees for multicast traffic. However, many available IP multicast applications are supported neither by multipoint control units nor by application level multicast concepts. This paper reviews application level multicast approaches and describes a solution how to support IP multicast applications using application level multicast. The solution also allows providing Quality-of-Service (QoS) to the applications, which is rather difficult to achieve for IP multicast, since the wide deployment of Integrated Services is not feasible and several problems raised by the integration of IP multicast and Differentiated Services such as the neglected reservation sub-tree problem [1] or the anonymous receiver problem [2] are rather difficult to solve.

2 Application Level Multicast

Application level multicast has recently been proposed to realize multicast distribution services. In this case, overlay networks are constructed for multicast data distribution via a distribution tree. Such distribution trees are built by end systems that exchange data with each other by unicast mechanisms based on either UDP or TCP. This allows using the unicast communication services offered by providers and - if available - QoS support for unicast communication, e.g. Differentiated Services. In order to establish and maintain a distribution tree, end systems belonging to a multicast group have to run an overlay protocol, which might be based on appropriate peer-to-peer protocols such as CAN [3], Chord [4], or Tapestry [5].

The “Application Level Multicast Infrastructure” is intended for small groups and based on a central session controller, which handles registration and maintaining multicast trees by running a control protocol with the session members. Performance monitoring is used to support QoS [6]. With the “NICE is the Internet Cooperative Environment” nodes are partitioned into clusters. Cluster leaders with minimal distance to the cluster members are elected and form a cluster on a higher level.

Multicast distribution is performed based on the built cluster hierarchy [7]. Narada avoids central components and hierarchical structures by forming a fully decentralized self-organizing overlay network [8]. Each member maintains member lists of the whole overlay network. After forming a mesh between the member nodes, a distance vector routing algorithm is used to identify the best paths of the mesh for multicast data distribution similar to IP multicast routing protocols. The mesh can be improved by adding and dropping overlay links depending on quality measurements. Due to the modest performance of the initial approach with a delay factor of 2-3 compared to the distance vector multicast routing protocol (DVMRP), a QoS routing protocol based on the shortest widest path algorithm has been proposed and implemented for audio/video conferencing support [9]. This resulted in significant performance improvements. In certain scenarios, the delay could be even improved compared to DVMRP. Another interesting concept has been proposed by Bullet. A sender can send disjoint data sets along the different links of a distribution tree dependent on the available bandwidth. Receiving peer nodes can search the missing data sets within the peer-to-peer (P2P) network using usual peer-to-peer search mechanisms [10].

Application level multicast mechanisms should provide special overlay application programming interfaces (APIs) such as Overlay Sockets [11] or Common API for Structured P2P Overlay [12]. Multicast applications that aim to utilize the overlay network for multicast distribution must use such an overlay API for accessing the overlay protocol in order to join / leave groups or to send / receive multicast data over / from the overlay network.

3 IP Multicast Support Using Overlays

Unfortunately, application level multicast requires modifying existing multicast applications: IP multicast socket calls for multicast communications (e.g., for joining and leaving groups) need to be replaced by overlay API calls. This requires to either modify application source code or at least to modify (dynamic) link libraries. We aim to avoid this drawback by leaving the multicast applications unchanged and intercepting all multicast messages (IP multicast data and Internet group management protocol) by a multicast network device and a multicast QoS middleware as depicted in Figure 1.

The network device delivers the IP multicast messages to a multicast QoS middleware that calls the appropriate functions of the overlay protocol for joining / leaving multicast groups or for transmitting multicast data over the overlay network. In the reverse direction, the multicast QoS middleware receives multicast data from the overlay protocol and forwards them via the multicast network device and the regular IP multicast enabled protocol stack to the IP multicast application.

QoS support for multicast communication can be achieved by appropriate extensions of either the multicast QoS middleware or the overlay protocol. The multicast distribution tree should be constructed such that only connections between peers are selected that can meet the QoS requirements of the multicast applications to be supported. This can be achieved by implementing multicast QoS routing and

measurement mechanisms in order to select the paths fulfilling the QoS requirements.

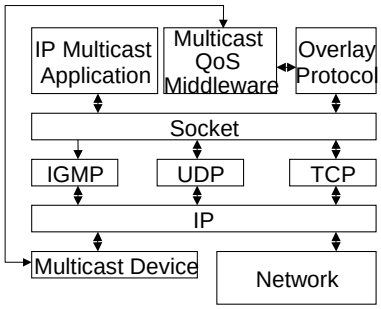


Fig. 1. QoS support for IP multicast applications using overlay protocols and multicast QoS middleware.

4 References

1. R. Bless K. Wehrle: IP Multicast in Differentiated Services Networks, Internet-Draft draft-bless-diffserv-multicast-07.txt, August 2002, work in progress
2. R. Balmer, T. Braun: Zugangskontrolle für einen Videoverteildienst mit IP Multicast, 17. DFN-Arbeitstagung über Kommunikationsnetze, Düsseldorf, Germany, June 10-13, 2003
3. S. Ratnasamy, P. Francis, M. Handley, R. Karp, S. Shenker: A Scalable Content Addressable Network", ACM SIGCOMM 2001, San Diego, August 2001,
4. I. Stoica, R. Morris, D. Karger, M. Kaashoek, H. Balakrishnan: Chord: A Scalable Peer-to-peer Lookup Service for Internet Applications, ACM SIGCOMM 2001, San Diego, August 2001, pp. 149-160
5. B Y. Zhao, L. Huang, J. Stribling, S. Rhea, A. Joseph, J. Kubiatowicz: Tapestry: A Global-scale Overlay for Rapid Service Deployment, IEEE Journal on Selected Areas in Communications, 2003, Special Issue on Service Overlay Networks
6. D. Pendarakis, S. Shi, D. Verma, M. Waldvogel: ALMI: An Application Level multicast Infrastructure, 3rd Usenix Symposium on Internet Technologies & Systems (USITS 2001), San Francisco, CA, USA, March 2001
7. S. Banerjee, B. Bhattacharjee, C. Kommareddy: Scalable Application Layer Multicast, ACM SIGCOMM 2002, August 19-23, 2002, Pittsburgh
8. Y. Chu, S. Rao, S. Seshan, H. Zhang: A Case for Endsystem Multicast, IEEE Journal on Selected Areas in Communications, Vol. 20, No. 8, October 2002, pp. 1456 - 1471
9. Y. Chu, S. Rao, S. Seshan, H. Zhang: Enabling Conferencing Applications on the Internet using an Overlay Multicast Architecture, ACM SIGCOMM 2001, August 27-31, 2001, San Diego
10. D. Kostic, A. Rodriguez, J. Albrecht, A. Vahdat: Bullet: High Bandwidth Data Dissemination Using an Overlay Mesh, ACM SIGCOMM 2003, Poster Abstracts, p. P-6, Karlsruhe, August 25-29, 2003
11. J. Liebeherr, J. Wang, G. Zhang: Programming Overlay Networks with Overlay Sockets, Fifth International Workshop on Networked Group Communications (NGC'03), September 16-19, 2003, Munich, Germany

12. F. Dabek, B. Zhao, P. Druschel, J. Kubiatowicz, I. Stoica: Towards a Common API for Structured Peer-to-Peer Overlays, Proceedings of the 2nd International Workshop on Peer-to-Peer Systems (IPTPS '03), Berkeley, February 2003

AAI Portal

Marc-Alain Steinemann

1 Introduction

Generating and maintaining user access to resources is a time and money consuming process for both users and resource providers. In authentication and authorization infrastructures, organizations authenticate their users and resources authorize those accessing them. A disadvantage of these infrastructures is that resource interfaces have to be adapted and maintained. We propose to fill the gap between authentication and authorization infrastructures and resources with a generic portal. All portal-enabled resources profit from the implemented interfaces to authentication and authorization infrastructures and resources as well as gaining from advanced user and resource management features. The proposed portal has been implemented and connected to an Internet2 middleware called Shibboleth [1] and several types of resources.

2 The Portal in More Detail

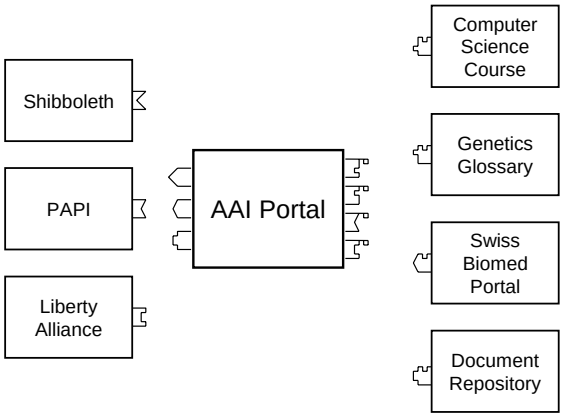


Fig. 1. AAI portal with its interfaces to AAI and resources.

Figure 1 gives an overview about the Authentication and Authorization Infrastructure (AAI) portal with possible AAI on the left side and possible resources on the right side [1,4,5]. The adaptors to the AAI and to the resources are implemented in a modular way to simplify development, reusability and

modification. The only implemented AAI adaptor is the one to the Swiss Shibboleth implementation [2] managed by SWITCH [3].
The portal provides many features for resource and user management. The list below represents a summary of the key features.

- Hosting of one or multiple resources.
- Resource-related management functions.
- Resources can be visible or invisible on the resource list.
- Resources can be open or closed for subscription.
- Resources can be set open for all or subscribers can be directed to a waiting list where tutors can manually grant or deny access.
- Resource can be suspended.
- Resources can be deleted from AAI portal.
- Users can be blocked out from resources.
- Users can be notified about status changes by Short Message Service (SMS) or e-mail.
- Tutors can notify their users by Short Message Service or e-mail.
- Additional *e*-community management features can be added on a modular base, such as personalized news or chat.
- Attribute request policy can be set individually for each resource.
- Attribute release policy can be set individually by each user and for each resource the user subscribes to.
- Missing attributes according to the resource's attribute request policy can be requested from the user.
- User provided information is marked as `user provided` in the database.

3 Results of the Discussion

The AAI portal is already known by RVS member and only a short summary with a focus on new and ongoing developments has been given at Pochtenalp.
A great part of the time has been used to gather new ideas or to discuss possible weaknesses of the architecture.
An interesting question concerned the further development of AAI to AAAI (i.e. integrating accounting). Although systems such as Kerberos offer this already they have certain disadvantages against AAI. In AAI users always authenticate with their home organizations and no central user database is necessary. Resources do no know user data except users want to release those data to specific resources.
Another question concerned a possible extension of the architecture towards Quality of Service QoS and content distribution. Such an extension is well imaginable but the portal would probably have to act as a proxy for the media content. But the portal could then adapt the content to user profiles, eg. High or low bandwidth, mobile or fixed line user, how much a user pays for a service, etc.

4 References

1 Wason Tom: Liberty ID-FF Implementation Guidelines. Draft Version 1.2-02. Liberty Alliance Project. April 14, 2003
2 Graf Christoph et. al.: Architecture Evaluation. SWITCH. Jan 20, 2003. www.switch.ch/aai
3 SWITCH. The Swiss Eduacation & Research Network. www.switch.ch
4 Castro-Rojo R., López D.R.: The PAPI System: Point of Access to Providers of Information. Terena. 2001
5 Wason Tom: Liberty ID-FF Implementation Guidelines. Draft Version 1.2-02. Liberty Alliance Project. April 14, 2003

Multipath Multimedia Transfer in Ad-hoc Networks

Marcin Michalak

Ad-hoc networks, with its varying conditions are a big challenge in terms of providing high transmission quality. Sending traffic over multiple links simultaneously can improve transmission rate, error resilience and delay characteristics, which are crucial for real-time, especially multimedia traffic.

There are three coupled issues in this topic: routing algorithm, encoding algorithm and transmission method.

Routing algorithm provides multiple, independent routes and distributes traffic according to the application request. There are currently several proposed solutions in this area, among them [1] and [2].

Encoding algorithm prepares multimedia streams to be transmitted in such a way that they are:

- highly compressed,
- independent of each other,
- error resilient, i.e. content can be recovered even if some packets are lost.

These features are provided by Multiple Description Coding method, described in [3].

Between those two an intermediate layer is needed, which is called meta-RTP [4] This layer is responsible for:

- traffic distribution at the sender,
- traffic resequencing at the receiver,
- providing path-quality information to application,
- monitoring path quality information

The research in this area includes interaction among the layers, optimizing traffic and encoding according to the network conditions.

References

1. Lee, M. Gerla, „Split Multipath Routing with Maximally Disjoint Paths in Ad hoc Networks", In Proc. of IEEE ICC 2001, pp. 3201 - 3205, 2001
2. Marina, S. Das, "On-demand Multipath Distance Vector Routing in Ad-Hoc Networks", ACM SIGMOBILE Mobile Computing and Communications Review**,** Volume 6 , Issue 3, July 2002
3. Goyal, "Multiple Description Coding: Compression Meets the Network", IEEE Signal Processing Magazine, vol 18, no. 5, pp. 74-93, Sep. 2001
4. .Gogate, D. Chung, S. Panwar, "Supporting Image and Video Applications in a Multihop Radio Environment Using Path Diversity and Multiple Description Coding", IEEE Transactions on Circuits and Systems for Video Technology, Vol. 12, No. 9, September 2002

Verification of Telecommunications Systems

Ulrich Ultes-Nitsche

In the context of linear-time temporal verification [1], one checks whether all possible behaviours of a system (specification) satisfy a linear time temporal property. In the context of distributed systems, such as telecommunications systems, the system specification very frequently contains behaviours that are perceived to be practically impossible in any concrete realisation of the system.

If these extreme behaviours violate the properties, one usually ignores this fact by saying that these behaviours are unfair anyway. To motivate this, let us look at two very simplified examples:

Consider the following "telecommunications" system: two users of the system may call one another; if the called user is not busy, the call will reach her/him, otherwise the call is rejected. A calling user has no control of whether the called user is engaged in another call (busy) or not. Such a system is normally modeled by a nondeterministic choice: whenever a user attempts to call another user, the system model decides nondeterministically whether the called user is busy or not. In such a scenario, there exists the extreme execution in which, whenever a user is called, the user is always busy. Since it is[2] impossible that the user is always busy if there is always the alternative for the call to get through, such an extreme execution is usually ignored by an explicit fairness assumption [2] restricting the permitted executions of the system. Even though such an explicit fairness assumption can always be found, it is not always easy to find an appropriate one and it appears to be attractive to establish a satisfaction relation for linear-time properties (e.g. the "not always busy" property) that contains a fairness assumption inherently in its definition. The satisfaction relation discussed in my presentation (satisfaction within fairness [4, 5]) meets exactly this requirement. In addition, a second way to motivate satisfaction within fairness relation is by considering system observability.

1 Assume, as a second example, two systems, both randomly selecting an unbounded positive integer n initially. The first system will operate n steps and then stop. The second system will either operate n steps and stop, or decide nondeterministically to operate forever. An observer of the two systems who does not know which system is which (black boxes) will at no point of the observation be able to distinguish the two systems: if a system has stopped, it may be either system; if it has not stopped, it may again be either system; system one stopping eventually, or system two stopping at some point or running forever. Only infinite observations could enable one to distinguish the two systems, when an infinitely long sequence of operations is observed (system two).

However, distinguishing systems based on infinite observations is practically impossible.

---

[2] Note that the case of infinitely many consecutive unsuccessful attempts to call someone is considered.

So, system one is as good as system two, since the two systems will not be distinguishable from one another by any finite observation. The lineartime temporal satisfaction relation will distinguish the two systems as system two does not satisfy the property “performing only finitely many operations” where the first one does. Linear-time satisfaction can therefore distinguish systems which are practically indistinguishable. The satisfaction within fairness relation discussed in my presentation does distinguish only those systems which can be distinguished by some finite observation. Hence it appears to be an improvement over the standard linear-time relation.
The discussed concepts can also be equipped with an abstraction concept [4] as well as an efficient partial-order construction technique of the abstract state-space [5], which makes satisfaction within fairness applicable in practical contexts [3].

References

[1] E. M. Clarke, O. Grumberg, and D. A. Peled. Model Checking. The MIT Press, 1999.
[2] N. Francez. Fairness. Springer Verlag, New York, first edition, 1986.
[3] U. Nitsche. Application of formal verification and behaviour abstraction to the service interaction problem in intelligent networks. Journal of Systems and Software, 40(3):227–248, March 1998.
[4] U. Nitsche and P. Wolper. Relative liveness and behavior abstraction (extended abstract). In Proceedings of the 16th ACM Symposium on Principles of Distributed Computing (PODC’97), pages 45–52, Santa Barbara, CA, 1997.
[5] U. Ultes-Nitsche and S. St James. Improved verification of linear-time properties within fairness – weakly continuation-closed behaviour abstractions computed from trace reductions. Software Testing, Verification and Reliability (STVR), 2003. to be published in December 2003.

Interdomain Modeling and Simulation

Florian Baumgartner

The InterMON Project aims on integrating several tools into a common platform for the modeling and simulation of real networks in a multi domain scenario. The concept of the project was not the development of new tools, but their integration in a common user-friendly framework. Another focus of the project is the availability of data. Network providers will hardly distribute measurement data about their networks, and tend to present their networks as a kind of black box to customers.

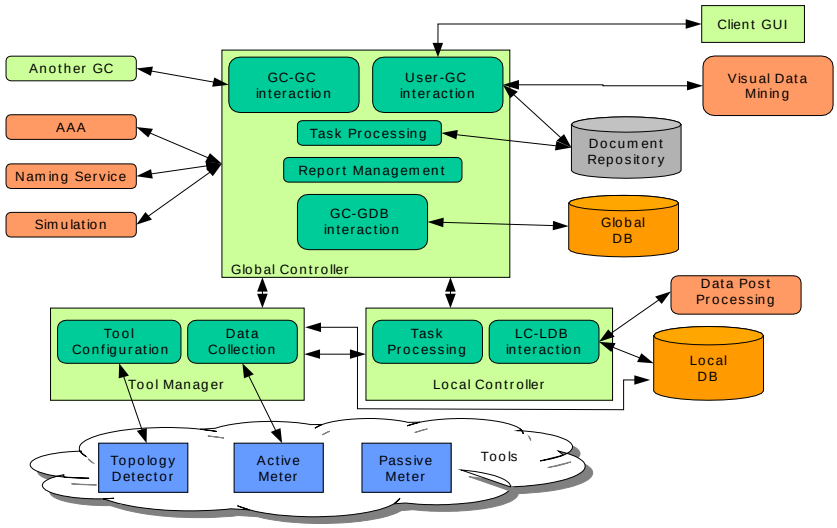


Figure 1: InterMON Architecture

This fact is reflected as by integrating a concept of distributed databases, providing measurement information, as well as by providing measurement and discovery tools, which so not require the collaboration of the Network provider. Besides the distributed Database, the InterMON project integrates simulation approaches based on analytical models as well as on measurement data and appropriate visual data mining techniques to present the results to the user. The InterMON system is a distributed system which uses the Java Messaging System and JBOSS for the communication between the single components. This system allows to send jobs to various processors (e.g. a simulation server) and get the results as an reply.

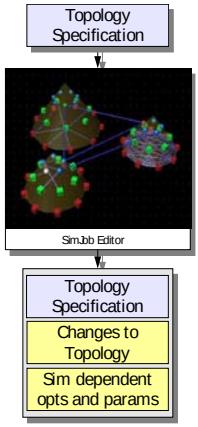


Figure 2: Creation of a Simulation Job

It was a central objective from the beginning to integrate different simulators within the system. This is important because it is obvious that not all simulators suit the same purpose and a comparison of simulation results based on different simulation principles can increase the accuracy of the simulation in total and is highly appreciated. Besides fluid and sequential time series simulations the focus of the University of Bern was on Hybrid simulation, a concept which was developed within the InterMON project. Using multiple simulation strategies is made easy by the distributed, modular architecture of the InterMON project. An XML scheme has been developed to cover the basic requirements of all kinds of simulation jobs. Since it seems not appropriate to provide a single job description all simulator dependent details, the XML scheme is only a basic framework covering a common part (e.g the topology), which is then changed and completed as shown in Figure 2 by the user using the graphical user interface.

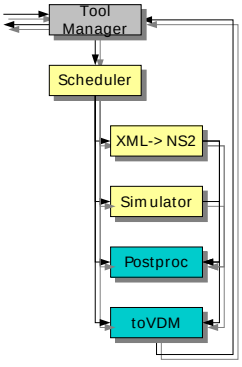


Figure 3: Simulation Pipeline

The concept of hybrid simulation was developed at the University of Bern and tries to combine the advantages of statistic simulation approaches with traditional

packet based simulation. The idea is to replace the simple forwarding characteristics, regarding delay and packet treatment, of a single node in a packet based simulator by the characteristics of a complete complex network (Figure 3). This allows a single node to model a whole network and therefore increases the scalability of such an approach. On the other hand this network nodes can be used within packet based simulations. Another advantage is that these models can be automatically created respectively trained using the measurement information in the InterMON database. This concept was further extended to allow the representation of multiple networks within a single node, using queuing theory concepts to model the queues between the domains. Since the model to be used for a network-node can be specified within the graphical user interface, the job description does not only describe the topology, but includes the model specification or even a binary plug-in for representing this network.

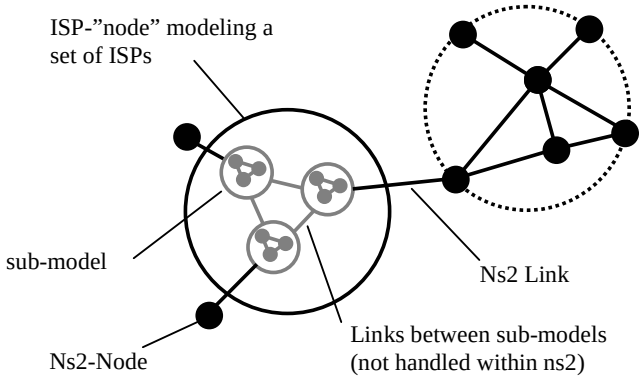


Figure 4: Hybrid Simulation

The hybrid simulator is based on the well known ns2 network simulator, which was modified significantly. The packet forwarding behavior of nodes was made more flexible and interfaces had to be added to allow the addition of network models and the passing of information between the simulator and the external model modules. Generic external modules containing network models can be loaded and removed dynamically during runtime into the ns2 simulator, which allows changing models within a single simulation run. The type of models realized within such a module is not restricted. The currently used model is designed to reproduce the statistical behavior of a given network, but also allows to add model internal traffic sources and sinks. These model internal traffic elements further increase the scalability of the approach.

To be able to process simulation requests automatically, the simulator was embedded within a simulator pipeline (). This allows triggering the processing of simulation jobs from the graphical user interface without any need for manual intervention and simplifies the usage of the InterMON system.

To be able to process simulation jobs automatically, the xml based job descriptions have to be translated into TCL based ns2 simulation scripts. After the execution of the simulator a post-processing of the simulation logs is required to filter the wanted observables out of the rather large simulation traces. In a final step the

output is converted into the XML based VDM format which is used as a common format for data representation within the project. A central scheduler receives the simulation jobs, keeps track of the simulation process and returns the results.
The rather modular architecture of the InterMON system and especially of the simulation component allows also the integration of new simulation approaches and concepts. Future concepts might include neural networks for the prediction of network utilization and Quality of Service as well as more sophisticated analytical models.

References

Florian Baumgartner, Matthias Scheidegger and Torsten Braun: *Enhancing Discrete Event Network Simulators with Analytical Network Cloud Models*, International Workshop on Inter-domain Performance and Simulation (IPS), Salzburg, Austria, February 20-21 2003, pp. 21-30

Value-Added IP Mechanisms

Georg Carle

Abstract. We propose a framework for enabling an open Internet service market, in which value added service providers can combine service components of different administrative domains. In order to enable such a component-based Internet service market, the existing network infrastructure has to be extended by meters, Authentication, Authorisation and Accounting (AAA), charging and payment elements. Meters enable to account for resource usage and to validate QoS. The meters have to perform measurements on behalf of service providers, intermediaries, or service consumers. AAA elements allow to manage trust, by authenticating service consumers and service providers, checking and enforcing authorisation to access service components, account for service usage and exchange measurement information. Charging and payment elements allow to announce tariffs and charging policies and to handle payments. Key components of the framework have been implemented and validated in a scenario where MPEG4 continuous media flows are transported via wireless links, are stored in a video server who handles access control via AAA, and offers value-added services to subscribers: QoS validation and FEC-based error control.

Motivation

A number of technical advances are required in order for Internet technology to meet the expectations of providing a variety of commercially viable services. The services to be supported include real-time, interactive and streaming services. Commercially viable service provisioning frequently requires accounting and charging of resource usage and also monitoring of the service provisioning, including measurements in order to validate whether the required Quality of Service (QoS) has been provided. Therefore, network components are required that provide functionality for authentication, authorization, accounting and various measurements.

A wide variety of applications require input from network measurements. Usage-based accounting is based on measurement results of the actual resource consumption in the network. The validation of guarantees given in service level agreements (SLAs) requires QoS measurements for specific traffic aggregates. Attack and intrusion detection systems rely on measurement input from the network and also traffic profiling and traffic engineering applications base on measurement results [QuZC03]. Due to the broad demand for measurements, several sophisticated and specialized measurement tools and solutions already exist. Nevertheless, existing protocols and propitiatory solutions for measurement configuration and data collection are not well suited for a convenient control of a heterogeneous measurement infrastructure in inter-domain scenarios. Existing protocols (like

SNMP, COPS) and approaches (e.g. NIMI architecture [PaAM00], one-way-delay protocol [ShTZ03]) with the potentials and possibilities that can be achieved by extending the AAA architecture proposed in [LaGG00] for measurement configuration and result data collection. AAA mechanisms and components have the potential to be utilized for flexible measurement configuration and data collection. As proposed in [ZZCa02], such an architecture can be used for policy-based inter-domain configuration and data collection in a heterogeneous measurement infrastructure.

AAA based Measurement Task Distribution

Instead of inventing a new and separate architecture for distributing measurement tasks we propose to use the Authentication, Authorization and Accounting (AAA) infrastructure proposed in [LaGG00]. A AAA infrastructure is required if access to services has to be controlled and information of resource usage has to be collected for later billing. Its is furthermore assumed that this infrastructure takes care of auditing of all AAA transactions and sessions. We propose that such an infrastructure is also used to audit provided QoS in case the SLA contains QoS guarantees.
We think this is a natural approach as a AAA infrastructure already fulfils a couple of the derived configuration and data collection requirements. A trust relationship between AAA servers of different domains must exist. These long-term security associations can be used to distribute measurement tasks in an authenticated and secure way. Since the applications we focus on are closely coupled to service provisioning, the distribution of these measurement tasks integrate seamlessly with the AAA framework. For accounting there must be flexibility since there are large differences between providers regarding their size and purpose, the QoS provisioning technique, the service classes offered, the business models and their respective charging schemes, the accounting services provided, accounting agreements with other providers and the capabilities of the existing infrastructure. In RFC3334 (c.f. [ZZCa02]), it is proposed to use and distribute accounting policies to cope with these needs. The accounting policies can be transformed in appropriate policies for the local measurement infrastructure. Similar QoS auditing policies can be distributed if the SLA contains QoS guarantees. Again these policies can be converted into measurement policies appropriate for the domain. The measurement policies are then enforced on the measurement devices best suited for a given task.

Streaming Scenario

One scenario in which the measurement service can be integrated seamlessly is provisioning of continuous media flows in combination with QoS auditing. Such auditing allows to offer distance education services in which SLAs can be used for specifying that a service provider can apply full charges only in cases where the QoS requirements have been fulfilled. Figure 1 shows a scenario in which the paradigm of

policy-based accounting is used for resource usage metering and QoS validation. In this scenario, additional elements - Error Control (EC) Boosters - can be used to reduce the loss rate as seen by the user, thereby offering the possibility for meeting end-to-end requirements even in the case of significant link loss, which may be desirable for scenarios with significant loss rates, e.g. for wireless links.

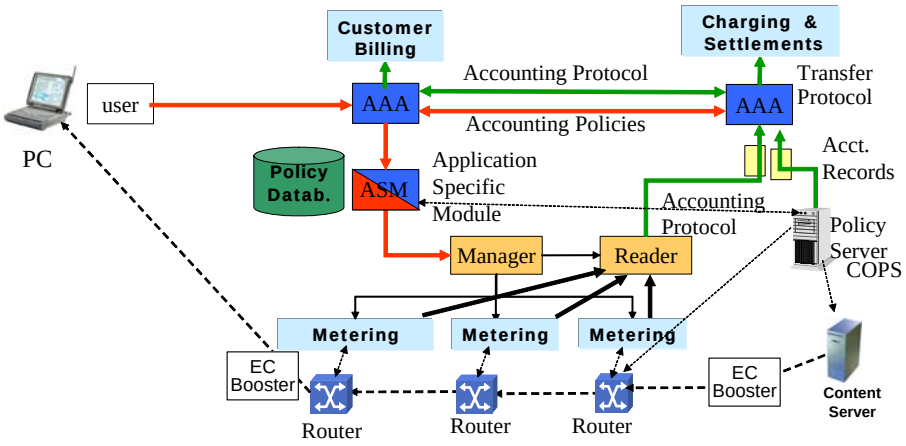


Figure 5: Streaming Service with policy-based AAA components for service access control and measurement configuration

Acknowledgements

This work was partially performed while the author was with the Fraunhofer Institute for Open Communication Systems (FOKUS) in Berlin. The contributions of members of the Global Networking (GloNe) Competence Center are gratefully acknowledged, in particular the fruitful cooperation with Tanja Zseby and Sebastian Zander.

References

[LaGG00] C. de Laat, G. Gross, L. Gommans, J. Vollbrecht, D. Spence: Generic AAA Architecture; Internet Engineering Task Force, Experimental RFC 2903, August 2000.

[PaAM00] V. Paxon, A. Adams, M. Mathis: “Experiences with NIMI”, The First Passive and Active Measurement Workshop PAM 2000, Hamilton, New Zealand, April 3-4, 2000

[QuZC03] J. Quittek, T. Zseby, B. Claise, S. Zander: "Requirements for IP Flow Information Export", IETF draft <draft-ietf-ipfix-reqs-12.txt>, Work in Progress, November 2003.

[ShTZ03]S. Shalunov, B. Teitelbaum, A. Karp, J. Boote, M. Zekauskas: A One-way Active Measurement Protocol (OWAMP), Internet Draft, <draft-ietf-ippm-owdp-07.txt>, October 2003

[ZZCa02]T. Zseby, S. Zander, G. Carle: *Policy-based Accounting*, Internet Engineering Task Force, Experimental RFC 3334, October 2002.

Basic Services for Peer-to-Peer Applications

Klaus Wehrle

Peer-to-Peer Networking

With *Peer-to-Peer Networking* a highly interesting communication paradigm is currently emerging in the Internet community. Though originally developed for very pragmatic applications like file sharing and online music exchange, the Peer-to-Peer-concepts offer scalable usage of distributed resources and thus new possibilities for various applications and solutions of long discussed problems.

Due to the continuous growth of the Internet in terms of participants and data volume, but also due to new demands by the increasing application spectrum, certain problems can not be solved anymore with client-server-centered approaches. Examples are file sharing applications, anti-censorship file systems or Grid computing. The principles of Peer-to-Peer-Networking allow completely new perspectives for globally distributed applications. Furthermore, such systems are extremely scalable, reliable and resistant against failures and external attacks.

The main focus of this contribution is to give a brief overview over basic methods for de-centralized self-organization and a first approach of provisioning basic mechanisms and services for Peer-to-Peer applications. New P2P-applications will base on these mechanisms and do not need to implement and perform them separately. This work has been performed by the author in cooperation with the International Computer Science Institute and UC Berkeley.

The Internet Indirection Infrastructure

The Internet Indirect Infrastructure (*i3*) is a first approach of realizing generic services for Peer-to-Peer applications. Based on the concept of indirection (cf. Fig. 1) *i3* supports a broad spectrum of applications. Different to traditional Internet routing, *i3* performs routing via indirection points. These so-called *i3*-identifiers are managed in a distributed hash table in a scalable, resilient and flexible way.

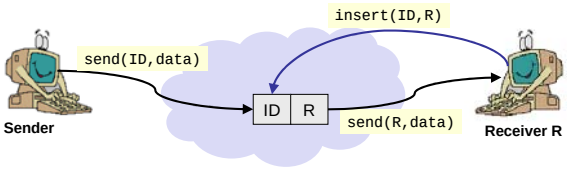
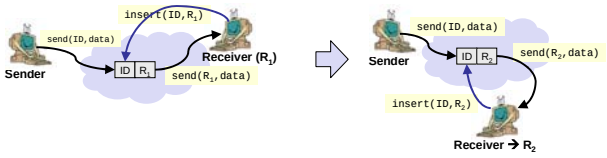


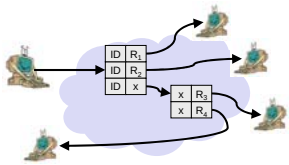
Figure 1: Indirection as basic principle in i3

Though the principle of indirection in *i3* differs significantly from Internet routing, it can be identified in most extensions added to the Internet Protocol in the last decade. These extensions could not be established successfully because each of them increased the complexity of the Internet Protocol too much. A generic solution like *i3*, that moreover bases on the scalable principle of a distributed hash table, promises a more realistic solution for these problems.

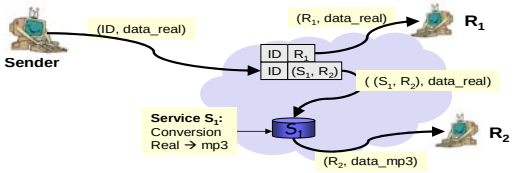
As shown in Fig. 2 the following basic communication services can be realized with the Internet Indirection Infrastructure:



(a) Mobility



(b) Group communication



(c) Service Composition

Figure 2: Generic Support of various Communication Patterns with *i3*

- *Mobility Support*: By changing the destination address in an *i3*-trigger receivers can move in the Internet and easily adapt their new destination addresses to be reachable and accessible. Furthermore, senders are also mobile and the indirection principle offers an integrated anonymity of both, senders and receivers.
- *Group Communication(Multicast)*: By registering multiple triggers to an *i3*-id, a group of receivers can register for a certain data. To avoid scalability problems and to perform an efficient distribution process, a tree of multiple indirection points can be established.

- *Anycast Communication*realizes the delivery of a message to only one member of a group. It can be realized with triggers that have a common prefix and a random tail.
- *Service Composition:*As aimed by several approaches in the Active Network area, *i3* offers a heterogeneous composition of several services in the network. Addressed by a stack of indirection points, a sender or receiver can initiate cascades of services acting on data streams on their way to the receivers.

The *i3*-architecture has been implemented and is currently under evaluation in the Peer-to-Peer-testbed Planet-Lab. Future work on *i3* aims increased security, resilience, and the implementation of more services like virtual private networks, distributed firewalls and a network weather service.

A Transparent Proxy connecting IP- and Overlay-Networks

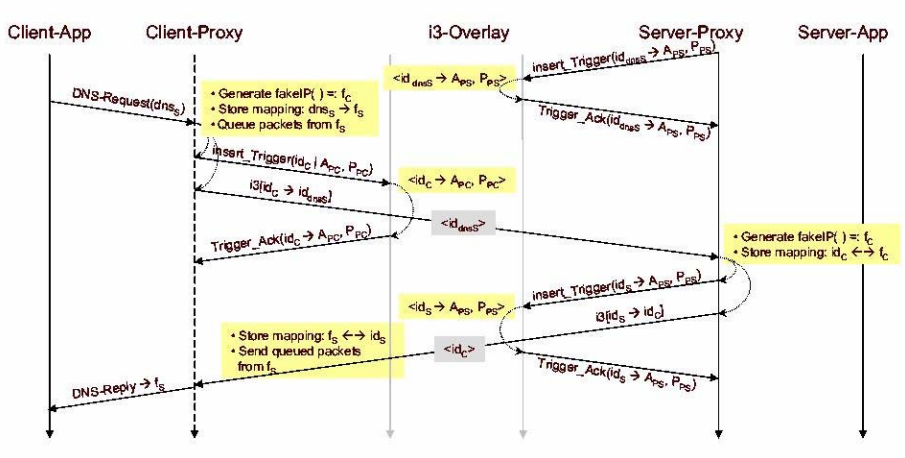
Legacy applications can not be used in Peer-to-Peer-overlay networks, that mostly base on completely different addressing schemes than the traditional IP world. So either new applications have to be developed or existing applications must be modified, if possible. Both approaches are time and work consuming.

Based on this problem, a general solution for connecting IP networks with differently addressed networks evolved and was realized with the *i3*-proxy. In this special case, legacy IP applications can communicate transparently to an *i3*-based overlay network and take advantage of the various *i3*-features. E.g., virtual private networks, distributed firewalls, and totally different and private name spaces can be realized within the DNS.

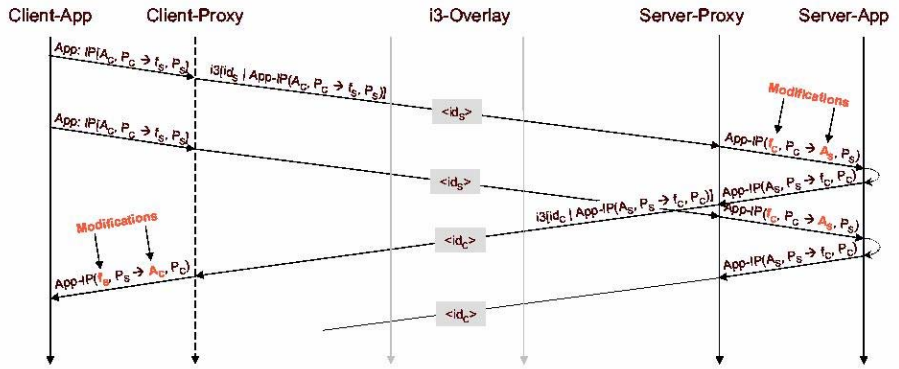
Assuming that IP-based applications use the Domain Name System to address other hosts in the Internet, *i3*-proxy performs an address mapping of DNS names to overlay addresses. Normally, the DNS is used to map DNS-names like www.uni-tuebingen.de on the corresponding IP address, that is necessary for an IP-based communication. This mapping is the basis for the *i3*-proxy-concept. DNS requests on a host or within a LAN are analyzed, and in case of an *i3*-related request, the DNS name is mapped on the related *i3*-address. *i3*-related requests can currently be identified by an DNS name ending with {.i3}, but other schemes are also possible. The requested *i3*-address is then calculated as result of a hash function applied on the DNS name.

Fig. 3a shows the establishing of a „private" *i3*-connection between the initiating legacy application and the called peer node -- that could also be a legacy application communicating via an *i3*-proxy. To camouflage the address space of the overlay network the *i3*-proxy returns a fake IP address to the legacy application. The fake address is part of a special address space that does not exist in the Internet. After successfully establishing a private i3-connection, data communication between the IP-based legacy application and the overlay network is performed as shown in Fig. 3b.

Next to coupling legacy IP-based applications with Peer-to-Peer overlay networks, this concept also allows the reachability of servers behind NAT gateways in private address spaces. This has been an enormous problem in the Internet so far and could only be solved insufficiently.



(a) Establishing a Connection



(b) Communication phase

Figure 3: Interactions between a legacy IP-application, the i3 -proxy and the i3 -overlay network

Cellular Assisted Heterogeneous Networking (CAHN)

Marc Danzeisen

Existing radio technologies like wireless LAN, Bluetooth, GPRS or UWB allow communication between different mobile devices like mobile phones, PDA or Laptops. As it will be discussed later in this document, these wireless technologies require appropriate configuration to work in a desired manner. Too often, more than a basic know-how about the technology itself is required to understand the different setting needed to interconnect devices. With the CAHN approach, this configuration is made automatically and transparent for the user. Therefore, the signaling channel is separated from the actual data channel. The need for a reliable, secure signaling plane with a high coverage makes the cellular network a promising candidate for this purpose. The actual bandwidth limitation of nowadays cellular networks like GSM (GPRS) is a big handicap for the competition against broadband wireless radio technologies. But on the other hand, the cellular networks benefit from the high coverage and the always on characteristic. The paging of a mobile device that is cellular aware is a common functionality. Therefore, the cellular network is very well meeting the requirements of a signaling plane. However, for fast data transfer, other technologies like wireless LAN, Bluetooth or Ultrawide Band (UWB) are much more appropriate. Taking these facts into account, a framework for "Cellular Assisted Heterogeneous Networking" was developed where the cellular network serves as the signaling plane for wireless broadband data channels. Within student projects and the diploma work of two students the first implementation of the CAHN architecture is being realized now.