HORST - Home Router Sharing based on Trust

Michael Seufert, Valentin Burger, Tobias Hoßfeld

University of Würzburg, Institute of Computer Science, Würzburg, Germany

Email: {seufert | valentin.burger | hossfeld}@informatik.uni-wuerzburg.de

Abstract—Today's Internet services are increasingly accessed from mobile devices, thus being responsible for growing load in mobile networks. At the same time, more and more WiFi routers are deployed such that a dense coverage of WiFi is available. Results from different related works suggest that there is a high potential of reducing load on the mobile networks by offloading data to WiFi networks, thereby improving mobile users' quality of experience (QoE) with Internet services. Additionally, the storage of the router could be used for content caching and delivery close to the end user, which is more energy efficient compared to classical content servers, and saves costs for network operators by reducing traffic between autonomous systems. Going one step beyond, we foresee that merging these approaches and augmenting them with social information from online social networks (OSNs) will result both in even less costs for network operators and increased QoE of end users. Therefore, we propose home router sharing based on trust (HORST) - a socially-aware traffic management solution which targets three popular use cases: data offloading to WiFi, content caching/prefetching, and content delivery.
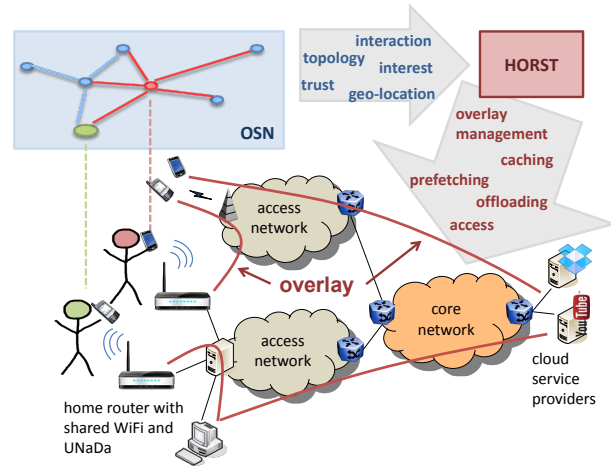
Fig. 1. Basic HORST functionality. HORST uses information from the OSN to provide end users access to shared WiFi access points based on their trust scores, to enable content prefetching and caching, and to control an efficient content delivery overlay.

I. INTRODUCTION

According to [1], the number of mobile-connected devices will exceed the world's population in 2013 and mobile data traffic is ever increasing. To handle the growth and reduce the load on the mobile networks, offloading to WiFi has come to the center of industry thinking [2]. In 2012 already 33% of total mobile data traffic was offloaded onto the fixed network through WiFi or femtocell, and the number of public WiFi hotspots is increasing up to several millions. Additionally, there is a much larger amount of private WiFi hotspots which could also be utilized for data offloading.

With users increasingly sharing their lives in online social networks (OSNs) and content spreading along connected friends (so called social cascades), there is a new reason to utilize private home routers. Social awareness, i.e. the collection and exploitation of social signals, can be used to predict social cascades, i.e. the propagation of content links in OSNs, and thus specify where and by whom content will be requested. As home routers are/can be equipped with storage capacities, a socially-aware traffic management mechanism is possible which proactively sends the content to a router at which it is/will be requested.

Home router sharing based on trust (HORST) is such a mechanism which addresses the three use cases data offloading, content caching/prefetching, and content delivery. Therefore, our solution consists of a firmware for a home router, an OSN app, and a mobile device app. The firmware

sets up two WiFi networks (SSIDs) - one for private usage and one for sharing. Additionally, a user-owned nano datacenter (UNaDa) is established on the home router. The owner of the home router uploads the WiFi access information of the shared WiFi to the OSN app. Each user can share his WiFi information to other trusted users via the app and request access to other shared WiFis. As the app knows the position of the users, it can recommend near WiFis to the users, or automatically request access and connect the users for data offloading. Social cascades can be used to predict which content will be requested by which user. As the app also knows about the current and future users of each WiFi, the UNaDa on the home router can be used to cache or prefetch delay-tolerant content which will be delivered when the user is connected to the WiFi. Finally, HORST federates all UNaDas to form an overlay content delivery network (CDN) which allows for efficient content placement and traffic management.

This paper, in which we describe HORST in detail, is structured as follows: Section II explains the three major use cases data offloading, content caching/prefetching, and content delivery, and Section III will present previous work on which we build on. In Section IV the components of HORST are described, and Section V discusses current and future work.

II. USE CASES

The main aspect of HORST is providing a ubiquitous Internet access via WiFi to all participating users. Additionally, it is a socially-aware traffic management solution which utilizes

network resources more efficiently and improves users' QoE. Figure 1 shows the basic functionality of HORST. HORST uses personal data, friendship relations, and communication patterns from OSNs to compute trust relations which e.g. can be based on common trusted connections, or reliability, or recent cooperative behavior. Furthermore, the OSN can provide information about the popularity of content and about the interest of specific users. The OSN may also provide geo-location information about the users which allows for recommendation of nearby shared WiFi access points of trusted users, and prediction of content request locations. HORST uses this information a) to authorize access to WiFi for data offloading, b) to enable content caching and prefetching, and c) to efficiently manage an overlay CDN.

A. Data Offloading

As users can access shared WiFis through HORST, they can use the WiFi network to connect to the Internet. This reduces the load on the 3G link and will eventually lead to less costs for mobile network operators. End users experience a higher bandwidth and their mobile device has a lower energy consumption because of lower signal strength and faster data transmission. Additionally, HORST can guide users to the nearest WiFi and manage the access request based on the trust between them and the owners. This leverages the scheduling of both upload and download transmissions for delay-tolerant content, such that they are conducted when the user is connected to a WiFi network.

B. Content Caching and Prefetching

OSN and UNaDas provide information such as social cascades and access history, which can be used to calculate and predict temporal and spatial popularity of content. Based on that, it is possible to decide which content to prefetch to which local cache, and how long to keep the content in the cache for best performance. As a result, users who want to access content which is shared via OSN (social cascade) or which is requested frequently via their friends' home routers, will often find that their home router already stores the wanted content. Additionally, users can indicate that they want to access content at a later time, e.g. when they have WiFi coverage or when they are back at home, and in the meantime HORST will prefetch this content to the specified UNaDa. When users request content via WiFi from their router, they can access it with much less delay and a higher bandwidth resulting in a higher QoE for almost all services. At the same time cloud operators benefit from reduced load on servers, decreased storage demand, and improved quality of service.

C. Content Delivery

Content which is about to become popular for end users will be requested from the original content provider and distributed via the UNaDa-induced overlay CDN. In doing so, HORST will efficiently utilize the network resources, e.g. if possible request and distribute content only in non-peak hours. If a user requests content which is not yet stored on her UNaDa, HORST will decide from which resource the content is requested. The selected resource can be e.g. another

UNaDa or the server of a cloud service provider, depending on network condition, resource location, and delay tolerance. Thus, HORST performs traffic management and optimizes the overlay in order to balance load, save (transit) traffic and transit costs, and improve the service and QoE for end users.

III. RELATED WORK

Our approach HORST combines several proposals which have been presented in literature, mainly in the field of WiFi sharing, nano datacenters, social awareness, and trust.

A. WiFi sharing

Sharing WiFi for ubiquitous Internet access has already been tackled by commercial services as well as research work. Fon[1] already started to build a WiFi-sharing community in 2006 by offering a home router with a public and a private encrypted SSID. The public WiFi could then be accessed by everybody who joined the community. Similar approaches are Karma[2] which adds a subtle social layer to WiFi sharing, and WeFi[3] and Boingo[4] which provide hotspot databases. The research community is interested in this topic, too, and investigated incentives and algorithms for broadband access sharing [3], and ubiquitous WiFi access architectures for deployment in metropolitan areas [4], [5]. The most similar work to our approach was conducted in [6], which describes trust-based WiFi password sharing via an OSN app. However, we extend this approach and combine it with content delivery via home routers and the incorporation of socially-aware traffic management.

B. Nano Datacenters

Nano datacenters (NaDa) are a distributed computing platform on ISP-controlled home gateways which were first presented in [7], [8]. They can be used for content delivery and showed to be significantly more energy efficient compared to traditional data centers by reuse of already committed baseline power, avoidance of cooling costs, and reduction of network energy consumption. NaDas can form a CDN on their own but also facilitate the deployment of applications such as peer (NaDa) assisted video on demand streaming [9]. In [10], it is described that shared WiFi routers could be utilized for prefetching of content which reduces the perceived end-to-end delay up to 50%. In [11], the end device is used as NaDa and serves as its own cache. Both content which is globally popular and content which is of personal interest is prefetched overnight directly on the end device. The results show that there is a high potential to reduce both response time and energy consumption compared to different access technologies.

C. Social Awareness

Social awareness is a novel approach to traffic management on the Internet [12]. With socially-aware caching future access to user generated content (e.g. videos) shall be predicted based

[1]http://www.fon.com

[2]https://yourkarma.com/

[3]http://wefi.com/

[4]http://www.boingo.com/

on information from OSNs. Hints are generated for replica placement and/or cache replacement. In [13], the classical approach of placing replicas based on the access history is improved. Therefore social cascades are identified in an OSN, and locations of potential future users (i.e. OSN friends of previous users) are taken into account. In [14], standard cache replacement strategies are augmented with geo-social information from OSNs. Again social cascades are analyzed to recognize locally popular content and keep it longer in the cache. Specialized solutions [15], [16] exist for video streaming which explore social relationships, interest similarity, and access patterns for efficient prefetching to improve users' QoE.

D. Trust in OSNs

Letting everybody contribute to a network by offering freely accessible WiFi connections and access to home routers opens the door for fraud users. Furthermore, home routers can be temporarily or permanently unavailable due to failure or other reasons. Therefore, we need trust scores which reflect the reliability and reputation of users based on their contributions and recent cooperative behavior in the OSN. One of the first works in this area is [17] which proposes the Eigentrust algorithm to compute trust values in P2P networks. Eigentrust assigns each peer a global trust value based on a distributed and secure method. Thus, malicious peers in the P2P networks can be identified. Since every peer uses the global trust values to choose its peers, the network regulates itself by segregating malicious peers. The drawback of such global trust values is that trustworthiness differs for each user as it is influenced by individual preferences, cautiousness, personal relations, and communities. Such personalized trust values have been addressed in [18], [19]. The models in these works rely on the transitive notion of trust, i.e. if node A trusts node B, and B trusts node C, it is assumed that A also trusts C. Such trust values can also be assigned to users that have not interacted so far. Computing all pairs of personal trust yields a huge computational overhead. The authors of [20] claim that the exhaustive computation of all pairs is often not necessary. They propose to present users just a personalized subset with a limited number of most trusted nodes. This could be applicable to our solution, since only the personalized trust values of owners of WiFi access points which are geographically close to the user have to be computed.

IV. COMPONENTS OF HORST

A. Home Router Firmware

Due to legal issues, a shared WiFi which is separated from the private WiFi network, is required for home router sharing. To provision at least two WiFi networks (SSIDs), the router needs appropriate hardware components and firmware which must support Virtual Access Points (VAPs). Projects that currently implement VAP support are DD-WRT[5], OpenWrt[6], and Freetz[7]. DD-WRT is a Linux based open source firmware alternative for WiFi routers and embedded systems. OpenWrt is a Linux distribution for embedded devices, which provides a

---

[5]http://www.dd-wrt.com/
[6]https://openwrt.org/
[7]http://freetz.org/

---

fully writeable file-system with package management. Freetz is a firmware extension for the AVM Fritz!Box and devices with identical hardware. The firmware has to be used to set up multiple SSIDs on the home router, but also to distinguish the BSSID in order to provide connectivity for every end user device. The BSSID uniquely identifies a specific (virtual) access point interface, in most cases with its MAC address. However, if multiple SSIDs share the same MAC address, problems may occur in end user devices, e.g. such that clients are unable to see or connect to the SSID.

To host a nano datacenter and to contribute to an efficient CDN overlay, further requirements arise. To serve as a cache and to support more complex operations, routers need memory and storage. However, the available memory on today's routers is enough for basic operations, which fit all our considered use cases, and storage can easily be added by external USB drives. The home routers must be able to run an overlay management software. They need to push or pull content from another node in the overlay network (which includes other UNaDas as well as original content providers, e.g. a cloud service). Then, they need to be able to intercept requests from end users to directly serve cached content. Based on the load and location of the home router, content requests can also be redirected to other nodes in the overlay. Thus, load balancing and traffic management can be established, and service quality is assured.

B. Online Social Network Application

The major innovation of HORST is the OSN application which provides input for all traffic management mechanisms. It allows for the utilization of the convenient and well-known user management of the OSN. Thus, to participate in HORST users simply log on with their OSN credentials and grant permissions to the app. The required permissions include access to personal data, communication data, and position data. Moreover, users have to specify information about their home router, i.e. WiFi SSID, WiFi and UNaDa access passwords, home router position, and IP address.

Furthermore, the OSN app provides a mechanism to compute trust scores. This may be an explicit rating of other users, i.e. a user indicates which other users she does or does not trust, or an implicit mechanism in which the app computes trust scores based on OSN topology, personal data, and communication data (cf. Section III-D). Users could then set a rule e.g. to automatically trust all users which have a score above a certain threshold. Moreover, also a combination of explicit and implicit mechanisms is possible, e.g. a system which recommends trustworthy users which have to be confirmed explicitly.

Users who want to get access to another WiFi have to send a request to the owner. If the owner trusts the user, she can get the WiFi credentials and access the new WiFi. While users are moving, the app can analyze their position data and recommend or automatically request access to near WiFis. An incentive mechanism which rewards users for sharing of their home router still has to be developed, e.g. a credit point system in which users gain credit points for each share, but have to pay some credit points for each request. This mechanism should also take into account users who have no router to share but also want to participate in HORST for improved QoE.

With the OSN app, information about users (interests, preferences, position) and content (popularity, social cascades) can be gathered and exploited for enhanced traffic management. First, popular content can be detected and distributed over the network of UNaDas on the home routers to minimize delay and increase reliability. Additionally, content access patterns can be taken into account, such that the content can be distributed more efficiently for network operators, e.g. during non-peak hours. Second, depending on the importance and sensitivity of the content, it is possible to share and distribute content only to UNaDas of trusted users. Finally, the same mechanisms can be used in combination with users' location data to prefetch or cache content which is interesting for a specific user, on that home router to which she already is or soon will be connected. Here again, it would be possible that a user explicitly indicates the content she wants to consume, the time of consumption, and the home router to which it shall be transported.

To put it in a nutshell, based on the information from the OSN, HORST allows for efficient user-centric content placement which minimizes the distance between content and users, reduces loading times, and thus increases the users' QoE. Additionally, it takes into account when and where the content is accessed, which makes it possible to utilize the resources of network operators more efficiently.

C. Mobile Device Application

Instead of using the OSN app in a browser, a mobile device application makes the usage of HORST more natural. The mobile device automatically provides the needed data to the HORST app (e.g. position), such that the user can benefit without the need to be constantly engaged and manually upload information. Moreover, the mobile device app not only requests the WiFi credentials from the OSN app, but also stores them on the device for automatic connection to the WiFi network. It manages the handover between different interfaces (3G, WiFi) or between different access points. Finally, it includes a transmission scheduler which manages for both upload and download, whether content is more or less delay-tolerant, and whether it can or cannot be offloaded to a WiFi network.

V. Discussion

In this paper we presented the concept of a socially-aware traffic management solution which builds on home router sharing based on trust. Our solution addresses three important use cases data offloading, content caching/prefetching, and content delivery, and aims at providing a win-win situation for both end users and network operators. Previous results from literature suggest that there is great potential to reach this goal.

However, a detailed stakeholder analysis and evaluation of the optimization potential of HORST is due to be done. The performance of our approach has to be evaluated by models and simulations to quantify the gain in terms of energy efficiency, network operator savings, and end user QoE. Firmware, OSN app, mobile device app, and the respective interfaces have to be developed and implemented. Furthermore, an incentive mechanism is needed and algorithms for the computation of trust, recommendations (of both trusted users and near WiFis), and content distribution have to be designed and integrated.

Finally, to test the performance of HORST, a small scale deployment of the solution is planned. Some of this future work will be conducted in the FP7 SmartenIT (Nov 2012 - Oct 2015) which focuses on socially-aware management of new overlay application traffic combined with energy efficiency in the Internet. Thus, in the talk we will raise discussion on the applicability of HORST and foster its further development.

References

[1] Cisco, "Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2012-2017," Tech. Rep., 2013.

[2] Wireless Broadband Alliance, "WBA Industry Report 2011: Global Developments in Public Wi-Fi," Tech. Rep., 2011.

[3] L. Mamatas, I. Psaras, and G. Pavlou, "Incentives and Algorithms for Broadband Access Sharing," in *ACM SIGCOMM Workshop on Home Networks*, 2010.

[4] N. Sastry, J. Crowcroft, and K. Sollins, "Architecting Citywide Ubiquitous Wi-Fi Access," in *6th Workshop on Hot Topics in Networks*, 2007.

[5] P. Vidales, A. Manecke, and M. Solarski, "Metropolitan Public WiFi Access Based on Broadband Sharing," in *Mexican Intl. Conf. on Computer Science (ENC)*, 2009.

[6] C. B. Lafuente, X. Titi, and J.-M. Seigneur, "Flexible Communication: A Secure and Trust-Based Free Wi-Fi Password Sharing Service," in *IEEE 10th Intl. Conf. on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2011.

[7] N. Laoutaris, P. Rodriguez, and L. Massoulie, "ECHOS: Edge Capacity Hosting Overlays of Nano Data Centers," *ACM SIGCOMM Computer Communication Review*, 2008.

[8] V. Valancius, N. Laoutaris, L. Massoulié, C. Diot, and P. Rodriguez, "Greening the Internet with Nano Data Centers," in *5th Intl. Conf. on Emerging Networking Experiments and Technologies*, 2009.

[9] J. He, A. Chaintreau, and C. Diot, "A performance evaluation of scalable live video streaming with nano data centers," *Computer Networks*, 2009.

[10] A. J. Mashhadi and P. Hui, "Proactive Caching for Hybrid Urban Mobile Networks," Tech. Rep., 2010.

[11] E. Koukoumidis, D. Lymberopoulos, K. Strauss, J. Liu, and D. Burger, "Pocket cloudlets," *ACM SIGARCH Computer Architecture News*, 2011.

[12] B. Stiller, D. Hausheer, and T. Hoßfeld, "Towards a Socially-Aware Management of New Overlay Application Traffic Combined with Energy Efficiency in the Internet (SmartenIT)," in *The Future Internet (LNCS 7858)*, 2013.

[13] N. Sastry, E. Yoneki, and J. Crowcroft, "Buzztraq: predicting geographical access patterns of social cascades using social networks," in *2nd ACM EuroSys Workshop on Social Network Systems*, 2009.

[14] S. Scellato, C. Mascolo, M. Musolesi, and J. Crowcroft, "Track Globally, Deliver Locally: Improving Content Delivery Networks by Tracking Geographic Social Cascades," in *20th Intl. Conf. on World Wide Web*, 2011.

[15] S. Traverso, K. Huguenin, I. Triestan, V. Erramilli, N. Laoutaris, and K. Papagiannaki, "Tailgate: handling long-tail content with a little help from friends," in *21st Intl. Conf. on World Wide Web*, 2012.

[16] Z. Li, H. Shen, H. Wang, G. Liu, and J. Li, "SocialTube: P2P-assisted video sharing in online social networks," in *IEEE INFOCOM*, 2012.

[17] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, "The Eigentrust algorithm for reputation management in P2P networks," in *12th Intl. Conf. on World Wide Web*, 2003.

[18] X. Liu, A. Datta, K. Rzadca, and E.-P. Lim, "Stereotrust: a group based personalized trust model," in *18th ACM Conf. on Information and Knowledge Management*, 2009.

[19] F. E. Walter, S. Battiston, and F. Schweitzer, "Personalised and dynamic trust in social networks," in *3rd ACM Conf. on Recommender Systems*, 2009.

[20] J. Chandra, I. Scholtes, N. Ganguly, and F. Schweitzer, "A Tunable Mechanism for Identifying Trusted Nodes in Large Scale Distributed Networks," in *IEEE 11th Intl. Conf. on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2012.