A Framework for Self-Healing Home Networks

Amy Csizmar Dalal
Department of Computer Science, Carleton College
Northfield, MN, 55057
Email: adalal@carleton.edu

***Abstract*—Self-healing networks, or computer networks that can detect existing or potential pathologies and mitigate them with minimal human intervention, are particularly attractive in the home networking space, as home networks are heterogeneous and are typically configured and maintained by non-experts. Home networks greatly benefit from the ability to independently detect and mitigate issues with minimal user intervention. In this work in progress paper, we propose a *proactive* framework for a self-healing home network that detects and mitigates network pathologies that may lead to reduced application QoE. The framework collects and analyzes both application-level and network-level data to assessing the current "health" of the home network. In addition, the framework will apply a set of heuristics to determine the best course of action to take when presented with a set of network conditions.**

I. Introduction

Self-healing networks are computer networks that can detect existing or potential pathologies and mitigate them with minimal human intervention. Because such pathologies are visibly evident in end-users' quality of experience (QoE) of networked applications, self-healing networks are responsive to the needs of these applications. Self-healing networks are particularly attractive to the home networking space. Home networks are typically configured and maintained by non-experts who have a limited understanding of network topologies, performance, and pathologies, much less how to troubleshoot and fix their networks. Thus, home networks greatly benefit from the ability to independently detect and mitigate issues with minimal user intervention. Home networks are highly heterogeneous. The exact mix of devices within a particular home network, along with the particular mix of applications within each network, can vary widely both between and within home networks, as can the type of connection between the home network and the home ISP, making network administration, monitoring, and measurement difficult.

Previous research on home networks focuses on performance issues [1], [2], architectural concerns [3], and reactive troubleshooting of existing topologies [4]–[7]. An ideal self-healing network reacts to existing network pathologies but also *proactively* discovers and mitigates network conditions that are likely to result in future degraded QoE. To do so, the network needs to utilize a mix of network-level measurements, such as packet loss, and application-level measurements, such as the packet arrival rate to a video application or the frame rate of a videoconference call.

In previous work [8]–[10], we demonstrate that application-layer measurements such as received packets, bandwidth, and frame rate, can discern the user-perceived quality of a video stream with a high degree of accuracy in short time scales with small amounts of data, making the idea of real-time video QoE prediction with minimal user intervention feasible. We leverage this work to develop a measurement framework and set of tools (Section II) that will collect and analyze, using statistical and data mining techniques similar to those used in our previous work, both application-level and network-level data to assess the current state or "health" of the home network. In addition, the framework will apply a set of heuristics to determine the best course of action to take when presented with a set of network conditions. We describe several of these scenarios in Section III. We conclude by discussing some challenges in the design of such a framework (Section IV).

II. System Architecture

Figure 1 illustrates the proposed framework. The framework is partially decentralized, with some functionality on the devices and others on the router or gateway of the home network.

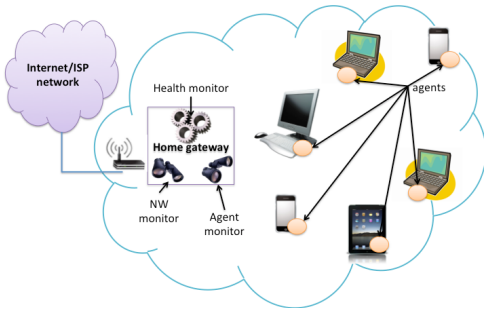

Fig. 1. The proposed self-healing home network framework.

1) On the gateway: The gateway entities control and manage the operation of the entire system.

Health monitor: The health monitor coordinates the activities of the network monitor and agent monitor. It receives and processes updates from the network monitor and the agent monitor, and uses these to calculate the current state, or "health" of the home network. It directs the network monitor and agent monitor to modify their monitoring activity based on the current state, including modifying the frequency of measurements and the quantities to measure.

Network monitor: The network monitor takes periodic measurements of the network state, using ping and other

widely available tools. It supplements the application measurements collected by the agents to form a complete picture of home network health. It updates the health monitor with the current network state, typically a summary report of current conditions including packet loss, host responsiveness, and current bandwidth usage.

Agent monitor: The agent monitor coordinates the measurement activity of the application agents. It communicates with the agents currently running on each device, and directs the agents to increase or decrease monitoring activity, depending on the current state of the network. The agent monitor also processes the incoming agent measurements, using data mining and/or statistical techniques to discover trends in the data.

2) On the devices: The devices in the home network host monitoring agents to determine the current quality of experience, as seen by the end user through the eyes of the applications the end user is actively using. These agents will collect QoE measurements in a similar manner to the video measurement tools we have designed and deployed previously, by hooking into the applications themselves. The agents detect which applications are running and have the user's focus, and start or wake the appropriate application hooks to collect data from these applications. They modify their sampling rates, the state data collected, etc., based on information sent back from the agent monitor.

III. Scenarios

Status quo The network monitor periodically polls the network to determine network state. The agent monitor polls the set of known devices to determine which devices are on and what applications they are running, analyzing data from the application agents. The health monitor uses this and network state data to derive a health score for the network as a whole and for particular applications and devices. Assuming these scores are acceptable, the system remains dormant until the next measurement period. Measurements over time reveal typical network conditions and QoE for *this network*.

Bandwidth hog? A common use case in the literature is allocating bandwidth to applications and devices within the home network [11]. Application agents measure the bandwidth used by active applications. Using application bandwidth usage and current network capacity information, the health monitor applies strategies to allocate bandwidth according to preset heuristics (for instance, streaming video gets a higher proportion unless there's a Skype call in the home office).

Sudden outage A router on the path to a game server goes down while a user is playing an online game. The network monitor detects higher delays and increasing packet losses, and collects targeted measurements to verify that the fault lies outside the home network. The health monitor identifies other potential game servers and automatically switches the user to another server before game QoE degrades. As a last resort, the health monitor sends a message to the gamer's device advising the user to manually try another server or to resume gameplay later.

IV. Challenges

Timing During normal operations, measurements can be infrequent, but not so infrequent as to miss potential pathologies. The frequency of measurements must also not overwhelm the network as conditions degrade.

Data freshness The system refers to historical data to predict the likely QoE level from a given set of network conditions. How much should the system favor recent measurements over past measurements, and how long should past data be archived?

Privacy Sharing data with outsiders, such as the home's ISP, can mitigate problems within the home network, but this data exposes sensitive information (devices on the network, web sites visited, applications in use, etc). One solution is to distill the set of current home network conditions into one of a number of predefined scenarios to capture the essence of network state without revealing sensitive information.

Third-party cooperation Besides the privacy issues outlined above, ISPs are concerned with liability from not fulfilling service contracts with end users, as well as protecting trade secrets. Agreements as part of the service contract can be brokered between the ISP and home user to address some of these issues.

References

[1] L. DiCioccio, R. Teixeira, and C. Rosenberg, "Characterizing home networks with HomeNet Profiler," UPMC Sorbonne Universits, Tech. Rep. CP-PRL-2011-09-0001, 2011.

[2] C. Kreibich, N. Weaver, G. Maier, B. Nechaev, and V. Paxson, "Experiences from netalyzr with engaging users in end-system measurement," in *Proceedings of the 1st ACM SIGCOMM Workshop on Measurements up the Stack (WMUST)*, New York, NY, 2011, pp. 25–30.

[3] K. L. Calvert, W. K. Edwards, and R. E. Grinter, "Moving toward the middle: The case against the end-to-end argument in home networking," in *Sixth Workshop on Hot Topics in Networks*, Atlanta, GA, 2007.

[4] K. L. Calvert, W. K. Edwards, N. Feamster, R. E. Grinter, Y. Deng, and X. Zhou, "Instrumenting home networks," *SIGCOMM Comput. Commun. Rev.*, vol. 41, no. 1, pp. 84–89, 2011.

[5] C. Dong and N. Dulay, "Argumentation-based fault diagnosis for home networks," in *Proceedings of the 2nd ACM SIGCOMM workshop on Home Networks (HomeNets)*, New York, NY, 2011, pp. 37–42.

[6] M. Chetty, D. Haslem, A. Baird, U. Ofoha, B. Sumner, and R. Grinter, "Why is my Internet slow?: making network speeds visible," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*, New York, NY, 2011, pp. 1889–1898.

[7] T. Karagiannis, E. Athanasopoulous, C. Gkantsidis, and P. Key, "HomeMaestro: Order from chaos in home networks," Microsoft Research, Tech. Rep. MSR-TR-2008-84, 2008.

[8] A. Csizmar Dalal, A. Bouchard, S. Cantor, Y. Guo, and A. Johnson, "Assessing QoE of On-Demand TCP Video Streams in Real Time," in *Proceedings of the IEEE International Conference on Communications (ICC)*, Ottawa, Ontario, Canada, June 2012.

[9] H. French, J. Lin, T. Phan, and A. Csizmar Dalal, "Real time video QoE analysis of RTMP streams," in *Proceedings of the 30th IEEE International Performance Computing and Communications Conference (IPCCC)*, Orlando, FL, November 2011.

[10] A. Csizmar Dalal, "User-perceived quality assessment of streaming media using reduced feature sets," *ACM Transactions on Internet Technology*, vol. 11, no. 2, December 2011.

[11] M. Chetty, R. Banks, R. Harper, T. Regan, A. Sellen, C. Gkantsidis, T. Karagiannis, and P. Key, "Who's hogging the bandwidth: The consequences of revealing the invisible in the home," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*, New York, NY, 2010, pp. 659–668.