Computer Networks 65 (2014) 84–98

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

Survey Paper

Network monitoring: Present and future

Sihyung Lee [a,*], Kyriaki Levanti [b], Hyong S. Kim [c]

[a] Seoul Women's University, 621 Hwarangro, Nowon-Gu, Seoul 139-774, South Korea
[b] Amazon.com, Inc., 410 Terry Avenue North, Seattle, WA 98109, USA
[c] Carnegie Mellon University, 5000 Forbes Ave., Pittsburgh, PA 15213, USA

ARTICLE INFO

Article history:
Received 22 February 2013
Received in revised form 4 March 2014
Accepted 17 March 2014
Available online 24 March 2014

Keywords:
Network configuration
Design
Management
Measurements
Monitoring

ABSTRACT

Network monitoring guides network operators in understanding the current behavior of a network. Therefore, accurate and efficient monitoring is vital to ensure that the network operates according to the intended behavior and then to troubleshoot any deviations. However, the current practice of network-monitoring largely depends on manual operations, and thus enterprises spend a significant portion of their budgets on the workforce that monitor their networks. We analyze present network-monitoring technologies, identify open problems, and suggest future directions. In particular, our findings are based on two different analyses. The first analysis assesses how well present technologies integrate with the entire cycle of network-management operations: design, deployment, and monitoring. Network operators first *design* network configurations, given a set of requirements, then they *deploy* the new design, and finally they verify it by continuously *monitoring* the network's behavior. One of our observations is that the efficiency of this cycle can be greatly improved by automated deployment of pre-designed configurations, in response to changes in monitored network behavior. Our second analysis focuses on network-monitoring technologies and group issues in these technologies into five categories. Such grouping leads to the identification of major problem groups in network monitoring, e.g., efficient management of increasing amounts of measurements for storage, analysis, and presentation. We argue that continuous effort is needed in improving network-monitoring since the presented problems will become even more serious in the future, as networks grow in size and carry more data.

1. Introduction

Monitoring a network is crucial to network-management operations, and it is used for many critical tasks. A major function of network monitoring is early identification of trends and patterns in both network traffic and devices. According to these measurements, network operators understand the current state of a network and then reconfigure this network such that the observed state can be improved. For example, the operators find a dramatic increase of P2P traffic, which begins to drop most of the other packets. In response to this problem, operators initiate rate-limiting of P2P traffic. The operators may also find that vulnerability in database-servers allows illegitimate access to sensitive information, and then they begin to apply patches to the database servers. Late detection of such incidents can lead to prolonged disruption to services and financial losses up to millions of dollars [1].

Due to the significance of network-monitoring operations, an extensive amount of work was done to advance these operations. However, network operators still spend the most of their time monitoring and troubleshooting

* Corresponding author. Tel.: +82 2 970 5608; fax: +82 2 970 5974.
E-mail addresses: sihyunglee@swu.ac.kr (S. Lee), kiki.levanti@gmail.com (K. Levanti), kim@ece.cmu.edu (H.S. Kim).

http://dx.doi.org/10.1016/j.comnet.2014.03.007
1389-1286/

problems in their networks [2]. Network outages continue to occur and prevent access to networks for several hours. For example, more than three hours of outages were reported in both Amazon [3] and YouTube [4] networks. As a result, enterprise networks spend an increasing amount of their IT budget in network monitoring, rather than to add new value-adding services and equipment [5].

Considering the significance and complexity of network monitoring, we identify challenges in network monitoring, summarize existing solutions, and suggest future directions for dealing with the challenges. This was performed by analyzing existing works published in 8 journals and the proceedings of 13 conferences[1] for the past 15 years (i.e. from January 1998 till December 2013), and by then selecting a set of significant challenges. This paper can be used in several different ways. It can help researchers better understand missing points in current practices of network monitoring and thus conceive new ideas that can improve the status quo. This paper can also be used to study a wide range of monitoring operations and their relationship with other network-management operations. We summarize the suggested guidelines in Table 1.

The scope of this paper is the management of one administrative domain in the Internet, and it covers different types of networks, such as ISPs, enterprise networks, and campus networks. Potential readers of this paper include researchers, network operators, as well as students.

Related work: A few surveys on network management exist, but their main focus is different from this paper. Some of these surveys are dedicated to sub-topics discussed in this paper [6,7]. Other surveys present several network-management issues in general [8,9]. In contrast, this paper is aimed at presenting a holistic view of network-monitoring operations. To this end, we examine both the internals of monitoring operations (e.g., efficiency improvement in packet sampling) and monitoring in relationship with other operations (e.g., automation of the interaction between monitoring and configuration design). [6] introduces several monitoring functions that analyze network traffic, such as traffic classification and application discovery. [7] presents an overview of one particular function of network monitoring, fault localization. The functions presented in [6,7] are components of the analysis layer, one of the five layers of monitoring, as we discuss in Section 3.5. [8,9] summarize several network-management issues, some of which are related to network monitoring (e.g., efficient storage of packet measurements in the face of large traffic volume). These issues are also discussed in this paper. To summarize, this paper focuses on network-monitoring operations, covering a wide range of problems in network monitoring.

The following sections are designed to analyze monitoring from a few different angles, in order to identify diverse areas that can be improved in monitoring. In Section 2, we present the position of monitoring in relationship with other network-management operations. We then utilize this relationship and suggest guidelines that improve monitoring. Sections 3 and 4 delve into monitoring operations and classify these operations into five different categories according to their functions. In particular, Section 3 describes challenges for each of the five categories, and Section 4 presents the challenges that are shared by multiple categories. The two sections also highlight existing solutions and future research directions. Finally, we summarize the proposed research directions and conclude in Section 5.

2. Monitoring within the big picture of network management

In Section 2.1, we first position monitoring in the entire cycle of network-management operations. This positioning of monitoring is then used in Section 2.2 for analyzing interactions between monitoring and other network-management operations. According to this analysis, we suggest guidelines for improving the operational cycle as a whole. The positioning of monitoring in Section 2.1 can also serve as background information on network monitoring.

2.1. Position of monitoring in the operational cycle of network management

To better understand the limitations of current network-management practices and to identify areas of improvement, we position monitoring within a sequence of operations that are performed as a network evolves: design, deployment, and monitoring. Fig. 1 depicts the three groups of operations and their interactions. We first describe two types of data sources that are frequently used in the three groups of operations. We then explain the details of the three groups and their interactions.

In managing networks, network operators use two types of data sources: *measurements* and *configurations*. Measurements show a network's current behavior, and they include packets collected at different vantage points as well as dynamic device-specific information, such as CPU load and forwarding table entries in a router. The configuration of a network device is a set of device-specific commands and parameters. These commands and parameters specify the device's intended behavior: how the device should operate, which protocols should be running, and what values the protocol options should take. Configurations also include information about the physical and logical connectivity between the network's devices.

Measurements and configurations are used by the three operational groups in the following ways. The *monitoring* operations collect measurements and analyze them, in order to infer the current behavior of a network. By considering this current behavior, the *design* operations create necessary changes in configuration and infrastructure. These changes help fulfill requirements specific to the network (e.g., evenly distribute traffic over N links).[2] The

[1] The 8 journals include Springer JNSM, Wiley IJNM, ACM CCR, IEEE TNSM/ToN/JSAC/Network/Communications.The 13 conferences include IFIP/IEEE IM/NOMS/CNSM, USENIX LISA/NSDI, ACM SIGCOMM/CoNEXT, IEEE POLICY/INFOCOM/DSN/Globecom/ICC/VizSec.

[2] Goals, requirements, and intended behavior (and consequently, configurations) are the results of network design. The network design takes requirements from applications and maps them to physical infrastructure setup, configurations, and goals on the operations.