Comparative Analysis of Different Protocols to Manage Large Scale Networks

Anil Rao Pimplapure[1], Prashant Sen[2], Dr Jayant Dubey[3]
Assistant Professor, Department of Computer Science and Engineering of
BTIRT Sagar M.P., India[1 & 2]
Professor and Head, Department of Computer Science and Applications,
BTIRT, Sironja, Sagar[3]
pimpu123@rediffmail.com, prashantsen@yahoo.com, drjayantdubey@gmail.com

Keywords: Large Scale Networks, Simple Network Management Protocol

Abstract

In recent year the numbers, complexity and size is increased in Large Scale Network. The best example of Large Scale Network is Internet, and recently once are Data-centers in Cloud Environment. In this process, involvement of several management tasks such as traffic monitoring, security and performance optimization is big task for Network Administrator. This research reports study the different protocols i.e. conventional protocols like Simple Network Management Protocol and newly Gossip based protocols for distributed monitoring and resource management that are suitable for large-scale networked systems. Results of our simulation studies indicate that, regardless of the system size and failure rates in the monitored system, gossip protocols incur a significantly larger overhead than tree-based protocols for achieving the same monitoring quality i.e., estimation accuracy or detection delay.

1. Introduction

To meet the growing and evolving requirements of management applications, equipment vendors and administrators now-a-days depend on incremental solutions. This increases the complexity of network elements and deployment costs for operators. However, in spite this increased complexity and cost, there is still a significant gap between the policy objectives of system administrators and the capabilities provided by today's mechanisms. A key concern in achieving these high-level objectives is that the network elements like routers, middle boxes that enable such management tasks have constraints on processing, memory and storage capabilities. Even though network devices are becoming more powerful with advances in technology, the traffic workloads and usage patterns are scaling nearly as fast as these technology advances. Thus, these resource constraints are fundamental. As a result, these network management tasks can be broadly viewed as resource management problems in large networked systems. Having cast the management tasks as resource management problems, we argue that the policy goals can be best achieved using a network-wide approach rather than a device centric approach. The network-wide approach we advocate in this thesis is based on three guiding principles:

1.1 Systematic selection and placement of device-level primitives.

1.2 Lightweight coordination mechanisms that enable different network elements to effectively complement each other.

1.3 Practical optimization models that capture operating constraints and policy objectives and produce close to optimal ways to configure the device-level primitives within their technological constraints.

At a high-level, we can think of this approach as being a middle ground between the configuration and analysis and the new middle boxes and router primitives approaches, i.e. we need practical, efficient primitives that do not significantly increase the complexity and resource requirements of network elements and frameworks to reason about how to configure/analyze these primitives to meet the high-level objectives of network operators.

2. Motivation

The size and complexity of large-scale networked systems (LNSs) has grown fast over the last decade, and this trend is expected to accelerate further. The Internet, for instance, is now expected to connect over billion devices, a number that will likely grow to some 22 billion by 2020. Using the internet as a basis, other LNSs are emerging. Examples include peer-to-peer file sharing networks, which are expected to be the second largest source of traffic in the coming five years, according to a Cisco study. Another example is the Skype network, the largest peer-to-peer Voice over Internet Protocol (VoIP) network, which currently counts 124 million unique users each month. The latest manifestations of LNSs are datacenters that provide cloud computing services. Some datacenters that are currently built will contain hundreds of thousands of servers. Cloud services follow a paradigm where resource demanding computation is moved from end-user devices (e.g., desktops, laptops and smart phones) to datacenters that are owned and operated by a third party. This paradigm is attractive for users of the service, as it gives them dynamic access to resources and satisfies their changing needs. It enables cloud service providers to exploit the economy of scale, as the cost per machine falls for increasingly large datacenters. The LNSs outlined above cannot be effectively and efficiently managed using traditional management systems that follow a centralized management paradigm. This is because the number of states and events that need to be monitored, as well as the number of control actions that need to be determined and executed become too large to handle. As a result, there is an urgent need for new management solutions that scale with the size of the managed system.

3. Technology

Network management challenges arise in domains such as Internet Service Providers (ISPs), enterprise networks, and data centers. Each domain involves several management tasks such as traffic monitoring, security and performance optimization. These management applications have natural high-level policy goals. For example, network operators may want: (1) good monitoring coverage in order to understand end-to-end traffic patterns for detecting anomalous patterns, (2) effective configurations for application acceleration services in order to provide good end-to-end performance for their customers, and (3) effective deployment of intrusion detection and prevention systems to detect and drop malicious traffic as efficiently as possible. However, as networks and traffic patterns evolve, the set of management applications and the requirements of existing applications change as well. This implies the need for new functions, more fine-grained capabilities, and more scalable solutions to understand and adapt to these changes. To put the work presented in this thesis in perspective, we discuss some possible approaches available to network operators today to meet the growing demands of network management applications.

4. Applications

The most common and easiest solution is for network operators to deploy techniques to work with existing router primitives. Router vendors (e.g., Cisco, Juniper) have provided in-built support in terms of configuration tools and router commands to support specific tasks like routing and access control. ISPs and enterprise networks also develop a suite of in-house analysis and configuration tools to simplify such functions. These include techniques that provide support for better traffic engineering and routing configurations, techniques for inferring patterns of interesting traffic activity from existing measurement feeds, and accounting for potential biases in measurements. Because such techniques do not require additional support from network elements, they are easy to develop and inexpensive to deploy. However, it might not always be possible to develop such tools. Often, management applications need new capabilities that might not be available on existing network elements. In such cases, network operators can deploy middle boxes developed by third party vendors. For example, these are commonly used for providing new security features and for performance acceleration. Unfortunately, such solutions have a narrow scope and each new application context requires additional middle boxes. Further, because these are often proprietary solutions, they run the risk of becoming “black-boxes” to network operators. Further down the cost/development cycle is for router vendors to integrate the requisite functionality directly. There are several proposals for better monitoring algorithms in-depth forensic capabilities, new diagnostic primitives, more efficient data structures etc. While these avoid the problems of having too many middle-boxes inside the network, they require router vendors and network managers to commit to a fixed set of capabilities without knowing if these will meet future application requirements.

5. Challenges

We have identified three properties of a management system that is suitable for LNSs. The first property is architectural and suggests using a decentralized management architecture where basic monitoring and control functions are pushed into the managed system and thus enable scalable operation and short reaction times. The research challenge here is the engineering of management protocols that can run in such a distributed setting. The second property relates to how the managed system is abstracted and calls for functions that can efficiently estimate the global state and how it evolves over time. The challenge here is to develop accurate and efficient protocols for the monitoring of global state variables that are computed from local state variables. The third property relates to how state variables are accessed for monitoring purposes and advocates a push approach, in contrast to the pull approach that is ubiquitous in traditional management systems. It states that the managed system itself should identify and push updates and alerts to the management system, which allows it to quickly take appropriate actions. Despite the increased complexity and cost, the challenges of network administrator are;

5.1 Accuracy requirement in traffic monitoring

5.2 Implementation of reducing of redundancy to improve the performance of network and

5.3 Management of intrusion detection.

5.4 The protocol uses the system resources for applications which are hosted through the cloud.

5.5 The resource allocation computed by the protocol converges exponentially fast to an optimal allocation of system resources by the different protocols.

5.6 Validation of quality of allocated resources and compare protocols with increasing in application for distributed management system. Results of protocols for achieving the same monitoring quality in terms of accuracy and detection delay

6. Related Work

The design of cSamp as a centrally managed network-wide monitoring system is inspired by recent trends in network management. In particular, recent work has demonstrated the benefits of a network-wide approach for traffic engineering and network diagnosis. Other recent proposals suggest that a centralized approach can significantly reduce management complexity and operating costs. Despite the importance of network-wide flow monitoring, there have been few attempts in the past to design such systems. Most of the related work focuses on the single-router case and on providing incremental solutions to work around the limitations of uniform packet sampling. This includes work on adapting the packet sampling rate to changing traffic conditions, tracking heavy-hitters, obtaining better traffic estimates from sampled measurements, reducing the overall amount of measurement traffic, and data streaming algorithms for specific applications. Early work on network-wide monitoring has focused on the placement of monitors at appropriate locations to cover all routing paths using as few monitors as possible. In contrast, cSamp assumes a given set of monitoring locations along with their resource constraints and, therefore, is complementary to these approaches. There are extensions to the monitor-placement problem to incorporate packet sampling. While the optimization formulations in these share some structural similarity to our approach, the specific contexts in which these formulations are applied are different. First, cSamp focuses on flow sampling as opposed to packet sampling. By using flow sampling, cSamp provides a generic flow measurement primitive that subsumes the specific traffic engineering applications that packet sampling (and the frameworks that rely on it) can support. Second, while it is reasonable to assume that the probability of a single packet being sampled multiple times across routers is negligible; this assumption is not valid in the context of flow-level monitoring. The probability of two routers sampling the same flow is high as flow sizes follow heavy-tailed distributions. Hence, cSamp uses mechanisms to coordinate routers to avoid duplicate flow reporting. To reduce duplicate measurements, Sharma and Byers suggest the use of Bloom filters. While minimizing redundant measurements is a common high-level theme between cSamp and their approach, our work differs on two significant fronts. First, cSamp allows network operators to directly specify and satisfy network-wide objectives, explicitly taking into account (possibly heterogeneous) resource constraints on routers, while their approach does not. Second, cSamp uses hash-based packet selection to implement coordination without explicit communication, while their approach requires every router to inform every other router about the set of flows it is monitoring.

7. Design Objectives & Dissertation Outline

As the previous discussion shows, to meet the growing and evolving requirements of management applications, equipment vendors and administrators today depend on incremental solutions. This increases the complexity of network elements and deployment costs for operators. However, in spite this increased complexity and cost, there is still a significant gap between the policy objectives of system administrators and the capabilities provided by today’s mechanisms. In particular, administrators have high-level network-wide objectives are often difficult to translate into router/device configurations that will meet the goals. Our hypothesis, in the spirit of the recent proposals for centralized network management is that much of the disconnect between the goals of network operators and the tools available to them arises from the narrow device centric view of current solutions. Such piecemeal solutions are inefficient: network elements duplicate tasks and some locations become overloaded. Worse still, administrators struggle to implement their high-level goals within device-centric configurations. A key concern in achieving these high-level objectives is that the network elements (e.g., routers, middle boxes) that enable such management tasks have constraints on processing, memory, and storage capabilities. We validate that the quality of the allocation does not change with increasing the number of hosted applications and machines, for the case where both metrics are scaled proportionally. We compare two approaches Simple Network Management Protocol and gossip-based to engineering protocols for distributed management, for the case of real-time monitoring. Results of our simulation studies indicate that, regardless of the system size and failure rates in the monitored system, gossip protocols incur a significantly larger overhead than tree-based protocols for achieving the same monitoring quality i.e., estimation accuracy or detection delay.

8. Conclusion

To achieve the goal we will be going to collect the primary data from different ISPs and analytical study will be done by using some mathematical and statistical tools. Some graphical representation will also be done to relate the study, if possible. The research will deal with resource management in Large Scale Networks based on the following three principles as under;

1. The approaches of SNMP & Gossip based Protocol for resource management in large scale networks
2. Coordination mechanisms of to enable network elements to effectively complement
3. Operating constraints and policy objectives.

Bibliography

- C. Adam and R. Stadler. Service middleware for self-managing large-scale systems. IEEE Transactions on Network and Service Management, 4(3):50-64, April 2008.
- IBM WebSphere Application Server, 2010. http://www.ibm.com/software/webservers/appserv/extend/virtualenterprise/.

- Bob hash. http://burtleburtle.net/bob/hash/doobs.html.
- Cisco Wide Area Application Acceleration Services. http://www.cisco.com/en/US/products/ps5680/Products_Sub_Category_Home.%html
- Narus Intercept Solution. http://www.narus.com/index.php/solutions/intercept.
- PAPI: Performance Application Programming Interface. http://icl.cs.utk.edu/papi/.
- A. Anand and C.Muthukrishnan and A. Akella and R. Ramachandran. Redundancy in Network Traffic: Findings and Implications. In Proc. of SIGMETRICS, 2009.
- A. Chakrabarti, K. Do Ba, and S. Muthukrishnan. Estimating entropy and entropy norm on data streams. In Proceedings of the 23rd International Symposium on Theoretical Aspects of Computer Science (STACS), 2006.
- A. Anand, V. Sekar, and A. Akella. SmartRE: An Architecture for Coordinated Network-Wide Redundancy Elimination. In Proc. SIGCOMM, 2009.
- G. R. Cantieni, G. Iannaccone, C. Barakat, C. Diot, and P. Thiran. Reformulating the Monitor Placement problem: Optimal Network-Wide Sampling. In Proc. Of CoNeXT, 2006.
- Dimitri P. Bertsekas and John N. Tsitsiklis. Parallel and distributed computation: numerical methods. Prentice-Hall, Inc., Upper Saddle River, NJ, USA,1989.
- Ken Birman. The promise, and limitations, of gossip protocols. SIGOPS Operating Systems Review, 41(5):8-13, 2007.
- David Breitgand, Danny Dolev, and Danny Raz. Accounting mechanism for membership size-dependent pricing of multicast tra_c. In Networked Group Communication, pages 276-286, 2003.
- George Cybenko. Dynamic load balancing for distributed memory multiprocessors. Journal of Parallel and Distributed Computing, 7(2):279 - 301, 1989.
- M. Dilman and D. Raz. E_cient reactive monitoring. IEEE Journal on Selected Areas in Communications, 20(4):668-676, 2002.
- Robert Elssser, Burkhard Monien, and Robert Preis. Di_usion schemes for load balancing on heterogeneous networks. Theory of Computing Systems, 35:2002, 2002
- Jeroen Famaey, Wouter De Cock, Tim Wauters, Filip De Turck, Bart Dhoedt, and Piet Demeester. A latency-aware algorithm for dynamic service placement in large-scale overlays. In International Conference on Integrated Network Management, pages 414-421, Piscataway, NJ, USA, 2009. IEEE Press.
- B. Claise. Cisco Systems NetFlow Services Export Version 9. RFC 3954.
- M. P. Collins and M. K. Reiter. Finding Peer-to-Peer File-sharing using Coarse Network Behaviors. In Proc. of ESORICS, 2006.
- N. Duffield and M. Grossglauser. Trajectory Sampling for Direct Traffic Observation. In Proc. of ACM SIGCOMM, 2001.

- N. Duffield, C. Lund, and M. Thorup. Charging from sampled network usage. In Proc. of IMW, 2001.
- E. W. Fulp. Optimization of network firewalls policies using directed acyclic graphs. In Proc. Internet Management Conference, 2005.
- C. Estan and G. Varghese. New Directions in Traffic Measurement and Accounting. In Proc. of ACM SIGCOMM, 2002.
- D. Fisher, D. A. Maltz, A. Greenberg, X. Wang, H. Warncke, G. Robertson, and M. Czerwinski. Using Visualization to Support Network and Application Management in a Data Center . In Proceedings of INM, 2008.
- B. Fortz, J. Rexford, and M. Thorup. Traffic Engineering with Traditional IP Routing Protocols. IEEE Communications Magazine, Oct. 2002.
- J. Gonzalez, V. Paxson, and N.Weaver. Shunting: A Hardware/Software Architecture for Flexible, High-Performance Network Intrusion Prevention. In Proc. ACM CCS, 2007.
- R. Kompella and C. Estan. The Power of Slicing in Internet Flow Measurement. In Proc. of IMC, 2005.
- R. R. Kompella, S. Singh, and G. Varghese. On scalable attack detection in the network. In Proc. IMC, 2004.
- A. Lakhina, M. Crovella, and C. Diot. Diagnosing Network-Wide Traffic Anomalies. In Proc. of ACM SIGCOMM, 2004.
- M_ark Jelasity, Alberto Montresor, and Ozalp Babaoglu. T-man: Gossip-based fast overlay topology construction. Computer Networks, 53(13):2321-2339, 2009.

* * * * *