International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 1, Issue 2, No 1, 2013. ISSN: 2348-6600
Reference ID: IJCS-008 PAGE NO: 040-043

Finding Misconfigurations in Router and Network Using Minerals

S.Arockia Rubi [#1], M.Brindha Devi [*2]

[#1] *PG IN COMPUTER SCIENCE AND ENGINEERING*
NPR COLLEGE OF ENGINEERING AND TECH
NATHAM DINDIGUL,INDIA
arockiaruby.s@gmail.com

[*2] *PG IN COMPUTER SCIENCE AND ENGINEERING*
NPR COLLEGE OF ENGINEERING AND TECH
NATHAM DINDIGUL,INDIA
birunda.devi@gmail.com

Abstract— **The router misconfigurations are common and can have dramatic consequences to the operation of the network. Misconfigurations can compromise the security of an entire network or even cause disruption to the Internet connectivity. The solutions have been proposed can detect a number of problems in real configurations files. These solutions share a common limitation, based on rules which need to be known beforehand. In order to overcome these limitations, address the problem of router misconfigurations using data mining technique. More specifically, minerals using association rule mining. While association rule mining has traditionally applied to the configuration files of routers across an administrative domain to discover local, network specific policies. Deviations from these local policies are potential misconfigurations. The configuration files are user accounts, interfaces and BGP sessions.**

Index Terms-Association rules mining, error detection, network management, static analysis.

I.INTRODUCTION

Router configuration is a challenging and complex task. Configuration needs to set the policies for the router, which is followed by every packet that uses the router. The rules violations are known as misconfiguration. It occurs in many aspects that we used in configuration.

In this project, address the problem of router misconfigurations using data mining. This method applies association rules mining to the configuration files of routers across an administrative domain to discover local, network-specific policies. Deviations from these local policies are potential misconfigurations. This system evaluated our scheme on configuration files from a large state-wide network provider, a large university campus and a high-performance research network.

In this evaluation, we focused on three aspects of the configurations:

- User accounts
- Interfaces
- BGP sessions

User accounts specify the users that can access the router and define the authorized commands. Interfaces are the ports used by routers to connect to different networks. Each interface may support a number of services and run various routing protocols. BGP sessions are the connections with neighboring autonomous systems (AS). BGP sessions implement the routing policies which select the routes that are filtered and the ones that are advertised to the BGP neighbor.

II.OVERVIEW OF THE PROJECT

In this system, the router and network misconfigurations can be detected by the datamining. A mineral is the main concept. Steps are:

Published by SK Research Group of Companies (SKRGC).

International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 1, Issue 2, No 1, 2013. ISSN: 2348-6600
Reference ID: IJCS-008 PAGE NO: 040-043

- Minerals use association rules mining to detect misconfigurations.
- The conversion of configuration files into the format that is suitable to apply the association rule mining.
- The process to find the violations from the local policies.

III.MINERALS

Data mining can be used to identify errors in network configurations as well. Policies are usually applied across a network and evident in most routers in a network. Minerals use data mining to discover local rules of a network and detect potential misconfigurations that deviate from these rules. Local rules of a network can be complex and usually not captured by universal rules set forth by common best practice documents.

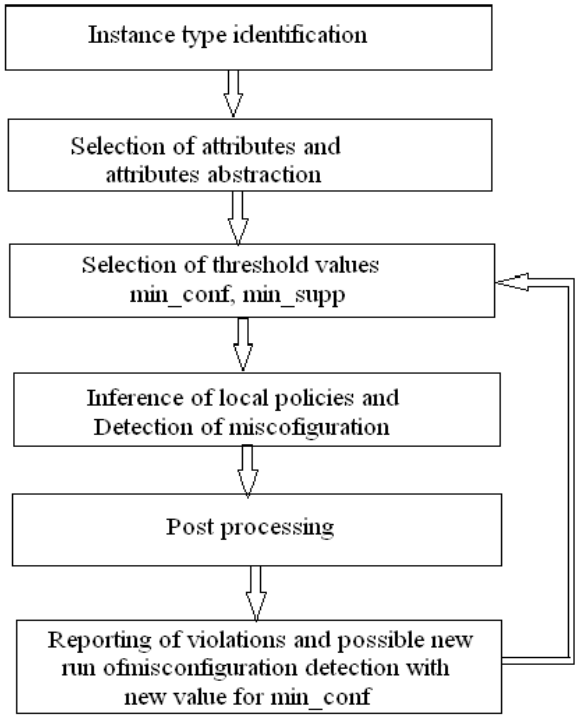

Fig. 1. Overview of the minerals

Open Shortest Path First (OSPF) protocol was deployed and one local policy consists in having all interfaces in passive mode by default and explicitly use the command no passive interface for backbone interfaces. This policy is to prevent users from injecting routes into the OSPF domain. Similarly, the network is deploying the Routing Information Protocol (RIP). The network has a number of subnets with user devices using RIP to learn their default paths. On non-backbone interfaces, the local policy mandates a distribute list out command so that only the default route would be sent out, and a distribute-list in command to ensure that routers do not accept announcements originated by user devices.

1. Preprocessing the Input Data

Routers‘configuration files are lists of commands and arguments that specify the routers‘behaviors. These files include the interfaces, the routing protocols, the remote access and all other aspects of a router‘s operations. However, those files have little structure and are not fit for data mining. This section describes a general method to process the data using domain knowledge into a representation for data mining.

- **Instance Type Identification**

Data mining techniques generally work on sets of instances. Each instance is characterized by a list of attributes. In Minerals, an instance type also represents a unit of error detection. We propose to divide the information in the network configuration into different instance types. Possible instance types include router, user account, interface, and BGP session.

- **Attribute Selection andAbstraction**

Even though an instance type is represented by a list of attributes, not all attributes are important and suitable for data mining we select attributes for each instance type so that only relevant information is retained. As an example, an interface can be characterized by the running routing protocols, the supported services, and the applied packet filters. Abstraction the type (e.g., Boolean, integer,string, etc.) that we select to represent the different attributes determines the rules and types of errors that will be discovered.

2. Background on Association Rule Mining

The association rules mining technique to detect anomalies in router configurations for the following reasons.

Published by SK Research Group of Companies (SKRGC).

International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 1, Issue 2, No 1, 2013. ISSN: 2348-6600
Reference ID: IJCS-008 PAGE NO: 040-043

- To be effective, network policies are usually applied on most or all objects of the same category across a network.
- Network policies can often be expressed as rules. For example, the policy "BGP sessions with external ASes must be authenticated" can be represented by the rule
- Deviations from local network policies can either be misconfigurations, nonconforming valid configurations, or temporary solutions, all of which should be audited periodically. At a high level, association rules mining examines the statistical properties of correlations present in a large data set.

3. Applying Association Rule Mining in Minerals and Post Processing

The network-specific local policies used to identify the potential misconfigurations.

- **An Algorithm to Infer Local Policies**

In Minerals, the generation of association rules and detection of violations from those rules consists of the following four steps.

Step1: Item Set Generation

For each instance type, this step generates all possible combinations of item sets, e.g., all 1-item item sets, 2-item item sets, etc., with the restriction that the support is over the threshold. A number of algorithms have been proposed by the data mining research community to compute item sets efficiently.

Step2: Interference of Local Policies

The goal of this step is to generate association rules. Minerals filters out rules with confidence values lower than the threshold as we want to find rules that are the most pertinent and more likely to be reflections of local policies. This step can also apply domain-specific knowledge to eliminate irrelevant rules and thus reduce the false alarm rate: if common sense says attribute cannot imply or be correlated with, we eliminate all rules of the form Even though this only needs to be done once and can be henceforth remembered by the minerals algorithm, it nevertheless can be labor intensive.

Step3: Violation Detection

Since we are focusing on misconfigurations, we do not consider rules with confidence equal to 1. Violations are instances that do not comply to a rule. The attribute that might be misconfigured is either in or usually, the rule has the expected, common value, whereas the violation has a potentially wrong value. We also eliminate rules that generate more than number of violations. The reason behind using is that the number of misconfigurations should be small in a network. If a rule results in a large number of violations, the violations are most probably not misconfigurations, and the rule unlikely to reflect a local policy. We use a simple default value of 10.

Step4: Filter and Support

The last step reports the identified violations in decreasing order of confidence. Since multiple rules can point to the same misconfigured instance, we only report the instance once and indicate the Rule with the Smallest Item Set Size on the Left Hand Side. Such An Operation Allows Focusing On The Attributes That Raised The Violations. Also, It Keeps The Rules Simple. Experience Shows That Those Rules Are Often Easier To Interpret

- **Selection Of Parameters**

Step1: Feedback Based Method

Because our approach assumes that the number of properly configured instances is high, should have a large value. It can be initialized to 0.99 and then incrementally decreased. After each run of Minerals, the network operator can provide direct feedback on whether and how a reported violation is a false alarm. The operator can indicate whether the discovered rule is or not a reflection of his network policy, and if the violation is an exception to a valid policy. This knowledge can then be fed back into subsequent runs of Minerals to filter rules and violations. The lists of rules and instances previously raised and confirmed as valid exceptions by the network operators are recorded. Subsequent results are then compared with these lists before being brought up to the attention of the operator.

Step2: Heuristic Based Method

Published by SK Research Group of Companies (SKRGC).

International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 1, Issue 2, No 1, 2013. ISSN: 2348-6600
Reference ID: IJCS-008 PAGE NO: 040-043

As an alternative, we can decide of the value of, based on the evolution of the number of reported violations as we decrease possible candidate values. For each value of, we apply the algorithms above to infer the local network-specific policies and then, we identify the instances that violate them. We apply a list of post-processing rules to eliminate several false alarms. As such, for each value of, we obtain a number of violations

Both the feedback-based and heuristic-based methods can be applied together. The heuristic-based technique can first be applied. Then, the feedback-based method canbe used to gradually decrease the values. Such approaches allow discovering errors while keeping the false positives and the number of analyses low.

After pre-processing the configurations and running our association mining algorithm on them, we apply a postprocessing step to filter the results. The goal is to reduce false alarms by demoting violations that are highly likely to be nonconforming, but valid configurations. The first post-processing step is related to routing policies and attempts to identify whether the policies for a group of neighbor routers in the same AS are nonconforming but intentional. Even though policies for a specific neighbor AS are not consistent with policies with other ASes peering with a network, they may not be misconfigurations because it is not uncommon for a network to customize policies for each neighboring AS. We assume that if policies are consistent across all BGP sessions to the same AS, the violation highlighted by Minerals is likely not a misconfiguration.

IV.CONCLUSION

Minerals were successful in detecting a number of errors that would have been missed by other techniques. The operators who experimented with it found minerals helpful and provided positive feedback. The extension of the model with additional attributescan helps to unearth further mistakes. The analysis of statistical properties of router configurations appears to be a promising approach to assist operators in detecting mistakes. This system exploring adding attributes and extending the number of instance types to broaden the scope of errors and areas where Minerals can be applied.

The analysis of the configurations over the temporal dimension could possibly reveal additional misconfigurations not detected by snapshot analysis. The systems have started to analyze successive snapshots of the configurations to expose patterns of change. This technology analyzed the evolution of user accounts on the routers and found that a handful of accounts are rotated regularly: a username would be added to almost all routers at about the same time, then deleted some time later, and replaced by another username. This turns out to be backdoor accounts that are created to ensure management access during times of failure, DoS, or planned maintenance events. Data mining can be applied to discover outliers in this pattern: e.g., routers that are misconfigured during rotation which either has multiple backdoor accounts, or new routers that are overlooked and have no backdoor accounts.

REFERENCES

[1] El-Arini, K. and Killourhy, K. (2005) 'Bayesian Detection of Router Configuration Anomalies', presented at the ACM SIGCOMM Workshop on Mining Network Data (MineNet'05), Philadelphia, PA.

[2] Wool, A. (2004) 'A Quantitative Study of Firewall Configuration Errors', *IEEE Computer*, vol. 37, no. 6, pp. 62–67.

[3] Caldwell, D. Gilbert, A. Gottlieb, J. Greenberg, A. Hjalmtysson, G. and Rexford, J. (2003) 'The Cutting EDGE of IP Router Configuration,' presented at the ACM SIGCOMM HotNets-II Workshop, Cambridge, MA.

[4] Mahajan, R. Wetherall, D. and Anderson, T. (2002) 'Understanding BGP Misconfiguration', in *Proc. ACM SIGCOMM*, Pittsburgh, PA, pp. 3–16.5.

[5] Feldmann, A. and Rexford, J. (2001) 'IP Network Configuration for Intradomain Traffic Engineering' *IEEE Network*, vol. 15, no. 5, pp. 46–57.

Published by SK Research Group of Companies (SKRGC).