

# Efficient Probing Method for Active Diagnosis in Large Scale Network

Lu Guan, Ying Wang, Wenjing Li, Congxian Yan

State Key Laboratory of Networking and Switching Technology  
Beijing University of Posts and Telecommunications  
Beijing, China

{guanlu, wangy, wjli}@bupt.edu.cn, [yancongxiang1423@163.com](mailto:yancongxiang1423@163.com)

**Abstract**—Adaptive active diagnosis method is widely adopted for fault diagnosis in networks. In active diagnosis, appropriate probes are selected sequentially and fault diagnosis is made by inference from results of selected probes. It is very important to select active probes with low cost and less impact on network performance. However, the selection of the most informative set of probes with limited cost is an NP-hard problem. The computational complexities of existing probe selection algorithms are still too high for large scale networks. In this paper, a lemma about mutual information provided by probes is proved based on the property of conditional entropy. Then an approximate method derived from this lemma is introduced to compute mutual information of probe. With this approximate method an efficient probe selection algorithm for active diagnosis is proposed. At last, the efficiency and effectiveness of the proposed algorithm is verified through simulation.

**Keywords**—Active probing; Bayesian network; information theory

## I. INTRODUCTION

With the rapid development of computer network, more and more IT services are accessible to remote user over the internet. Guaranteeing the quality of network service becomes a vital part in network management. As the computer networks grow bigger and more complex, many works [1]-[9] focus on active diagnosis method in large scale network. Considering the heterogeneity of network, passive event correlation [10] [11] is not practical in today's computer networks, as it is based on the premise that all the managed entities could send out appropriate alarms. Thus active diagnosis technology based on end-to-end probes becomes a good solution for this problem.

Active diagnosis technology adaptively selects probes and requires no excess instrumentations. Diagnosis is made by inference from results of selected probes. As the responses of probes depend on the states of managed entities in network, probabilistic inference based on Bayesian network (which is probabilistic model for dependencies among network), with responses of probes could reason the root cause in the network. The form of the probes is flexible. Any end-to-end services e.g. a ping command or database query could be the probes.

As probes consume operation cost and lead to additional network load, the probe set should be appropriately selected. The most informative set of probes with limit cost is optimal. However, it is an NP-hard problem to select this optimal probe set. Thus a heuristic greedy approach that repeatedly selects the

most informative probe sequentially is widely used. Whenever to be chose a probe, the quality of each probe (which is often quantified by the mutual information of the probe) is computed. The probe with maximum mutual information is to be selected. As computation complexity of mutual information is very high, probe selection process consumes most of runtime of active diagnosis. Although previous work [5] [9] tried to reduce computation complexity of probe selection process, the computing complexity of quality evaluation method is still too high for large scale network.

In this paper, we focus on efficient probe selection method with low computation complexity for active diagnosis in large scale networks. As quality evaluation of probes consumes most of the runtime, we try to simplify the quality evaluating process. In brief, the main contribution of this paper is as follows:

- 1) Based on the property of conditional entropy, a lemma about mutual information provided by probes is proved. Then we propose an approximate method to compute the information gain of probe. This approximate method could largely reduce computation complexity and save runtime for probe quality evaluation process.

- 2) Based on the approximate method we propose for probe quality evaluation, an efficient probe selection algorithm for active diagnosis in large scale networks is proposed. Simulation in this paper verified the efficiency and effectiveness of our algorithm in comparison with the representative BPEA algorithm.

## II. FAULT DIAGNOSIS WITH BAYESIAN NETWORK

The Bayesian network is used to build graph model in many fields. In this paper, Bayesian network is used to model the dependencies between probes, network nodes and noise in the network. Network nodes include physical entities e.g. routers and servers, and logical entities e.g. virtual machines (VM) in the network. Probes could be end-to-end services that reflect information about states of network nodes.

Bayesian network is a directed acyclic graph (DAG) with nodes of the states of the network nodes, called  $X_1, X_2, \dots, X_n$ , responses of probes (which is also called symptoms) called  $S_1, S_2, \dots, S_m$ , and edges representing direct dependencies between network nodes and symptoms. The edges are weighted by the conditional probability distribution  $P(S_i | \text{parent}(S_i))$  or  $P(X_i | \text{parent}(X_i))$ , where  $\text{parent}()$  denote the nodes pointing to  $S_i$  or  $X_i$  [12].

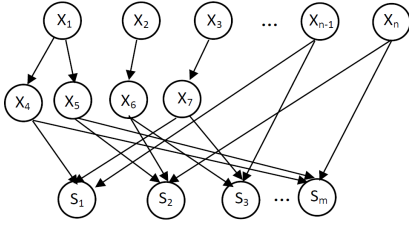


Fig. 1. Bayesian network that models noises and dependencies in network

Figure 1 shows a three layered Bayesian network. The bottom layer is consists of managed entities whose states does not depend on others e.g. servers and routers. The middle layer contains the managed entities that depend on the first layer e.g. VMs (whose states depend on the states of the servers they hosted on). And the top layer is made up of observed symptoms.

With Bayesian network that models dependencies among network as a tool and responses of probes as well as alarms as evidence, the fault diagnosis problem could be formulated as Maximum A posteriori Probability (MAP) problem: given a set of symptoms (observation), to find the most likely states  $\arg \max_x P(X|S)$  for the managed entities in network. However, this inference problem is NP-hard [13]. Many prior work like [4] [6] [8] [21] researched on this inference problem.

### III. EFFICIENT ACTIVE PROBING

#### A. Probe selection problem

In active probing, large set of probes leads to high cost of management and negative impact on networks performance. In large scale network, active probe set should be appropriately chosen. The most informative set of probes with cost constraint is optimal. Many literature [2]-[7] and [9] concerns about selecting an optimal subset of probes from a large number of candidates. Information entropy is usually used to quantify the uncertainty of network state as in [5] [9]. Assume vector  $X = (X_1, X_2, \dots, X_n)$  denotes the state of the managed entities to be diagnosed in the network. The uncertainty of the network before any symptom is observed could be quantified as:

$$H(X) = \sum_x P(X) \log \frac{1}{P(X)} = -\sum_x P(X) \log P(X) \quad (1)$$

The uncertainty of network decreases as symptoms accumulates. When a set of symptoms  $D = (t_1, t_2, \dots, t_m)$  is observed, where  $t_i$  represents the outcome of probe  $T_i$  that has been sent, the uncertainty of network turns into:

$$H(X|D) = -\sum_x P(X|D) \log P(X|D) \quad (2)$$

Selecting the most informative set of probes with cost constraint is an NP-hard problem. Therefore, a heuristic greedy approach that repeatedly selects the most informative probe is widely used for this problem. This greedy algorithm achieves near-optimal performance in many situations [5].

The information gain that the probe  $T_i$  contributes to decreasing the uncertainty of the network could be quantified as:

$$G(T_i) = H(X|D) - H(X|D, T_i) \quad (3)$$

The most informative probe  $T_i^* = \arg \max_{T_i} G(T_i)$  is to be selected in each time. However the computation complexity of  $G(T_i)$  is too high especially in large scale networks. That is why literatures [2]-[4] just concern on the computation of the approximation of  $G(T_i)$  in a single-fault scenario where all variables have the same prior faulty probability. Authors in [5] propose an approximate algorithm named BPEA based on BP algorithm to figure out the approximation of  $H(X|D, T_i)$ . Cheng et al. [9] propose an algorithm named IAP to reduce the computation of  $G(T_i)$  based on the conditionally independent property in Bayesian network they prove in their work. Our probe selecting algorithms MEAP derives from their IAP algorithm but is more efficient than theirs. In our work, an approximate approach is used to compute  $G(T_i)$ . In next section, we will introduce the approximate approach to compute  $G(T_i)$ .

#### B. Information gain of probe

At first, a lemma about  $G(T_i)$  is introduced. Then an approximate method based on the lemma is proposed to compute  $G(T_i)$ . Lemma 1 and its proof are shown as below:

$$\textbf{Lemma 1. } G(T_i) = H(T_i|D) - H(T_i|X, D)$$

Proof: According to the property of information entropy [14], we get:

$$H(X|D, T_i) = H(X, T_i|D) - H(T_i|D) \quad (4)$$

$$H(T_i|X, D) = H(X, T_i|D) - H(X|D) \quad (5)$$

Applying (4) (5) to (3):

$$\begin{aligned} G(T_i) &= H(X|D) - H(X|D, T_i) \\ &= H(X|D) - H(X, T_i|D) + H(T_i|D) \\ &= H(T_i|D) - H(T_i|X, D) \end{aligned} \quad (6)$$

Lemma 1 is proved.

According to property of information entropy [14]:

$$H(T_i|X, D) \leq H(T_i|X) \quad (7)$$

For low noise environment, given the state of network nodes, the state of probe is nearly certain and the value of  $H(T_i|X)$  is very small, which could be elided in computation. Considering (7),  $H(T_i|X, D)$  is less than  $H(T_i|X)$  and could be elided in computation of  $G(T_i)$  in low noise environment.

Thus the approximation of  $G(T_i)$  could be quantified as:

$$G(T_i) \approx H(T_i|D) = -\sum_{T_i} P(T_i|D) \log P(T_i|D) \quad (8)$$

As probe  $T_i$  only has two kinds of outcomes (good or bad symptom),  $H(T_i|D)$  could be calculated easily with  $P(T_i|D)$ .  $P(T_i|D)$  could be computed with approximation method such as the BP algorithm. Thus we get an approximate method to efficiently compute  $G(T_i)$  with small biases. Using (8) to figure approximation of  $G(T_i)$ , the computation complexity is largely reduced and much active diagnosis runtime could be saved.

#### C. Conditionally independent property of entropy in Bayesian network

Cheng et al. [9] proved the conditionally independent property of entropy in Bayesian network that:

**Lemma 2.** Let  $T_1, T_2, \dots, T_m$  denote a set of probes and  $D^{(0)} = \emptyset, D^{(1)} = \{t_1\}, D^{(2)} = \{t_1, t_2\}, \dots, D^{(i)} = \{t_1, t_2, \dots, t_i\}$  denote the outcomes of selected probes. Then:  $G(T_j | D^{(i)}) \leq G(T_j | D^{(i-1)})$  with equality if and only if, given  $D^{(i-1)}, T_i$  and  $T_j$  are conditionally independent.

This is a useful property of entropy and the IAP algorithm [9] uses Lemma 2 to reduce the computation time when conditionally independency exists between probes.

#### D. More Efficient Active Probing Algorithm

In [9], the following formula (9), the computation complexity of which is higher than (8), is used to update the information gain of probes

$$G(T_i) = - \sum_{T_i, \text{par}(T_i)} P(T_i, \text{par}(T_i) | D) \log P(T_i | \text{par}(T_i)) + \sum_{T_i} P(T_i | D) \log P(T_i | D) \quad (9)$$

Our MEAP algorithm makes an improvement upon IAP algorithm and uses our approximate method to efficiently update information gain of probes. As the computation of  $G(T_i)$  consumes a large part of runtime, our MEAP algorithm is more efficient than IAP.

Figure 2 shows the pseudo code of our algorithm. Observed symptoms  $D$  and  $G(T_i)$  of each probe are initialized at the beginning of the active probing. A new probe could be sent when there still exist candidate probes and the cost of active probing doesn't exceed the budget  $B$ . The most informative probe  $T^*$ , whose information gain is MaxGain, is selected in each time of probe selection. Candidate probes are descending sorted in term of  $G(T_i)$  in each round. We search for  $T^*$  from the first one of candidate probes. If the MaxGain is less than  $G(T_i)$ , and  $T_i$  is independent of all the probes that have been selected since last update of  $G(T_i)$ , then  $T_i$  is the most informative probe in this round. Because the information gain of  $T_i$  doesn't change since its update and the probes ranked behind of  $T_i$  can't be more informative than  $T_i$  (**Lemma 2**). Function  $\text{getSelected}(T_i)$  returns the set of probes that have been selected since last update of  $G(T_i)$ . Function  $\text{Independent}(\text{getSelected}(T_i), T_i)$  determines the independency between the outcome of  $\text{getSelected}(T_i)$  and probe  $T_i$ . Else, the search goes on and the information gain of  $T_i$  needs to be updated with our approximate method.

#### IV. EVALUATION

In simulation our MEAP algorithm is compared with BPEA [5]. The experiment setup is similar to that of [5] and [9].

As Internet like topology follows the power-law degree distribution [15] [16], we use the INET generator [17] to generate five networks of different sizes. The network size is varying from 100 to 500. Three nodes are randomly selected as probe stations. Assuming probes starting from probe stations and heading for managed entities following the shortest path, a complete set of candidate probes could be got. Removing redundant probes, a subset of candidate probes could be used for probe selection. We set the cost limit to 30 and select 30 probes from candidates in each experiment.

Similar to [5] [9], we assume the probes to be noisy-OR tests. The joint probability distribution of symptoms and network nodes forms the QMR-DT model [18]:

$$P(T_j = 0 | \text{parent}(T_j)) = (1 - \rho_{i0}) \prod_{X_i \in \text{parent}(T_j)} \rho_{ij}^{X_i} \quad (11)$$

Here,  $\rho_{ij}$  is the inhibition probability, that a measurement of the amount of noise in network.  $\rho_{i0}$  is the leak probability of an unaccounted-for faulty element.  $P(T_j = 0 | \text{parent}(T_j))$  is the probability which account for the case where probe  $T_j$  returns a good symptom given the states of its parent nodes. In this experiment, we randomly generate a prior fault probability for each node with the Normal distribution (0.005, 0.003) and set the value of  $\rho_{ij}$  to be varying from 0.01 to 0.3 and  $\rho_{i0}$  to 0.01. Assuming  $T_j$  gets the value 0 if its response is OK, 1 otherwise. Then  $P(T_j = 0 | \text{parent}(T_j))$  denotes the probability that  $T_j$  returns a good symptom given the states of the parents of  $T_j$ .

We implement the BPEA and our MEAP algorithm by Matlab(R2008b) with the belief propagation and junction tree engine in Kevin Murphy's Bayes Net Toolbox[19].

**Algorithm MEAP: More Efficient Active Probing**  
**Input:** Candidate probes S, Budget B, and detection results  $D_{\text{initial}}$   
**Output:** the most probable explanation (MAP) given the detection results  $D$   
 $D = D_{\text{initial}}$   
**for** (Probe  $T_i \in S$ ) **do** update  $G(T_i)$ ; **end for**  
**while** ( $S \neq \emptyset$ ) {  
    Sort(S);  
     $i=1$ ;  
    MaxGain=0;  
    **while** (MaxGain <  $G(T_i)$ ) **do**  
        **if** ( $\text{Independent}(\text{getSelected}(T_i), T_i)$ ) **do**  
            MaxGain =  $G(T_i)$ ;  
             $T^* = T_i$ ;  
            break;  
        **else do**  
            update  $G(T_i)$ ;  
            **if** (MaxGain <  $G(T_i)$ ) **do**  
                MaxGain =  $G(T_i)$ ;  
                 $T^* = T_i$ ;  
            **end if**  
        **end if**  
         $i++$ ;  
    **end while**  
    **if** ( $\text{cost}(S \cup T^* \leq B)$ ) **do**  
        execute Probe  $T^*$ ; Returns t;  
         $D = D \cup \{t\}$ ; remove  $T^*$  from S;  
    **else do** break;  
    **end if**  
**end while**  
**return** MAP:  $\arg \max_X P(X|S)$  //result of fault

Fig. 2. Algorithm MEAP: More Efficient Active Probing

## A. Empirical results

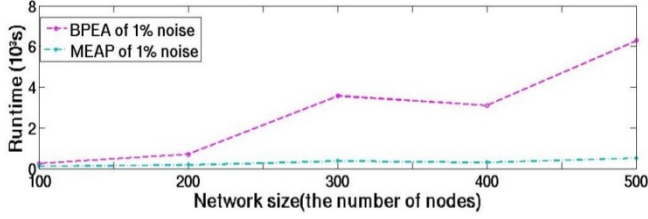


Fig. 3. Runtime of MEAP and BPEA under various network sizes

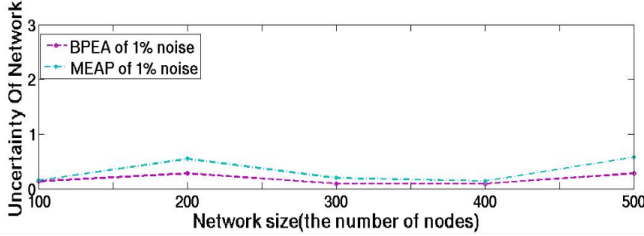


Fig. 4. Uncertainty of network after active probing

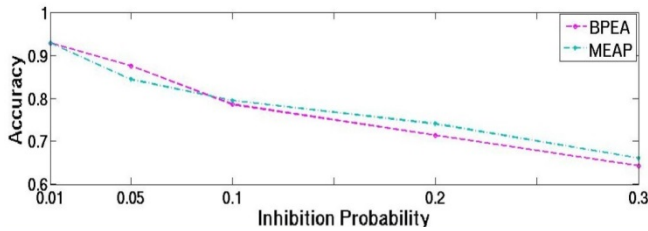


Fig. 5. Diagnosis Accuracy by taking response of selected probes as input

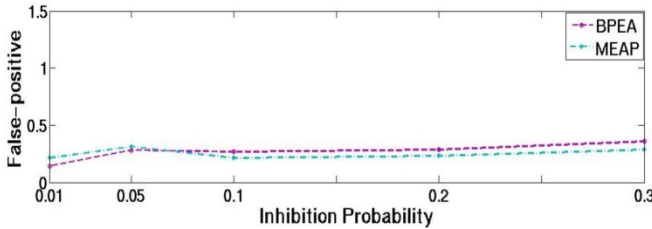


Fig. 6. Diagnosis Precision by taking response of selected probes as input

Figure 3 compares the runtime of MEAP and BPEA algorithms on different sizes of networks. The two algorithms consume a similar runtime in a network with 100 nodes. The runtime of BPEA increase rapidly with the extended scale of network whereas the runtime of MEAP increase slowly. In a network with 500 nodes, BPEA takes nearly 105 minutes to select 30 most-informative probes from candidates, whereas MEAP uses only 8.5 minutes. Figure 4 shows the uncertainty of the system that still exist after active probing. The uncertainty of the system is quantified in (2). The uncertainties of system after two active probing methods are very low and in the same order of magnitude. The result of MEAP is a little higher than BPEA in this metric.

To evaluate the efficiency of active probing algorithms, a classical diagnosis algorithm shrink [20] is performed with the responses of probes selected by BPEA and MEAP as inputs. Two metrics, namely accuracy and false positive are used to evaluate diagnosis results. Let  $F$  to be the set of real faults,  $\bar{F}$

be the set of nodes in good states, and  $H$  be the set of nodes diagnosed to be faulty. Then accuracy and false positive can be defined as followed:

$$Accuracy = \frac{|H \cap F|}{|F|}, False\ positive = \frac{|H \cap \bar{F}|}{|F|} \quad (13)$$

Figure 5 and 6 show the diagnosis accuracy and false positive ratio with BPEA and MEAP algorithm in a network with 100 nodes. The diagnosis accuracy and precision with the probe responses got from the two algorithms is roughly equivalent.

Thus, MEAP could significantly reduce probe selection time in large scale network in comparison with BEAP, without drops of diagnosis accuracy and precision and information gain. MEAP is very feasible to handle probe selection problem in large scale networks.

## V. RELATED WORK

Many work focus on the active probing for fault diagnosis. This section gives a brief review of this related work.

Natu et al. [6] [7] proposed their adaptive probing method for fault diagnosis and employed a worth function to select the most informative probe. The probe  $T^*$  with maximum worth is selected to probe suspected node  $S$ . However, their method is vulnerable to noises.

Zheng et al.[5] proved that the information entropy of uncertainty about system could be decomposed into a cross entropy, a negative conditional entropy and a constant in their word. Then, they proposed an approximate algorithm BPEA to simultaneously compute the cross and conditional entropy with the loopy belief propagation infrastructure.

Lu Cheng et al. [9] proposed an algorithm IAP to efficiently select probes based on the conditionally independent property in Bayesian network they proved.

The selection of most-informative probes is also studied in many other fields like feature selection in machine learning, etc. Due to space limitation, we do not give a detailed review here.

## VI. CONCLUSIONS

In this paper, a lemma about mutual information of probe is proved. Then an approximate method to evaluate quality of probes is derived. With the approximate method, an efficient probe selection algorithm in large scale networks improved from IAP algorithm is proposed. Simulation results prove that our active probing algorithm MEAP is more efficient than BPEA and pretty feasible to handle the probe selection problem in large scale networks.

Our algorithm is a generic probe selection methodology that could be used for probe selection problems in many large scale network environments such as IP network, cloud computing and virtualization network environment.

## ACKNOWLEDGMENT

This work was supported by National High Technology R&D Program of China (2011AA01A102, 2013AA013502) and the Fundamental Research Funds for the Central Universities BUPT 2013RC1103.

## REFERENCES

- [1] Irina Rish, Mark Brodie, and Sheng Ma. Intelligent probing: a Cost-Efficient Approach to Fault Diagnosis in Computer Networks. *IBM Systems Journal*,41(3):372–385, 2002.
- [2] M. Brodie, I. Rish, S. Ma, N. Odintsova, and A. Beygelzimer. Active Probing Strategies for Problem Diagnosis in Distributed Systems. In *Proc. International Joint Conference On Artificial Intelligence (IJCAI'03)*,2003
- [3] I. Rish, M. Brodie, N. Odintsova, S. Ma, and G. Grabainik. Real-time problem determination in distributed systems using active probing. In *Proc. IEEE/IFIP Network Operations Management Symposium (NOMS'04)*, pages 133–146, 2004.
- [4] I. Rish, M. Brodie, S. Ma, N. Odintsova, A. Beygelzimer, G. Grabainik, and K. Hernandez. Adaptive Diagnosis in Distributed Systems. *IEEE Trans. Neural Networks*, 16(5):1088-1109, 2005.
- [5] A. X. Zheng, I. Rish, and A. Beygelzimer. Efficient test selection in activediagnosis via entropy approximation. In *Proceedings of Uncertainty in AI(UAI' 05)*, 2005
- [6] M. Natu and A. S. Sethi. Probabilistic Fault Diagnosis Using Adaptive Probing. In *Proc. DSOM, LNCS 4785*, pp. 38–49, 2007.
- [7] M. Natu and A. S. Sethi. Application of Adaptive Probing for Fault Diagnosis in Computer Networks. In *Proc. IEEE/IFIP Network Operations Management Symp (NOMS'08)*, pp:1055-1060, 2008
- [8] L. Cheng, X.S. Qiu, L.M. Meng, Y. Qiao and Z.Q. Li. Probabilistic Fault diagnosis for IT Services in Noisy and Dynamic Environments. In *Proc. IEEE/IFIP International Symposium on Integrated Network Management(IM'09)*, New York, June 2009.
- [9] L. Cheng, X.S. Qiu, L.M. Meng, Y. Qiao, Efficient Active Probing for Fault Diagnosis in Large Scale and Noisy Networks, in *Proc. IEEE INFOCOM*, 2010
- [10] G. Jakobson and M. Weissman. Alarm Correlation. *IEEE Network*, 1993.
- [11] S. A. Yemini, S. Kliger, E. Mozes, Y. Yemini, and D. Ohsie. A Coding Approach to Event Correlation. In *Proc. IEEE/IFIP International Symposium on Integrated Network Management(IM'95)*, Pages 266-277, 1995.
- [12] J. Pearl. *Probabilistic reasoning in intelligent systems: networks of plausible inference*. Morgan Kaufmann, San Mateo, California, 1988.
- [13] G.F. Cooper. The computational complexity of probabilistic inference using Bayesian belief networks. *Artificial Intelligence*, 42(2–3):393–405, 1990.
- [14] Thomas M. Cover and Joy A. Thomas, *Elements of information theory*, 2nd ed, John Wiley & Sons, Inc, Hoboken, New Jersey, 2005
- [15] M. Faloutsos, P. Faloutsos, and C. Faloutsos. On power-law relationships of the Internet topology. *ACM SIGCOMM Computer Communication Review*, 29(4):251–262, 1999.
- [16] N. Odintsova and I. Rish. Empirical Study of Topology Effects on Diagnosis in Computer Networks. In *Proc. Mobile Adhoc and Sensor Systems*, 2007
- [17] J. Winick and S. Jamin. Inet-3.0: Internet topology generator. Technical Report CSE-TR-456-02, University of Michigan, 2002.
- [18] T. Jaakkola and M. Jordan. Variational probabilistic inference and the qmr-dtdatabase. *Journal of Artificial Intelligence Research*, pages 291–322, 1999.
- [19] K. P. Murphy. *The Bayes Net Toolbox for Matlab*. In *Computing Science and Statistics: Proceedings of the Interface*, volume 33, 2001.
- [20] S. Kandula, D. Katabi, and J. P. Vasseur. Shrink: A tool for failure diagnosis in IP networks. In *Proc. ACM SIGCOMM MineNet Workshop*, Aug. 2005.
- [21] Y. Tang, E. Al-Shaer, and R. Boutaba. “Active Integrated Fault Localization in Communication Networks,” in *Proc. Integrated Management (IM'05)*, Nice, France, 2005.