International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-2 Issue-4, March 2013

Measurouting Approach for Flow Utility in Routing Assisted Traffic Monitoring

S.Priya, S.Pushpa

Abstract—The network operators are interested in monitoring passing traffic in a network for reasons of traffic accounting, debugging or troubleshooting, forensics, and traffic engineering. Previous research has focused on monitor placement across the network for maximizing the monitoring utility. But, traffic characteristics and measurement objectives can change dynamically, rendering a placement of monitors suboptimal. It will not be the feasible solution to dynamically reconfigure measurement infrastructure. The problem is addressed by strategically routing traffic subpopulations over fixed monitors. This approach is referred as MeasuRouting. The challenge of MeasuRouting to work within the intradomain TE operations that are geared for utilizing bandwidth resources and meeting quality-of-service (QoS). A feature of intradomain routing, is specified for aggregate flows which is feasible for measurouting. MeasuRouting can route the components of an total flow while ensuring that the placement of monitor is compliant to original TE objectives. In this paper, a theoretical framework for MeasuRouting and flow utility function for packet is presented.

Index Terms: aggregate flow, intradomain routing, network management, traffic engineering, traffic measurements.

I. INTRODUCTION

Numerous factors associated with technology, business, regulation and social behaviour naturally and logically speak in favor of wireless *ad hoc* networking. In terms of price, portability and usability and in the context of an *ad hoc* network, many computing and communication devices, such as PDAs and mobile phones, already possess the attributes that are desirable. A*d hoc* network is a network formed without any central administration which consists of mobile nodes that use a wireless interface to send packet data. Since the nodes in a network of this kind can serve as routers and hosts, they can forward packets on behalf of other nodes and run user applications. An ad-hoc network is a self-configuring network of wireless links connecting mobile nodes. These nodes may be routers and/or hosts. The nodes communicate directly with each other and without the aid of access points, and therefore have no fixed infrastructure. They form an arbitrary topology, where the routers are free to move randomly and arrange themselves as required.

Manuscript published on 30 March 2013.
***Correspondence Author(s)
Ms. S.Priya, Networking Department, Sri Manakula Vinayagar Engineering College, India.
Dr. S.Pushpa, Associate Professor, Sri Manakula Vinayagar Engineering College, India.

Each node are said to be purpose-specific, autonomous and dynamic. This compares greatly with fixed wireless networks, as there is no master slave relationship that exists in a mobile ad-hoc network. Nodes rely on each other to established communication, thus each node acts as a router. Therefore, in a ad-hoc network, a packet can travel from a source to a destination either directly, or through some set of intermediate packet forwarding nodes.

II. OVERVIEW OF MEASUROUTING

The optimal placement and configuration of monitoring infrastructure for a specific measurement objective typically assumes *a priori* knowledge about the traffic characteristics. Furthermore, these are typically performed at longer timescales to allow provisioning of required physical resources. However, traffic characteristics and measurement objectives may evolve dynamically, potentially rendering a previously determined solution suboptimal. We propose a new approach called *MeasuRouting* to address this limitation. MeasuRouting forwards network traffic across routes where it can be best monitored. MeasuRouting takes monitor deployment as an input and decides how to route traffic to optimize measurement objectives. Since routing is dynamic in nature, MeasuRouting can conceptually adjust to changing traffic patterns and measurement objectives.

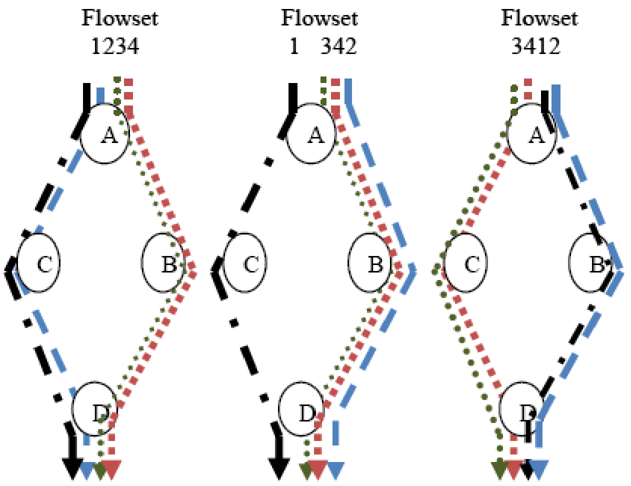


Fig 1: Focus on a traffic subpopulations
(a) Original (b) Violating (c) Compliant

It shows four traffic subpopulations f1, f2, f3 and f4 that have the same ingress and egress nodes. Suppose that f1, f2, f3 and f4 are of equal size.

Router B has some dedicated monitoring equipment, and it is important for the network operator to monitor f2. Our TE policy is to minimize the maximum link utilization. Fig. 1(a) depicts the original routing that obeys the TE policy.

*Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)*

Fig. 1(b) represents a routing that violates the TE policy in order to route f2 through router.

However, if the traffic subpopulations are routed as in Fig. 1(c), f2 is allowed to pass through the dedicated monitoring equipment, and the routing is indistinguishable from the original from the perspective of our TE policy. It is important to note that the aggregate traffic must span multiple paths in order for MeasuRouting to be useful in this way. If the aggregate traffic traverses a single path, then no opportunity exists to differentially route subsets of the traffic. MeasuRouting has global information of : 1) the TE policy; 2) the topology and monitoring infrastructure deployment; and 3) the size and importance of traffic subpopulations. They are three fundamental ways in which MeasuRouting enhances traffic monitoring utility without violating TE policy.

1. TE policy is usually defined for aggregated flows. On the other hand, traffic measurement usually deals with a finer level of granularity. For instance, we often define a flow based upon the five-tuple (srcip, dstip. srcpt, dstpt, proto) for measurement purposes. Common intradomain protocols (IGPs) like OSPF and IS-IS use link weights to specify the placement of traffic for each origin–destination (OD) pair. The TE policy is oblivious of how constituent flows of an OD pair are routed as long as the aggregate placement is preserved. It is possible to specify traffic subpopulations that are distinguishable from a measurement perspective but are indistinguishable from a TE perspective. MeasuRouting can, therefore, route fine-grained measurement traffic subpopulations without disrupting the aggregate routing.

2. TE objectives may be oblivious to the exact placement of aggregate traffic and only take cognizance of summary metrics such as the maximum link utilization across the network. An aggregate routing that is slightly different from the original routing may still yield the same value of the summary metric.

3. A network operator can specify a certain permissible level of TE policy violations. Such a specification would enable a tradeoff between the advantage derived from MeasuRouting and adherence to TE policy.

III. RELATED WORK

Earlier work in the area of traffic monitoring has focused on: 1) inferring characteristics of original traffic from sampled traffic; 2) investigating and improving the effect of oblivious sampling on monitoring certain traffic subpopulations; and 3) placing monitor agents at certain strategic network locations.

Guanyao Huang, Chia-Wei Chang, Chen-Nee Chuah, and Bill Lin presented an MMPR (Measurement-aware Monitor Placement and Routing) framework that jointly optimizes monitor placement and dynamic routing strategy to achieve maximum measurement utility. The main challenge in solving MMPR is to decouple the relevant decision variables and adhere to the intra-domain traffic engineering constraints. They formulate it as an MILP (Mixed Integer Linear Programming) problem and propose several heuristic algorithms to approximate the optimal solution and reduce the computation complexity. Through experiments using real traces and topologies they showed that heuristic solutions can achieve measurement gains that are quite close to the optimal solutions.

Anirudh Ramachandran, Srinivasan Seetharaman, Nick Feamster and Vijay Vazirani presented the design, implementation, and evaluation of FlexSample, a traffic monitoring engine that dynamically extracts traffic from subpopulations that operators define using conditions on packet header fields. FlexSample uses a fast, flexible counter array to provide rough estimates of packets membership in respective subpopulations. Based on these coarse estimates, FlexSample then makes per-packet sampling decisions to sample proportionately from each subpopulation, subject to an overall sampling constraint. They applied FlexSample to extract subpopulations such as port scans and traffic to high-degree nodes and find that it is able to capture significantly more packets from these subpopulations than conventional approaches.

A. Medina, N. Taft, K. Salamatian, S. Bhattacharyya and C. Diot makes two contributions for POP-to-POP traffic matrices (TM) . The primary contribution is the outcome of a detailed comparative evaluation of the three existing techniques. They evaluated those methods with respect to the estimation errors yielded, sensitivity to prior information required and sensitivity to the statistical assumptions. The secondary contribution of their work is the proposal of a new direction for TM estimation based on using *choice models* to model POP *fanouts*. These models allow us to overcome some of the problems of existing methods because they can incorporate additional data and information about POPs and they enable to make a fundamentally different kind of modeling assumption. Their proposed approach can be used in conjunction with existing or future methods in that it can be used to generate good priors that serve as inputs to statistical inference techniques.

C. Chaudet, E. Fleury, I. Guerin Lassous and H. Rivano studied the passive approach that attaches specific devices to links in order to monitor the traffic that passes through the network and the active approach that generates explicit control packets in the network for measurements and the problem of assigning tap devices for passive monitoring and beacons for active monitoring. Minimizing the number of devices and finding optimal strategic locations is a key issue, mandatory for deploying scalable monitoring platforms. They presented a combinatorial view of the problem from which they derived complexity and approximability results, as well as efficient and versatile Mixed Integer Programming (MIP) formulations.

IV. PROPOSED WORK

A. Definition

G(V,E) represents our network, where V is the set of nodes and E is the set of directed links. A *macro-flowset* represents a set of flows for which an aggregate routing placement is given. In the context of intradomain IP routing, a macro-flowset comprises all flows between an OD pair. For MPLS networks, macro-flowsets can be defined as all flows between an ingress–egress pair in the same QoS class. Our only requirement is that flows in a macro-flowset have the same ingress and egress nodes. In this paper, consider all flows between an OD pair to constitute a single macro-flowset. A macro-flowset may consist of multiple *micro-flowsets*. θ denotes the set of micro-flowsets.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

There is a many-to-one relationship between micro-flowsets and macro-flowsets. γ_x represents the set of micro-flowsets that belong to the macro-flowset . We represent the fraction of traffic demands belonging to micro-flowset y, placed along link (i,j) by γ_{ij}^{y}. $\{\gamma\}_{(i,j)\epsilon E}^{y\epsilon\theta}$ represents our *micro-flowset routing* and gives the decision variables of the MeasuRouting problem.. $\{S\}_{(i,j)\epsilon E}$ denotes the *sampling characteristic* of all links. The sampling characteristic is the ability of a link to sample traffic. It could be a simple metric like the link sampling rate. $\{I\}_{y\epsilon\theta}$ denotes the *sampling utility* of the micro-flowsets. This is a generic metric that defines the importance of measuring a micro-flowset. $\{S\}_{(i,j)\epsilon E}$ and $\{I\}_{y\epsilon\theta}$ are inputs to our problem. The *sampling resolution function* (β) *are s follows*

$$\beta : (\{\gamma\}_{(i,j)\epsilon E}^{y\epsilon\theta}, \{S\}_{(i,j)\epsilon E}, \{I\}_{y\epsilon\theta}) \rightarrow \Re$$

β assigns a real number representing the monitoring effectiveness of a micro-flowset routing for given link sampling characteristics and micro-flowset sampling utilities. The objective of MeasuRouting is to maximize β. Specifying β, $\{S\}_{(i,j)\epsilon E}$ and $\{I\}_{y\epsilon\theta}$ defines a concrete MeasuRouting application.

B. *Measurouting Problems*

1) Least TE Disruption MeasuRouting (LTD):

It tries to maximize β by computing a micro-flowset routing, $\{\gamma\}_{(i,j)\epsilon E}^{y\epsilon\theta}$, that obeys the flow conservation constraints. LTD requires that the aggregate TE policy does not violate.

$$(1+\epsilon)\sigma^{\Gamma} \geq \sigma^{\gamma}$$

σ^{Γ} gives the value of the TE metric of the original macro-flowset routing. Similarly σ^{γ} is a function of the micro-flowset routing that gives the corresponding value of the TE metric for it. The above equation specifies that σ^{γ} does not exceed σ^{Γ} by more than a certain percentage, signified by a tolerance parameter ϵ. LTD is the most flexible, but may result in routing loops or traffic between an OD pair traversing links it does not traverse in the original routing.

2) No Routing Loops MeasuRouting (NRL):

NRL ensures that the microflowset routing is loop-free. Loops are avoided by restricting the set of links along which a micro-flowset can be routed. This restriction is accomplished by supplementing the LTD problem with the following additional constraint:

$$\gamma_{i,j}^{y} = 0 \qquad y\epsilon\theta,\ (i,j) \notin \Psi_{x:y\epsilon\gamma_x}$$

The above equation states that only links included in $\Psi_{x:y\epsilon\gamma_x}$ may be used for routing micro-flowset yϵθ. NRL ensures that there are no routing loops. However, depending upon the exact forwarding mechanisms and routing protocol, NRL may still not be feasible.

3) ***Relaxed Sticky Routes MeasuRouting (RSR):***

RSR ensures that the micro-flowset routing does not route a macro-flowset's traffic along a link that the macro-flowset's traffic was not routed along in the original routing.

C. *Flow size Estimation*

In the flow-size estimation, the less priority is given to sample many packets from large flows, compared to equal number of small flows.

V. SYSTEM ARCHITECTURE

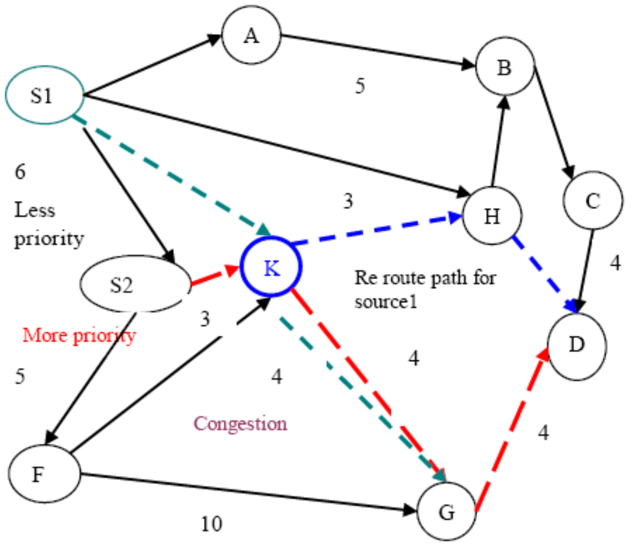


Fig 2: System Architecture

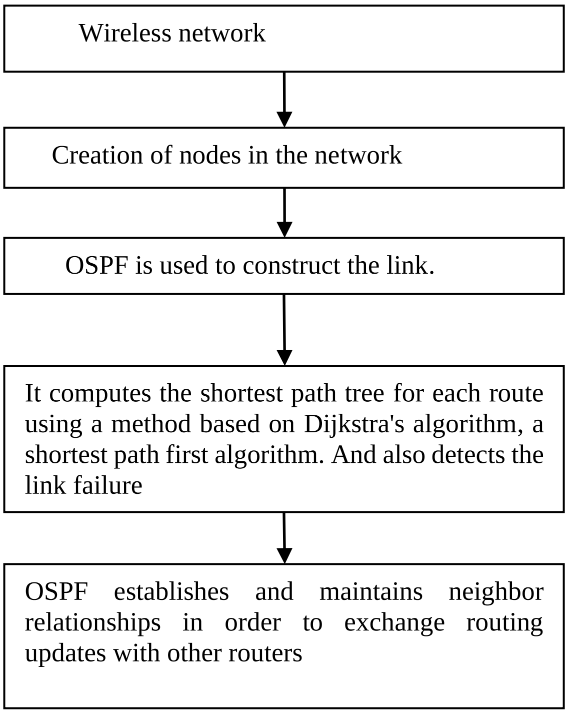
In the above figure2 source1 sends the packet to its destination and the same time source2 sends the packet to its desired destination. The two source node chooses the same shortest path k. So the node k is congested. By measurouting approach , one of the source node packet is rerouted by identifying the monitoring capacity of an router. In the flow size estimation the large flow is sampled into equal number of small flows.

VI. MODULES DESCRIPTION

1) Network creation and route discovery

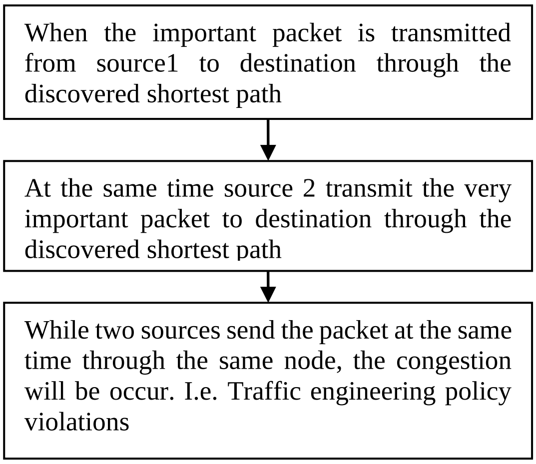
In network creation, set of nodes will be plot, after plotting the nodes in the network, using OSPF protocol have to gathers link state information from available routers and constructs a topology map of the network. OSPF establish and maintains the neighbor information.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)



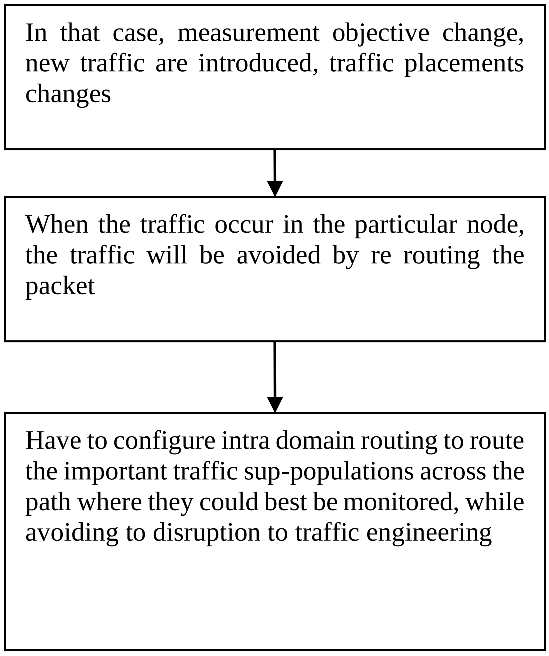
2) TE policy violation

When the two different packet is send at the same time via discovered shortest path by the same node, the traffic congestion will occur. In order to clear the traffic , only one packet will be allowed to the particular node, another packet will be re routed in the another shortest path i.e other packet will be re routed.



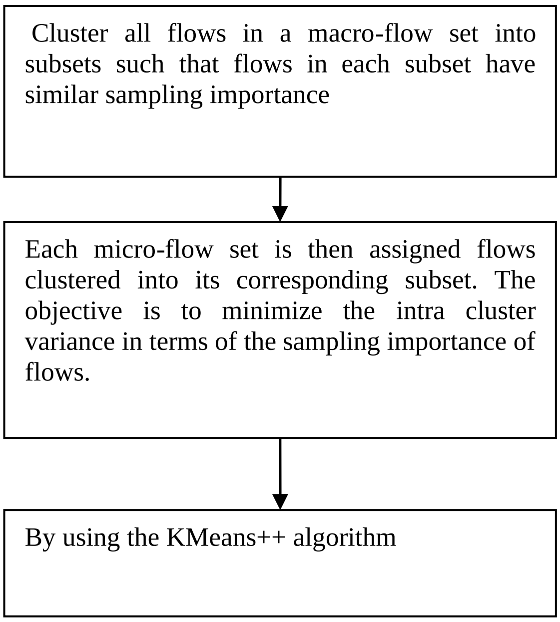
3) Traffic avoidance

When the traffic is occurred in the network, the traffic is best monitored by rerouting the packet. The packet is rerouted using measu routing algorithm across the path where they could be best monitored



4) Flow utility function for link

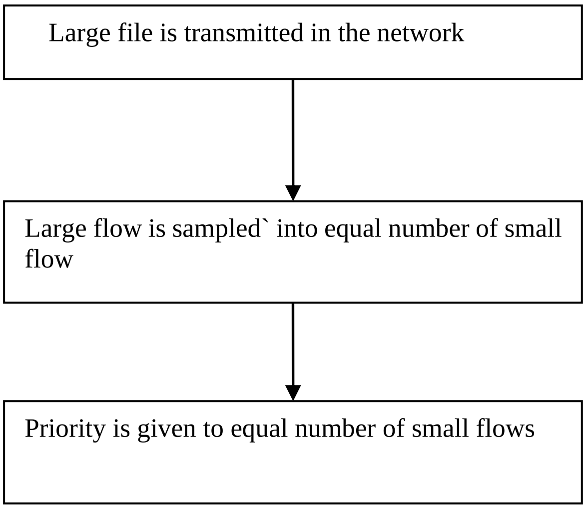
Every link is clustered in the network. Macro flow set is clustered as subset these subset have same sampling characteristics. Then each micro-flow set is then assigned flows clustered into its corresponding subset. To cluster K means algorithm is used.



5) Flow utility function for packet

When the file is transmitted in the network, the file is sampled into equal number of small files. ie.,sampled into equal number of small flows.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)



VII. CONCLUSION

Effective coordination across multiple traffic monitors to improve network-wide flow monitoring.

REFERENCES

1. A. Ramachandran, S. Seetharaman,N. Feamster, and V. Vazirani, "Fast monitoring of traffic subpopulations," in Proc. *ACM SIGCOMM IMC*, Vouliagmeni, Greece, Oct. 2008, pp. 257–270.
2. C. Estan and G. Varghese, "New directions in traffic measurement and accounting: Focusing on the elephants, ignoring the mice", *Trans.Comput. Syst.*, vol. 21, no. 3, pp. 270–313, 2003.
3. C. Chaudet† E. Fleury‡ I. Gu´erin Lassous‡ H. Rivano "Optimal positioning of active and passive monitoring devices" in *Proc.ACM CoNEXT*, Toulouse, France, Oct. 2005, pp. 71–82.
4. J. Mai, C.-N. Chuah, A. Sridharan, T.Ye, and H. Zang, "Is sampled data sufficient for anomaly detection?," in *Proc. ACM SIGCOMM IMC*, Rio de Janeiro, Brazil, Oct. 2006, pp. 165–176.
5. N. Duffield and C. Lund, "Predicting resource usage and estimation accuracy in an IP flow measurement collection infrastructure," in *Proc. ACM SIGCOMM IMC*, Miami Beach, FL, 2003, pp. 179–191.
6. K. C. Claffy, G. C. Polyzos, and H.-W. Braun, "Application of sampling methodologies to network traffic characterization," in *Proc. ACM SIGCOMM*, San Francisco, CA, Sep. 1993, pp. 194–203.
7. G. R. Cantieni,G. Iannaccone,C.Barakat,C.Diot, and P. Thiran, "Reformulating the monitor placement problem: Optimal network-wide sampling," in *Proc. ACM CoNEXT*, Lisboa, Portugal, Dec. 2006, Article no. 5.
8. S. Raza, G. Huang, C.-N. Chuah, S. Seetharaman, and J. P. Singh, "MeasuRouting: A framework for routing assisted traffic monitoring," in *Proc. IEEE INFOCOM*, San Deigo, CA, Mar. 2010, pp. 1–9.
9. B. Fortz and M. Thorup, "Internet traffic engineering by optimizing OSPFweights," in *Proc. IEEE INFOCOM*, Tel-Aviv, Isreal,Mar. 2000, vol. 2, pp. 519–528.
10. A. David and V. Sergei, "K-means++: The advantages of careful seeding," in *Proc. ACM–SIAM SODA*, Philadelphia, PA, 2007, pp. 1027–1035.
11. .Medina, N. Taft, S. Battacharya, C.Diot, and K. Salamatian, "Traffic matrix estimation: Existing techniques and new directions," in Proc. *ACM SIGCOMM*, Pittsburgh, PA, Aug. 2002, pp. 161–174.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)