实时流测量体系结构的研究

张 睿，陈 鸣，宋丽华

(解放军理工大学指挥自动化学院 南京 210007)

【摘要】通过对基于流概念的实时流测量系统RFC 2722 RTFM的形式化描述，讨论了实时流测量系统中各元素之间的关系。在实时流测量系统的基础上，通过测量目标定义了系统中各元素间的协作关系，引入了资源策略服务器组件，建立了维护系统资源一致性的机制和适合目前因特网流量统计的分布式实时流监测体系结构，并讨论了其原型系统的实现。

关 键 词 实时流测量; 分布式实时流监测; 资源策略服务器
中图分类号 TP393.06 文献标识码 A

Research on the Real Time Traffic Flow Measurement System

ZHANG Rui，CHEN Ming，SONG Li-hua

(Institute of Command Automation, PLA University of Science and Technology Nanjing 210007)

Abstract Realtime Traffic Flow Measurement (RTFM) system architecture RFC2722 is described based on the concept of flow. The relations among elements RTFM system are also discussed. Based on RTFM, resource policy service component maintaining the consistency of system resource is introduced. The cooperating relations between each element are defined on the measurement object. Consequently, a distributed traffic flow measurement system architecture that adapt to Internet traffic management is given and the implementation of prototype system is discussed.

Key words realtime flow measurement; distributed traffic flow measurement; resource policy service

IETF RTFM工作组提出的实时流测量(Realtime Traffic Flow Measurement，RTFM)体系结构是网络测量研究中的一个极为重要的成果[1]。RTFM体系结构为用户提供了一种通用的监测实时流的架构，它有4个特点：(1) 流量统计测量具有实时性；(2) 用户可以动态地定义所要监测的流；(3) 所有的对象采用了管理信息库(Management Information Base，MIB)树的结构进行定义[2]，系统在控制、数据、规则和性能报告方面具有开放性和可扩展性；(4) 能够实现链路级流量监测功能，即对通过某一段共享链路、交换机或者路由器公共端口的数据进行监测。

流是指一次呼叫或者连接的人为的逻辑对应[1]。一个流是流量的一部分，对其进行开始时间和停止时间定界后，流就具有实时性，与一个流相关的属性值(源/目的地址、开始/停止时间、方向性、分组计数、字节计数等)具有聚合性质。通过微观上对具有实时特性流的记录、观察、统计和分析，可以获得实时流量的行为特征。

在因特网测量中，基于流概念的流量统计分析方法在工程上已被接受[1]，它在网络运行维护、网络管理、计费、流量工程和网络安全等方面已经得到了广泛应用[3-5]。

1 RTFM的体系结构

RTFM体系结构包含管理中心(Manager)、采集器(Meter)、收集器(Meter Reader)3类元素。

定义 1 RTFM的体系结构可以定义为$RTFM=<M, P, C, A_r, A_a, A_d>$：

(1) $M=\{M_1, M_2, \cdots, M_n\}$是RTFM系统中管理中心的集合； $P=\{P_1, P_2, \cdots, P_m\}$是流量采集器的集合；$C=\{C_1, C_2, \cdots, C_l\}$是流量收集器的集合。

收稿日期：2003 – 12 – 24
基金项目：国家“863”计划资助项目(2001AA112090)；江苏省自然科学基金资助项目(BK2001022)
作者简介：张 睿(1977 –)，男，山东威海人，博士生，主要从事网络测量和分布式计算方面的研究.

(2) M中的元素可以定义M_n =< R, A, L, α, β >。R={R_1, R_2, … , R_j}是流量采集规则的集合；A={ A_1, A_2, … , A_o }是管理中心的授权策略；L={L_1, L_2, … , L_s}是流生命周期的集合[1]；α：$R\rightarrow 2^M$，2^M表示管理中心集合M的幂集，$\alpha(R_j)$表示下载了规则R_j的管理中心集合；β：$M\rightarrow 2^R$，2^R表示采集规则集合R的幂集，$\beta(M_n)$表示名为M_i的管理中心加载的采集规则集合。

(3) C中的元素可以定义C_i=< D, T, γ,ζ > ：D={D_1, D_2, … , D_k}是流量采集器所采集数据的集合；T={T_1, T_2, … , T_q}是流量收集器收集数据的时间粒度的集合；γ：$D\rightarrow 2^C$，2^C表示流量收集器C的幂集，$\gamma(D_k)$表示收集流量数据D_k的流量收集器集合；ζ：$C\rightarrow 2^D$，2^D表示流量数据集合D的幂集，$\zeta(C_i)$表示名为C_i的采集器所采集数据的集合。

(4) A_r表示下载测量规则的动作[6]，可以定义A_r={<m, p, l >} ($r\in R$)；< m, p, l > ($m\in M$，$p\in P$，$l\in L$)表示管理中心m向流量采集器p下载流量采集规则r，并定义流的生命周期为l。

(5) A_a表示发布授权策略的动作，可以定义A_a= {< p, c>} ($a\in A$)；< p, c> ($p\in P$，$c\in C$)表示管理中心授予流量收集器c收集流量采集器p上的流量。

(6) A_d表示流量收集的动作，可以定义d={<p, c, t >}($d\in D$)；<p, c, t > ($p\in P$，$c\in C$，$t\in T$)表示收集器c以时间间隔t从采集器p上收集流量数据d。

管理中心可以通过操作命令动态地向采集器下载规则load r, m；卸载规则unload r, m。收集器可以通过操作命令实时地从采集器收集流量数据collect d, c。操作命令语义如表1所示。

表1 **RTFM**操作命令的语义

Load r, m	Unload r, m	Collect d, c
$\alpha(m)=\alpha(m)\cup\{r\}$	$\alpha(m)=\alpha(m)-\{r\}$	$\gamma(d)=\gamma(d)\cup\{c\}$
$\beta(r)=\beta(r)\cup\{m\}$	$\beta(r)=\beta(r)-\{m\}$	$\zeta(c)=\zeta(c)\cup\{d\}$

通过对RTFM体系结构的形式化分析能够得到结论：(1) P与C都隶属于M。P与C中每个元素与M中每个元素都存在对应关系，这表明系统资源能够得到充分的使用，同时也表明存在资源浪费问题，例如多个管理中心向同一个采集器下载相同的采集规则。(2) M中元素间是相互独立的，使用P, C上资源的权限也是平等的，这种关系会导致RTFM系统存在全局资源状态的不一致性问题。P, C中的资源是有限的，而RTFM系统缺少分配、统计系统全部资源和已用资源的机制。(3) P，C，M中元素之间是松耦合的关系且3种元素之间没有自发现机制。这种松耦合关系不利于各元素间的协作测量的实现。

2 DTFM的体系结构

定义 2 分布式实时流监测(Distributed Traffic Flow Measurement，DTFM)的体系结构为$DTFM$=<M, P, C, E, A_r, A_d, A_{mpc}>：

(1) M，P，C的定义与RTFM体系结构的定义相同。E是资源策略服务器可以定义为E=<(m', $m_{\max}$), (p', $p_{\max}$), (c', $c_{\max}$), O, φ, τ, μ, ρ, ξ >，其中m'，p'，c' 分别表示DTFM系统中正在使用的管理中心，采集器和收集器的资源数目；$m_{\max}$ ，$p_{\max}$ ，$c_{\max}$ 分别表示DTFM系统中管理中心，采集器和收集器资源的资源总数目；O={O_1, O_2, … , O_h,}是测量目标的集合，即测量的网络性能参数集合。

(2) φ：$M\rightarrow 2^{<P,C>}$，$2^{<P,C>}$表示<P, C >对集合的幂集；$\varphi(M_n)$表示每个管理中心可以使用的采集器和收集器资源集合，其中<P, C >表示收集器c对采集器上的数据进行收集。

(3) τ：$O\rightarrow 2^{<P,R>}$，$2^{<P,R>}$表示<P, R >对集合的幂集；$\tau(O_h)$表示完成测量目标O_h所需要的采集器和规则集合，其中<P, R>表示在采集器P上执行规则R。

(4) μ：$R\rightarrow 2^D$，$\mu(R_j)$表示规则R_j所产生的数据文件集合。由(3)，(4)可以推导出：

(5) ρ：$O\rightarrow 2^{<P,D>}$，$2^{<P,D>}$表示<P, D >对集合的幂集；ρ (O_h)表示测量目标O_h生成的数据与采集器的集合，可以根据该函数获得测量目标所需要的流量数据。由(2)，(5)可以推导出：

(6) ξ：$O\rightarrow 2^{<M,P,C>}$，$2^{<M,P,C>}$表示<M, P, C >对集合的幂集；ξ (O_h)可以获得完成测量目标数据所需要的管理中心、采集器、收集器的资源集合。

(7) A_{mpc}表示资源分配的动作，可以定义A_{mpc}={<m, p, c>}(a∈A)；<m, p, c >(m∈M，p∈P，c∈C)表示授予管理中心m使用采集器p上的一个流量采集资源，并使用流量收集器c进行收集。

定义 3　NUM()为求资源数值函数，则∑NUM($\varphi(M_n)$)=∑NUM(P^i)+ ∑NUM(C^j)并且∑NUM(P^i)≤p_{max}，∑NUM(C^j) ≤c_{max} 。

在DTFM体系中，O集合中的一个元素就代表了DTFM中的一个分布式流量测量任务。要实现任务集合O中某个元素的测量，管理中心首先要执行操作命令Booking o向资源策略服务器进行资源预约，预约成功后再通过操作命令dispense o发布测量目标任务，结束测量目标任务callback o。操作命令语义如表2所示。每个管理中心采用表1中定义的load r, m，unload r, m操作命令执行测量任务；每个收集器采用collect d, c操作命令执行数据采集的任务。

表2　**DTFM**操作命令的语义

Booking o	Dispense o	Callback o
$\xi(o) \rightarrow$ {<m, p, c>}	$\xi(o) \cup$ {<m, p, c>}	$\xi(o)-$ {<m, p, c>}
if　(NUM($\varphi(m)$)>0) then success else failure	$\varphi(m)-$ {<p, c>}	$\varphi(m) \cup$ {<p, c>}

通过DTFM结构解决的问题主要有：

(1) 利用资源策略服务器分配并维护DTFM系统资源的使用状况，解决了RTFM系统中资源状态的不一致性问题，同时提高系统的灵活性和资源利用效率。

(2) 通过在资源策略服务器中预定义测量目标O与采集器间的协作关系实现了分布式测量任务的定义。

(3) 定义了测量目标O与流量数据D、测量目标O与收集器C间的关联关系，根据上面定义的关系，资源策略服务器可以推导出完成测量目标所需要的资源集合。

3　DTFM原型的实现

基于DTFM结构的原型系统功能主要有两大部分：系统资源管理和测量任务执行。系统分布情况如图1所示，系统结构和相关接口如图2所示。系统资源管理功能由资源策略服务器完成，包括：

(1) 组件信息服务。维护各类组件(管理中心或者采集器)的命名、隶属、地址、权限、状态等信息，提供组件信息的全局视图。每个合法的管理中心和采集器入网后都必须向资源策略服务器发送注册信息和自身的资源状态报告信息。

(2) 利用$\varphi(M_n)$函数为每个管理中心分配可以使用的采集器资源。使用$\tau(O_h)$函数定义测量目标与测量资源(管理中心和采集器)的对应关系。

(3) 时钟服务。提供全系统时钟同步。资源策略服务器物理上可能不止一个，但逻辑上应是唯一。

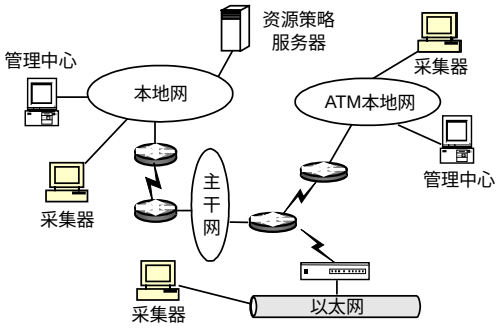

图1　DTFM系统组件分布

测量任务执行由管理中心(原型中的管理中心集成了收集器的功能)和采集器实现。

管理中心的功能：

(1) 根据测量目标，管理中心使用load指令向一个或多个采集器发布采集规则。

(2) 根据测量目标使用collect指令从一个或多个采集器上收集流量数据。收集的方式可以根据测量目标的需求选用实时收集方式或者历史文件收集方式。RTFM系统采用了实时收集的方式，采集器上并不保存流量数据的记录。在DTFM系统中，引入了历史数据文件的概念，对于无实时性需求的采集数据，例如事后故障分析和行为追踪的数据，不实时传回管理中心，而是将数据文件存储在采集器上，形成历史文件，一个管理中心下发的采集规则所采集的流量数据可以提供给其他管理中心使用。这些文件只在需要或者网络空闲时才被传输，过期的历史文件则被定期删除。

采集器的功能：

(1) 流量采集。采集器位于共享网段、路由器或者交换机的监听接口处，根据采集规则对监听的数据进行过滤，采集有用数据。采集器可以根据管理中心的需求产生实时流记录或者历史文件。

(2) 历史数据文件的管理。采集器将流量记录以文件的方式在本地保存，并定期进行更新。

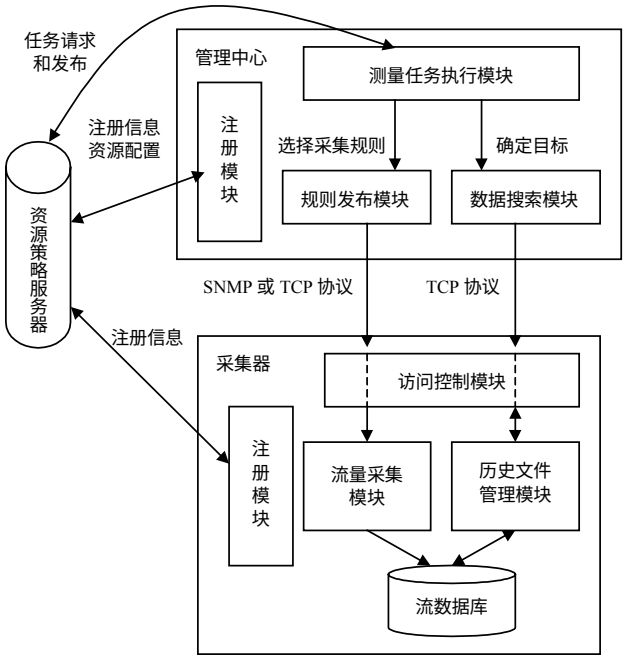

图2 DTFM的体系结构及相关接口

4 结 束 语

本文实现了一个(Network mEsurement System Platform，NESP)的网络监测平台，已经达到了实用化的程度。某些大型网络系统已经使用了NESP网络监测系统作为监控网络运行状况的流量监测平台。实践证明，DTFM系统比RTFM系统具有更好的稳健性和更强大的监测功能。

参 考 文 献

[1] Brownlee N, Mills C, Ruth G. Traffic flow measurement: Architecture[S]. RFC2722, 1999.

[2] Brownlee N. Traffic flow measurement: Meter MIB[S]. RFC2720, 1999.

[3] Barakat C, Thiran P, Iannaccone G, et al. Modeling internet backbone traffic at the flow level[J]. IEEE Transactions on Signal Processing Special Issue on networking, 2003, 51(8): 2 111-2 124.

[4] Ata S, Murata M, Miyahara H. Analysis of network traffic and its application to design of high-speed routers[J]. IEICE Transactions on Information and Systems, 2000, E83-D(5): 988-995.

[5] Agarwal D, Gonzalez J M, Jin Gujun, et al. An infrastructure for passive network monitoring of application data streams[C]. 2003 Passive and Active Measurement Workshop, Lajolla, California, 2003.

[6] Brownlee N. SRL: A language for describing traffic flows and specifying actions for flow groups[S]. RFC2723, 1999.

编 辑 漆 蓉