

基于主动网络的 Policy-control 研究

王宣政^{1,2}, 钱德沛¹, 马素刚²

(1. 西安交通大学电信学院, 西安 710049; 2. 西安邮电学院计算机系, 西安 710061)

摘要: 结合主动网络的机制和 IntServ 体系结构, 提出了一种主动网络支持的基于代理-管理者的策略控制机制, 可以简化中间节点策略控制复杂性, 保证在一个管理域中的策略一致性, 并且可以实现控制策略代理的动态部署、更新。在此基础上, 提出了基于发送用户的策略控制方法。

关键词: 主动网络; 策略控制; RSVP

Research of Policy-control Based on Active Network

WANG Xuanzheng^{1,2}, QIAN Depei¹, MA Sugang²

(1. Institute of Telecommunication, Xi'an Jiaotong University, Xi'an 710049;

2. Computer Department, Xi'an Institute of Post & Telecommunication, Xi'an 710061)

【Abstract】 Based on active networks and IntServ architecture, a policy-control mechanism based on agent-manager supported by active networks is presented, the policy-control in intermediate nodes can be simplified, the consistence can be kept, and the RPA can be deployed or updated dynamically. And a policy-control method based on sender is provided.

【Key words】 Active network; Policy-control; RSVP

在 IntServ 体系结构中, 策略控制(Policy-control)负责判断用户是否具有合法的身份获得相应的服务质量。信令协议 RSVP 的相关消息携带的策略控制信息经过中间节点的策略控制模块处理, 从而判断出用户是否可以获得请求的资源。

策略控制的实现可以集中在中间节点实现, 这样在中间节点需要有策略控制代码及用户信息。这种方法在实现时存在一些问题, 一方面, 节点中需要存储与策略控制相关的用户信息, 因此, 需要解决在中间节点加载和存储用户信息的问题; 另一方面, 在各 RSVP 主动节点中存在如何保持用户信息数据及策略处理的一致性的问题。

为此, 提出了一种主动网络支持的基于代理-管理者的策略控制机制并且基于发送用户身份实现策略控制。

1 主动网络支持的基于代理-管理者的策略控制

1.1 功能模型

定义 1 一个基于代理-管理者的策略控制系统 AMPCS 由一个四元组构成, $AMPCS = \{N, PA, PM, f\}$ 。其中:

N : 网络中中间节点的集合, 提供策略控制机制。记作 $N = \{n_1, n_2, \dots, n_i\}, i \rightarrow \infty$ 。

$PA(PolicyAgent)$: 策略代理的集合。记作 $PA = \{pa_1, pa_2, \dots, pa_k\}, k \rightarrow \infty$ 。

$PM(PolicyManager)$: 策略管理者的集合。记作 $PM = \{pm_1, pm_2, \dots, pm_l\}, l \rightarrow \infty$ 。

f : N, PA, PM 之间的运算关系, 在 AMPCS 中任何一个中间节点, 都存在一个策略代理与一个策略管理者进行交互。即 $\forall n_s \exists pa_i, f(pa_i, pm_u)$, 其中, $n_s \in N, pa_i \in PA, pm_u \in PM$ 。

定义 2 一个主动网络支持的基于代理-管理者的策略控制系统 ANPCS 由一个四元组构成, $ANPCS = \{N, E, PA, g\}$, 其中:

N : 主动节点的集合。可记作 $N = \{n_1, n_2, \dots, n_i\}, i \rightarrow \infty$ 。

E : 主动节点中主动网络执行环境的集合。记作 $E = \{e_1, e_2, \dots, e_j\}, j \rightarrow \infty$ 。

PA : 策略代理的集合。记作 $PA = \{pa_1, pa_2, \dots, pa_k\}, k \rightarrow \infty$ 。

g : N, E, PA 之间的运算关系, 在任何一个主动节点中, 存在一个主动网络的执行环境, 支持对应的策略代理按照部署策略在该主动节点中动态部署, 即: $\forall n_x \exists e_y, pa_z = g(n_x, e_y)$, 其中, $pa_z \in PA, n_x \in N, e_y \in E$ 。

定义 3 策略域 d 是一些节点和对应的管理代理的集合, 有权决定其中的控制策略, 即用户使用该域中资源的权限。表示为 $d = \{pm, n_1(pa), n_2(pa), \dots, n_j(pa) \mid j=1, 2, \dots\}$, 其中 $n_j(pa)$ 表示节点 n_j 中部署有策略代理 pa , 而策略代理 pa 通过与 pm 的交互实现该域中的控制策略。

在一个主动网络支持的 IntServ 体系结构的管理域 d 中, 有一个 RSVP 策略管理者 RPM(RSVP Policy Manager), 每个主动节点中有一个 RSVP 主动网络执行环境 RANEE, RSVP 策略代理 RPA(RSVP Policy Agent)按照部署策略在 RANEE 中动态部署。当 RSVP 协议的消息到达中间节点, 其中的策略控制对象传递到 RPA, RPA 按照某种协议(如 COPS 协议)与 RPM 进行交互, 获得策略控制的结果, 结果返回到 RSVP 协议实体。

1.2 体系结构

如图 1 所示, 为 RSVP 的策略控制实施机制: 两个相邻的域 d_x, d_y, d_x 中有主动节点 $\{n_i, n_j, n_k, n_l, \dots\}$, 每个节点中动态部署有策略控制代理 RPA_x , 该域中有策略控制管理者 RPM_x 。 d_y 中有主动节点 $\{n_u, n_v, n_w, n_x, \dots\}$, 节点中部署有 RPA_y , 可

基金项目: 国家自然科学基金资助项目(69973036, 90104022)

作者简介: 王宣政(1966 -), 男, 副教授, 主研方向: 计算机网络及体系结构; 钱德沛, 教授、博导; 马素刚, 助教

收稿日期: 2006-02-28 **E-mail:** wangxuanzheng@263.net

以与该域中的RPA_x进行交互。

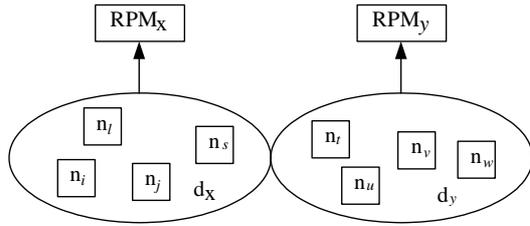


图1 Policy_control 的实施机制

在基于主动网络的RSVP体系结构中，每一个主动节点存在RSVP主动网络执行环境RANEE，RPA策略控制代理代码在RANEE的支持下动态部署到主动节点中。

在一个域中，负责策略控制部署的站点按照某种部署策略在同一个域的所有主动节点中部署相同的控制策略代码，主动节点中策略控制的相关模块如图2所示。

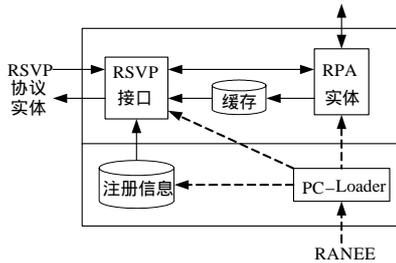


图2 策略控制的加载和执行示意图

PC-Loader：即策略控制加载器，接收RANDP（RSVP主动网络部署包），按照策略控制类的加载树，加载RPA实体及与RSVP接口类并在RANEE中执行。

注册信息库RIB：在PC-Loader接收RANDP包时，注册所在域的标识以及该域中RPM的标识，RPM的标识为IP地址及端口号。

RSVP接口：与RSVP协议的接口，该接口的作用为：

(1)接收RSVP相关消息中的策略控制对象，根据策略控制对象中的信息、注册信息库中的注册信息、缓存中的信息判断该用户在该域中是否已经通过认证，如果已经通过认证，则返回策略控制对象及认证结果到RSVP协议；否则，将相关信息传送到RPA实体处理。

(2)接收RPA实体返回的策略控制信息及认证结果，按照策略控制对象的格式组织信息，并返回策略控制对象及认证结果到RSVP协议。

缓存（Policy cache）：在缓存中存放有最新的用户认证信息，如果有策略控制对象需要认证，先查找缓存信息，这样，可以减少策略控制所消耗的时间。

RPA实体（RPA entity）：接收RSVP接口的认证请求，向该域中的RPM发出认证请求，接收RPM返回的认证结果，返回策略控制信息及认证结果到RSVP接口。

RPA实体与RPM的交互按照COPS协议进行。在RPM中，有该域中需要QoS保证的注册用户及请求资源预留的权限等信息，以及其他域中的注册用户在本域中的权限信息。RPM根据这些信息以及RPA的认证请求，判断出相应的用户是否有请求资源预留的权限，并作出允许或拒绝的判断，返回到RPA。

这种体系结构的特点体现在：

(1)简化中间节点：在中间节点中，只需要部署RPA，而无须保存用户信息。

(2)用户信息的一致性：用户的信息保留在RPM中，在同一个域中没有用户信息的一致性问题。在不同域中用户信息的一致性问题可以通过不同域的RPM之间的交互实现。

(3)策略的灵活性：在不同域中实现不同的管理策略，只需要在同一域中实现RPA和RPM的匹配。而且可以在中间节点中动态部署RPA、更新RPM，实现控制策略的更新。

2 基于发送用户的Policy_control

RSVP协议的操作的基本过程是：由发送方发出PATH消息，在所经过的中间节点建立“Path-State”；接收方返回RESV消息，在中间节点设置包分类器、调度器的参数并建立“Resv-State”。在“Path-State”和“Resv-State”中有策略控制的信息。

在IntServ模型的应用中，存在一个问题，即协议的伸缩性问题，资源的预留是针对特定的流，对于需要服务质量保证的每一个流，在中间节点上都需要保留相关的状态信息。因此，在应用策略控制时，必须考虑对协议的伸缩性的影响，即在中间节点上不因为引入策略控制机制而增加状态项，从而保持与RSVP协议一样的伸缩性。

如图3所示是一个简单的多播树。从q经过p，在p点复制报文，向r和s传输。假设一个流从q、p、r、s方向传输，则RSVP协议的PATH消息在q、p、r、s节点中为该流建立“Path-State”状态信息。而从r、s方向的RESV消息在p点要进行“Resv-State”状态的合并，如果从r、s方向的RESV消息中的策略控制信息包含有不同的决策信息，则在节点p中要保持不同的预留状态信息，这样就会存在“状态爆炸”的可能。而基于发送用户的策略控制在RESV消息中的策略控制信息是发送用户的相关信息，因此，在节点中可以进行状态合并。

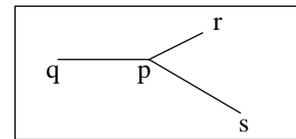


图3 传输路径示意图

2.1 RSVP消息中POLICY_DATA的定义

在RSVP的消息中，POLICY-DATA对象用于策略控制。在基于发送用户的策略控制中，需要对RSVP相关消息的POLICY_DATA进行定义。RSVP的PATH消息、RESV消息中，用于策略控制的POLICY_DATA，POLICY_DATA定义为：

<POLICY_DATA> ::= <CLIENT ID><DOMAIN ID><CURRENT-DOMAIN ID>

其中

CLIENT ID：用户标识，一个用户在一个特定域中注册，获得CLIENT ID。

DOMAIN ID：域标识，每一个域有唯一的标识。由CLIENT ID和DOMAIN ID唯一标识一个用户。

CURRENT-DOMAIN ID：当前域的标识。标识PATH消息所经过节点所在的域。

2.2 处理过程

当PATH、RESV消息到达中间节点时，RSVP协议实体提取其中的POLICY-DATA，传递到策略控制代理RPA处理，处理流程如下：

if <CURRENT-DOMAIN ID> == <DOMAIN ID in RIB>

```

return (POLICY-DATA , accept) to RSVP
/* 如果 POLICY-DATA 中 CURRENT-DOMAIN ID 与 RIB 中注册的
DOMAIN ID 相同,表示该 POLICY-DATA 中的用户在当前域中已
经得到认证。当一个消息在同一个域中传输时,只需要一次认证,
即只需要在该域的边界节点得到认证。 */
else
    if found ( CLIENT ID , DOMAIN ID ) in Policy cache
        return ( POLICY-DATA , accept) to RSVP
/*如果在缓存中有该用户的标识 ( CLIENT ID , DOMAIN ID ),表
示该用户在最近已经得到认证,不需要重新认证。由于 RSVP 协议
的 PATH、RESV 消息是周期性的,周期性的消息可以在缓存中获得
认证信息,从而减少处理时间*/
else
    if ( RPA entity ( CLIENT ID , DOMAIN ID )) ==accept
        {<CURRENT-DOMAIN ID>:=<DOMAIN ID in RIB>;
        write to Policy cache ;
        return ( POLICY-DATA , accept) to RSVP ;}
/*通过 RPA 与 RPM 的交互作用,获得该用户的认证结果。如果通
过认证,则修改 POLICY-DATA 中 CURRENT-DOMAIN ID 信息;
写用户信息到缓存;返回新的 POLICY-DATA*/
else
    return ( POLICY-DATA , deny )

```

根据策略控制部分返回的信息, RSVP 协议实体进行相应处理:

如果通过策略认证,并通过许可控制认证,则修改消息的有关部分,继续向下一个节点传输消息;如果没有通过认证,则发出 PathErr 或 ResvErr 消息,拆除在相关节点上建立的状态。

RSVP 针对特定的流进行资源预留,而用户应用的交互是双向的,存在着两个方向的预留,因此,两个方向上的发送用户在所经过的域中都会经过认证。

3 结束语

本文提出了一种主动网络支持的基于代理-管理者的策略控制机制,利用主动网络的特点,在每一个策略管理域中,设置一个 RPM 站点,并且在该域的主动节点中部署对应的 RPA,这样可以保证 RPM 和 RPA 的匹配,并有效地实现策略控制功能。

在此基础上,提出了一种基于发送用户的 Policy-control 策略,当 RSVP 消息到达中间节点,根据消息中的发送用户信息进行策略判断。这样可保持策略控制的伸缩性与 RSVP 协议的伸缩性一致。对于该策略还有一些问题需要研究:

(1)对用户申请的资源进行控制。包括限制申请的资源,在资源不足的情况下,对预留情况进行主动控制,例如,根据用户的权限不同,实现对预留的控制,包括拆除、预留资源的修改等。

(2)在不同域中注册的用户在跨越多个域进行资源预留时的策略控制问题。例如:在每个域的边界节点,对相应的用户要进行策略控制认证,在 RPM 中如何获得其他域中注册的用户信息;其他域中的注册用户在本域中的资源预留的认证如何判断等。

参考文献

- 1 Jackson A W, Sterbenz J P G, Condell M N, et al. SENCComm Architecture[Z]. 2000-04. <http://www.ir.bbn.com/projects/senccomm/>.
- 2 Wetherall D, Legedza U, Gutttag J. Introducing New Internet Services: Why and How[J]. IEEE Network, 1998, 12(3): 12-19.
- 3 Peterson L. Node OS Interface Specification[Z]. 2001-01. <http://www.dcs.uky.edu/~calvert/arch-docs.html>.
- 4 Calvert K L. Architecture Framework for Active Networks Version 1.0[Z]. 1997-07. <http://www.dcs.uky.edu/~calvert/arch-docs>.
- 5 Yavatkar R, Pendarakis D, Guerin R. A Framework for Policy Based Admission Control[S]. RFC 2753, 2000-01.
- 6 王宣政, 钱德沛. RSVP 主动网络执行环境的设计[J]. 计算机工程, 2005, 31(9): 51-53, 111.

(上接第 101 页)

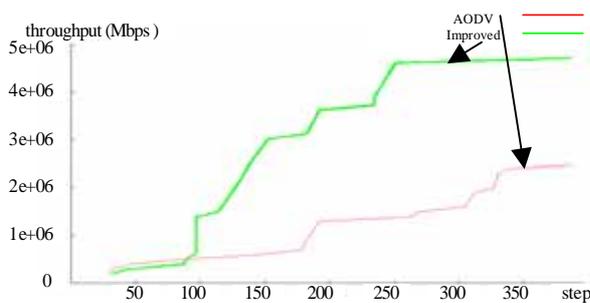


图 3 AODV和AODV改进协议的吞吐率比较

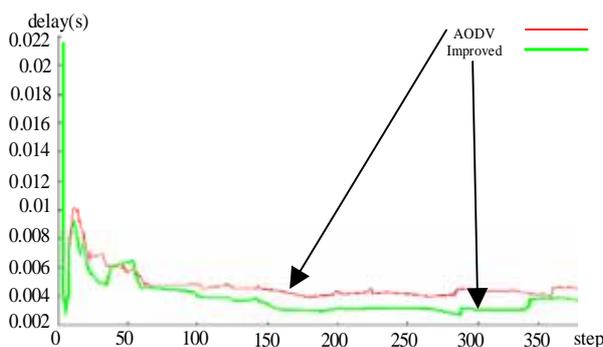


图 4 AODV 和 AODV 改进协议的时间延迟比较

4 结语

本文提出了一种基于概率推理的路径选择算法,并用 OMNET++ 对原 Ad-hoc 网络和改进的 Ad-hoc 网络进行了仿真,并根据所获得的节点适应度值,采用智能决策,更好地认知网络拓扑变化,提高网络 QoS。仿真结果显示,改进的 AODV 比原 AODV 有较高的吞吐量、较低的延迟。

参考文献

- 1 Elizabeth M, Belding R, Charles E P. Evolution and Future Directions of the Ad Hoc On-demand Distance-vector Routing Protocol[C]//Proc. of IEEE International Conference on Computer Communications and Networks. 2003: 125-150.
- 2 Nicola C. Simulation of Ad Hoc Network[D]. Berlin, Germany: Bologna University, 2003.
- 3 Abolhasan M, Wysocki T, Dutkiewicz E, et al. A Review of Routing Protocols for Mobile Ad Hoc Networks[J]. Ad Hoc Networks, 2004, 2(1): 1-22.
- 4 Xu Bangnan, Hirschke S, Walke B. The Role of Ad Hoc Networking in Future Wireless Communications[C]//Proc. of International Conference on Communication Technology.
- 5 Chung Weiho. Probabilistic Analysis of Routes on Mobile Ad Hoc Networks[J]. IEEE Communications Letters, 2004, 8(8): 506-508.