基于 QoS 的 IP VPN 的研究

李振东　谢　立
（南京大学计算机软件新技术国家重点实验室　南京210093）
（南京大学计算机科学与技术系　南京210093）

A QoS-Based IP VPN Architecture Research

LI Zhen-Dong　XIE Li
(State Key Lab for Novell Software, Nanjing University, Nanjing 210093)
(Depertment of Computer Science and Technology, Nanjing University, Nanjing 210093)

Abstract　Constructing Virtual Private Network (VPN) over public network infrastructure (Internet) is becoming the foundation of the next generation network service. At present, VPN mainly focuses on the security property, while it is lack of consideration of QoS. On the basis of analyzing the Differentiated Services (Diffserv) and IPsec, we put forward a QoS-based IP VPN Architecture Model which is a tri-tier model that is composed of ESN, ISN and VPN node. It combines encrypted channel mechanism of IPsec and the edge-and-core-model of Diffserv. It provides end-to-end QoS while assures security.

Keywords　Virtual Private Network (VPN), QoS, IPsec, Diffserv

1　引言

简单讲，虚拟专用网(Virtual Private Network)是利用公共网络基础设施(如 Internet)来仿真专有广域网络[1-3]，以下简称 VPN。它正快速成为新一代网络服务的基础。

目前 VPN 有多种类型，其中最主要的是基于 IP 的 VPN 与 MPLS-VPN，这两种 VPN 各有优势。本文所关心的不是如何论证谁更合适，这超出本文的范围。我们所关心的是如何在 IP-VPN 体系结构上提供服务质量保证。

正如定义中所描述的，VPN 是利用公共网络设施模拟专用广域网络，它利用的是公共网络低廉的价格优势与分布优势提供高性能价格比的服务。这就带来两个问题，安全和服务质量。由于 VPN 的基础设施是公共网络，那么它面临着被攻击、泄密的风险；同时，公共网络随时可能由于访问量等原因造成阻塞，导致服务质量急剧下降。如果无法解决上述问题，那么 VPN 所带来的性价比将无法真正超过专用网络。

以往的文献对 IP-VPN 的讨论主要集中于安全领域(IPsec[1,3,4,8])，如何防止攻击与泄密，而缺乏对 QoS 的考虑。在框架性文献[1]中，对 QoS 的考虑也只是 OSI 7层模型中的物理层、链路层，而对大范围 IP-VPN 部署时端到端的 QoS 保证，仍是未解决的问题。

本文主要从 QoS 角度出发，通过对 Internet 区分服务体系结构(Diffserv)和 IP 安全体系 IPsec 的介绍分析，提出一种结合 Diffserv 与 IPsec 的 IP-VPN 体系框架结构，在保证安全的前提下提供端到端的服务质量保证。

2　区分服务与 IP 安全体系简介

2.1　区分服务

Internet 的飞速普及正深刻地改变着人们的生活，随着多媒体技术的发展，Internet 正逐步由单一的数据传输转化为数据、语音、图像等综合信息传输。但是 Internet 现有的传输方式仍旧为尽力而为(best-effort)，这主要因为 Internet 体系结构的构建思想[10]是：应将流相关的状态等信息保留在终端系统中，而网络则尽可能简单。也就是所谓的智能边缘一简单网络模型。它在 Internet 发展中取得巨大成功，但是随着多媒体、实时业务对网络的可预测性、可控性(延时、抖动、带宽、丢失率)的严格要求，它已经无法满足。

针对这种情况，IETF 的 IntServ 工作组从文[9]起，制定很多的框架文件，在此方面作了很多工作。IntServ 提供的是基于每个流的分类、排队、调度(CQS)，动态的资源预留机制，这种依赖于每个流的状态和对每个流的管理一方面：使 Intserv 能够提供很高的灵活性，可以提供多级别的服务；但是另一方面它导致了极大的复杂性，可扩展性和鲁棒性问题。这使得 Intserv 始终无法走出实验室，在 IntServ 遭遇困难的时候，近几年区分服务 Diffserv[5]应运而生。

与前者不同，区分服务不需要一个单独的资源预留信令机制和相应的显式资源分配过程，同时简化了内部节点的服务对象，服务对象是流的汇聚(stream aggregate)，而非单个的流。这样整个网络被转化为：所有相关业务量的分类、调节、及状态的保存全部推到网络的边缘路由器，而内部节点是状态无关的，它只处理数量有限的汇聚流。

边界路由器根据用户业务量规约(traffic profile)将进入网络的业务量(Traffic)通过多域(MF)分类、标记、整形，聚合为不同的流聚集。每种汇聚可能将得到网络不同的服务，这种聚集信息存储在 IP 包头的 DS 标记域中(IPv4TOS 域)[12]，称为 Diffserv 编码点(DSCP)。主干路由器在转发 IP 包时，根据 DSCP 选择特定质量的调度转发服务，这种中继行为称为每跳行为(Per-Hop-Behavior, PHB)。

在同一个域内对 PHB 的定义与行为必须一致，在两个 DS 域之间，允许对 PHB 分别定义，它们之间通过服务等级协

李振东　博士研究生，主要研究领域为计算机安全、网络服务质量。谢　立　博士生导师，主要研究领域为计算机安全、分布式计算、并行系统。

定(Service Level Agreement, SLA)与业务量调节协定(Traffic Conditional Agreement,TCA)来协调跨区域的服务。

2.2 IPsec

VPN 最主要的特点是其私有(private)性,由于它的载体是公用网络,则必须保证它所传送信息的机密、完整、可用、可信。目前,在网络层主要的实现方式是 IPsec[8]。

IPsec 提供了一种标准的、健壮的以及包容广泛的机制,可用它为 IP 层提供安全的保证。它定义了默认的、强制实施的算法,以确保不同的实施方案相互间可以互通。IPsec 本身是一个协议套件,包括验证头(AH),封装安全载荷(ESP),Internet 密钥交换(IKE)等,它的主要机制是采用隧道(tunnel)机制与加解密技术。

验证头(AH)提供了数据包的完整性、数据源验证以及抗重播攻击的能力,但不能保证数据的机密性,封装安全载荷(ESP)则更进一步,除具验证头能力外,确保数据包的机密性。AH 与 ESP 的安全保障能力完全取决于所采用算法的强度。IPsec 提供的安全服务需要参与会话的双方共享密钥,IKE 协议就是在通信双方之间,建立起共享安全参数及验证过的密钥。一种典型的隧道化的包保护(图1)。

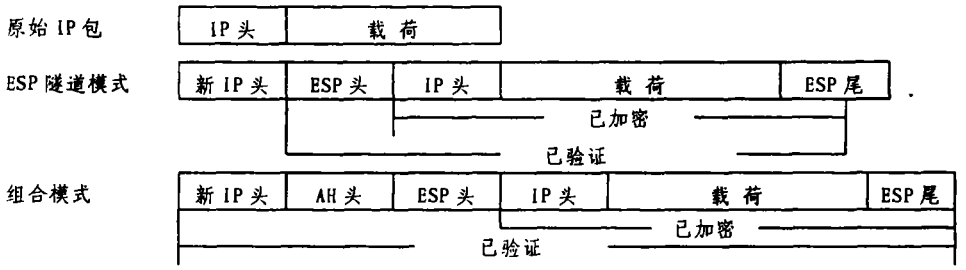

图1 一种典型的隧道的包保护

通信的双方由受保护的 IP 包的内部头指定,发送方安全网关(隧道起点)负责将原始 IP 包加密封装(Encapsulate)到新的 IP 包,加密终点(隧道终点)则是外部 IP 包头指定的地点,它在处理结束时,会剥离出原始 IP 包,并转发到目的地。

两个安全网关之间可能建立多个隧道,每个隧道内可容纳多个流,隧道采用 AH 和 ESP 头中的安全参数索引(SPI)作为隧道的唯一性标识。

3 基于 QoS 的 VPN 体系结构

在上节中我们简要介绍了区分服务和 IPsec,可以看出,它们的体系结构存在相似之处,并有着很好的结合点,这也是本文研究的重点。

1)流汇聚 vs 隧道:区分服务处理的是流的汇聚,根据相同的 DSCP 值得到特定的 PHB,而单个隧道是汇聚多个流后被加密。它们处理的粒度非常相似(两个端点之间可能有多个不同的流汇聚,也可以有多个隧道)。

2)区分服务处理的是粗粒度的流汇聚,因此具备很强的伸缩性,非常适合在主干上部署。而 VPN 隧道在穿越 ISP 时,其内部的流对外是透明的,不需要非常细粒度 QoS 支持。

3)区分服务与 VPN 本身主要都是加强了边界路由器的功能。区分服务要完成多域(MF)的分类,流状态的保存,DSCP 映射,IPsec 完成流进出隧道的加解密。

因此,可以看到,区分服务与 IPsec 可以很好地结合,关键的结合点就是在边界路由器上,它同时作为区分服务和隧道的入出口,它在保留流的状态,完成分类后,还要进行原始数据包进出隧道的加解密,以及 DSCP 值的映射。

此外,今天的 Internet 是由多个 ISP 所控制的自治系统(AS)组成的,端到端往往会跨越多个 ISP。因此,端到端的 QoS 是 ISP 之间边缘到边缘的 QoS 以及 ISP 内部提供的 QoS 级联而成。ISP 内部的 QoS 是较容易控制的,ISP 之间的边缘到边缘的 QoS 是本文所关心的。文[13]中提出了带宽代理(Bandwidth Broker,BB)的概念,它的作用是在两个相邻的 DS 域之间,通过协商来完成相互的资源分配、流量控制、维护双方的协定。若两个不相邻 DS 域之间存在非运行 DS 的域,则逻辑上把它简化为一条链路。

下面给出基于 QoS 的 IP VPN 的体系框架。

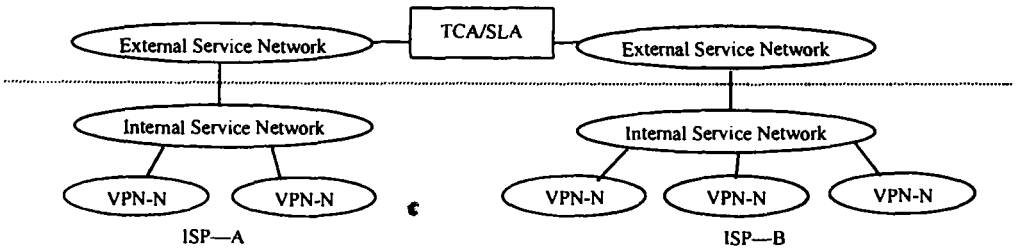

图2 基于 QoS 的 IP VPN 体系框架图

整个 ISP 主干运行的是区分服务,在这个基础上,在每个 ISP 范围内,IP VPN 的体系框架由三层组成:外部服务网(External Services Network,ESN),内部服务网(Internal Services Network,ISN),VPN 节点(VPN-N)。其中,ESN 与 ISN 属于 ISP 主干,其上提供的是区分服务,由管理器与其控制的路由器和链路组成;而 VPN-N 则是用户的本地网络。它们之间的关系是自上而下,上层管理直接下属,制定下层遵循策略,下层向上层提出服务请求。同时,ISP 之间的协商由最上层完成。

在此体系框架中,外部服务网 ESN 是 ISP 内部管理 VPN 的最顶层机构。首先,它要负责制定整个 ISP 内部的整体策略;其次,它负责管理各个 ISN,协调 ISN 之间的关系;再

者，它负责与相邻的ISP的ESN协商、签署、维护双方的业务量调节协定/服务等级协定TCA/SLA，同时据此动态地与之协商边缘到边缘的资源预留与分配；最后，多个VPN节点共同在逻辑上构成一个VPN域，这些节点可能跨多个ISP，而ESN也是ISP内部唯一了解和管理全部VPN域构成的拓扑结构的组织。

在ISP的内部，ESN可以只有一个，也可以由于规模原因有多个。前者明显是一个集中式管理方式，比较简单；后者则将是一个分布式系统，各个ESN之间将动态共享信息，这增加了实现的复杂性，但是有较强的健壮性。

ISP内部有多个ISN，它们处于模型的中层，每个ISN都唯一地服从某个ESN的管理，同时它又管理着多个VPN节点。它的职责是向上负责动态向ESN提出资源要求，报告资源的释放；向下它管理各个VPN节点，负责制定VPN节点的带宽，提供服务的等级，接纳用户的业务量，负责计费和流量控制。同时作为VPN业务量的接入点，它与VPN节点的边缘也是VPN隧道的进出点，要完成数据包的封装、加密、认证等安全相关工作。

ISN的边缘路由器对VPN节点注入网络的业务量起到直接管理的作用，它通过对业务量的多域分类、排队、整形、管制、调度等方法，抑制了流之间的干扰，保证业务得到的服务，将VPN域的业务平滑地注入到网络中。同时，它还要在将用户的数据包封装加密的同时完成DSCP域的映射。

VPN节点(VPN-N)也就是用户的本地网络，是整个结构中的叶子节点，它是结构中业务的发起点。多个VPN节点(一个ISP或多个ISP上)共同逻辑上组成一个虚拟专用网VPN，简称一个VPN域。一个VPN节点可以很简单，如一台移动主机，也可以很复杂，如某企业、组织的大型本地网络。

VPN节点除了根据与ISP的合约(Traffic Profile)来使用带宽外，有关授权、访问控制等安全方面的工作将由VPN节点来完成。对于规模较大的节点，它本身也会对注入网络的流量作相应的控制(并不强制要求其中路由器具备QoS功能)。

下节中将对组成的每个部分的结构及功能详细描述。

4 详述及分析

4.1 模型组成部件

4.1.1 ESN的组成 由主控部分(ESN主管理器，带宽代理器(BB)、带宽管理守护进程(BD))、与相邻的ISP连接的边界路由器(BR)及相应资源数据库(TCA/SLA、State、Resource、Price、VPN拓扑等数据库)组成(见图3)。

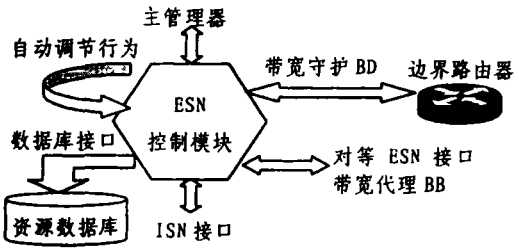

图3 ESN结构

根据ESN的职责，ESN主管理器负责管理与相邻的ISP协商制定相互的TCA/SLA；通过与ISN的接口管理所属的ISN，制定ISN所遵循的策略，如PHB映射；维护它的资源数据库；同时对VPN域进行全局的管理。

由于VPN节点网络内部的地址空间可以完全与整个网络无关，因此需要在ISP的边缘路由器上提供虚拟路由表[1]。对于IP-VPN，一个很重要的问题是随着VPN域的改变，虚拟路由表的全局动态维护问题。在本文框架中，ESN全局了解VPN逻辑拓扑结构并进行管理，因此对VPN域的任何操作，ESN的主控程序将动态地通过与ISN的接口将更新信息传递到ISN，并由ISN更新边缘路由器中的虚拟路由表，保证了全局一致、可控。

带宽管理(BB)：负责动态地与相邻的ISP的带宽代理根据TCA/SLA协商带宽的分配、预留；负责向BD下达带宽预留、撤销指令；对带宽的预留结果作主动回答。

带宽管理守护进程(BD)：负责根据指令配置边界路由器，根据策略动态维护状态数据库，并防止边界链路因为未主动释放而长期被占用。

边界路由器(BR)：两个相邻的ISP通过各自的边界路由器直接相连，它的作用是根据带宽代理协商的预留带宽将业务量平滑注入对方网络，对于进入本网络的超过预留的业务量作OUT标记，当出现阻塞时这些包将被优先丢弃。同时，它们根据带宽代理协商的结果动态地完成数据包的DSCP值的映射转换，以得到期望的服务。

主要资源数据库描述：

VPN-logic 拓扑结构数据库：描述了ISP内的VPN域、VPN节点的拓扑结构

VPN域描述〈VPN-D-ID(域标识)，Desc〉

VPN节点描述〈VPN-N-ID(节点标识)，Desc〉

VPN关系描述〈VPN-D-ID，VPN-N-ID，destAddress，邻接ISP，目的ISP〉

状态State数据库：动态描述两个正在通信的VPN节点对ISP之间链路资源的使用

〈链路标识，VPN-D-ID，源VPN-D-ID，目的地址，协商带宽，启动时间，生存期〉

资源Resource数据库：描述ISP之间的链路资源

〈边界路由器地址，对方路由器地址，链路标识，带宽〉

TCA/SLA：

〈ISP，链路标识，价格，带宽，时段……〉

4.1.2 ISN的组成 由主控部分(ISN主管理器，连接守护进程(CD)，连接中心(CC)，与ESN接口)、所控边缘路由器(ER)，以及资源数据库(SLA、连接数据库、链路资源数据库、计费数据库)等组成(见图4)。

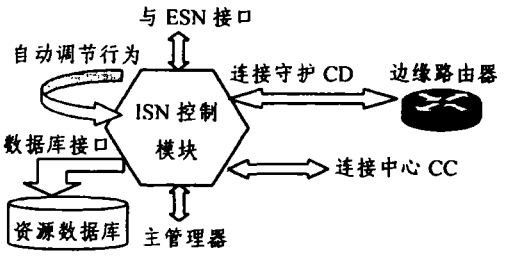

图4 ISN结构

ISN管理器：管理所属的VPN节点，维护所属的资源数据库，密钥管理，根据整体ISP的策略计费等；

ESN对ISN的管理行为通过与ESN的接口传递下来，调用相应的功能模块完成(如虚拟路由VR)。随时ISN对

ESN 的查询行为也通过该接口完成。

连接守护进程(CD):接受 ISN 的指令,配置与 VPN 节点相连的边缘路由器,并维护相关的数据库:如日志、连接状态数据库等。

连接中心(CC):相当于 ISN 的动态管理中心,它负责接受用户的服务请求,向 ESN 的带宽代理请求 ISP 之间边缘到边缘的资源预留,决定业务的服务等级(DSCP 值),以及与隧道的对应关系,通过连接守护进程 CD 完成对边缘路由器的配置等。

边缘路由器(ER):ER 是用户网络业务进入 ISP 的入口点,也是区分服务与 IPsec 的主要结合点。它要完成的功能有 VPN 域的实体间的身份认证、隧道标识的建立、密钥的交换、IP 数据包的封装、加密/解密;将用户的某种业务流送入隧道,并将该隧道与某种 PHB 联系起来(改写数据包 DSCP 值);负责根据 SLA 将用户的业务流平缓地注入网络,来满足所需的 QoS 特性;同时还要记录业务流量日志以计费。

主要的资源文件描述:

SLA 数据库:用于存储用户与 ISP 协商后的协定。

〈用户 ID,口令,服务类型,最大带宽,合法 VPN 区域范围〉

连接数据库:用于存储当前激活的 VPN 的隧道。

〈用户 ID,源地址,目标地址,带宽,隧道 ID,激活时间〉

资源数据库:存储边缘路由器与 VPN 节点之间的可用资源。

〈边缘路由器地址,链路容量,VPN 节点标识,类型,可用性〉

价格数据库:存储不同隧道的价格。

4.1.3 VPN-N 组成 VPN 节点是普通的网络,对网络的设备并不要求必须支持 QoS,当然具有 QoS 特性的路由器能够更好地保证内部用户按等级来使用网络的资源,提供一种积极的公平保证。

通常,VPN 节点网络对外体现为某个地址范围的网络,而在内部,网络的地址是根据 VPN 域的规划分配的内网地址,它们之间一般并没有直接联系。

此外,在 VPN 节点网络的出口出处,通常是防火墙,来保证对内网访问的控制。

4.2 各组成部分交互

4.2.1 ESN-ESN 之间的交互 ESN 之间的协作是系统比较复杂的部分,同其他的交互一样,ESN 之间也需要必要的认证机制,并且最好采用一种私有的安全连接进行。ESN 储存和操作 TCA/SLA,有时可能还要包括必要的支付机制。另外,为了更好地进行协作,ESN 可能还需要和其他的实体如:网络管理员或策略数据库进行交互。

4.2.2 ISN 与 ESN 之间的交互 为了相互处理对方的请求,保证 SLA 的一致性,相互对应的 ESN 与 ISN 之间必须进行交互。它们必须能够查询并同步 ISP 网络当前的服务配置状态。在 ESN 与对等 ISP 的 ESN 协商结束之前,ESN 需要根据 ISN 提供的反馈信息协调各 ISN 保证给定的服务要求。同时这种交互也是全局策略与配置一致的保证。

4.2.3 ISN 与 VPN 节点之间的交互 ISN 作为 VPN 节点的直接接入点(服务提供者),它要协调、访问包括本地数据库在内的各种资源,来直接处理 VPN 节点的各种请求,并做出应答,同时正确地对网络进行配置,完成诸如隧道的建立,边缘资源的分配、服务等级的确定、映射等。VPN 节点根据应答信息及查询信息,可以了解到网络的状态。

4.3 信令、协议

在 QoS 的资源协商中,需要一定的信令机制(如 ISP 的带宽代理之间的协商),在各部件的交互中也需相应协议。本文所提出的是基于 QoS 整个 IP-VPN 的框架结构,它并没有强制要求采用某种信令机制,同时各部件之间的协议、接口也可在实现时制定。

这种框架体系与具体实现的分离更能够保证它的通用性。

4.4 安全性

整个框架的安全性分为两个部分,一是隧道的安全性,另一则是管理功能实体本身以及它们交互的安全性。前者依靠的是 IPsec 本身的安全机制,如密钥的交换、强制采用的加密算法,加密的强度(密钥长度)等等。

而对于后者,因为在整个框架中存在大量实体之间的交互,它们本身的安全由具体的实现所决定,如采用冗余备份等解决方案。任何部件之间在进行交互之前都需要相互的身份认证,关于认证的解决方案如采用可靠第三方等。我们在此并不讨论,具体参考相关文献。

4.5 性能及伸缩性分析

VPN 的一个重要指标是其性能及伸缩性,如前所述,本文所提出的基于 QoS 的 IP-VPN 框架实质上是在区分服务(DS)基础之上的一种增值服务。它实现的前提是 VPN 节点所属的 ISP 网络采用 DS 体系,而区分服务由于结构简单清晰、良好的伸缩性为整个 VPN 的伸缩性打下良好的基础。同时,本文提出的 IPsec 与 DS 的结合点非常明确,它对整个 DS 体系的改动仅仅在于 ISP 之间的边界路由器与 VPN 节点的接入路由器(主要改动点),同时它本身还拥有自己的 ESN、ISN 控制中心。这种结构并不影响 ISP 原有的业务,整个网络的路由,而且这种 ESN-ISN-VPN 节点的三层管理结构可以很好地保证策略、拓扑等关键数据的全局一致性。因此,它具备很好的伸缩性。

此外,除区分服务本身提供的服务质量外,对性能的主要影响集中于边缘路由器对 IP 包进出隧道的加/解密操作运算,这与具体实现有关,在这里并不具体讨论。

总结与展望 基于 ESN、ISN、VPN 节点三层结构的 IP-VPN 体系,结合了区分服务 DS 的网络服务优势与 IPsec 的安全技术特点,在保护用户数据安全性的同时,真正提供了可以与租用线路相比的性能优势。DS 在主干上易于伸缩,为 VPN 提供了很好的扩展性。

由于 DS 体系调度粒度较粗,缺乏单独的资源预留机制,没有高度的灵活性与多级别的服务。而这正是 IS 所特有的,如何将双方的优势结合起来是目前的研究热点,文[11]提出了一种 IS over DS 的结构。我们目前也正在研究这种结构与 VPN 技术的结合,基本思想是在 ISN 部署集成服务 IS,而在 ESN 部署区分服务,但是目前还有很多问题有待研究。

参 考 文 献

1 Gleeson B, Lin A, Heinanen J, et al. A Framework for IP Based Virtual Private Networks. IETF RFC 2764, Feb. 2000

2 Fox B, Gleeson B. Virtual Private Networks Identifier. IETF RFC 2685, Sep. 1999

3 Ferguson P, Huston G. What is a VPN?. Revision 1, April 1998. http://www.employees.org/~ferguson/vpn.pdf

一种 Ad hoc 网络中分布式无环路由算法设计

康 凯 郭 伟 吴诗其
(电子科技大学通信抗干扰国防重点实验室 成都610054)

A Novel Distributed Loop-free Routing Algorithm in the Ad hoc Networks

KANG Kai GUO Wei WU Shi-Qi
(National Communication Lab, UESTC, Chengdu 610054, China)

Abstract The routing algorithm is one of the important problems in the Ad hoc networks. The performances of the networks are heavily depended on the property of the routing algorithm. In this paper, we present a new loop-free routing algorithm in the Ad hoc networks. By virtue of the correlation of routing information among neighbor nodes, the formation of the temporary loops during the topological changes can be prohibited. The new algorithm can avoid the waste of the wireless bandwidth, and accelerate the convergence of the routing during the network transitions.

Keywords Ad hoc network, Routing, Loop-free, Temporary loop

1 引言

自组网,又称为 Ad hoc 网,是指一组带有无线收发装置的移动节点组成的一个多跳的临时性自治系统[3]。自组网不需要依赖于任何预先架设的网络设施,能够实现临时快速自动组网和支持节点的移动性,并具有动态网络管理和动态网络优化的功能,主要用于在高度机动和无线通信的环境下为移动节点提供通信服务。在军事通信、抢险救灾、计算机支持协同工作(CSCW)等方面都具有广泛的应用[1~3]。

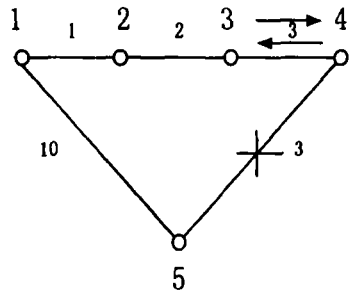

图1 3、4节点间暂态环路的形成

自组网的拓扑结构具有动态变化的特性,因此路由算法是自组网中最为重要的问题之一。自组网的路由协议用于监控网络拓扑变化,交换路由信息,产生、维护和选择路由,并根据选择的路由转发数据包。选择一个好的路由算法是保证网络性能的主要因素[3,4]。自组网的路由算法通常可以分为以下几种:固定式路由算法;集中式路由算法;孤立式路由算法;分布式路由算法,其中以分布式路由算法应用得最为普遍。本文集中讨论自组网中的分布式路由算法。

自组网中的路由算法设计中必须考虑移动性造成的网络拓扑频繁变化的问题,包括链路的增加、减少和链路代价的变化等,在相关的更新消息的扩散达到收敛过程中,会造成网络中的路由出现暂态环路。环路会消耗有限的无线带宽资源。对于暂态环路问题,可见图2、3示例。

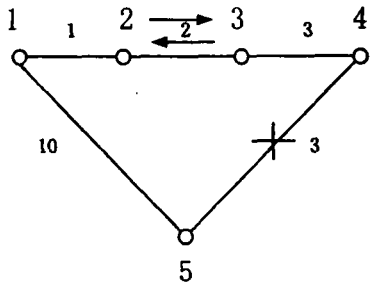

图2 2、3节点间暂态环路的形成

当因某种原因链路 l_{45} 断开时,节点4发往其他节点的数据包以3节点为下一跳,而3节点在未接收到有关状态更新消息时,仍将1、2、3节点发往5节点的数据包以4节点作为下一跳,因此在链路 l_{34} 上会形成3、4节点之间的暂态环路。当3节点从4节点接收到有关状态更新消息后,会修改自己的路由表。此时 l_{34} 上的暂态环路会消除,但在 l_{23} 上会形成同样的环路。

解决移动环境下的暂态环路抑制的最优路由算法是自组

4 Braun T, Gunter M, Khail I. Virtual Private Network Architecture. April 1999. URL: http://www.tik.ee.ethz.ch/~cati/
5 Blake S, Black D, Carlson M, et al. An Architecture for Differentiated Services. IETF RFC 2475, Dec. 1998
6 林闯,单志广,盛立杰,等. Internet 区分服务及其几个热点问题的研究. 计算机学报,2000,23(4): 419~433
7 Duffield N G, Goyal P, Greenberg A, et al. A flexible Model for Resource Management in Virtual Private Networks
8 Kent S, Atkinson R. Security Architecture for the Internet Protocol. IETF RFC 2401, Nov. 1998
9 Braden R, Clark D, Shenker S. Integrated Services in the Internet Architecture: an Overview. IETF RFC 1633, June 1994
10 Clark D. The Design Philosophy of the DARPA Internet Protocols. ACM SIGCOMM'88, Aug. 1988
11 Bernet Y, Ford P, Yavatakr R, et al. A Framework for Integrated Services Operation over Diffserv Networks. IETF RFC 2998. Nov. 2000
12 Nichols K, Blake S, Baker F, et al. Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers. IETF RFC 2474, Dec. 1998
13 Nichols K, Jacobson V, Zhang L. A Two-bit Differentiated Services Architecture for the Internet. IETF RFC 2638, July 1999