



# 一种新型安全路由协议——势能导向多下一跳路由协议<sup>\*</sup>

兰巨龙<sup>1</sup>, 张建辉<sup>1</sup>, 王艳红<sup>2</sup>, 马海龙<sup>1</sup>, 卜佑军<sup>1</sup>

(1. 国家数字交换系统工程技术研究中心 郑州 450002;

2. 大连环宇移动科技有限公司 大连 116600)

**摘 要:**路由协议是网络的核心控制协议,通过路由协议增强网络可用性和安全性显得尤为重要。在研究网络路由协议及其安全机制的基础上,充分考虑网络路由过程的动态可用性和节点可信度,在路由机制中首次定义了寻路和可信势能,并设计实现了基于节点势能导向的多下一跳路由协议,很好地解决了目前互联网中突发事件易引起网络拥塞和不安全节点对用户信息安全的隐患,对加强网络抗毁性、保障用户信息安全具有重要价值。

**关键词:**安全路由;节点势能;多下一跳路由

**doi:** 10.3969/j.issn.1000-0801.2014.07.005

## A Novel Secure Routing Protocol ——Multi-Next Hop Routing Protocol Based on Node Potential

Lan Julong<sup>1</sup>, Zhang Jianhui<sup>1</sup>, Wang Yanhong<sup>2</sup>, Ma Hailong<sup>1</sup>, Bu Youjun<sup>1</sup>

(1. National Digital Switching System Engineering & Technological Center, Zhengzhou 450002, China;

2. Dalian Huanyu Mobile Technology Co., Ltd., Dalian 116600, China)

**Abstract:** Routing protocol is the core network protocol. It is very important to enhancing network availability and security through improving the routing protocol. Based on the research of routing protocol and security mechanism, the concepts of routing potential and credible potential have been defined to characterize the availability and security feature. Furthermore, a novel routing protocol——multi-next hop routing protocol based on node potential was proposed. A good solution was given to deal with the network congestion caused by network unexpected events and the user information safety hazard from unsafe nodes simultaneously. The solution will play an important role to strengthen the network survivability and to safeguard network user information.

**Key words:** secure routing, node potential, multi-next hop routing

### 1 引言

随着信息技术对人类生产、生活影响力的不断增强,各种网络基础设施逐渐成为关系到国计民生的重要战略资源,网络的安全性和生存性日益凸显。在新的历史条件

下,网络安全性和生存性面临两大挑战:一是平时环境下针对网络设备的恶意攻击和侵害造成的网络失效;二是军事打击、恐怖袭击及自然灾害等极端环境下,网络局部或全局失效。传统商用路由器已有的网络生存性和快速自愈技术都不足以应对上述挑战,当前结合网络路由技术进行

<sup>\*</sup> 国家高技术研究发展计划(“863”计划)基金资助项目(No. 2007AA01Z2A1, No. 2007AA01Z212, No. 2008AA01Z214),国家重点基础研究发展计划(“973”计划)基金资助项目(No. 2012CB315901, 2012CB315905)

网络可生存性的研究集中体现在 3 个方面:基于 MPLS 协议的路径快速保护切换技术、基于传统成熟 IP 路由协议的参数调整机制和基于传统 IP 路由技术的扩展方法。

基于 MPLS 协议的路径快速保护切换技术是一种基于预先确定故障恢复的生存性技术,针对网络中特定链路或路径进行资源预留,即在传输路径建立的同时就建立起备份路径。当在数据传输过程中检测到链路故障发生时,传输的业务就自动切换到备份链路或路径。根据受保护的 LSP 和备份 LSP 之间的比例,保护技术通常采用 4 种结构来实现:1+1 LSP 保护、1:1 LSP 保护、1:n LSP 保护和 n:m LSP 保护。由于此技术依赖人工配置,虽然可以实现路径的快速切换,但其灵活性和扩展性具有很大的局限,一般只用来保护关键的节点和链路。

基于 IP 路由协议的参数调整机制是通过调整路由协议中计数器的参数值加快协议收敛的。传统的 OSPF(open shortest path first)路由协议和 IS-IS(intermediate system to intermediate system)路由协议周期性地发送网络路由协议报文探测各邻居节点,当检测到网络发生故障时,会触发路由协议的收敛过程,此时路由协议产生并洪泛网络链路状态信息,接收到链路状态信息的路由器依据最短路径树计算结果更新网络路由和路由表。为了加快网络故障发生时路由协议的收敛过程,可以通过调整路由协议中采用的计数器的值,将较大规模网络的路由收敛过程控制在 100 ms 内完成。但传统路由协议本身不具备根据网络环境变化自适应调整路由配置参数的能力,协议参数的调整需要人工干预方能完成,使得该技术的应用仅能局限在单一网络故障场景,无法适应多种网络故障并发的情况。

基于传统 IP 路由技术的扩展方法主要包括了基于备份路径技术的故障恢复技术、基于多拓扑的故障恢复机制和多路径路由机制。基于备份路径技术的故障恢复技术无需为保护路径预留网络资源,故障恢复能够在毫秒数量级的时间内完成,这类方法特别适合解决频繁发作的故障,保障了路由收敛期间的通信畅通,这类恢复方案主要有:快速重路由<sup>[1]</sup>、故障抑制路由<sup>[2]</sup>、基于偏转的备份路由。基于多拓扑的故障恢复机制是 IP 网络所独有的提高生存性技术,其主要思想就是路由器在原有拓扑的基础上建立多个备份拓扑,每个备份拓扑保护部分链路或节点,所有备份拓扑保护全部链路和节点。这类技术不仅可以处理单链路、单节点故障,也可以解决多故障问题,目前的相关研究工作主要有:多拓扑路由机制<sup>[3]</sup>、多配置路由机制<sup>[4]</sup>、基于故

障推理的快速重路由<sup>[1]</sup>、弹性路由层机制<sup>[5,6]</sup>。多路径路由方法中,典型的研究成果是 Vutukury 和 Garcia-Luna-Aceves 等提出的多路距离矢量算法(MDVA)<sup>[7]</sup>、多路径局部分发算法与结合服务质量的局部分发算法<sup>[7]</sup>等改进的 MDVA 算法以及在时延容迟网络等场景下的多径路由机制<sup>[8,9]</sup>。这些方法可为每个目的 IP 地址提供多个可用下一跳链路,在算法设计时采用一组无环不等式条件来避免瞬时的环路和计数无穷大等问题;但算法的计算开销过大,其可用下一跳节点数量较少,网络资源利用率不高。

另外在路由安全性方面,IETF 成立了路由协议安全工作组,研究路由协议的安全威胁,有研究人员提出的建立主路由信息库方法<sup>[10]</sup>,如采用密码技术的安全 RIP(routing information protocol,路由信息协议)(SRIP)<sup>[11]</sup>、三角理论安全距离矢量协议(SDV 协议)<sup>[13]</sup>,但这些方案路由负载和计算开销过大,只针对特定攻击手段设计,抵御攻击类型有限。

## 2 基于势能的网络多下一跳路由思想

自然界中的水流具有从高处向低处流动的特性,因为水在所流经地点的相对海拔高度不同而具有不同的势能,任何存在海拔差的相通的地方,水流均能由高势能点流向低势能点。由此现象启发,在 IP 网络中引入势能的思想,规定数据报文可以由高势能节点向低势能节点转发,从而形成了由源节点到目的节点的多个可用下一跳路径,在这些可用下一跳路径中进行数据报文转发时不会形成环路。

以图 1(a)的网络拓扑为例,经过网络势能通告过程后得到图 1(b)所示的相对于目的节点  $i$  的网络层次图,势能的计算过程如图 1(a)中实线箭头所示。在势能计算过程,所有节点均知道自己邻居节点的势能值,然后各个节点依据势能计算式算出自己节点的势能值,进行报文转发

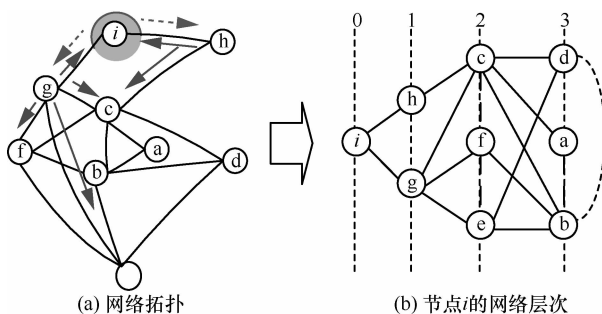


图 1 节点势能的报文转发方法



时各节点选择低势能节点进行数据的转发,如图 1(a)中虚线箭头所示。

### 3 协议设计

协议的设计思路是在不改变现有网络基本路由架构的情况下,提出“节点势能”路由机制,设计基于寻路势能和可信势能的势能导向多下一跳路由协议(multi-next hop routing protocol based on node potential, NP-MNRP),通过对节点可信度的有效评估实现了不可信节点的检测和避免;通过局部的流量感知和自适应的多下一跳并行转发解决了异常流量导致的网络不可用,保证了网络级的自主可控和应用级的持续可用。

#### 3.1 势能计算方法

##### 3.1.1 寻路势能计算方法

**步骤 1** 计算节点在所处网络中的势能层值。对于网络中指定的目的节点,定义其势能层值为 0;而对于网络中其他节点,势能层值为其邻居节点势能层值中的最小值加 1,具体的计算式为:

$$\begin{cases} L(i, j)=0(i=j, i \in N, j \in N) \\ L(i, j)=\min[L(k, j)]+1(i \neq j, k \neq i, i \in N, j \in N, k \in K) \end{cases} \quad (1)$$

其中,  $L(i, j)$  表示节点  $i$  相对于目的节点  $j$  的势能层值,  $N$  为网络中的节点集合,  $K$  为节点  $i$  的邻居节点集合。

**步骤 2** 计算节点势能值。如果待计算节点的势能层值为 0, 则其势能值为 0; 如果待计算节点的势能层值非零, 则在其同层或低一层邻居节点中选出性能最高且势能值未确定的节点, 将该邻居节点的势能层值加 1 作为待计算节点的势能值。

**步骤 3** 生成多下一跳集合。势能值为 0 的节点的多

下一跳集合为空; 对于其他节点, 其多下一跳集合由势能值小于本节点的所有邻居节点组成。

规定数据传送时, 选择本节点的多下一跳集合进行数据转发, 即多下一跳路由。

##### 3.1.2 可信势能计算方法

协议首次将节点可信程度作为路由度量考虑因素之一, 引入路由计算过程, 从根本上解决了路由协议面临的路由安全问题。设计的可信势能计算方法如下: 依据路由通告的真实性鉴别结果, 在一定时间周期  $T$  和网络路由空间范围  $R$  内, 统计每一个节点的路由通告真伪频次  $D$ , 结合节点重要度  $K$  和拓扑结构熵  $E$  等要素, 计算节点的可信势能值  $P_j$ 。

$$P_j = a \sum_{i=1,2,\dots,N} \left[ \frac{\sum_k D_{ki}}{N} - D_{ji} \right] + bK_j + cE_j \quad (2)$$

将低于可信势能阈值的节点判定为可疑节点, 同时将网络中承载的用户业务进行安全属性分级, 高安全级的业务映射到可信势能值高的节点组成的路径上。

而在时间周期  $T$  内路由前缀在路由空间  $R$  内的所有用户业务流不经过被判为可疑的节点, 只选择可信势能满足业务安全要求的路径进行数据转发。

#### 3.2 协议设计

##### 3.2.1 协议的网络视图

考虑到网络拓扑信息和网络可达性信息的来源、动态性、信息变化对路由转发的影响等因素, 协议的网络视图将网络划分为终端用户网络和业务承载网络, 如图 2 所示。终端用户网络的节点运行传统单下一跳路由协议, 把目的 IP 地址不是本网的数据报文转发给业务承载网络, 完成本地通信; 业务承载网络中的节点运行节点势能导向多下一跳路由协议, 节点势能导向路由协议在业务承载网

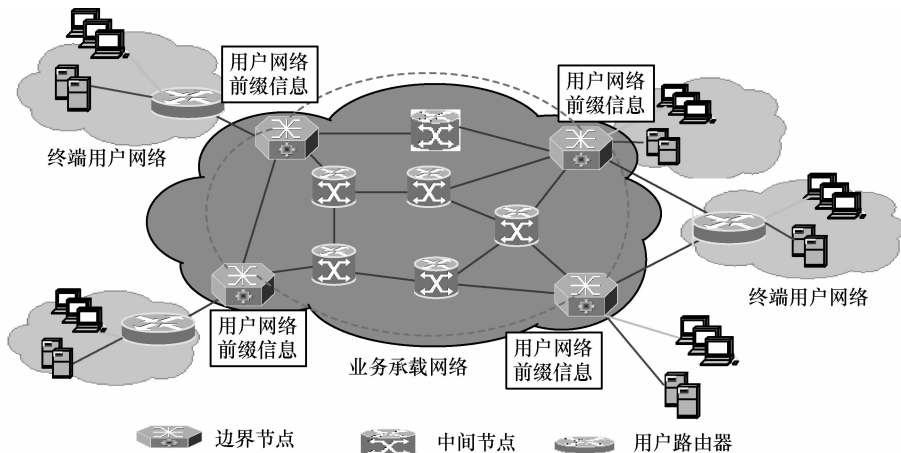


图 2 协议网络模型

络内计算并选择到达终端用户网络的路径,并负责将用户网络前缀信息通告给网络中其他节点。通过将终端用户网络和业务承载网络分离,用户网络前缀等网络可达性信息通过网络层可达信息洪泛通告报文、网络层可达信息特定请求报文和网络层可达信息特定应答报文按照协议流程进行通告;不同类型信息选择适合自身的通告更新流程。

### 3.2.2 协议主要流程

#### 3.2.2.1 协议报文与前缀通告过程

节点势能导向多下一跳由协议设计了 3 类 9 种协议报文,其中链路状态探测类报文实现邻居节点发现和链路质量动态检测,势能层级图建立类报文实现网络寻路势能的分布式计算,可达性信息通告类报文完成承载网络势能层级图与用户网络路由前缀的映射。

终端用户网络前缀的维护和通告功能由业务承载网络的边界节点完成。当业务承载网络中的某个节点(包括出口节点或中间节点)不知道某个用户网络前缀绑定的出口节点时,该节点洪泛发送报文进行查询,直到得到对应前缀的出口节点信息。

#### 3.2.2.2 节点势能的计算

##### (1) 节点势能的分布式计算

协议通过势能层级图建立类报文完成节点势能的分布式计算,首先每个出口节点按照广度优先算法将自己的势能层级发送给邻居节点,每个未计算出势能值的邻居节点按照第 3.1 节的势能计算方法得到自身势能后,再从本节点发起一个类似的过程,通过广度优先遍历过程完成相对给定出口节点的势能值的全网计算,通过这一过程,将可发现从每个节点到达出口节点的多个可行下一跳。势能计算过程在网络中没有终止条件,通过特定出口节点势能值的不同计算版本,确定当前节点势能值的时效性。

##### (2) 节点势能的动态更新

当发生以下两种情形时,需要进行节点势能值的更新。

- 某个节点发现自己相对于某个出口节点无势能更低的邻居节点(某些链路或者节点发生故障时会发生),需要查询自己邻居节点的势能值,触发势能跃迁过程,需要提升本节点的势能值或认定某个出口节点不可达,确保数据转发过程适应网络动态变化。
- 某个节点新添加到网络中时,主动向邻居节点发起势能查询过程,并根据查询结果按照第 3.1 节方法计算势能。

#### 3.2.2.3 基于信息真实性检测的可信势能计算

网络数据传送路径上不可信节点的存在会导致信息泄

漏,必须对之进行有效甄别和避让。节点势能导向多下一跳路由协议,在传统路由报文认证、传输加密等保证信息源真实可信、传输过程完整性保证的基础上,引入的路由信息真实性检测方法。该方法借鉴现实生活中常用的评断谎言和个人信誉的方法,即大多数人都说实话,只有极个别别人说假话,而少数人所说的假话的内容一定和其他多数人说的不同,依此鉴别谎言;而一个人说谎的次数和频率决定了其信誉度。

利用该方法,将节点通告的路由度量信息比作人说的话,通过鉴别比对不同节点的路由度量信息评判其可信度;综合考虑节点在一定时间空间内通告路由度量信息真伪的频度、节点的网络拓扑位置信息等,按照第 3.1 节可信势能计算式,计算节点的“可信势能”;在数据传送时依据节点可信势能进行避让,保障数据传送的安全可控。

### 3.3 逐跳流量分派的路由策略实现机制

依据势能导向路由协议计算出的多个路由下一跳信息,使得节点可采用灵活多变的路由策略来保证网络安全性和高生存性。每个节点可并发使用多个低势能下一跳节点进行数据转发,提高了网络利用率和运载能力;在网络出现局部拥塞、故障或安全隐患高时,凭借寻路势能的感知和自适应机制,可实现传送路径的迅速调整,保证数据传送的持续畅通。本文提出了一种区分流量的动态负载均衡(traffic-distinguished dynamic load balancing, TDLB)算法,按照势能计算结果,通过流量分配过程选择下一跳进行路由转发,实现用户路由策略。

TDLB 算法的流程如图 3 所示。当接收到数据分组时,其五元组信息经散列计算后,得到数据流标识,由散列分配单元确定输出口。选择器给动态调整单元和散列分配单元的输出结果赋予不同的优先级;为实现流量精确分配,该算法把数据流区分为极大流和普通流,在负载分配不均衡时,通过负载调整单元对过载输出口上的极大流进行重映射,实现负载的动态均衡分配;强调均衡时可设定动态调整单元的优先级高于散列分配单元,反之亦然。依据选择器选择的结果,报文送往相应的输出口。

## 4 实验测试

### 4.1 实验测试方法

在针对节点势能导向的多下一跳路由协议仿真测试中,使用拓扑生成软件 BRUTE,基于 WAXMAN 模型生成测试网络的拓扑,该测试网络拓扑包含 15 个网络节点,共 60 条链路,如图 4 所示。分析时,将距离矢量类协议单下

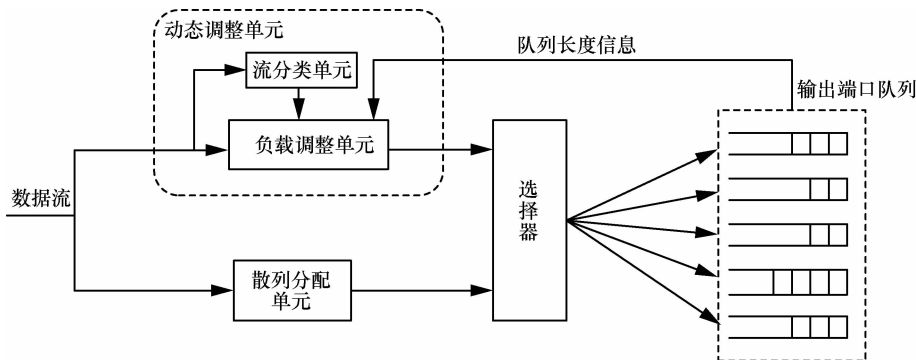


图3 区分流量的动态负载均衡算法结构

一跳 RIP、NP-MDVA 协议（多路径协议）和本文提出的 NP-MNRP 进行对比。

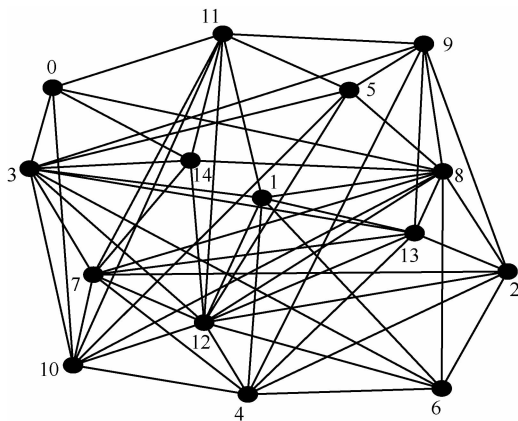


图4 距离矢量路由算法验证的仿真拓扑

采用 UDP(user datagram protocol, 用户数据报协议) 进行数据分组传输试验, 检测仿真拓扑中各节点和链路中传输的 UDP 数据分组数作为分析 MNRP 性能的依据。每个 UDP 数据分组的大小设定为 1 000 byte, 在仿真拓扑中传输的 UDP 数据分组总量为 20 MB, 数据分组发送的时间间隔为 1 ms。在仿真拓扑中设定了 3 个基于 UDP 进行数据传输的节点对: 节点 2→节点 3、节点 4→节点 11、节点 9→节点 10。

#### 4.2 多下一跳资源发现与利用能力

分析表 1 中的仿真结果: 采用 MDVA 协议和采用单下一跳 RIP 的仿真实验中数据分组完成接收的时间基本一致, 而采用 NP-MNRP 的数据分组完成接收时间提前了约 30%。

统计分析传输实验中网络的负载均衡度, 如图 5 所示, 采用 NP-MNRP 和 MDVA 协议进行数据传输时的负载均衡度优于采用单下一跳 RIP 传输, 其均衡度相差多个数量级; 而采用 NP-MNRP 进行数据传输时的负载均衡度相比采用 MDVA 协议提高了 20%。

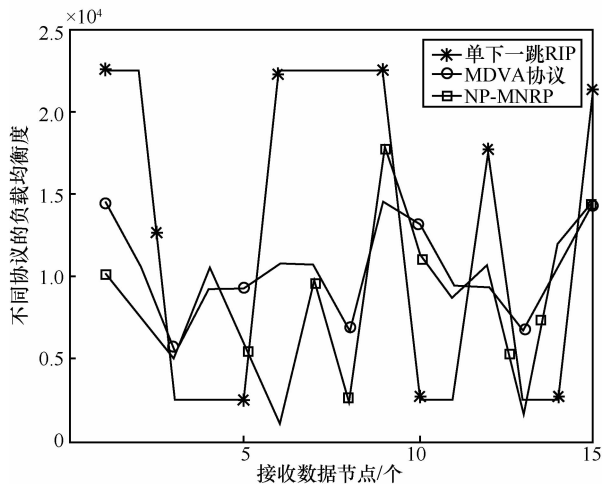


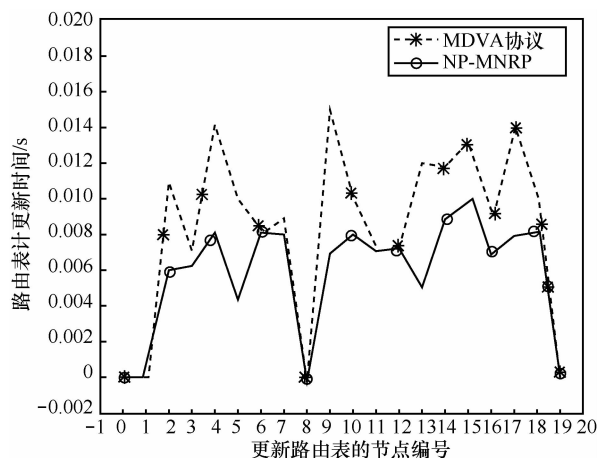
图5 不同路由协议下节点负载均衡度

#### 4.3 节点故障、不可信时快速避让的性能

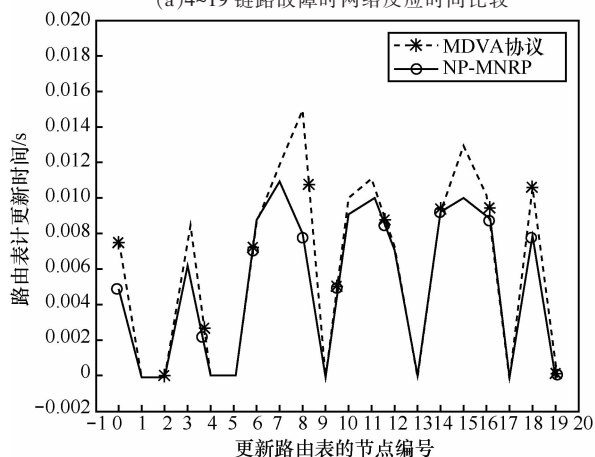
在图 6 中对比分析了链路 4~19 和 8~19 发生故障时, 分别采用 MDVA 协议和 NP-MNRP 时, 网络反应时间的差异。其中, 反应时间定义为网络检测到故障的时间与路由表重新计算并稳定的时间的差值, MDVA 协议和 NP-MNRP 都是可实现局部自愈的路由算法, 但 NP-MNRP 的平均反应时间比 MDVA 协议减少了 20%。

表 1 传输完成时间

| 传输节点对      | 起始时间/s        | 单下一跳 RIP 完成时间/s | MDVA 协议完成时间/s | NP-MNRP 完成时间/s |
|------------|---------------|-----------------|---------------|----------------|
| 节点 2→节点 3  | 100.013 574 8 | 120.046 18      | 120.046 18    | 116.048        |
| 节点 4→节点 11 | 100.358 675 9 | 120.361 33      | 120.361 33    | 114.364        |
| 节点 9→节点 10 | 100.572 676 5 | 120.575 32      | 120.575 32    | 113.586        |



(a) 4~19 链路故障时网络反应时间比较



(b) 8~19 链路故障时网络反应时间比较

图6 MDVA 协议和 NP-MNRP 的故障处理性能对比

## 5 结束语

本文受自然界水顺势而流特性启发,将势能引入路由机制中,通过路由机制创新增强网络的安全可控能力。在网络路由机制中定义了节点的“寻路势能和可信势能”,以寻路和可信势能为核心设计了节点势能导向路由协议,并基于距离矢量路由算法实现,按照将网络划分为用户网络和承载网络的视图,设计协议报文和处理流程,完成了基于势能的多下一跳路由的分布式计算。

本协议将网络寻路与安全一体化设计,实验测试表明了该协议在均衡利用网络资源、快速避绕故障节点或安全隐患节点方面的有效性;协议从路由机制角度提高了网络的安全可控性方面,具有重要的应用价值。

## 参考文献

- 1 Iyer S, Bhattacharyya S, Taft N, *et al.* An approach to alleviate link overload as observed on an IP backbone. Proceedings of

INFOCOM'03, San Francisco, CA, USA, 2003:406~416

- 2 Zhong Z, Nelakuditi S, Yu Y, *et al.* Failure inferencing based fast rerouting for handling transient link and node failures. Proceedings of IEEE Global Internet, Miami, FL, USA, 2005
- 3 Menth M, Martin R. Network Resilience through Multi-Topology Routing. Technical Report No.353, University of Wuerzburg, Institute of Computer Science, May 2004
- 4 Kvalbein A, Cicic T, Gjessing S. Post-failure routing performance with multiple routing configurations. Proceedings of IEEE 26th Annual Conference on Computer Communications (INFOCOM 2007), Anchorage, Alaska, USA, 2007
- 5 Kvalbein A, Hansen A F, Cicic T, *et al.* Fast recovery from link failures using resilient routing layers. Proceedings of 10th IEEE Symposium on Computers and Communications (ISCC), Cartagena, Spain, June 2005
- 6 Kvalbein A, Hansen A F, Cicic T, *et al.* Fast IP network recovery using multiple routing configurations. Proceedings of INFOCOM 2006, Spain, April 2006
- 7 Vutukury S, Garcia-Luna-Aceves J J. MDVA: a distance-vector multipath routing protocol. Proceedings of the INFOCOM, Anchorage, AK, USA, 2001
- 8 Huo H, Shen W. Virtual hypercube routing in wireless sensor networks for health care systems. Proceedings of ICFIN, Beijing, China, 2009
- 9 Wu J, Wang Y S. Social feature-based multi-path routing in delay tolerant networks. Proceedings of INFOCOM 2012, Orlando, FL, USA, 2012
- 10 Mittal V, Vigna G. Sensor-based intrusion detection for intra-domain distance-vector routing. Proceedings of CCS'02, Washington, D C, USA, Nov 2002
- 11 Wan T, Kranakis E, Oorschot P C. S-RIP: a secure distance vector routing protocol. Proceedings of ACNS, Yellow Mountain, China, 2004:103~119
- 12 Babakhouya A, Challal Y, Bouabdallah M, *et al.* SDV: a new approach to secure distance vector routing protocols. Proceedings of IEEE SecureCom, Baltimore, Maryland, USA, 2006

## [作者简介]



兰巨龙,男,国家数字交换系统工程技术研究中心教授、总工程师、博士生导师,国家下一代广播网(NGB)总体专家委员会委员,通信学会高级会员,国家重点基础研究发展计划(“973”计划)项目首席科学家。主要研究方向为宽带信息网络和新型网络体系结构,先后主持了3项国家高技术研究发展计划(“863”计划)重大课题、1项国家“973”计划重大项目、1项国家支撑计划重大项目,先后获得省部级科学技术进步奖一等奖2项,出版专著2部,申请国际专利2项,国家发明专利30余项,发表论文80余篇。

(下转第61页)