距离矢量路由协议的网络可生存性研究

王滨[1,2]，郭云飞[2]，兰巨龙[2]，吴春明[1]

（1. 浙江大学 计算机科学与技术学院，浙江 杭州 310027；2. 国家数字交换系统工程技术研究中心，河南 郑州 450002）

摘 要：研究了距离矢量路由协议对网络可生存性的影响，给出了网络可生存性的定义和计算方法，为了有效的提高距离矢量路由协议的网络生存性，提出了一种能够对消息真实性的度量方法，分析结果显示该方法能够抵御网络中攻击节点发起的虚假路由消息攻击，可以有效提高距离矢量路由协议的网络可生存性。

关键词：距离矢量路由；网络可生存性；虚假路由消息；真实性度量

中图分类号：TP393.4 **文献标识码**：A **文章编号**：1000-436X(2010)10-0121-07

Research on network survivability of distance vector routing protocol

WANG Bin[1,2], GUO Yun-fei[2], LAN Ju-long[2], WU Chun-ming[1]

(1. Computer Science College, Zhejiang University, Hangzhou 310027, China;

2. National Digital Switching System Engineering & Technological R&D Center, Zhengzhou 450002, China)

Abstract: The network survivability based on distance vector routing protocol of the network was studied, and the definition of network survivability and its calculation method were given. In order to effectively improve the network survivability of the distance vector routing protocol, A method to measure the authenticity of the update routing message was proposed. Analysis showes that the method can effectively resist false routing messages attacks which is launched by the attack nodes in the network, so it can improve the network survivability of the distance vector routing protocol.

Key words: distance vector routing; network survivability; false routing information; authenticity of measurement

1 引言

近年来，新科学技术的推出、新业务种类的出现促进了网络的迅速发展，Internet 承载了越来越多的流量，为了保障用户业务的服务质量（QoS），研究在故障、攻击等意外情况下网络的生存性受到广泛的关注[1,2]。

目前网络生存性的研究主要分为 2 个方面：1)使用故障处理技术来提高网络的故障处理能力，从而提高网络的生存性[3]。这些技术按照机制来划分可以分为反应式（reactive）[4,5]和先应式（proactive）[6~9]2 种。主要是通过提高现有动态路由的故障处理能力和提前计算备份路径，在故障发生时对故障进行本地处理；2)使用安全机制使网络

收稿日期：2010-01-28；**修回日期**：2010-08-27

基金项目：国家高技术研究发展计划（“863”计划）基金资助项目（2008AA01A323, 2009AA01A334, 2008AA01A325, 2008AA01A326, 2008AA01Z214）；国家重点基础研究发展计划（“973”计划）基金资助项目（2007CB307102）；国家科技支撑计划基金资助项目（2008BAH37B02）；国家自然科学基金资助项目（60773182, 61070157，61070213）

Foundation Items: The National High Technology Research and Development Program of China (863 Program) (2008AA01A323, 2009AA01A334, 2008AA01A325, 2008AA01A326, 2008AA01Z214); The National Basic Research Program of China (973 Program) (2007CB307102); The National Key Technology R&D Program of China (2008BAH37B02); The National Natural Science Foundation of China (60773182, 61070157, 61070213)

系统减少甚至免受恶意入侵，从而提高网络的生存性[10,11]。该类技术主要分为保护、检测和容忍 3 类。

本文不研究故障的处理技术，主要研究如何通过使用安全机制中的检测技术来提高路由协议的网络可生存性。路由协议作为网络的核心，其可生存性直接影响到整个网络的可用性，目前无论 IP 网络还是无线网络中大量的使用距离矢量类路由协议，如 IP 网络中使用的 RIP、IGRP、BGP 等；ad hoc 网络中的：DSDV、TORA、AODV 等，这些协议大都是基于 Bellman-Ford 算法。目前对距离矢量路由协议的可生存性研究主要是使用各种密码技术来对报文进行安全认证[12~15]，实现报文完整性和机密性，这些方法虽然可以有效地抵御外部攻击者发起的各种攻击，但是由于距离矢量路由更新消息是来自于其他节点的分布式计算的结果[16,17]，所以这些方法无法对内部攻击者发起的虚假路由消息进行消息真实性验证，从而导致网络被攻击。

基于上述原因本文研究了基于距离矢量路由协议网络的可生存性，并给出了网络可生存性的定义和计算方法，通过对网络可生存性的定量计算可以看到在网络拓扑一定的情况下，网络的可生存性是一个固定值，为了提高网络的可生存性，本文给出了一种消息真实性的度量方法，分析和仿真结果显示该方法可以有效地抵御网络中合法节点发起的虚假路由消息攻击，提高网络可生存性。

2 网络路由的安全性分析

2.1 网络路由的攻击方法

关于攻击方式，本文的研究仅仅局限于针对路由协议发起的攻击，按照文献[18]中对攻击的分类，可以将这些攻击分为主动攻击和被动攻击，主动攻击者的目的是试图改变系统的资源或者影响系统的操作；被动攻击者的主要目的是试图学习或者使用系统的信息，但是并不影响系统的资源。

目前针对距离矢量路由协议主要存在以下几类攻击。

1) 嗅探攻击：此类攻击的发起者可以是内部攻击者，也可以是外部攻击者，是一种被动攻击，攻击者主要是通过监视并记录某条链路或节点上路由数据的传输情况，从而获取一些网络的信息。

2) 伪造攻击：此类攻击是一种主动攻击，其主要包括以下几种攻击方式。

① 替换攻击：用虚假的路由信息替换有效的路由信息。

② 插入攻击：将错误的路由信息添加到有效的路由信息中，对合法的路由器进行欺骗。

③ 伪装攻击：冒充一个合法的路由器，发送各类虚假的路由信息。冒充攻击者通常是将替换和插入攻击同时进行。

3) 中断攻击：此类攻击也是一种主动攻击方式，其主要目的就是使得合法路由器无法正常的工作，这种攻击可分为如下几种。

① 干扰攻击：攻击者能够阻塞链路的传输，通过切断传播链路，或通过引入噪声到传输链路，使得接收者无法接受到正确的路由信息。

② 超载攻击：攻击者向被攻击者发送大量虚假的路由流量，使得被攻击者输入缓冲区溢出或计算资源被耗尽。

4) 重放攻击：这是一种主动攻击，攻击者将一个有效过期路由数据传输给合法的路由器。

根据以上对距离矢量类路由协议主要存在的安全威胁的分类可以看出，目前对于该类路由协议的攻击危害最大的是伪造攻击，其实质是发送虚假的路由更新消息，主要攻击方式可概括如下 2 种。

① 短距虚假路由信息：是在宣告路由信息中宣告自己到达某个节点的距离短于真实的距离或者直接宣告到达一个和自己并不直接相连的网路的距离为 0，从而可以发起各种攻击（黑洞攻击、劫持会议攻击等）。

② 长距虚假路由信息：是在宣告路由信息中宣告自己达到某个节点的距离大于真实的距离，这样节点可以减少信息传输，导致不公平的利用网络的链路资源，甚至会引起网络的拥塞。

这 2 种攻击方法中，又以短距虚假路由信息攻击的危害最大。

2.2 虚假路由信息攻击分析

假设网络中一个恶意的节点对网络中的其他节点发起攻击，其发送一条虚假的路由更新消息 (D,V_X,C)，D 为目的节点，V_X 表示为下一跳，C 表示到达目的节点的距离，下面来分析这条虚假的路由消息的影响范围。

假设网络中某节点 N 到达目的节点 D 的实际距离为 D_2，而攻击节点 A 与节点 N 的实际距离为 D_1，那么如果 A 想成功的欺骗 N，那么 C 必须满

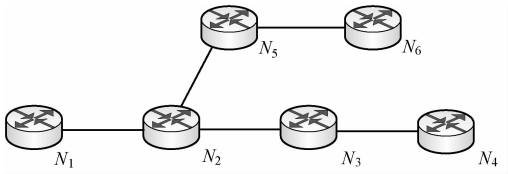
足 $D_1+C<D_2$，即 $C<D_2-D_1$，且 $C\geqslant 0$，可得只要 D_1 和 D_2 满足不等式(1)的目的节点，A 均可发送虚假路由信息。

$$D_2-D_1>0 \tag{1}$$

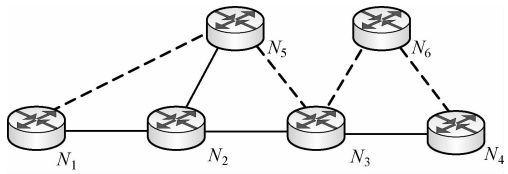
由式(1)可以看出，对于网络中的一个节点，离自己越近的节点对自己的威胁越大其可以发布的虚假路由信息数量越多。例如在图 1(a)所示的网络拓扑中，所有节点之间的距离矩阵为

$$\boldsymbol{D}=\begin{bmatrix}0&1&2&3&2&3\\1&0&1&2&1&2\\2&1&0&1&2&3\\3&2&1&0&3&4\\2&1&2&3&0&1\\3&2&3&4&1&0\end{bmatrix}$$

其中，$d_{ij},(i,j=1,2,\cdots,6)$ 表示节点 i 到节点 j 的距离，假设 N_1 为攻击节点，其到达网络中其他节点的距离为 $d_{1j}=(0,1,2,3,2,3)$；对于节点 N_2 来说，有 $d_{2j}=(1,0,1,2,1,2)$，节点 N_1 可以发送到达目的节点 N_4 和 N_6 虚假路由信息，并且这些虚假的路由信息可以成功的欺骗节点 N_2，导致节点 N_2 发往 N_4 和 N_6 的数据会转发给了 N_1，但是这些数据本来是应转发给 N_3 和 N_5。



(a) 原始网络拓扑图



(b) 添加链路后的网络拓扑图

图 1　网络拓扑图

3　网络可生存性

3.1　距离矢量路由协议的网络可生存性

假设网络中 2 个节点之间的最大距离为 m，网络中的节点数为 n，依据每个节点到网络中的某个目的节点 N_i 的距离，将网络的节点划分为 m 个集合，记为 $L_{Ni}=\{l_{i1},l_{i2},\cdots,l_{im}\}$ 表示，其中 l_{ij} 表示到节点 Ni 距离为 j 的节点集合。其中 $\sum_{j=1}^{m}\left|l_{ij}\right|=n-1$，$\left|l_{ij}\right|$ 表示集合 l_{ij} 中节点的个数。

当攻击者成功的占领了一个节点之后，就称这个节点为破坏节点，并且假设攻击者获得了所有破坏节点原有的资源。

网络中的节点 N 对应的集合划分记为 $L_N=\{l_{N1},l_{N2},\cdots,l_{Nn}\}$，对于网络中任意的节点 A，有 $A\in l_{Nj},j\in\{1,2,\cdots,n\}$ 由式(1)可知对于节点 N 来说，A 可以伪造能够被 N 接受的到达 $\{l_{N(j+1)},\cdots,l_{Nn}\}$ 中的节点的路由信息，所以对于节点 N 来说，其他节点分别成为攻击节点后可以导致节点 N 累计产生的错误信息量如下：

l_{N1} 中节点导致的错误路由信息数量为

$$\left|l_{N1}\right|(\left|l_{N2}\right|+\cdots+\left|l_{Nn}\right|)$$

l_{N2} 中节点导致的错误路由信息数量为

$$\left|l_{N2}\right|(\left|l_{N3}\right|+\cdots+\left|l_{Nn}\right|)$$

…

$l_{N(n-1)}$ 中节点导致的错误路由信息数量为

$$\left|l_{N(n-1)}\right|\left|l_{Nn}\right|$$

l_{Nn} 中节点导致的错误路由信息数量为

$$\left|l_{Nn}\right|\times 0$$

累计产生的错误信息为

$$\sum_{i=1}^{n}\sum_{j=i+1}^{n}\left(\left|l_{Ni}\right|\left|l_{Nj}\right|\right)$$

用 Γ_N 表示节点 N 的可生存性：

$$\Gamma_N=1-\frac{\sum_{i=1}^{n}\sum_{j=i+1}^{n}\left(\left|l_{Ni}\right|\left|l_{Nj}\right|\right)}{n(n-1)} \tag{2}$$

用 Γ 表示网络可生存性：

$$\Gamma=E(\Gamma_N) \tag{3}$$

依据矩阵 $\boldsymbol{D}$ 可得 $L_1=\{1,2,2\}$，$L_2=\{3,2\}$，$L_3=\{2,2,1\}$，$L_4=\{1,1,2,1\}$，$L_5=\{2,2,1\}$，$L_6=\{1,1,2,1\}$，由此可计算得到 $\Gamma_1=0.7$，$\Gamma_2=0.6$，Γ_3=0.7，$\Gamma_4=0.6$，$\Gamma_5=0.7$，$\Gamma_6=0.6$，从而得到网络可生存性为 $\Gamma=0.65$。

3.2　网络的可生存性分析

从网络可生存性定义可以看到，要提高网络可生存性就必须要让节点能接受的错误路由信息尽量的少，即让 $\sum_{i=1}^{n}\sum_{j=i+1}^{n}\left(\left|l_{Ni}\right|\left|l_{Nj}\right|\right)$ 尽量的小。而 $\min\left(\sum_{i=1}^{n}\sum_{j=i+1}^{n}\left(\left|l_{Ni}\right|\left|l_{Nj}\right|\right)\right)=0$，如果要满足此条件，此时网络为一个全连通的网络，网络的可生存性和

每个节点的可生存性均为 1。也就是说网络可以通过增加链路来提高网络的生存性，如果在图 1(a)的网络拓扑中增加 3 条链路，得到图 1(b)的网络拓扑，其连接矩阵变为：

$$\boldsymbol{D}'=\begin{bmatrix}0&1&2&3&1&2\\1&0&1&2&1&2\\2&1&0&1&1&1\\3&2&1&0&2&1\\1&1&1&2&0&1\\2&2&1&1&1&0\end{bmatrix}$$

依据矩阵 $\boldsymbol{D}'$ 可得 $L_1'=\{2,2,1\}$， $L_2'=\{3,2\}$， $L_3'=\{4,1\}$， $L_4'=\{2,2,1\}$， $L_5'=\{4,1\}$， $L_6=\{3,2\}$，由此可计算得到 $\Gamma_1=0.7$， $\Gamma_2=0.7$， $\Gamma_3=0.8$， $\Gamma_4=0.7$， $\Gamma_5=0.8$， $\Gamma_6=0.7$，从而得到网络的可生存性为 $\Gamma'=0.733$，显然 $\Gamma'>\Gamma$。网络的生存性由于链路的增加而得到提高。

4 消息真实性度量方法

从 3.2 节可知道，通过增加链路可以提高网络生存性。但在网络拓扑一定的情况下无法增加链路，此时要想提高网络的可生存性除了使用增加链路的方法，还有就是阻止虚假路由消息在网络中传播，本节将给出一种有效的检测路由消息真实性的方法，通过节点之间相互的检测对方发送过来的路由消息的真实性，减少虚假路由消息在网络中传播，以此来提高网路的可生存性。

4.1 相关假设及定义

消息真实性度量方法基于以下的 2 点前提条件：

1) 网络使用的路由协议为距离矢量类路由协议，且网络的初始收敛已经完成；

2) 节点对收到的路由更新消息的来源、完整性是可以验证的。

消息真实性度量方法就是对通过安全验证的路由消息的真实性进行检测。该检测方法需要引入以下定义。

定义 1 路由信息数据库(RIB, routing Information base)，每一个节点有一个 RIB，保存最近收到的所有最新路由信息，RIB 中的保存格式为 $(dest\_id,neighbour,nexthop,\cos t)$ 这里的 $dest\_id$ 就是目的节点的地址； $neighbour$ 表示发送 update 创建了这个条目的邻居（也就是这个路由的下一跳）； $nexthop$ 表示邻居节点到达目的节点的下一跳； $\cos t$ 是邻居节点到达目的节点的距离。节点可以依据 RIB 知道其邻居节点的所有邻居。

4.2 消息真实性度量方法

运行距离矢量路由协议的网络中，当协议收敛完成后可以有这样的结论：每个节点到达某个目的节点的距离和其邻居到达该目的节点的距离差的绝对值不大于 1。如图 2 所示节点 N_3 到达目的节点 D 的距离与其邻居 $N=\{N_1,N_2,N_4,N_5\}$ 到达目的节点 D 的距离差的绝对值将不超过 1，即 $|d_{N3}-d_{Nx}|\leqslant 1$，$N_x\in N$。

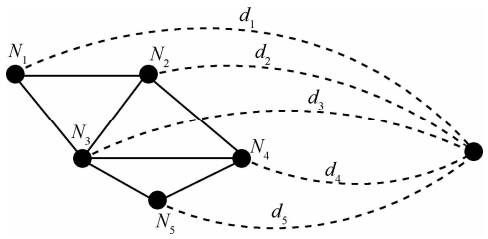


图 2 网络拓扑图

消息真实性度量方法： 现假设节点 N_0 要检测节点 N_M 发来的某条路由信息 (D,N_N,C_M) 的真实性，那么按照如下的规则进行比较。

1) 如果 $C_M=0$，此时需要对节点进行路由前缀认证，所谓路由前缀认证就是查看该节点是否有权发布关于网络地址 D 的权利（其一般采用节点与地址前缀进行绑定颁发相应的证书），认证不通过则直接判定为该节点为恶意节点；如果通过，则认为信息真实。

2) 如果 $C_M>0$， N_0 执行下面的操作：

① N_0 依据 RIB 中记录的数据取出节点 N_M 的邻居节点集合 $N=\{N_1,N_2,\cdots,N_x\}$；

② N_0 向节点集 N 中的所有节点发出路由表请求，要求这些节点将其路由表发送给节点 N_0；

③ N_0 根据收到的路由表，得到 N_M 的邻居节点集到达目的节点 D 的距离 $C_D=\{C_1,C_2,\cdots,C_x\}$，然后进行下面步骤的比较。

3) 从 RIB 中取出 $(dest\_id,V_M,nexthop,\cos t)$，从中提取出 $nexthop=N_y$ 和 $\cos t$，再取出 $(dest\_id,V_y,nexthop,\cos t')$，看 $\cos t-\cos t'=1$ 是否成立，如不成立，说明消息为虚假消息；否则进行下面的步骤。

4) 如果 $C_M=1$，那么 $\cos t'=0$，按照假设前提 2)可知路由消息 $(dest\_id,V_y,nexthop,\cos t')$ 的来源、完整性是可以验证的，故此时可以判定路由消息是真实的。

5) 如果 N_M 不是目的节点，且 $C_M>1$，如果 $\forall C_i \in C_D\,(i=1,\cdots,x)$，都有 $C_i \leqslant C_M$，那么判定该条消息为虚假消息；如果 $\forall C_i \in C_D\,(i=1,\cdots,x)$，都有 $C_i \geqslant C_M$，那么将不再对该信息进行任何操作，算法结束；否则进行下面的步骤。

6) 统计 $C_M>C_i+1$ 和 $C_M<C_i-1\,(i=1,\cdots,n)$ 成立的个数，如果不超过 T 条成立，那么判定该条路由消息为真，否则为虚假路由消息，其中 T 为网络中设定的路由信息安全阈值，T 设置的设置依据用户对网络安全的需求，当 T 设置为 1 时网路的安全性最高，但是由于节点在计算转发表时可能存在一定的误算率，另外网络也应该有一定的容侵能力，所以 T 设置为 2 或 3 是比较合适的。

4.3　度量方法的有效性

在网络无合谋攻击的前提下，如果网络满足 4.1 节中给出的 2 个前提条件，假设 N_0 发起虚假路由欺骗节点 N_1，T 设置为 1。到达 D 的网络节点划分为 $L_D=\{l_{D1},l_{D2},\cdots,l_{Dn}\}$，$N_0$ 在网络中的位置关系有如下 4 种情况。

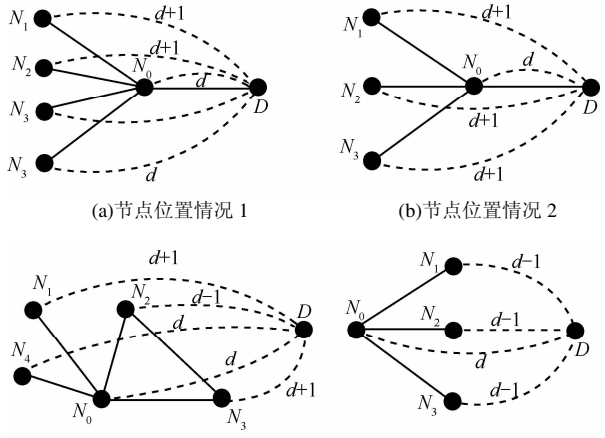
1) N_0 为目的节点，既 D 为 N_0；此时节点发布路由信息 $(D,-,0)$，其邻居节点按照度量方法中的步骤 1)，将对其进行前缀认证，由路由更新消息的源可认证，决定其可以发布该条路由消息；但是如果节点发布虚假的路由消息 $(D',-,0)$，且 D' 并不是自己的子网，那么其将无法通过其他节点对其进行的前缀认证，因为可发布的网络前缀和路由器是进行绑定的。

2) $N_0 \in l_{D1}$，即 N_0 为到达 D 的最后一跳；此时 N_0 如要发起短距虚假路由攻击，那么其只能宣称自己到达 D 的距离为 0，依据 1)的分析，无法攻击成功，故 N_0 无法发起短距虚假路由攻击；如果其发起长距虚假路由信息 $(D,Nx,d+n)$，此时分下面 2 种情况讨论。

① 如图 3(a)所示，N_0 的邻居节点集为 N，当 $N\bigcap l_{D1}\neq\phi$，且 $n=1$，此时如果 N_1 的邻居中没有距 D 的距离为 1 的节点，那么 N_1 仍然以 N_0 作为到达 D 的下一跳，这种情况下攻击无意义；$n>1$ 时，虚假路由消息将无法通过消息真实性度量方法步骤 5 的检测，所以攻击不成功。

② 如图 3(b)所示，N_0 的邻居节点集为 N，此时 $N\bigcap l_{D1}=\phi$，此时检测节点 N_1 可以依据消息真实性度量方法得到 $d_{N0}-d_{N2}\geqslant 0$ 和 $d_{N0}-d_{N3}\geqslant 0$，显然 N_0 没有到达 D 的下一跳，由此可以判断消息是虚假的，攻击失败。

3) 如图 3(c)所示，N_0 为中间节点，N_0 的邻居节点集为 N，且 $N\bigcup l_{Dd}\neq\phi$，$N\bigcup l_{Dd-1}\neq\phi$，$N\bigcup l_{Dd+1}\neq\phi$，如果其发起短距虚假路由信息 $(D,Nx,d-n)$，其中 $n\geqslant 1$，N_1 可以依据消息真实性度量方法得到 $|d_{N0}-d_{N4}|>1$；发起长距虚假路由攻击 $(D,Nx,d+n)$，其中 $n\geqslant 1$，N_1 可以依据消息真实性度量方法得到 $|d_{N0}-d_{N2}|>1$，所以此时 N_0 发起的任何虚假消息都无法成功。



(a)节点位置情况 1　(b)节点位置情况 2

(c)节点位置情况 3　(d)节点位置情况 4

图 3　N_0 与 D 的位置关系

4) 如图 3(d)所示，N_0 为边缘节点，其所有邻居到达 D 的距离都不大于自己到达 D 的距离；此时节点不承担任何到达目的节点 D 的流量，所以其发起长距虚假路由信息攻击无意义；如果其发起短距虚假路由信息 $(D,Nx,d-n)\,(n\geqslant 1)$，那么 N_1 可以依据消息真实性度量方法得到 $|d_{N0}-d_{N2}|=n+1$ 和 $|d_{N0}-d_{N3}|=n+1$，不论 n 取何值均不满足度量方法中的第五条，可以判断消息是虚假的。

综上所述，消息真实性度量方法在满足假设的条件下一定可以检测出节点发送的任何虚假路由更新消息。

4.4　对合谋攻击的抵御能力

4.3 节对消息真实性度量方法的正确性分析是在无合谋攻击的假设下进行的，但是在实际的网络中合谋攻击是存在，下面来分析消息真实性度量方法对合谋攻击的抵御能力。

假设节点 N_0 联合其邻居节点 $\{N_1,N_2,\cdots,N_k\}$ 对其邻居 M 发起合谋攻击，发送虚假的路由消息 (D,V_X,C)，节点 N_0 的邻居节点集为 $N=\{N_1,N_2,\cdots,N_n\}$，$M\in N$，邻居节点到达目的节点的距离为 $C_D=\{d_1,d_2,\cdots,d_n\}$，$M$ 的路由信息安全阈值设置

为 T ($T \geqslant 1$)。下面分析几个合法的节点发起合谋攻击，如想攻击成功需要多少个节点进行合谋。

1) 如果节点 N_0 发起短距虚假路由信息 $(D, Nx, d-n)$，其中 $n \geqslant 1$。当 $n=1$ 时，此时 N_0 要想成功的欺骗 M，那么必须要保证有一个邻居节点的距离等于 $d-n-1$，另外必须要保证 $\{Ni \| d_i-(d-1)|>1\}$ 的个数不大于 T，即要和 $L=\{N_i|d_i>d\}$ 中的 k' 个节点进行合谋，其中 $k'>|L|-T$，所以要想攻击成功 k 需要满足 $k>|L|-T+1$；当 $n>1$ 时，要和 $L'=\{N_i|d_i>d-n+1\}$ 中的 k 个节点进行合谋，并且还要合谋一个距离为 $d-n-1$ 的邻居，$|L'|=n$，即 $k>n-T+1$。

2) 如果节点 N_0 发起长距虚假路由信息 $(D, Nx, d+n)$，其中 $n \geqslant 1$。当 n=1 时，此时 N_0 要想成功的欺骗 M，那么必须要保证有一个邻居节点的距离等于 $d-n-1$ 和 $\{Ni|(d+1)|-d_i|>1\}$ 的个数不大于 T，即要和 $L=\{N_i|d_i<d\}$ 中的 k' 个节点进行合谋，其中 $k'>|L|-T$，所以要想攻击成功 k 需要满足 $k>|L|-T+1$；当 $n>1$ 时，N_0 要和 $k>n-T+1$ 个节点进行合谋，分析方法同短距虚假路由攻击。

通过以上的分析可以得到如下的结论：如果节点想发起 $n \geqslant 2$ 的虚假路由攻击，那么节点必须要和至少 $(n-T+1)$ 个邻居节点进行合谋，例如，当节点 $n=5, T=2$ 时，节点必须联合其中的 4 个节点才能攻击成功。但是如果发起 $n=2$ 的短距虚假路由消息攻击，当节点的上游节点的数目越多，合谋的攻击的难度越大，最好的情况是无上游节点如图 3(d)，此时节点只要和任一邻居节点合谋，该节点将自己的距离修改为 $d-2$，然后 N_0 发送虚假路由消息 $(D, Nx, d-1)$，此时是能够成功的，但是这样的攻击是没有意义的，因为 N_0 邻居节点也到达目的节点的距离也为 $d-1$，所以并不会将 N_0 作为达到目的节点的下一跳。

综上所述，消息真实性度量方法可以有效地抵挡节点发起的虚假路由攻击，即便在一些极端情况下可以成功地进行攻击，但是并不会对网络中的其他节点造成影响。

4.5 度量方法的复杂度

本节来分析消息真实性度量方法的计算复杂度，假设节点的平均连接度为 β，N 为网络的节点集合，当节点要对某邻居节点发送过来的一条路由更新消息进行真实性度量时，节点至多需要进行 $\beta-1$ 步的计算就可以判断消息的真实性；当节点要对邻居节点发送过来的所有路由消息进行真实性度量时，至多需要 $|N|(\beta-1)$ 步的计算就可以完成度量，所以节点对邻居节点发送过来的所有路由消息进行一次度量的复杂度为 $O(|N|)$。

4.6 度量方法对路由协议的影响

本节主要分析由于链路变化造成的正常更新在网络中是否能正常的扩散传播。假设网络存在如图 4 所示的网络拓扑，其中存在 $N_1 \sim N_6$ 的路径，其距离为 5 跳，此时网络中新加入一个和 N_1 相连的节点 N_0，下面分析当 N_0 分别和 N_2、N_3、N_4、N_5、N_6 相连时路由消息在网络中扩散传播情况。

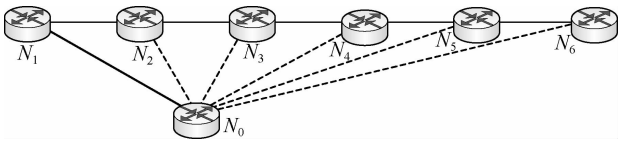


图 4 正常更新在网络的传播

1) 当 N_0 和 N_6 相连时，此时当节点 N_0 将路由更新消息 $(N_6, N_6, 1)$ 发送给 N_1 时，N_1 依据度量方法的步骤 4)可以判断路由更新消息是真实的。

2) 当 N_0 和 N_5、N_4 分别相连时，此时当节点 N_0 将路由更新消息 $(N_6, N_5, 2)$ 和 $(N_6, N_4, 3)$ 发送给 N_1，这种情况下由于当 N_0 加入网络中时必然向其邻居节点发送路由请求，当收到路由请求答复后必然会做一个局部的收敛，当收敛完成后，节点 N_0 到目的节点 N_6 的距离和其邻居节点到达 N_6 的距离的差值必然满足不大于 1，所以此时节点 N_1 是可以依据度量方法判断消息的真实性。

3) 当 N_0 和 N_3、N_2 分别相连时，此时发送的路由消息中的距离不影响 N_1 的选路，这些消息将不会在进行传播和扩散。

综上所述，度量方法不影响由于链路变化造成的正常路由更新在网络中的扩散和传播。

4.7 度量方法的仿真实验

本节将使用 SSFNet[19]仿真工具对度量方法的有效性进行仿真实验验证，网络使用的路由协议是 RIPv2，使用的接口是 10Mbit/s 的以太网口，设定链路延迟为 0.001s，路由器检测链路失效的时间设定为 0.02s，使用的网络拓扑是 BRITE[20]生成的最大的连接度数是 30，平均连接度数是 7.9 的 100 个节点的随机拓扑。

仿真实验设定网络中有 10 个节点为发起虚假路由消息的攻击，每次路由更新 10 个节点分成 5

组发送 1 条与实际距离差值为 2、3、4、5、6 的虚假路由信息，实验分别设置安全阈值 T 为 1、2、3、4、5。通过实验数据可以看到不论 T 如何设置，只要邻居节点的连接度大于 T，检测节点均可以 100%的检测出虚假路由消息。但是当将 T 设置为 1 时，网络存在一定的误报，其原因在于网络节点在计算转发表时可能存在一定的时延和误算率，所以为了避免误报将 T 设置为 2 或 3 是比较合适的。

5　结束语

本文主要研究了距离矢量路由协议的网络可生存性，研究发现影响距离矢量路由协议网络可生存性的主要原因是虚假路由信息在网络中的传播，文中给出了距离矢量路由协议网络可生存性的定义和计算方法，研究表明可以通过增加链路来提高网络的可生存性，但是在网络拓扑一定的情况下，无法通过增加链路来提高网络的可生存性，此时为了提高网络的可生存性给出了一种有效检测路由信息真实性的方法，分析和实验表明该方法可以有效的阻止虚假路由信息在网络中传播，有效地提高距离矢量路由协议的网络可生存性。

参考文献：

[1] FISHER E B, LINGER D. Survivable Network Systems: An emerging Discipline[R]. CMU/SEI-2001-TN-001. Pittsburgh, PA,USA: Software Engineering Institute, Carnegie Mellon University, 2001.

[2] AVIZIENIS A, LAPRIE J C, RANDELL B, *et al*. Basic concepts and taxonomy of dependable and secure computing[J]. IEEE Trans on Dependable and Secure Computing, 2004, 1(1):11-33.

[3] RAI S, MUKHERJEE B, DESHPANDE O. IP resilience within an autonomous system: Current approaches, challenges, and future directions[J]. IEEE Communications Magazine, 2003, 43(10):142-149.

[4] FILSFILS F C, EVANS J. Achieving sub-second IGP convergence in large IP networks[J]. ACM SIGCOMM Computer Communication Review, 2005, 35(2): 35-44.

[5] FORTZ B, THORUP M. Optimizing OSPF/IS-IS weights in a changing world[J]. IEEE JSAC, 2005, 20(4): 756-767.

[6] NELAKUDITI S, LEE S, YU Y, *et al*. Fast local rerouting for handling transient link failures[J]. IEEE/ACM Transaction on Networking, 2007, 15(2):359-372.

[7] WANG F, GAO L X. A backup route aware routing protocol - fast recovery from transient routing failures[A]. INFOCOM 2008[C]. Phoenix, 2008.2333 -2341.

[8] KVALBEIN A, HANSEN A F, *et al*. Multiple routing configurations for fast IP network recovery[J]. IEEE/ACM Transactions on Networking, 2009, 17(2): 473-486.

[9] HANSEN A F, KVALBEIN A, CICIC T, *et al*. Effective and stable ip recovery using resilient routing layers[A]. Proc 19th Int'l. Teletraffic Congress (ITC'19)[C]. Beijing, China, 2008

[10] WANG C, MA J F, ZHU J. Design and implementation of survivable network system[A]. 2005 International Conference on Intelligent Computing(ICIC'05)[C]. Springer-Verlag Berlin Heidelberg.2005.

[11] LIN X G, XU R S, ZHU M. Survivability computation of networked information systems[A]. International Conference on Computational Intelligence and Security(CIS'2005)[C]. Xi'an, China: Springer-Verlag Berlin Heidelberg. 2005.

[12] MITTAL V, VIGNA G.. Sensor-based intrusion detection for intra-domain distance-vector routing[A]. Proc of CCS'02[C]. Washington, D.C., USA, 2002.

[13] HU Y C, PERRIG A, JOHNSON D B. Efficient security mechanisms for routing protocols[A]. Proc NDSS'03[C]. San Diego, USA, 2003.

[14] WAN T, KRANAKIS E, OORSCHOT P C. S-RIP: a secure distance vector routing protocol[A]. ACNS, Maryland[C]. USA, 2004.103-119.

[15] HAIM Z, HANOCH L. Area avoidance routing in distance-vector networks[A], Proceedings INFOCOM 2008. The 27th Conference on Computer Communications[C]. IEEE, Phoenix, USA, 2008. 1148-1156.

[16] WANG F Y, WU F S. On the vulnerability and protection of OSPF routing protocol[A]. Proceedings of IEEE Seventh International Conference on Computer Communications and Networks[C]. Lafayette, LA, USA, 1998.12-15.

[17] MITTAL V, VIGNA G. Sensor-based intrusion detection for intra-domain distance-vector routing[A]. Proc of CCS'02[C]. Washington, D.C., USA, 2002.

[18] MEDHI D, HUANG D. Secure and Resilient Routing: a Framework for Resilient Network Architectures[M]. Information Assurance: Dependability and Security in Networked Systems, Morgan Kaufmann Publishers (an imprint of Elsevier),2007. 417-457.

[19] SSFnet (The Network Simulator) [EB/OL]. http://www.ssfnet.org.2010.

[20] BRITE[EB/OL]. http://www.cs.bu.edu/brite/.2010.

作者简介：

王滨（1978-），男，山东泗水人，浙江大学博士后，主要研究方向为宽带信息网络技术、高性能路由、信息安全。

郭云飞（1963-），男，河南郑州人，国家数字交换系统工程技术研究中心教授、博士生导师，主要研究方向为宽带信息网络技术、高性能交换技术、下一代网络。

兰巨龙（1962-），男，河北张家口人，国家数字交换系统工程技术研究中心教授、博士生导师，主要研究方向为高速宽带信息网络技术、网络路由与交换技术、军事信息网络工程。

吴春明（1967-），男，浙江萧山人，浙江大学计算机科学与技术学院教授、博士生导师，主要研究方向为网络服务质量、可重构网络、网络虚拟化。