基于可信度的域间路由机制

谭 晶 罗军舟 李 伟 于 枫
(东南大学计算机科学与工程学院 南京 210096)

摘 要 当前的域间路由系统缺乏对路径真实性的验证,可能导致虚假路径信息大量传播,带来大规模的网络失效.为了提高路由抑制虚假路径的能力,文中将信任机制引入到域间路由中,采用可信度表示路径的真实可信程度,提出了基于可信度的域间路由机制,其主要思想为在路径选择时考虑路径的可信度,选取可信度高的路径作为最优路径.在该机制下,构建了一个 Chord 环进行信任信息的发布与获取,部署了虚假路径检测措施的 AS 根据检测结果在 Chord 环中发布信任信息,没有部署虚假路径检测措施的 AS 从 Chord 环中获取信任信息来计算候选路径的可信度,基于可信度进行路径选择.实验结果表明基于可信度的域间路由机制能够快速抑制虚假路径,在一定程度上解决路由机制的不可信问题.

关键词 可信可控网络;域间路由;可信度;Chord 环
中图法分类号 TP393 **DOI 号**: 10.3724/SP.J.1016.2010.01763

Trust Degree Based Inter-Domain Routing Mechanism

TAN Jing LUO Jun-Zhou LI Wei YU Feng
(*School of Computer Science and Engineering, Southeast University, Nanjing* 210096)

Abstract Current inter-domain routing does not verify the reality of the received routes, it may cause the large-scale spread of false routes. To filter false routes, trust is introduced to inter-domain routing and an Trust Degree based Inter-domain Routing Mechanism(TDIRM) is proposed in this paper. The main idea of TDIRM is computing the trust degree of candidate paths and selecting the best path according to the trust degree. In TDIRM, Some ASes are selected to build a Chord ring for publishing and acquiring trust information of routing. ASes that can detect the false paths publish the trust information in the Chord ring, and other nodes can obtain the trust information from the Chord ring, compute the trust degree of the routes and select the trustworthy route information to distribute. The experimental results show that TDIRM can filter the false routes timely and improve the trustworthiness of routing.

Keywords trustworthy and controllable network; inter-domain routing; trust degree; Chord ring

1 引 言

随着互联网规模的增大以及应用需求的增多,对路由可靠性的要求越来越高.然而,作为当前域间路由协议的事实标准,BGP 在选路时不对路径真实性进行判定,可能接收到虚假的路径信息,无法保障路由服务的可靠性.例如,由于配置错误,伊朗电信

收稿日期:2010-04-26;最终修改稿收到日期:2010-08-15.本课题得到国家自然科学基金(60903161,60903162,90912002)、高等学校博士学科点专项科研基金(200802860031)、江苏省自然科学基金(BK2008030)、国家"九七三"重点基础研究发展规划项目基金(2010CB328104)、江苏省"网络与信息安全"重点实验室(BM2003201)、"计算机网络和信息集成"教育部重点实验室基金(93K-9)资助.**谭 晶**,男,1984 年生,博士研究生,主要研究方向为下一代互联网、路由机制.E-mail: tanjing@seu.edu.cn. **罗军舟**,男,1960 年生,博士,教授,博士生导师,主要研究领域为下一代网络体系结构、协议工程、网络安全与管理、网格计算. **李 伟**,男,1978 年生,博士,讲师,主要研究方向为下一代互联网、网络管理、服务计算. **于 枫**,女,1974 年生,博士研究生,讲师,主要研究方向为下一代互联网、网络管理.

服务商发布的虚假路径信息导致了全球用户长时间无法访问 YouTube[1].

为了提高 BGP 抵御虚假通告的能力,近年来提出了很多 BGP 的安全方案,主要分为安全保护[2-3]和异常检测[4-8]两大类. 典型的 BGP 安全保护方案有使用集中的路由权威机构和公钥基础设施的 SBGP[2]和 SoBGP[3]. 然而,这些方法对 BGP 改动过大,无法实现递增部署,并且需要消耗大量的运算资源,很难在全网范围内部署. 在异常检测方案中,Siganos 等提出基于互联网路由注册中心(IRR)提供的路由注册信息和某些已知的全局路由信息对自治系统的路由表进行异常和错误分析[4];文献[5-6]提出了基于多自治系统协同的思想对路由信息真实性进行验证的方法;文献[7-8]通过对路由信息进行安全监测来保证域间路由系统的安全. 这些方法多为在 BGP 外构建安全措施,能够实现递增部署. 然而,由于政治经济等因素以及方法本身的可扩展性,这些异常检测措施通常适用于小范围的检测,难以在整个 Internet 中得到部署.

除了基于安全机制的 BGP 方案外,部分研究者提出基于信任机制提高路由抵御虚假通告的能力. 胡宁等提出通过综合多个推荐者对目标 AS 的信任值构建目标 AS 的信誉,优先选择信誉高的 AS 提供的路径[9]. 该方法能够提高路由的可信性,但是其并没有阐述推荐者对目标 AS 的信任值如何产生,而是假设这类值可以得到. 在无线网络中,基于信任机制的路径选择得到了很多的研究[10-14]. Eschenauer 等提出了一种无线网络下信任证据产生、分发以及度量的高层框架[10]. Zouridaki 等采用基于贝叶斯的信任模型提高无线网络选路的准确性[11]. Pirzada 等提出了仅仅使用第一手信息对路径的可靠性进行评价,将评价结果转化为可信度的路由信任构建过程[12]. 然而,Internet 中信任构建与无线网中有很大的不同. Internet 规模远远超过移动网络,无法采用移动网络中常用的广播机制收集信任信息,同时如何在如此大的网络规模下构建一种可扩展、高效的信任信息发布与获取机制是一个很大的挑战.

为了解决网络的可控性和可信性,前期工作中本项目组提出了一种新的可信可控网络体系结构[13-15],该体系结构为把信任机制引入到域间路由打下了良好的基础. 可信可控网络提出将所有选路控制功能从路由器上剥离,由域内控制平台集中实现. 由于采用了逻辑集中的路由控制方式,高性能的处理设备可以被引入,便于信任信息的计算、存储与发布. 因此,在可信可控网络体系框架下,我们提出了一种基于可信度的域间路由机制. 该机制的基本思想为在路径选择时计算路径的可信度,选择可信度高的路径作为最优路径. 在该机制下,在网络中构建一个 Chord 环进行信任信息的发布与获取,部署了虚假路径检测措施的 AS 根据检测结果在 Chord 环中发布信任信息,没有部署虚假路径检测措施的 AS 从 Chord 环中获取信任信息来计算候选路径的可信度,基于可信度进行路径选择. 本文主要贡献如下:(1)提出了一种基于 Chord 环的信任信息发布与获取机制,具备较好的可扩展性,满足大规模的网络需求;(2)提出了域间路由中 AS 和路径的信任关系以及可信度的表示和计算方式;(3)对 BGP 进行扩展提出了基于可信度的域间选路机制. 为了简便起见,在本文以下的讨论中用节点表示网络中的 AS.

本文第 2 节介绍可信可控网络中的路由机制;第 3 节提出一种基于 Chord 环的路由信任信息发布与获取机制;第 4 节提出域间路由中信任关系及可信度的表示和计算方式;第 5 节对 BGP 的选路过程进行扩展,提出基于可信度的域间选路机制;第 6 节为实验以及结果分析;第 7 节总结全文并提出未来工作.

2 可信可控网络中的路由机制

在前期工作中,我们提出了可信可控的网络体系结构[14-15]. 可信可控网络的主要目的是提高网络的可控性以及可信性. 如图 1 所示,可信可控网络主要特征是在现有网络体系架构的基础上增加一个 4 层逻辑结构,其包括 4 个层面,即决策层、观测层、资源层和可信接口层. 其中“可信接口层”以协议跨层的方式实现现有网络体系与资源层的交互;“资源

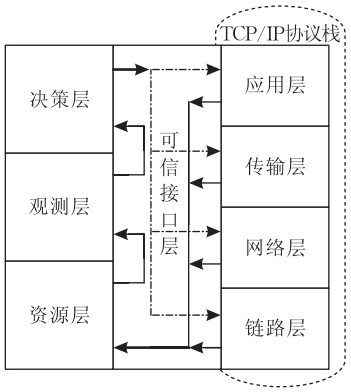


图 1 可信可控网络体系结构图

层”通过可信接口层的协议为观测层提供“资源流”；“观测层”从资源层提取特征，为决策层提供一个具有较好一致性及可观性的视图；“决策层”根据可观视图提出控制方案，通过接口层提供给网络，达到控制的目的.

与传统网络相比，可信可控网络具有以下优势：(1) 可信可控网络能够实现网络级别的控制目标. 由于可信可控网络具有集中的决策层面，这个决策层面集成了所有网络级别的控制机制，因而可以消除各个控制机制之间的决策冲突. (2) 可信可控网络能够容纳各种异构网络体系. 可信可控网络并不涉及网络传输的细节，只是针对网络控制结构，因而可信可控网络能够在各种网络环境中实现.

可信可控网络中采用域内集中、域间分布的路由方式，将控制逻辑从路由器上剥离，由域内路由控制平台(IRCP)集中实现，路由器不再进行任何路由决策，直接从路由控制平台接收控制指令完成配置. 域间可达性信息由相邻域的 IRCP 直接交互，如图 2 所示. 可信可控网络通过集中的路由控制平台，使得传统路由方式中路由器计算能力有限的限制不再存在，便于基于信任的路由机制中信任信息的处理.

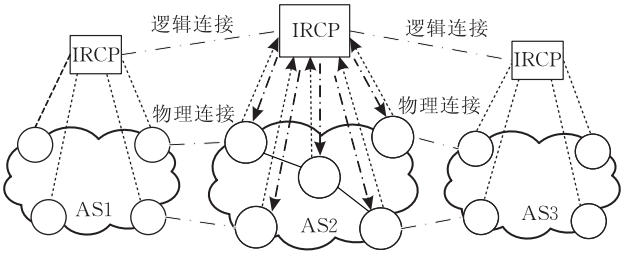


图 2　可信可控网络路由示意图

3　基于 Chord 环的信任信息发布

当前的研究已经提出了不少虚假路径检测方案. 这些措施在局部范围内部署比较可行. 然而，由于政治经济以及可扩展性等原因，难以在 Internet 范围内部署. 将各种检测措施的检测结果转化为信任信息在网络中共享，实现各种机制的互通互补，势必将提高 Internet 抵御虚假路径的能力.

由于 Internet 的规模极其巨大，采用移动网络中常用的邻居节点推荐信任信息的方式实现信任信息的共享的效果有限，需要更为有效的方式实现大规模的信任信息共享. 我们选取网络中的某些节点构成 Chord 环，在环中发布和获取路由信任信息. Chord[16] 协议是一种分布式资源查找协议，具有良好的健壮性和可扩展性. 它利用一致性散列算法(consistent hashing)将关键信息随机分散到一组被组织成 Chord 环的主机中，并能从环中的任何一台主机上查找存储的信息. 如图 3 所示，在基于 Chord 的信任发布网下，如果 Chord 环中的节点需要发布信任信息，其根据散列算法直接定位信息的存储节点并且将信任信息提交至该节点；如果 Chord 环外的节点需要发布信任信息，其将结果提交到最近的 Chord 环节点，由 Chord 环节点根据散列算法将结果转发至对应的存储节点. 如果 Chord 环中的节点需要获取某个节点的信任信息，其根据一致性散列算法可以定位到存储该信息的节点，获取所需的信任信息. 如果 Chord 环外的节点需要获取网络中某个节点的信任信息，其可以向最近的 Chord 环节点发出信任信息获取请求，收到信任信息获取请求的节点在 Chord 环中获取对应的信任信息，将其返回至请求节点.

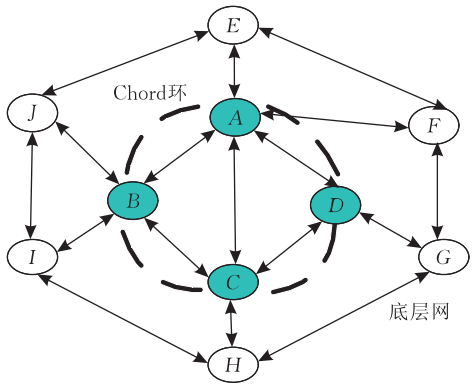


图 3　基于 Chord 环的信任发布网

基于 Chord 环构建一个 Internet 范围内的信任发布网进行信任信息的发布与获取有着以下优点：(1) 解决了传统信任构建方式中常用的广播机制可扩展性不强的问题，通过一个分布式的信任信息发布结构降低了网络的负载；(2) 分布式的信息存储方式能够实现均衡的网络信任信息存放，满足 Internet 规模下的信任信息存放需求；(3) 能够实现高效的信任信息的发布与获取，在规模为 n 的 Chord 环下基于 Finger 表的信任信息发布与获取时间不会超过 $\Theta(\log(n))$ 时间，满足信任信息发布与查找需求.

4　域间路由中节点和路径的信任关系及可信度计算

为了能够将当前主要的虚假路径检测措施的结

果转化为信任,需要一种合适的域间路由信任表示方式.我们采用了基于D-S理论[17]的信任关系表示及计算框架,采用三元组〈信任,不信任,不确定〉表示对象间的信任关系.可信度是信任关系在特定环境下的转化结果,为数值的形式,通过将信任关系的各元素权衡得到,相同的信任关系在不同的环境下可能转化得到不同的可信度.

4.1 基于D-S理论的信任关系计算框架

在Internet环境下,收集进行信任计算的证据可能是不全面、不具体的,需要找到适合Internet环境的信任关系计算方法.D-S证据理论[17]将概率论中的单点赋值扩展为集合赋值,弱化了相应的公理系统,满足了比概率更弱的要求,适合于不确定推理的场合,在计算机科学的很多领域得到了应用.考虑域间路由系统的分布式特性且信任证据的收集具有模糊、不确定的特征,利用D-S证据理论对路由中的信任关系进行分析是一个合适的选择.

定义1. 信度分配函数 m 定义为从 Θ 的幂集 $P(\Theta)$ 到[0,1]区间的映射:

$$m:P(\Theta)\rightarrow[0,1],\ m(\varnothing)=0,\ \sum_{A\in P(\Theta)} m(A)=1.$$

D-S证据理论中另外一个比较重要的定义为多个证据的组合规则,即Dempster规则.

定义2. 对 n 个证据进行组合的Dempster一般化规则为

$$m_{1..n}(A)=K_n^{-1}\sum_{\cap_i A_i=A} m_1(A_1)m_2(A_2)\cdots m_n(A_n),$$

其中 $A\neq\varnothing$,K_n 为归一化因子,

$$K_n=\sum_{\cap_i A_i\neq A} m_1(A_1)m_2(A_2)\cdots m_n(A_n).$$

定义3. 网络实体的信任识别框架 Θ 为集合{信任,不信任},Θ 的幂集合为{$\varnothing$,{T},{F},{T,F}},实体的信任关系采用三元组 $C=\langle m(\{T\}),m(\{F\}),m(\{T,F\})\rangle$ 描述,其中有 $m(\{T\})+m(\{F\})+m(\{T,F\})=1$.

我们采用类概率函数来表示路由中的信任关系,由文献[17]可知,网络中具有交互行为的实体间的信任的类概率函数为

$$f_B^A(\{T\})=(1+2m_B^A(\{T\})-m_B^A(\{F\}))/3.$$

由文献[18]可知,类概率在一定条件下,成为此时的确实可信度,具体如下.

定义4. 实体 A 对实体 B 的可信度为

$$H_B^A(T)=MD(P/E)\times f_B^A(\{T\}),$$

其中 $MD(P/E)$ 为知识的前提 P 与相应的证据 E 的匹配程度.

在我们以下的讨论中,知识的前提 P 与相应的证据 E 都是匹配的,因此据D-S理论的定义可知,$MD(T/E)=1$,所以有

$$H_B^A(T)=f_B^A(\{T\})=(1+2m_B^A(\{T\})-m_B^A(\{F\}))/3 \quad (1)$$

4.2 信任关系及可信度

域间路由包括两种信任关系:节点和路径信任关系,由于我们的目标是抑制网络中的虚假路径,因此节点的信任关系应当表示其发布路径信息的真实可信程度,路径的信任关系则表示该路径的真实可信程度.

将具备路径真实性判定能力的节点称为检测方,被检测的节点称为被检方,检测方对被检方发布的路径信息进行真实性检测,根据检测结果计算被检方的信任关系,并将被检方的信任关系发布到Chord环中;Chord环存储节点将所有检测方对某个被检方的信任关系组合,计算该被检方的全局信任关系;没有部署虚假路径检测措施的节点在Chord环中获取路径上节点的全局信任关系,并根据路径上节点的全局信任关系计算路径的信任关系及可信度,实现基于可信度的路径选择.

我们将虚假路径检测机制的检测结果统一用真实、虚假以及不能确定三种标准表示,根据我们对现有域间路由虚假路径检测方案的分析,我们认为这种表示方式是合适的,其基本能够表示现有的所有检测措施的检测结果.Siganos等[4]提出的基于IRR的路由表异常检测方式能够准确判定路径的真实性,然而,由于其可能并不能获得完整的网络拓扑,对部分路径并不能准确判定,检测结果对应真实、虚假以及不确定3种方式.同样地,文献[5-6]中提出的构建独立的机构进行路由诊断的方法也只能对部分路由信息进行诊断,诊断结果同样可以分为真实、虚假以及不确定3种.其它方法我们不一一列出.

4.2.1 节点信任关系及其可信度

如图4所示,检测方对被检方的信任关系可以分为3种:基于被检方某个阶段表现构建的对其阶段信任关系;基于被检方过去表现构建的对其历史信任关系;基于被检方一贯表现构建的对其一贯信任关系.阶段信任关系每隔一个时间段计算一次,距离当前时刻超过一个阶段的阶段信任关系即为历史信任关系.一贯信任关系是检测方对被检方可信程度的全面描述,根据对被检方当前阶段信任关系以及当前阶段之前 I 个时间段内的历史信任关系计算节点的一贯信任关系.节点的一贯信任关系被发布

到 Chord 环中.

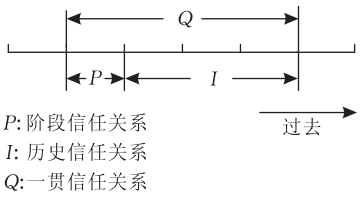


图 4　节点信任关系示意图

检测方采用如下的方式计算被检方的在第 t 次更新后的一贯信任关系：如果在第 t 次时间段内检测方 B 接收到了被检方 A 所在的 n 条路径，B 首先计算 A 在每条路径 $P_i(1\leq i\leq n)$ 中的信任关系 $C_B^{A,P_i}(t)$，根据 $C_B^{A,P_i}(t)(1\leq i\leq n)$ 计算 A 在第 t 个时间段内的阶段信任关系 $C_B^A(t)$，再根据 $C_B^A(t)$ 以及 $C_B^A(t-1)$、$C_B^A(t-2)$，…，$C_B^A(t-I)$ 计算 A 的一贯信任关系.

(1) 节点在路径中的信任关系

我们采用如下的方式计算 B 对节点 N_i 在路径 P 中的信任关系 $C_B^{N_i,P}(t)$. 节点 B 收到节点 N_1 转发的路径 $P=N_1N_2\cdots N_k$，如果 B 无法确定路径 P 的真实性，则设定 P 上所有节点 N_i 在路径 P 中的信任关系为无法确定，即 $C_B^{N_i,P}(t)=\langle 0,0,1\rangle(1\leq i\leq k)$；如果 B 能够准确判定 P 的真实性，则按照以下的方式计算 N_i 在路径 P 中的信任关系. 如果路径 P 中 $N_{j+1}N_{j+2}\cdots N_k$ 部分是真实的，从 P 中 $N_j(j\leq k)$ 处起出现虚假路径信息，则根据域间路径的传播机制，节点 $N_1,N_2,\cdots,N_{j-1}$ 都可能是生成虚假路径信息的节点. 检测方 B 认为节点 $N_{j+1},N_{j+2},\cdots,N_k$ 是可信的，有 $C_B^{N_i,P}(t)=\langle 1,0,0\rangle(j+1\leq i\leq k)$；路径 P 的一部分 $P'=N_1N_2\cdots N_{j-1}(j>1)$ 为虚假的，其信任关系为 $\langle 0,1,0\rangle$，节点 $N_1,N_2,\cdots,N_{j-1}$ 生成虚假信息的概率是等价的，其在路径 P 中的信任关系也应当是等价的，采用 $\langle x,y,z\rangle$ 表示节点 $N_1,N_2,\cdots,N_{j-1}$ 在路径 P 中的信任关系. 既然路径 $P'=N_1N_2\cdots N_{j-1}$ 的信任关系已知为 $\langle 0,1,0\rangle$，我们需要求解 P' 中每个节点的信任关系，根据路径上节点信任关系计算路径信任关系的方法(参见 4.2.2 小节)，我们得到式(2)的方程组.

$$\begin{cases} x^{j-1}=0 \\ (j-1)y-(j-2)y^2+(j-3)y^3+\cdots+(-1)^{n+1}y^{j-1}=1 \\ z=1-x-y \end{cases} \tag{2}$$

经过对式(2)化简，我们得到式(3)：

$$\begin{cases} x^{j-1}=0 \\ (j-1)y+(j-1)y^2-(-y)^{j+3}-2y-1=0 \\ z=1-x-y \end{cases} \tag{3}$$

在式(3)中，由于 $y<1$，在 j 极大时，$(-y)^{j+2}$ 趋向于 0，我们可以将该项省略，求解得到式(4).

$$\begin{cases} x=0 \\ y=\dfrac{3-j+\sqrt{(j-1)^2+4}}{2(j-1)} \\ z=1-x-y \end{cases} \tag{4}$$

从而得到 $N_1,N_2,\cdots,N_{j-1}$ 在路径 P 中的信任关系如式(5).

$$C_B^{N_i,P}(t)=\left\langle 0,\frac{3-j+\sqrt{(j-1)^2+4}}{2(j-1)},1-\frac{3-j+\sqrt{(j-1)^2+4}}{2(j-1)}\right\rangle \tag{5}$$

其中 $1\leq i\leq j$.

(2) 节点阶段信任关系

根据节点在路径中的确定的信任关系，可以计算节点的阶段信任关系. 对第 t 个时间段内检测方 B 对被检方 A 所在的 n 条路径 $P_i(1\leq i\leq n)$ 中的信任关系 $C_B^{A,P_i}(t)(C_B^{A,P_i}(t)\neq\langle 0,0,1\rangle)$ 求取平均值，计算出在第 t 个时间段内的 B 对 A 的阶段信任关系 $C_B^A(t)$ 如式(6)所示.

$$C_B^A(t)=\langle m_B^A(\{T\},t),m_B^A(\{F\},t),m_B^A(\{T,F\},t)\rangle \tag{6}$$

其中

$$m_B^A(\{T\},t)=\frac{\sum_{i=1}^{n}m_B^{A,P_i}(\{T\},t)}{n},$$

$$m_B^A(\{F\},t)=\frac{\sum_{i=1}^{n}m_B^{A,P_i}(\{F\},t)}{n},$$

$$m_B^A(\{T,F\},t)=1-m_B^A(\{T\},t)-m_B^A(\{F\},t).$$

(3) 节点一贯信任关系

根据节点的阶段信任关系以及历史信任关系，可以计算节点的一贯信任关系. 根据 B 对 A 的阶段信任关系以及历史信任关系计算在第 t 次更新后 B 对 A 的一贯信任关系 $TC_B^A(t)$ 如式(7)：

$$TC_B^A(t)=\langle tm_B^A(\{T\},t),tm_B^A(\{F\},t),tm_B^A(\{T,F\},t)\rangle \tag{7}$$

其中有

$$tm_B^A(\{T\},t)=\alpha_1\times m_B^A(\{T\},t)+\beta_1\times\frac{1}{I}\times\int_{t-I}^{t-1}m_B^A(\{T\},x)\mathrm{d}x \tag{8}$$

$$tm_B^A(\{F\},t)=\alpha_2\times m_B^A(\{F\},t)+\beta_2\times\frac{1}{I}\times\int_{t-I}^{t-1}m_B^A(\{F\},x)\mathrm{d}x \quad (9)$$

$$tm_B^A(\{T,F\},t)=1-tm_B^A(\{T\},t)-tm_B^A(\{F\},t).$$

其中在式(8)中有 $\alpha_1+\beta_1=1$,式(9)中有 $\alpha_2+\beta_2=1$.

式(8)通过加权节点的阶段信任关系与历史信任关系求取节点的一贯信任关系.其中 $m_B^A(\{T\},t)$ 表示了在第 t 个时间段内的 B 对 A 的确定信任程度;$\frac{1}{I}\times\int_{t-I}^{t-1}m_B^A(\{T\},x)\mathrm{d}x$ 表示在过去的 I 个时间段内 B 对 A 的确定信任程度的平均值,在本文中 $m_B^A(\{T\},x)$ 为离散变量,积分形式即为离散量的平均值.α_1、β_1 可以用来调节各部分变量所占的权值,使得计算公式适应不同的需求.α_1 取值较大则表示更加注重阶段信任关系在一贯信任关系中占据的比例,更加注重被检方的当前状态;β_1 取值较大则表明更加注重其历史表现.式(9)与式(8)基于同样的原理.由于域间路由的实时性特性,我们希望节点的可信度遵循"慢升快降"的原则,即如果节点发布了虚假路径信息,则对其确定信任程度将快速下降,不信任程度将快速上升,根据式(1)其可信度将会快速下降;而如果其有稳定优异表现,则对其确定信任程度将缓慢上升,根据式(1)其可信度将会缓慢上升.我们采用了自适应的 α_1、β_1 以及 α_2、β_2 的取值来达到可信度"慢升快降"的效果.

$$\begin{cases}\alpha_1<\beta_1\ m_B^A(\{T\},t)>\dfrac{1}{I}\times\displaystyle\int_{t-I}^{t-1}m_B^A(\{T\},x)\mathrm{d}x\\ \alpha_1>\beta_1\ m_B^A(\{T\},t)<\dfrac{1}{I}\times\displaystyle\int_{t-I}^{t-1}m_B^A(\{T\},x)\mathrm{d}x\\ \alpha_2>\beta_2\ m_B^A(\{F\},t)>\dfrac{1}{I}\times\displaystyle\int_{t-I}^{t-1}m_B^A(\{F\},x)\mathrm{d}x\\ \alpha_2<\beta_2\ m_B^A(\{F\},t)>\dfrac{1}{I}\times\displaystyle\int_{t-I}^{t-1}m_B^A(\{F\},x)\mathrm{d}x\end{cases} \quad (10)$$

式(10)根据被检方信任关系的变化趋势确定 α_1、β_1 的取值,如果在过去一段时间内的对被检方确定信任程度提高了,则表明被检方发布的真实路径比例提高了,设定 α_1 的取值小于 β_1,则确定信任程度将缓慢上升,节点的可信度将会缓慢上升;如果在过去的一段时间内被检方的确定信任程度降低了,则设定 α_1 的取值大于 β_1,确定信任程度将会快速下降,节点可信度将会快速下降.α_2、β_2 的取值基于同样的道理.

(4) 节点全局信任关系

根据各个检测方提供的被检方的一贯信任关系,Chord 环存储节点生成被检方的节点全局信任关系.在第 t 次更新计算时刻如果有 K 个节点 $N_1,\cdots,N_i,\cdots,N_K(1\leq i\leq K)$ 向 Chord 环中提交了节点 A 的信任关系,则第 t 次更新时刻节点 A 的全局信任关系如式(11).

$$TC^A(t)=\langle tm^A(\{T\},t),tm^A(\{F\},t),tm^A(\{T,F\},t)\rangle \quad (11)$$

其中有

$$tm^A(\{T\},t)=\Big(\sum_{i=1}^{K}H^{N_i}(t)\times tm_{N_i}^A(\{T\},t)\Big)\Big/\sum_{i=1}^{K}H^{N_i}(t)$$

$$tm^A(\{F\},t)=\Big(\sum_{i=1}^{K}H^{N_i}(t)\times tm_{N_i}^A(\{F\},t)\Big)\Big/\sum_{i=1}^{K}H^{N_i}(t),$$

$$tm^A(\{T,F\},t)=1-tm^A(\{T\},t)-tm^A(\{F\},t).$$

式(11)中 $H^{N_i}(t)$ 为节点 N_i 在第 t 次更新后的全局可信度,其可以根据 N_i 的全局信任关系通过式(1)计算出.我们将节点 N_i 的全局可信度作为其提交结果的权值计算节点 A 的全局信任关系.通过这种方式,如果某些恶意节点对 A 进行诽谤,则其诽谤结果不会对 A 的全局信任关系造成大的影响.

4.2.2 路径信任关系及其可信度

对于没有部署路径真实性检测措施的节点,如果其收到了某条新的路径 $P=\langle N_1,N_2,\cdots,N_M\rangle$,其可以在 Chord 环中查询路径上每个节点的全局信任关系,并且根据路径上每个节点的全局信任关系计算路径的全局信任关系,再根据式(1)将路径的全局信任关系转化为路径 P 的全局可信度.

路径 P 上的节点 N_i 在第 t 次更新后的全局信任关系表示为

$$TC^{N_i}(t)=\langle tm^{N_i}(\{T\},t),tm^{N_i}(\{F\},t),tm^{N_i}(\{T,F\},t)\rangle.$$

根据路径 P 上节点 $N_i\in P$ 的全局信任关系 TC^{N_i} 计算出路径 P 在第 t 次更新后的全局信任关系 $TC^P(t)$,其根据如下的原则:只有当路径上所有节点都可信时,路径才是可信的;只要路径上有一个节点不可信,路径就不可信.我们通过一个例子阐述路径信任关系的计算方式.

路径 $P=N_1N_2\cdots N_M$ 可以看作 $(((N_1N_2)N_3)\cdots N_M)$,其中 $P'=N_1N_2$ 的信任关系 $TC^{P'}(t)=\langle tm^{P'}(\{T\},t),tm^{P'}(\{F\},t),tm^{P'}(\{T,F\},t)\rangle$,计算方式如下:

$$tm^{P'}(\{T\},t)=tm^{N_1}(\{T\},t)\times tm^{N_2}(\{T\},t),$$

$$tm^{P'}(\{F\},t)=tm^{N_1}(\{F\},t)+tm^{N_2}(\{F\},t)-tm^{N_1}(\{F\},t)\times tm^{N_2}(\{F\},t)$$

$$tm^{P'}(\{T,F\},t)=1-tm^{P'}(\{T\},t)-tm^{P'}(\{F\},t).$$

将 P' 看作一个节点，采用以上方法综合 P' 的信任关系以及节点 N_3 的信任关系，可以计算出路径 $P''=(N_1N_2)N_3$ 的信任关系，将该过程迭代，最终能够计算出路径 $P=N_1N_2N_3\cdots N_M$ 的信任关系如式(12).

$$TC^P(t)=\langle tm^P(\{T\},t),tm^P(\{F\},t),tm^P(\{T,F\},t)\rangle \tag{12}$$

其中 $tm^P(\{T\},t)=\prod_{i=1}^{M}(tm^{N_i}(\{T\},t))$，$N_i\in P$，$M$ 表示 P 上的节点的个数.

$$tm^P(\{F\},t)=\sum_{i=1}^{M}(tm^{N_i}(\{F\},t))+(-1)^1\sum_{i,j=1\&\&i\neq j}^{M}((tm^{N_i}(\{F\},t))\cdot(tm^{N_j}(\{F\},t)))+(-1)^2\sum_{i,j,k=1\&\&i\neq j\neq k}^{M}((tm^{N_i}(\{F\},t))\cdot(tm^{N_j}(\{F\},t))\cdot(tm^{N_k}(\{F\},t)))+\cdots+(-1)^{M-2}\sum_{i,j,\cdots,q=1\&\&i\neq j\neq\cdots\neq q}^{M}\cdot\underbrace{((tm^{N_i}(\{F\},t))\cdot(tm^{N_j}(\{F\},t))\cdot\cdots\cdot(tm^{N_q}(\{F\},t)))}_{M-1\text{个}}$$

$$tm^P(\{T,F\},t)=1-tm^P(\{T\},t)-tm^P(\{F\},t).$$

根据式(1)，得到路径 P 在第 t 次更新后的全局可信度 $H^P(T,t)$ 如式(13)：

$$H^P(T,t)=(1+2tm^P(\{T\},t)-tm^P(\{F\},t))/3 \tag{13}$$

5　基于可信度的域间路由机制

在本节中我们对 BGP 的选路机制进行了扩展，在路径选择过程中考虑了路径的可信度，构建了基于可信度的域间路由机制. 由于 BGP 路径通告中包含了路径中每个 AS 的 AS 号，可以直接基于 AS 号进行路径可信度的计算. 基于可信度的域间路由决策过程改变了 BGP 中 *LocalPref* 参数的设定方式并且采用一个新的参数 *LengthVSTrust* 替换了传统 BGP 路径选择过程中的 *AS path length* 参数，将可信度融入到路径选择中，我们称扩展后的域间路由协议为 T-BGP.

作为事实上的域间路由标准，BGP 的选路过程可以简单地分为 3 个步骤：路径接收、路径选择以及路径转发. 路径的接收过程接收邻居转发的路径，提交路径选择过程进行路径选择；路径选择过程基于一系列的属性值进行比较，从而确定最优路径；路径转发过程将选择的最优路径转发给邻居. 其中路径选择过程是路由过程的关键步骤，Caesar 等阐述了 BGP 中路径选择的 7 个参数，如表 1 所示，路径选择过程依照步 1～7 的参数对候选路径进行比较，直至选择出最优路径[19].

表 1　BGP 路径选择参数

步骤	属性参数
1	*LocalPref*
2	*AS-path-length*
3	*Origin-type*
4	*MED*
5	*eBGP-learned over iBGP-learned*
6	*IGP-cost*
7	*Router-ID*

T-BGP 选路仍然采用与 BGP 相似的 7 步比较过程，但是对其中 *LocalPref* 值的设定方式与 *AS-path-length* 参数进行了改变. 在BGP中，选路的第一步选择 *LocalPref* 最高的路径，*LocalPref* 一般由 ISP 根据网络的流量工程、网络安全等需求设定. 在修改后的 T-BGP 中，ISP 在设定本地 *LocalPref* 时加入路径可信度的考虑，将可信度高又满足 ISP 利益需求的路径设定较高的 *LocalPref* 值，可信度低的路径设定较低的 *LocalPref* 值. 通过这种方式，在 T-BGP 中路径选择的第 1 步可以将可信度低的路径排除. 同时，为了选择可信度高且跳数尽可能少的路径，在 T-BGP 中路径选择的第 2 步采用一个新的属性 *LengthVSTrust* 替代了 BGP 中的 *AS path length* 属性. *LengthVSTrust* 参数基于路径的跳数以及可信度综合计算，其计算方式在式(14)中给出.

$$LengthVSTrust=H^P/Hops \tag{14}$$

在式(14)中 H^P 表示路径 P 的可信度，*Hops* 参数表示路径 P 的跳数. *LengthVSTrust* 的计算兼顾了跳数与路径可信度，与路径的可信度成正比，与路径的跳数成反比. 出于提高路由可信度的考虑，我们希望选择 *LengthVSTrust* 值最大的路径作为最优路径，然而，这种情况可能带来域间路由的振荡. 比如，如果路径 P_1 与路径 P_2 间的 *LengthVSTrust* 值相差不大，且交替领先，则会出现最优路径在 P_1 和 P_2 间反复切换，带来路由振荡问题. 为了避免路由振荡问题，我们设定 T-BGP 决策过程的第 2 步不是选择 *LengthVSTrust* 值最大的路径作为最优路径，

而是设定 *LengthVSTrust* 值与最大 *LengthVSTrust* 差值小于阈值 M 的路径都作为 T-BGP 第 3 步决策的候选路径. 在图 5 中,我们采用 *SelectTrustworthyPath*( )函数从 T-BGP 决策过程第一步后剩余的候选路径中选择 *LengthVSTrust* 值满足要求的路径作为第 3 步决策的候选路径. 在 T-BGP 中节点在设定路径 *LocalPref* 时就已经计算过路径的可信度了,在图 5 中省略了路径可信度的计算过程,直接采用 *CPath*[*i*]. *TrustDeg* 表示第 i 条路径的可信度.

在 T-BGP 中,可以根据网络状况选择合适的信任信息发布及获取方式. 定时更新以及当信任关系的变化超出某个阈值时才发布更新都是可行的方法. 信任信息需求节点可以采用定时获取的方式从 Chord 环中获取信任信息,也可以向 Chord 环中存储节点订阅信任信息. 实验中分析了采用不同的信任信息更新策略时 T-BGP 的性能.

此外,T-BGP 仅仅修改了 BGP 的决策过程,对于 BGP 的报文格式并没有进行修改,便于了 T-BGP 在网络中的递增部署,提高了其可行性.

```
Path Selection Algorithm based-on Trust Degree(PSATD)
1. SelectTrustworthyPath(CPath[], M)
      //CPath 为候选路径的集合,M 为 LengthVSTrust 阈值
2. {
3.    BestPath=CPath[1];
4.    While(i<=CPath.Size)
5.    {
6.      CPath[i].LengthVSTrust=CPath[i].TrustDeg/
                                CPath[i].Hops;
                    //计算路径的 LengthVSTrust 属性值
7.      if(BestPath.LengthVSTrust)<
                                CPath[i].LengthVSTrust)
8.          BestPath=CPath[i]; //选取最优路径
9.      i++;
10.   }
11.   While (t<=CPath.Size)
12.   {
13.     if (BestPath.LengthVSTrust-M)<
                                CPath[t].LengthVSTrust)
14)         AddPath(TrustworthyPath[], CPath[t]);
       //将CPath[t]加入到候选路径集 TrustworthyPath[]中
15.     t++;
16.   }
17.   Return TrustworthyPath[];
              //返回结果作为 T-BGP 第 3 步决策候选路径
18. }
```

图 5 T-BGP 中基于可信度路径选择算法

6 实 验

为了更加直观地阐述基于可信度的域间路由的价值,本节通过实验验证了该机制提高域间路由安全性、选路准确性的效果.

6.1 实验部署

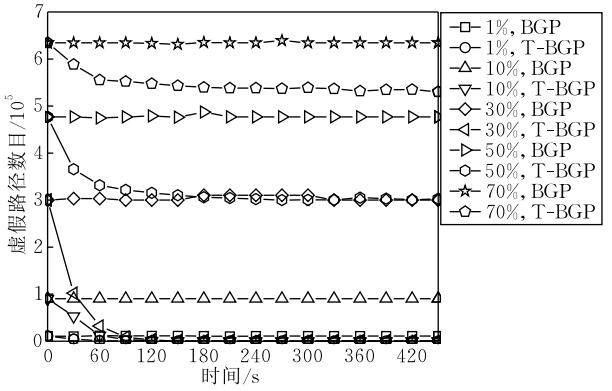
我们采用 SSFNet[20] 实现了基于可信度的域间路由机制并考察其性能. 我们采用 BRITE[21] 拓扑产生器来产生了一个 500 个节点的拓扑,每个节点代表网络中的 AS. 为了仿真 Internet 中的策略关系[22],我们将拓扑中某些具备较高连接度的节点设定为 tie-1 的服务者,其下的节点设定为 tie-2 的节点,其它的节点关系依此设定. 每条连接的延迟被 BRITE 自动设定在 0～5ms 之间,在实验中我们忽略每个节点处理消息的延迟.

我们将选取出的 tie-1 的节点作为 Chord 环节点,构建了一个包含了 10 个节点的 overlay. 在 overlay 中实现了对信任信息的发布与获取,我们在 500 个节点中随机选择了 20 个节点部署了文献[4]的虚假路径检测措施,每个节点拥有全网十分之一的拓扑结构,判定与拓扑结构不相符合的路径为虚假路径. 网络中的每个节点都部署 T-BGP. 我们将默认的初始信任关系设定为〈0,0,1〉. 式(8)中的 I 值设定为 10. 将式(10)中 α_1、β_1 中的较小值设定为 0.3,较大值设定为 0.7;α_2、β_2 同样也是较小值设定为 0.3,较大值设定为 0.7. 在实验 1、2、3、5 中设定阈值 M 为最大 *LengthVSTrust* 值的 $\frac{1}{5}$. *LocalPref* 的值设定采用如下的标准:节点可信度在 0.7～1 时 *LocalPref* 设定为 5;在 0.5～0.7 时设定为 4;在 0.3～0.5 时设定为 3;在 0～0.3 时设定为 2.

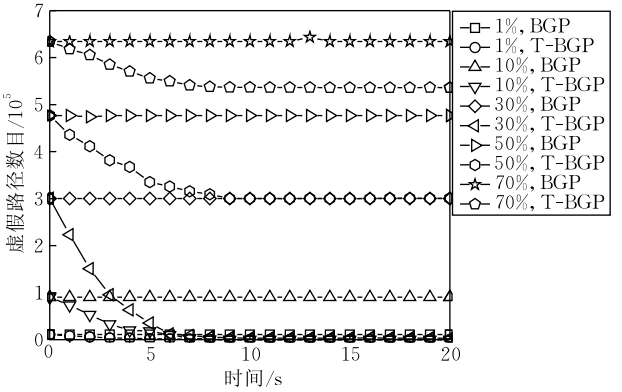
6.2 实验结果分析

实验 1. 验证基于可信度域间路由机制抑制虚假路径的能力. 在当前的路由系统中,路径不可信的原因主要有两方面:(1) 恶意节点发布了虚假路径信息;(2) 非恶意节点发布了该节点认为是真实的路径信息,然而由于网络收敛慢或者拓扑发生改变等第三方原因造成其它节点收到该路径信息时却与真实网络环境不一致. 为了表示第 1 种原因造成的网络虚假路径,我们在除去 Chord 环节点以及虚假路径检测节点外的节点中分别随机选择 1%、10%、30%、50%以及 70%的节点设定为恶意节点发布虚假路径信息. 为了表示第 2 种原因造成的网络虚假路径,我们将网络中的节点失效概率设定为 0.3%[23],失效的持续时间随机设定为 5s～300s 之间. 我们在两种信任关系更新策略下考察了 T-BGP 抑制虚假路径的速度. 在第 1 种策略中设定检测节点检测到节点的新可信度比原可信度变化超过 20%后立即向 Chord 环中发布更新,Chord 环立即

将节点的可信度发布至需求节点；在第 2 种策略中，检测节点每隔 30s 向 Chord 环中发布一次信任信息，Chord 环节点同样每隔 30s 向外发布一次信任信息. 我们构建了两个环境，第 1 个环境中运行 BGP，在第 2 个环境中运行 T-BGP. 进行 50 次实验，取 50 次的平均值作为实验结果，见图 6，其中每个项由两个参数标记，第 1 个参数表示网络中恶意节点的规模，第 2 个参数表示网络中运行的协议，比如(1%，BGP)表示运行 BGP 协议时网络中有 1%的节点为恶意节点. 图 6(a)给出了采用 30s 更新间隔时 T-BGP 抑制虚假路径信息的能力，图 6(b)给出了一旦节点的可信度变化超过其原可信度 20%的情况下就发布更新策略下 T-BGP 的抑制能力.



(a) 30s信任信息更新间隔下T-BGP效果



(b) 节点可信度变化超过20%发布更新下T-BGP效果

图 6　T-BGP 抑制虚假路径效果

通过图 6 可以看到，在每种更新策略下，T-BGP 在各种恶意节点规模下都能够有效地将部分虚假路径排除出网络. 当恶意节点数目小于 30%时，抑制的效果非常好，网络中残余的虚假路径极少. 在恶意节点比例为 50%以及 70%的情况下，网络最终会残余部分虚假路径. 我们分析这是由网络的连接状况决定的，在恶意节点规模过大的情况下，某些节点除去恶意节点提供的路径外再没可用路径. 而在 BGP 中，如果没有人工的参与，虚假路径信息会一直存在. 在图 6 中还可以看出，在节点可信度变化超过 20%立即更新的策略下 T-BGP 抑制虚假路径的速度较快，而在固定更新间隔的方式下 T-BGP 抑制虚假路径的速度与更新间隔有关，速度较慢.

实验 2.　验证了 T-BGP 采用不同信任信息更新策略时网络的负载情况. 我们同样构建了两个环境，第 1 个环境中运行 BGP，在第 2 个环境中运行 T-BGP，分别统计运行 BGP 与 T-BGP 时的网络负载情况. 与实验 1 相同，网络中的节点的失效概率设定为 0.3%[23]，失效的持续时间随机设定为 5s～300s 之间. 我们统计了每隔 30s 定时更新方式下的网络负载情况以及节点可信度变化超过 20%立即发布更新两种情况下的网络负载情况. 在不同更新策略下，我们又考察了不同规模恶意节点对网络负载造成的影响，在除去 Chord 环节点和虚假路径检测节点外的节点中随机选择了 1%、10%、30%、50%以及 70%的恶意节点发布虚假路径信息，并且在 BGP 环境下也让这些节点发布相同的路径信息. 网络负载采用如下方式计算，统计 60s 时间间隔内各种环境下的网络消息的总数，重复 50 次实验，取平均值. 实验结果在图 7 中给出，我们采用 OTD 表示节点的原有可信度，采用 NDT 表示最新一次计算获得的节点可信度，采用 $|NDT-ODT|/ODT$ 衡量节点可信度的变化情况.

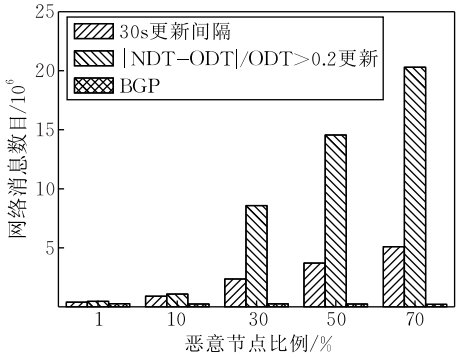
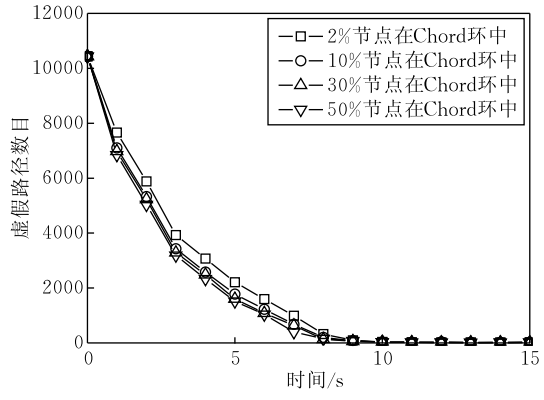


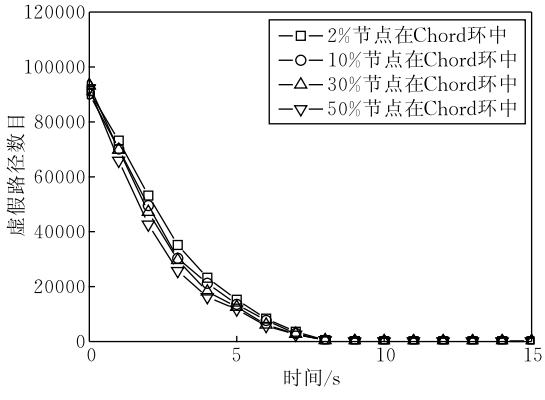
图 7　T-BGP 不同信任信息更新策略时网络负载

通过图 7 可以看到，在两种信任信息更新策略下，当网络中恶意节点数目较少时，T-BGP 的负载都较低；而当网络中出现大规模恶意节点时，采用 30s 定时更新策略时的网络负载比采用节点可信度变化超过 20%立即更新策略时的网络负载小很多，我们分析这是因为定时更新方式下在 30s 间隔内路径更新次数较少. 而在节点可信度变化超过 20%立即更新的情况下路径可信度变化较频繁，路径更新次数较多.

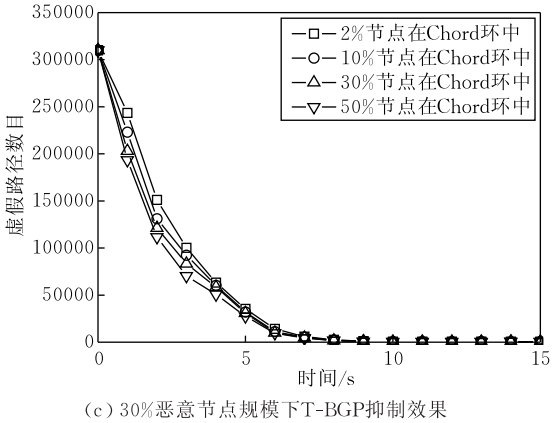
实验 3. 验证不同比例 Chord 环节点数目下 T-BGP 抑制虚假路径的效果. 在定时更新可信度方式下,相比于更新间隔,信任信息发布与查找的时间几乎可以忽略,因此本实验中我们只考虑了节点可信度变化超过 20% 则发布信任更新的策略下的 T-BGP 性能. 我们按照连接度由高至低的方式在网络中分别选取了 2%、10%、30%以及 50%的节点作为 Chord 环节点,随机设定了除 Chord 环节点与虚假路径检测节点外 1%、10%、30%的节点作为恶意节点发布虚假路径信息,分别统计每种情况下 T-BGP 抑制虚假路径的情况. 重复 50 次实验,将 50 次实验的平均值作为实验结果在图8中给出. 图8(a)给出了恶意节点规模为总结点个数的 1%时 T-BGP 的抑制效果,图 8(b)以及图 8(c)分别给出了当恶意节点规模为 10%以及 30%时 T-BGP 抑制虚假路径效果.



(a) 1%恶意节点规模下T-BGP抑制效果



(b) 10%恶意节点规模下T-BGP抑制效果



(c) 30%恶意节点规模下T-BGP抑制效果

图 8 Chord 环节点比例与 T-BGP 有效性关系

通过图 8 我们可以看到,在不同的 Chord 环节点数量下,T-BGP 抑制虚假路径的速度有稍许变化. 随着 Chord 环节点数目的增多,T-BGP 抑制虚假路径的速度稍许加快,然而幅度很小. 我们分析这种情况是因为在 T-BGP 中抑制虚假路径的时间主要由两部分组成:信任信息的传递时间以及网络收敛的时间,其中网络收敛时间占据了绝对大的比例. 虽然 Chord 环节点数目增多后节点发布与获取信任信息的速度加快了,然而其并不会对网络的收敛时间有很大影响.

实验 4. 验证不同最优路径替换策略下的路由的振荡情况. 我们在网络中选取了 10%的节点作为恶意节点,采用了 30s 的信任信息更新间隔,验证了 500s 时间内不同最优路径替换策略下路由的振荡情况. 当两条路径出现连续两次替换对方后,就算做一次路由振荡. 在第 1 种策略中,我们总是选取 $LengthVSTrust$ 值最大的路径,一旦计算出了新的最优路径,立即进行替换;在第 2 种策略中,只有新的最优路径 $LengthVSTrust$ 值比原有路径高出一定比例后才进行替换. 我们采用 OLT 表示当前正在使用最优路径的 $LengthVSTrust$ 值,NLT 表示最近一次计算的最优路径的 $LengthVSTrust$ 值,我们采用 $(NLT-OLT)/OLT$ 作为度量标准,实验仿真了只要 $NLT>OLT$ 就替换、在 $(NLT-OLT)/OLT>0.2$ 时替换以及在 $(NLT-OLT)/OLT>0.5$ 时替换 3 种不同的路径替换策略下的路由振荡情况. 实验结果如图 9 所示.

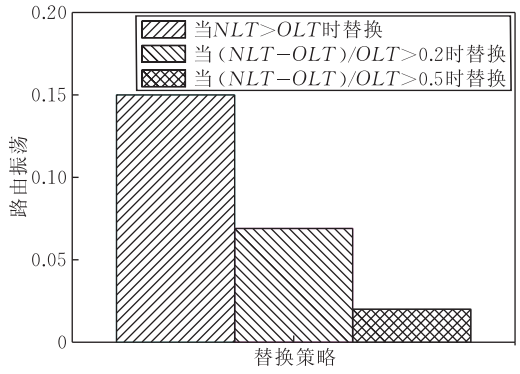


图 9 不同路径更新策略下的路由振荡情况

通过图 9 我们可以看到,在 $|NLT-OLT|/OLT>0.2$ 就更新的条件下,振荡路径比例只在

7%不到，具备较好的可行性. 并且，随着路径替换条件的严格，网络振荡路径的比例显著降低.

实验 5. 验证不同的 T-BGP 部署规模下抑制虚假路径的效果. 我们在网络中部分节点部署 T-BGP，其它节点部署 BGP，验证不同 T-BGP 部署规模下网络中虚假路径的变化情况. 我们采用了 30s 的信任信息更新间隔，随机选择了 1%节点作为恶意节点在网络中发布虚假路径信息，随机选择网络中除虚假节点外的 10%、30%、50%以及 100%的节点部署 T-BGP，其它节点部署 BGP，验证在各种 T-BGP 部署规模下的网络虚假路径情况. 实验结果在图 10 中给出.

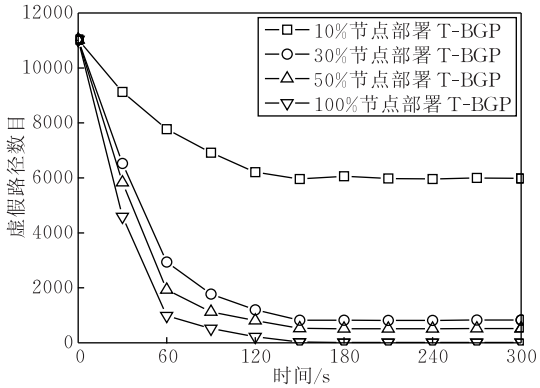


图 10　不同的 T-BGP 部署规模下抑制虚假路径效果

通过图 10 我们可以看到，在各种部署规模下 T-BGP 都能抑制部分虚假路径. 随着部署节点的增多，T-BGP 抑制虚假路径的效果更好. 在网络所有节点都部署 T-BGP 的情况下，网络中残余的虚假路径接近于 0.

7　结论及未来工作

当前域间路由缺乏对路径真实性的判定，可能导致虚假路径大范围传播，带来大规模的网络失效. 为了提高路由抵御虚假路径信息能力，本文提出了基于可信度的域间路由机制. 在该机制下，在网络中构建一个 Chord 环进行信任信息的发布与获取，部署了虚假路径检测措施的 AS 根据检测结果在 Chord 中发布信任信息，没有部署虚假路径检测措施的 AS 从 Chord 环中获取信任信息来计算候选路径的可信度，基于可信度进行路径选择. 实验结果表明了基于可信度的域间路由机制能够抑制虚假路径，具备较好的性能.

在未来的工作中，我们拟结合某些优化理论研究存在多条可信路径时的优化方法，进一步提高基于可信度选路机制的性能.

参　考　文　献

[1] Li Qi, Wu Jian-Ping, Xu Ming-Wei, Xu Ke, Zhang Xin-Wen. GesBGP: A good-enough-security BGP. Chinese Journal of Computers, 2009, 32(3): 506-515(in Chinese)
(李琦，吴建平，徐明伟，徐恪，张新文. 自治系统间的安全路由协议 GesBGP. 计算机学报，2009，32(3)：506-515)

[2] Kent S, Lynn C, Seo K. Secure border gateway protocol. IEEE Journal on Selected Areas in Communications, 2000, 18(4): 582-592

[3] White R. Securing BGP through secure origin BGP. The Internet Protocol Journal, 2003, 6(3): 15-22

[4] Siganos G, Faloutsos M. Analyzing BGP policies: Methodology and tool//Proceedings of the 23rd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2004). Hong Kong, 2004: 1640-1651

[5] Goodell G, Aiello W, Griffin T. Working around BGP: An incremental approach to improving security and accuracy of interdomain routing//Proceedings of the ISOC NDSS 2003. San Diego, 2003: 75-85

[6] Pei D, Lad M, Massey D, Zhang L. Route diagnosis in path vector protocols. Computer Science Department, University of California, Los Angeles, CA: Technical Report TR040039, 2004

[7] Lad M, Massey D, Pei D, Wu Y, Zhang B, Zhang L X. PHAS: A prefix hijack alert system//Proceedings of the 15th USENIX Security Symposium (Security 2006). Vancouver, 2006: 153-166

[8] The RIPE NCC MyASN service. 2008. http://www.ris.ripe.net/myasn.html

[9] Hu Ning, Zou Peng, Zhu Pei-Dong. Reputation-based collaborative management method for inter-domain routing security. Journal of Software, 2010, 21(3): 505-515(in Chinese)
(胡宁，邹鹏，朱培栋. 基于信誉机制的域间路由安全协同管理方法. 软件学报，2010，21(3)：505-515)

[10] Eschenauer L, Gligor V D, Baras J. On trust establishment in mobile ad-hoc networks//Proceedings of the 10th International Security Protocols Workshop. Cambridge, UK, 2002: 47-66

[11] Zouridaki C, Mark B L, Hejmo M, Thomas R K. Hermes: A quantitative trust establishment framssework for reliable data packet delivery in MANETs. Journal of Computer Security, 2007, 15(1): 3-38

[12] Pirzada A A, McDonald C. Establishing trust in pure ad-hoc networks//Proceedings of the 27th Australasian Computer Science Conference (ACSC'04). Dunedin, New Zealand, 2004: 47-54

[13] Luo Jun-Zhou, Han Zhi-Geng, Wang Liang-Min. Trustworghy and controllable network architecture and protocol framework. Chinese Journal of Computers, 2009, 32(3): 391-404(in Chinese)

(罗军舟，韩志耕，王良民. 一种可信可控的网络体系及协议结构. 计算机学报，2009，32(3)：391-404)

[14] Wang Peng, Luo Junzhou, Li Wei, Qu Yansheng. Control information description model and processing mechanism in the trustworthy and controllable network//Proceedings of the IM'09. Long Island, NY, 2009: 398-405

[15] Qu Yansheng, Luo Junzhou, Li Wei, Wang Peng. RCM: A new resource control model based on trustworthy and controllable network architecture//Proceedings of the 2010 IEEE/IFIP Network Operations and Management Symposium (NOMS2010). Osaka, Japan, 2010: 201-208

[16] Stoica I, Morris R, Karger D, Kaashoek M F, Balakrishnan H. Chord: A scalable peer-to-peer lookup service for Internet applications//Proceedings of the ACM SIGCOMM'01. San Diego, CA, 2001

[17] Sentz K. Combination of evidence in dempster-shafer theory. Sandia National Laboratories, Albuquerque, USA: Technical Report SAND2002-0835, 2002

[18] Hu Chun-Hua, Mu Min, Liu Guo-Ping. QoS scheduling based on trust relationship in Web service workflow. Chinese Journal of Computers, 2009, 32(1): 42-53(in Chinese)
(胡春华，吴敏，刘国平. Web 服务工作流中基于信任关系的 QoS 调度. 计算机学报，2009，32(1)：42-53)

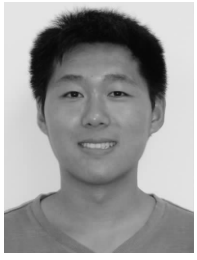
[19] Caesar M, Rexford J. BGP routing policies in ISP networks. IEEE Network Magazine, 2005, 19(6): 5-11

[20] SSF-Scalable Simulation Framework[Z]. [2010-04-23]. http://www.ssfnet.org

[21] Medina A, Lakhina A, Matta I, Byers J. BRITE: An approach to universal topology generation//Proceedings of the MASCOTS. Cincinnati, OH, USA, 2001: 346-353

[22] Gao L. On inferring autonomous system relationships in the Internet. IEEE/ACM Transactions on Networking, 2001, 9(6): 733-745

[23] Lu Xi-Cheng, Zhao Jin-Jing, Zhu Pei-Dong, Dong Pan. Self-organization of inter-domain routing system. Journal of Software, 2006, 17(9): 1922-1932(in Chinese)
(卢锡城，赵金晶，朱培栋，董攀. 域间路由系统自组织特性. 软件学报，2006，17(9)：1922-1932)



TAN Jing, born in 1984, Ph. D. candidate. His research interests include next generation network, routing mechanism.

LUO Jun-Zhou, born in 1960, Ph. D., professor, Ph. D. supervisor. His research interests include next generation network architecture, protocol engineering, network security and management, and grid computing.

LI Wei, born in 1978, Ph. D., lecturer. His research interests include next generation network, network management and service computing.

YU Feng, born in 1974, Ph. D. candidate, lecturer. Her research interests include next generation network and network management.

Background

This work is supported by National Natural Science Foundation of China under grant No. 60903161 and No. 60903162 and No. 90912002, China Specialized Research Fund for the Doctoral Program of Higher Education under grant No. 200802860031, Jiangsu Provincial Natural Science Foundation of China under grant No. BK2008030, National Key Basic Research Program of China under grant No. 2010CB328104, Jiangsu Provincial Key Laboratory of Network and Information Security under grant No. BM2003201 and Key Laboratory of Computer Network and Information Integration of Ministry of Education of China under grant No. 93 K-9.

Improving the security of routing is of great significance to the further development of the Internet. Two common ways to solve this problem are security protection and anomaly detection. Security protection is limited to its high cost and anomaly detection usually cannot be deployed globally because of some reasons such as privacy. This paper proposes to share the detection results of different detecting nodes by trust degree and improve the trustworthiness of routing globally with low cost.

This work is the fundamental work of building Trustworthy and Controllable Network (TCN). TCN is proposed to address the challenges on security and management of the Internet. TCN can reduce the load of routers, simplify the control and management of network and improve its security. In the previous research, the authors have proposed Trustworthy and Controllable Network Architecture, a control information description and processing model and a resource control model for TCN. As the cornerstone of network, improving the trustworthiness of routing is an important step of implementing Trustworthy and Controllable Network. With these issues in mind, a trust degree based inter-domain routing model is presented in this paper to improve the trustworthiness of routing.