计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2016.20151121
53(4):845-860, 2016

一种面向域间路由系统的信任模型

夏 怒 李 伟 陆 悠 蒋 健 单 冯 罗军舟
(东南大学计算机科学与工程学院 南京 211189)
(xia_nu@seu.edu.cn)

A Trust Model for the Inter-Domain Routing System

Xia Nu, Li Wei, Lu You, Jiang Jian, Shan Feng, and Luo Junzhou
(*School of Computer Science & Engineering, Southeast University, Nanjing* 211189)

Abstract In the inter-domain routing system, the running of the border gateway protocol (BGP) is on the assumption that ASes trust each other, and there is lack of effective verification on the validity of the routing information, so the false information publishers have the chance to seriously threaten the security of the inter-domain routing system. However, the existing works can not effectively limit the generation and transmission of the false routing information, so this paper presents a trust model for inter-domain routing system to achieve the trust evaluation on the routing behavior of the ASes. In this model, the evaluator's direct evaluation of the evaluated AS's routing behavior and the evaluated AS's neighbors' direct evaluation, weight value is assigned to different direct evaluation to compute the trust degree of the evaluated AS. A routing announcement behavior prediction method is used to make the direct evaluation result accurately reflect the evaluated AS's future probability of sending true routing information. In addition, in order to promote ASes to join in the trust recommending positively, an incentive mechanism is used, in which every AS evaluates the other ASes' recommendation behavior in history and computes the corresponding recommendation probability for them. The simulation results show that, compared with other trust models for inter-domain routing system, the trust evaluation result of our model is more accurate to reflect the evaluated AS's future probability of sending true routing information.

Key words inter-domain routing system; trust model; trust degree; routing behavior predication; incentive for trust recommendation

---

收稿日期:2015-12-21;**修回日期**:2016-02-03

基金项目:国家自然科学基金项目(61320106007);国家"八六三"高技术研究发展计划基金项目(2013AA013503);江苏省未来网络创新研究院未来网络前瞻性研究项目(BY2013095-2-07);教育部计算机网络与信息集成重点实验室(东南大学)基金项目(93K-9);江苏省网络与信息安全重点实验室基金项目(BM2003201);无线通信技术协同创新中心资助项目;软件新技术与产业化协同创新中心资助项目;住建部科研项目(2015-K6-012)

This work was supported by the National Natural Science Foundation of China (61320106007), the National High Technology Research and Development Program of China (863 program) (2013AA013503), the Prospective Research Project on Future Networks of Jiangsu Future Networks Innovation Institute (BY2013095-2-07), the Project Funded by Key Laboratory of Computer Network and Information Integration (Southeast University) of Ministry of Education of China (93K-9), the Project Funded by Jiangsu Provincial Key Laboratory of Network and Information Security (BM2003201), the Project Funded by Collaborative Innovation Center of Wireless Communication Technology, the Project Funded by Collaborative Innovation Center of Novel Software Technology and Industrialization, and the Project Funded by Ministry of Housing and Urban-Rural Development (2015-K6-012).

摘 要 在域间路由系统中,边界网关协议(border gateway protocol, BGP)的运行基于对自治域路由通告行为的可信假设,给了虚假路由信息发布者可乘之机,导致影响 Internet 稳定运行的安全事件时有发生,然而现有研究工作并不能有效抑制虚假路由信息的产生和传播,因此提出一种面向域间路由系统的信任模型,以实现对自治域路由通告行为准确的可信评估.在该模型中,在每个评估周期,评估自治域对其邻居自治域的历史路由通告行为进行直接评估,同时收集被评估自治域的其他邻居自治域对其的直接评估,最后综合多方来源的直接评估结果计算被评估自治域的信任度.采用路由通告行为预测方法,以使直接评估结果可准确反映被评估自治域的未来路由通告行为,此外,为使评估自治域可获得充分的信任信息以保障信任度评估结果的准确性,采用信任推荐激励机制促进自治域积极参与信任推荐,自治域间相互根据对方的历史信任推荐积极性计算信任推荐概率,并基于该概率进行信任推荐.实验结果表明:相比于其他信任模型,在不同的评估环境中,信任模型的信任评估结果可更为准确地反映被评估自治域未来发布真实路由通告的可能性.

关键词 域间路由系统;信任模型;信任度;路由行为预测;信任推荐激励

中图法分类号 TP391

域间路由系统由众多自治域系统(autonomous system, AS)互联而成,肩负着维护网络可达的重任,是 Internet 稳定运行的基石.在该系统中,自治域间基于边界网关协议(border gateway protocol, BGP)交换路由通告以实现域间路由收敛,BGP 协议的运行基于对自治域路由通告行为的可信假设,然而这种可信假设却导致域间路由系统的稳定运行时常遭受由前缀劫持、错误配置、软件故障等产生的虚假路由信息的干扰[1-2].例如,2005 年 Google 的一个前缀被劫持导致部分用户将近 1 h 无法访问 Google[3],2008 年巴基斯坦电信错误散播 YouTube 的一个前缀导致后者的服务中断 2 h[4],这些安全事件同时也造成了重大的经济损失.为了应对域间路由系统所面临的安全挑战,当前的研究工作主要是从完善路由协议的安全机制以及加强对路由信息的诊断监测这 2 方面展开的.在安全机制方面,常用的解决方案如使用公共密钥设施(public key infrastructure, PKI),通过对自治域与其可发布前缀的绑定[5-7],以限制虚假路由信息的传播,然而,在分布式的域间路由系统内设置集中式的密钥授权管理机构尚缺乏现实可行性.在路由信息诊断监测方面,主要是基于数据层面(前缀是否可达)或控制层面(路由路径是否变化)的行为监测结果分析是否存在虚假前缀等安全威胁[8-10],然而,此类方法实质上是对域间路由通告的有效性进行后验式诊断,并没有对路由通告来源进行风险评估,从而难以有效抑制虚假路由信息的产生和传播.

鉴于信任机制在电子商务和 P2P 等领域[11-13]内遏制实体恶意行为方面的功效,目前信任机制也被逐渐引入到域间路由系统中,以实现对自治域的路由行为如所发布路由通告的前缀真实性等进行信任评估,评估结果可以作为路由决策规避路由风险的有效依据.在文献[14]提出的信任模型中相邻自治域间相互交换自身的路由策略、授权状态等指标,并基于这些指标展开信任评估,所使用的评估方法为对多个归一化的行为指标进行加权平均,然而,在该模型中信任评估所基于的一些行为指标并非来源于评估方的直接监测结果而是由被评估方提供,因此这些指标的可靠性无法得到保障,此外,要求被评估方提供如路由策略等隐私信息的做法缺乏现实可行性.在文献[15]所提出的信任模型中,自治域分别基于其他自治域所发布的路由通告的前缀真实性、所包含路由是否为谷底路由(valley free routing)以及所包含域间链路稳定度来计算相应的有效通告所占比例,随后基于不同的有效通告所占比例,分别评估自治域在不同路由通告行为指标方面的信任度.值得注意的是由于现有的路由行为监测方法并不能完全保障监测结果的准确性,并且由于不同自治系统之间的路由策略受商业关系的约束,有些路由通告可能被路由过滤器(route filter)所屏蔽进而无法被路由监测系统所发现,因此单个自治域仅仅依靠自身路由行为监测所得出的评估结果往往难以准确地反映被评估自治域的路由行为.尽管文献[16]所提出的信任模型在评估自治域信任度时综合考虑多个自治域所提供的信任信息,然而该模型没有采取过滤虚假信任推荐信息的措施,使得当存在虚假信任推荐信息时信任评估的准确性无法得到保障.在文献[17]所提出的信任模型中,域间路由系统被

分割成若干个信任联盟,每个联盟中有一个自治域担任盟主,其他自治域(联盟成员)之间基于 Beta 分布理论相互展开直接评估,针对某一成员,盟主收集联盟其他成员所提供的关于该成员的直接评估,随后过滤掉与直接评估平均值偏离较大的直接评估值,最后取未被过滤的直接评估值的平均值作为该成员的信任度.然而,这种在信任模型中常用的过滤不可靠推荐信任度的方法需要在大多数推荐者为善意的情况下才能保障过滤效果,当在局部范围内恶意推荐者所占比例较大时该信任推荐过滤方法的效能将大打折扣.此外,在该模型中,为实现大范围内信任信息共享需要不同联盟的盟主之间交互所管辖成员的信任信息,这种盟主-成员式的信任模型所带来的问题是:各个独立的自治域并非乐意让其他自治域成为自己的信任代理,因此盟主的选择很难在自治域间展开并最终达成共识;盟主行为难以被监管,若盟主提供虚假信任信息会对域间路由系统的安全性造成严重破坏.还需要指出的是,在被评估自治域路由行为波动较大的情况下,上述信任模型基于加权平均、Beta 分布等方法所得信任评估结果难以准确反映其未来路由行为变化,因此不能有效地为路由决策规避未来路由风险提供支持.此外,由于在现有面向域间路由系统的信任模型中没有采取方法促进自治域积极的参与信任推荐,会导致在自治域出于私利不积极反馈直接评价的情况下,评估者由于无法获取足够的信任信息而无法保障信任度评估结果的准确性,因此,有必要建立促进自治域积极参与信任推荐的激励机制.通过研究面向其他研究领域的激励机制后发现,在基于一次一罚策略的激励机制中[18-19],实体一旦有 1 次不合作行为后其将被迫进入 1 个惩罚期,被惩罚实体需无偿向其他未被惩罚实体提供若干次服务才能脱离惩罚期,并且在该期间内被惩罚实体不能享受其他实体提供的服务,这种激励机制的问题在于没有对实体的历史合作行为进行有效区分,会严重影响长期合作偶尔无法合作的实体的合作积极性.此外,在合作双方初始积极性不高的情况下,2 个实体很有可能由于 1 次同时不合作而双双陷入惩罚期,导致相互不能提供服务而都无法脱离惩罚期即陷入合作僵局.在基于行为阈值的激励机制中[20-21],实体合作行为一旦低于某个阈值将被迫经历 1 个惩罚期,在该惩罚期内被惩罚实体需无偿向其他未被惩罚实体提供若干次服务,并不能享受服务,这种激励机制虽然避免了一次一罚策略对实体合作积极性的影响,但是在这种机制中合作行为高于阈值的实体所受到的奖励相同,会导致实体采取保持合作行为达标(高于阈值)即可的投机策略.此外,这种基于行为阈值的激励机制也存在使实体陷入合作僵局的风险,即当 2 个实体合作行为都低于阈值后将相互不能提供服务.

为实现对自治域路由通告行为进行准确的信任评估,使得评估结果可作为域间路由决策的依据,以有效抑制虚假路由信息的产生和传播,本文提出一种面向域间路由系统的信任模型 TMIRS(trust model for inter-domain routing system),在该模型中,在每个评估周期,评估自治域对其邻居自治域的历史路由通告行为进行直接评估,同时收集被评估自治域的其他邻居自治域对其的直接评估,最后综合多方来源的直接评估结果计算被评估自治域的信任度.本文采用路由通告行为预测方法以使直接评估结果可准确反映被评估自治域的未来路由通告行为.此外,为使评估自治域可获得充分的信任信息以保障信任度评估结果的准确性,本文采用信任推荐激励机制促进自治域积极参与信任推荐,自治域间相互根据对方的历史信任推荐积极性计算信任推荐概率,并基于该概率进行信任推荐,一个自治域历史上向其他自治域信任推荐积极性越高,其从其他自治域获取信任信息的概率就越大,反之亦然.

1　信任模型

在本文的信任模型中,自治域对其邻居自治域的路由通告行为展开信任度评估,在评估时评估方综合考虑自身获取的以及被评估自治域其他邻居所提供的直接评估信息,在有效区分不同来源直接评估值的可靠性的基础上计算被评估自治域的信任度.

在当前的域间路由系统中,恶意攻击、软件故障或配置错误都有可能导致自治域对外发布包含虚假前缀的路由通告,这类通告会快速传播到多个自治域的边界路由器并引发路由表项的变动,最终导致数据流量无法到达自治域所宣称的目的前缀,虚假前缀已经成为当前域间路由系统所面临的最严重威胁.因此,为抑制包含虚假前缀的路由通告的产生,有必要对自治域的路由通告行为进行可信评估,评估结果应能够反映出被评估自治域在未来发布包含真实前缀的路由通告的可信程度.鉴于现有的路由信息诊断和监测研究工作[8-10]在发现前缀劫持行为方面取得了一定的成效,对自治域路由通告行为的

可信评估提供了良好的基础,可以通过现有的路由信息诊断和监测方法验证被评估自治域所发布前缀的真实性.综上所述,本文设计一种面向域间路由系统的信任模型,在该模型中,在每个评估周期,评估自治域基于其自身对被评估自治域路由通告行为的监测结果做出直接评估,考虑到现有的路由行为监测方法并不能完全保障诊断结果的准确性,并且有些路由通告可能被路由过滤器(route filter)所屏蔽进而无法被路由监测系统所发现,会导致单个自治域的直接评估结果难以准确反映被评估自治域的实际路由通告行为,因此评估自治域还需要参考被评估自治域的其他邻居自治域对其的直接评估,为实现不同自治域间信任信息的交互,可以采取如在不同域内设置信任服务器相互交互信任信息,或采取带外连接的方式如管理员之间通过电话和邮件等进行信任信息的交互.在收集到其他自治域的信任推荐信息后,评估自治域对不同来源的直接评估设以相应的权重,最后计算被评估自治域的信任度.由上述可知,在每个评估周期,评估自治域首先需要对被评估自治域做出直接评估:

定义 1. 直接评估 $DT_{i,j}(t)$. $DT_{i,j}(t)$为在第 t 个评估周期自治域 i 对自治域 j 在未来发布满足前缀真实性的路由通告的可信预期,该值是基于自治域 i 自身对自治域 j 的历史路由通告行为监测结果得出的,取值范围为[0,1].

随后,评估自治域综合多方来源的直接评估计算被评估自治域的信任度.

定义 2. 信任度 $CT_{i,j}(t)$. $CT_{i,j}(t)$为在第 t 个评估周期自治域 i 认为自治域 j 在未来发布满足前缀真实性的路由通告的可信程度,该值是自治域 i 综合多方直接评估得出的,取值范围为[0,1].

需要指出的是,在信任度计算时,评估自治域参考的是其他自治域对被评估自治域的直接评估而非信任度,这是因为:信任度可能综合了第三方自治域所提供的直接评估,在第三方直接评估不可靠的情况下,会导致不可靠信任信息的传播和扩散即形成以讹传讹.为有效降低不可靠直接评估对信任度评估的影响,在信任度计算时评估自治域需要对比历史上不同来源的直接评估与被评估自治域的实际路由通告行为的总体偏差程度,根据对比结果对不同来源的直接评估设置相应的权重.本文的信任模型示意图如图 1 所示,当一个自治域 i 对其邻居自治域 j 进行信任度评估时,自治域 i 需要综合考虑 i 对 j 的直接评估以及 j 的其他邻居(k 和 m)对 j 的直接评估,这些评估值通过自治域间信任推荐的方式获取,随后自治域 i 赋予不同来源的直接行为值相应的权重,最后综合多个赋有权重的直接行为值计算被评估自治域 j 的信任度.

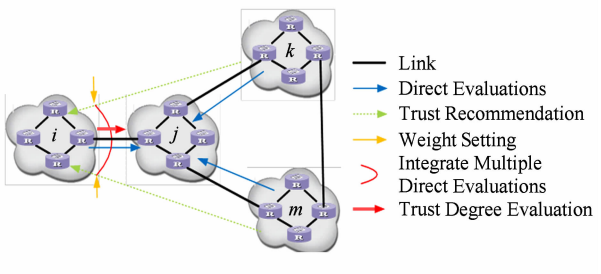


Fig. 1 The diagram of the trust model.

图 1 信任模型示意图

设在第 t 个评估周期,自治域 i 对自治域 j 的信任度计算方法为

$$CT_{i,j}(t)=\sum_{k=1}^{m}(w_k\times DT_{k,j}(t)),\qquad(1)$$

其中,$CT_{i,j}(t)$为自治域 i 对自治域 j 的信任度,$DT_{k,j}(t)$为自治域 k(包括自治域 i)对自治域 j 的直接评估,m 表示在当前评估周期自治域 i 收集到的关于自治域 j 的直接评估的数量($m\geqslant 1$),w_k 为自治域 k 对自治域 j 的直接评估在此次信任度评估中所占的权重.需要指出的是,对于同一个被评估自治域 j,在同一个评估周期,其不同邻居自治域计算得出的信任度是不一样的,原因是:在 1 个评估周期里,由于自治域并非总是积极地参与信任推荐,不同邻居收集到的对自治域 j 的直接评估的来源会有所不同,进而所得信任度会不一样;即便不同邻居收集到的对自治域 j 的直接评估的来源是相同的,但是不同的评估自治域对于同一个由第三方提供的直接评估所设置的权重是不一样的,因为评价第三方直接评价可靠性的指标要基于评估自治域自身对被评估自治域的路由通告行为的验证结果(详见 1.2 节),而不同评估自治域所获的验证结果是不一样的,因此对同一个第三方直接评估设置的权重会不一样,进而所得信任度会有所不同.下面将分别详细介绍信任度计算所需的直接评估以及不同直接信任评价值所对应权重的计算方法.

1.1 直接评估

由定义 1 可知,本文对直接评估的计算是基于对被评估自治域历史路由通告行为的验证结果,如果仅仅以被评估自治域历史上所发布的满足前缀真实性的路由通告的比例作为评估依据,会由于缺乏对不同时期被评估自治域的路由通告行为的分析,

导致评估结果只是反映被评估自治域以往发布满足前缀真实性的路由通告的总体比例,而无法有效反映其未来发布满足前缀真实性的路由通告的可能性.因此,为了有效把握被评估自治域路由通告行为的变化规律,在本文的信任模型中,评估自治域以评估周期为单位来统计对被评估自治域所发布路由通告的前缀真实性的验证结果,进而计算出以评估周期为单位的被评估自治域的路由通告行为指标:路由通告行为值.

定义 3. 路由通告行为值 $AB_{i,j}(t)$. $AB_{i,j}(t)$为在第 t 个评估周期自治域 i 计算得出的自治域 j 在该周期内向其发布满足前缀真实性的路由通告的比例,该值的取值范围为[0,1].

$AB_{i,j}(t)$的计算方法为

$$AB_{i,j}(t)=u/n, \tag{2}$$

其中,n 为在第 t 个评估周期内自治域 i 收到的来自自治域 j 的路由通告数量,u 为满足前缀真实性的路由通告数量.由此可知,经过 t 个评估周期,自治域 i 可获得自治域 j 历史上各个评估周期的行为指标即路由通告行为值 $AB_{i,j}(1),AB_{i,j}(2),\cdots,AB_{i,j}(t)$.值得注意的是,现有的信任模型在计算直接评估时,对历史行为指标往往采用加权平均、贝叶斯算法、Beta 分布等方法,所得评价结果在被评估对象路由行为非平稳变化的情况下难以准确反映其未来路由通告行为状态,导致评价结果不能有效帮助路由决策规避未来的路由风险.因此,在本文的信任模型中,为了使得直接评估结果可准确反映被评估自治域在未来 1 个评估周期内的路由通告行为表现,设当前为第 t 个评估周期,评估自治域 i 基于对被评估自治域 j 未来一个评估周期的路由通告行为值的预测,来计算直接评估 $DT_{i,j}(t)$,有 $DT_{i,j}(t)=AB_{i,j}(t+1)$,$AB_{i,j}(t+1)$为评估自治域 i 基于自治域 j 历史上各个评估周期的路由通告行为值预测出的其在第 $t+1$ 个评估周期的路由通告行为值.由此可知,该直接评估可以有效反映自治域未来路由通告行为,将有助于路由决策规避未来的路由风险.

本文所使用的对自治域路由通告行为值的预测方法基于早先的 1 个在路由行为预测方面的研究成果[22],与现有的 AR 模型、人工神经网络、小波变换、灰色模型相比,该研究成果的优点是:在小样本状态下(样本数量不少于 4 个)即可实施预测、无样本分布要求、不依赖专家经验、在样本数据值波动较大的情况下预测精度更高.设自治域 i 获得的自治域 j 的历史路由通告行为值序列为($AB_{i,j}(1)$,$AB_{i,j}(2),\cdots,AB_{i,j}(t)$),本文在预测路由通告行为值时,所基于的路由行为预测算法定义了 2 种波动类型:1)突发波动,该波动只干扰波动出现时刻的行为值,对后续行为值无影响,具有突发性;2)迁移波动,该波动不仅干扰波动出现那一刻的行为值并会对后续行为值产生一定影响,导致行为曲线发生如水平迁移以及趋势改变等.该预测算法定义了 1 个级比序列,此序列由相邻路由通告行为值的比值构成,表示为($r_1,r_2,\cdots,r_{t-1}$),其中有 $r_u=AB_{i,j}(u+1)/AB_{i,j}(u)$.随后,基于一个分组标准 $|\max(r_i)-\min(r_i)|<v(v=0.2)$ 在路由通告行为值序列($AB_{i,j}(1),AB_{i,j}(2),\cdots,AB_{i,j}(t)$)中找出波动值,进而可以得到 2 个分组:1)平滑分组,包含偏差不超过阈值 v 的相邻路由通告行为值的比值;2)波动分组,包含路由通告行为值序列中出现的所有波动值.进而基于平滑分组,该算法可预测出下一个级比值 r_t.同时,对于波动分组,该算法可实现对未知波动类型的识别即预判 1 个波动属于突发波动还是迁移波动.最后,根据当前周期路由通告行为值所属类型,该算法对下一个周期的路由通告行为值 $AB_{i,j}(t+1)$进行预测:1)如果当前周期路由通告行为值 $AB_{i,j}(t)$是 1 个迁移波动,这意味着该值会影响到未来序列值的变化趋势,即未来路由通告行为值 $AB_{i,j}(t+1)$会随该值发生整体的迁移变化,也意味着未来值与该值的偏差不大,因此 $AB_{i,j}(t+1)$与 $AB_{i,j}(t)$的比值可以通过对平缓分组的灰色预测得出,由于 $AB_{i,j}(t)$已知,可计算出 $AB_{i,j}(t+1)$;2)如果当前周期路由通告行为值 $AB_{i,j}(t)$是 1 个非波动类型,这意味着未来路由通告行为值与该值的偏差不大,因此可以将 $AB_{i,j}(t)$当做迁移波动处理,$AB_{i,j}(t+1)$的计算方法同上;3)如果当前周期路由通告行为值 $AB_{i,j}(t)$是 1 个突发波动,这表明未来路由通告行为值 $AB_{i,j}(t+1)$与该值的偏差较大,为避免在数据较大的波动甚至是接近随机波动的情况下寻找近似随机变化的波动规律,该预测方法转而寻找随时间变化的波动所围绕的基线,而灰色预测恰好具有准确把握时间序列变化趋势的能力,因此在 $AB_{i,j}(t+1)$和 $AB_{i,j}(t)$可能存在较大差异的情况下,将 $AB_{i,j}(t+1)$的计算基于对整个行为序列灰色预测的结果.综上所述,自治域路由通告行为值预测方法的流程如图 2 所示,其中,序列 3 和序列 9 为突出波动值,序列 6 为迁移波动值,其他序列为非波动值.图 2 中从路由通告行为值中将平滑数据(包含

迁移波动值)和波动数据(包含迁移波动值和突发波动值)区分出来构成 2 个序列,然后分别基于这 2 个具有不同特征行为值的序列计算出平滑数据的级比值并对未来级比值($AB_{i,j}(11)/AB_{i,j}(10)$进行预测,同时根据不同类型的波动值之间的变化规律预测出未来行为值 $AB_{i,j}(11)$的波动类型,最后结合当前行为值 $AB_{i,j}(10)$以及预测出的未来行为值 $AB_{i,j}(11)$的类型(非波动、平滑波动、突发波动)对 $AB_{i,j}(10)$的取值进行预测.

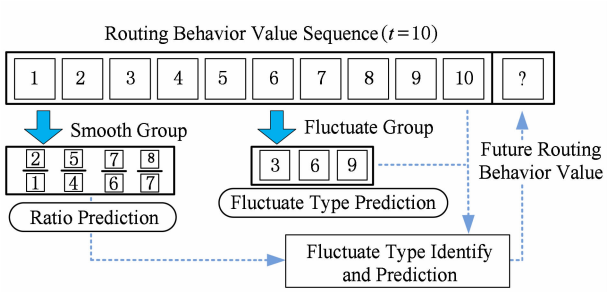


Fig. 2 Prediction method of the routing behavior value.

图 2 路由行为值预测方法示意图

1.2 直接评估的权重设置

设评估自治域 i 获得的被评估自治域 j 的历史路由通告行为值序列为($AB_{i,j}(1)$, $AB_{i,j}(2)$, …, $AB_{i,j}(t)$),由于 $AB_{i,j}(u)$为自治域通过自身监测所得到的自治域 j 在第 u 个评估周期($1<u\leqslant t$)的实际路由通告行为状态,同时由于本文的直接评估结果反映的是被评估自治域 j 未来的路由通告行为,因此 $AB_{i,j}(u)$可以作为 1 个标准,用于自治域 i 衡量在第 $u-1$ 个评估周期里自治域 k(包含自治域 i)所提供的直接评估 $DT_{k,j}(u-1)$对自治域 j 未来路由通告行为的预测准确程度,为了反映自治域 k 历史上所提供的直接评估的总体预测准确程度,自治域 i 首先计算自治域 k 历史上所提供的直接评估与被评估自治域 j 的路由通告行为值的平均偏差 $DevDT_{i,k,j}(t)$.

$$DevDT_{i,k,j}(t)=\frac{1}{n_{k,i,j}}\sum_{u=1}^{n_{k,i,j}}\left|DT_{k,j}(t_u)-AB_{i,j}(t_u+1)\right|, \quad (3)$$

其中,$n_{k,i,j}$为在过去的 t 个评估周期里自治域 k(包含自治域 i)向自治域 i 提供的关于自治域 j 的直接评估的次数,出于策略或开销的考虑,其他自治域不一定会在每个评估周期都向自治域 i 提供关于自治域 j 的直接评估,因此第 u 次($1\leqslant u<t$)信任推荐并不一定与第 u 个信任评估周期相对应,所以使用 t_u 表示第 u 次信任推荐所对应的评估周期,由此可知,在式(3)中 $DT_{k,j}(t_u)$为自治域 k 第 u 次向自治域 i 提供的关于自治域 j 的直接评估,$AB_{i,j}(t_u+1)$为自治域 i 在第 t_u+1 个评估周期计算得出的自治域 j 的路由通告行为值,其中 $t_u<t$. 由此可知,根据平均偏差 $DevDT_{i,k,j}(t)$,自治域 i 可判断自治域 k 所提供的直接评估是否能够准确反映自治域 j 的未来实际路由行为,随后自治域 i 对比不同来源(包括其自身)提供的直接评估所对应的平均偏差. 如果相比于其他自治域,某个自治域提供的直接评估所对应的平均偏差比其他自治域提供的直接评估所对应的平均偏差小,这说明该自治域提供的直接评估可更为准确地反映被评估自治域 j 的未来路由通告行为,因此,在当前对自治域 j 的信任度评估时,评估自治域 i 有理由赋予该自治域所提供的直接评估更高的权重,反之亦然. 由此可知,式(1)中直接评估权重 w_k 的计算方法如下:

$$w_k=\begin{cases}\dfrac{(1-DevDT_{i,k,j}(t))}{\sum_{v=1}^{m}(1-DevDT_{i,v,j}(t))}, \\ \quad \sum_{v=1}^{m}(1-DevDT_{i,v,j}(t))\neq 0, \\ 0,\ \sum_{v=1}^{m}(1-DevDT_{i,v,j}(t))=0.\end{cases} \quad (4)$$

由式(4)可知,如果历史上自治域 k 所提供的关于自治域 j 的直接评估与自治域 j 路由通告行为值的平均偏差相对于其他自治域的更小,则在当前自治域 i 对自治域 j 的信任度评估中自治域 k 所提供的直接评估所占权重更大,反之亦然. 在极端情况下,如果每个自治域的历史直接评估与自治域 j 的路由通告行为值的平均偏差都为 1,这说明参与评估的自治域总是提供与自治域 j 实际路由通告行为相反的评估结果,显然在这种情况下各个自治域所提供的直接评估毫无价值,故权重都设为 0.

1.3 算法描述

基于上述对本文信任模型的介绍,本节给出对信任度评估的算法描述,设评估自治域为 A,被评估自治域为 B,自治域 B 的邻居集合为 $N(B)$,该集合包含自治域 A,$N(B)$中任意 1 个自治域 R 在 A 对 B 信任评估时所提供的直接评估值序列为 $SeqR$,自治域 B 的路由通告行为值序列为 $SeqB$,自治域 A 对自治域 B 的信任度评估算法如下所示:

算法 1. 信任度评估算法.

输入:$N(B)$, $SeqR(R\in N(B))$, $SeqB$;

输出:$CT_{A,B}(t)$.

① $t=1$, $\forall\, SeqR=[]$, $SeqB=[]$;

② 计算路由通告行为值 $AB_{A,B}(t)$,并将其加入到 $SeqB$ 中;
③ if ($t\neq1$) then
④　for each $R\in N(B)$ do
⑤　　计算边路由通告行为值的平均偏差 $DevDT_{A,R,B}(t)$;
⑥　end for
⑦　for each $R\in N(B)$ do
⑧　　计算直接评估权重 w_R;
⑨　end for
⑩ else then
⑪　$\forall w_R=1/|N(B)|$;
⑫ end if
⑬ 计算直接评估值 $DT_{A,B}(t)$,并将该值添加到 $SeqA$ 中;
⑭ for each $R\in N(B)$ && $R\neq A$ do
⑮　收集 R 提供的直接评估值 $DT_{R,B}(t)$,并将该值添加到 $SeqR$ 中;
⑯ end for
⑰ 计算信任度 $CT_{A,B}(t)$;
⑱ t++;
⑲ 转②.

2　信任推荐激励机制

在本文的信任推荐激励机制中,自治域间相互根据对方的历史信任推荐行为计算信任推荐概率,并基于该概率决定是否向对方推荐信任信息即反馈对被评估自治域的直接评估值,自治域参与信任推荐的积极性越高,其从其他自治域获取信任推荐的可能性越大,反之亦然.此外,为保障自治域间的信任推荐不会陷入合作僵局,本文还设置了补偿概率,信任推荐行为不好的自治域可以通过付出较大补偿概率的方式来提升与其他自治域的合作水平,而信任推荐行为较好的自治域只需付出有限的补偿概率来维持合作.

由本文第 1 节可知,评估自治域通过综合考虑多方对评估自治域的直接评价可提高信任度量结果的准确性,然而,在自治域出于私利不积极反馈直接评价的情况下,评估自治域无法获取足够的信任信息,最终使得信任度评估结果的准确性无法得到保障.考虑到现有面向域间路由系统的信任模型中没有采取方法促进自治域积极地参与信任推荐,因此,有必要建立促进自治域积极参与信任推荐的激励机制.同时鉴于现有激励机制所存在的不足,本文提出一种激励机制.在该激励机制中,设当前为第 t 个评估周期,自治域 A 基于自治域 B 对其的历史信任推荐行为设置相应的信任推荐概率 $RP_{A,B}(t)$,有 $0\%\leqslant RP_{A,B}(t)\leqslant100\%$,随后,当 B 向 A 发送信任查询请求时,A 首先判断其资源策略是否允许其对 B 信任推荐,如果不允许则不推荐,否则 A 则以信任推荐概率 $RP_{A,B}(t)$ 向 B 进行信任推荐.本文使用信任推荐有效性来刻画自治域历史信任推荐行为:

定义 4. 信任推荐有效性 $C_{B,A}(t)$. $C_{B,A}(t)$ 为自治域 B 历史上向自治域 A 反馈信任信息的比例,有 $0\%\leqslant C_{B,A}(t)\leqslant100\%$.

$C_{B,A}(t)$ 的计算方法为

$$C_{B,A}(t)=\frac{k_T}{n_T}\times100\%,\tag{5}$$

其中,n_T 为在信任推荐有效性评估窗口(最近 T 个评估周期)中 A 向 B 发送过的信任信息查询请求次数,k_T 为在该评估窗口内 B 向 A 信任推荐的次数.设当前为第 t 个评估周期,在计算出信任推荐概率 $RP_{A,B}(t)$ 后,由上述可知,本文的激励机制基于"多劳多得少劳少得"理念,A 对 B 的信任推荐概率与 B 对 A 的历史信任推荐行为相挂钩:B 对 A 的历史信任推荐合作积极性越高,当 A 在策略资源允许的情况下,B 从 A 获取信任信息的概率就越大,反之亦然.因此,相比于现有的激励机制,本文激励机制的优点是:1)历史信任推荐积极性较高的自治域偶尔几次不推荐,只会一定程度降低其他自治域对其信任推荐的概率,不会如基于一次一罚策略的激励机制那样必然遭受无法获取信任信息的惩罚,而是仍然有较大可能性从其他自治域获取信任信息,然而,随着不推荐次数的增多,其他自治域对其的信任推荐概率会不断下降,最终会使其无法有效从其他自治域获取信任信息;2)自治域是否能够有效地从其他自治域获取信任信息与该自治域的历史信任推荐积极程度有关,而非与某个行为阈值挂钩,因此越积极地参与信任推荐,从其他自治域获取信任信息的可能性就越大,使得自治域不会采取在信任推荐积极性到达一定程度就不加努力的投机策略.本文信任推荐激励机制流程图如图 3 所示.

由图 3 可知,设在第 t 个评估周期,在自治域 A 和自治域 B 相互展开信任推荐之前,自治域 A 需要计算自治域 B 对其的信任推荐有效性 $C_{B,A}(t)$,并依此计算其对其自治域 B 的信任推荐概率 $RP_{A,B}(t)$,自治域 B 也是如此.在 A 收到 B 的信任查询请求

后,A 对 B 的信任推荐概率并不是决定 A 向 B 信任推荐的唯一要素:在 A 受资源策略限制的情况下,即便 A 对 B 的信任推荐概率为百分之百,A 也不能向 B 推荐信任信息. 只有在 A 不受自身资源策略的限制下,A 对 B 的信任推荐概率才能成为左右 A 是否向 B 信任推荐的唯一要素. 下面将介绍信任推荐概率的计算方法.

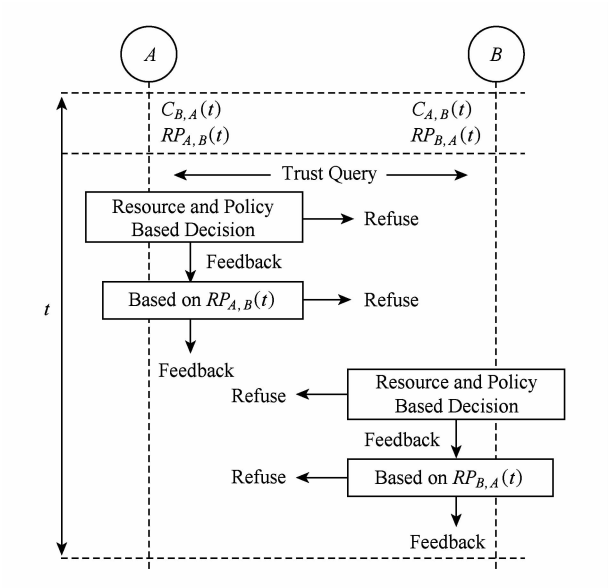


Fig. 3 The trust recommendation incentive mechanism for the inter-domain routing system.

图 3 面向域间路由系统的信任推荐激励机制示意图

2.1 信任推荐概率的计算方法

如果 2 个自治域之前并无信任推荐历史,出于对合作的激励,在本文的激励机制中,初次开展信任推荐的自治域将相互的信任推荐概率设置为 100%,在随后的评估周期再根据对方实际的信任推荐行为(信任推荐有效性)来调整信任推荐概率. 在介绍本文的信任推荐概率的计算方法之前,首先分析 1 个问题:是否可以直接将自治域 B 对自治域 A 的信任推荐有效性作为自治域 A 对自治域 B 的信任推荐概率? 下面通过 1 个实例来讨论上述猜想的可行性,在这个实例中 A 与 B 相互将对方对自己的信任推荐有效性作为自己向对方的信任推荐概率,设 A 与 B 之间相互信任推荐 100 次,并设 A 和 B 的资源策略所允许推荐的概率相同,当 A 和 B 的资源策略所允许信任推荐的概率分别为 90%,50%以及 30%时,分别计算在每次信任推荐时 A 对 B 的信任推荐概率,重复上述测试 100 遍后对每次信任推荐所得信任推荐概率取平均值,测试结果如图 4 所示. 从图 4 可以发现,如果双方仅仅将对方的信任推荐有效性作为计算信任推荐概率的唯一要素,会导致信任推荐合作水平远低于预期,特别是当资源策略所允许推荐的概率较低时,合作水平下降非常快直至趋于不合作状态. 由此可知,不能将自治域 B 对自治域 A 的信任推荐有效性直接作为自治域 A 对自治域 B 的信任推荐概率.

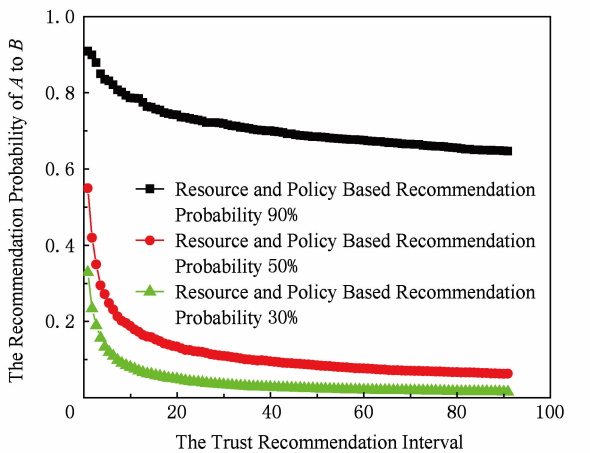


Fig. 4 The change of trust recommendation probability.

图 4 信任推荐概率变化示意图

下面对造成上述问题的原因进行分析,在本文的激励机制中,自治域 A 是否向自治域 B 信任推荐需要 A 首先判断资源策略是否允许信任推荐,如果允许则 A 将基于其对 B 的信任推荐概率决定是否推荐,因此即便 A 与 B 相互的初始信任推荐概率为 100%,但如果双方资源策略允许推荐的概率小于 100%,则当资源策略不允许信任推荐时 A 也不能给予 B 信任推荐,进而随后从 B 的角度来说 A 对其的信任推荐概率将小于 100%,因此 B 也会降低对 A 的信任推荐概率,进而又会导致未来 B 对 A 的信任推荐有效性小于 100%,如此往复,A 和 B 不断降低向对方的信任推荐概率,导致最终 A 与 B 的信任推荐合作水平会远低于预期. 显然,这种当双方都具有较高理论上的合作水平(资源策略允许推荐概率为 90%)却无法达到高水平合作的现象是不合理的. 为解决这个问题,本文设在第 t 个评估周期自治域 A 对自治域 B 的信任推荐概率计算为

$$RP_{A,B}(t)=\min(100\%, C_{B,A}(t)+FC(t)), \quad (6)$$

其中,$C_{B,A}(t)$为 B 对 A 的信任推荐有效性;$FC(t)$为补偿概率,设置该值的目的是为了避免图 4 所示情况的发生:自治域 A 与自治域 B 之间由于一方或双方的历史不合作,导致相互降低向对方信任推荐的概率,最终使得双方都不愿意主动提升合作积极性,导致双方的信任推荐陷入僵局.

2.2　补偿概率的计算方法

补偿概率 $FC(t)$的计算方法为

$$FC(t)=(100\%-SC'_{A,B}(t))\times(100\%-(SC'_{A,B}(t)-C_{A,B}(t))),\quad(7)$$

其中,$C_{A,B}(t)$为 A 对 B 的信任推荐有效性,$SC'_{A,B}(t)$为 A 的理论信任推荐有效性.

定义 5. 理论信任推荐有效性 $SC'_{A,B}(t)$. $SC'_{A,B}(t)$为在第 t 个评估周期自治域 A 计算得出的历史上其资源策略允许向 B 信任推荐的概率,有 $0\%\leqslant SC'_{A,B}(t)\leqslant 100\%$.

$SC'_{A,B}(t)$的计算方法为

$$SC'_{A,B}(t)=\frac{v_T}{m_T}\times 100\%,\quad(8)$$

其中,m_T 为在信任推荐有效性评估窗口(最近 T 个评估周期)中 B 向 A 发送过的信任信息查询请求次数;v_T 为在该期间 A 的资源策略允许其向 B 提供信任推荐的次数;$SC'_{A,B}(t)$体现出 A 在不受 B 的信任推荐行为影响下,即仅受 A 自身资源策略影响下能够达到的合作水平,反映了 A 理论上对 B 的合作水平.下面对补偿概率计算方法的合理性进行说明:

1) 当自治域 A 对自治域 B 的理论信任推荐有效性 $SC'_{A,B}(t)=100\%$时,这表明 A 对 B 的信任推荐不会受到任何资源策略的限制,如果 B 也是百分之百合作,则必然有最终 A 对 B 的信任推荐有效性 $C_{A,B}(t)=SC'_{A,B}(t)=100\%$,而如果实际上 $C_{A,B}(t)<SC'_{A,B}(t)$,这必然是由于 B 在之前采取不合作行为导致 A 也相应地降低了对 B 的信任推荐概率,因此根据式(7)中 $1-SC'_{A,B}(t)$,A 无需给予任何补偿概率.

2) 当自治域 A 对自治域 B 的理论信任推荐有效性 $SC'_{A,B}(t)<100\%$时,A 可基于 $SC'_{A,B}(t)$与 $C_{A,B}(t)$的差值判断其自身合作行为对当前双方合作水平的影响程度,如果 $SC'_{A,B}(t)$与 $C_{A,B}(t)$的差值较大,表明当前 A 与 B 的合作水平远未达到 A 的理论合作水平,因此 A 有理由相信造成当前状况的责任多来自于 B,由式(7)中 $1-(SC'_{A,B}(t)-C_{A,B}(t))$可知,$A$ 需要付出的补偿概率多少与 $SC'_{A,B}(t)$与 $C_{A,B}(t)$的差值成反比,在差值较大的情况下 A 无需给出过多的补偿概率,特别由式(7)中 $1-SC'_{A,B}(t)$可知,当 A 具有较高理论信任推荐有效性时,A 所需付出的补偿概率更少.而如果 $SC'_{A,B}(t)$与 $C_{A,B}(t)$的差值较小,说明目前 A 与 B 合作水平接近 A 的理论合作水平,这里需要分 2 种情况来讨论:①$SC'_{A,B}(t)$较低,由于 A 的理论合作水平不高导致其与 B 的实际合作水平较低但是却没有与 $SC'_{A,B}(t)$有过大差距,这表明是 A 的不合作导致 B 的被动不合作,未来 A 是否能够有效地从 B 获取信任信息完全取决于 A 自身推荐行为的变化,因此 A 如果希望能提升双方的合作水平,应该给予较大的补偿概率;②$SC'_{A,B}(t)$较高,由 $SC'_{A,B}(t)$与 $C_{A,B}(t)$的差值较小可知 B 也具有较高的合作水平,不然当前合作水平肯定要远低于 $SC'_{A,B}(t)$,此时 A 需要通过一定的补偿概率来维持与 B 的高水平合作,否则会出现如图 4 所示的双方理论上合作水平都较高却无法实现高水平合作的状况,然而值得注意的是,与第 1 种情况不同的是,式(7)中 $1-SC'_{A,B}(t)$可降低具有较高理论合作水平的 A 为维护合作所需提供的补偿概率大小.

3) 当自治域 A 对自治域 B 的理论信任推荐有效性 $SC'_{A,B}(t)$趋近于 0%时,不论 B 的理论合作水平多高都会导致 A 与 B 双方的合作趋于完全不合作,因此会有 $C_{A,B}(t)$趋近于 0%,根据式(7)中 $1-SC'_{A,B}(t)$可知,此时 A 的补偿概率趋近于 100%,这表明未来在资源和策略允许 A 推荐时,其应该以 100%的概率推荐信任信息以提升与 B 的合作水平,如果 A 并不采取补偿措施,则 A 和 B 的合作将永远无法开展.

3　实　　验

为验证本文信任模型的有效性,本文分析了 RIS 项目网站[①]提供的位于美国迈阿密的 1 台边界路由器(AS12654)上的路由通告数据,绘制出了以 AS12654 为中心的 1 个局部网络拓扑,如图 5 所示,其中自治域 A 代表 AS12654.

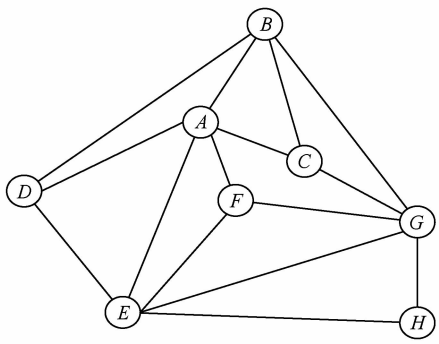


Fig. 5　The network topology of simulation.

图 5　实验网络拓扑

① http://www.ripe.net/data-tools/stats/ris/routing-information-service

鉴于RIS项目所提供的每个边界路由器路由通告数据样本所对应的时间跨度为5 min,因此本文设置1个信任评估周期的时间跨度为5 min.设置实验网络拓扑中每个自治域拥有10个前缀,在每个评估周期,这些自治域都要将自己的前缀宣告出去,随后在此基础上设置相应的发布虚假前缀的行为(见3.1节).需要指出的是,在前缀真实性验证方面,当前研究主要采用的方法是查询地区级互联网路由注册中心(Internet routing registry, IRR)[23]的"网络前缀-来源"对应关系数据库,依此来判断1个前缀是否真实存在且属于相应的自治域,为模拟真实的前缀认证环境,在本文实验中设置1个数据库存放所有自治域与其所拥有的前缀的对应关系,通过查询数据库,实验网络中的自治域 i 可以验证来自其邻居自治域 j 的路由通告前缀真实性即只要没有在数据库中查到相关的前缀与自治域对应关系则认为1条通告不满足前缀真实性.此外,为了模拟实际中自治域在验证路由通告前缀真实性时由于IRR所存信息陈旧或查询请求未得到响应等所造成的验证结果不准确的情况,本实验设1个自治域 i 在1个评估周期内从自治域 j 收到的每个路由通告有10%的概率由于未能得到数据库响应而不将该路由通告纳入到对路由通告行为值的计算中,随后如果对该通告的验证查询可以得到数据库的响应,则再设有10%的概率该通告的前缀因无法验证(模拟IRR所存信息陈旧)而被认为是虚假前缀.由上可知,在每个评估周期自治域 i 可计算出相应的路由通告行为值 $AB_{i,j}(u)=v/n$,其中 n 为在第 u 个评估周期内自治域 j 向自治域 i 发送的路由通告数量(不包括在验证前缀真实性时未能得到数据库响应的路由通告数量),v 为前缀真实性得以验证的路由通告数量.本实验环境为2.0 GHz的P4处理器、2 GB内存、Windows XP平台,使用Java作为开发工具.

3.1 自治域都积极信任推荐时信任模型有效性验证

在这个实验部分不考虑自治域不积极参与信任推荐即不提供直接评估的情况,将实验网络中的自治域 A 作为被评估自治域,当其任意1个邻居自治域如 B 为评估自治域时,A 的其他邻居自治域如 C,D,E,F 则为信任推荐自治域.设置 A 每次在应该宣告自己所拥有的前缀时都有30%的概率将非自己所拥有的前缀宣告出去以模拟前缀劫持行为.鉴于当前面向域间路由系统的信任模型中最常用的评估方法是基于算术平均法或Beta分布,因此本文选取2个信任模型作为比较:1)文献[15]提出的信任模型,简称为AVE,该模型分别计算出各个评估周期满足前缀真实性的路由通告比例,然后对这些比例值取平均值作为直接评估,该模型不采用信任推荐;2)文献[17]提出的信任模型,简称为Beta_Filter,该模型统计历史评估周期中满足前缀真实性的路由通告个数,然后基于Beta分布计算直接评估,此外,该模型采用信任推荐并基于平均值过滤偏离较大的直接评估,最后将未被过滤的直接评估的平均值作为信任度.为了验证不同信任模型的评估效能,在每个评估周期自治域 A 的所有邻居分别采用不同的信任模型计算 A 的信任度,并将信任评估结果与 A 实际的对其不同邻居下一个评估周期的路由通告行为值进行对比以计算评估偏差(取绝对值),进而再计算 A 的多个邻居评估偏差的平均值,将该值作为比较不同信任模型评估效能的指标.还需要指出的是,由于本文所采用的路由通告行为预测方法需要积累4个评估周期的路由通告行为值才能进行预测,因此在本实验中从第5个评估周期开始对不同信任模型的评估效能进行对比.此外,在本实验中信任推荐者被分为诚实推荐者和虚假推荐者,诚实推荐者将自身所获直接评估不做修改地提供给评估者;虚假推荐者又分为长期虚假推荐者和非长期虚假推荐者,长期虚假推荐者在每次信任推荐时都将其实际所获直接评估提高10%~20%后提供给评估者,而非长期虚假推荐者在每次信任推荐时有10%的概率提供高出实际所获直接评估10%~20%的直接评估.下面将在不同的信任评估环境中比较不同信任模型的评估效能.

实验1. 在包含不同比例的诚实推荐者与长期虚假推荐者的环境中信任评估有效性验证.

本实验分析100个数据样本即评估时长为100个周期(每周期间隔5 min),将长期虚假推荐者的个数分别设为0~4个(由实验拓扑可知,以 A 的任意1个邻居作为评估自治域都会存在最多4个信任推荐者),实验结果如图6(a)~(e)所示.其中,不同类型的线对应不同模型所得100个评估偏差的平均值,实线代表TMIRS模型所得平均值,虚线代表AVE模型所得平均值,点划线代表Beta_Filter模型所得平均值.可以看出,由于采用路由通告行为预测方法进行直接评估,TMIRS所得信任评估结果与被评估者路由通告行为值的偏差最小;随着诚实推荐者数量的减少,由于AVE模型没有考虑信任推荐,所以该模型的信任评估偏差不随虚假推荐者数量增加而增大;而对于Beta_Filter模型,由于其基于平均值

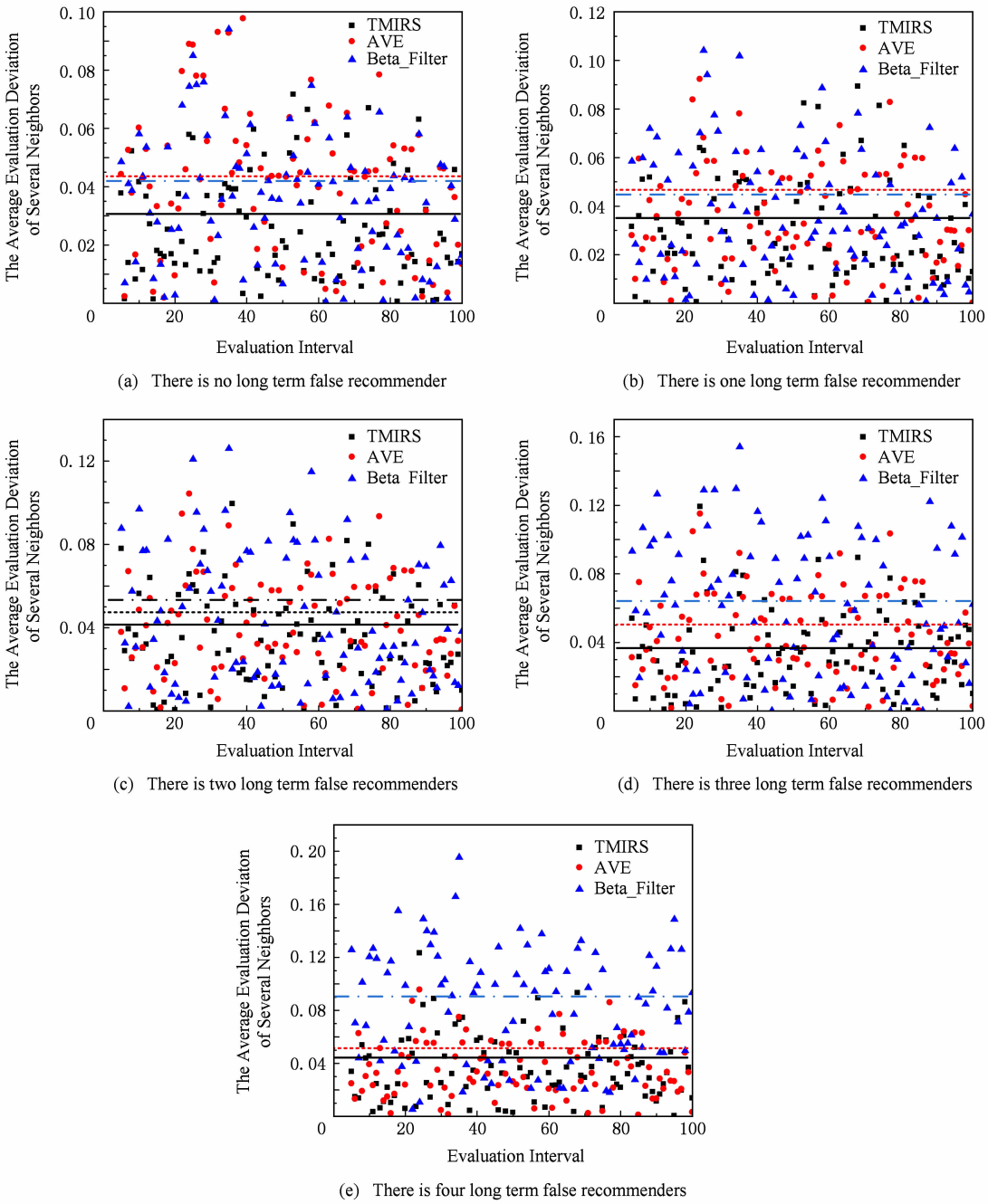


Fig. 6　The trust evaluation comparison on the condition of long-time malice recommenders.

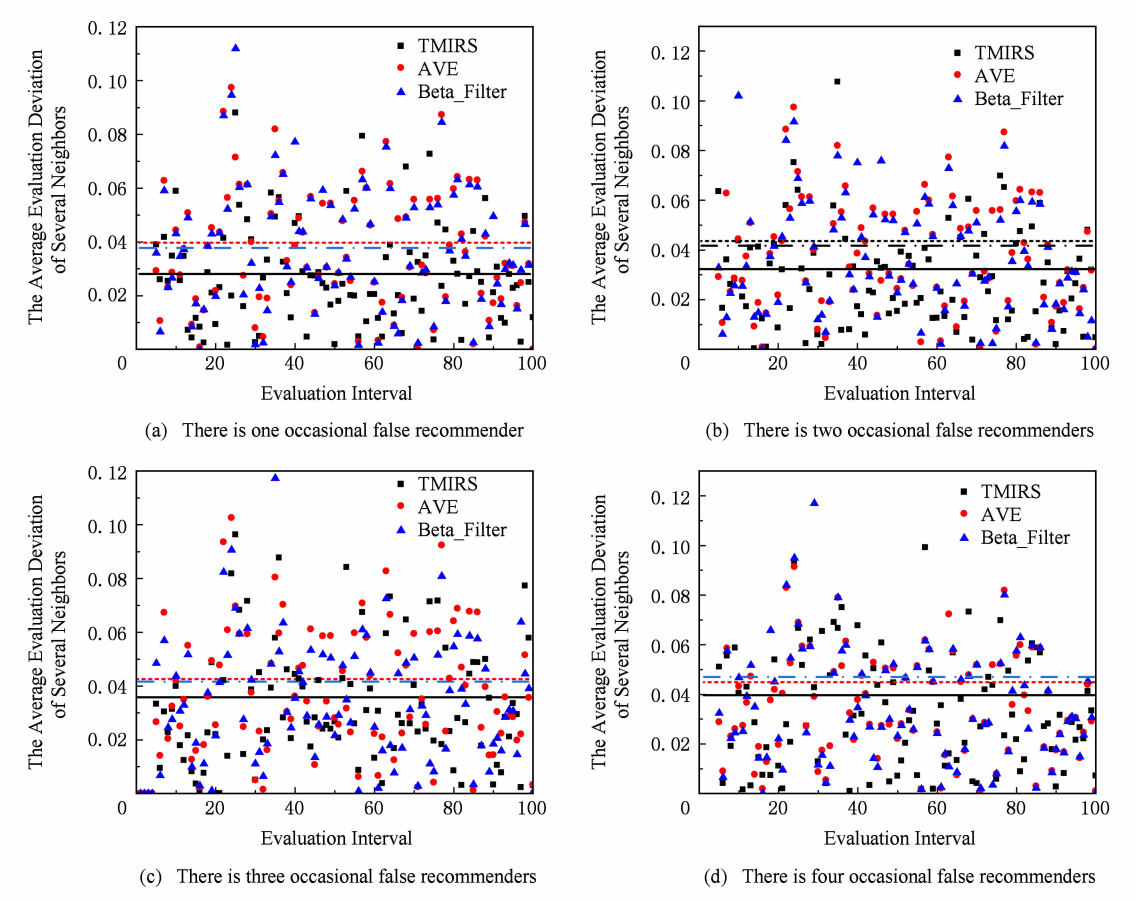
图 6　在包含长期虚假推荐者的环境中信任评估效果比较

过滤偏离较大的直接评估,因此随着虚假推荐者数量的增加,该模型的信任评估偏差逐渐增大.作为比较,随着虚假推荐者数量的增加,本文的信任模型 TMIRS 所得评估结果仍然与被评估者路由通告行为值偏差较小,这是因为 TMIRS 模型基于推荐者过往提供的直接评估与自治域路由通告有效值的整体偏差程度来设置相应的直接评估的权重,可以有效降低持续虚假推荐者所提供直接评估的权重,从而有效限制了长期虚假推荐者对于信任评估的影响力.

实验 2. 在包含不同比例的诚实推荐者与非长期虚假推荐者的环境中信任评估有效性验证.

本实验将非长期虚假推荐者的个数分别设为 1～4,实验结果如图 7(a)～(d)所示.其中,不同类型的线对应不同模型所得 100 个评估偏差的平均值,实线代表 TMIRS 模型所得平均值,虚线代表 AVE 模型所得平均值,点划线代表 Beta_Filter 模型所得平均值.可以看出,由于推荐者偶尔实施虚假推荐,不会导致他们所提供的直接评估权重下降太

多,因此会对 TMIRS 模型的信任评估产生一定影响即在虚假推荐发生时评估值会增大(恶意吹捧),因此 TMIRS 模型所得结果中出现了一些偏差值较大的情况;相比 Beta_Filter 模型,TMIRS 模型遭受的影响相对较小,这是因为该模型基于路由通告行为预测方法进行直接评估,评估者自身所得直接评估结果与被评估自治域的路由通告行为偏差较小,因此评估者会赋予自身所获直接评估较大的权重,进而削弱了其他来源的直接评估对信任度评估的影响程度.



(a) There is one occasional false recommender

(b) There is two occasional false recommenders

(c) There is three occasional false recommenders

(d) There is four occasional false recommenders

Fig. 7 The trust evaluation comparison on the condition of several occasional malice recommenders.

图 7 在包含不同数量的非长期虚假推荐者的环境中信任评估效果比较

3.2 信任推荐激励机制有效性验证

在这个实验部分验证本文所提出的面向域间路由系统的信任推荐激励机制(IMTRGT)的有效性,使用 2 个激励机制作为对比:1)类似文献[20-21]中博弈模型所设置的激励机制 GTIS,设置 1 个阈值 0.6,对于信任推荐有效性低于阈值的自治域将被迫进入惩罚期,在惩罚期中的自治域只能响应其他未被惩罚的推荐者的信任查询而自身不能进行信任查询,直到其信任推荐有效性高于阈值后才可脱离惩罚期;2)类似文献[18-19]中的一次一罚的机制 SEV,在该机制中当 1 个自治域不给予信任推荐后,该自治域将被迫进入惩罚期并同时设置 1 个初始值为 2 的计数值 *count*,在惩罚期中自治域需积极响应其他未被惩罚的推荐者的信任查询而自身不能进行信任查询,完成 1 次信任推荐 *count* 值减 1 直到 *count* 值为 0 后自治域脱离惩罚期. 同样将图 5 所示的实验网络拓扑中的自治域 A 作为被评估自治域,当其任意 1 个邻居自治域如 B 为评估自治域时,其他 A 的邻居自治域如 C,D,E,F 则为信任推荐自治域. 为了验证不同激励机制的效能,计算自治域 A 的所有邻居在每个评估周期能够获取的关于自治域 A 的信任信息数量的平均值,并将该值作为不同激励机制激励效能的对比指标.

实验 1. 自治域信任推荐行为稳定情况下不同激励机制有效性分析.

为模拟整体的信任推荐环境,统一设置自治域资源策略允许信任推荐的概率分别为 90%,80%,60%,30%. 实验结果如图 8 所示. 可以看出,在自治域整体合作水平较高的情况下(90%),在 GTIS 机制下自治域可获得的信任推荐数量最多,这是因为

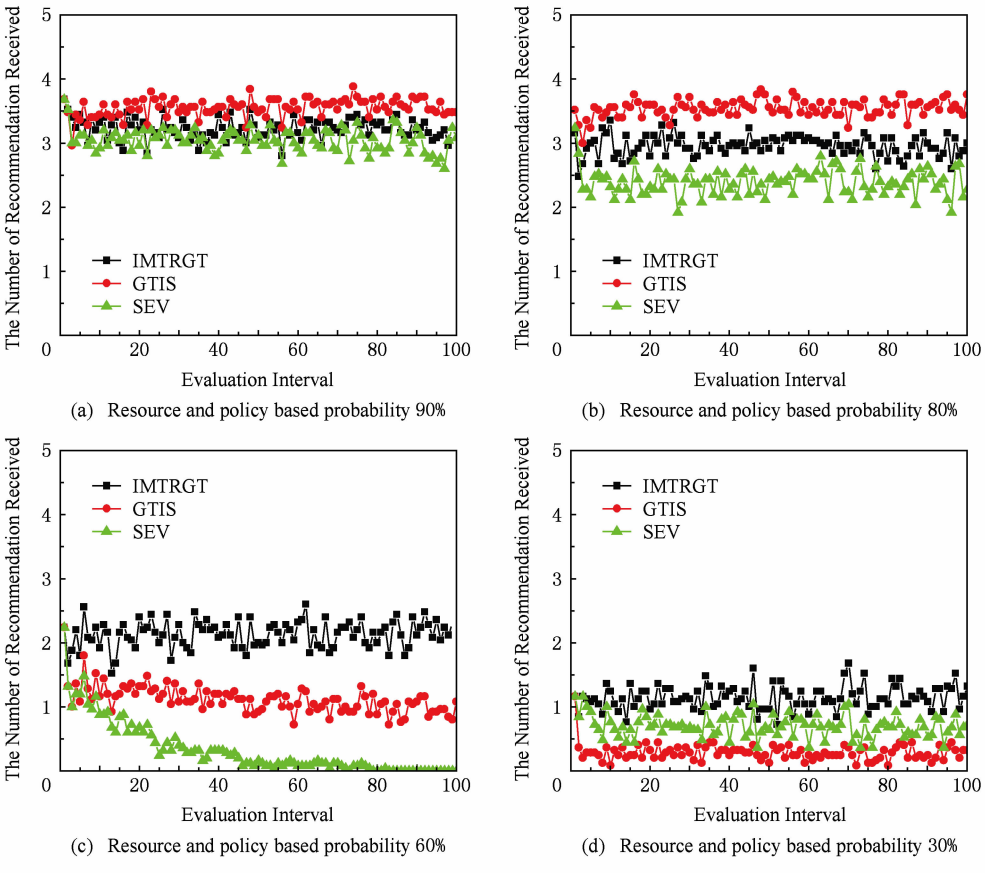


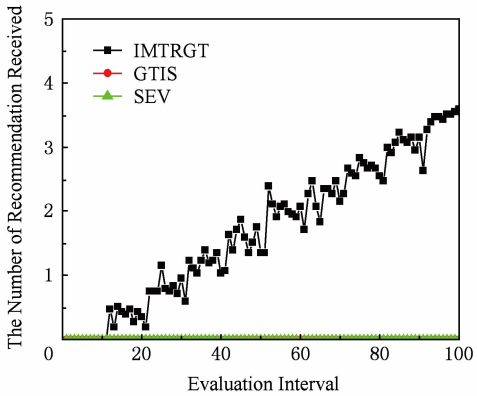
Fig. 8　The incentive mechanism comparison on the condition of the stable ASes behavior.

图 8　自治域信任推荐行为稳定情况下不同激励机制有效性对比

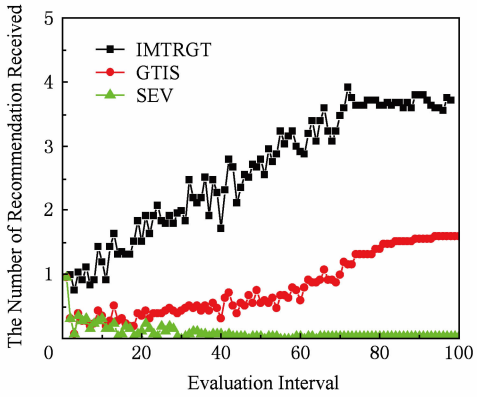
在该机制中如果 1 个自治域 i 对任意 1 个自治域 j 的信任推荐有效性超过阈值,只要 j 的资源策略允许则自治域 j 一定会给予 i 信任推荐;而在 IMTRGT 方法中,自治域 j 还需要基于对 i 的信任推荐率决定是否推荐. 在自治域整体合作水平较低的情况下,IMTRGT 机制中采用补偿概率可有效维持自治域间的信任推荐合作水平,因此自治域仍然可以获得一定数量的信任推荐,而 GTIS 和 SEV 机制没有设置相应的维持合作的方法导致自治域间信任推荐合作水平快速降低. 此外,还值得注意的是,由图 8(a)~(b)可知,在自治域合作水平有所下降(从 90%下降到 80%)的情况下,在 GTIS 机制中自治域可获取的信任推荐数量并没有明显下降,这是因为在该机制中只要 1 个自治域的信任推荐有效性超过阈值则该自治域的信任查询请求必然会得到相应自治域的响应.

实验 2. 自治域信任推荐行为变化情况下不同激励机制有效性分析.

设置所有自治域行为持续变化即资源策略允许信任推荐的概率发生变化,变化函数为 $y=a+b(i-1)$. 其中,a 为资源策略允许信任推荐的概率初始值;i 表示评估周期数,取值范围为[1,100];b 为每周期推荐概率变化值. 设 $a=0\%,30\%$,设 $i=10\%$. 实验结果如图 9(a)~(b)所示,当自治域初始资源策略允许信任推荐的概率为 0%时,在 GTIS 和 SEV 机制中自治域将相互陷入惩罚期即出现合作僵局使得信任推荐过程陷入停滞,而在 IMTRGT 机制中没有惩罚期的概念而是根据自治域的信任推荐有效性计算信任推荐概率来决定是否信任推荐,因此即便初始合作积极性再差的自治域也可以通过不断地改善合作水平(放宽资源策略限制),从而最终能够有效地从其他自治域得到信任信息. 当自治域初始资源策略允许推荐的概率为 30%的情况下,相比在其他激励机制中,在 IMTRGT 机制中自治域所获取信任推荐数量的增长速度更快,而对于 GTIS 和 SEV 机制,由于部分自治域仍然会陷入合作僵局导致相互合作水平无法提升,这说明这 2 个激励机制并不适用于在自治域初始信任推荐合作水平都比较低的环境中使用,而 IMTRGT 机制则不受限于自治域的初始信任推荐合作水平.



(a) The trust recommendation behavior is improving (initial 0%)



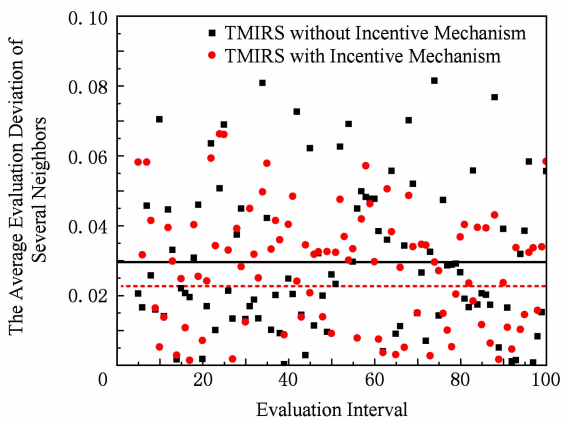
(b) The trust recommendation behavior is improving (initial 30%)

Fig. 9 The incentive mechanism comparison on the condition of the changing ASes behavior.

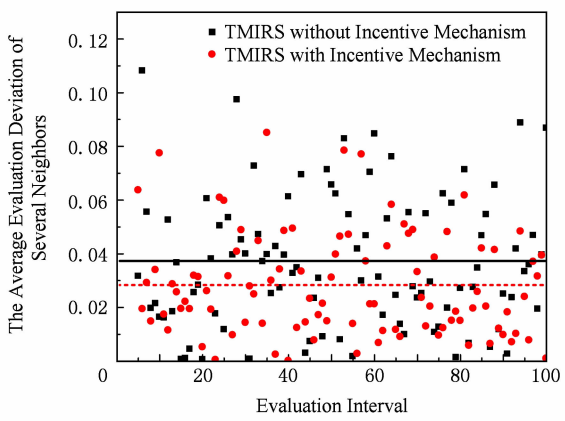
图 9 自治域信任推荐行为变化时不同激励机制有效性对比

3.3 自治域并非总是积极参与信任推荐情况下信任模型有效性验证

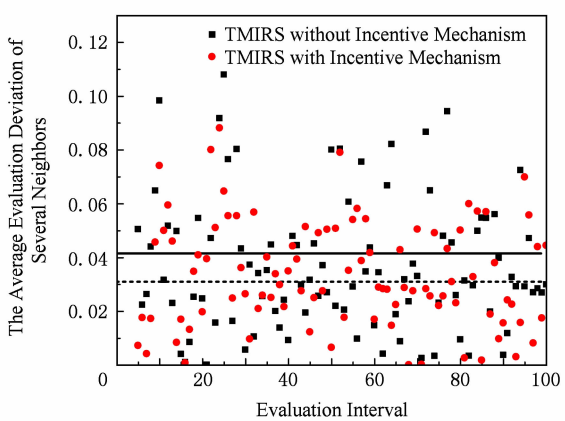
本节在自治域会出于私利不积极参与信任推荐情况下,验证本文所提出的信任推荐激励机制能否有效激励信任推荐以保障信任评估的准确性. 将图 5 所示实验网络拓扑中的自治域 A 作为被评估自治域,当其任意 1 个邻居自治域如 B 为评估自治域时,其他 A 的邻居自治域如 C,D,E,F 则为信任推荐自治域. 在每个评估周期自治域 A 的所有邻居分别采用不同的信任模型计算 A 的信任度,并将信任评估结果与 A 实际的对不同邻居的下一个评估周期的路由通告行为值进行对比以计算评估偏差(取绝对值),进而再计算 A 的多个邻居评估偏差的平均值,将该值作为验证本文信任模型评估效能的指标. 为模拟整体的信任推荐环境,统一设置自治域资源策略允许信任推荐的概率为 80%,随后分别在没有虚假推荐者、有长期虚假推荐者(2 个)、非长期虚假推荐者(2 个)的环境中,对比不使用本文提出的激励机制以及使用该机制的情况下 A 的多个邻居评估偏差的平均值. 实验结果如图 10(a)~(c)所示,其中不同类型的线对应使用或不使用信任推荐激励机制时 TMIRS 模型所得 100 个评估偏差的平均值,实线代表不使用信任推荐激励机制时 TMIRS 模型所得评估偏差的平均值,虚线代表使用信任推荐激励机制时 TMIRS 模型所得评估偏差的平均值.



(a) There is no false recommender



(b) There are two long term false recommenders



(c) There are two occasional false recommenders

Fig. 10 The trust evaluation comparison with incentive mechanism or not.

图 10 使用或不使用信任推荐时信任评估效果比较

可以看出,在不同的信任推荐环境中,如果采用本文提出的信任推荐激励机制,自治域所得信任评估结果与被评估自治域的实际路由通告行为值的偏差将会更小,这说明本文信任推荐激励机制可以有效地激励自治域间相互分享信任信息,从而有助于对被评估自治域做出准确全面的信任评估.

4　结束语

为实现对自治域路由通告行为的准确信任评估,本文提出了一种面向域间路由系统的信任模型TMIRS,在该模型中自治域对其邻居自治域进行信任度评估,信任度的计算基于评估自治域对被评估自治域的直接评估以及其他自治域提供的直接评估.在直接评估中,本文基于路由通告行为预测方法以使信任评估结果有效反映被评估自治域的未来路由行为.为降低不可靠直接评估对信任度评估的影响,对于同一个被评估自治域,本文对比历史上来源于不同自治域的直接评估与被评估自治域路由通告行为的偏差,依据对比结果设置来源于不同自治域的直接评估的权重.此外,为保障评估自治域可以获得足够的信任信息以实现对被评估自治域的准确信任度评估,本文还设置了信任推荐激励机制,自治域间相互根据对方的历史信任推荐积极性计算信任推荐概率,并基于该概率向相应的自治域进行信任推荐.实验结果表明,相比于其他信任模型,在不同的评估环境中,本文信任模型的信任评估结果可更为准确地反映被评估自治域未来发布满足前缀真实性的路由通告的可能性.

参　考　文　献

[1] Lychev R, Goldberg S, Schapira M. BGP security in partial deployment: Is the juice worth the squeeze? [J]. ACM SIGCOMM Computer Communication, 2013, 43(4): 171-182

[2] Butler K, Farley T R, McDaniel P, et al. A survey of BGP security issues and solutions [J]. Proceedings of the IEEE, 2010, 98(1): 100-122

[3] Wan T, Oorschot P C. Analysis of BGP prefix origins during Google's May 2005 outage [C] //Proc of the 20th IEEE Int Paralleland Distributed Processing Symp(IPDPS 2006). Los Alamitos, CA: IEEE Computer Society, 2006: 422-429

[4] Hunter P. Pakistan YouTube block exposes fundamental Internet security weakness: Concern that Pakistani action affected YouTube access elsewhere in world [J]. Computer Fraud & Security, 2008, 28(4): 10-11

[5] Kent S, Lynn C, Mikkelson J, et al. Secure border gateway protocol [J]. IEEE Journal on Selected Areas in Communications, 2000, 18(4): 582-592

[6] Zhang F, Jia L, Basescu C, et al. Mechanized network origin and path authenticity proofs [C] //Proc of the 2014 ACM SIGSAC Conf on Computer and Communications Security. New York: ACM, 2014: 346-357

[7] Lychev R, Goldberg S, Schapira M. BGP security in partial deployment: Is the juice worth the squeeze? [J]. ACM SIGCOMM Computer Communication, 2013, 43(4): 171-182

[8] Shi X, Xiang Y, Wang Z, et al. Detecting prefix hijackings in the Internet with argus [C] //Proc of the 2012 ACM Conf on Internet Measurement. New York: ACM, 2012: 15-28

[9] Zhang Z, Zhang Y, Hu Y C, et al. ISPY: Detecting IP prefix hijacking on my own [J]. IEEE/ACM Trans on Networking, 2010, 18(6): 1815-1828

[10] Hong S, Ju H, Hong J W. Network reachability - based IP prefix hijacking detection [J]. International Journal of Network Management, 2013, 23(1): 1-15

[11] Oscar W X, Cheng W, Mohapatra P, et al. ARTSense: Anonymous reputation and trust in participatory sensing [C] //Proc of IEEE INFOCOM 2013. Piscataway, NJ: IEEE, 2013: 2517-2525

[12] Ghaffarinejad A, Akbari M K. An incentive compatible and distributed reputation mechanism based on context similarity for service oriented systems [J]. Future Generation Computer Systems, 2013, 29(3): 863-875

[13] Grenadier S R, Malenko A, Strebulaev I A. Investment busts, reputation, and the temptation to blend in with the crowd [J]. Journal of Financial Economics, 2014, 111(1): 137-157

[14] He L. A novel scheme on building a trusted IP routing infrastructure [C] //Proc of the Int Conf on Networking and Services(ICNS06). New York: ACM, 2006: 13-18

[15] Chang J, Venkatasubramanian K K, Kannan A G, et al. Ascred: Reputation and alert service for interdomain routing [J]. IEEE Systems Journal, 2013, 7(3): 396-409

[16] Ahmed A, Qian D. Dynamic trust management based on routing system [C] //Proc of the 2nd Int Conf on Computer Technology and Development (ICCTD 2010). New York: ACM, 2010: 333-337

[17] Zhu Peidong, Cao Huayang, Deng Wenping. A systematic approach to evaluating the trustworthiness of the Internet inter-domain routing information [J]. IEICE Trans on Information and Systems, 2012, 95(1): 20-28

[18] Lu Yin, Shi Jin, Xie Li. Repeated-game modeling of cooperation enforcement in wireless ad hoc network [J]. Journal of Software, 2008, 19(3): 755-768 (in Chinese)

(陆音, 石进, 谢立. 基于重复博弈的无线自组网络协作增强模型[J]. 软件学报, 2008, 19(3): 755-768)

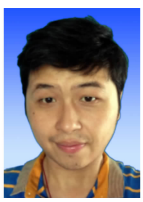
[19] Gui Jinsong, Chen Zhigang, Deng Xiaoheng. A game-based interaction scheme among mobile nodes in wireless access networks [J]. Journal of Computer Research and Development, 2013, 50(12): 2539-2548 (in Chinese)
(桂劲松, 陈志刚, 邓晓衡. 无线接入网中移动节点间基于博弈的交互方案[J]. 计算机研究与发展, 2013, 50(12): 2539-2548)

[20] Guo Yi, Wang Zhenxing, Cheng Dongnian. A game-based incentive strategy for the inter-domain routing collaborative monitor [J]. SCIENTIA SINICA Informationis, 2012, 42(7): 803-814 (in Chinese)
(郭毅, 王振兴, 程东年. 基于博弈的域间路由协同监测激励策略[J]. 中国科学: 信息科学, 2012, 42(7): 803-814)

[21] Xu Z, Yin Y, Wang J, et al. A game-theoretic approach for efficient clustering in wireless sensor networks [J]. International Journal of Hybrid Information Technology, 2014, 7(1): 67-80

[22] Xia Nu, Li Wei, Luo Junzhou, et al. A routing node behavior prediction algorithm based on fluctuation type identification [J]. Chinese Journal of Computers, 2014, 37(2): 326-334 (in Chinese)
(夏怒, 李伟, 罗军舟, 等. 一种基于波动类型识别的路由行为预测算法[J]. 计算机学报, 2014, 37(2): 326-334)

[23] Merit Network. Internet routing registries [EB/OL]. (2010-01-12) [2010-04-15]. http://www.irr.net



Xia Nu, born in 1981. PhD candidate in Southeast University. His research interests include network management.

Li Wei, born in 1978. Associate professor and master supervisor in Southeast University. Member of China Computer Federation. His research interests include next generation network architecture and service computing.

Lu You, born in 1977. PhD candidate in Southeast University. Member of China Computer Federation. His research interests include network management.

Jiang Jian, born in 1986. PhD candidate in Southeast University. His research interests include network management.

Shan Feng, born in 1985. PhD candidate in Southeast University. His research interests include wireless sensor network and algorithm design.

Luo Junzhou, born in 1960. Professor and PhD supervisor in Southeast University. Senior member of China Computer Federation. His research interests include next generation network architecture, protocol engineering, network security, wireless network and cloud computing.