第41卷 第6A期
2014年6月

计 算 机 科 学
Computer Science

Vol. 41 No. 6A
June 2014

基于信任量化的自治系统恶意性判定

王 禹 王振兴 张连成 郭 毅 孔亚洲
(数学工程与先进计算国家重点实验室 郑州 450002)

摘 要 鉴于当前域间路由系统未能有效解决自治系统节点的行为恶意性判定问题,论文在研究人际网络信任关系的基础上,提出一种基于信任量化的自治系统恶意性判定模型。模型通过定义直接判定、协作判定及配合度3项判定准则,综合分析及量化目标自治域的路由交互行为,同时定义节点参与度作为最终判定结果的放大因子。基于仿真路由拓扑进行验证,结果表明,在面对典型的路由欺骗、服务受限及协作节点误报的情况下,该模型均能够有效识别和判定目标自治域节点的恶意行为,具备较好准确性和稳定性。

关键词 域间路由系统,自治系统,信任量化,恶意性判定

中图法分类号 TP393 **文献标识码** A

Decision for Autonomous System Maliciousness Based on Quantitative Trust Measurement

WANG Yu WANG Zhen-xing ZHANG Lian-cheng GUO Yi KONG Ya-zhou
(State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450002, China)

Abstract Decision for Autonomous System maliciousness has not been effectively resolved within the current inter-domain routing system. On the basis of the research on trust relationship via the human society networks, a model of decision for the Autonomous System maliciousness based on the quantitative trust measurement is proposed. Three criteria including direct decision, collaborative decision and degree of coordination are defined, on which the comprehensive analysis and quantization towards the interactive routing behaviors of target Autonomous System, and the degree of participation is also defined as the amplifying factor. Experiments based on simulation topology is launched and the result indicates that, under the typical circumstances of routes spoofing, services restriction and intended incorrect decision by collaborative Autonomous System, the model can effectively discriminate and make reasonable decisions to the target malicious behavior, with good accuracy and stability.

Keywords Inter-domain routing system, Autonomous system, Quantitative trust measurement, Maliciousness decision

1 引言

域间路由系统由多个自治系统(Autonomic System, AS)构成,通过AS间的互联协作完成数据的转发。然而,BGP协议作为域间路由实际标准,出于对可扩展性和灵活性的考虑,对AS内部信息进行了隐藏,从而造成路由信息的真实性难以验证。此外,由于各AS通常隶属于不同管理者(商业结构、大学或政府等),出于竞争关系,AS势必会隐藏其路由策略、网络拓扑及链路带宽等信息以维护其私有利益。利用上述安全缺陷,恶意AS节点能够轻易降低网络服务质量、掩藏域间路由信息或宣告虚假前缀地址,对域间路由系统造成极大安全隐患[1]。因此,判定发现恶意AS成为维护域间路由系统安全运行的一个关键问题。

当前针对域间路由系统安全性的研究主要关注两方面,即如何完善BGP等路由协议的安全机制[2-4],以及如何加强对路由信息的检测与分析[5-7]。在检测评估域间路由节点恶意行为方面,刘欣[8]等人通过研究域间路由系统的层次特性,提出了一个基于BGP异常路由的安全评估模型,用于计算每个实体的路由安全状态。郭毅[9]等人将域间路由系统中的多节点交互抽象为非合作博弈问题,据此提出一种域间路由协同监测激励策略,通过奖惩机制优化系统中AS节点的行为。Shen[10]等人给出了一种基于标签的域间真实源地址验证方法,通过构建AS信任联盟,每对交互的AS利用状态机生成标签,从而对源地址的真实性进行检验。然而,针对单个AS节点的恶意性判定这一重要问题,仍然缺乏成熟有效的方法。

面向域间路由系统,论文提出一种基于信任关系量化的自治系统恶意性判定模型。该模型定义了包含直接判定、协同判定以及配合度在内的多维判定准则,并引入节点参与度作为其放大因子,基于历史交互记录来计算当前目标自治域节点的恶意性程度。仿真实验表明,该模型能够有效判定目标自治系统的多种恶意行为,提高域间路由系统的安全监测能力。由于无需改变现有BGP协议,仅根据节点间的信任关

本文受国家863计划项目(2009AA01A334,2008AA01A323,2008AA01A326)资助。

王 禹(1984—),男,博士生,主要研究方向为域间路由系统安全,E-mail:stonchor@163.com;王振兴(1959—),男,博士,教授,主要研究方向为域间路由系统安全与IPv6;张连成(1982—),男,博士,讲师,主要研究方向为网络与信息安全;郭 毅(1984—),男,博士,讲师,主要研究方向为域间路由系统安全;孔亚洲(1989—),男,研究生,主要研究方向为域间路由系统安全与IPv6。

系和历史行为进行判定，因此模型易于实现与部署。本文第2节在介绍信任关系的基础上，给出AS节点恶意性判定模型的基本构成；第3节针对两个核心问题——判定准则与放大因子的定义及意义进行详细阐述；第4节依照域间路由系统设计仿真拓扑结构，开展试验并分析结果；最后总结全文。

2 域间路由系统AS恶意性判定模型

域间路由系统中对于AS节点的恶意性判定问题，同现实社会中人际关系网络的个体行为评估问题非常相似，主要体现为：

(1)域间路由系统与人际关系网络均属复杂系统，由相对独立而又相互作用的实体构成。域间路由系统的独立实体为AS节点，而人际网络中为自然人，每类个体在维持自身独立性的同时，都不可避免地要与周围个体产生交互。

(2)域间路由系统与人际关系网络中，每类个体的目标基本一致，即从交互活动中充分寻求利益的最优化。对于域间路由系统而言，AS会制订其私有策略，尽可能利用路由选择、流量控制等多种手段实现其收益的最大化。

(3)域间路由系统与人际关系网络均在不断变化，每类个体在挖掘自身发展最优性的同时，也必须充分判断评估与周围个体之间的关系，不断调整对内对外的交互策略。对于AS来说，在寻求利益优化的同时，需要不断评估自身及邻居节点在整个系统中的关系，以期持续发展。

由于人际社会网络中的信任关系是实施个体评估的重要依据，因此，对AS节点的恶意性判定可以充分借鉴并利用信任模型。信任关系本身具备多重特性，主要包括不确定性、非对称性、部分传递性以及时空减性。同时，文献[11]指出，如果不能准确量化两个实体之间的信任关系，则这一关系是不稳定的。因此论文在对节点间信任关系进行量化的基础上，提出一种AS节点恶意性判定方法。

定义1 域间路由系统$G=(V,E)$，V表示自治域节点集合，对于$\forall v_i \in V$，v_i由唯一标识编号表示；E代表自治域之间的链路集合。假设v为域间路由系统中任一待判定节点，v_1^d，v_2^d，…，v_n^d表示多个针对v的判定方节点，则称$D_v=\{v_1^d, v_2^d, \cdots, v_n^d\}$为判定节点集。

定义2 一个判定节点v_i^d对于自治域节点的恶意性判定包含多项衡量标准，假设$T=\{T_1, T_2, \cdots, T_L\}$代表判定准则集合，称$T_i$为一个判定准则(Decision Criteria, DC)。由于每项准则作用不尽相同，令θ_i表示T_i的重要性程度(即权重)，且满足：

$$\sum_{i=1}^{L}\theta_i=1, 0\leqslant\theta_i\leqslant 1 \tag{1}$$

定义3 若域间路由系统对某节点v的恶意性判定包含L项准则，设$E(v_i^d, v)$表示一个判定节点v_i^d对自治域节点v的恶意性判定度，它依据每项判定准则及其对应的权重进行计算，则有：

$$E(v_i^d, v)=\rho \cdot \sum_{k=1}^{L}(T_k \cdot \theta_k) \tag{2}$$

为了准确度量一个自治域节点的恶意性，势必需要引入多个判定准则共同刻画待判定节点的行为恶意程度，这里引入的准则主要涵盖3方面：基于相邻节点信任度量的直接判定、基于非相邻节点信任度量的协作判定以及节点配合度。此外，还引入节点参与度ρ作为放大因子，以期更为充分地体现节点行为。

定义4 节点的恶意性判定结果被划分为m个级别，$R=\{r_1, r_2, \cdots, r_m\}$代表判定级别集合，令$r_i(E)$代表$i$级别对应的恶意性判定值区间。对$\forall r_i \in R$，具有：

$$r_1(E)\cup r_2(E)\cup\cdots\cup r_m(E)=[0,1], r_i(E)\subseteq[0,1] \tag{3}$$

当R中元素满足：当$r_i(E)\cap r_j(E)=\varnothing\ (i\neq j)$，$\overline{r_1(E)}<\overline{r_2(E)}<\cdots<\overline{r_m(E)}$，其中$\overline{r_i(E)}$表示$i$级别对应区间的最大判定值，则称$R$为一个增序集。

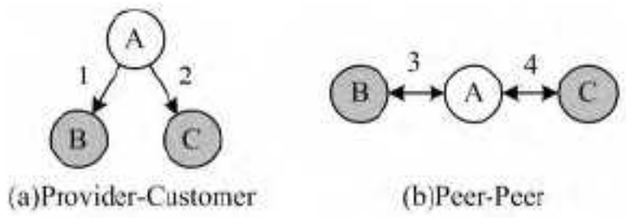
3 判定准则及放大因子

3.1 直接判定

域间路由系统具有显著的层次特性，根据自治域功能和商业关系，可以将其归类为Hub AS、Transit AS以及Stub AS 3种类型。Hub AS作为当今互联网的通信枢纽，处于商业关系的中心层面，是其它自治域的服务提供者(Provider)。Stub AS是指位于路由系统边缘，不具备数据转发能力的自治域，只能作为服务请求方(Customer)。Transit AS是指具有转发能力的非Hub AS，既可以是Provider也可以是Customer。

相邻自治域间的商业关系决定了路由选择策略，AS间关系主要包括Provider-Customer和Peer-Peer。对于前者，Provider自治域为Customer提供网络接入服务，将全部路由发送至Customer；而Customer只将源自本自治域及来自下级Customer的路由发送至Provider。而Peer-Peer中两个自治域为对等关系，将自身及下属Customer路由提供给对方，互相提供网络访问服务。

定义5 根据BGP协议的路由向量机制，直接判定(Direct Decision)是指待判定节点与判定节点在相互邻接、具备Provider-Customer(如图1(a)所示的活动1和2)或Peer-Peer(如图1(b)所示的活动3和4)关系的情况下，根据相互间网络服务请求与服务提供行为，判定方对待判定节点的恶意性判定。



(a)Provider-Customer　　(b)Peer-Peer

图1 相邻节点间的直接判定

若待判定节点v与判定节点v_i^d在最近k次服务交互中，设v_i^d对v的直接恶意性判定的历史记录集合$R=\{r^1, r^2, \cdots, r^k\}$，$r^i \in [0,1]$。$R$中各个判定值依照从$t_1$到$t_k$的时间次序进行排列，即$r^k$代表最近一次的服务交互判定值$r$。则$v_i^d$对$v$的当前直接判定为：

$$T_1: R(v, v_i^d)=\begin{cases}\sum_{i=1}^{k}(r^i \cdot \beta(i)) \cdot \frac{1}{k}, & k\neq 0\\ 0, & k=0\end{cases} \tag{4}$$

考虑到信任关系所具有的时空减性，以往不同时刻的交互对当前恶意性判定的影响不尽相同，因此引入$\beta(n)$作为刻画该影响的衰减函数，用来提高信任量化的准确度。$\beta(i)$表示i时刻的衰减系数，且$\beta(i)\in[0,1]$。由于时空减性决定了

人们普遍更加信赖近期结果，因此定义衰减函数为：

$$\beta(n-1)=\begin{cases}\beta(n)\cdot(1-\dfrac{1}{n-1}), & 1<n\leqslant k\\ 1, & n=k+1\end{cases} \tag{5}$$

基于时间戳的衰减函数能够更好地针对节点过往交互行为进行判定，一方面反映该判定值随时间的变化而衰减，另一方面利用时间戳能够提高动态判定能力。

3.2 协作判定

仅依靠直接判定，难以全面掌握目标自治域的行为特征。尤其当该节点不与待判定节点 v 相邻，不存在 Provider-Customer 或 Peer-Peer 关系时，根本无法实施直接判定。然而，由于信任关系具备动态的传递性，因此可借助其他可信节点的反馈信息作为参考，制定相应策略进行判定。

定义 6 协作判定是指节点 v_i^d 通过构建并利用协作集 C，根据 C 中节点与待判定节点的直接判定结果，基于信任传递与反馈机制所实施的恶意性判定。设 v_i^d 对应的协作域集合为 $C=\{Col_1,Col_2,\cdots,Col_k\}$，对于其中任一 Col_i，$Col_i\in D_v$ 或 $Col_i\notin D_v$，即 v_i^d 自主选择对应的协作域，协作节点未必来源于判定节点集。则 v_i^d 对 v 的当前协作判定值为：

$$T_2:H(v,v_i^d)=\begin{cases}\sum_{i=1}^{k}(\varphi(Col_i)\cdot T_1(v,Col_i))\cdot\dfrac{1}{k}, & k\neq 0\\ 0, & k=0\end{cases} \tag{6}$$

式中，$T_1(v,Col_i)$ 表示协作集中第 i 个协作节点对 v 的直接判定。如果 v_i^d 不存在协作伙伴，即 $k=0$，则协作判定值为 0；反之，如果 v_i^d 对应的协作域 $C\neq\varnothing$，考虑到协作集中的每个实体同 v 之间存在不同的商业或隶属关系，因此引入 $\varphi(Col_i)$ 作为协作加权函数，增加协作判定的准确性。

以图 2 为例，假定判定节点 v_1^d 构建的协作集 $C=\{C_1,C_2,C_3,C_4\}$，均为待判定节点 v 的相邻节点。其中，具备 Provider-Customer 关系的节点对为 (C_1,v)，(v,C_3) 和 (v,C_4)，保持 Peer-Peer 关系的节点对为 (v,C_2)。由于各个协作节点同 v 的关系不尽相同，这里认为：$C1$ 作为 v 的服务提供者，通常具有管理自治域 v 的职责且熟知 v 的路由行为，因此其直接判定结果的置信度最高，用 Class 1 表示，例如设该级别的协作加权函数 $\varphi(C_1)=0.9$；$C2$ 作为 v 的对等节点，二者交互较为频繁且往往具有相似的路由策略，因此其判定结果的置信度次高，用 Class 2 表示；由于 $C3$ 和 $C4$ 均为 v 的服务请求者，缺乏对自治域 v 的监测能力，因此较前两个等级更次之，值得注意的是，由于 $C3$ 同 v_1^d 之间为 Provider-Customer 关系，因此将 $C3$ 裁定为 Class 3，$C4$ 为 Class 4。类似地，判定节点 v_2^d 也可以构建自己的协作集对 v 进行判定，并根据自身情况，对集合中的不同协作节点赋予不同的加权函数。

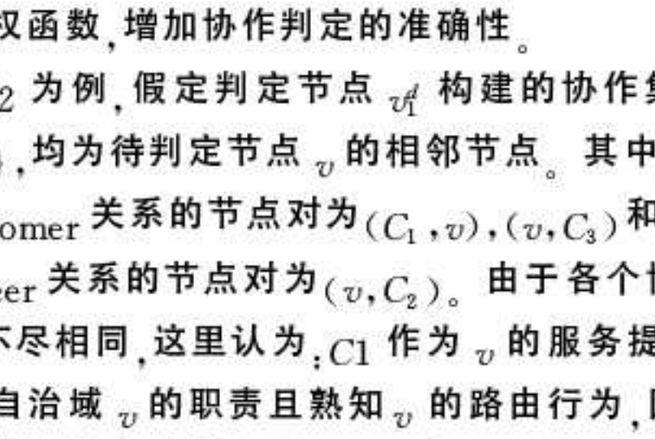


图 2 协作判定节点的分级

3.3 配合度

定义 7 待判定 AS 节点的配合度 $S(v)$ 是指，在整个域间路由系统中有效的 AS 交互记录里，该节点同其他节点之间正常完成通信交互的比率。令

$$T_3:S(v)=\frac{\sum_{i=1}^{n}s(v,v_i^d)}{W} \tag{7}$$

式中，函数 $s(v,v_i^d)$ 表示待判定节点 v 与系统中另一节点 v_i^d 正常交互的次数，n 为域间路由系统中 AS 总数，W 代表该系统中同 v 进行通信交互的历史记录数目。

配合度能够反映待判定节点在整个域间路由系统中参与路由通信的合作程度。可以推知，恶意 AS 节点通常会利用多种方式破坏通信的完整性，包括拒绝通信请求、提供次等路由选择或有意篡改路由信息，从而导致通信活动未能正常完成。根据配合度这一统计信息，配合度较低的节点意味着它很可能是一个恶意节点。

3.4 参与度

定义 8 待判定节点 v 之于判定节点集 $D_v=\{v_1^d,v_2^d,\cdots,v_n^d\}$ 的参与度，体现 v 与 D_v 集合节点在近一段时间内进行通信交互的活跃程度。首先对于 $v_i^d\in D_v$，其 v 之于 v_i^d 的参与度为：

$$P(v,v_i^d)=\frac{\sum_{k=w-m}^{w}(t_{k+1}-t_k)/m}{\sum_{k=1}^{w}(t_{k+1}-t_k)/w} \tag{8}$$

假设节点 v 与 v_i^d 之间共进行过 w 次通信，$(t_{k+1}-t_k)$ 表示相邻两次交互的时间间隔，则式(8)分母部分代表了双方平均交互时间间隔，分子代表了最近 m 次交互的平均时间间隔。由于信任关系具有一定的时间衰减效应，因此 $P(v,v_i^d)$ 能够体现节点 v 参与域间路由活动的阶段活跃性。在此基础上，定义全局参与度，即 v 之于判定节点集 D_v 的参与度，作为最终恶意性判定的放大因子。

$$\rho:P(v)=\frac{\sum_{n}P(v,v_i^d)}{n} \tag{9}$$

如式(9)所示，全局参与度综合了 v 同所有判定个体之间的参与情况，充分体现了待判定节点同其他节点间的通信交互频率，频率越高，表明待判定 AS 节点对域间路由行为参与的程度越高。节点参与度本身并不能表征其行为的善恶与否，但协助上述判定准则能够更好地放大并体现节点近期行为。

4 仿真试验与结果分析

为了验证论文所提方法的有效性，我们通过简化域间路由系统，设计了一个近似于真实应用的仿真拓扑，并以此为基础进行仿真实验。我们设计的拓扑不涉及具体 AS 号等信息。

4.1 拓扑构成与实验设计

域间路由系统仿真拓扑如图 3 所示，相邻自治域节点间的商业关系已用不同箭头标识。其中相互信赖的自治域组成判定节点集 $D=\{v_1^d,v_2^d,v_3^d,v_4^d\}$，待判定自治域节点分别为 v 和 v'。假定拓扑中每对相邻节点间均进行 20 次交互，包括路由通告、路由更新以及数据传输。仿真实验中，设置 3 项判定准则的相应权重为 $[\theta_1,\theta_2,\theta_3]=[0.35,0.5,0.15]$。简单起

见，将节点间的交互频率设为一致，即节点参与度均相同。

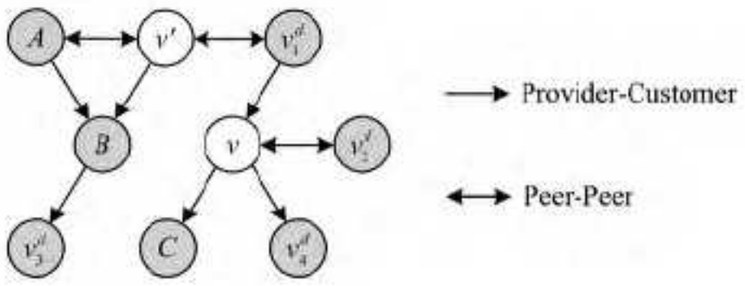


图 3　域间路由系统仿真拓扑

仿真实验包含 3 组恶意性判定：(1) v_1^d 对节点 v' 进行判定，v_1^d 选择的协作集合为 $C1=\{B\}$；(2) v_4^d 对节点 v 进行判定，v_4^d 选择的协作集合为 $C2=\{v_1^d, v_2^d, C\}$，各协作节点对应的权值分配为 $\varphi(v_1^d)=0.9$，$\varphi(v_2^d)=0.8$ 和 $\varphi(C)=0.5$。(3) v_3^d 对节点 v' 进行判定，由于二者并不相邻，v_3^d 只能利用协作判定、参与度及配合度进行计算，v_3^d 选择的协作集合为 $C3=\{v_1^d, A, B\}$，各协作节点的权值分配为 $\varphi(v_1^d)=\varphi(A)=0.8$ 和 $\varphi(B)=0.5$。

待判定节点及协作节点的行为设置方面：(1) 令 v' 是正常节点，无任何恶意行为。(2) 由于节点 A 与 v' 为 Peer-Peer 关系，假设二者均想争取节点 B 为其用户，A 出于其私有目的，在第 5 至 10 次交互中，作为协作节点，持续地向 v_3^d 提供虚假信任度量值。(3) 令 v 为恶意节点，在其与节点 v_1^d 进行的第 4 至 8 次交互中，v 有意降低了用户通信带宽，之后恢复正常服务；节点 v 作为 C 的 Provider，在最后的 5 次交互中，向节点 C 提供错误路由信息，导致其数据通信无法正常进行。

域间路由系统中，鉴于 BGP 协议下自治域对于路由信息的隐蔽，邻居节点行为的真实性和可靠性难以验证，因此在短时间内直接判定方法其实具有很大的局限性。相应地，利用协作节点从多个信任来源评价目标自治域，能够更为充分地掌握其行为特征。配合度是从全局的角度出发，综合考察目标节点的历史行为，藉此反映该节点的可信程度。参与度表征了节点近期内进行通信交互的活跃程度，具有对上述判定结果的放大效应，有助于最终的识别与分析。

4.2　恶意性判定结果分析

基于上述仿真拓扑和节点行为设定，图 4 给出 3 组恶意性判定的结果。其中，3 条曲线 MD1、MD2 与 MD3 分别代表了 v_1^d 对 v'、v_4^d 对 v 以及 v_3^d 对 v' 的恶意性判定，d 表示对应于各个时刻的节点恶意程度(degree of maliciousness)。

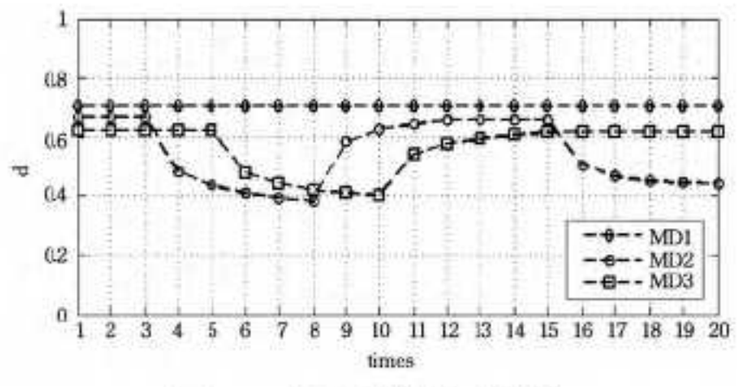


图 4　3 组恶意性判定曲线

针对第一组判定，v_1^d 对 v' 的评估过程中涉及到二者间的直接判定、单一协作节点 B 对 v' 的协作判定以及配合度。由于 v' 没有实施任何恶意行为，因此，如 MD1 所示，v_1^d 对 v' 的判定结果始终未有变化。相比于后两组判定，因为 v_1^d 的协作判定节点只有 B，且 B 给出的评判值持续较高，所以 MD1 的 d 值要略大于 MD2 和 MD3 的最大值。

针对第二组判定，由于待判定节点 v 在与 v_1^d 进行的第 4 至 8 次交互中，有意降低了通信带宽，因此严重影响了对 v_1^d 的服务质量，导致 v_1^d 对 v 的直接判定急剧下降，该阶段 MD2 曲线的 d 值出现了明显降低。待 v 恢复正常服务后，判定结果才逐步回升。值得注意的是，由于出现过此历史事件，v_1^d 对 v 的恶意性判定值要略低于交互之初。最后 5 次交互中，由于 v 向节点 C 宣告了错误路由，导致其无法正常通信，因而 C 作为 v_1^d 的协作节点给予了极低的协作判定值，同时 v 的配合度下降。

并且，对比第二组判定中 4—8 阶段与 16—20 阶段的恶意性判定曲线，可以推知，由于 v_1^d 对 v 的直接判定权值($\theta_1=0.35$)大于 C 作为最低级别协作节点的协作判定权值($\theta_2 \cdot \varphi(C)=0.25$)，因此在赋予相同服务交互判定值 r 的情况下，v_1^d 对最终判定结果 d 值的影响要略大于 C。如 MD2 所示，4—8 阶段的最小判定值 d 要低于 16—20 阶段。

针对第三组判定，由于节点 A 在第 5 至 10 次交互中，持续向 v_3^d 提供虚假的信任度量值，因此该点产生的协作判定值要远远小于正常值。如 MD3 所示，d 值在该阶段出现了显著下降。待节点 A 不再恶意误报，v_3^d 对 v' 的判定结果才逐步回升。类似地，恶意事件之后的 d 值仍然略低于节点 v_3^d 与 v' 交互之初。通过比较 MD2 与 MD3 曲线可以发现，前者的最大判定值要高于后者，这是由于 v_3^d 对节点 v' 的判定过程只能依赖于协作集合，缺乏直接判定手段；而基于拓扑结构方面的优势，v_4^d 对 v 能够充分运用 3 种判定准则，在未出现恶意行为时保持了较高的可信度。

借鉴文献[12]对于实体信任程度的分级，我们将 AS 节点的恶意性分为 5 个级别：即 $R=\{$完全不信任，不信任，弱不信任，弱信任，信任$\}$，对应的判定值区间分别为：$[0,0.2]$，$(0.2,0.4]$，$(0.4,0.6]$，$(0.6,0.8]$，$(0.8,1]$。由图 4 可知，当待判定节点或协作节点发生短期恶意行为时，其判定结果落入不信任或弱不信任的级别范畴，这一结论符合信任关系中的基本认识。

结束语　当前域间路由系统缺乏对自治域行为真实性的判定，出于自身利益的考虑，部分自治域节点可能会实施恶意的路由行为，影响域间路由系统的正常通信，同时损害其他自治域的利益。为此，论文提出了一种基于信任量化的自治域节点恶意性判定模型，该模型定义了多维判定准则，包括直接判定、协作判定以及节点配合度，并引入节点参与度作为最终判定结果的放大因子。仿真实验表明，面对典型的路由欺骗、限制服务及协作节点误报等恶意行为，该模型均能有效判定目标自治域节点的恶意行为，为自治域后期决策提供准确依据。

参 考 文 献

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

[2] 王娜，智英建，张建辉，等. 一个基于身份的安全域间路由协议[J]. 软件学报，2009，20(12)：3223-3239

[3] Oorschot P C, Wan T, Kranakis E. On interdomain routing security and pretty secure BGP (psBGP)[J]. ACM Transactions on Information and System Security (TISSEC), 2007, 10(3): 11-25

(下转第 368 页)

(4) 正确性证明

因为 $(s+h(r))^2Y=t^2x^{-2}Y=t^2G$，所以 $r_2=r_1$，$M'=(r_2+r) \bmod n=m'$，$M=m$，$e'=e$，因此 $e'=h((M'-r) \bmod n, M) \bmod n=h(r_1,m) \bmod n=e$。

6 安全性及效率分析

6.1 对抗从公钥中求出私钥 x 的攻击

攻击者从方程 $Y=x^2G$ 中求解 x，由引理 2 知其难度相当于因子分解和求解离散对数问题。

6.2 对抗从签名中求出密钥 x 的攻击

签名方程 $s=(tx^{-1}-h(r)) \bmod n$ 中有两个变量 x，t，故无法求出密钥 x。

6.3 对抗伪造签名攻击

任取整数 $t(1<t<n)$，虽可计算出 $R=t^2G$，r_1，e，m'，r，但因不知私钥 x，不能计算出 s，攻击不成功。

6.4 对抗具有计算椭圆曲线离散对数问题能力的攻击

假设攻击者具有计算离散对数问题的能力，则可由 $Y=x^2G$ 计算出 x^2，而由 $x^2 \bmod n$ 求解 x 相当于求解 n 的因子分解[7]，故无法求出 x，同理无法求出随机数 t，则由方程 $s=(tx^{-1}-h(r)) \bmod n$ 无法求出签名 s。

6.5 对抗具有计算因子分解问题的攻击

假设攻击者具有计算因子分解的能力，若想由式 $Y=x^2G$ 计算私钥 x，需要首先解决离散对数问题求出 x^2，然后才能利用因子分解计算 x；另外，攻击者想伪造签名也无法成功，假设攻击者任取消息 m，随机选取 t，可计算出 $R=t^2G$，r_1，e，m'，r，但若要计算 $s=(tx^{-1}-h(r)) \bmod n$，仍需 x。

6.6 随机数 t 同态攻击分析

假设签名者使用了 3 个随机数 t_1,t_2,t_3 分别对消息 m_1，m_2,m_3 进行签名，其中随机数 t_1,t_2,t_3 满足 $t_3=(t_1+t_2) \bmod n$，签名分别为 (r_1,s_1)、(r_2,s_2)、(r_3,s_3)，对应签名方程列成方程组为：

$$\begin{cases} s_1=(t_1x^{-1}-h(r_1)) \bmod n \\ s_2=(t_2x^{-1}-h(r_2)) \bmod n \\ s_3=((t_1+t_2)x^{-1}-h(r_3)) \bmod n \end{cases}$$

可计算出 x^{-1}，故方案不能抵抗随机数 t 同态攻击，参数 t 的选取需保持随机性。

6.7 效率分析

利用椭圆曲线因子分解双难题设计消息恢复数字签名方案的相关研究较少。与最新的利用椭圆曲线单难题设计消息恢复数字签名的方案比较，本文方案的运算效率和签名长度亦达到最优，见表 2。

表 2 3 种方案比较

	阚元平方案[9]		周克元方案[10]		本文方案	
	签名	验证	签名	验证	签名	验证
模乘	1	2	1	1	1	1
模逆	0	0	0	0	0	0
点积	1	0	2	1	2	1
Hash 运算	1	1	1	1	1	1
签名长度	3|n|		5|n|		2|n|	
数学难题	椭圆曲线		椭圆曲线		椭圆曲线、因子分解	

结束语 对沈群提出的基于椭圆曲线离散对数和因子分解双难题的数字签名方案进行了分析，指出了错误，进行了攻击分析。给出了一个新的签名方案，证明了其正确性和安全性，并与已有方案进行了比较。另给出一个基于椭圆曲线离散对数和因子分解双难题的消息恢复数字签名方案，证明了其正确性和安全性，并与已有方案进行了比较。

参 考 文 献

[1] Harn L. Public-key Cryptosystem Design Based on Factoring and Discrete Logarithms[J]. IEEE Proceedings-Computers and Digital Techniques, 1994, 141(3): 193-195

[2] 邵祖华. 基于因数分解和离散对数的数字签名协议[J]. 通信保密, 1998(4): 36-41

[3] 沈忠艳, 于秀源. 一个基于两大难题的数字签名方案[J]. 信息技术, 2004, 28(6): 21-22

[4] Zheng Ming-hui, Cui Guo-hua. New signature scheme based on two cryptographic assumptions[J]. Journal of Southeast University(English Edition), 2007, 23(3): 461-464

[5] Ismail E S, Tahat N M F. The Modified Signature Scheme Based on Factoring and Discrete Logarithms[J]. Information Security Journal: A Global Perspective, 2011, 20: 245-249

[6] 沈群, 陈桢. 同时基于两种数学难题的数字签名方案[J]. 福建电脑, 2008(2): 16, 28

[7] 陈景润. 初等数论(3)[M]. 哈尔滨: 哈尔滨工业大学出版社, 2012: 120-124

[8] 崔哲, 余梅生. 一种改进的 H-K 数字签名方案[J]. 计算机科学, 2005, 32(8): 337-338

[9] 阚元平. 基于椭圆曲线的具有消息恢复特性的签名方案[J]. 计算机工程与科学, 2010, 32(2): 58-59

[10] 周克元. 快速椭圆曲线消息恢复数字签名方案[J]. 西北师范大学学报: 自然科学版, 2013, 49(5): 54-56

(上接第 360 页)

[4] 胡乔林, 孙一品, 苏金树. BAR-BGP: 基于备份通告和恢复转发的可靠域间路由[J]. 计算机研究与发展, 2011, 48(12): 2242-2252

[5] Lad M, Massey D, Pei D, et al. PHAS: a prefix hijack alert system[C]// Proceedings of the 15th USENIX Security Symposium. Vancouver, Canada, 2006: 108-119

[6] Schapira M, Zhu Y, Rexford J. Putting BGP on the right path: A case for next-hop routing[C]// Proceedings of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks. Monterey, CA, USA, 2010: 1-6

[7] RIPE. Ripe's MyASN[EB/OL]. http://www.ris.ripe.net/myasn.html, 2011-05-01/2013-04-22

[8] 刘欣, 王小强, 朱培栋, 等. 互联网域间路由系统安全态势评估[J]. 计算机研究与发展, 2009, 46(10): 1669-1677

[9] 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, 2012, 42(7): 803-814

[10] Shen Y, Bi J, Wu J P, et al. A two-level source address spoofing prevention based on automatic signature and verification mechanism[C]// Proceedings of the IEEE symposium on computers and communications. Tarrytown, NY, USA, 2008: 392-397

[11] Ning H, Peidong Z, Peng Z. Reputation Mechanism for Inter-domain Routing Security Management[C]// Proceedings of the 9th International Conference on Computer and Information Technology. Xiamen, China, 2009: 98-103

[12] 李峰, 申利民, 司亚利, 等. 一种基于实体上下文和时间戳的信任预测模型[J]. 电子与信息学报, 2011, 33(5): 1217-1223