软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2011,22(3):481−494 [doi: 10.3724/SP.J.1001.2011.03734]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

域间路由协同监测中的信息共享机制*

胡 宁+, 朱培栋, 邹 鹏

(国防科学技术大学 计算机学院,湖南 长沙 410073)

Information Sharing Mechanism for Inter-Domain Routing Cooperative Monitoring

HU Ning+, ZHU Pei-Dong, ZOU Peng

(School of Computer, National University of Defense Technology, Changsha 410073, China)

+ Corresponding author: E-mail: ning_hu@163.com

Hu N, **Zhu PD**, **Zou P. Information sharing mechanism for inter-domain routing cooperative monitoring.** ***Journal of Software*, 2011,22(3):481−494.** http://www.jos.org.cn/1000-9825/3734.htm

Abstract: The cooperative routing monitoring constructs a more complete global information view by information sharing among autonomous systems (ASes), which can eliminate the negative impact of the autonomous inter-domain routing system characteristic and improve the route monitoring ability of AS. This paper designs an information sharing mechanism called CoISM that is based on self-organization for the information sharing, which is the essential issue of cooperative route monitoring. CoISM leverages the localization caused by BGP policy to reduce and control the transmit range of information. It also uses information reflection to implement the information active push and builds AS profit on its altruistic information sharing behavior. This mechanism leads to information aggregation, as needed in self-organization, and facilitates cooperation among AS by its incentive. CoISM adopts a distributed architecture and has good expansibility and a lower communication overhead. In addition, it does not modify the BGP protocol, but supports an incremental deployment and can be used in many cross-domain cooperative management applications such as inter-domain routing monitoring, cooperative routing failure analysis, cooperative intrusion detection, and so on.

Key words: inter-domain routing system; route monitoring; information sharing; cooperation; BGP

摘 要: 路由协同监测通过在自治系统之间共享路由监测信息来形成更为完整的全局监测视图,从而克服域间路由系统自治性的制约,提高单个自治系统的路由监测能力.针对路由协同监测的核心问题——监测信息共享,基于自组织思想设计了信息共享机制 CoISM.该机制利用 BGP 路由策略引起的信息局部性对路由监测信息的传播范围进行裁减和控制,在被动查询的基础上增加了信息"反射"行为,利用路由监测信息之间的相关性实现信息的主动推送,将自治系统的利益建立在主动信息共享这一利他行为的基础上.CoISM 能够引导自治系统实现路由监测信息的自组织聚合与按需共享,具有激励性,能够促进自治系统之间的协同.该机制采用分布式体系结构,具有良好的扩展性和较低的通信开销,不需要修改 BGP 协议,支持可渐进部署,适用于域间路由协同监测、路由故障协同分析、协同入侵检测等多种跨域协同管理应用.

关键词: 域间路由系统;路由监测;信息共享;协同;边界网关协议

* 基金项目: 国家自然科学基金(60873214); 国家高技术研究发展计划(863)(2008AA01A325, 2008AA01Z414)
收稿时间: 2009-06-18; 定稿时间: 2009-08-26

中图法分类号: TP393 文献标识码: A

基于 BGP[1]的域间路由系统正面临严峻的安全挑战[2],路由监测是弥补 BGP 安全能力不足的重要方法,其目的在于通过监测 BGP 路由信息和事件来发现和抑制虚假路由行为[3].由于缺乏全局协调组织机构和管理基础设施,集中式跨域路由监测难以实施,而单个自治系统受信息隐藏性和局部自治性的制约,对虚假路由的识别能力不足.域间路由协同监测是指多个具备路由监测能力的自治系统为实现共同的安全管理目标,对 BGP 路由的可信性进行分析和确认以及对虚假路由信息进行收集、分析和通告的过程[4].域间路由协同监测通过在自治系统之间共享路由监测信息来形成更为完整的全局监测视图,从而克服信息隐藏性和局部性的制约,提高单个自治系统对虚假路由信息的识别能力.域间路由协同监测信息共享机制的核心目标在于帮助自治系统解决如何获取和传播路由监测信息的问题.在集中式路由监测系统中,节点之间没有利益冲突,由控制中心调度各节点实现监测信息的获取与传播.在域间路由协同监测中,参与协同的自治系统分属不同的管理机构,没有集中的管理中心,自治系统根据自身的利益和需要,制定获取和传播路由监测信息的策略,这是一种无中心结构环境下的自组织行为,需要由特定的机制来引导[5].

本文基于自组织思想设计了信息共享机制−CoISM.该机制利用 BGP 路由策略引起的信息局部性对路由监测信息的传播范围进行裁减和控制,在被动查询的基础上增加了信息”反射”行为,利用路由监测信息之间的相关性实现信息的主动推送,将自治系统的利益建立在主动信息共享这一利他行为的基础上.CoISM 能够引导自治系统实现路由监测信息的自组织聚合与按需共享,具有激励性,能够促进自治系统之间的协同.整个机制的实现不需要修改 BGP 协议,支持可渐进部署,适用于域间路由协同监测、路由故障协同分析、协同入侵检测等多种跨域协同管理应用.

本文第 1 节讨论相关研究.第 2 节分析问题并给出问题的抽象描述.第 3 节介绍核心思想与算法.第 4 节通过模拟与分析对机制的有效性进行评估和验证.第 5 节讨论部分开放性问题.最后总结全文.

1 相关研究

现有域间路由协同监测研究主要采用两类信息共享模型:集中式信息共享模型和分布式信息共享模型.

集中式信息共享模型通过服务中心收集信息并对外提供信息访问服务.互联网路由注册中心 IRR(Internet Routing Registry)[6]采用集中式信息共享模型,自治系统向中心注册自己的路由策略并利用中心提供的其他自治系统路由策略数据进行路由诊断与调试.许多路由监测项目都将路由监测信息集中保存在指定的服务器并对外提供信息查询服务,例如:RIPENCC 的 MyASN 公共服务[7]、窥镜服务器(looking glasses)[8]以及 Renesys 公司的 GRADUS 商业服务[9]等.集中式信息共享模型依赖可信任第三方,在实际运行中存在局限性:(1) 服务中心的存储和通信开销巨大;(2) 自治系统需要主动搜索海量数据并从中提取对自身有用的信息,增加了处理开销和计算复杂性,没有实现信息按需共享;(3) 信息提供方无法主动选择信息使用方,也无法预知信息使用目的,为避免暴露安全漏洞,信息提供方不保证所提供信息的真实性和准确性[10].

分布式信息共享模型通过自治系统之间相互询问和应答的方式实现信息交换和共享,与集中式信息共享模型相比,分布式信息共享模型更为灵活和高效.文献[11]提出一种多自治系统协同的路由验证思想(IRV),当自治系统收到新的 BGP 路由时,主动向 BGP 路由 AS_PATH 属性中包含的自治系统发出路由验证请求并根据应答结果判断 BGP 路由的真实性,收到路由验证请求的自治系统根据本地网络知识,如:路由策略、网络拓扑等对指定路由的真实性进行判断并返回应答.文献[12]提出一种基于主动询问的 BGP 路由监测方式(DRAQ).自治系统在收到新的 BGP 路由时,主动询问上游节点,以确定 BGP 路由的真实性.文献[13]设计了一种基于投票机制的路由真实性监测方法,自治系统主动选择其他自治系统进行投票,并根据收集到的投票结果评价路由信息的可信性.上述研究都采用主动询问的方式实现信息共享,不依赖第三方机构,信息的提供方和使用方直接交互,保证了信息的实时性与可信性,然而,对于如何选择询问对象这一问题所给出的解决方法在可实施性上存在一定的不足.IRV 和 DRAQ 都选择 AS_PATH 中包含的自治系统作为询问对象,这样的做法存在局限性.首先,要求被

询问的自治系统必须部署 IRV 或者 DRAQ 服务的做法难以被运营商接受;其次,单纯使用 AS_PATH 作为启发信息可能存在监测盲点.例如:AS_PATH 包含的自治系统不具备验证路由真实性的知识或者具备验证路由真实性知识的自治系统没有出现在 AS_PATH 中.

现有研究在路由监测过程中,信息使用方大多通过主动查询获取路由监测信息,而信息提供方在信息共享过程中缺乏主动性,由于信息使用方无法及时感知新信息的产生,使得路由监测信息难以及时发挥作用.另外,路由监测信息在信息提供方和信息使用方之间一对一的传播限制了信息的覆盖范围和传播速度,例如:在文献[14]中,当监测点发现前缀劫持行为时,仅仅通知真实前缀持有者,没有考虑其他可能受到欺骗的自治系统,而路由监测往往希望将某一监测点发现的虚假路由信息尽快通知给所有可能的受害节点.大规模网络环境下如何在多个协同代理之间进行信息共享和数据分发是分布式协同管理的典型问题,文献[15]采用马尔科夫模型来解决共享信息分发的决策问题,文献[16]提出了一种面向大规模团队的信息共享机制.文献[17]使用流言(gossip)机制进行概率可靠传播.上述研究主要考虑在分布式环境下,如果在保持低通信开销的前提下,尽可能扩大信息的有效传播范围,增加信息的传播速度,对如何促进自组织协同和鼓励主动信息共享方面考虑不足.

2 信息共享问题

2.1 问题描述

本文中,路由协同监测包括:(1) 自治系统之间协同验证路由可信性;(2) 主动宣告检测到的虚假路由.由于缺乏全局信息视图和调度中心,路由协同监测面临如下问题:① 如何选择或确定能够验证指定路由可信性的自治系统以及可能受到虚假路由信息影响的自治系统;② 如何在众多自治系统之间发布路由监测信息;③ 如何激励自治系统参与信息共享.本文将上述问题统称为路由协同监测中的信息共享问题.

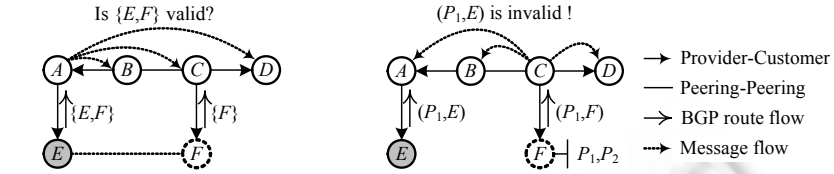
路由可信包括源可信和路径可信,源可信是指路由宣告者所属的自治系统确实是路由前缀的所有者,路径可信是指 BGP 路由 AS_PATH 属性中记录的 AS 序列与路由真实的传播路径一致.在验证路由可信时需要多方面的信息(简称为知识),例如:AS 级别的网络拓扑图,自治系统之间的商业关系,网络流量的跟踪情况等等.由于这些信息的动态变化,或者涉及自治系统的商业秘密,因此难以在全网范围内公开.这使得自治系统往往不知道哪些自治系统具备验证指定路由可信性的知识,而逐个询问又会引起较大的通信开销.另外,为了抑制虚假路由的传播,一旦发现需要及时通知相关自治系统,以防受到路由欺骗.然而,由于 BGP 路由信息的传播是受路由策略控制的,而自治系统的路由策略往往不对外空开,因此难以得知哪些自治系统会受到虚假路由信息的欺骗,而采用泛洪式广播虽然能够保证所有的自治系统感知到虚假路由信息的存在,但是由此引起的广播风暴会对网络性能造成影响.综上所述,路由协同监测中的信息共享机制需要为参与协同的自治系统提供启发信息,提供更为丰富的信息共享模式以及良好的激励机制.

图 1 给出了路由协同监测中的两个典型场景.图 1(a)中,自治系统 A,B,C,D 上部署了路由监测服务(协同路由监测采用渐进式部署,并不要求在所有节点上部署路由监测服务),恶意自治系统 E 向 A 宣告去往 F 的虚假 BGP 路由(该路由并不存在),其 AS_PATH 为 $\{E,F\}$,A 在收到该路由后,可以通过询问其他自治系统来验证该路由的可信性,由于 F 是 C 的客户,C 根据已知的路由策略可知该路由不存在,并告知 A(为了降低规模复杂性,客户自治系统可以委托供应商监测自己的路由和前缀).在图 1(b)中,E 向 A 宣告自己拥有地址前缀 P_1,对 F 进行前缀劫持攻击.同理,当 C 发现这一虚假信息时,将主动通知其他自治系统.

2.2 问题分析

在域间路由环境下,由于 BGP 路由策略和路由监测系统的作用,恶意节点发布的虚假路由并不会被传递到所有的自治系统,本文称这种特性为监测信息局部性.本节根据虚假路由信息对自治系统路由行为的影响,借助免疫学概念将所有自治系统划分为:感染节点、免疫节点与隔离节点.当某恶意节点发布虚假路由信息 R_f 时,能够收到 R_f 但无法识别其为虚假路由的自治系统称为感染节点,能够收到 R_f 且可以识别其为虚假路由的自治系统称为免疫节点,无法收到 R_f 的自治系统称为隔离节点.显然,由于监测信息局部性的存在,当某节点监测到 R_f

时,只需要通知该信息的感染节点.以路由前缀劫持为例,在图 1(b)中,当 E 向 A 宣告去往地址前缀 P_1 的路由时,按照最短路径优先和客户路由优先的原则,A 和 B 会优选 E 的路由作为去往 P_1 的优选路由,此时 A 和 B 成为感染节点.由于 C 知道 F 是 P_1 的真正拥有者,因此不会受到欺骗,此时 C 是免疫节点.因为 C 不会向 D 宣告错误的去往 P_1 的路由,因此 D 成为隔离节点.



(a) Cooperative routing validation (b) Prefix hijacking announcement

(a) 协同路由验证 (b) 路由劫持宣告

Fig.1 Illustration of cooperative routing monitoring

图 1 路由协同监测示意图

如果两条虚假路由引起的感染节点、免疫节点和隔离节点划分相同,则称这两条虚假路由引起的监测信息具有相关性.通过分析 IRR[6]公开的路由策略可知,现有 ISP 大多在自治系统级别上制定路由策略,对于属于同一自治系统的地址前缀在策略上不加区分.由于恶意路由攻击行为需要利用路由策略上存在的缺陷传播虚假路由信息,因此大多路由攻击行为也是针对自治系统级别设计的.因为自治系统拥有多个地址前缀,一旦某前缀受到攻击,则其他前缀也可能受到同一行为的攻击.利用监测信息的相关性,有助于构造虚假路由信息的感染节点集合.例如,在图 1(b)中,E 对地址前缀 P_1 和 P_2 实施的劫持攻击都是针对 F 的,因此这两次攻击引起的感染节点集合都包含 A 和 B,而 C 既能识别 E 对 P_1 的攻击也能够识别对 P_2 的攻击.

通过监测信息的局部性和相关性可知:(1) 必然存在具有更高共享效率和更低通信开销的信息共享方式,使得无需将监测信息通知所有的自治系统;(2) 历史信息有助实现信息的按需共享.

2.3 问题模型

根据前面两节的分析,本节对后续内容需要用到的一些重要概念进行定义并且给出问题的抽象描述.

定义 1(监测信息). 监测信息是指在路由协同监测过程中,由自治系统产生的路由可信性验证请求以及虚假路由通知消息.

定义 2(信息主体). 信息主体是指具备产生、认知和传播路由监测信息能力的自治系统.

信息主体抽象表示为三元组〈P,Ω_P,Π_P〉,P 为信息主体的标识信息,Ω_P 为信息主体 P 产生和收到的监测信息集合,Π_P 为信息主体 P 产生、认知和传播监测信息时需要使用的各种本地知识集合.自治系统通过部署在其内部的路由监测服务器来产生、认知和传播路由监测信息,信息主体特指部署了路由监测服务的自治系统.

定义 3(信息覆盖). 对于信息主体 P 和监测信息 X,如果 $X\in\Omega_P$,则称 X 覆盖 P.

定义 4(信息有效). 对于信息主体 P 和监测信息 X,如果 X 的可信性能够被 P 验证(X 为路由可信性验证请求)或者 P 是 X 的感染节点(X 为虚假路由通知消息),则称 X 对 P 有效.

定义 5(有效覆盖). 对于信息主体 P 和监测信息 X,如果 X 覆盖 P 且对 P 有效,则称 X 有效覆盖 P,否则为无效覆盖.

定义 6(最小有效覆盖子集). 给定的信息主体集合 S 和路由监测信息集合 M,如果存在 $S_M\subseteq S$,对于任意 $P\in S_M$,至少存在一个元素 $m\in M$ 使得 m 对 P 有效,并且对于任意 $P\notin S_M$,必不存在元素 $m\in M$ 且 m 对 P 有效,则称 S_M 为 S 关于 M 的最小有效覆盖子集.

定义 7(信息共享行为收益与开销). 信息共享行为收益是指信息主体通过对外共享路由监测信息得到的回报.如果信息主体 P 对外发送路由监测信息 X,并由此得到应答或反射信息序列 $R_X=\langle R_1,\ldots,R_m\rangle$,则 P 本次的信息共享行为收益为 R_X 中对 P 有效的信息数量.信息共享行为开销是指信息主体对外发送路由监测信息引起的

通信开销,本文使用发送路由监测信息的数量计算通信开销.

定义 8(路由相关). 假设存在两条 BGP 路由 R_A 与 R_B 以及与之对应的路由监测信息 M_A 与 M_B,如果满足如下条件之一,则称 M_A 与 M_B 路由相关,简称相关:

1) R_A 与 R_B 的目标前缀属于同一自治系统;

2) R_A 的 AS_PATH 与 R_B 的 AS_PATH 包含相同的子路径.

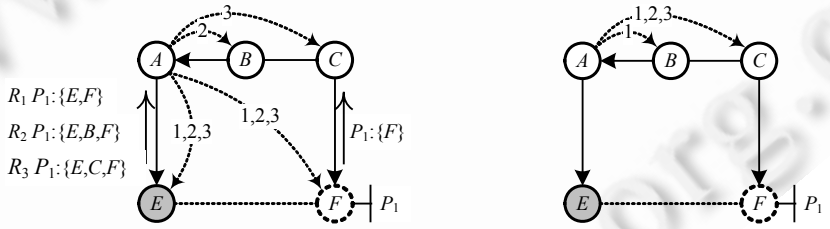
根据上述定义,路由协同监测中的信息共享问题可以描述为:给定信息主体集合 $S=\{P_1,\ldots,P_N\}$以及由信息主体 P_0 产生的路由监测信息集合 $M=\{M_1,\ldots,M_m\}$,要求为信息主体集合 S 计算关于 M 的最小有效覆盖子集,并且使得 P_0 的信息共享行为收益最大,而信息共享行为开销最小.

3 信息共享机制

本节提出一种信息共享机制 CoISM,该机制具有自学习特性,能够向最优解收敛.CoISM 利用监测信息的相关性引导自治系统实现监测信息的有效覆盖,通过信息“反射”行为增加信息接收方的主动性,提高了监测信息的传播速度,将自治系统的收益建立在对外共享信息的基础上,具有激励性.

3.1 路由可信验证

IRV[5]将 BGP 路由的 AS_PATH 中包含的自治系统节点作为路由可信验证方,通过逐个询问的方式验证指定路由的可信性,这种做法存在盲点问题,并且由此引起的通信开销与验证路由数量呈线性增长关系.图 2(a)给出了在 IRV 中路由验证消息的发送过程,自治系统 A,B 和 C 均部署了路由监测服务,负责监测属于自己和自己客户的地址前缀路由,恶意自治系统 E 先后 3 次向 A 发送不同的去往前缀 P_1 的伪造路由,虚线箭头表示 A 发出的路由验证消息.由于 E 和 F 都没有部署 IRV 服务,因此 A 无法判别 R_1~R_3 的可信性.虽然 C 能够识别 R_1~R_3(因为 C 负责监测 F 的路由,所以假设 C 知道 F 有哪些下游节点),但没有被包含在 R_1 的 AS_PATH 中,因此 A 不会请求 C 验证 R_1.在图 2(b)中,自治系统 A 采用另外一种方法验证路由 R_1~R_3,首先依次询问 B 和 C,并在 C 处得到 R_1 的验证应答,在验证 R_2~R_3 时,因为 R_1~R_3 彼此相关,所以优先向 C 发送验证请求,并得到 R_2~R_3 的验证应答,与图 2(a)相比避免了盲点问题且具无效通信次数更少.



(a) Routing validation method in IRV
(a) IRV 路由验证请求发送方式

(b) Routing validation method in CoISM
(b) CoISM 路由验证请求发送方式

Fig.2 Comparison of routing validation methods in IRV and CoISM

图 2 IRV 与 CoISM 路由验证请求发送方式对比

考虑如下社会事实:当某人 A 需要咨询问题 X 但不知道应该问谁时,如果 B 曾经向 A 回答过与 X 类似的问题,则 A 会优先咨询 B,其次,如果 C 曾经向 A 咨询过与 X 相关的问题,则 C 可能也知道谁能回答问题 X.受上述事实启发,CoISM 按照如下原则发送和处理路由可信验证请求:(1) 如果在发送方本地存在由 P 返回的对 R'的可信验证结果,且 R'与 R 相关,则优先向 P 发送路由 R 的可信验证请求;(2) 接收方在收到路由 R 的可信验证请求时,如果能够验证则直接返回验证结果;否则,如果接收方曾收到由 P 返回的对 R'的可信验证结果,且 R'与 R 相关,则向发送方推荐 P;如果不存在与 R 相关的路由验证结果,但曾经收到由 Q 发来的关于 R'的可信性验证请求,且 R'与 R 相关,则向请求者推荐 Q;(3) 对于已经发送路由可信验证请求的自治系统不再发送;(4) 在没有任

何启发信息的情况下,逐个发送直至得到成功应答.

与 IRV 的验证方选择算法相比,CoISM 利用监测信息相关性及历史应答情况作为发送路由可信验证请求的启发信息,同时增加了信息提供方利用历史知识主动提供推荐信息的机制.为避免引起循环推荐和收敛问题,监测信息携带传输路径,当传播路径过长或者出现环路时,将停止传播.图 3 给出 3 种可能的运行案例:(1) *A* 向 *B* 发送路由可信验证请求消息 *M*,*B* 能够验证 *M* 并直接返回应答;(2) *B* 无法验证 *M*,但 *C* 曾为 *B* 验证过 *M*′且 *M*′与 *M* 相关,则 *B* 向 *A* 推荐 *C*,*A* 进一步请求 *C* 验证 *M*;(3) *B* 无法验证 *M*,但 *C* 曾经请求 *B* 验证 *M*′且 *M*′与 *M* 相关,则 *B* 向 *A* 推荐 *C*,由于 *D* 为 *C* 验证 *M*′,*C* 向 *A* 返回 *D*,*D* 为 *A* 完成对 *M* 的验证.

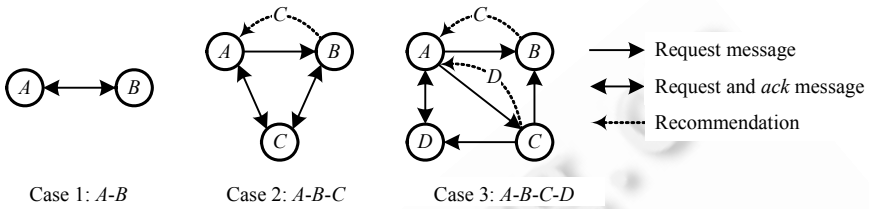


Fig.3 Illustration of routing validation request transmission

图 3 路由验证请求发送示意图

根据上述思想,路由可信验证请求发送与接收算法如图 4 所示,算法中使用的变量和函数描述参见表 1.

```
newM ←⟨ID,P,newR,unauth unknown,null,null⟩;
buildPSet(pSet);
for all (m ∈ localMSet) do {
  if isRelated(newM,m) and (m.authServer!=P) then {
    if (m.authStatus=auth) then
      addByOrder(m.authServer,serverSet);
    if (m.authStatus=unAuth) then
      addByOrder(m.authServer,applicantSet);
    remove(m.authServer,PSet);}   //end of if
}   //end of for
buildSList(authServerList,serverSet,applicantSet,pSet);
authServer←getFirst(authServerList);
while (authServer≠null) do {
    while (newM.status≠finished) do {
      if (length(newM.authPath)>MaxQueryLen) or
        (exist(authServer,newM.authPath)) then break;
      appendPath(newM.authPath,authServer);
      send(authServer,newM);
      newM←receive(authServer);
      if (newM.status=finished) then return;
      if (newM.authServer=null) then break;
        authServer←newM.authServer;
    }//end of inside while
    authServer←getNext(authServer);
}   //end of outside while
return;
```

(a) Algorithm for sending route validation request

(a) 路由可信验证请求发送算法

```
newM←receive(anyApplicant);
if ableToAuth(newM.route) then {
    newM.authStatus←auth;
    newM.authResult←authRoute();
    newM.authServer←Q;
    send(anyApplicant,newM);
    return;}   //end of if
for all (m ∈ localMSet) and isRelated(newM,m) do {
  if (m.authStatus=auth) then
    addByOrder(m.authServer,serverSet);
  if (m.authStatus=unAuth) then
    addByOrder(m.authServer,applicantSet);
}   //end of for
authServer←getFirst(serverSet);
if authServer≠null then {
    newM.authServer←authServer;
    send(anyApplicant,newM);
    return;}   //end of if
authServer←getFirst(applicantSet);
if authServer≠null then {
    newM.authServer←authServer;
    send(anyApplicant,newM);
    return;}   //end of if
return;
```

(b) Algorithm for receiving route validation request

(b) 路由可信验证请求接收算法

Fig.4 Algorithms for sending and receiving route validation request

图 4 路由可信验证请求发送与接收算法

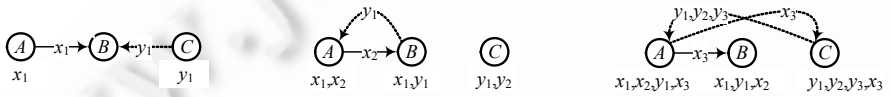
Table 1 Description of functions and variables in Fig.4

表 1 图 4 算法函数、变量定义及说明

Name	Description
authServerList	List of authenticating server ready to receive validation request(is ordered)
buildSList(...)	Add AS node of serverSet, applicantSet and pSetby into authServerList
isRelated(*newM*, *m*)	Check whether the message newM is related with message m
addByOrder(*m.authServer*,*serverSet*)	Insert m.authServer into serverSet by the order of descending
BuildRelatedMset(*newM*,*localMSet*)	Collect the message in localMSet which is related with message newM
isValidCover(*newM*)	Check whether the message newM is valid to the local receiver
getBayesProb (...)	Calculate the valid expectation with Bayes method
cover(*newM*,*tempM.Origin*)	Check whether the local receiver receives message newM before
reflection(*tempM*,*newM.Origin*)	Reflect message tempM to the origin sender of message newM

3.2 虚假路由通知

当监测到虚假路由时,需通知其他可能存在的感染节点,由于无法得知哪些自治系统是感染节点,因此在IRV中没有主动通知的机制.与IRV及其他路由监测项目相比,CoISM引入信息“反射”行为,利用相关性引导自治系统进行监测信息的主动推送,主要思想是:当信息主体P从Q处收到虚假路由通知消息X时,如果X对自己有效,则产生一个有效回应,然后P搜索本地信息库中与X相关的信息形成信息集合Ψ_X,对于所有属于Ψ_X的信息Y,P根据历史经验猜测Q是否需要Y,如果需要则将Y回送给Q,然后使用同样方法猜测是否需要将信息X发送给集合Ψ_X中所有信息的源主体.以图5为例:A和C每轮依次产生一条彼此相关的虚假路由通知消息x_1~x_3和y_1~y_3,其中x_1~x_3对B,C有效,y_1~y_3仅对A有效.在第1轮中,A和C分别向B发送x_1和y_1,在第2轮中,由于x_1对B有效,所以A继续向B发送x_2,当B收到x_2时,向A反射y_1,而因为y_1对B无效,C不再向B发送y_1.在第3轮中,A继续向B发送x_3,由于y_1对A有效,A将x_3同时发送给C,当C收到x_3时,向A反射y_1~y_3.



(a) First loop (a) 第1轮 (b) Second loop (b) 第2轮 (c) Third loop (c) 第3轮

Fig.5 Illustration of information reflection

图5 信息反射示意图

对于虚假路由R和自治系统A,如果R出现在A的BGP路由表中,则A是R的感染节点,否则A是R的隔离节点.由于A不对外公开自己的BGP路由表,因此只有A自己知道是否感染了R,所以当A收到虚假路由通知时,需要向信息提供者返回应答,告知信息提供者所收到的通知消息是否对自己有效.因为只有感染节点才需要虚假路由通知,为避免引起过多的无效覆盖,在发送虚假路由通知时,需要根据历史应答对本次将要发送的通知进行有效性猜测.

本文使用贝叶斯概率估计方法猜测虚假路由通知是否对目标自治系统有效.当信息主体Q向P发送了一组彼此相关的虚假路由通知消息$\langle X_1,\ldots,X_m\rangle$时,将会从$P$处收到一组应答$\langle ACK_1,\ldots,ACK_m\rangle$,若将该过程视为一个贝奴利实验,则对于消息$X_{m+1}$,$Q$向$P$返回的$ACK_{m+1}$取值为有效的概率服从Beta分布,其概率密度函数公式见式(1),X_{m+1}对P有效的期望见式(2),其中Γ为伽玛函数,θ表示返回应答为有效的概率,u表示返回应答为有效的次数,v表示返回应答为无效的次数,由于自治系统的路由策略和路由表都会随时间变化,因此只统计在过去t时间内的消息应答,当期望超过指定阈值时,X_{m+1}被认为对P有效.

$$Beta(\theta\,|\,u,v)=\frac{\Gamma(u+v+2)}{\Gamma(u+1)\Gamma(v+1)}\theta^u(1-\theta)^v \tag{1}$$

$$E(Beta(\theta\,|\,u+1,v+1))=\frac{u+1}{u+v+2} \tag{2}$$

上述方法具有自学习特性,在初始阶段,由于自治系统并未对外交换监测信息,因此得到的有效覆盖期望为0.5,此时,当自治系统发现了虚假路由信息时,将向所有其他自治系统广播,并接收从其他自治系统返回的有效覆盖结果,经过一段时间的运行,对于无效覆盖的自治系统其有效覆盖期望值将低于阈值,此时,新的监测信息将不再向该自治系统发送,如果某自治系统重新对某类路由监测信息感兴趣,随着该自治系统对外宣告相关的监测信息,其在其他自治系统的有效覆盖期望值又会逐渐增加,当超过阈值时,该自治系统又能够收到来自其他自治系统的通知信息.

CoISM 在计算路由监测信息对目标自治系统的有效覆盖期望时,将历史监测信息对目标自治系统的有效覆盖情况保存在信息覆盖矩阵中,其定义是:*CoverMatrix*(*MessageID*,*TargetAS*)→{*NoCover*,*ValidCover*,*InvalidCover*},其中,*MessageID* 和 *TargetAS* 分别对应监测信息的 ID 和目标自治系统的 AS 编号,*NoCover*,*ValidCover* 和 *InvalidCover* 表示与 *MessageID* 对应的监测信息对与 *TargetAS* 对应的自治系统的覆盖情况.所有监测信息对于产生的者的覆盖情况均为有效覆盖(*TargetAS*).

虚假路由通知发送算法如图 6 所示,算法中使用的变量和函数描述参见表 1.

```
newM←receive(anyServer);
buildRelatedMset(relatedMset,newM,localMSet);
for all (m∈relatedMset) do {
   if not isSelf(newM.Origin) and isValidCover(newM) then {
      sendACK(valid,newM.Origin);
      prob←getBayesProb(newM.Origin,relatedMset,CoverMatrix);
      if (prob>minSendProb) and not cover(m,newM.Origin) then reflection(m,newM.Origin);
   }   //end of if
   prob←getBayesProb(m.Origin,relatedMset,CoverMatrix);
   if (prob>minSendProb) and not cover(newM,m.Origin) then reflection(newM,m.Origin);
}   //end of for
result←receiveAck(anyServer);
updateCoverMatrix(result,CoverMatrix);
add(newM,localMSet);
return;
```

Fig.6 Algorithm for bogus route detection sending

图 6 虚假路由通知发送算法

3.3 消息格式与传输控制

自治系统之间通过路由监测消息进行交互,路由监测消息用于封装路由可信性验证请求以及虚假路由通知,路由监测消息主要包括如下字段:⟨*ID*,*Origin*,*Route*,*AuthStatus*,*AuthResult*,*AuthServer*,*Path*⟩,各字段含义描述如下:(1) *ID*,消息 ID 是路由监测信息的唯一标识;(2) *Origin*,产生消息的源主体,使用自治系统的 AS 编号表示;(3) *Route*,需要验证或者通告的路由;(4) *AuthStatus*,路由可信验证状态,0:未验证 1:已验证;(5) *AuthResult*,路由可信验证结果,0:未知 1:可信 2:不可信;(6) *AuthServer*,提供路由可信验证结果的自治系统,取值方式与 *Origin* 相同;(7) *Path*,消息传播路径,记录消息在传递过程中经过的信息主体序列.

路由监测消息在传递时,遵循如下原则:(1) 消息传播路径长度超过阈值的不继续传递;(2) 对于路由监测消息已经覆盖的信息主体,不再重复覆盖.

3.4 算法分析

- 有效性分析

有效性是指对于给定的信息主体集合 $S=\{P_1,\ldots,P_N\}$以及路由监测信息集合 $M=\{M_1,\ldots,M_m\}$,CoISM 产生的监测信息覆盖集合能够在有限时间内向 S 关于 M 的最小有效覆盖子集收敛.对于任意监测信息 M_i,必然存在对 S 的划分:$D_S=\langle X,Y,Z\rangle$,其中 X 为感染节点集,Y 为免疫节点集,Z 为隔离节点集.如果 M_i 被发送给 X 中节点的概率

能够逐渐大于被发送给 Y 和 Z 中节点的概率,则最终产生的监测信息覆盖集合会向最小有效覆盖子集收敛.假设在初始阶段,M_i 被发送往 X,Y 和 Z 的概率相等,分别为 $ProbX(M_i)$,$ProbY(M_i)$和 $ProbZ(M_i)$,则:

Case 1:如果 M_1 被送往 X,则为有效覆盖.由于 M_2 与 M_1 相关,根据信息反射原理,M_2 也会送往 X.依次类推可知,对于所有 $M_i(1<i\leqslant m)$,都有 $ProbX(M_i)>ProbY(M_i)$和 $ProbX(M_i)>ProbZ(M_i)$,因此得到一个 S 关于 M 的最小有效覆盖子集.

Case 2:如果 M_1 被送往 Y 或 Z,则为无效覆盖,根据公式(2)可知,M_2 被送往 Y 或 Z 的概率将减小.依次类推可知,必然存在 $M_k(1<k\leqslant m)$,使得 $ProbX(M_k)$大于 $ProbY(M_k)$或 $ProbZ(M_k)$.至此,对于 $M_j(k<j\leqslant m)$皆有 $ProbX(M_j)>ProbY(M_j)$和 $ProbX(M_j)>ProbZ(M_j)$.由 Case 1 可知,最终可以得到一个 S 关于 $M-\{M_k\}(1<k\leqslant m)$的最小有效覆盖子集.如果将 $M_k(1<k\leqslant m)$以前的过程可以视为算法的学习过程,当 M 包含的监测信息远远大于 k 时,这个学习过程可以被忽略,M 近似等于 $M-\{M_k\}$.

路由监测信息在传播过程中通过传输路径限制传播长度和避免出现环路,使用覆盖矩阵记录信息的覆盖情况,对于已经覆盖的自治系统不会重新覆盖,这就保证了路由监测信息不会被无穷尽传递.由于自治系统的路由策略是相对稳定的,因此对指定虚假路由监测信息的有效性判定相对稳定不变,而 S 与 M 都是有限集合,因此,算法会在有限时间内结束.综上可知,路由可信验证方选择算法和虚假路由通知算法产生的 S 关于 M 的覆盖集合能够向最小有效覆盖子集收敛.

本文未考虑彼此无关的路由事件序列,因为:(1) 单次出现的独立异常事件破坏程度有限;(2) 由配置错误引起的路由事件具有时空局部性,往往会连续发生;(3) 对于恶意节点来说,路由攻击行为有攻击开销,为提高效率,攻击者不会单纯实施一次攻击.

- 激励性分析

文献[18]指出,个体对外共享信息的动机在于从信息共享中获益.对于自治系统而言,只有在信息共享中获利才会促使自治系统参与监测信息共享.基于反射的路由监测信息共享机制使得信息主体可以通过利它行为获利,自治系统对外提供的有效监视信息越多,收到的反射信息也会越多,对虚假路由信息的识别能力也会越强,对于一个自私的信息主体,如果不主动对外提供有效的信息,也将难以得到其他信息主体的信息.另外,因为只有有效信息覆盖才会触发信息反射,信息主体为了降低不必要的开销会主动抑制无效信息覆盖行为,从而保证整体通信开销较小.

- 性能分析

根据文献[19]提供的路由统计数据,目前 BGP 路由的 AS_PATH 属性的平均长度约为 5.3943,这意味着每条虚假 BGP 路由经过的感染节点数量有限,由此产生的路由可信验证请求和虚假路由通知消息数量也有限.域间路由系统拓扑结构具有幂律特性[20],大部分 ISP 往往在路由上依赖少数的大型 ISP,一些小型的 ISP 可以委托上游的大型 ISP 为自己监测路由,而不需要在自身部署 CoISM,这就减少了 CoISM 节点的数量,从而降低的通信开销.因为在互联网环境下的信息传播与获取具有小世界特性[21],任何节点经过有限次数可以得到一次有效信息覆盖,这也保证了无效通信开销会处于一个较低的范围.

3.5 部署与实施

CoISM 在部署与实施时涉及两类实体:路由监测服务器(monitor)和 CoISM 注册中心(CoISM registry).路由监测服务器的其主要功能包括:(1) 与所属自治系统中的边界路由器建立哑 iBGP 会话采集 BGP 路由;(2) 与其他路由监测服务器协同监测 BGP 路由的可信性;(3) 当发现虚假 BGP 路由时,通知其他可能受欺骗的自治系统.CoISM 注册中心用于登记所有部署了 CoISM 服务的自治系统以及各路由监测服务器的访问信息.

在实际部署时,CoISM 有以下特点:(1) 路由监测服务器是单独部署在自治系统的服务器,每个自治系统只需设立一个;(2) 路由监测服务器之间的通信建立在应用层协议之上,不依赖 BGP 会话;(3) 任何自治系统在部署 CoISM 服务后,需向 CoISM 注册中心注册,每个路由监测服务器应定时从 CoISM 注册中心下载最新的服务器名单;(4) 规模较小的自治系统可以委托其供应商自治系统代为监测路由,而无需部署 CoISM 服务.CoISM 的部署与实施示意图如图 7 所示.

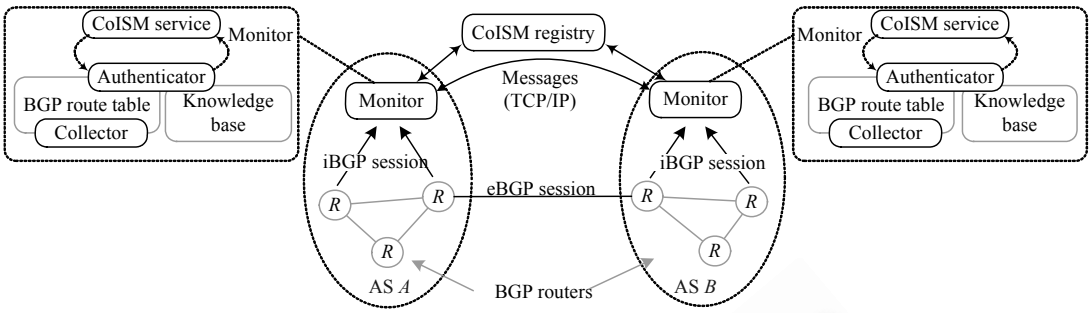


Fig.7 Deployment and implementation of CoISM

图 7 CoISM 部署与实施示意图

4 模拟与分析

4.1 评估标准

信息有效覆盖率用于检验信息共享机制能否实现信息的按需共享,信息有效覆盖率越高,表明路由监测信息对感染节点的覆盖率越高,路由协同监测效果越好,其计算方法如公式(3)所示.函数 $Cover(M_i,P_j)$表示信息 M_i 是否覆盖信息主体 P_j,如果 M_i 覆盖 P_j 则返回 1,否则为 0.函数 $Valid(M_i,P_j)$表示信息 M_i 对信息主体 P_j 是否有效,如果有效则返回 1,否则返回 0.

$$\alpha=\sum_{j=1}^{n}\left(\sum_{i=1}^{m}((Cover(M_i,P_j)\times Valid(M_i,P_j))\Big/\sum_{i=1}^{m}Cover(M_i,P_j)\right) \tag{3}$$

信息主体收益率用于检验信息主体在信息共享行为中的获利情况,信息主体收益率越高,表明信息共享机制的激励性越好,其计算方法见式(4).函数 $Import(M_i,P_j)$表示信息 M_i 是否由 P_j 从外部获得,1 表示真,0 表示假.函数 $Export(M_i,P_j)$表示信息 M_i 是否由 P_j 产生并对外共享,1 表示真,0 表示假.

$$\beta_j=\sum_{i=1}^{m}\frac{Import(M_i,P_j)\times Valid(M_i,P_j)}{Export(M_i,P_j)+Import(M_i,P_j)\times Valid(M_i,P_j)} \tag{4}$$

通信开销用于检验信息共享机制的共享效率,对于任意路由监测信息 M_i,当其有效覆盖率达到指定阈值 t 时引起的通信开销越低,则表明无效信息覆盖越少,算法效率越高,通信开销的计算方法如公式(5)所示.为简化问题,本文使用信息覆盖次数来度量通信开销.

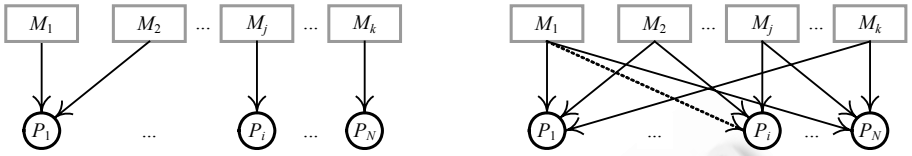
$$\tau_t=\sum_{j=1}^{n}(Cover(M_i,P_j)) \tag{5}$$

4.2 实验设计

路由监测节点通过部署在应用层的层叠网(overlay)互联,因此本文忽略网络拓扑和 BGP 路由策略对路由监测信息共享的影响,并且假设任意两个路由监测节点之间均通过一跳可达.鉴于此,设计实验如图 8 所示.将所有的路由监测信息组成集合 A,将所有产生路由监测信息的信息主体组成集合 B,对于任意路由监测信息 $M_i\in B$ 以及 $P_j\in A$,如果 M_i 有效覆盖 P_j,将在 M_i 与 P_j 之间增加一条有效覆盖边(采用实线箭头表示),如果 M_i 无效覆盖 P_j,将在 M_i 与 P_j 之间增加一条无效覆盖边(采用虚线箭头表示),图 8(a)所示为每轮开始时,每条路由监测信息仅覆盖产生该信息的信息主体,图 8(b)所示为每轮结束时路由监测信息的覆盖情况.通过统计图 8(b)中有效覆盖边和无效覆盖边就可以计算第 4.1 节提出的评估标准.

实验过程如下:首先,产生信息主体集$S=\{P_1,\ldots,P_N\}$以及每个信息主体的路由监测信息集:$\Omega=\{\Omega_1,\ldots,\Omega_N\}$,每个路由监测信息集用于保存由信息主体自己产生或者外来的路由监测信息,所有的路由监测信息都与自治系统集合$AS=\{AS_1,\ldots,AS_K\}$相关.采用时间片轮转的方式运行L轮,各信息主体每轮随机产生W条路由监测信息(包

括路由可信验证请求和虚假路由通知),对于任意信息主体P_j和路由监测信息M_i,$Cover(M_i,P_j)$为1的概率为θ.然后,各信息主体通过CoISM依次对外共享本地路由监测信息集合中的新信息,只至所有信息主体完成自身路由监测信息集合的处理.在每轮结束时,分别计算所有路由监测信息的有效覆盖率,信息主体的平均收益以及单个节点产生的路由监测信息在有效覆盖率达到指定阈值T时引起的通信开销.



(a) Initial information coverage
(a) 信息覆盖初始状态

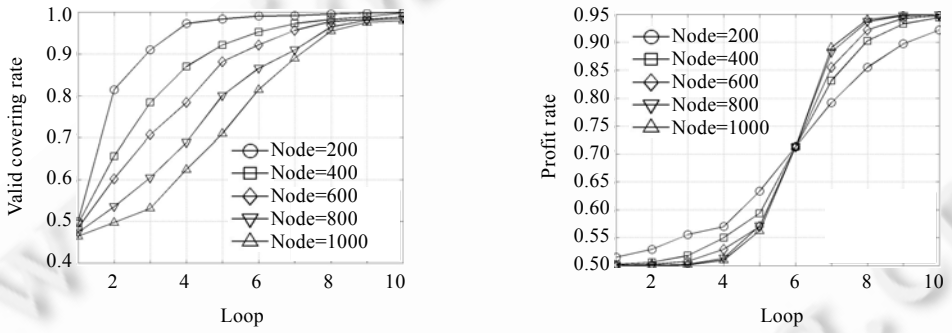
(b) Final information coverage
(b) 信息覆盖最终状态

Fig.8 Illustration of information coverage in the simulation

图 8 模拟实验信息覆盖示意图

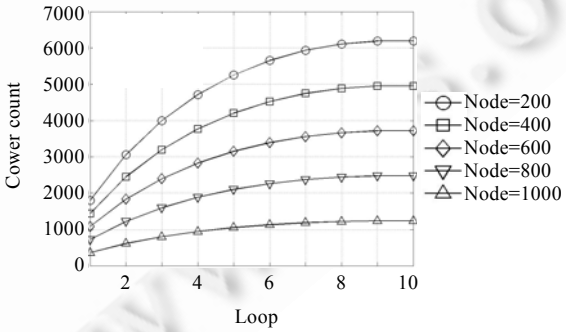
4.3 实验结果与数据分析

本节给出在 OPNET 环境下完成的模拟计算结果,第 4.2 节设计的实验中主要参数取值情况如下:N={200,400,600,800,1000};K=1000;L=10;w=20;θ=0.5;T=0.9.实验采用时间片轮转模型,每个节点依次运行和处理各自路由监测信息库中产生和收到的新信息,实验结果如图 9 所示.



(a) Percentage of valid coverage
(a) 有效覆盖率

(b) Percentage of reward
(b) 收益率



(c) Communication overhead
(c) 通信开销

Fig.9 Result of CoISM simulation

图 9 CoISM 模拟实验结果

图 9(a)为信息有效覆盖率的变化情况,横轴为迭代轮数,纵轴为信息有效覆盖率.通过图 9(a)可知:(1) 在指定自治系统集合的情况下,使用CoISM进行路由监测信息共享,随着迭代轮数的增加,信息有效覆盖率会趋近1.这表明CoISM具有自学习性,通过信息相关性减少了无效信息覆盖次数;(2) 信息主体数量的增加,会减缓有效覆盖率向1收敛的速度,但不会改变向1收敛的趋势.这是因为当信息主体数量增加时,在开始阶段由于缺乏足够的启发信息,在较大规模的节点集合中产生有效覆盖的概率偏低.而向1收敛的趋势不变,则意味着大规模部署路由监测节点的有效性.

图 9(b)为信息主体的平均收益率变化情况,横轴为迭代轮数,纵轴为平均收益率.由图 9(b)可知:(1) 节点的收益率随节点对外提供的有效信息数量增加而增加,这表明CoISM具有激励性.(2) 当信息数据数量较少时,在开始阶段受到信息有效覆盖率的影响,信息主体收益率的增长速度偏慢,这表明信息主体为了自身利益应该主动增加有效覆盖次数.在具体域间路由管理中,这种主动性表现为自治系统管理人员主动交换彼此感兴趣的监测目标,例如地址前缀.随着信息有效覆盖率的上升,在信息反射机制的作用下,信息主体每次对外提供有效路由监测信息时,都会收到反射回来的相关路由监测信息,此时信息有效覆盖率迅速上升.当信息有效覆盖率趋于1时,在信息共享环路避免机制和重复有效覆盖避免机制的作用下,信息主体收到反射信息数量增加速度开始减缓.(3) 在大规模节点数量下,虽然开始阶段信息主体的收益率增长速度偏慢,但是一旦信息有效覆盖超过一定阈值,由于监测节点数量的优势,信息主体每次对外共享路由监测信息时都会引起大量相关监测信息的反射,因此,信息主体的收益率增长速度反而更快.需要特别指出的是,图 9(b)的实验结果与路由监测信息的产生点有关.在本实验中,各信息主体以等概率方式产生路由监测信息.如果路由监测信息过于集中产生在单一自治系统上,则其收益率会明显偏低,因此该节点无法从别处得到对自己有益的路由监测信息.这并不会影响CoISM的有效性,因为这种情况表明攻击点非常集中,对协同管理的需求不大,即使信息主体不对外共享信息,也不会造成大的损失.

图 9(c)为某随机选择的信息主体在其产生的路由监测信息有效覆盖率达到0.9时引起的通信开销变化情况,横轴为迭代轮数,纵轴为通信开销.图 9(c)表明:(1) 随着迭代轮数和路由监测信息数量的增加,通信开销增长速度开始变慢,这得益于信息有效覆盖率的提高;(2) 当信息主体数量偏多时,迭代轮数增加对减缓通信开销增长效果更为明显,这得益于有效信息反射数量的增加.

5 讨 论

本节讨论几个与CoISM相关的问题:

- 半诚实信任模型与PKI信任模型.CoISM采用半诚实信任模型,即假设信息主体不会恶意提供虚假路由监测信息,这一假设保证了信息反射不会引起过多无效的覆盖.这样的假设理由在于路由协同监测是ISP自发的行为,所有加入协同监测体系的ISP身份都经过了严格的认证,因此不会主动实施欺骗行为.另外,如果不考虑数字证书管理对信息可实施性带来的影响,也可以采用PKI信任模型.
- CoISM与BGP.CoISM致力于解决路由协同监测过程中的路由监测信息共享问题,路由监测结果为ISP管理人员维护BGP路由提供参考,但不会直接作用于BGP协议,因此CoISM自身的安全性不会对BGP安全造成影响.另外,与安全路由协议不同,CoISM部署在应用层实施,不需要修改BGP.因此CoISM引起的信息交换和传播不会对BGP协议本身的性能造成影响.
- 管理与部署.CoISM在具体部署时采用与IRV类似的部署方式,通过设立第三方管理中心对参与协同路由监测的自治系统进行登记注册,任何自治系统可以通过注册服务器获取所有部署CoISM服务的节点.另外,与IRV不同的是,CoISM允许位于边缘的小型ISP通过向指定上游ISP提供相应的虚假路由识别信息来实现委托路由监测,例如:委托其他ISP代为监测属于自己的地址前缀,这样做使得小型ISP无需部署CoISM,具有更好的可渐进部署性.
- 隐私信息保护.在多自治系统协同管理中,还存在隐私信息的保护和共享问题[22],例如BGP路由策略、BGP路由表等都属于隐私信息,不便对外公开.对路由可信性进行诊断往往涉及隐私信息的访问,文献

[11,12]在设计信息共享机制时,均未考虑自治系统保护自身隐私的需求对方案可实施性的影响,CoISM 将对隐私信息的访问转化为对路由判断结果的访问,不会引起隐私信息的泄漏.

- 系统局限性.CoISM 的性能依赖路由监测信息的分布和变化,虽然路由监测信息存在相关性,但这种相关性并不是绝对的,因此当路由攻击者的攻击对象过于分散时,CoISM 的无效覆盖率会明显增加.另外,CoISM 没有选择 BGP 的 AS_PATH 作为寻找信息共享对象的参考信息,这使得在开始阶段信息有效覆盖率偏低,甚至不如 IRV.

6 结束语

信息共享是域间路由协同监测中的关键问题,CoISM 发掘了路由监测信息的局部性和相关性,通过引入信息“反射”行为来提高路由监测信息的有效覆盖率,与泛洪式广播方法相比,具有更高的信息传播效率和更低的通信开销.另外,CoISM 将自治系统收益建立在利他行为的基础上,具有激励性.我们将来的工作主要集中在 CoISM 的实际应用与实现推广等方面.另外,考虑利用 CoISM 支持更为丰富的自治系统协同行为也是我们着重关注的问题.

References:

[1] Rekhter Y, Li T, Hares S. A border gateway protocol (BGP version 4). IETF Internet RFC, RFC 4274, 2006.

[2] Murphy S. BGP security vulnerabilities analysis. IETF Internet RFC, RFC 4272, 2006.

[3] Zhang Y, Zhang Z, Mao ZM, Hu C, Maggs BMD. On the impact of route monitor selection. In: Murai J, ed. Proc. of the 7th ACM SIGCOMM Conf. on Internet Measurement. New York: ACM Press, 2007. 215−220. [doi: 10.1145/1298306.1298336]

[4] Hu N, Zou P, Zhu PD. Cooperative management framework for inter-domain routing system. In: Rong C, ed. Proc. of the ATC 2008. LNCS 5060, Heidelberg: Springer-Verlag, 2008. 567−576. [doi: 10.1007/978-3-540-69295-9_45]

[5] Lu XC, Zhao JJ, Zhu PD, Dong P. Self-Organization of inter-domain routing system. Journal of Software, 2006,17(9):1922−1932 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/17/1922.htm [doi: 10.1360/jos171922]

[6] Internet routing registry. 2009. http://www.irr.net/index.html

[7] The RIPE NCC MyASN service. 2009. http://www.ris.ripe.net/myasn.html

[8] Looking glasses. 2009. http://www.traceroute.org

[9] GRADUS. 2009. http://www.renesys.com/index.shtml

[10] Georgos S, Michalis F. Analyzing BGP policies: Methodology and tool. In: Li VOK, ed. Proc. of the IEEE INFOCOM 2004. New York: IEEE Society Press, 2004. 1640−1651. [doi: 10.1109/INFCOM.2004.1354576]

[11] Goodell G, Aiello W, Griffin T. Working around BGP: An incremental approach to improving security and accuracy of inter-domain routing. In: Neuman C, ed. Proc. of the ISOC NDSS 2003. San Diego: National Security Agency Press, 2003. 75−85.

[12] Pei D, Lad M, Massey D, Zhang LX. Route diagnosis in path vector protocols. Technical Report, TR040039, Los Angeles: UCLA CSD, 2004.

[13] Yu H, Rexford J, Felten EW. A distributed reputation approach to cooperative Internet routing protection. In: Fahmy S, ed. Proc. of the Secure Network Protocols 2005. New York: IEEE Society Press, 2005. 73−78. [doi: 10.1109/NPSEC.2005.1532057]

[14] Lad M, Massey D, Pei D, Wu Y, Zhang B, Zhang LX. PHAS: A prefix hijacks alert system. In: Keromytis AD, ed. Proc. of the 15th USENIX Security Symposia. New York: USENIX Press, 2006. 153−166.

[15] Goldman CV, Zilberstein S. Optimizing information exchange in cooperative multi-agent systems. In: Karl A, ed. Proc. of the 2nd Int’l Joint Conf. on Autonomous Agents and Multi-Agent Systems. New York: ACM Press, 2003. 137−144. [doi: 10.1145/860575.860598]

[16] Xu Y, Lewis M, Sycara K, Scerri P. Information sharing in large scale teams. In: Sen S, ed. Proc. of the Workshop on Challenges in Coordination of Large Scale Multi Agent Systems (AAMAS 2004). New York: ACM Press, 2004. 123−133.

[17] Eugster P, Guerraoui R, Kermarrec A. Epidemic information dissemination in distributed systems. IEEE Computer, 2004,37(55): 60−67. [doi: 10.1109/MC.2004.1297243]

[18] Arney DC, Peterson E. Cooperation in social networks: Communication, trust and selflessness. In: Ashe J, ed. Proc. of the 26th Army Science Conf. New York: Military and Naval Science Press, 2008. 291−298.

[19] AS65000 BGP routing table analysis report. 2009. http://bgp.potaroo.net/as1221/bgp-active.html

[20] Newman MEJ. The structure and function of complex networks. SIAM Review, 2003,45(2):167−256. [doi: 10.1137/S003614450342480]

[21] Watts D, Strogatz S. Collective dynamics of small world networks. Nature, 1998,393:440−442. [doi: 10.1038/30918]

[22] Machiraju S, Katz RH. Reconciling cooperation with confidentiality in multi-provider distributed systems. Technical Report, UCB/CSD-04-1345, Berkeley: University of California, 2004.

附中文参考文献:

[5] 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. http://www.jos.org.cn/1000-9825/17/1922.htm [doi: 10.1360/jos171922]

胡宁(1972－),男,湖南长沙人,博士,副教授,主要研究领域为路由技术,网络安全技术.

朱培栋(1971－),男,博士,教授,主要研究领域为路由技术,网络安全技术.

邹鹏(1957－),男,教授,博士生导师,主要研究领域为分布操作系统,分布式计算.