互联网自治系统的前缀信誉模型

王 娜[1,3] 汪斌强[2]

(解放军信息工程大学电子技术学院 郑州 450004)[1] (解放军信息工程大学 郑州 450002)[2]

(河南省信息安全重点实验室 郑州 450004)[3]

摘 要 BGP面临的前缀劫持攻击会严重破坏互联网网络的可靠性。引入信任技术,构建自治系统的前缀信誉模型(Autonomous System Prefix Reputation Model,简写为"AS-PRM")来评估自治系统发起真实前缀可达路由通告行为的信任度。从而,自治系统可选择相对前缀信誉好的自治系统发起的前缀可达路由通告,来抑制前缀劫持攻击的发生。AS-PRM模型根据多个前缀劫持攻击检测系统的检测结果(考虑了误报、漏报率),基于beta信誉系统,计算自治系统的前缀信誉,并遵循"慢升快降"原则,更新前缀信誉。最后,仿真实验验证了模型的有效性。

关键词 BGP,前缀劫持攻击,信誉

中图法分类号 TP393 **文献标识码** A

Internet Autonomous System Prefix Reputation Model

WANG Na[1,3] WANG Bin-qiang[2]

(College of Electronic Technology, PLA Information Engineering University, Zhengzhou 450004, China)[1]

(PLA Information Engineering University, Zhengzhou 450002, China)[2]

(Henan Key Laboratory of Information Security, Zhengzhou 450004, China)[3]

Abstract Prefix hijacking faced by BGP can highly disrupt the Internet network reliability. By introducing trust technology, the paper proposed an autonomous system prefix reputation model AS-PRM to evaluate the trust of an autonomous system (AS) originating the prefix belonging to the AS. An AS selectively prefers the prefix route announcement originated by the AS with higher prefix reputation. As a result, prefix hijacking can be suppressed. According to multiple prefix hijacking detection systems' results, AS-PRM model computes AS prefix reputation based on the beta reputation system, after considering false positives and false negatives of detection systems, and updates prefix reputation following the "slowly rising, quickly falling" principle. In the end, the model validity was verified by simulation experiments.

Keywords BGP, Prefix hijacking, Reputation

1 引言

事实上的域间路由协议标准BGP(the Border Gateway Protocol,边界网关协议)[1]面临的前缀劫持攻击会对互联网的网络可靠性造成严重破坏[2],甚至影响云计算面向互联网资源的可用性[3]。BGP未提供自治系统认证收到路由通告的前缀源自治系统真实性的安全能力[4]。利用这个安全漏洞,恶意自治系统可发起前缀劫持攻击。当某个自治系统发出一个非本自治系统内前缀的可达路由通告,导致网络中以该前缀为目的地址的全部或部分数据报文被路由到这个自治系统时,称该前缀被这个自治系统劫持。前缀劫持攻击轻则增加路由器的负载,危及被劫持网络的连通性或安全性,重则造成全球网络的不稳定和瘫痪[5,6]。

近年来,学者和网络运营商发现了大量的前缀劫持攻击事件。特别是2008年2月24日发生的Pakistan Telecom劫持YouTube事件使全球互联网安全专家更加关注BGP的前缀劫持问题[6]。另外,为避免身份暴露,垃圾邮件发送者经常通过劫持前缀发送垃圾邮件[7]。eBay上也出现了被售卖或出租的被劫持前缀[8]。研究人员甚至发现互联网中确实存在大量的恶意自治系统[9]。

针对前缀劫持攻击的安全技术主要包括基于密码学的防护技术[10-13]和异常检测技术[14-17]。通过采用密码学技术认证前缀源自治系统的真实性,基于密码学的防护技术很好地修补了BGP的安全缺陷,但其面临开销过大、修改路由协议和路由器、密钥管理困难等挑战[18,19],难以部署实现。目前检测前缀劫持攻击的研究为网络管理员事后分析提供了有效依据。然而,存在重检测轻响应的问题[20,21],导致检测技术的研究成果无法转化成对域间路由系统的切实保护。

到稿日期:2011-11-07 返修日期:2012-02-23 本文受国家"九七三"重点基础研究发展规划项目基金(2011CB311801),河南省科技创新人才计划(114200510001)资助。

王 娜(1980—),女,博士,讲师,主要研究方向为路由安全技术、网络安全技术等,E-mail:tinatwf@163.com;汪斌强(1963—),男,博士,教授,主要研究方向为宽带信息网络。

在这种背景下，本文考虑将信任技术[22]引入域间路由安全，构建自治系统之间在发起前缀可达通告这一路由行为(简称为“前缀路由行为”)上的信任关系，建立自治系统前缀路由行为的信任度(简称为“前缀信誉”)，以达到抑制前缀劫持攻击的目的。人类社会之所以能够平稳健康地运行，很大程度上得益于个人、团体和组织之间的信任关系。自治系统的自组织特性和彼此之间商业关系、商业行为的存在，导致自治系统在前缀路由行为已经表现出典型的社会行为特征[23]。如果自治系统之间能够建立起这种信任关系，自治系统可选择相对信誉好的自治系统发起的前缀可达路由通告，从而抑制前缀劫持攻击的发生，保护域间路由系统。

虽然已有学者提出采用相似的方法[24-29]保护域间路由系统，但是，它们的域间路由信任模型不是自治系统真实前缀路由行为的信誉评估，难以达到有效抑制前缀劫持攻击的目的。例如，文献[24-26]中的信任模型用于评估自治系统真实前缀路由行为和传播路由通告行为的综合信誉；文献[27]的信任模型用于评估自治系统传播路由通告行为的可信度，以抑制虚假路径攻击；文献[28,29]中的自治系统信誉是自治系统发起前缀路由通告的真实和稳定度的刻画。

基于此，本文提出了一个评估自治系统真实前缀路由行为信任度的前缀信誉模型 AS-PRM(Autonomous System Prefix Reputation Model)。该模型基于自治系统前缀路由行为全局性、公开性的特征，定义了自治系统的前缀信誉；基于beta信誉系统，采用多个检测系统的检测结果作为自治系统历史前缀路由行为的分析结果，在充分考虑检测系统的误报和漏报率的基础上，给出自治系统前缀信誉的计算方法和遵循“慢升快降”原则的更新方法；最后，仿真实验验证了模型的有效性。

2 前缀信誉模型

2.1 定义

自治系统的前缀路由行为具有全局性、公开性的特征。如图1所示，AS_i 发起前缀 P_1 可达的路由通告，相当于向互联网中所有自治系统“广播”自己可达前缀 P_1。基于此观察，本文给出前缀信誉的定义。

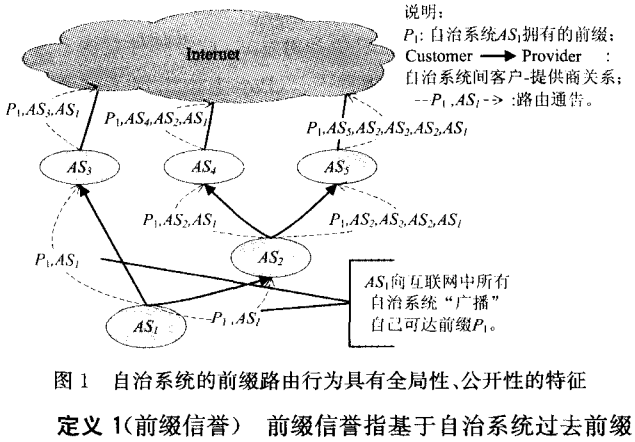

图1 自治系统的前缀路由行为具有全局性、公开性的特征

定义 1(前缀信誉) 前缀信誉指基于自治系统过去前缀路由历史行为的观察而得出的对它未来前缀路由行为的期望，表示所有自治系统对该自治系统前缀路由行为的信任程度，是一个全局信任值。

本文定义前缀信誉的取值被映射到实数区间[0,1]。自治系统的前缀信誉为1表示对该自治系统的前缀路由行为完全信任，反之，表示完全不信任；前缀信誉值介于0和1之间则表示信任程度。

2.2 计算方法

2.2.1 基于beta信誉系统的前缀信誉函数和前缀信誉值

自治系统的前缀路由行为是一个二项事件。如果自治系统发起真实的前缀可达路由通告，则为肯定事件；反之，如果自治系统发起虚假的前缀可达路由通告，即发动前缀劫持攻击，则为否定事件。肯定和否定事件的发生具有随机和连续性。这与真实情况是一致的。根据研究报告[30,31]，大量的前缀劫持攻击事件多因管理员配置错误造成，这种配置错误的发生具有随机性和连续性的特点。

根据二项事件的后验概率服从 beta 分布的特性，在已知肯定事件次数和否定事件次数的情况下，可计算出自治系统下一次发起真实前缀路由通告的概率，采用此概率的期望值作为该自治系统的前缀信誉。下面给出基于 beta 信誉系统[32]的自治系统前缀信誉函数和前缀信誉值的定义。

定义 2(前缀信誉函数) 假设 r_T 和 s_T 分别表示目标自治系统 T 的肯定和否定事件次数($r_T\geqslant 0, s_T\geqslant 0$)，那么目标自治系统 T 的前缀信誉函数定义如下：

$$\varphi(p_T\mid r_T,s_T)=\frac{\Gamma(r_T+s_T+2)}{\Gamma(r_T+1)\Gamma(s_T+1)}p_T^{r_T}(1-p_T)^{s_T}$$

式中，p_T 表示自治系统 T 下一次发生肯定事件的概率，$0\leqslant p_T\leqslant 1$；伽玛函数 Γ 表示 p_T 的概率密度函数 pdf。

定义 3(前缀信誉值) 假设 r_T 和 s_T 分别表示目标自治系统 T 的肯定和否定事件的次数($r_T\geqslant 0, s_T\geqslant 0$)，那么目标自治系统 T 的前缀信誉值定义如下：

$$PR_T=E(\varphi(p_T\mid r_T,s_T))=(r_T+1)/(r_T+s_T+2)。$$

2.2.2 根据攻击检测结果的前缀信誉计算方法

本文选取前缀劫持攻击检测系统(简称为“检测系统”)的检测结果作为自治系统历史路由行为的分析结果。目前前缀劫持攻击检测技术的研究已经有丰硕的成果，如 PHAS[17] 系统已经部署实现且检测结果可通过网站查询。假设自治系统发起前缀可达路由通告，若被检测系统检测出是前缀劫持攻击，则提供否定反馈，认为发生一次否定事件，反之，发生肯定事件。如果自治系统在一个路由通告中同时发起 $i(i\geqslant 1)$ 个前缀可达，检测系统检测出其中 $j(j\geqslant 0)$ 个是被劫持的前缀(即发生前缀劫持攻击)，则认为一共发生 i 次事件，其中否定事件 j 次，肯定事件 $i-j$ 次。

因为原始路由数据来源片面或检测技术缺陷，检测系统不可避免地存在误报和漏报率。如果某个检测系统的误报或漏报率很高，说明该检测系统的检测能力有限，不应基于此检测系统的检测结果计算前缀信誉。本文引入检测力的概念，来评估检测系统的检测能力。

定义 4(检测力) 假设 fp_D^T 和 fn_D^T 分别表示前缀劫持攻击检测系统 D 针对目标自治系统 T 的误报率和漏报率($fp_D^T\geqslant 0, fn_D^T\geqslant 0$)，那么检测系统 D 针对目标自治系统 T 的检测力 $Dability_D^T$ 定义如下：

$$Dability_D^T=\frac{1}{fp_D^T+fn_D^T}$$

根据检测系统对目标自治系统 T 的检测力构建一个该自治系统的有效检测系统集合 $\Omega_T=\{D_1,D_2,\cdots D_n\}(n\geqslant 1)$，其中，$\forall D_i\in\Omega_T, Dability_{D_i}>\theta$，即有效检测系统集合中所有检测系统的检测力都必须大于最低检测力 θ。下面给出根据 Ω_T 的检测结果计算目标自治系统 T 前缀信誉的方法。

假设：①在时间 t 内，自治系统 T 发起 $m(m\geqslant 1)$ 个前缀

可达的路由通告，基于检测系统 D_i（$D_i \in \Omega_T$）的检测结果，肯定和否定事件次数分别表示为 $r_T^{D_i}$ 和 $s_T^{D_i}$（$r_T^{D_i}+s_T^{D_i}=m$）；②在时间 t 内，自治系统 T 的肯定和否认事件次数分别表示为 r_T 和 s_T（$r_T+s_T=m$）；③N_{D_i} 表示检测系统 D_i 检测出真实前缀劫持攻击的次数，显然，$N_{D_i} \leqslant s_T^{D_i}$。

存在以下两种情况：

（1）若 $\forall i,j(1 \leqslant i,j \leqslant n)$，$r_T^{D_i}=r_T^{D_j}$，$s_T^{D_i}=s_T^{D_j}$，那么，$r_T=r_T^{D_i}$，$s_T=s_T^{D_i}(1 \leqslant i \leqslant n)$，自治系统 T 的前缀信誉 PR_T 为

$$PR_T=(r_T+1)/(r_T+s_T+2)$$

（2）若 $\exists i,j(1 \leqslant i,j \leqslant n)$，$r_T^{D_i} \neq r_T^{D_j}$，$s_T^{D_i} \neq s_T^{D_j}$，说明存在检测系统误报或漏报的情况，那么，

①要求检测系统提供每个否定反馈（即发生前缀劫持攻击）的证据。检测系统 D_i 的否定反馈证据集合 $E_{D_i}=\{E_{D_i}^1, E_{D_i}^2, \cdots, E_{D_i}^{D_i}\}$，其中，$E_{D_i}^j=(Time, AS, prefix)(1 \leqslant j \leqslant k)$，$Time$ 表示前缀劫持攻击发生的时间，AS 表示发起前缀劫持攻击的自治系统（即目标自治系统 T），prefix 表示被劫持的前缀（即 T 劫持的前缀）。

②对每个检测系统提供的否定反馈证据依次比较，若存在一致的反馈证据，即 $\forall i,j(1 \leqslant i,j \leqslant n)$，$\exists l_{D_i}, l_{D_j}$，$(1 \leqslant l_{D_i} \leqslant k_{D_i}, 1 \leqslant l_{D_j} \leqslant k_{D_j})$，$E_{D_i}^{l_{D_i}}=E_{D_j}^{l_{D_j}}$ [1]，则认为发生一次真实的前缀劫持攻击，否定事件次数 s_T 加 1，所有检测系统的 N_{D_i} 加 1（$1 \leqslant i \leqslant n$）。

3）对不一致的否定反馈证据，即 $\exists i,j(1 \leqslant i,j \leqslant n)$，$\exists l_{D_i}, l_{D_j}$，$(1 \leqslant l_{D_i} \leqslant k_{D_i}, 1 \leqslant l_{D_j} \leqslant k_{D_j})$，$E_{D_i}^{l_{D_i}} \neq E_{D_j}^{l_{D_j}}$ [2]，依次进行真实性判断。判断方法包括 IRR（Internet Routing Registry，互联网路由注册处）查询、RouteViews[33] 历史路由数据分析或询问源自治系统等。如果判断是真实的前缀劫持攻击，则 s_T 加 1，提供此否定反馈证据检测系统 D_j 的 N_{D_j} 加 1（$1 \leqslant j \leqslant n$）。

最后，根据 m、s_T，可计算目标自治系统 T 的前缀信誉 PR_T：

$$PR_T=(r_T+1)/(r_T+s_T+2)=(m-s_T+1)/(m+2)$$

根据 s_T、N_{D_i} 和 $s_T^{D_i}$，可计算检测系统 D_i 针对目标自治系统 T 的误报率 $fp_{D_i}^T$、漏报率 $fn_{D_i}^T$ 和检测力 $Dability_{D_i}^T$：

$$fp_{D_i}^T=\frac{s_T^{D_i}-N_{D_i}}{s_T}$$

$$fn_{D_i}^T=\frac{s_T-N_{D_i}}{s_T}$$

$$Dability_{D_i}^T=\frac{1}{fp_{D_i}^T+fn_{D_i}^T}$$

根据计算获得的 $Dability_{D_i}^T$，可定期更新该自治系统的有效检测系统集合。

2.3 更新方法

自治系统的前缀信誉需要根据该系统的近期前缀路由行为不断进行更新。本文设计 3 种前缀信誉：根据自治系统在更新时间 t 内前缀路由行为构建的更新前缀信誉 $PR_T(t)$、当前前缀信誉 PR_T 和最新前缀信誉 PR_T'。下面给出根据 PR_T 和 $PR_T(t)$ 计算 PR_T' 的方法。

自治系统的路由行为已经表现出典型的社会行为特征。观察人类社会的信任行为特点可知，信任是缓慢增加、快速减少的。也就是说，自治系统通过许多次真实前缀路由行为才建立起来的良好信誉，可能在几次前缀劫持攻击行为后就会丧失。即信任的增长或减少速度是不同的。基于此观察，本文采用如下前缀信誉更新方法：

①如果 $PR_T(t)<PR_T$，$PR_T'=PR_T(t)$；

②如果 $PR_T(t)>PR_T$，$PR_T'=\alpha \cdot PR_T(t)+\beta \cdot PR_T$，其中，$\alpha+\beta=1$。可通过设置 α 和 β 的值控制前缀信誉的增加速度。

3 仿真评估

本文采用 SSFNet[34] 搭建模拟仿真环境，使用由 BRITE[35] 拓扑产生器生成的 110 节点的拓扑，其中每个节点代表网络中的自治系统。设置两类节点：①A 类节点：好节点，正常发起真实的前缀可达路由通告；②B 类节点：恶意节点，发起前缀劫持攻击，根据发起攻击的频率，分为 B-1 和 B-2 两类，B-1 类节点指偶尔发起前缀劫持攻击的恶意节点，B-2 类节点指频繁发起前缀劫持攻击的恶意节点。

（1）实验 1：验证模型的有效性。

不考虑检测系统的误报和漏报率，设置更新参数 $\alpha=\beta=0.5$，分别选取 A 类和 B-1、B-2 类的代表性节点，节点的前缀信誉变化情况如图 2 所示。A 类节点的前缀信誉比较稳定，B-1 类节点在发生一次前缀劫持攻击后，前缀迅速下降，需要多次更新才能够恢复，体现了“慢升快降”的更新特点，B-2 类节点因频繁的前缀劫持攻击，前缀信誉迅速下降，且一直处于较低的信誉水平。

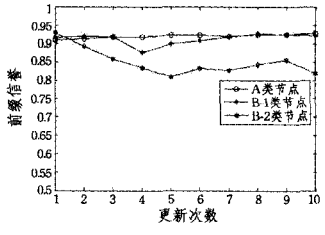

图 2 前缀信誉的变化

（2）实验 2：验证不同更新参数 α 和 β 对信誉更新变化的影响。

不考虑检测系统的误报和漏报率，采用表 1 所列数据分别设置更新参数 α 和 β，选取 A 类节点，获得如图 3 所示的前缀信誉变化情况。当 $\alpha=1$ 且 $\beta=0$ 时，前缀信誉的起伏变化最大，当 $\alpha=0.2$ 且 $\beta=0.8$ 时，前缀信誉的变化平缓但更新速度慢，当 $\alpha=\beta=0.5$ 时，前缀信誉的变化较平缓且更新速度居中。

表 1 α 和 β 参数表

α	β
1	0
0.8	0.2
0.6	0.4
0.5	0.5
0.4	0.6
0.2	0.8

1) $E_{D_i}^{l_{D_i}}=E_{D_j}^{l_{D_j}}$ 表示这两个证据中所有项（前缀劫持攻击发生的时间、发起源自治系统和被劫持前缀）都相同，实际是一个前缀劫持攻击。

2) $E_{D_i}^{l_{D_i}} \neq E_{D_j}^{l_{D_j}}$ 表示这两个证据中存在某一项（前缀劫持攻击发生的时间、发起源自治系统或被劫持前缀）不相同，不是一个前缀劫持攻击。

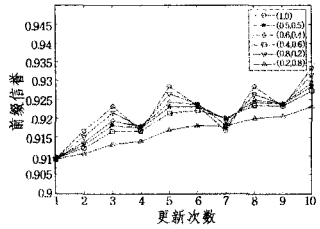

图 3 α 和 β 对前缀信誉更新变化的影响

(3)实验 3:验证检测系统的误报和漏报对自治系统前缀信誉的影响。

设置更新参数 $\alpha=\beta=0.5$,依次选取 A 类节点和 B-1 类节点,仿真检测系统误报和漏报对节点前缀信誉的影响,获得仿真结果,如图 4、图 5 所示。不剔除检测系统的误报会导致节点的前缀信誉出现下降,且经过多次更新才能够恢复正常(见图 4);不考虑检测系统的漏报会导致节点的前缀信誉较真实情况高,出现信誉偏差,直接影响模型的有效性(见图 5)。

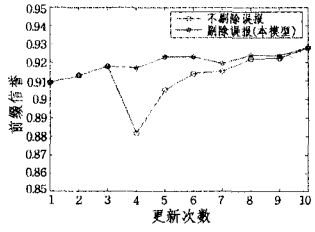

图 4 不剔除检测系统的误报导致节点前缀信誉非正常降低

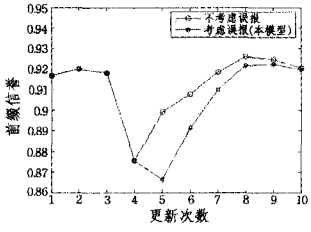

图 5 不考虑检测系统的漏报导致节点前缀信誉非正常升高

结束语 BGP 域间路由系统是互联网的核心基础设施。BGP 面临的前缀劫持攻击会大幅降低互联网网络的可靠性。本文通过评估自治系统真实前缀路由行为的信任度,使自治系统可选择相对信誉好的自治系统发起的前缀路由通告,以抑制前缀劫持攻击的发生,保护域间路由系统的安全。

参 考 文 献

[1] Rekhter Y, Li T, Hares S. A Border Gateway Protocol 4 (BGP-4)[R]. RFC 4271, Jan. 2006

[2] Nordstrom O, Dovrolis C. Beware of BGP attack[J]. ACM Computer Communications Review, 2004, 34(2): 1-8

[3] Mather T, Kumaraswamy S, Latif S. 云计算安全与隐私[M]. 刘戈舟,杨泽明,刘宝旭,译. 北京:机械工业出版社,2011:43-45

[4] Murphy S. BGP security vulnerabilities analysis[R]. RFC 4272. Jan. 2006

[5] Chinese ISP hijacks the Internet[EB/OL]. http://bgpmon.net/blog/?p=282

[6] Pakistan hijacks Youtube[EB/OL]. http://www.renesys.com/blog/2008/02/pakistan_hijacks_youtube_1.shtml

[7] Anirudh R, Nick F. Understanding the network-level behavior of spammers[C]// ACM SIGCOMM. Pisa, Italy: ACM, 2006: 291-302

[8] The relationship between network security and spam[EB/OL]. NANOG 29 Meeting: http://www.nanog.org/mtg-0310/spam.html

[9] Kalafut A J, Shue C A, Gupta M. Malicious hubs: detecting abnormally malicious autonomous systems[C]// IEEE INFOCOM. San Diego, CA, USA, 2010: 1-5

[10] Oorschot P C V, 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): 11-46

[11] Kent S, Lynn C, Seo K. Secure Border Gateway Protocol (Secure-BGP)[J]. IEEE Journal on Selected Areas in Communications, 2000, 18(4): 582-592

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

[13] 王娜,张建辉,马海龙,等. 基于前缀分配路径长度的 BGP 源自治系统验证机制[J]. 电子学报,2009,37(10):2220-2227

[14] 刘欣,朱培栋,彭宇行. Co-Monitor:检测前缀劫持的协作监测机制[J]. 软件学报,2010,21(10):2584-2598

[15] Zhang Z, Hu Y C, Mao Z M, et al. Ispy: detecting ip prefix hijacking on my own[J]. SIGCOMM Comput. Commun. Rev., 2008, 38(4): 327-338

[16] Signanos G, Faloutsos M. Neighborhood watch for Internet routing: Can we improve the robustness of Internet routing today? [C]// IEEE INFOCOM. Washington, USA: IEEE Computer Society Press, 2007: 1271-1279

[17] Lad M, Massey D, Pei D, et al. PHAS: A prefix hijack alert system[C]// the 15th conference on USENIX Security Symposium. Volume 15. Vancouver, BC, Canada: USENIX Association, 2006

[18] Goldberg S, Schapira M, Hummon P, et al. How secure are secure interdomain routing protocols [J]. SIGCOMM Comput. Commun. Rev., 2010, 40(4): 87-98

[19] Kent S, Lynn C, Mikkelson J, et al. Secure Border Gateway Protocol (Secure-BGP) -real world performance and deployment issues[C]// Symposium on Network and Distributed System Security (NDSS' 00). San Diego, CA, 2000: 103-116

[20] Zhang Z, Zhang Y, Hu YC, et al. Practical defenses against BGP prefix hijacking[C]// the 2007 ACM CoNEXT Conference. New York, USA: ACM, 2007: 1-12

[21] Zhang M, Liu B, Zhang B. Safeguarding data delivery by decoupling path propagation and adoption[C]// IEEE INFOCOM 2010. San Diego. CA, USA: IEEE Press, 2010: 1-5

[22] 贺利坚,黄厚宽. MAS 中信任和信誉系统的研究进展[J]. 计算机科学,2011,38(4):1-8

[23] 卢锡城,赵金晶,朱培栋,等. 域间路由系统自组织特性[J]. 软件学报,2006,17(9):1922-1932

[24] 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[J]. 软件学报,2010,21(3):505-515

[25] Yu H, Rexford J, Felten EW. A Distributed reputation approach to cooperative Internet routing protection[C]// Secure Network Protocols, 2005 (NPSec). 1st IEEE ICNP Workshop on. Boston: IEEE Press, 2005: 73-78

[26] Rantala P, Virtanen S, Isoaho J. Hybrid trust model for Internet routing[J]. International Journal of Computer Networks & Communications (IJCNC), 2011, 3(4): 1-12

[27] 谭晶,罗军舟,李伟,等. 基于可信度的域间路由机制[J]. 计算机学报,2010,33(9):1763-1774

[28] Chang J, Venkatasubramanian KK, West AG, et al. AS-CRED: reputation service for trustworthy inter-domain routing[R].

MS-CIS-10-17. University of Pennsylvania, 2010

[29] Chang J, Venkatasubramanian K K, West A G, et al. AS-TRUST: a trust characterization scheme for autonomous systems in BGP[R]. MS-CIS-10-25. University of Pennsylvania, 2010

[30] Short-Lived Prefix Hijacking on the Internet[EB/OL]. http://www.nanog.org/mtg-0602/pdf/boothe.pdf

[31] Ratul M, David W, Tom A. Understanding BGP misconfiguration[C]// ACM SIGCOMM. Pittsburgh. Pennsylvania, USA: ACM, 2002: 3-16

[32] Josang A, Ismail R. The beta reputation system[C]// the 15th Bled Electronic Commerce Conference. Bled, 2002: 1-14

[33] RouteViews [EB/OL] http://www.routeviews.org/

[34] The SSFNET Project[EB/OL]. http://www.ssfnet.org

[35] BRITE topology generator[EB/OL]. http://www.cs.bu.edu/brite/

(上接第 50 页)

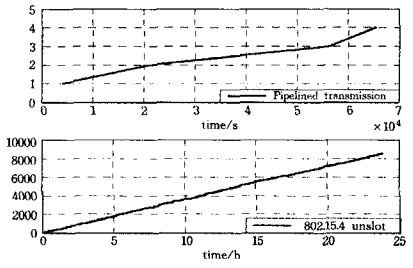

图 10 mac 层重传次数

从图 11 中可以看出，采用 IEEE 802.15.4 非时隙 CSMA/CA 平均每轮需要进行约 60 次重传，而采用流水线式的传输方式通过在时间上规避竞争及隐藏终端，在整个过程中(共 47520 次有效传输)只使用了 4 次重传，验证流水线式的传输方式能够极大地改善输电线路监测应用中的隐藏终端。

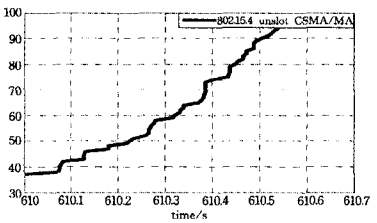

图 11 某一轮数据收集时 mac 层重传次数的情况

结束语 本文首先分析在面向输电线路在线监测应用中部署无线传感器网络对通信的需求，以及由于应用的特殊性给无线传感器网络带来的特点，根据这些特点提出了一系列的传输协议来优化传输性能并解决这些特点带来的问题(如隐藏终端)。在 MAC 层，为了应对应用中网络流量在不同时期呈现不同特征，采用了一种混合的 MAC 协议：在空闲时期采用基于 X-MAC 的 MAC 协议，并且不同角色的节点采用不同的 MAC 参数来节省能量，以满足一定网络实时性的要求；在繁忙时期采用了流水线式的传输调度方法来解决隐藏终端的问题。仿真结果表明这些方法都达到了其设计要求。在将来的工作中，还将在此基础上研究无线传感器网络针对舞动传感器、网络 trace back 数据等大流量数据的实时高效传输。

参 考 文 献

[1] Yi Y, Lambert F, Divan D. A Survey on Technologies for Implementing Sensor Networks for Power Delivery Systems[C]// Power Engineering Society General Meeting. Florida USA, 2007: 1-8

[2] Gungor V C, Lambert F C. A survey on communication networks for electric system automation[J]. Comput. Netw., 2006, 50(7): 877-897

[3] Leon R A, Vittal V, Manimaran G. Application of Sensor Network for Secure Electric Energy Infrastructure[J]. IEEE Transactions on Power Delivery, 2007, 22(2): 1021-1028

[4] Jawhar I, Mohamed N, Agrawal D P. Linear wireless sensor networks: Classification and applications[J]. Journal of Network and Computer Applications, 2011, 34(5): 1671-1682

[5] 程真，李腊元，杨少华，等. 基于带状区域路由的无线传感器网络 QoS 协议[J]. 计算机科学，2010，37(2)：4

[6] 吴华君，张自力，李卫. 一种适用于煤矿井下无线传感网的能量均衡路由协议[J]. 计算机科学，2011，38(4)：146-150

[7] Zhang H, Shen H, Tian H. Reliable and real-time data gathering in multi-hop linear wireless sensor networks[J]. Wireless Algorithms, Systems, and Applications, 2006: 151-162

[8] Karveli T, Voulgaris K, Ghavami M, et al. A Collision-Free Scheduling Scheme for Sensor Networks Arranged in Linear Topologies and Using Directional Antennas[C]//Sensor Technologies and Applications, 2008. SENSORCOMM '08. Second International Conference. 2008: 18-22

[9] De Caneva D, Montessoro P L. A Synchronous and Deterministic MAC Protocol for Wireless Communications on Linear Topologies[J]. Int'l J. of Communications, Network and System Sciences, 2010, 3(12): 925-933

[10] Wei Y, Heidemann J, Estrin D. An energy-efficient MAC protocol for wireless sensor networks[C]// INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE, 2002, 3: 1567-1576

[11] Dam T V, Langendoen K. An adaptive energy-efficient MAC protocol for wireless sensor networks[C]// Proceedings of the 1st International Conference on Embedded Networked Sensor Systems. Los Angeles, California, USA, 2003: 171-180

[12] Ganeriwal S, Tsigkogiannis I, Shim H, et al. Estimating clock uncertainty for efficient duty-cycling in sensor networks[J]. IEEE/ACM Trans. Netw., 2009, 17(3): 843-856

[13] Buettner M, Yee G V, Anderson E, et al. X-MAC: a short preamble MAC protocol for duty-cycled wireless sensor networks [C]// Proceedings of the 4th International Conference on Embedded Networked Sensor Systems. Boulder, Colorado, USA, 2006: 307-320

[14] Pakzad S N, Fenves G L, Kim S, et al. Design and implementation of scalable wireless sensor network for structural monitoring[J]. Journal of infrastructure systems, 2008, 14(89)