

网络、通信、安全

利用 Sybil 攻击提升 PageRank 值

张大陆, 陈 晴, 胡治国

ZHANG Da-lu, CHEN Qing, HU Zhi-guo

同济大学 电信学院 计算机科学与技术系, 上海 201804

Department of Computer Science, Tongji University, Shanghai 201804, China

E-mail: Daluz@acm.org

ZHANG Da-lu, CHEN Qing, HU Zhi-guo. Using Sybil attack to optimize PageRank. Computer Engineering and Applications, 2008, 44(19): 96-97.

Abstract: PageRank, as the most important reputation ranking factor of Google, is prone to Sybil attack as recently research results prove. A higher ranking may offer an economic benefit. Based on some convenient efforts on finding the best Sybil strategy to manipulate PageRank on its simplest version, the paper focuses on how to use strategy to optimize PageRank into its aimed ranking. Pay attention that the optimization work is done simulative without consideration for complex network environment, so it would still be far away to put such strategy into actual implementation, which is also the future work.

Key words: Sybil; PageRank; reputation system

摘要: 最近的研究证明 Google 的页面等级策略 PageRank 容易受到 Sybil 攻击。着眼于对如何构造 Sybil 攻击来优化 PageRank 值。提出了构造 Sybil 攻击的策略模型, 考虑节点生成成本和迭代收敛性的前提下, 证明了攻击的有效性。最后在模拟环境下对攻击进行了量化分析。

关键词: 女巫攻击; 页级; 信任系统

DOI: 10.3778/j.issn.1002-8331.2008.19.028 文章编号: 1002-8331(2008)19-0096-02 文献标识码: A 中图分类号: TP393.08

1 引言

虚拟环境阻碍了用户直接了解远程实体的物理特性。作为一种替代方法, 用户只能通过表示实体信息抽象的身份来了解它。在网络中, 一个恶意节点通过模拟其他节点或只是简单使用虚假身份来使自己对外呈现为多个节点被称为 Sybil 攻击。

Sybil 攻击在 Douceur^[1]中首次被提到。E.St 和 R.Morris 也在他们的点对点分布式哈希表的安全性考量一文中指出, 一个安全的身份配方法应使得一个节点无法任意选择它的节点标识即身份。Castro 等人^[2]也认为对一个 P2P 网络来说, 防御 Sybil 攻击最根本的是节点身份的统一分发不能被攻击者控制。他们提出基于可信的权威中心进行 ID 分配的解决方案。同时, Srivatsa 和 Liu^[3]也在基于外部 ID 的正式模型中定义了一个 ID Mapping 方案可以部分防御 Sybil 攻击。

当大部分的研究者将他们的对 Sybil 的分析研究工作都集中在身份分配方案上时, A.Cheng^[4]提出对称的信任系统更容易被 Sybil 攻击。他提出许多等级系统容易被用户操控, 并且用户经常有欺骗的动机, 即在系统中获得更高信用等级。因为一个更高的等级意味着更高的经济利益。在对 ebay 信任系统的研究中也发现, 购买者宁愿去多支付 8% 的额外费给高信用的卖家。

Google 搜索引擎中使用 PageRank 进行等级评定, 它能够

帮助用户更快的了解万维网的异质性。PageRank 基于一个网络图来计算每个网页的等级, 这种方法也可以应用在 P2P 网络中。虽然 PageRank 已经被证明是一个十分有效的等级评定系统, 但它也易于被各种攻击策略如共谋或 Sybil 的操控^[5]。

2 定义

给定一个集合 V , 用有向图 $G=(V, E)$ 其中边界集合 E 代表用户之间的直接信任关系。例如, 在网络中, 一个边界 (v, u) 代表从节点 v 出发到节点 u 的向外链接, 那么假定 F_u 是 u 所指向的集合, B_u 是指向 u 的集合, u 的链接数 $N_u=|F_u|$, c 是一个正常化因子。

2.1 PageRank 算法

Lawrence Page 和 Sergey Brin 提出了用户行为的随机冲浪模型, 来解释上述算法。他们把用户点击链接的行为, 视为一种不关心内容的随机行为。而用户点击页面内的链接的概率, 完全由页面上链接数量的多少决定的。一个页面通过随机冲浪到达的概率就是链入它的别的页面上的链接的被点击概率的和。 c 可以视为用户无限点击下去的概率, $(1-c)$ 则就是页面本身所具有的网页级别。

在网络图 G 中 PageRank 的值由在图中随机步进的概率决定。在图中用 c 表示从节点 u 沿 u 的向外链接边界集以概率

基金项目: 国家自然科学基金 the National Natural Science Foundation of China under Grant No.90204010。

作者简介: 张大陆 (1949-), 男, 博士生导师, 主要研究领域为网络安全、语义网; 陈晴 (1982-), 女, 硕士, 主要研究领域为网络安全。

收稿日期: 2007-12-24 修回日期: 2008-02-29

$1/N_s$ 选择边界步进。这样可计算得出 PageRank 的值:

$$PR_{ij} \in 1-d + c \sum_{v \in B_i} \frac{PR_v}{N_v} \quad (1)$$

2.2 策略模型

正如图 1 和图 2 所示, 黑色节点表示正是提升 PageRank 的目标节点, 白色节点是 Sybil 节点。目标页 p 个出链接 (向外界) 和 q 个入链接 (向内边界)。假定目标节点的入链接的 PageRank 分别是 $r_1, r_2, r_3, \dots, r_q$ 。可以证明, 当一个 Sybil 节点插入中时, 节点的数量, 链接中出链接及入链接是影响提升 PageRank 值的关键因素。

因为 Sybil 攻击的系统稳定性和不可侦测性, 现确保在攻击时使目标节点的出链接和入链接数目保持稳定, 使得在其他节点不能感知到目标节点的任何变化的同时, 优化 PageRank 值。因此, 评估策略必须考虑到生成 Sybil 节点的代价和迭代计算中 PageRank 的收敛性。



图 1 原形模型

图 2 目标模型

3 Sybil 策略内部构造

已经在前期的研究中证明, Sybil 策略的内部构造和最终优化结果有关。根据本文的研究结果, 如果 Sybil 的数量是 m, 那么目标节点所能提升的 PageRank 的值为 $PR_{ij}^j, 1 \leq i \leq m, 1 \leq j \leq n$, 请注意 i 在第 j 次的迭代。

$$PR_{ij}^j \in 1-d + c PR_{ij}^j (m+p)$$

$$PR_{ij}^j \in 1-d + c (r_1 + r_2 + \dots + r_q + PR_{i1}^j + PR_{i2}^j + \dots + PR_{in}^j) =$$

$$(1-d) + c \sum_{k=1}^q k + \sum_{i=1}^m PR_{ij}^j$$

第 1 次迭代:

$$PR_{ij}^1 \in 1-d; PR_{ij}^1 \in 1-d + c \sum_{k=1}^q r_k$$

第 2 次迭代:

$$PR_{ij}^2 \in 1-d + c ((1-d) + c \sum_{k=1}^q r_k) (m+p) = (1-d) + c (1-d) (m+p) + c^2 \sum_{k=1}^q r_k (m+p)$$

$$c^2 \sum_{k=1}^q r_k (m+p)$$

$$PR_{ij}^2 \in 1-d + c \sum_{k=1}^q k + m ((1-d) + c (1-d) (m+p) + c^2 \sum_{k=1}^q r_k) /$$

$$(m+p)) \in 1-d + c \sum_{k=1}^q k + c (1-d) m + c^2 (1-d) m (m+p) +$$

$$c^2 \sum_{k=1}^q r_k m (m+p)$$

第 3 次迭代:

$$PR_{ij}^3 \in 1-d + c ((1-d) + c (1-d) m + c^2 (1-d) m (m+p) +$$

$$c \sum_{k=1}^q k + c^2 \sum_{k=1}^q r_k m (m+p)) (m+p) \in 1-d + c (m+p) (((1-d) +$$

$$+ c (1-d) m + c^2 (1-d) m (m+p) + c \sum_{k=1}^q k + c^2 \sum_{k=1}^q r_k m (m+p))) \in 1-d +$$

$$c (1-d) (m+p) + c^2 (1-d) m (m+p) + c^2 (1-d) m (m+p)^2 + c^2 \sum_{k=1}^q r_k /$$

$$(m+p) + c^2 \sum_{k=1}^q r_k m (m+p)^2$$

$$PR_{ij}^3 \in 1-d + c \sum_{k=1}^q k + m ((1-d) + c (1-d) (m+p) + c^2 (1-d) m ($$

$$(m+p) + c^2 (1-d) m (m+p)^2 + c^2 \sum_{k=1}^q r_k (m+p) + c^2 \sum_{k=1}^q r_k m (m+p)^2) =$$

$$(1-d) + c (1-d) m + c^2 (1-d) m (m+p) + c^2 (1-d) m^2 (m+p) + c^2 (1-d) m^2 /$$

$$(m+p)^2 + c \sum_{k=1}^q k + c^3 \sum_{k=1}^q k m (m+p) + c^2 \sum_{k=1}^q r_k m^2 (m+p)^2$$

第 4 次迭代:

$$PR_{ij}^4 \in 1-d + c \sum_{k=1}^q k + c (1-d) m + c^2 m ((1-d) + c \sum_{k=1}^q k + c (1-d) m +$$

$$c^2 (1-d) m (m+p) + c^2 (1-d) m^2 (m+p) + c^3 \sum_{k=1}^q k m (m+p) + c^2 (1-d) m^2 /$$

$$(m+p)^2 + c^2 \sum_{k=1}^q r_k m^2 (m+p)^2) (m+p) \in 1-d + c (1-d) m + c^2 (1-d) m /$$

$$(m+p) + c^2 (1-d) m^2 (m+p) + c^2 (1-d) m^2 (m+p)^2 + c^2 (1-d) m^2 (m+p)^2 +$$

$$c^2 (1-d) m^2 (m+p)^3 + c \sum_{k=1}^q k + c^3 \sum_{k=1}^q k m + c^2 \sum_{k=1}^q k m^2 (m+p)^2 + c^2 \sum_{k=1}^q r_k m^2 /$$

$$(m+p)^3; \dots$$

$$PR_{ij}^n \in 1-d + c \left(\sum_{t=0}^{n-1} c^{2t} m^t (m+p)^t + \sum_{t=1}^{n-1} c^{2t+1} m^{t+1} (m+p)^t \right) +$$

$$\sum_{k=1}^q k \left(\sum_{t=1}^n c^{2t-1} m^t (m+p)^t \right)$$

显然, PageRank 通过 Sybil 策略可以成功被提升。在另一篇文章中提出其他方案来改进该策略。

4 模拟和结果评估

本章通过模拟实验来评估本文的 Sybil 策略。模拟模型有 20 个入链接, 每一个节点的默认 PageRank 被设定为 1。比较在使用 Sybil 策略前后的 PageRank。策略模型如图 3 所示, Sybil 节点的出链接和入链接同时作用于目标节点。计算 PageRank 的迭代数设为 100, 如图 4 所示, 能够发现目标节点 PageRank 值被成功提高了近 2 倍。

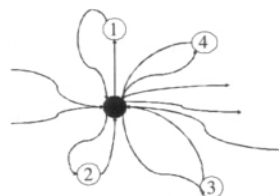


图 3 具有 4 个 Sybil 节点的模型

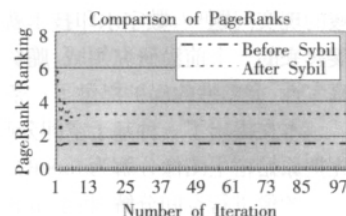


图 4 模拟实验结果

5 结论

本文的研究是基于 PageRank 的现行算法, 利用 Sybil 攻击来优化 PageRank 值。必须指出的是, 本文优化策略已经在模拟环境中被证实是有效的, 但本文研究成果还不能直接应用于真实的网络环境中。后期的研究工作包括在实际网络中实现

(下转 108 页)

MOSRA、WSP、BSP 算法所选路径的最大带宽利用率都在不断增大,但 MOSRA 算法所选路径的最大带宽利用率小于 WSP 算法和 BSP 算法的值,此结果表明, MOSRA 算法在优化其他目标和满足约束情况下,所选路径的带宽更符合此刻网络负载的要求,因此更不容易引起网络阻塞。图 9 表明,第一等级流到达时, MOSRA 算法所选路径占用的公用缓冲池带宽比率小或不弱于 WSP 算法和 BSP 算法的值,表明 MOSRA 算法在高服务业务到达时,更少的占用低优先级带宽的公共缓冲池,这样就公平使用网络资源,有效的避免“类间效应”^[12]和均衡网络负载。仿真结果图 10~图 12 表明,在网络安全参数发生多次改变时, MOSRA 算法所选路径的三类安全度量数值都明显小于 WSP、BSP 算法所选路径的安全度量值,表明 MOSRA 算法所选路径整体安全性能更高。综上所述,在存在多优化目标和多约束条件下,本文提出的 MOSRA 算法较 WSP、BSP 算法引起网络阻塞更小,能更公平使用网络资源。同时,能够选择一条符合安全性能要求的可行路,所选的可行路安全性能明显优于上述传统算法。

5 结束语

安全路由是一个有价值和挑战性的研究课题,将安全度量引入 QoS 框架是安全路由研究的一个新思路。在已有的安全度量研究中,大多仅仅侧重于一种策略或目标对安全进行简单度量,或者对安全度量进行简单定性的描述。本文根据网络安全服务的要求,通过对链路安全进行多重量化和定义,把这些安全度量引入 QoS 框架,和常规的 QoS 参数一块作为路由选择依据,形成多目标多约束模型;并且基于区分服务模型提出了多目标最优化安全路由算法(MOSRA)。结果表明,此方法明显的提高了路由选择的安全性能。同时,为用户提供不同等级要求的服务质量,有效地提高了网络资源利用率,平衡了网络负载,减少了网络拥塞。因此,是一种具有实际意义的多目标最优化安全路由算法。

参考文献:

- [1] Duflos S, Gay V, Kervella B, et al. Integration of security parameters in the service level specification to improve QoS management of secure distributed multimedia services[C]//Proceedings of the 19th International Conference on Advanced Information Networking and Applications, 2005, 2: 145-148.
- [2] Sakarindr P, Ansari N, Rojas-Cessa R, et al. Security-enhanced quality of service (SQoS): a network analysis[C]//Military Communications Conference, 2005, 4: 2165-2171.
- [3] Lindskog S, Jonsson E. Adding security to quality of service architectures[C]//Proceedings of the SSGRR Conference, 2002.
- [4] Naqvi S, Riguidel M. Quantifiable security metrics for large scale heterogeneous systems[C]//Proc of 40th IEEE International, 2006: 209-215.
- [5] Pamula J, Ammann P. A weakest-adversary security metric for network configuration security analysis[C]//Proceedings of the 2nd ACM Workshop on Quality of Protection, Alexandria, Virginia, USA, 2006, 31-38.
- [6] Alkhatmi, Woodward M E. The analytic hierarchy process applied to best effort QoS routing with multiple metrics: a comparative evaluation[C]//5th European, Personal Mobile Communications Conference, 2003: 539-544.
- [7] Almerhag I A, Woodward M E. Security as a quality of service routing problem[C]//Proceedings of the 2005 ACM Conference on Emerging Network Experiment and Technology, 2005: 222-223.
- [8] Kalyanmoy D. A fast and elitist multiobjective genetic algorithm: NSGA- [J]. IEEE Trans on Computation, 2002, (2): 182-197.
- [9] Baltatu M, Liyo A, Maino F. Security issues in control, management[C]//TERENA Networking Conference, 2000: 22-25.
- [10] Goncalves M. Firewalls complete[EB/OL] (2002-10-16). http://www.secinf.net/firewalls_and_VPN/Firewalls_Complete.
- [11] Almerhag I A, Woodward M E. Key length as a QoS routing metric[C]//Proc of Sixth Informatics Workshop, 2005: 23-24.
- [12] 沈晶. 以流量工程和服务质量控制为目标的高性能路由技术[D]. 杭州: 浙江大学, 2003.
- [13] Zegura E W, Calvert K L, Donahoo M J. A quantitative comparison of graph-based models for Internet topology[J]. IEEE/ACM Trans on Networking, 1997, (6): 770-783.
- [14] 张宇, 张宏莉. Internet 拓扑建模综述[J]. 软件学报, 2004, 15(8): 1220-1226.
- [15] Ma Q, Steenkiste P. On path selection for traffic with bandwidth guarantees [C]//Proc of 5th IEEE International Conference on Network Protocols, Atlanta, GA, 1997, (1): 191-202.

(上接 97 页)

Sybil 攻击。另一方面,这些攻击方案如果被恶意攻击者滥用,它也会带来许多更为复杂和不可预知的问题,会在以后的研究中对其进行深入的研究。

参考文献:

- [1] Douceur J R. The Sybil attack[C]//Proc for the 1st International Workshop on Peer-to-Peer Systems, Cambridge, Massachusetts, 2002.
- [2] Castro M, Druschel P, Ganesh A, et al. Secure routing for structured peer-to-peer overlay networks[C]//Proc of the 5th USENIX Symposium on Operating System Design and Impl, Boston, MA, USA, 2002.
- [3] Srivatsa M, Liu L. Vulnerabilities and security threats in structured overlay network: a quantitative analysis[C]//Proceedings of 20th Annual, Computer Security Application Conference, 2004: 252-261.
- [4] Cheng A, Frieman E. Manipulability of PageRank under Sybil strategies[C]//Proc of First Workshop on the Economics of Networked Systems, 2006.
- [5] Cheng A, Fridman E. Sybilproof reputation mechanisms[C]//Proc of the 2005 ACM SIGCOM Workshop on Economics of Peer-to-Peer Systems, 2005: 128-132.
- [6] Page L, Brin S. PageRank, an eigenvector based ranking approach for hypertext[C]//21st Annual ACM/SIGR International Conference on Research and Development in Information Retrieval, Melbourne, Australia, 1998.