一种基于蚁群算法的Sybil攻击防御

王 峰 李 亚 朱 海 王迤然

(周口师范学院计算机科学与技术学院 周口 466001)

摘 要 由于结构化对等网络管理的非集中性、参与者参与系统的自由性,使得Sybil攻击成为其所面临的特有的安全威胁。通过对当前Sybil攻击防御的文献综述,得出利用社交网络解决Sybil攻击防御具有良好的前景。利用社交网络,结合蚁群算法解决NP难问题的优势,提出了一种基于蚁群算法的Sybil攻击防御模型ASDM以及相关算法。实验表明,ASDM能有效地识别出Sybil结点。

关键词 Sybil攻击,对等网络,蚁群算法,社交网络

中图法分类号 TP393 **文献标识码** A

Sybil Attack Defense Based on Ant Colony Algorithm

WANG Feng LI Ya ZHU Hai WANG Yi-ran

(School of Computer Science and Technology, Zhoukou Normal University, Zhoukou 466001, China)

Abstract In the structured peer to peer networks, non concentration of management and the freedom of participants involving the system make the Sybil attack becomes a special security threat which faces. By reviewing and studying the current Sybil defense, the social network which defenses Sybil attacks has good prospects. Using social network, combining ant colony algorithm to solve NP problem, an ant colony algorithm based on Sybil attack defense model ASDM and the related algorithm was presented. The experimental results show that the ASDM can effectively identify the Sybil node.

Keywords Sybil attack, P2P network, Ant colony algorithm, Social network

随着结构化对等网络的广泛应用,其安全问题也逐渐引起人们的重视。结构化的对等网络以DHT技术为主,主要通过对结点IP(或者其他关键子)进行HASH运算生成标识符ID,然后将〈ID,IP〉信息对存储在相应的结点上来构造分布式路由表。结构化对等网络最大的优势在于其管理的非集中性、会员参与的自由性,而正是这些特性给对等网络的应用带来了一些特有的安全问题。文献[4]指出基于DHT的结构化对等网络针对安全攻击的防御比较困难,目前典型的攻击有:(1)Sybil攻击;(2)Eclipse攻击;(3)寻径攻击、存储攻击。本文主要讨论Sybil攻击的防御。文献[1]指出在对等网络中,一些恶意用户获取多个结点身份,假装成多个不同的结点,这些虚假的结点称为Sybil结点。文献[2]指出结构化的对等网络容易遭受Sybil攻击。文献[4]指出一旦攻击者控制了较多的Sybil结点,他就可以击败任何针对节点失败的安全防御。

文献[8]Castro等于2002年指出防御Sybil攻击可行的方法是采用可信中心来验证结点标识与现实结点身份的方法。但其不适合CAN,此外基于IP的结点标识生成规则面临着如何穿越防火墙的问题。Dinger and Hartenstein[9]提出了分布式的结点注册方法,其只能在一定程度上抵御Sybil攻击。Wang等[10]通过对等网络的实际的物理特征来检验结点,但是网络的动态性变化可能导致这种识别的失败。Borisov[12]提出了一种通过强制结点耗费计算资源来解决数学难题的来以验证结点,但是计算的难度不好选择,文献[3]中Yu等提出一种基于社交网络的分布式协议,基于社区检测的方法能有效地限制Sybil攻击对对等网络的影响。文献[11]中Yu等对该协议进行了改进。文献[5,7]指出利用社交网络防御Sybil结点攻击是不错的选择。文献[6]提出利用社交网络来构造安全的路由表的机制。

1 相关工作

在对等网络中,我们约定恶意攻击者生成的虚假的结点为Sybil结点或者恶意结点,未知的结点为可疑结点,可信的结点为好结点。同时将结点之间可以通过电话等方式建立的信任关系称为信任边,恶意结点通过欺骗手段与好结点建立起来的信任关系称为攻击边,如图1所示。

文献[3]指出可以利用对等网络上已经建立的社交网络进行Sybil攻击防御,同时指出社交网络具有高度融合性,最大融合时间为$W(\log n)$跳。如图1所示,社交网络中可信结点间联系紧密,构成可信社区,Sybil结点联系紧密,构成恶意

到稿日期:2012-08-20 返修日期:2012-11-2 本文受国家"973"重点资助项目(2002CB312105),国家自然科学基金项目(61103143),河南省高校科技创新人才支持计划项目(2012HASTIT032),河南省科技厅基础与前沿技术研究计划项目(112300410307)资助。

王 峰(1981-),男,硕士生,主要研究方向为网络与信息安全,E-mail:wang7984@163.com;李 亚(1973-),男,硕士生,副教授,主要研究方向为网络与信息安全;朱 海(1978-),男,硕士生,主要研究方向为云计算、信息安全;王迤然(1976-),男,硕士生,主要研究方向为网络与信息安全。

社区，可信社区与恶意社区间通过较少的边进行联系，这些就是攻击边，攻击边即是网络的 shortcut。在整个网络如果能有效地找出攻击边就能有效限制 Sybil 攻击。我们会发现这是一个 NP 难的问题。然而大多数基于社交网络的 Sybil 攻击防御研究并没有尝试解决寻找攻击边的问题，而是依据社交网络的高度融合性来对整个网络做宏观划分，将其划分成可信社区和恶意结点构成的恶意社区。划分的过程如下：当一个可疑结点向好结点请求服务时，好结点和可疑结点同时执行类似于随机游走的算法，均执行 W 跳，然后判断好结点的多条路径和可疑结点的多条路径之间是否存在多条路径交叉，以此判别好结点和可疑结点是否在一个社交网络中。如果存在多条路径交叉，依据社交网络的高度融合性可知，好结点和可疑结点在一个社区中，则好结点信任该可疑结点。然而这种划分法也有不足之处，并不能准确有效地找出攻击边，也就决定了所进行的社区划分没有精确的定量分析。本文在利用社交网络技术的基础上，结合蚁群算法[13]解决 NP 难问题的优势，提出一种新的防御 Sybil 攻击方法：基于蚁群算法的 Sybil 攻击防御方法。

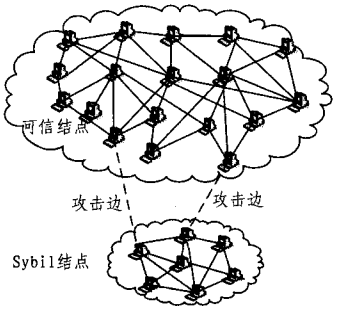

图 1　结构化对等网络的结构图

2　基于蚁群的 Sybil 攻击防御模型 ASDM

2.1　模型的防御思想及流程

在我们的系统中，要求每个结点必须产生一对密钥，包括私钥和公钥，此外结点保存自己的私钥，在访问过的结点上留下自己的公钥，以便别的结点验证其确实访问过。在信任边的两端结点上均保存一个共享密钥作为进入该信任边的凭借。基于蚁群的 Sybil 攻击防御模型如图 2 所示：当结点 A 访问结点 B 时，如果 A 和 B 通过社区关系建立的有信任关系，则 A 和 B 之间通过共享的密钥建立起信任边。否则 A 和 B 没有信任边，B 必须对 A 进行认证，即 A 发起寻径目标为 B 的寻径任务，采用一种特殊的蚁群算法进行寻径。最后可信结点根据蚁群寻径的结果对可疑结点进行认证。

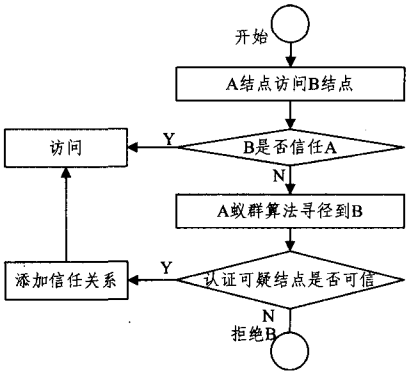

图 2　基于蚁群的 Sybil 攻击防御模型 ASDM

2.2　模型的数据结构

依照模型的工作流程，模型需要维护以下几个数据结构，蚂蚁数据结构 Ant 以及结点上数据结构：信息素表的数据结构 SPTable。下面是对以上数据结构的描述。

2.2.1　Ant 的数据结构

在 Ant 中，SNnum 是每次寻径的任务号，可以通过真随机序列生成，保证了其不可被猜测；TarId 是寻径的目标 Id；Type 是蚂蚁的类型，当 Type 取值为 0 时表示为寻径蚂蚁，寻径蚂蚁负责寻径；当 Type 取值为 1 时表示成功蚂蚁，负责更新信息素表；路径栈 RouteLine 存储寻径蚂蚁访问过的结点信息。Ant 的数据结果如图 3 所示。

SNum	TarId	Type	RouteLine
...	...	...	.....

图 3　蚂蚁 Ant

2.2.2　SPTable 的数据结构

加入协议的每个结点需分配信息素表 SPTable 的存储空间，SPTable 如图 4 所示，采用类似邻接表的数据结构，每个头域由 3 项构成：邻居结点信息 NNode；信息素的值 Pheromone，由成功蚂蚁负责更新；Next 指针指向一个链表，链表结点项存储最近通过该边的蚂蚁的任务号 SNum。

NNode	Pheromone	Next	SNum	Next	...	...
Node1	...		...	...	...	...
Node2	...		...	...	...	...
...	...	..	...	...	..	..

图 4　信息素表 SPTable

2.3　结点的认证

可疑结点创建 N 个寻径蚂蚁，寻径结束后，若有 S 个蚂蚁寻径成功，就说明从可疑结点到可信结点之间至少有 S 条不同的路径存在，在这些路径中没有任何边是相同的，称这样的路径为独立路径。如图 1 所示，如果采用蚁群算法从 Sybil 结点区寻径到可信结点区，那么所有的独立路径都有经过攻击边，也就意味着，从 Sybil 结点到可信结点间的独立路径数和攻击边数有关。由于在真实的网络中，攻击边的数量非常有限，那么从 Sybil 结点到可信结点的独立路径边数 w 也非常有限，因此从可疑结点到可信结点间的独立路径边数越多，说明可疑结点可信度越高。此外每条独立路径的跳数越多，通过攻击边的概率就越大。故可信结点对可疑结点的认证依据为可疑结点的可信度，可信度的计算如下：

$$T=K.\ S/N+L/K\sum_{i=1}^{i=S}w_i \tag{1}$$

式中，K、L 为系数。当 $T\geqslant T_0$ 时，可信结点和可疑结点建立信任关系，T_0 为门限值，设为 0.5。

3　ASDM 的相关算法

3.1　基于蚁群算法的寻径流程图

如图 5 所示，当一个好结点对一个可疑结点进行认证时，可疑结点启动寻径任务，任务号为 SNum，生成 N 个寻径蚂蚁，每个寻径蚂蚁以好结点为目标，单独寻径。当结点收到寻径蚂蚁时，判断是否寻径成功，如寻径成功，则创建成功蚂蚁，

成功蚂蚁依据路径回溯更新各结点信息素表 SPTable 中的信息素 Pheromone 的值；否则选择本次任务没有访问过的边，且对信息素较高的边进行转发，在该边上留下任务号。如果蚂蚁到一个结点上发现所有的边都已经被该种群访问过，则寻径终止。

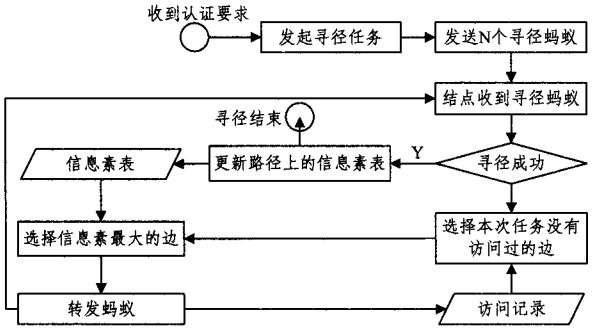

图 5　基于蚁群算法的寻径流程图

3.2　优化的蚁群的寻径算法

蚁群寻径算法的核心算法由以下 3 部分构成：

发起寻径任务

```
IF A. routing
  DO Creat SNum
  FOR t:=1 to N
  DO Creat routing-ant
     Send routing-ant
```

转发蚂蚁

```
IF Node. receive (routing-ant)
  DO node ← SPTable[1]. node
FOR t:=1 to SPTable. length
  WHILE SPTable[t]. node. next ! =null
    IF SPTable[t]. node. next. SNum==SNum
    DO t++
       BREAK
Else Node. next=Node. next. next
  IF node. Pheromone < SPTable[t]. node. Pheromone
  DO Node ← SPTable[t]. node
  ELSE t++
DO forward (ant,edge. node)
```

更新信息素表

```
IF Node. receive (success-ant)
  FOR t:=1 to ant. routeline. length
  DO update ( ant. node. SPTable. pheromone)
```

4　模拟仿真

为了综合分析 ASDM 模型参数、性能，下面进行两组仿真实验。试验硬件：Intel 酷睿双核 CPU、4G 内存；试验软件：Winxp 系统、NS2 仿真平台；在 NS2 仿真平台上产生 1000 个结点，无标度拓扑，并随机取 100 个为 Sybil 结点，且 Sybil 结点均匀分布。

试验 I：针对式(1)中的(K、L)参数进行测试分析。

首先随机地取一组可信结点和一组 Sybil 结点，然后选取可信结点，利用 ASDM 模型可信结点间的可信度。在(K，L/K)取不同数值的情况下，可信度仿真测试结果如表 1 所列。

表 1　可信结点间可信度分析结果表

K L/K	K=0.3 L/K=0.3	K=0.4 L/K=0.4	K=0.5 L/K=0.6	K=0.6 L/K=0.5	K=0.7 L/K=0.5	K=0.8 L/K=0.8
S	7	6	7	8	10	7
N	10	8	8	9	12	11
W	0.2	0.2	0.3	0.3	0.2	0.1
T	0.26	0.36	0.61	0.68	0.68	0.69

结果表明，(K，L/K)在取值(0.5，0.6)之后，可信度均在 0.5 阈值以上，且(K，L/K)取值越大，可信度越高。

最后利用 ASDM 模型测试可信结点对可疑结点的可信度。在(K，L/K)取不同数值的情况下，可信度仿真测试结果如表 2 所列。结果表明，可信结点对可疑结点的可信度随(K，L/K)增大而增大，可信度越大，说明误识别 Sybil 结点的概率越高。为此，(K，L/K)最佳取值应该在(0.6，0.5)数值附近，也就是 K=0.6，L=0.3。

表 2　可信结点对可疑结点可信度分析结果表

K L/K	K=0.3 L/K=0.3	K=0.4 L/K=0.4	K=0.5 L/K=0.6	K=0.6 L/K=0.5	K=0.7 L/K=0.5	K=0.8 L/K=0.8
S	2	2	1	2	3	2
N	10	8	8	9	12	11
W	0.2	0.2	0.3	0.3	0.2	0.2
T	0.12	0.18	0.02	0.28	0.28	0.36

试验 II　针对 ASDM 模型识别 Sybil 结点的成功率进行试验。在 ASDM 模型中设置 K=0.85，L=8，T_0=0.6。通过已存在的 Sybil 结点逐次引入 200 个新的 Sybil 结点进行 3 组仿真试验。

试验结果如图 6 所示：Y 坐标表示正确识别出 Sybil 结点的概率，X 坐标表示通过已存在的 Sybil 结点新增加 Sybil 结点的数量。通过试验表明，基于蚁群的 Sybil 结点攻击防御相比 SybilGuard[3]、SybilLimit[11] 等防御能策略，能更准确地识别 Sybil 结点。

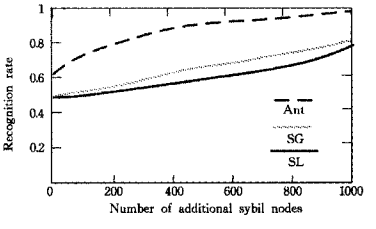

图 6　试验结果对比

结束语　通过对当前结构化对等网络所面临的安全问题进行综述分析，得出 Sybil 攻击是结构化对等网络安全所面临的一个严重威胁，结合当前主要的 Sybil 攻击防御策略，即利用社交网络来实现可信结点对可疑结点的认证，同时借鉴蚁群算法解决 NP 难问题的优势，提出了一种基于蚁群算法的 Sybil 攻击防御策略 ASD。本文的贡献在于：(1)在基于社交网络技术的基础上，首次提出利用蚁群算法来解决对可疑结点的认证。(2)本文提出的寻径算法能更有效地获得可疑结点到可信结点间的独立路径。试验表明，ASDM 在同等条件下对 Sybil 结点有着更高的识别率。

参 考 文 献

[1]　Douceur J. The Sybil attack [C]// Proceedings of the 1st International Workshop on Peer-to-Peer Systems. London, U K: Springer-Verlag, 2002: 251-260

(下转第 107 页)

可证。

4.4 协议安全性分析

端到端的安全：协议遵循远程证明思想，DRM 客户端不仅被许可证服务器验证身份，而且被验证完整性，使得 DRM 客户端平台软硬件环境安全被纳入通信安全保障边界，保证了所建立的许可证分发通道满足端到端的安全保护。

完整的认证链：协议中客户端的身份及完整性认证通过 $Cert_{enc}$ 和 $Cert_{AIK}$ 组成的证书链来保证。$Cert_{enc}$ 由一个 CA 签名，并用其公钥验证有效性。$Cert_{enc}$ 扩展项中的 TPM_CERTIFY_INFO 结构由 AIK 私钥签名，并由 AIK 的公钥进行验证，其完整性和有效性保证了 PCR 值的可信。而同时，该结构中的公钥摘要值域 pubkeyDigest 的验证又保证了主题公钥 PK_{enc} 的完整性。通过这些签名和认证，可以向对方保证平台的完整性值及用于协商的密钥都是被密封和保护在同一个 TPM 内的，是可以被信任的。

隐私的机密性：本着隐私保护的原则，协议设计中所有进行签名、加密的密钥和生成密钥的材料以及 PCR 值都被封存在 TPM 中，平台中的任何其他实体或者通信双方之外的任何第三者都不能获取或访问。而且所有的密钥操作和运算都在 TPM 内部完成，即使 DRM 控制器也只作为建立连接的门户，而不参与任何明文的存取和计算，只能获得最终共享密钥的句柄。

结束语 基于可信计算技术的 DRM 系统能更好地保护数字内容的合法、合理使用。本文首先给出了可信 DRM 系统的一般结构，并具体给出了可信计算技术在许可证分发和数字内容使用两个重要环节的应用。之后，给出了可信 DRM 系统中 DRM 客户端和许可证服务器之间的认证协议，并对其安全性进行了分析，该协议基于可信计算规范定义的带 SKAE 扩展项的证书，实现，许可证服务器对 DRM 客户端的身份认证及完整性验证，能够防止被篡改的、存在恶意软件的客户端平台连接服务器获取数字许可证的危险。在今后的工作中，DRM 客户端平台的可信度量方法以及可信 DRM 认证协议的效率改善将是进一步的研究内容。

参 考 文 献

[1] Rosenblatt W, Trippe W, Mooney S. Digital Rights Management: Business and Technology[M]. New York: M&T Books, 2002

[2] 俞银燕，汤帜. 数字版权保护技术研究综述[J]. 计算机学报，2005，28(12)：1957-1966

[3] 张志勇，牛丹梅. 数字版权管理中数字权利使用控制研究进展[J]. 计算机科学，2011，38(4)：48-54

[4] Stamm S, Sheppsrd N P. Implementing trusted terminals with a TPM and SIDDRM[C]// Proceedings of REM 2007. 2007：73-85

[5] Sadighi A R, Wolf M. Christisn stuble enabling fairer rights management with trusted computing[C]// Proceedings of ISC 2007. 2007：53-70

[6] 邱罡，王玉磊，周利华. 基于可信计算的 DRM 互操作研究[J]. 计算机科学，2009，36(1)：77-80

[7] Gallery E. Authorisation Issues for Mobile Code in Mobile Systems[D]. London: Royal Holloway, University of London, 2007

[8] Grawrock D. TCG Specification Architecture Overview Revision 1. 4[EB/OL]. https://www. trusted computinggroup. org/groups/TCG_1. 4_Archiecture_Overview. pdf, 2011-05-01

[9] Sailer R, Jaeger T, Zhang Xiao-lan, et al. Attestation-based Policy Enforcement for Remote Access[C]// Proceedings of the 11th ACM conference on Computer and communications security, CCS'04. 2004：308-317

[10] TCG Infrastructure Workgroup. Subject Key Attestation Evidence Extension Specification Version1. 0[EB/OL]. http://www. trustedcomputinggroup. org/specs/IWG/IWG _ SKAE _ Extension_1-00. pdf, 2005-06-16

[11] Housley R, Polk W, Ford W, et al. Internet X. 509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (RFC 3280)[Z]. Internet Engineering Task Force, Network Working Group, 2002

(上接第 102 页)

[2] Danezis G, Lesniewski-Laas C, Kaashoek M F, et al. Sybil-Resistant DHT Routing[C]// ESORICS. 2005

[3] Yu H, Kaminsky M, Gibbons P B, et al. SybilGuard: Defending Against Sybil Attacks via Social Networks[C]// Proc. SIGCOMM (Pisa, Italy). New York, NY: ACM Press. 2006：267-278

[4] Urdaneta G. A Survey of DHT Security Techniques[J]. ACM Computing Surveys, 2011, 43(2)：1-35

[5] Rodrigues R, Druschel P. Peer-to-Peer Systems [J]. communications of the ACM, 2010, 53(10)：72-85

[6] Lesniewski-Laas M C, Kaashoek F. Whanau: A Sybil-proof Distributed Hash Table[C]// NSDI'10 Proceedings of the 7th USENIX Conference on Networked Systems Design and Implementation. 2010

[7] Viswanath B. An Analysis of Social Network-Based Sybil Defenses[C]// SIGCOMM'10. New Delhi, India, 2010

[8] Castro M, Druschel P, Ganesh A, et al. Secure Routing for Structured Peer-to-Peer Overlay Networks[C]// Proc. 5th Symposium on Operating System Design and Implementation (Boston, MA). New York, NY: ACM Press, 2002：299-314

[9] Dinger J, Hartenstein H. Defending the Sybil Attack in P2P Networks: Taxonomy, Chal-lenges, and a Proposal for Self-Registration[C]// Proc. 1st International Conference on Availability, Reliabilityand Security (Vienna, Austria). Los Alamitos, CA: IEEE Computer Society Press, 2006：756-763

[10] Wang H, Zhu Y, Hu Y. An Efficient and Secure Peer-to-Peer Overlay Network[C]// Proc. 30th Local Computer Networks. Los Alamitos, CA: IEEE Computer Society Press, 2005：764-771

[11] Yu H, Gibbons P B, Kaminsky M, et al. SybilLimit: A Near-Optimal Social Network Defense against Sybil Attacks[C]// Proc. International Symposium on Security and Privacy. Los Alamitos, CA: IEEE Computer Society Press, 2008：3-17

[12] Borisov N. Computational Puzzles as Sybil Defenses[C]// Proc. 6th International Conference on Peer-to-Peer Computing. Los Alamitos, CA: IEEE Computer Society Press, 2006：171-176

[13] 王峰，周佳骏. 基于蚁群算法的对等网络，自适应寻径协议[J]. 计算机工程与应用，2010，17