

基于多维度的 P2P 网络信任管理机制

赵源^{1*}, 陆天波²

(1. 包头职业技术学院 计算机与信息工程系, 内蒙古 包头 014030; 2. 北京邮电大学 软件学院, 北京 100876)

(* 通信作者电子邮箱 zhaoyuan_2013@126.com)

摘要:针对分布式点对点(P2P)网络中的信任管理问题,提出了一种多维度的信任管理机制。它运用直接信任评估和间接信任评估方法,依据各用户的行为来判定系统中用户的可信任程度,从而避免因恶意用户的恶意反馈对网络造成的负面影响。在 Bad Mouthing 和 on-off 攻击场景下与 EigenTrust 方法进行对比,所提出的方法取得了较好的有效传输率(SRT),表明该机制能够有效地抑制恶意用户的行为。

关键词:网络安全;点对点网络;信任管理;信任评价;攻击场景

中图分类号: TP309.2 **文献标志码:** A

Multi-dimensional trust management mechanism for peer-to-peer networks

ZHAO Yuan^{1*}, LU Tianbo²

(1. Department of Computer and Information Engineering, Baotou Vocational and Technical College, Baotou Nei Mongol 014030, China;

2. School of Software Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China)

Abstract: Concerning the trust management in Peer-to-Peer (P2P) networks, a multi-dimensional trust management mechanism was put forward. It utilized direct and indirect trust evaluation methods to determine the trust degree of trusted users in the system according to each user's behavior, so as to prevent malicious users from the negative impact caused by malicious feedback on the network. Compared with the EigenTrust in Bad Mouthing and on-off attack scenarios, the proposed method got a higher Success Rate of Transmission (SRT). The simulation results show that the mechanism can effectively inhibit the malicious user behavior.

Key words: network security; Peer-to-Peer (P2P) network; trust management; trust evaluation; attack scenario

0 引言

在点对点(Peer-to-Peer, P2P)网络中,当出现了某些具有恶意意图的节点时情况就会变得非常不乐观。例如,用户之间相互信任的降低会导致整个网络服务质量的恶化^[1-3]。为了防止这些恶意威胁,业界已经深入研究了在人类社会普遍存在的信任关系评估方法,并试图将其很好地引入到计算机网络中进行推广使用^[4-14]。然而,现有研究只是试图分辨哪些恶意用户在共享相同资源,并没有考虑如何根据具体的威胁来给出一个信任评估以及如何保证该信任评估的信任值本身的合理性。此外,他们的研究在区分恶意用户方面还不是很清楚,无法进行有效区分。

基于上述情况,本文提出一个对抗恶意节点攻击的信任管理方案。所提方案采用了时间衰减函数以更多反映节点近期而不是过去的信任行为;并且,它还利用可信性以及该用户之间的相似性有效地反映相邻节点所提供的信任值。

1 相关工作

1.1 针对信任评估的攻击类型

Bad Mouthing、on-off、sybil 攻击是三类最典型的针对信任评估的攻击,它们都可以基于信任管理来进行防范。在 Bad Mouthing 攻击中^[15],一个恶意的用户总是给网络中的其他用

户以差评,从而破坏整个信任评价体系的公正和可信。

如图1为经典的 Bad Mouthing 攻击,图1(a)为正常场景,节点 A 对于节点 C 有一个客观的信任评价指数 R_c ; 而图1(b)是一个典型的 Bad Mouthing 攻击场景。假设节点 B 是恶意节点,它评价节点 C 的信任值为 $-R_c$,这个行为是异常的,它干扰了对于节点 C 的信任度评价的公正性,并将该评价值传递给了节点 A。在这种情况下,节点 C 虽然是非恶意节点,但是仍将被节点 A 视为恶意节点而从网络中剔除。

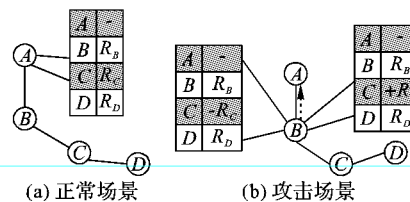


图1 Bad Mouthing 攻击场景示意图

on-off 攻击是危害性最大的针对信任评估的攻击类型^[16]。它交替性地进行正常-异常-正常-异常的行为和动作以躲避检测,从而能够长期地参与网络的共享和信任评估,在行为方式上与 sybil 攻击有较大的相似之处。如图2所示,如果节点 B 被视为一个恶意节点,它评价节点 C 的信任度并将结果传递给节点 A。在图2(b)所示的攻击场景中,节点 B 依次将对节点 C 的评价指数 $+R_c$ (正常)、 $-R_c$ (异常) 传递给节

收稿日期: 2014-06-05; 修回日期: 2014-08-03。 基金项目: 国家自然科学基金资助项目(61170273)。

作者简介: 赵源(1981-),男,内蒙古包头人,讲师,硕士研究生,主要研究方向: 计算机网络、信息安全; 陆天波(1977-),男,贵州毕节人,副教授,博士,主要研究方向: 分布式计算、计算机网络、信息安全。

点A, 这样它既能保证长期地隐藏在P2P网络中, 也能很大程度地负面影响对节点信任度的评价结果。因此, 这种恶意攻击需要尽早地发现和预防, 否则将对网络产生较大的负面影响。

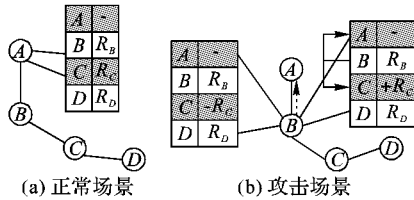


图2 on-off攻击场景示意图

与上述两种攻击略有不同, sybil攻击是通过利用大量正常节点的身份标识信息ID来进行信任管理的攻击。图3显示了恶意节点使用该攻击的场景。首先, 一个恶意节点使用一个身份标识产生器获得一个节点ID以节点A的身份进入网络; 然后, 该节点交替地以正常和异常的行为(该特征与on-off攻击相似)来影响网络的信任度评估管理。如果该节点被网络检测并剔除出网络, 则它通过身份标识产生器以另一个身份(除图中A所示以外的其他身份)加入网络并实行破坏。这样的攻击较难发现且难以完全将其阻止。

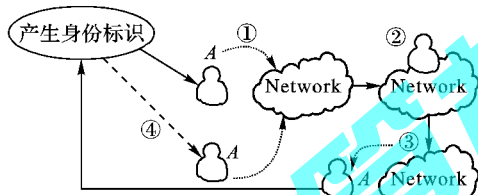


图3 sybil攻击场景示意图

1.2 现有信任管理方法分析

目前, 业界已经有相关的研究来从不同方面和程度上来解决信任管理的问题。

EigenTrust^[4]是一个非常知名的方法, 它不仅可以通过阻止恶意节点对于网络资源的共享, 并且可以通过审查节点的信任度来限制恶意用户针对网络的参与度, 从而降低损失。然而, 该方法存在较大的误报, 并且它采用了迭代式的矩阵乘法方法进行计算, 因此开销很大, 不是非常实用。PeerTrust^[8]方法则通过邀请网络中的节点对其相邻节点进行信任度评估的方法来建立信任机制, 然而该方法的主要问题是并没有相应的方法来保证评价本身的可信度。

PowerTrust方法最初在分布式哈希表(Distributed Hash Table, DHT)网络中被提出并采用^[8], 因此它很难直接应用在分布式网络中; 并且它还有一个非常重要的问题, 网络中所有节点都具有相同的信任度, 并没有对不同的节点信任度进行不同的区分。文献[9]提出了一个SFTrust框架, 该框架仅仅对网络中节点间的通信满意度进行评价, 它的评估范围有限, 并未针对节点其他属性的可信度进行评估和管理。另外, FileTrust^[10]则通过共享同一资源的用户评价来评估网络中节点的可信度, 然而, 如果没有共享资源或者不对共享资源进行评估, 则它无法保证评价的公平和完整。

2 多维度的信任管理机制

基于上面的分析, 目前业界并无一个非常有效的信任管理机制来对P2P网络中的节点进行准确、有效的信任管理。因此, 本章提出一个多维度的信任管理机制, 它采用所有参与

用户的信任相似度, 结合使用直接和间接的评价方法来建立网络中的信任管理, 从而防范恶意用户。

2.1 信任管理

P2P网络中的节点关系可以分为两类: 直接相邻和间接相邻。因此, 对于邻居节点的信任度管理, 本文定义为直接信任管理。对于邻居节点的相邻节点的信任度管理, 本文定义其为间接信任管理。整个信任管理的机制如式(1)所示:

$$T_{ij} = \alpha * DT_{ij} + (1 - \alpha) * IdT_{ij} \quad (1)$$

其中: T_{ij} 表示节点*i*对节点*j*的信任度评价; DT_{ij} 是节点*i*根据体验对节点*j*的直接信任评价; IdT_{ij} 是相邻节点对节点*j*的间接信任评价; α 是一个评价可信指数, 表明节点*i*对于节点*j*评价的可信程度。如果节点*i*与节点*j*通信*k*次, 那么该可信指数可以参照式(2)进行计算:

$$\alpha = \begin{cases} k/Threshold, & k < Threshold \\ 1, & \text{其他} \end{cases} \quad (2)$$

其中 $Threshold$ 为通信次数的阈值。

2.2 直接信任度(Direct Trust)

如果节点*i*与另外一个节点能够直接通信, 那么节点*i*可以根据自己的体验来对直接通信的节点进行直接信任度评价, 这个直接信任度用 DT_{ij} 表示。如果节点*i*与节点*j*通信*k*次, 那么可以计算满意度 ex_{ij}^k , 计算方法见式(3):

$$ex_{ij}^k = \begin{cases} 1, & \text{满意} \\ 0, & \text{不满意} \end{cases} \quad (3)$$

通过使用这个满意度值, 可以为节点*j*计算直接可信度(也就是 DT_{ij}), 其计算方法见式(4):

$$DT_{ij} = \frac{\sum_{k=1}^n f(x) * ex_{ij}^k}{\sum_{k=1}^n f(x)} \quad (4)$$

每次通信的满意度值通过映射时间衰减函数 $f(x) \rightarrow f(x) = \lambda^{n-k}$ 获得。其中: n 是通信的总次数(取值为正整数), $0.5 \leq \lambda \leq 1, 1 \leq k$ 。

如图4所示, 本文采用时间衰减函数来降低 on-off 攻击给网络带来的影响。在例子中, λ 和 n 分别取值 0.8 和 4。即使场景 1 和场景 2 具有相同的满意度, 它们的直接信任度结果根据通信的顺序也是不一样的。在本文的例子中, 可以通过将近期的通信满意度值相对过去的通信赋予更高的权重来有效地管理直接信任度。

k	ex	$eval$	k	ex	$eval$
1	1	0.512	1	0	0.0
2	1	0.640	2	0	0.0
3	0	0.000	3	1	0.8
4	0	0.000	4	1	1.0

(a) 节点A对节点B的直接信任度评价 (b) 场景1($DT_{ij}=0.390$) (c) 场景2($DT_{ij}=0.444$)

图4 Direct Trust 计算方法举例($\lambda=0.8, k=4$)

2.3 间接信任度(Indirect Trust)

间接信任度的计算基于两个节点的相似度以及提供评价的节点的可信度。间接信任度的计算原理参考图5, 它通过式(5)计算得出:

$$IdT_{ij} = \frac{\sum_{k=1}^n CR_{im} * DT_{mj}^{New}}{\sum_{k=1}^n CR_{im}} \quad (5)$$

其中: DT_{mj}^{New} 反映了节点 i 和节点 j (它们之间是间接信任度) 与它们共有的直接信任节点 m 之间的通信数量, 该数值可由式(6) 计算得出; n 表示节点 m 和节点 j 之间的通信次数; β 是反映直接信任的松弛指数, 它的取值区间为 $(0.5, 1]$ 。

$$DT_{mj}^{New} = DT_{mj} * \beta^{1/n} \quad (6)$$

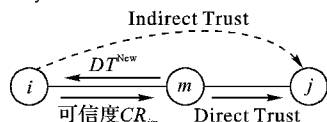


图 5 Indirect Trust 原理示意图

图 5 中可信度 (Credibility) CR_{im} 表明节点 i 对于节点可信程度的评价; 同理, 节点 j 对节点 m 也有类似的评价方法。因此, 当节点 m 提供给节点 i 有关节点 j 的间接信任度评价时, 节点 i 将参照其对节点 m 的可信度评价来使用有关节点 j 的间接信任度。

3 实验与分析

3.1 参数设置

为验证本文方法的合理性和有效性, 将本文方法与著名的 EigenTrust^[4] 方法、无任何信任管理方法在文件共享的场景下进行了仿真实验, 在实验中实验了多种攻击场景 (Bad Mouthing 和 on-off 攻击), 根据攻击场景本文按照预定的用户模式并对其进行评价。

使用业界非常知名的 QTM 模拟器进行模拟仿真实验, 对 3 种用户模型进行了模拟 (见表 1)。在表 1 中, 清除模式表明用户自主从库中删除无效文件的概率; 诚信模式反映用户对其他用户给出公正、诚信言论的概率。实验所使用的参数如表 2 所示。

表 1 用户模型初始化参数

用户模型	清除模式	诚信模式
正常用户	90% ~ 100%	100%
Bad Mouthing 攻击	90% ~ 100%	0%
on-off 攻击	50% ~ 100%	50% ~ 100%

表 2 仿真参数设定

参数	值
用户个数	100
事务个数	10 000
文件个数	5 000
阈值	50
最大邻居个数	2
λ	0.5
β	0.8
EigenTrust	0.2

对于实验结果的评价, 本文集中关注用户对于有效文件的接收率。评价指标采用了文献 [17] 中的有效传输率 (Success Rate of Transmission, SRT), 如式(7) 所示:

$$SRT = \frac{\text{用户有效文件的接收数目}}{\text{用户的尝试事务 (请求接收文件) 个数}} \quad (7)$$

如果 SRT 值越高, 则表明相应的信任管理机制越优。

3.2 结果与分析

在第一个 Bad Mouthing 攻击场景中, 评估了非恶意用户对于文件共享的 SRT。从图 6 可发现, 本文所述的多维度评价

方法能够保证随着系统恶意用户的增多, 用户仍然能够准确地从其他非恶意用户处共享到文件, 从而使得 SRT 水平一直接近 100%。而对于 EigenTrust 方法来说, 其在恶意用户比率小于 70% 的情况下能够导致较好的 SRT 水平, 而一旦恶意用户高于 70%, 则其效果显著下降。对于没有采用任何信任管理机制的场景来说, 其 SRT 则随着恶意用户数量的增加而一直下降。

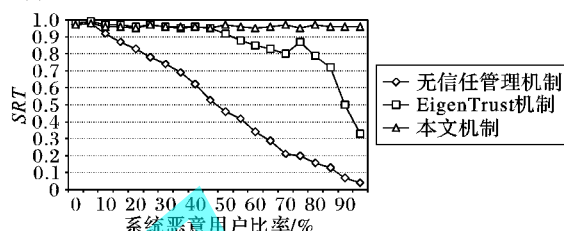


图 6 Bad Mouthing 攻击场景下的 SRT 结果

在 on-off 攻击的场景中, 本文方法相对 EigenTrust 给出了更佳的 SRT 效果。不过 on-off 攻击显然比 Bad Mouthing 攻击更加复杂和难以发现, 本文机制虽然比在 Bad Mouthing 攻击场景中效率有所下降, 但是相比其他方法来说仍然表现更加优秀。

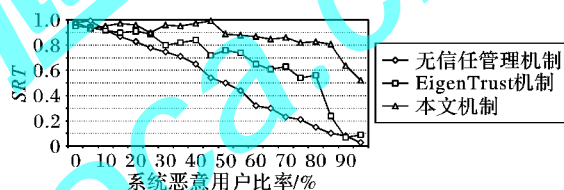


图 7 on-off 攻击场景下的 SRT 结果

4 结语

本文提出了一种适用于 P2P 分布式网络的节点信任管理机制, 它能够在存在恶意节点的情况下, 使用直接信任度和间接信任度方法, 有效地减少恶意节点对于 P2P 网络信任体系的破坏, 从而保证整个网络的健壮性和服务质量。并且, 本文通过仿真实验证明了该方法在真实攻击场景下相对于其他方法的有效性。

参考文献:

- [1] BLAZE M, FEIGENBAUM J, LACY J. Decentralized trust management [C]// Proceedings of the 1996 IEEE Symposium on Security and Privacy. Piscataway: IEEE Press, 1996: 164 - 173.
- [2] JESANG A, TRAN N. Trust management for e-commerce [EB/OL]. [2000-10-19]. <http://citeseer.nj.nec.com/375908.html>.
- [3] LIU Y. A two-hop solution to solving topology mismatch [J]. IEEE Transactions on Parallel and Distributed Systems, 2008, 19(11): 1591 - 1600.
- [4] KAMAR S, GARCIA M H. The EigenTrust algorithm for reputation management in P2P networks [C]// Proceedings of the 12th International Conference on World Wide Web. New York: ACM Press, 2003: 640 - 651.
- [5] ZHOU R F, HWANG K. PowerTrust: a robust and scalable reputation system for trusted peer-to-peer computing [J]. IEEE Transactions on Parallel and Distributed Systems, 2007, 18(4): 460 - 473.
- [6] ABRAMS Z, MCGREW R, PLOTKIN S. A non-manipulable trust system based on EigenTrust [J]. ACM SIGecom Exchanges, 2005, 5(4): 21 - 30.

(下转第 3169 页)

5 结语

本文提出了一种基于能量均衡、路径可靠的 GBUC 算法,通过在簇间选择一些中继节点来分担一些簇头的能耗,在路径选择时利用路由博弈模型选择出能耗均衡、可靠性高的最优路径。从仿真效果来看,GBUC 算法在可靠性、能耗均衡、生命周期等方面都要优于 EEUC 和 UCCER 算法。但是 GBUC 算法在分簇算法中采用随机的方式产生候选簇头,会造成簇的分配不合理;而为了避免节点空洞问题,采用迭代的方式产生簇头,也消耗了一定的时间和能量资源。今后的工作中需对该问题进行改进。

参考文献:

- [1] SUN L, LI J, CHEN Y, *et al.* Wireless sensor networks[M]. Beijing: Tsinghua University Press, 2005. (孙利民,李建中,陈渝,等. 无线传感器网络[M]. 北京:清华大学出版社,2005.)
 - [2] LI C, CHEN G, YE M, *et al.* An uneven cluster-based routing protocol for wireless sensor networks[J]. Chinese Journal of Computers, 2007, 30(1): 27 - 36. (李成海,陈贵海,叶懋,等. 一种基于非均匀分簇的无线传感器网络路由协议[J]. 计算机学报, 2007, 30(1): 27 - 36.)
 - [3] HU J, SHEN L. Clustering routing protocol of wireless sensor networks based on game theory[J]. Journal of Southeast University: Natural Science, 2007, 30(1): 27 - 36. (胡静,沈连丰. 基于博弈论的无线传感器网络分簇路由协议[J]. 东南大学学报: 自然科学版, 2010, 40(3): 441 - 445.)
 - [4] WU T, LIU K, LIU W. An energy-efficient coalition game model for wireless sensor networks[C]// Proceedings of the 2011 30th Chinese Control Conference. Piscataway: IEEE Press, 2011: 4940 - 4945.
 - [5] WANG T, WUJ, HE X, *et al.* A cross unequal clustering routing algorithm for sensor network[J]. Measurement Science Review, 2013, 13(4): 200 - 205.
 - [6] CUI Y, XU Y, XU R, *et al.* A heterogeneous wireless network selection algorithm based on non-cooperative game theory[C]// Proceedings of the 2011 6th International ICST Conference on Communications and Networking in China. Piscataway: IEEE Press, 2011: 720 - 724.
 - [7] TU Z. Game theory[M]. Beijing: Peking University Press, 2010. (涂志勇. 博弈论[M]. 北京: 北京大学出版, 2010.)
 - [8] ZHONG L, CHENG L. Unequal clustering energy-economical routing algorithm based on game-theory for WSN[J]. Application Research of Computers, 2009, 26(5): 1865 - 1867. (衷柳生,程良伦. 基于博弈论的无线传感器网络非均匀分簇路由算法[J]. 计算机应用研究, 2009, 26(5): 1865 - 1867.)
 - [9] LI H, JIANG S, WEI G. Game-theoretic modeling on routing in wireless sensor networks[J]. Chinese Journal of Sensors and Actuators, 2007, 20(9): 2075 - 2079. (李慧芳,姜胜明,韦岗. 无线传感器网络中基于博弈论的路由建模[J]. 传感技术学报, 2007, 20(9): 2075 - 2079.)
 - [10] WANG X, MA J, WANG S, *et al.* Cluster-based dynamic energy management for collaborative target tracking in wireless sensor networks[J]. Sensors, 2007, 7(7): 1193 - 1215.
 - [11] JIANG C, SHI W, TANG X, *et al.* Energy - balanced unequal clustering routing protocol for wireless sensor networks[J]. Journal of Software, 2012, 23(5): 1222 - 1232. (蒋畅江,石为人,唐贤伦,等. 能量均衡的无线传感器网络非均匀分簇路由协议[J]. 软件学报, 2012, 23(5): 1222 - 1232.)
 - [12] ARISIAN B, ESHCHI K. A game theory approach for optimal routing: in wireless sensor networks[C]// Proceedings of the 2010 6th International Conference on Wireless Communications Networking and Mobile Computing. Piscataway: IEEE Press, 2010: 1 - 7.
-
- (上接第 3159 页)
- [7] RAO S, WANG Y, TAO X. The comprehensive trust model in P2P based on improved EigenTrust algorithm [C]// Proceedings of the 2010 International Conference on Measuring Technology and Mechatronics Automation. Piscataway: IEEE Press, 2010, 3: 822 - 825.
 - [8] XIONG L, LIU L. PeerTrust: supporting reputation based trust for peer-to-peer electronic communities [J]. IEEE Transactions on Knowledge and Data Engineering, 2004, 16(7): 843 - 857.
 - [9] ZHANG Y C, CHEN S S, YANG G. SFTrust: a double trust metric based trust model in unstructured P2P system [C]// Proceedings of the 23rd IEEE International Parallel and Distributed Processing Symposium. Piscataway: IEEE Press, 2009: 1 - 7.
 - [10] KWON O, LEE S, KIM J. FileTrust: reputation management for reliable resource sharing in structured peer-to-peer networks[J]. IEICE Transactions on Communication, 2007, E90-B(4): 826 - 835.
 - [11] DONG X, YU W, PAN Y. A dynamic trust management scheme to mitigate malware proliferation in P2P network [C]// Proceedings of the 2008 IEEE International Conference on Communications. Piscataway: IEEE Press, 2008: 1605 - 1609.
 - [12] WANG Y F, NAKAO A. Poisonedwater: an improved approach for accurate reputation ranking in P2P networks[J]. Future Generation Computer System, 2010, 26(8): 1317 - 1326.
 - [13] TIAN C, YANG C B. R2Trust: a reputation and risk based trust management framework for large-scale, fully decentralized overlay networks[J]. Future Generation Computer Systems, 2011, 27(8): 1135 - 1141.
 - [14] LIANG Z, SHI W. PET: a personalized trust model with reputation and risk evaluation for P2P resource sharing [C]// Proceedings of the 38th International Conference on System Science. Piscataway: IEEE Press, 2005: 1 - 10.
 - [15] PATHAN A K. Security of self-organizing networks [M]. Florence: CRC Press, 2010: 102 - 113.
 - [16] MIAO W, FEI T, YU J Z, *et al.* An adaptive and robust reputation mechanism for P2P network [C]// Proceedings of the 2010 IEEE International Conference on Communications. Piscataway: IEEE Press, 2010: 1 - 5.
 - [17] WEST A G, KANNAN S, LEE I, *et al.* An evaluation framework for reputation management systems. Working chapter for trust modeling and management in digital environments: from social concept to system development [EB/OL]. [2013-10-10]. http://repository.upenn.edu/cgi/viewcontent.cgi?article=1430&context=cis_papers.