ISSN 1000-1239/CN 11-1777/TP
48(8): 1473-1480, 2011

P2P 声誉系统中 GoodRep 攻击及其防御机制

冯景瑜[1,2] 张玉清[2] 陈深龙[2] 付安民[1,2]

[1](计算机网络与信息安全教育部重点实验室(西安电子科技大学) 西安 710071)

[2](中国科学院研究生院国家计算机网络入侵防范中心 北京 100043)

(fengjy@mail.xidian.edu.cn)

GoodRep Attack and Defense in P2P Reputation Systems

Feng Jingyu[1,2], Zhang Yuqing[2], Chen Shenlong[2], and Fu Anmin[1,2]

[1](*Key Laboratory of Computer Networks and Information Security (Xidian University), Ministry of Education, Xi'an* 710071)

[2](*National Computer Network Intrusion Protection Center, Graduate University of Chinese Academy of Sciences, Beijing* 100043)

Abstract Reputation systems are playing critical roles in P2P networks as a method to assess the trustworthiness of peers and to combat malicious peers. However, the characteristic of aggregating ratings makes reputation systems vulnerable to be abused by false ratings, and thus offering opportunities for malicious peers. They can conspire with each other to form a collusive clique and unfairly increase the reputation of them. Under the cover of high reputation, malicious peers can masquerade as trusted ones and violate P2P networks arbitrarily. This attack model, called GoodRep, is described in this paper. In order to defend against GoodRep attack, the RatingGuard scheme is proposed to secure P2P reputation systems. This scheme is built with three functional modules: DC, DP and AD. The data collection (DC) module supports the collection of the previous rating data among raters. The data processing (DP) module measures the rating similarity of raters' activities by analyzing these data. To identify GoodRep cliques, the abnormal detection (AD) module detects the abnormalities through clustering partition technology. The experimental results show that our RatingGuard scheme is effective in suppressing GoodRep attack, and the reputation system with RatingGuard gains higher detection ratio of malicious peers compared with the traditional schemes.

Key words peer-to-peer; trust; reputation; GoodRep attack; collusive

摘 要 声誉系统由于其聚集评价的特点,为恶意节点提供了可乘之机.一些恶意节点合谋形成GoodRep攻击组,相互虚假夸大,进而在高声誉值的掩饰下危及P2P网络安全.提出了GoodRep的攻击模型及其防御机制——RatingGuard,并给出了该机制的数学描述和模块化实现过程.RatingGuard通过分析推荐节点之间的评价行为相似度,对推荐节点进行聚类划分和异常检测,识别出存在的GoodRep攻击组节点,从而帮助声誉系统排除GoodRep攻击组的干扰.仿真结果表明,RatingGuard在GoodRep攻击组的抵制方面效果显著,有效提高了声誉系统在面对GoodRep攻击时的恶意节点检测率.

关键词 P2P;信任;声誉;GoodRep攻击;合谋欺骗

中图法分类号 TP393.08

收稿日期:2011-04-07;**修回日期**:2011-06-07

基金项目:国家自然科学基金项目(60573048,60773135,90718007)

P2P(peer-to-peer)是一种新兴的不依赖中心实体的分布式网络环境,在分布式计算、文件共享、电子市场等领域得到了广泛的应用[1].但由于P2P网络的开放性和匿名性,恶意节点可以在网络中实施各种恶意攻击[2].具体地,恶意节点针对P2P网络的攻击方式有"搭便车"[3]、掩蔽攻击[4]、欺诈以及散播恶意资源等.

声誉系统的应用,在很大程度上增强了P2P网络的安全性,明显抑制了恶意节点在网络中的活动.因此,许多恶意节点转变策略,将攻击目标指向声誉系统本身.特别地,声誉系统自身在安全问题上也存在着脆弱性,为恶意节点提供了可乘之机.目前已发现多种针对声誉系统的攻击[5-8],其中以Self-promoting[8]攻击的潜在危害性最大.恶意节点可以通过发动Self-promoting攻击来提升自身声誉值,骗取源节点的信任.然而,单节点执行的Self-promoting攻击所能造成的威胁有限,攻击手法也相对容易识别.如果多个恶意节点合谋形成攻击组,有组织、有预谋地发起攻击,危害性更大,也更难以抵制.本文提出了一种新的针对声誉系统的攻击——GoodRep,用来描述这种合谋形式的Self-promoting攻击.

加入GoodRep攻击组的恶意节点,在共同利益的驱使下,能迅速地抬高恶意节点的声誉值,降低声誉系统的恶意节点检测能力.这种以抬高恶意节点声誉值为目标的合谋攻击行为,如不能得到阻止,节点会被恶意节点的高声誉值迷惑,丧失防范能力.

防御GoodRep攻击的关键,在于声誉系统对虚假评价的抑制能力上.已存在的解决方案是:评估推荐节点的评价可信度,使之用于权重评价数据,以此降低可能存在的虚假评价在声誉值计算中的影响.比较典型的方案有,文献[9-10]采用推荐节点的声誉值作为其评价可信度.PeerTrust[11]认为声誉值高的节点,评价行为未必可靠,并且危害性更大.对此,文献[11-12]基于个人经验计算评价可信度.此外,也有基于"大多数成员判决"的均值分析法[13].这些方案对单节点攻击或少数节点组攻击能起到一定的抑制作用,但出现GoodRep攻击组占推荐节点大多数节点的情况时,声誉系统将会面临严重威胁.

本文深入分析GoodRep攻击的特点,提出了防御机制——RatingGuard.该机制对推荐节点之间的评价行为进行相似度测量,计算出评价可信度.在此基础上,使用聚类划分和异常检测的方法,识别出推荐节点中可能存在的GoodRep攻击组.以此,达到提高声誉系统的恶意节点检测率,阻止GoodRep攻击的目的.

1 声誉系统的脆弱性及相关攻击

在P2P网络中部署声誉系统时,需要收集相关节点的推荐信息,通过聚集这些推荐节点提交的评价数据,计算出声誉值,以此判断目标节点的可信性.然而,并不是所有的推荐节点都是可靠的,声誉系统的这种聚集评价特性,使其具有严重的脆弱性及安全隐患,针对声誉系统的攻击方式也层出不穷.

目前,已存在多种针对声誉系统的攻击方式,如:Whitewashing[5],Sybil[6],RepTrap[7],以及Hoffman等人[8]提出的DOS,Slandering和Self-promoting.

在Whitewashing攻击中,恶意节点在声誉值降低后,以新的身份进入网络,重新活动.Sybil攻击则是恶意节点通过申请多个身份来夸大自己的声誉值.解决这2种攻击的措施是,严格区分新加入网络的节点和原有节点,限制节点的多重身份申请.由此,增加了攻击难度,逐渐被其余攻击方式取代.在RepTrap攻击中,恶意节点交替执行不同的服务策略,影响推荐的评价可信度,从而造成声誉值的错误计算.这种攻击在中心控制的声誉系统中,具有很强的危害性.DOS攻击也适用于中心控制的声誉系统,恶意节点伪造大量评价数据流,使声誉系统丧失计算能力.但是,由于P2P网络的分布式特性,缺乏中心控制设施,每个节点都能独立运行声誉系统,并不是由一个声誉系统服务于多个节点,因而增加了这2种攻击的实施难度.

新出现的Slandering和Self-promoting是2种提交虚假评价的源数据伪造攻击.前者被恶意节点用来诋毁正常节点的声誉值.但在同样多个服务可选的情况下,一个正常节点的声誉值被诋毁后,还有其余节点可选.后者就是恶意节点以抬高自身声誉值为动机的攻击,而GoodRep正是这种攻击的合谋形式.相比单节点的Self-promoting攻击,GoodRep攻击更难抑制,能更有效地影响声誉系统的恶意节点检测能力.

本文详细描述了GoodRep的攻击模型,并设计出相应的防御机制.

2 GoodRep攻击模型

本节提出一种新的Self-promoting攻击模型——

GoodRep. 该攻击能针对声誉系统聚集评价的特性,注入虚假的高评价数据(虚高评价),达到迅速抬高恶意节点声誉值的目的. 相比单节点的 Self-promoting 攻击,由恶意节点相互合谋实施的 GoodRep 攻击,目的明确、组织严谨,因而危害性更大.

定义 1. 设 $m_1, m_2, \cdots, m_n$ 表示参与 GoodRep 攻击的 n 个恶意节点,$M=\{m_1, m_2, \cdots, m_n\}$ 称为攻击组.

1) 攻击组形成策略

假定恶意节点 m_i 不甘心其在 P2P 网络中的活动被限制,串联其他不甘心的恶意节点形成 GoodRep 攻击组. 同时,为了保证攻击组的规模,提高攻击力度,要求新加入的恶意节点发展新成员后才能成为攻击组中的成员,共同享受攻击带来的利益.

如图 1 所示,若每个新加入攻击组的恶意节点再发展 2 个节点,k 次后,攻击组的规模 $|M|=2^{k-1}$.

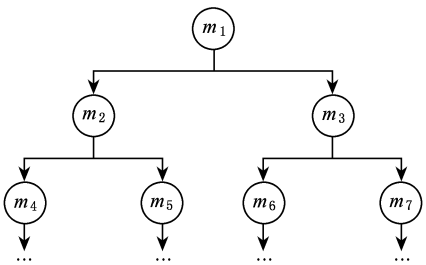


Fig. 1 Construction of GoodRep clique.

图 1 GoodRep 攻击组形成图

2) 攻击行为实施策略

攻击组的攻击行为实施策略包括:监听→报告→实施.

① 监听:由于源节点使用声誉系统时,需要向 P2P 网络广播评价查询请求报文(query). 因此,GoodRep 攻击组节点分布于网络中,监听 query.

② 报告:若其中一个节点,监听到 query 是关于攻击组内某个节点的评价查询请求,该节点将此报文发送给攻击组内的所有节点,进行报告.

③ 实施:收到报告后,攻击组内的所有节点,除被查询节点外,全都提交虚高评价,实施攻击.

3 GoodRep 攻击的防御机制

针对 GoodRep 攻击模型的特点,本节提出了防御机制——RatingGuard,并给出了具体的模块化设计方案.

3.1 基本结构

属于同一 GoodRep 攻击组的恶意节点,相互间的评价行为具有一定的相似性,通常对内相互夸大、对外正常评价,这是 RatingGuard 检测并抑制 GoodRep 攻击的理论基础.

如图 2 所示,源节点收到当前评价数据后,触发 RatingGuard. 首先,运行 Data Collection(DC)模块收集评价数据,采集出推荐节点之间的历史评价数据. 其次,运行 Data Processing (DP)模块对历史评价数据进行相似度测量和离群性分析,得出评价可信度. 之后,将计算结果输入 Abnormal Detection (AD)模块,检测当前评价数据中的异常,识别出 GoodRep 攻击组节点,剔除这些节点的当前评价数据. 最后,在声誉系统中,可使用经过处理的当前评价数据计算声誉值.

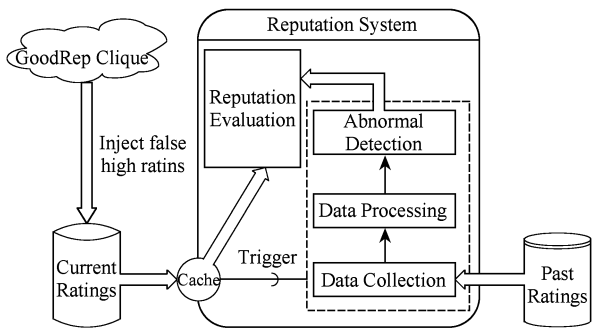


Fig. 2 Functional modules in RatingGuard.

图 2 RatingGuard 结构图

3.2 DC 模块

鉴于 P2P 网络缺乏中心控制的特点,提出了一个基于 Chord[14] 机制的分布式协议(CDP),用于实现 DC 模块收集历史评价数据的功能.

定义 2. 使用一个 Hash 函数(如 SHA-1),对节点 k 的 ID 进行 Hash 运算,根据计算结果和 Chord 机制的定位规则,指定 k 的评分档案节点,负责记录 k 提交的历史评价数据.

下面给出 CDP 协议的 4 个原语及其语义.

1) $SubmitCrating\ (ID_k, ID_j, Frating)$:$k$ 提交关于目标节点 j 的当前评价;

2) $QueryPratings\ (ID_k)$:查询 k 的历史评价数据;

3) $ReportPratings\ (ID_k, Pratings)$:评分档案节点将 k 的历史评价数据报告给源节点 i;

4) $FeedbackFrating\ (ID_i, ID_j, Frating)$:$i$ 向自己的评分档案节点提交其对 j 的交易评价结果.

如图 3 所示,整个 CDP 协议的工作流程可分为如下步骤:

Step1. i 收到 $SubmitCrating\ (ID_k, ID_j, Frating)$

后，$Hash\ ID_k$ 得到 k 的评分档案节点，发送 $QueryPratings\ (ID_k)$.

Step2. k 的评分档案节点收到查询请求后，给 i 发回 $ReportPratings\ (ID_k,\ Pratings)$.

Step3. i 筛选出 k 关于其余推荐节点的历史评价数据.

Step4. 重复执行 Step1，Step2 和 Step3，查询其余推荐节点相互间的历史评价数据，直至遍历完所有的推荐节点.

Step5. 交易结束后，i 向自己的评分档案节点提交 $FeedbackFrating(ID_i, ID_j, Frating)$.

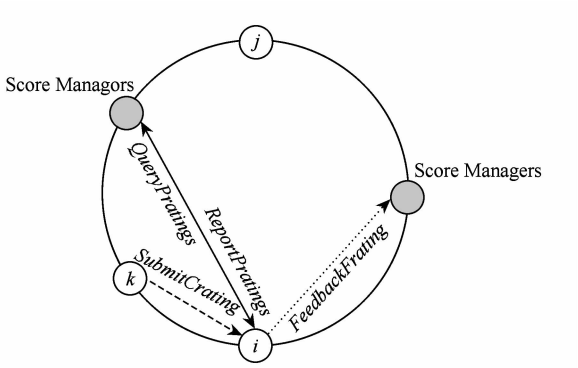


Fig. 3 Relationship of peers in CDP protocol.

图 3 CDP 协议中的节点关系

在 CDP 协议中，每个节点都可能承担 4 种不同的角色：源节点、目标节点、推荐节点和评分档案节点. 在担任这 4 种角色时，分别执行不同的任务. 并且，节点之间相互交易，不断运行 CDP 协议，会产生大量的评价数据存储，为后续的协议运行提供了基础.

3.3 DP 模块

建立在 DC 模块的基础上，DP 模块分析推荐节点之间的历史评价数据，实现评价行为相似度测量和评价可信度计算的功能.

定义 3. 对历史评价数据归纳整理，得到一个评价矩阵 $\boldsymbol{P}_{n\times n}$. 矩阵的行表示评价节点，列表示被评价节点，行向量表示节点的评价向量.

2 个推荐节点之间的评价行为相似度测量通常建立在对其评价向量的相似度测量上. 常用的相似度测量函数有余弦相似度和相关相似度[15]. 其中，相关相似度（也称修正余弦相似度）函数在计算相似度时，需要先减去评价数据的平均值. 文献[16]分析得出：2 个节点位于不同评价体系时，采用相关相似度函数可以有效地减少因评价尺度不同带来的误差，但对于 2 个节点位于同一评价体系时，并不适用，因为相关相似度不考虑实际评价情况，可能将导致 2 个实际评价行为差异很大的节点认为具有高度相似性. 由于声誉系统中的评价尺度一致，节点都位于同一评价体系中，因此 DP 模块采用余弦相似度函数计算评价行为相似度.

设推荐节点 k 和 l 的评价向量分别为 $\boldsymbol{K}$ 和 $\boldsymbol{L}$，且 $\boldsymbol{K}=[x_1,\ x_2,\ \cdots,\ x_n]$，$\boldsymbol{L}=[y_1,\ y_2,\ \cdots,\ y_n]$，则 k 和 h 的余弦相似度为

$$sim_{kl}=\frac{\sum_{i=1}^{n}x_iy_i}{\sqrt{\sum_{i=1}^{n}x_i^2}\sqrt{\sum_{i=1}^{n}y_i^2}}. \tag{1}$$

定义 4. 计算出各推荐节点之间的评价行为相似度后，构造评价相似度矩阵

$$\boldsymbol{SIM}_{n\times n}=\begin{bmatrix} sim_{11}\cdots sim_{1n} \\ \vdots \quad\quad \vdots \\ sim_{n1}\cdots sim_{mn}\end{bmatrix}.$$

显然，评价行为相似度是一种多维数据，只是描述了推荐节点之间的行为相似性，不能直接反映出推荐节点的评价可信程度. 考虑到：1) GoodRep 攻击组内节点相互夸大、行为相似；2) 不隶属于攻击组的推荐节点，缺乏利益驱动，通常客观地提交评价. 因而，组外推荐节点相对于组内节点具有一定的离群性. 离群性越高的节点，表明其为组内节点的概率就越低，其评价也就越可信. 基于这一点，我们对评价相似度矩阵 $\boldsymbol{SIM}_{n\times n}$ 中的数据进行一维化处理，计算推荐节点的离群值，即评价可信度.

在 $\boldsymbol{SIM}_{n\times n}$ 中，行向量中的数据为某个推荐节点相对于其余节点的评价行为相似度. 设推荐节点 k 对应的行向量 $\boldsymbol{ROW}^{\boldsymbol{K}}=[sim_{k1},\ sim_{k2},\ \cdots,\ sim_{kn}]$，则 k 的离群值（评价可信度）为

$$c_k=\frac{1}{|\boldsymbol{ROW}^{\boldsymbol{K}}|}\sum_{i=1}^{n}(1-sim_{ki}). \tag{2}$$

3.4 AD 模块

经过对各推荐节点之间的历史评价数据进行相似度测量后，得到离群值，下一步就是将这些节点中可能存在的 GoodRep 攻击组识别出来，以达到最终抑制 GoodRep 攻击的目的. AD 模块使用聚类划分和异常检测的方法，实现这一功能.

1) 聚类划分

GoodRep 攻击产生的根源是恶意节点以抬高自身声誉值为动机，相互合谋形成攻击组. 前面已经分析，攻击组表现出对内夸大、对外正常评价的特征，组内节点之间的评价行为具有一定的相似性. 这

种特征决定了组内节点的评价行为相似度经过一维化处理后,节点之间的离群值具有较小的差异.对此,通过聚类划分算法(算法 1)将推荐节点集合 S 分解为 S_h 和 S_l,其中,S_h 为高离群值节点的集合,S_l 为低离群值节点集合.

算法 1. *DividingCluster*(S).

Input:S;

Output:S_h,S_l.

① for $k\in S$ do

② *Calculate* c_k;

③ $C\leftarrow c_k$;

④ end for

⑤ Initialize $S_h=S$, $S_l=\varnothing$;

⑥ for $k\in S_h$ do

⑦ $S_l\leftarrow t\leftarrow$one element with the hightest outlier score in S_h;

⑧ Compute the variance

$$D(S_h-\{t\})=\frac{1}{|S_h|-1}\sqrt{\sum_{t\in S_h,k\neq t}(c_k-\bar{C})^2};$$

⑨ for $m\in S_l$ do

⑩ $$\sigma=D(S_h-\{t\})-\frac{1}{|S_l|}\sqrt{\sum_{m\in S_h}(c_m-\bar{C})^2};$$

⑪ end for

⑫ if ($\sigma<0$) then

⑬ exit;

⑭ end if

⑮ end for

2) 异常检测

AD 模块从 2 个角度检测异常.1)GoodRep 攻击的执行方式是攻击组注入虚高评价到当前评价数据中,因此须将当前评价数据中的高评价列为怀疑对象;2)GoodRep 攻击组内节点相互夸大,因此再次使用 CDP 协议,提取目标节点关于推荐节点的历史评价数据.综上,在 S_l 上运行异常检测算法(算法 2)识别出 GoodRep 攻击组(Ψ).

算法 2. *AbnormalitiesDetector*(S_l).

Input: S_l;

Output: Ψ.

① for $k\in S_l$ do

② if (*Crating* (ID_k, ID_j) is high) then

③ if (*Prating* (ID_j, ID_k) is high) then

④ $\Psi\leftarrow k$;

⑤ end if

⑥ end if

⑦ end for

4 仿真实验及结果分析

4.1 仿真环境

本文使用 matlab 7.0 搭建实验平台,对 RatingGuard 的性能进行仿真分析.仿真环境参数设置如表 1 所示:

Table 1 Description of Simulation Elements

表 1 仿真环境参数设置

Parameter	Description	Default
P_N	Number of peers	200
P_S	Number of raters	100
m_{rate}	Percentage of malicious peers	0.5
g_{rate}	Percentage of GoodRep clique	0.5
$R_{\text{threshold}}$	Reputation threshold	0.5

仿真的目的在于评估 RatingGuard 在增强声誉系统防御 GoodRep 攻击行为方面的效果,为了方便工程实现,对仿真实验的具体细节作了一定的简化处理,并作如下设定.1)参照推荐节点的评价行为类型,将 S 划分为 2 种类型的集合:正常评价节点集合与虚假评价节点集合,2 个集合之间的交集为$\varnothing$;2)进一步将虚假评价集合划分 2 个子集:合谋 GoodRep 攻击组节点集合(M)与非合谋节点集合(N);3) 集合 M 由多个恶意节点组成,其规模 $|M|=g_{\text{rate}}\times P_S$;4)仿真实验按照设置的参数初始化后,$i$ 发出对 j 当前评价数据的查询请求,相关节点响应查询请求,这一过程中,若 j 为 GoodRep 攻击组内成员,其余攻击组节点则实施攻击,提交虚高评价.

为了与传统防御机制比较,同时仿真实现了文献[9-13]中的虚假评价抑制方案,并分别采集每个机制的实验数据,与 RatingGuard 进行对比.这些方案从不同的角度提出评价可信度的计算方法,然后用评价可信度权重推荐节点的评价,最后使用加权系数的方法计算出声誉值.给定当前评价数据集合 Φ,且 $r_{kj}\in\Phi$,则目标节点 j 的声誉值为

$$R_j=\sum_{r_{kj}\in\Phi}r_{kj}\times\frac{c_k}{\sum_{k\in S}c_k}. \tag{3}$$

可见,提高声誉系统对虚假评价免疫力的关键在于有效的评价可信度计算上.下面,将文献[9-13]中的评价可信度计算方法归纳如下:

1) 声誉值法 (RVM). 文献[9-10]用推荐节点的声誉值量化其评价行为,则 $c_k=R_k$.

2) 个人经验 (PEM). 在文献[11-12]中,i 收集其与 k 共同评价过的节点,构成集合 IK,则

$$c_k=1-\frac{1}{|IK|}\sqrt{\sum_{x\in IK}(r_{ix}-r_{kx})^2}.$$

3) 均值分析(MAM). 基于"大多数成员判决",文献[13]认为当前评价数据与均值 $\bar{\Phi}$ 之间的差值越大,评价可信性就越低,则 $c_k=1-|r_k-\bar{\Phi}|$.

4.2 性能评价指标

通常,声誉系统中设置一个阈值 $R_{\text{threshold}}$,将声誉值低于 $R_{\text{threshold}}$ 的节点标记为恶意节点,高于 $R_{\text{threshold}}$ 的节点标记为正常节点. 由于 GoodRep 攻击组的干扰,声誉系统的计算结果可能会出现错误,这种错误可能会导致将恶意节点判断为正常节点. 因此,防御 GoodRep 攻击是为了有效排除 GoodRep 攻击组的干扰,降低声誉值计算误差 ε,最终达到提高声誉系统恶意节点检测率 ω 的目的.

设 R'_j 为节点 j 的实际声誉值,P_{D} 为网络中被检测出的恶意节点数,则 ε 和 ω 的定义如下:

$$\varepsilon=\frac{1}{P_N}\sum_{j=1}^{P_N}\sqrt{\frac{1}{R'_j}(R'_j-R_j)^2}; \tag{4}$$

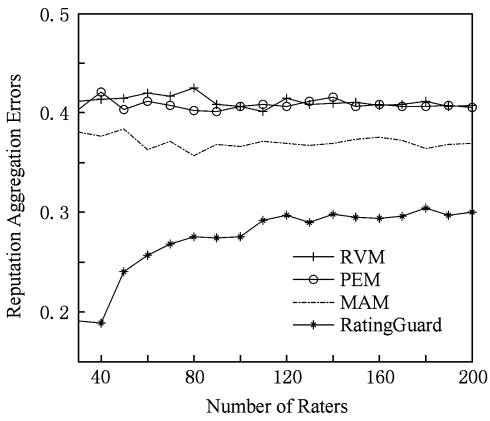
$$\omega=\frac{P_{\text{D}}}{m_{\text{rate}}\times P_N}. \tag{5}$$

4.3 仿真及其结果分析

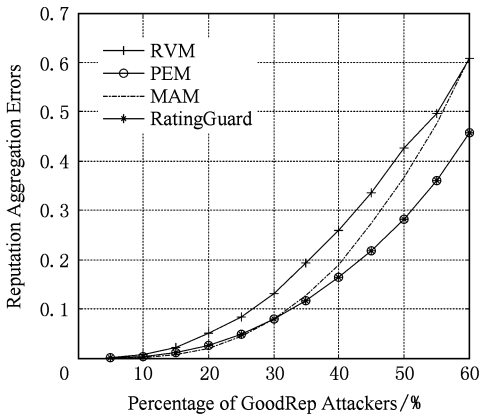
4.3.1 声誉值计算误差

为了测试评价可信度对声誉值计算的影响,分别给出了 ε 随推荐节点数量和 GoodRep 攻击组比例变化的情况. 如图 4 所示,各防御机制的曲线随推荐节点数量变化变为一条平稳曲线,而随 GoodRep 攻击组比例变化表现为一条上升曲线,说明 GoodRep 的攻击力度取决于 GoodRep 攻击组在推荐节点中所占的比例,而与推荐节点数量无关.

图 4(a)中,RatingGuard 的曲线低于其余防御机制,说明 RatingGuard 依据 GoodRep 攻击的特点,通过对历史评价数据进行相似性和离群性处理,得出评价可信度,提高了声誉值计算的准确性. 在图 4(b)中,GoodRep 攻击组比例低于 30% 时,MAM 的曲线甚至低于 RatingGuard,这是因为"大多数成员判决"原则在虚假评价节点较少时,真实评价起着主导作用. 此外,由于此次仿真未引入 AD 模块,从 PEM 和 RatingGuard 的曲线重合来看,说明二者在推荐节点的评价行为相似性问题处理上,具有一定的一致性.



(a) Reputation aggregation errors vs. the number of raters



(b) Reputation aggregation errors vs. the percentage of GoodRep attackers

Fig. 4 Reputation aggregation errors with respect to two factors.

图 4 声誉值计算误差

4.3.2 恶意节点检测率

图 5 给出了在 GoodRep 攻击组占推荐节点数量 50% 的情况下,ω 随恶意节点比例变化的情况.

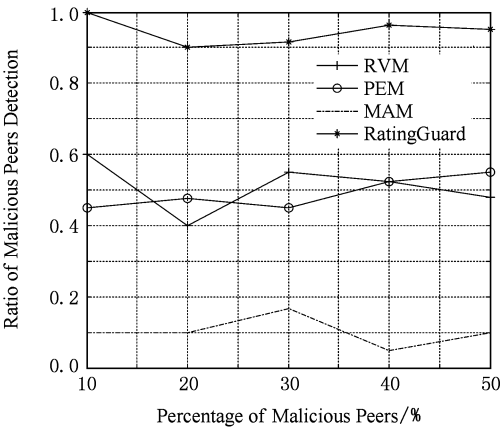


Fig. 5 Ratio of malicious peers detection vs. the percentage of malicious peers.

图 5 不同规模恶意节点比例下的检测率

如图 5 所示,即使恶意节点比例不断增加,各防御机制的曲线未发生较大波动,再次说明了 GoodRep 的攻击力度取决于 GoodRep 攻击组比例,并不会因恶意节点的比例增加而受到影响. 图 5 中,RatingGuard 的曲线依旧高于其余防御机制,这是因为我们在此次仿真中引入 AD 模块,过滤删除 GoodRep 攻击者,从而起到了降低攻击组比例的效果.

下面,对 AD 模块的性能进一步仿真分析.

如图 6 所示,实线为 RatingGuard 含有 AD 模块时得到的仿真结果,虚线为缺乏 AD 模块时的仿真结果. 显然,当推荐节点中 GoodRep 攻击组所占比例很低时,2 条曲线相互重合,都拥有很高的恶意节点检测率. 但随着 GoodRep 攻击组比例增加,尤其是超过 60%后,虚线急剧下降,而实线因为 AD 模块具有检测及过滤 GoodRep 攻击组的能力,则缓慢下降.

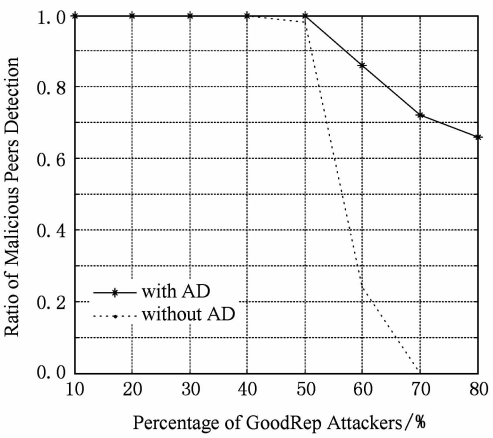


Fig. 6 Performance of AD module.

图 6 AD 模块的性能仿真

仿真实验结果表明:合谋形式的 GoodRep 攻击危害力巨大,尤其是攻击组节点成为推荐节点中的大多数成员时,能有效降低声誉系统检测恶意节点的能力. 因此,在恶意节点合谋问题比较严重的网络环境中,有效的 GoodRep 防御机制对于声誉系统的正常运行是必不可少的.

5 结束语

本文提出了一种新的 Self-promoting 攻击模型——GoodRep,该攻击主要针对 P2P 声誉系统聚集评价数据的特性,通过合谋形成攻击组和注入虚高评价的攻击方法,抬高恶意节点的声誉值,造成声誉系统对恶意节点检测性能的下降. 为了阻止 GoodRep 攻击,提出了防御机制 RatingGuard. 该机制通过分析推荐节点之间的历史评价数据,计算出评价行为相似度和离群值. 在此基础上,运用聚类分析和异常检测的思想,进行 GoodRep 攻击组节点的识别和过滤. 仿真实验表明,RatingGuard 能够有效排除 GoodRep 攻击组对声誉系统的干扰,提高了声誉系统的恶意节点检测率.

参 考 文 献

[1] Granville Z, Rose M, Panisson A, et al. Managing computer networks using peer-to-peer technologies [J]. IEEE Communications Magazine, 2005, 43(10): 62-68

[2] Jin Yu, Gu Zhimin, Ban Zhijie. A new reputation management mechanism based on bi-ratingsin peer-to-peer systems [J]. Journal of Computer Research and Development, 2008, 45(6): 942-950 (in Chinese)
(金瑜, 古至民, 班志杰. 一种新的 P2P 系统中基于双 ratings 的声誉管理机制[J]. 计算机研究与发展, 2008, 45(6): 942-950)

[3] Adar E, Huberman B. Freeriding on gnutella [J]. FirstMonday, 2000, 5 (10): 42-68

[4] Singh A, Castro A, Druschel, et al. Defending against eclipse attacks on overlay networks [C] //Proc of the 11th Workshop on ACM SIGOPS Europen Workshop. New York: ACM, 2004: 115-120

[5] Feldman M, Papadimitriou C, Chuang J, et al. Free-riding and whitewashing in peer-to-peer systems [C] //Proc of ACM SIGCOMM. New York: ACM, 2004: 228-236

[6] Douceur J R. The sybil attack [C] //Proc of the 1st Int Workshop on Peer-to-Peer Systems. Berlin: Springer, 2002: 251-260

[7] Yang Y, Feng Q, Sun Y L, et al. Reptrap: A novel attack on feedback-based reputation systems [C] //Proc of 4th Int conf on Security and Privacy in Communication Networks. New York: ACM, 2008

[8] Hoffman K, Zage D, Nita-Rotaru C. A survey of attack and defense techniques for reputation System [J]. ACM Computing Surveys, 2009, 41(1): 1-31

[9] Kamvar S, Schlosser M. The eigentrust algorithm for reputation management in P2P networks [C] //. Proc of the 12th Int World Wide Web Conf (WWW2003). New York: ACM, 2003: 123-134

[10] Zhou R, Hwang K. PowerTrust: A robust and scalable reputation system for trusted P2P computing [J]. IEEE Trans on Parallel and Distributed Systems, 2007, 18(7): 460-473

[11] Xiong L, Liu L. PeerTrust: Spporting reputation-based trust in peer-to-peer communities [J]. IEEE Trans on Knowledge and Data Engineering, 2004, 16(7): 843-57

[12] Xiong L, Liu L, Srivatsa M. Trustguard: Countering vulnerabilities in reputation management for decentralized overlay networks [C] //Proc of the 14th World Wide Web Conf. New York: ACM, 2005: 422-431

[13] Feng J Y, Zhang Y Q, Wang H. A trust management model based on bi-evaluation in P2P networks [J]. IEICE Trans on Information and Systems, 2010, E93-D(3): 466-472

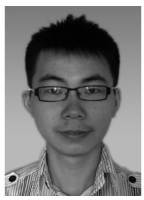
[14] Stoica I, Morris R, Nowell D, et al. Chord: A scalable peer-to-peer lookup protocol for internet applications [C] // Proc of ACM SIGCOMM. New York: ACM, 2001: 1-14

[15] Deng Ailin, Zhu Yangyong, Shi Baile. A collaborative filtering recommendation algorithm based on item rating prediction [J]. Journal of Software, 2003, 14(9): 1621-1628 (in Chinese)
(邓爱林, 朱扬勇, 施伯乐. 基于项目评分预测的协同过滤推荐算法[J]. 软件学报, 2003, 14(9): 1621-1628)

[16] Miao Guangsheng, Feng Dengguo, Su Purui. Colluding clique detector based on cativity similarity in P2P trust model [J]. Journal on Communications, 2009, 30(8): 9-20 (in Chinese)
(苗光胜, 冯登国, 苏璞睿. P2P 信任模型中基于行为相似度的共谋团体识别模型[J]. 通信学报, 2009, 30(8): 9-20)

Feng Jingyu, born in 1984. PhD candidate. His main research interests include trust management and P2P security.

Zhang Yuqing, born in 1966. Professor and PhD supervisor of the Graduate University of Chinese Academy of Sciences. His main interests include cryptography, wireless security and trust management(zhangyq@nipc.org.cn).



Chen Shenlong, born in 1984. PhD candidate. His main research interests include trust management and wireless security(chensl@nipc.org.cn).

Fu Anmin, born in 1981. PhD candidate. His main interests include wireless security and cryptography(fuam@mail.xidian.edu.cn).