Journal of Computer Applications
计算机应用,2013,33(8):2222 - 2224,2231
ISSN 1001-9081
CODEN JYIIDU
2013-08-01
http://www.joca.cn

文章编号:1001-9081(2013)08-2222-03
doi:10.11772/j.issn.1001-9081.2013.08.2222

基于评价相似度对 WSN 声誉系统合谋攻击的检测机制

王　勇*,袁巢燕,唐　靖,胡良梁
(重庆理工大学 计算机科学与工程学院,重庆 400054)
(*通信作者电子邮箱 ywang@cqut.edu.cn)

摘　要:针对无线传感器网络(WSN)声誉系统中可能存在的多个恶意节点合谋攻击网络节点,并影响其准确定位等安全问题,提出了恶意推荐(BS)合谋攻击团及其检测机制(BSCD),并给出了该机制的实现方法。该机制通过对推荐节点进行异常检测,分析推荐节点间的评价行为相似度,有效检测出存在的合谋攻击团,从而降低其对声誉系统的破坏和影响。仿真实验表明,BSCD 在检测和抵制 BS 合谋攻击团方面效果显著,有效提高了声誉系统中恶意节点检测率和整个系统抵抗恶意节点破坏的能力。

关键词:无线传感器网络;声誉系统;合谋攻击;恶意节点;评价相似度
中图分类号:TP393　　**文献标志码**:A

Colluding clique detector based on evaluation similarity in WSN reputation system mechanism

WANG Yong*, YUAN Chaoyan, TANG Jing, HU Liangliang
(*College of Computer Science and Engineering, Chongqing University of Technology, Chongqing* 400054, *China*)

Abstract: Bad Mouthing and Self-Promoting (BS) collusion attack group and its detection mechanism, called BSCD, were proposed to resolve the security issues of the multiple malicious node collusion attack network nodes and affect their accurate positioning in the Wireless Sensor Network (WSN) reputation system. And the implementation method of the mechanism was given. It detected the abnormal recommended node, analyzed the evaluation behavior similarity between recommended nodes, and effectively detected the existence of collusion attack group, thereby reduced its damage and impact on the reputation of the system. The simulation results show that, BSCD has significant effect on the detection and resisting BS collusion attack group, effectively improves the malicious node detection rate in the reputation system and the capacity of the entire system to resist malicious node.

Key words: Wireless Sensor Network (WSN); reputation system; collusion attack; malicious node; evaluation similarity

0　引言

无线传感器网络(Wireless Sensor Network, WSN)[1-2]是当前国内外备受关注、涉及多学科、知识高度集成的前沿热点研究领域,已广泛应用于军事国防、生物医疗、环境监测、抢险救灾等重要领域。由于其部署环境的开放性与恶劣性,WSN 不仅面临外部攻击者对网络发起的攻击,也可能面临内部节点被俘获而发起的内部攻击。相对外部攻击而言,内部攻击的隐蔽性对系统攻击的影响更大。

基于信誉机制的 WSN 中,需要收集第三方节点(推荐节点)的推荐信息作为信誉值计算和整合的一个重要组成部分[3-4]。通过聚集这些由推荐节点提交的评价数据,得到间接信誉值,然后整合出综合信誉值,来判断待评估信标节点的可信性,选择可靠的信标节点来实现未知节点的定位。声誉系统的应用,在很大程度上增强了 WSN 的定位安全性,明显抑制了恶意节点在网络中的破坏行为。然而,并不是所有的推荐节点都是可靠的,即并不是所有来自第三方节点的推荐信息都是可信的。针对声誉系统自身存在的脆弱性和安全隐患,许多恶意节点转变攻击策略,将攻击目标指向声誉系统自身并且攻击方式呈现多样化。

目前,已存在多种针对声誉系统的攻击方式,如:虫洞攻击、女巫攻击[5]、诋毁(Bad Mouthing)攻击和恶意推荐(Self-Promoting)攻击等。诋毁攻击和恶意推荐攻击是指第三方节点分别通过诋毁贬损良性节点信誉和故意抬高恶意节点信誉,达到影响网络正常运行目的的一种攻击。与单个节点的恶意诋毁/推荐攻击相比,以恶意节点合谋攻击的危害性最大。因此,检测并剔除合谋攻击的恶意节点对提高系统安全性有着重要的研究意义,也是 WSN 亟待解决的安全问题。

1　相关工作

针对声誉系统中存在的攻击问题,一系列基于信誉机制的恶意节点识别模型被提出[6]。Ganeriwal 等[7]提出的 BRSN(Beta Reputation system for Sensor Networks)模型对于高信誉节点发送的信息给予较高权重,有效抵御了低信誉节点的恶意推荐/诋毁行为,但对高信誉节点的恶意推荐/诋毁行为却束手无策。其实,第三方节点评价行为的可信度并不能完全由其信誉值来决定。因为恶意节点可以通过良好的通信行为来故意抬高自己的信誉值,从而进行恶意推荐/诋毁行为。

Srinivasan 等[8]提出一种基于分布式声誉机制的信标节点信任模型(Distributed Reputation-based Beacon Trust System,

收稿日期:2013-01-31;**修回日期**:2013-03-07。
基金项目:重庆市自然科学基金资助项目(cstc2011jjA40026);重庆理工大学研究生创新基金资助项目(YCX2012316)。
作者简介:王勇(1974 -),男,重庆人,副教授,博士,主要研究方向:物联网、嵌入式系统;　袁巢燕(1987 -),女,安徽合肥人,硕士研究生,主要研究方向:无线传感器网络、嵌入式系统;　唐靖(1988 -),女,湖南永州人,硕士研究生,主要研究方向:无线传感器网络、嵌入式系统;胡良梁(1987 -),男,湖南娄底人,硕士研究生,主要研究方向:无线传感器网络、嵌入式系统。

DRBTS)。在该模型中信标节点之间互相监督和提供信息,当信标节点作为检查点时,通过监听的方式获取其他信标节点的信誉,未知节点根据接收的信誉值进行信任分级,为选取可信信标节点采用投票表决的方法,以此来检测恶意信标节点。但对于投票过程中恶意节点共谋制造错误评论的情况只进行了分析,并未提出有效的解决方法。

文献[9]是对 DRBTS 模型的改进,引入信标节点的相互监督机制,且在间接信誉计算时,采用差值阈值比较进行可信度检测,排除恶意诽谤或恶意推荐节点。通过簇头节点选择可靠信标节点实现未知节点定位,以此来排除恶意信标节点。该模型在一定程度上提高了恶意信标节点的检测率,但未对间接信誉计算和投票过程中恶意信标节点共谋制造虚假评论的情况提出有效的解决方案。

文献[10]提出一种 P2P(Peer-to-Peer)环境下的基于节点行为相似度的共谋团体识别(Colluding Clique Detector,CCD)模型,该模型通过分析节点间行为相似度,有效识别网络中的团体合谋行为,在共谋团体检测和抵制方面效果显著。

单节点发起的攻击行为所造成的安全威胁有限,攻击手法也相对容易识别,但多个恶意节点隐蔽地合谋形成攻击团,有组织、有目的地发动攻击,则其危害性和抵制难度将更大。而现有信任模型的重点仍在抵制单个恶意节点的攻击行为上,缺乏有效针对合谋攻击的检测机制。通常参与合谋的恶意信标比率越高,引起的定位误差越大[11]。

2　BS 合谋攻击团检测机制——BSCD

定义 1　BS 合谋攻击指合谋形式的诋毁攻击和恶意推荐攻击。

定义 2　BS 合谋攻击团指两个或两个以上恶意节点在共同利益的驱使下,共同参与合谋攻击,并对团伙内的节点提交虚高评价,对团伙外的节点进行诋毁贬低,以此提升自身信誉值,骗取待定位节点信任并影响其定位。

针对 BS 合谋攻击的形成策略和攻击特点,本章提出其相应的检测机制——BSCD。为有效检测出 BS 合谋攻击团,首先需要识别出单个推荐节点的异常行为,这是检测合谋团体的理论依据。

2.1　检测单个异常推荐节点

2.1.1　信誉值变化率比较法

节点的信誉度一般相对稳定,只有当恶意节点处于恶意贬低良性节点或者有意抬高恶意节点时,才出现信誉值的异常变化。提出的信誉值变化率比较法,即在一个特定的时间间隔内,观察节点观察广播邻居信誉值的信标节点 B_i 及其邻居信标节点信誉值变化情况,并根据经验值给定一个阈值 $|\tau|(\tau>0)$,如果变化率超过该阈值,则此观察节点向外发送举报警告报文,如果被观察节点 B_i 周围的邻居信标节点中有过半的发送了举报警告报文,则认为该被观察节点 B_i 为异常节点,对其提供的信息不予采纳。

信誉值变化率公式如下:

$$T_{ij_{\text{rate}}}=\frac{\Delta T_{ij}}{\Delta t}=\frac{T_{ij_{n+1}}-T_{ij_n}}{t_{n+1}-t_n}$$

根据上述公式可知,$T_{ij_{\text{rate}}}$ 反映了信誉值的变化情况:当 $-\tau<T_{ij_{\text{rate}}}<\tau$ 时,表示信誉值变化较稳定,可以接受;当 $T_{ij_{\text{rate}}}<-\tau$ 时表示可能恶意节点故意贬低良性节点,不可以接受;当 $T_{ij_{\text{rate}}}>\tau$ 时表示可能恶意节点有意抬高恶意节点,也不可以接受。

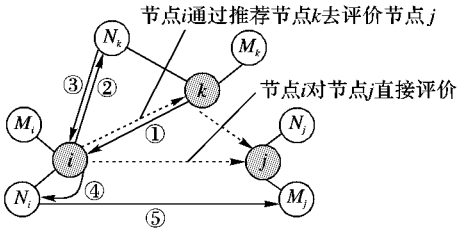
2.1.2　探测节点的引入

为进一步检测出网络中的异常评价节点,引入探测节点概念。假设 WSN 初始化时,给少量良性信标节点分配几个伪传感器 ID。当网络活动量处于较低状态时,这些良性信标节点使用拥有的伪传感器 ID 伪装成其他信标节点,重新进入网络参与信誉评测并触发其他信标节点对其进行评价。由于自身是良性节点,故若某信标节点对其评价的信誉值低于一定的阈值,或者频繁投其反对票,则可以将其判为可疑节点,降低其信誉值,并向自己周围的节点发出警告信息,未知节点进行统计,警告次数超过一定数值的,则为异常节点,对其提供的位置信息不予考虑,将其排除出网络。

通过上述两种方法来检测网络中存在的异常推荐节点,在发现多个评价异常节点之后,对其评价行为相似度进行分析,评价行为相似度达到一定程度的节点,将会被怀疑具有共谋的可能。为了有效找出可能存在的共谋团体,本文将注意力集中在评价异常的推荐节点身上,而不是盲目地对所有节点进行分析,这样不仅大大降低系统的处理负担,提高效率,而且提高了识别的准确度。

2.2　评价档案数据的收集

定义 3　设两个不同的 Hash 函数 H_m 和 H_n,对于同一个节点 i 的 ID 分别进行两次 Hash 运算,根据计算结果和 WSN 定位规则分配 2 个不同的节点,分别负责节点 i 的被评价数据记录和评价行为数据记录。设节点 M_i 负责管理节点 i 的被评价数据记录,即负责管理其他节点对节点 i 的评价;N_i 负责记录节点 i 评分行为,即节点 i 对其他节点的评价。称节点 M_i 为节点 i 的被评价数据管理节点,节点 N_i 为节点 i 的评分数据管理节点。



注:

① k 向 i 提交关于目标节点 j 的当前评价;

② i 向 k 的评分数据管理节点 N_k 发送评价档案查询请求;

③ N_k 返回 k 的评价档案数据给 i;

④ i 向自己的评分数据管理节点 N_i 提交其对 j 的评价结果;

⑤ N_i 将获得的评价结果报告给 j 的被评价数据管理节点 M_j。

图 1　节点关系图

评价档案数据收集算法具体步骤如下:

1) k 提交关于目标节点 j 的当前评价给节点 i(经异常检测后,确定 k 为异常推荐节点);

2) 当 i 收到评价结果后,向 N_k 提交查询请求,查询 k 的评价档案;

3) N_k 将 k 的评价档案数据报告给 i,节点 i 筛选出 k 关于其余推荐节点的评价档案数据;

4) 重复执行 1) ~3),查询除 k 外的其余推荐节点相互间的评价档案数据,直至遍历完所有推荐节点;

5) 前 4 步结束后,i 向自己的评分数据管理节点 N_i 提交其对 j 的评价结果;

6) N_i 也将此评价结果提交给节点 j 的被评价数据管理节点 M_j 记录并保存。

2.3　BS 合谋攻击团检测算法

属于同一 BS 合谋攻击团体的恶意节点,相互间的评价

行为具有一定的相似性,对内相互吹嘘夸大、对外贬低评价,这是本合谋攻击团体检测机制的理论依据。该检测机制通过计算节点之间的评价相似度,来检测声誉系统中存在的合谋攻击行为,从而达到识别共谋团体的目的。

为问题描述的方便,对共谋团体行为作以下“双一致”假定:

1)其攻击目标是一致的,即共谋团体对目标发起攻击时,其所有成员都参与对该目标的攻击。

2)其对同一目标的攻击行为是一致的,即当共谋团体对某目标发起攻击时,若其攻击目的是发动诋毁(或恶意推荐)攻击,则其所有成员的攻击行为都致力于发动诋毁(或恶意推荐)攻击。

2.3.1 评价行为相似度定义和表示

在收集到评价档案数据之后,分析推荐节点之间的评价数据,并对其进行相似度测量。

定义 4 对评价档案数据归纳整理后,可以用一个 $n \times n$ 阶矩阵 $\boldsymbol{p}_{n\times n}$ 表示,行表示节点对所有其他节点的评价,列代表被评价节点。由该行组成的行向量为节点的评价向量。评价向量是衡量节点评价行为相似度的基础。第 i 行第 j 列的元素 p_{ij} 表示节点 i 对节点 j 的评价。

2 个推荐节点之间评价行为相似度的衡量通常转换为相应评价向量相似度的测量。常用相似度测量函数有 3 种[12]:余弦相似度、修正的余弦相似度以及相关相似度。其中余弦相似度函数在衡量向量相似性方面应用较广泛,可直接用来衡量节点间评价行为相似程度。其余两种函数在计算时需先减去节点评分的平均值,目的是减小因不同评分尺度而带来的误差。由文献[13]可知:当 2 个节点处于不同评价体系时,采用修正的余弦相似度(或相关相似度)函数可以有效减少因评价尺度不同带来的误差,但对同一声誉系统(或评价体系)中的 2 个节点,该方法并不适用,因为余弦相似度函数在计算过程中仅考虑节点的评分差异而不考虑节点的实际评分,这样可能导致 2 个实际评价行为差异很大的节点被认为具有高度的相似性。因此,本文采用余弦相似度函数计算节点的行为相似度。

设推荐节点 x 和 y 的评价向量分别为 $\boldsymbol{X}$ 和 $\boldsymbol{Y}$,且 $\boldsymbol{X}=[x_1,x_2,\cdots,x_n]$,$\boldsymbol{Y}=[y_1,y_2,\cdots,y_n]$,则 x 和 y 的余弦相似度为:

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

2.3.2 BS 共谋团体的识别

本文参考文献[10]中 P2P 信任模型中共谋团体识别算法。

定义 5 计算出各推荐节点之间评价行为相似度后,构造评价相似度矩阵:

$$\boldsymbol{SIM}_{n\times n}=\begin{bmatrix} sim_{11} & sim_{12} & \cdots & sim_{1n} \\ sim_{21} & sim_{22} & \cdots & sim_{2n} \\ \vdots & \vdots & & \vdots \\ sim_{n1} & sim_{n2} & \cdots & sim_{nn} \end{bmatrix}$$

设 sim_{ij} 为矩阵 $\boldsymbol{SIM}_{n\times n}$ 中任意元素,表示节点 i 和节点 j 之间的评价行为相似度。

在计算得到各节点之间的评价行为相似度并构造出相似度矩阵以后,需要将这些节点中可能存在的共谋团体识别出来,以实现检测恶意共谋团体攻击的目的。文献[10]中的共谋团体识别算法使用矩阵变换算法对矩阵 $\boldsymbol{SIM}_{n\times n}$ 进行等价变换,得到对角矩阵后确定主对角线子矩阵的节点集合即为共谋团体。

3 仿真结果与性能分析

3.1 仿真环境

本文采用 Matlab 在 100 m × 100 m 的仿真区域平台上仿真,对 BSCD 的性能进行仿真分析。仿真环境参数设置如表 1 所示。

表 1 仿真环境参数设置

参数	取值	参数	取值
网络节点总数 P_A	400	合谋攻击团体比例	50%
推荐节点总数 P_R	200	合谋攻击团规模阈值 η	10
恶意节点比例 m_r	50%	相似度阈值 δ	60%
信誉值阈值	0.5		

仿真的目的在于评估 BSCD 在增强声誉系统检测抵制 BS 合谋攻击团方面的效果。为了仿真实验以及问题分析和描述的方便,对仿真实验的具体细节处理及设定如下:

1)按推荐节点的评价行为类型,将 R 划分成 2 个集合:正常评价节点集合 S 和恶意评价节点集合 T,且两者交集为空。

2)再将恶意评价节点集合划分为 2 个子集:BS 合谋攻击团节点集合(M)与非合谋攻击团节点集合(N,即单个恶意节点组成的集合,它们单独行动而不组成任何共谋团体),集合 M 中的成员都属于且只属于某一个共谋团体,任意 2 个不同的合谋团体之间的交集为空。

3)所有节点的初始信誉值都为 0,初始评价向量也为 0。

3.2 性能评价指标

1)设 P_m 为网络中被检测出的恶意推荐节点数,则恶意节点检测率如下所示:

$$\omega=\frac{P_m}{m_r * P_A}\times 100\%$$

2)定位误差定义为未知节点经定位算法得到的估算坐标位置和其实际坐标位置间的距离与节点通信半径的比值,公式如下:

$$\partial=\sqrt{(x_i-x_e)^2+(y_i-y_e)^2}/R$$

其中:(x_i,y_i) 是未知节点的实际坐标位置,(x_e,y_e) 是经定位算法得到的估算坐标位置,R 是节点通信半径。

3.3 仿真及结果分析

3.3.1 恶意节点检测率的仿真与分析

图 2 的是上述实验参数环境下,恶意节点检测率随恶意节点比例变化的情况。如图 2 所示,在恶意节点比例不断增加(大于 10%)时,DRBTS 模型和文献[9]算法的恶意节点检测率出现总体下降趋势,而 BSCD 的曲线依旧高于其他两种方案,且保持稳定上升趋势,这是因为随着恶意节点数目的增多,合谋攻击几率增大,使恶意节点的检测难度相对增大,故检测合谋攻击的 BSCD 的检测率高于其他两种方案。

3.3.2 节点定位误差的仿真与分析

图 3 是网络中不同恶意节点比例对未知节点定位误差的影响曲线。从图 3 中可以看出,随着恶意节点比例的增大,DRBTS 模型、文献[9]算法和 BSCD 的定位误差均在增大,但是在相同的恶意信标节点比例下,与 DRBTS 模型和文献[9]算法相比,BSCD 的定位误差偏小,而且效果比较明显。随着恶意节点比例的不断增大,BSCD 有效地检测出网络中隐藏的合谋攻击团,过滤其提供的信息,降低其对未知节点定位的影响,从而减小定位误差,有效提高节点定位的精度。

(下转第 2231 页)

定时间应对训练集进行更新。

4　结语

本文阐述了应用层 DDoS 攻击的原理,分析了现有攻击检测方法的不足,从用户访问行为的角度提出了一种 DDoS 攻击检测方法。该方法计算单位时间内 IP 请求熵,通过等时间采样构成时间序列,并使用 AAR 模型进行参数向量估计,最后采用 SVM 进行分类检测。本文的仿真仅模拟了基于 HTTP 的攻击行为,同样也可以适用于其他应用层攻击行为的检测,如:FTP 服务器的匿名登录等。下一步的工作目标是如何在实际应用场景中自适应地给出一种有效的参数设置。

参考文献:

[1] XIE Y, YU S. A large-scale hidden semi-Markov model for anomaly detection on user browsing behaviors [J]. IEEE/ACM Transactions on Networking, 2009, 17(1): 54 – 65.

[2] XIE Y, TANG S, HUANG X, *et al*. Detecting latent attack behavior from aggregated Web traffic [J]. Computer Communications, 2013, 36(8): 895 – 907.

[3] OIKONOM G, MIRKOVIE J. Modeling human behavior of defense against flash-crowd attacks [C]// ICC'09: Proceedings of the 2009 IEEE International Conference on Communications. Piscataway: IEEE, 2009: 14 – 18.

[4] CHEN Y, KU W-S, SAKAI K, *et al*. A novel DDoS attack defending framework with minimized bilateral damages [C]// Proceedings of the 7th IEEE Conference on Consumer Communications and Networking Conference. Piscataway: IEEE, 2010: 1 – 5.

[5] CHOI Y-S, JANG J-T, RYOU J-C. Integrated DDoS attack defense-infrastructure for effective attack prevention [C]// Proceedings of 2010 2nd International Information Technology Convergence and Services. Piscataway: IEEE, 2010: 71 – 76.

[6] BEITOLLAHI H, DECONINCK G. Analyzing well-known countermeasures against distributed denial of service attacks [J]. Computer Communications, 2012, 35(11): 1312 – 1332.

[7] BEITOLLAHI H, DECONINCK G. Tackling application-layer DDoS attacks [J]. Procedia Computer Science, 2012, 10: 432 – 441.

[8] WEN S, JIA W J, ZHOU W, *et al*. CALD: surviving various application-layer DDoS attacks that mimic flash crowd [C]// NSS'10: Proceedings of 2010 Fourth International Conference on Network and System Security. Washington, DC: IEEE Computer Society, 2010: 247 – 254.

[9] 孙钦东, 张德运, 高鹏. 基于时间序列分析的分布式拒绝服务攻击检测[J]. 计算机学报, 2005, 28(5): 767 – 773.

[10] HAYKLN S. Adaptive filter theory [M]. 3rd ed. Upper Saddle River, New Jersey: Prentlce-Hall, 1995.

[11] YAN R Y, ZHENG Q H, LI H F. Combining adaptive filtering and if flows to detect DDoS attacks within a router [J]. KSII Transactions on Internet and Information Systems, 2010, 4(3): 428 – 449.

[12] VIINIKKA J, DEBAR H. Processing intrusion detection alert aggregates with time series modeling [J]. Information Fusion, 2009, 10(4): 312 – 324.

[13] PLATT J C. Sequential minimal optimization: a fast algorithm for training support vector machines, MSR-TR-98-14 [R/OL]. http://www.bradblock.com/Sequential_Minimal_Optimization_A_Fast_Algorithm_for_Training_Support_Vector_Machine.pdf.

[14] ARLITT M, JIN T. 1998 World Cup Web Site Access Logs[EB/OL]. [2012 – 12 – 22]. http://www.acm.org/sigcomm/ITA/.

(上接第 2224 页)

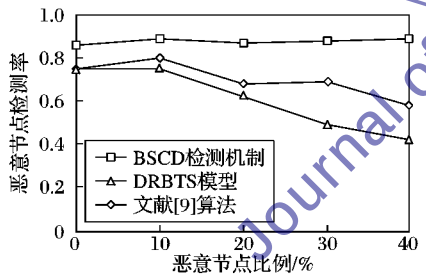


图 2　恶意节点检测率与恶意节点比例的关系

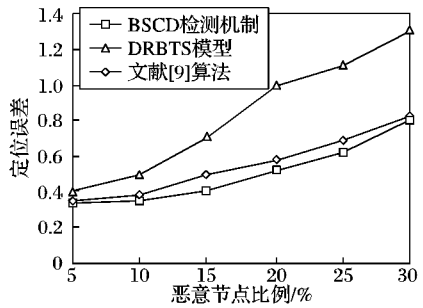


图 3　定位误差与恶意节点比例的关系

4　结语

本文提出了 BS 合谋攻击团及其检测机制——BSCD,针对声誉系统中恶意节点合谋提交虚假评价信息的行为,提出的 BSCD 通过检测单个异常推荐节点,分析推荐节点之间的评价行为相似度,并结合 BS 合谋攻击团检测算法定位出合谋攻击节点。仿真实验表明,BSCD 能够有效检测识别出 BS 合谋攻击团,提高声誉系统的恶意节点检测率和节点定位的安全性。

参考文献:

[1] 熊炼. 无线传感器网络的安全定位研究[D]. 太原: 太原理工大学, 2011.

[2] 许力. 无线传感器网络的安全和优化[M]. 北京: 电子工业出版社, 2010: 191 – 230.

[3] 杨光, 印桂生, 杨武, 等. 无线传感器网络基于节点行为的信誉评测模型[J]. 通信学报, 2009, 30(12): 18 – 26.

[4] 于满洋. 基于恶意信标节点检测的 WSNs 安全定位技术研究[D]. 哈尔滨: 哈尔滨工程大学, 2011.

[5] 张婷, 何泾沙. 基于抗局部攻击的无线传感器网络定位方法[J]. 北京交通大学学报, 2012, 36(6): 80 – 86.

[6] 杨光, 印桂生, 杨武, 等. WSNs 基于信誉机制的恶意节点识别模型[J]. 哈尔滨工业大学学报, 2009, 41(10): 158 – 162.

[7] GANERIWAL S, SRIVASTAVA M B. Reputation-based framework for high integrity sensor networks [C]// SASN'04: Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks. New York: ACM Press, 2006: 66 – 77.

[8] SRINIVASAN A, TEITELBAUM J, WU J. DRBTS: distributed reputation-based beacon trust system [C]// Proceedings of the 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing. Piscataway: IEEE, 2006: 277 – 283.

[9] 凌远景, 叶阿勇, 许力, 等. 基于声誉机制的传感器网络节点安全定位算法[J]. 计算机应用, 2012, 32(1): 70 – 73.

[10] 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.

[11] 钱雷, 王行甫. 无线传感器网络节点安全定位研究[D]. 合肥: 中国科学技术大学, 2010.

[12] 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.

[13] 冯景瑜, 张玉清, 陈深龙, 等. P2P 声誉系统中 GoodRep 攻击及其防御机制[J]. 计算机研究与发展, 2011, 48(8): 1473 – 1480.