一种基于 AOA 信任评估的无线传感器网络 Sybil 攻击检测新方法 *

张 艳[1], 范科峰[2], 张素兵[3], 莫 玮[3]
(1. 桂林电子科技大学, 广西 桂林 541004; 2. 北京邮电大学 信息安全中心, 北京 100876; 3. 中国电子技术标准化研究所 国家数字音视频及多媒体产品质量监督检测中心, 北京 100007)

摘 要: 随着无线传感器网络(WSN)技术广泛应用在数字家庭网络及其他领域,其安全问题日益突出。针对无线传感器网络中典型的 Sybil 攻击,提出了一种基于信号到达角信任评估检测新方法 TEBA。信标节点基于 Sybil 节点创建多个虚拟身份。但其物理位置相同的思想,利用信号到达角相位差对邻居节点身份作出信任评估,将低于某一信任阈值的节点身份归为 Sybil 攻击。方案引入多节点协作思想,摒弃了复杂的质心计算,实现了低时延高效性检测。仿真结果表明,该方法能防御及检测 Sybil 攻击, 有效保护系统性能。

关键词: 无线传感器网络; Sybil 攻击; 信任评估; 信号到达角; 多节点协作
中图分类号: TP393.08 **文献标志码**: A **文章编号**: 1001-3695(2010)05-1847-03
doi:10.3969/j.issn.1001-3695.2010.05.068

AOA based trust evaluation scheme for Sybil attack detection in WSN

ZHANG Yan[1], FAN Ke-feng[2], ZHANG Su-bing[3], MO Wei[3]
(1. *Guilin University of Electronic Technology*, *Guilin Guangxi* 541004, *China*; 2. *Information Security Center*, *Beijing University of Posts & Telecommunications*, *Beijing* 100876, *China*; 3. *National Digital Video*, *Audio & Multimedia Products Quality Supervision & Inspection Center*, *China Electronics Standardization Institute*, *Beijing* 100007, *China*)

Abstract: As wireless sensor networks (WSN) are widely applied in smart home networks and other new emerging areas, its security issues become increasingly prominent. Aiming at the typical Sybil attack in WSN, this paper proposed a new trust eva luation based on AOA (angle of arrival) detection scheme TEBA (trust evaluation based on AOA). According to the feature that Sybil node could create multi-identities but only with one physical position, beacon node identified Sybil identities whose signal phase difference below trust threshold by means of evaluating trust degree for adjacent sensor nodes . TEBA introduced multi-node collaborative ideas and discarded complex centroid calculation, realizing a low-latency, efficient detection. The simulation results show that TEBA can not only detect and defense Sybil attack but also protect system performance effectively.
Key words: WSN(wireless sensor network); Sybil attack; trust evaluation; AOA; multi-node collaboration

无线传感器网络(WSN)综合了分布式计算、嵌入式无线通信和传感器技术,广泛应用于计算机、半导体、通信、军事、农业等众多领域。WSN 由传感器节点协作实时监测、感知和采集监测对象的信息,通过无线和多跳中继的方式将信息汇集到中央处理节点。同时,由于其自身有限的存储空间、计算能力、有限的带宽和通信能量、无线信道的脆弱性等特点,WSN 安全问题日益突出。

Sybil 攻击是一种常见的对无线传感器网络危害巨大的攻击方式。恶意节点通过冒充其他节点身份或简单地对外声称伪造的身份,对外表现为多个传感器节点[1]。这种攻击危害到传感器网络中的诸多层面,包括路由的发现与建立、资源分配、竞争投票机制、异常行为检测等。

本文提出了一种基于 AOA 信任评估模型的 Sybil 攻击检测方案 TEBA(trust evaluation based on AOA):以信号到达角相位差为基础,信标节点(beacon node, BN)结合信任评估模型对传感器节点(sensor node,SN)信任度作出评估;系统将低于某一信任门限的节点身份列入 Sybil 黑名单并在未来的通信过程中予以排除。仿真结果表明,TEBA 能够有效防御和检测 Sybil 攻击,不失为一种好的 Sybil 攻击检测手段。

1 Sybil 攻击的危害与防御

Douceur 首次在 P2P 网络中描述了 Sybil 攻击,即在无线网络中,单一节点具有多个身份标志 ID,通过控制系统的大部分节点来削弱分布式存储算法中冗余备份的作用。Sybil 攻击主要体现在以下方面:

a)资源分配。许多网络资源是基于节点分配的,在时分复用通信模式中,物理位置相近的节点共享同一无线信道,不同节点传输使用不同时隙。Sybil 攻击利用可伪造多重虚拟身份的特性,使恶意节点得以非法方式占据大量网络资源,对合法节点造成拒绝服务攻击,为其他攻击提供有利条件。

收稿日期: 2009-09-22; **修回日期**: 2009-11-06 **基金项目**: 中国博士后科学基金资助项目(20080440333, 200902073); 国家自然科学基金委—广东联合基金重点项目(U0835004); 国家自然科学基金资助项目(60672112)

作者简介:张艳(1985-),女,广西南宁人,硕士研究生,主要研究方向为无线传感器网络技术(zhangyu1@yeah.net);范科峰(1978-),男,陕西礼县人,博士,主要研究方向为无线通信、数字版权管理;张素兵(1973-),男,山西人,博士;莫玮(1956-),男,广西南宁人,教授,博导,主要研究方向为智能化仪器、信息处理.

b)路由。Sybil 攻击可在传感器网络中对抗路由算法,如在多路径或分散路由算法中,恶意节点可通过声明多个 Sybil 身份,其被选为转发节点的可能性增大,造成看似不相交的多个路径实际上经过同一恶意节点。

c)数据融合。高效的查询协议中,簇节点或骨干节点需要对簇内多个分散的传感器节点所采集的数据进行融合,以获得所需信息的精度和可信度,从而提高系统能源与资源的利用率。少数恶意节点的误报或许不足以明显影响融合数据的准确度。然而,Sybil 攻击通过足够多的多个虚拟身份可造成信息的完全误报。

为了防御 Sybil 攻击,目前一般性的检测方法主要有基于身份认证、关系认证、地理信息认证等方式。文献[2]提出一种基于簇的平面 Merkle 哈希树的 Sybil 攻击防御机制,它将网络分成簇,单个簇内的节点维护一棵 Merkle 哈希树,利用 Merkle 哈希树生成密钥。文献[3]通过随机秘密信息预分配,利用节点身份证人确认机制,基于单向累加器建立了传感器网络节点秘密信息管理和分配方案。文献[4]提出一种引入受信节点构成分布式认证系统,由受信节点对新加入节点进行认证,保证节点签名和 ID 不能伪造,同时引入记录洗牌加入过程的票据来判定节点合法性。

基于位置认证的方式目前有基于 TOA、TDOA 和 RSSI 等认证方式。TDOA[5] 主要利用节点信号到达时间差来估算节点位置。RSSI[6] 与 TDOA 方式相似,所不同的是 RSSI 使用的是信号能量接收强度。两种方式虽然算法简单,但是容易受到环境制约,检测精度较低,且大多需要质心算法作出节点的最后定位,计算复杂度不低。

2 TEBA 网络与 AOA 数学模型

2.1 TEBA 网络模型

假设在数字家庭网络应用环境中,网络中存在一系列位置未知的普通传感器节点和部分坐标位置已知并配备测量 AOA 硬件装置的信标节点。信标节点较普通的传感器节点具有更多的额外功能,它们拥有最高的安全信任度,可从相邻的传感器节点接收数据并进行数据融合,此外,信标节点还应当有传输、对比及维护信任列表的功能。

区别于大规模的无线传感器网络应用环境,在数字家庭网络环境中,网络结构为可控配置。考虑到家庭网络中设备的可移动性以及方便扩展到一般性应用环境,这里假设传感器节点与信标节点被随机放置在一个大小为 s 的区域中,放置密度应足够大而使得任意一个信标节点通信范围至少存在一个邻居信标节点(满足齐次泊松过程)。从而传感器密度和信标节点的密度分别为 ρ_s 和 ρ_t,ρ_s 和 ρ_t 的关系应当满足 $\rho_s \geqslant \rho_t$。若至少存在 k 个传感器节点位于信标节点的天线通信范围 R 内,则信标节点可测到传感器节点信号到达角的概率为

$$P_{(SN=t)} = \frac{(P_s \pi R^2)^t}{k!} e^{-\rho_s \pi R^2} \tag{1}$$

同时,传感器节点和信标节点的随意放置意味着信标节点能侦听到传感器节点的数目存在统计独立性,因此,对于整个网络区域 S,N 个信标节点侦听到传感器节点信号到达角的概率为

$$P_{(SN\geqslant t)} = P_{(SN\geqslant t)}^{|N|} = (1 - P_{(SN<t)}^{|N|} = (1 - \sum_{i=0}^{t-1} \frac{(\rho_s \pi R^2)^i}{i!} e^{-\rho_s \pi R^2})^{|N|} \tag{2}$$

2.2 AOA 数学模型

对于信号到达角的测量,在很多场合,可通过天线阵列或多个接收器结合来实现。在 E911 系统和智能机器人导航领域中,使用 AOA 技术确定目标方向和位置的方案大多使用了高能耗的天线阵列测量信号方向,不适用于能源紧张的应用场合。针对这个问题,MIT 提出了一种融合 TDOA 和信号到达相位差的硬件解决方案——cricket compass[7],其原型系统可在 ±40°角内以 ±5°的误差确定接收信号方向。AOA 测量体现为对合作信号的多路反射参数估计,这些反射信号相互之间相关,在频谱上重叠。假设远场彼此独立的 P 个窄带信号 $S_p(t)$,$p=1,2,\cdots$,信号 P 波长为 λ,中心频率为 f,并以平面波入射到一个 M 元的任意天线阵列,从而到达角分别为 θ_1,θ_2,θ_3,$\cdots$,θ_p。假设各阵元的噪声是均值为 0、方差为 σ^2、与信号源不相关的高斯白噪声,则阵列输出可写成:

$$X(n) = A(\theta)S(n) + N(n) \tag{3}$$

$$A(\theta) = [\alpha(\theta_1), \alpha(\theta_2), \cdots, \alpha(\theta_p)] \tag{4}$$

其中:
$$\alpha(\theta_p) = [\exp(-j2\pi(x_1\cos\theta_p + y_1\sin\theta_p)/\lambda)], \cdots, \exp(-j2\pi(x_M\cos\theta_p + y_M\sin\theta_p/\lambda)^T \tag{5}$$

其中:$X(n)$ 为 M 维阵列输出列向量;$N(n)$ 为 M 维噪声列向量;$S(n)$ 为 P 维信号源列向量。于是,取接收信号的 N 次快拍,则任意阵列的协方差矩阵 R 为

$$R = E[X(n)X^H(n)] = AE[S(n)S^H(n)]A^H + \sigma^2 I = APA^H + \sigma^2 I \tag{6}$$

3 TEBA 检测方案

在初始化阶段,信标节点对其通信范围内的每个传感器节点皆设置相同的信任度 α(图 1)。值得注意,方案中假设 Sybil 节点的数目应当小于正常工作节点数,否则合法的节点将会被误报为恶意节点而遭到孤立。尽管 Sybil 节点可以伪装多重并不存在的虚拟身份,但其物理位置相同。在理想情况下,这些 Sybil 身份信号到同一信标节点的迎角应当一致,但考虑到信号在无线信道传输时加入的信道噪声,因此信号到达角会产生误差。在视距传输的简单情况下,信标节点对信号到达角度作出测量估计,将相位相差值小于门限的身份 ID 列入嫌疑列表。表 1 给出了论文中使用到的术语符号。

表 1 术语符号解析

符号	范围	意义
γ	(0,1)	判决门限
δ	(0,1)	初始嫌疑率
ε	(0,1)	最后嫌疑率
α	(0,1)	初始信任度
T	(0,60)	周期/s
ζ	$(-4/\pi, 4/\pi)$	信号到达角相位差
η	$(0,k)$	身份交集数

然而,仅一个信标节点的检测工作会造成大量的攻击误报。例如,相互独立的三个传感器节点(SN_1, SN_2, SN_3)同时与信标节点 S 通信,如果它们的物理位置相邻,同时由于信号在无线信道传输过程中环境的影响如存在折射、反射和衍射等,即使(SN_1, SN_2, SN_3)的身份皆不相同,其到达信标节点 S 的信号角度相位差仍然可能非常相近。为了提高检测精度,本文在 TEBA 检测方案中参考加入多节点协作检测[8]。

如图 2 所示,TEBA 检测方案中基本的多节点协作检测信任评估流程如下:

a)每隔一段周期 T,信标节点 A 与其邻居信标节点各自独立测量周围传感器节点身份的信号到达角(AOA),假设信标节点 A 通信范围内存在 u 个传感器节点,则它们的信号到达角将分别为 $\theta_1,\theta_2,\theta_3,\cdots,\theta_u$。为了正确评估角度相位差值,假设以 A 为基点建立坐标轴,以 45°轴线划分分别取 $\angle\theta_{A1}$、$\angle\theta_{A2}$、$\angle\theta_{A3}$、$\angle\theta_{A4}$作为四维上的基准角,如图 3 所示。

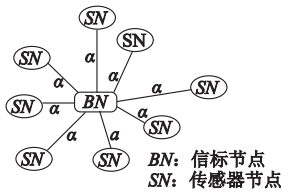

图1　TEBA网络传感器节点信任度初始化

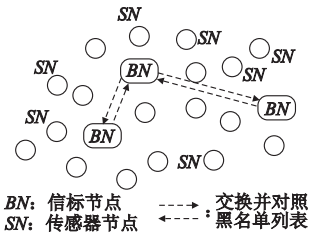

图2　多节点协作检测

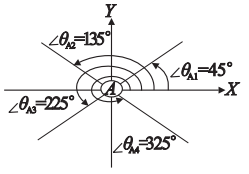

图3　四维基准角

则各节点信号相位差 $\angle\theta_{di}$ 可写成:

$$\angle\theta_{di}(i\in[1,u])=\begin{cases}\angle\theta_i-\angle\theta_{A_1},\theta_i\in[0,90^\circ]\\ \angle\theta_i-\angle\theta_{A2},\theta_i\in(90^\circ,180^\circ]\\ \angle\theta_i-\angle\theta_{A3},\theta_i\in(180^\circ,270^\circ]\\ \angle\theta_i-\angle\theta_{A4},\theta_i\in(270^\circ,360^\circ]\end{cases}\tag{7}$$

b)基于各身份信号到达角相位差,信标节点 A 挑选那些信号相位差小于门限 ζ 的节点身份归类入嫌疑身份列表,并将它们的初始身份嫌疑值设为为 δ。

c)信标节点 A 将自身嫌疑身份列表 $A1$ 与相邻信标节点(B, C, D, $E\cdots$)的嫌疑身份列表($B1$, $C1$, $D1$, $E1\cdots$)对比,找出最大嫌疑身份交集并将它们列入 Sybil 黑名单,再置名单内身份嫌疑系数 ε。

d)最后,Sybil 黑名单内信任值低于信任门限 γ 的节点身份将被视为最终的 Sybil 攻击身份。此时,可用 Flood 广播的方式将 Sybil 黑名单在网内广播。上述逻辑关系表达如下:

$$E_n=\begin{cases}\alpha-(1-\sum_{\kappa}\delta\times\varepsilon^{\kappa}) & \text{if}(SN\in\text{blacklist})\\ \alpha & \text{其他}\end{cases}\tag{8}$$

其中:κ 代表信标节点 A 联络的信标邻居数。

那些被判断为 Sybil 攻击的身份在未来的通信中应予以剔除,这在源路由协议网络中很容易实现,如 DSR 协议等。

e)注意当出现嫌疑列表身份交集数小于 η 时,系统视该次检测产生了一个意外的随机错误,该次判断过程应当予以取消并在间隔另一个周期 T 后重新进行检测。

下面对 TEBA 的检测概率进行评估。假设对于信标节点 A,它的通信范围内有 n 个传感器节点,其中 m 个为 Sybil 节点。在一次检测过程中,信标节点 A 能检测到 C 个同时位于信标节点 A 及其信标邻居检测范围内的传感器节点。而在这 C 个传感器节点中,假设存在 M 个 Sybil 节点。以 ID 代表一个任意的传感器节点身份,根据逻辑关系,Sybil 身份的检测概率为

$$P_r(\text{ID})=P_r(\Omega(\text{ID})\subseteq m)=\frac{\binom{m}{M}\binom{n-m}{C-M}}{\binom{n}{C}}\frac{m}{C}\tag{9}$$

考虑信标节点 A 与 κ 各信标邻居通信的情况,假设初始的信任值 $\alpha=1$,结合 TEBA 检测方案,此时,信标节点 A 对 Sybil 身份的检测概率为

$$P_{\text{detection}}=P_{\text{detection}}(\alpha=1\mid\kappa)=\sum_{\kappa}\frac{\binom{m}{M}\binom{n-m}{C-M}}{\binom{n}{C}}\frac{m}{C}\times\delta\times\varepsilon^{\kappa}\tag{10}$$

4　性能评估与安全分析

当实验场景为 300 m × 300 m 区域内的无线传感器网络,设节点通信距离为 30 m,信标节点数与传感器节点数分别为 10 和 100。信号传播模型为 Two-way Ground,路由协议为 DSR。网络流量为饱和 UDP 流,每次实验运行 300 s。假设网络中存在 5 个 Sybil 节点,并产生 5 个附加 Sybil 身份时,联络不同信标邻居数 κ 的检测失效率如图 4 所示。在信标节点联络数 κ 一定的情况下,检测重复次数越多,Sybil 节点检测失效率降低。假设要求检测率达到 70% 的情况下,仅与 1 个邻居信标节点联系时,需要系统重复大约 15 次左右的检测次数,大大增加了检测的时延性。在 $\kappa=5$ 的情况下,系统只需大约重复三次左右的检测就能达到 90% 以上的攻击检测率;但此时信标节点需要与 5 个信标节点数联络,通信开销会造成很大的能源消耗。因此,取中间值 $\kappa=3$ 可使系统通信开销与检测时延间的较为理想。在不同要求的应用环境下,可通过选取不同的 κ 值从而达到系统性能与开销平衡。

图 5 给出了当无线传感器网络规模为 50 个节点的实验场景下,包含 3 个 Sybil 节点并创建 10 个虚拟身份时,CRSD[8](cooperative RSS-based Sybil detection)与 TEBA 方法系统吞吐量的性能对比。由图可见,Sybil 攻击的破坏效应相当明显。无论是 CRSD 还是 TEBA,随着网络内数据流量的增多,皆会造成系统吞吐量性能大幅度降低,尤其当网络中存在 40 个饱和 UDP 流时,该效应愈加明显。这是由于当网络内部数据流增大,系统需要更多节点路径来转发数据包。在这样的情况下,Sybil 节点伪造的虚拟身份被选入有效路径的概率增大,虽然从表面上这些路径并不相交,而实际上有相当部分的数据包经过同一 Sybil 节点,造成大量的数据包被丢弃或恶意转窜改。即使仅存在 3 个 Sybil 节点,TEBA 也将降低至少 30% 的网络性能,CRSD 甚至达到 40%。无论如何,TEBA 还是能够有效地检测到 Sybil 攻击,表现出了良好的安全防御性,有力地保护了系统性能。

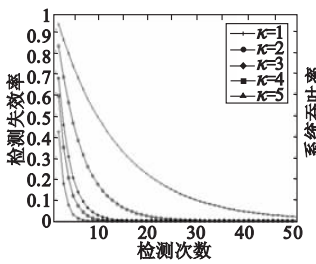

图4　信标邻居联络数κ取值不同时,TEBA检测失效率

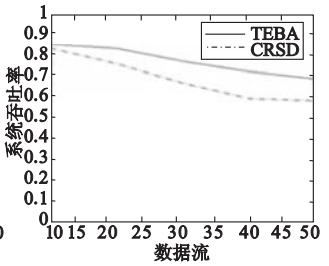

图5　TEBA与CRSD系统吞吐率性能对比

5　结束语

本文提出了无线传感器网络中一种结合信任评估模型的基于信号到达角技术的 Sybil 攻击检测方案,其基本思想是假设具有最高信任度的信标节点对与其联络的传感器节点作出信任评估。当传感器节点的信号到达角相位低于门限 ζ,信标

(下转第 1866 页)

提取出具有抗几何失真特性的归一化自相似性块作为水印嵌入块。b)利用伪 Zernike 矩的良好性质,有效地弥补了分形的不足,从而使所设计的算法对几何攻击具有高度的鲁棒性。c)利用幅度改变量测试,在自相似性块中计算出最适合嵌入水印的伪 Zernike 矩,使水印提取更加准确。此外,本方案还具有容易实现、提取水印时无须原始载体等优点,这大大增强了其用于数字图像作品版权保护的实用性,具有一定的应用价值。

表 3 算法对几何攻击及联合的抵抗能力(失真率 BER)

攻击方式		本算法	Xin[5]
旋转单位(度)	5	2.03	6.25
	10	0.98	1.56
	15	2.12	7.81
	20	0	3.12
	25	2.18	4.68
	30	3.09	5.12
	45	4.87	9.76
	60	2.08	6.02
	90	0	0
缩放	0.8	3.86	7.81
	0.9	1.08	1.56
平移(水平、垂直方向)	10	19.54	48.43
	20	12.62	43.75
	30	10.83	42.18
垂直翻转		0	0
水平翻转		0	0
缩放 1.2 + 旋转 10		3.86	4.68
缩放 1.2 + 平移 10		11.97	50.00
旋转 10 度 + 平移 20		11.04	45.31

参考文献:

[1] DONG P, BRANKOV J. G, GALATSANOS N P, *et al*. Digital watermarking robust to geometric distortions[J]. IEEE Trans on Image Processing, 2005, 12(14): 2140-2150.

[2] CHEN Qing, YANG Xiao-li, ZHAO Ji-ying. Robust image watermarking with Zernike moments[C]//Proc of CCECE 2005. Canada: IEEE, 2005: 1340-1343.

[3] LI Lei-da, GUO Bao-long, SHAO Kai. Geometrically robust image watermarking using scale-invariant feature transform and Zernike moments[J]. Chinese Optics Letters, 2007, 5(6): 332-335.

[4] 李雷达,郭宝龙,刘雅. 基于伪 Zernike 矩的抗几何攻击图像水印[J]. 光电子· 激光, 2007, 18(2): 231-235.

[5] XIN Yong-qing, LIAO S, PAWLAK M. A multibit geometrically robust image watermark based on Zernike moments[C]// Proc of the 17th International Conference on Pattern Recognition. Cambridge, UK: IEEE Press, 2004: 861-864.

[6] KANG Xian-gui, HUANG Ji-wu, YUN Shi, *et al*. A DWT-DFT composite watermarking scheme robust to both affine transform and JPEG compression, [J]. IEEE Trans on Circuits and Systems for Video Technology, 2003, 13(8): 776-786.

[7] JIN S S, CHANG D Y. Image watermarking based on invariant regions of scale-space representation[J]. IEEE Trans on Signal Processing, 2006, 54(4): 1537-1549.

[8] PAUTE J, JORDAN F. Using Fractal compression scheme to embed a digital signature into an image[C]// Proc of SPIE Photonics East Symposium. Boston: [s. n], 1996: 108-118.

[9] PI Ming-hong, LI Chun-hung, LI Hua. Anovel fractal image watermarking watermarking[J]. IEEE Trans on Multimedia, 2006, 8(3): 488-499.

[10] XIE Rong-sheng, YANG Shu-guo. A digital image watermarking method based on fractal transform in DWT domain[C]// Proc of the 1st International Conference on Modelling and Simulation. 2008.

[11] HADDADNIA J, AHMADI M, FAEZ K. An efficient feature extraction method with Pseudo-Zernike moment in RBF neural network-based human face recognition system[J]. EURASIP Journal on Applied Signal Processing, 2003, 2003(9): 890-901.

(上接第 1849 页)节点依据相关信任模型降低其信任度。为了提高检测的精确度,TEBA 参考使用了多节点协作检测思想。仿真结果表明,TEBA 能对 Sybil 节点作出有效检测,且在仿真条件相近的情况下较之于 CRSD 检测方案具有更高的系统吞吐量。事实上,为了验证其正确性和有效性,本文对于 TEBA 检测方案仅仅是做出了初步的调查结果。如何使其更为适用于普遍的路由协议如 AODV、DSDV 等和提高安全防范性能将是未来研究的工作重点。

参考文献:

[1] AYDAY E, DELGOSHA F, FEKRI F. Location-aware security services for wireless sensor networks using network coding [J]. IEEE International Conference on Computer Communications, 2007 (6-7): 1226-1234.

[2] 王晓东,孙言强,孟祥旭. WSN 中基于簇的 Sybil 攻击防御机制[J]. 计算机工程, 2009, 35(15): 129-131.

[3] 冯涛, 马建峰. 防御无线传感器网络 Sybil 攻击的新方法[J]. 通信学报, 2008, 29(6): 13-19.

[4] 聂晓文, 卢显良, 唐晖. 基于洗牌策略的 Sybil 攻击防御[J]. 电子学报, 2008, 36(11): 2144-2149.

[5] WEN M, LI H, ZHENG Y, *et al*. TDOA-based Sybil attack detection scheme for wireless sensor networks [J]. Journal of Shanghai University: English Edition, 2008, 12 (1): 66-70.

[6] DEMIRBAS M, SONG Y. An RSSI-based scheme for Sybil attack detection in wireless sensor networks[C]// Proc of International Symposium on a World of Wireless, Mobile and Multimedia Networks. 2006: 568-570.

[7] PRIYANTHA N B, MIU A K L, BALAKRISHNAN H, *et al*. The cricket compass for context-aware mobile applications[C]// Proc of the 7th Annual International Conference on Mobile Computing and Networking (MOBICOM). New York: ACM Press, 2001: 1-14.

[8] LV Shao-he, WANG Xiao-dong, ZHAO Xin, *et al*. Detecting the Sybil attack cooperatively in wireless sensor networks[C]// Proc of International Conference on Computational Intelligence and Security. 2008: 442-446.

[9] DAI Hong-jun, JIA Zhi-ping, DONG Xiao-na. An entropy-based trust modeling and evaluation for wireless sensor networks[C]// Proc of International Conference on Embedded Software and Systems. Washington DC: IEEE Computer Society, 2008: 27-34.

[10] 朱运波,胡向东. WSN 中防御 Sybil 病毒攻击的密钥预分配方案[J]. 通信技术, 2008, 41(8).

[11] BOUKERCH A, XU L, EL-KHATIB K. Trust-based security for wireless Ad hoc and sensor networks [J]. Computer Communications, 2007, 30(11-12): 2413-2427.

[12] ATAKLI I M, HU Hong-bing, CHEN Yu, *et al*. Malicious node detection in wireless sensor networks using weighted trust evaluation [C]// Proc of Spring Simulation Multi Conference. 2008: 1066-1069.