文章编号:1001 - 893X(2011)09 - 0087 - 05

无线传感器网络中检测女巫攻击的节点定位方法*

程海青[1],王 华[2],王华奎[1]

(1.太原理工大学 信息工程学院,太原 030024;2.太原理工大学 计算机科学与技术学院,太原 030024)

摘 要:为了有效抵制女巫攻击,在攻击存在的情况下提高无线传感器网络节点的定位精度,分析、总结了女巫攻击所固有的薄弱环节,提出了基于接收功率验证的检测女巫攻击的节点安全定位方法。检测机制分为两步,首先检测节点通过比较接收功率,从所接收的全部信标节点中选择出距其距离相同的信标节点,列为可疑 Sybil 节点,然后通过邻居节点间的信息交互和距离验证,最终检测出攻击节点,利用去除了 Sybil 节点的信标节点集合实现定位。仿真实验显示,当存在攻击时,检测成功概率能达到 95% 以上,定位精度提高了 9 ~ 11.64 m,表明该方法能有效检测女巫攻击,实现节点安全定位。

关键词:无线传感器网络;定位技术;安全定位;女巫攻击

中图分类号:TP393 **文献标识码**:A doi:10.3969/j.issn.1001 - 893x.2011.09.018

Detection of Sybil Attack in Localization Mechanisms of Wireless Sensor Networks

CHENG Hai-qing[1], *WANG Hua*[2], *WANG Hua-kui*[1]

(1. College of Information Engineering, Taiyuan University of Technology, Taiyuan 030024, China;
2. College of Computer Science and Technology, Taiyuan University of Technology, Taiyuan 030024, China)

Abstract: In order to resist the Sybil Attacks effectively and improve the accuracy of location discovery for wireless sensor networks(WSNs) in hostile environments where Sybil attacking nodes exist, the vulnerability of Sybil Attacks is analysed and summarized. And effective secure location approach to detect such Sybil Attacks through verifying the received power is proposed. The detecting mechanism is divided into two steps. First, the detection node finds all suspicious Sybil beacon nodes with the same distance from detection node to itself by comparing the power. And then, the Sybil beacon nodes are removed out through mutual information exchanging with neighbors. Simulation results show that the successful detection probability can achieve 95% and the proposed algorithm can improve the location discovery accuracy by 9 m to 11.64 m. Experiment proves that the attacking nodes can be detected effectively by utilizing the proposed approach and the nodes' precise locations can be obtained.

Key words: wireless sensor network(WSN); localization technique; secure localization; Sybil attack

1 引 言

在无线传感器网络的应用中,传感器节点的位置信息保障了传感器网络信息采集的有效性。现有的节点定位技术大都假设传感器节点处于安全的环境中[1-5],但是在实际的工程应用领域,由于传感器节点自身的弱安全性和脆弱性,节点失效、环境毁坏等不可控因素将影响局部乃至整个网络的定位效果。节点的安全、可靠的定位算法对于无线传感器网络必不可少。在常见的针对定位技术的攻击模型

* 收稿日期:2011 - 04 - 20;修回日期:2011 - 05 - 30

中,女巫攻击是较为常见的一种攻击[6,7]。文献[3,6-8]利用为节点分配密钥,从而对节点的身份和权限进行确认,能有效地防御女巫攻击(Sybil Attack),但是由于传感器节点的能量和计算能力的限制,不适宜使用复杂、运算量大的加密算法[9,10]。文献[11]通过对比接收功率比值的大小对信源进行检测,确定攻击节点是否存在,该算法需要至少 4 个检测节点才能达到理想的效果,检测效率不高。本文分析了女巫攻击的性质,总结了恶意节点实施女巫攻击所采用的途径及其固有的薄弱环节,提出了一种检测女巫攻击的安全定位方法。

2 节点定位技术及女巫攻击

2.1 节点定位技术

节点定位技术可大致分为两种类型:基于距离(range - based)的定位技术和距离无关(range - free)的定位技术[2,3]。在传感器网络节点定位技术中,自身位置信息未知的节点(未知节点)通过与已知自身位置信息的节点(信标节点)通信获得参考信息,然后通过一定的算法计算自身位置坐标。信标节点在网络节点中所占的比例很小,可以通过携带 GPS 定位设备或固定位置安装等手段获得自身的精确位置。恶意节点在发起攻击时一般充当信标节点的角色。

2.2 女巫攻击原理

女巫攻击就是指一个恶意节点违法地以多个身份出现,通常把该节点的多余身份称为 Sybil 节点。如图 1,当接收到未知节点 S 的定位请求时,恶意节点 B_4以多个不同身份向未知节点发送多个具有不同身份的定位参数。恶意节点 B_4以 id_1、id_2、id_3 3 个不同身份发送定位参数{(id_1, x_1, y_1),(id_2, x_2, y_2),(id_3, x_3, y_3)},未知节点虽然已经接收到 3 个不同节点的定位信息,但是这 3 个参数都是从 B_4发送来的,故 B_4破坏了信息的真实性,致使 S 计算坐标错误。

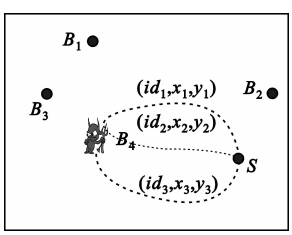

图 1 女巫攻击示例
Fig.1 Sybil attack example

在节点定位的过程中,恶意节点直接与合法节点通信。当合法的未知节点向周围发送一个定位请求时,恶意节点将监听此请求消息,同时,恶意节点伪造身份发起攻击,从所有 Sybil 节点发送出的消息事实上也是从同一个恶意节点发出的。

3 基于接收功率的女巫攻击检测方案

3.1 检测攻击的依据

分析女巫攻击的过程,其实质是由一个恶意节点虚拟出多个不同身份的节点,具有不同 id 的虚拟节点都来自于同一个物理节点,所以虚拟节点应位于以接收节点为圆心、接收节点与恶意节点为半径的圆上。如图 2 所示,Sybil 节点 id_1、id_2、id_3必然在以接收节点 S 为圆心的某一个圆上。

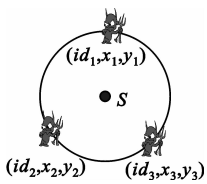

图 2 女巫攻击特点示例
Fig.2 Illustration for the character of Sybil attack

恶意节点向未知节点发送定位参数的过程中,在其通信范围内其它节点也将收到恶意节点所发送的信息,此时其它节点可充当检测节点,Sybil 节点 id_1、id_2、id_3也必然在以此检测节点为圆心、距离为半径的圆上。由于平面上不共线的三点确定一圆,id_1、id_2、id_3唯一确定一个圆,此时检测节点和未知节点将重合,否则可以判定攻击存在。如图 3 所示,S 为未知节点,S_1充当检测节点。

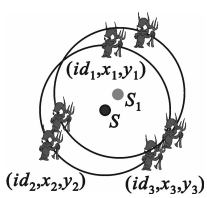

图 3 检测原理示例
Fig.3 The detection principle

由于 Sybil 节点源于同一个物理节点,攻击者为了达到攻击的目的必须修改定位参数中的坐标信息,所以女巫攻击过程必定伴随着篡改坐标的欺骗攻击。还可以利用合法的信标节点通过检测功率损耗与计算距离的一致性检测攻击是否存在。

3.2　方案实现

本文通过信号在传播过程中的衰减,估计节点之间的距离,如式(1)所示:

$$P_{rcv}=c\frac{P_{tx}}{d^{\alpha}}\Leftrightarrow d=\sqrt[\alpha]{\frac{cP_{tx}}{P_{rcv}}} \tag{1}$$

式中,P_{rcv}为接收到的信号强度,c 为常数,d 表示节点之间的距离,α 表示损耗系数,P_{tx}表示发送信号的功率。在同样的发送功率的情况下,如果节点接收功率相同,认为节点之间的距离相同。未知节点和信标节点都可以承担检测的任务,承担检测任务的节点称为检测节点。

3.2.1　未知节点作为检测节点

假设未知节点 A、B 互为邻居,即 A、B 可以互相通信。A、B 充当检测节点,检测步骤如下:

(1)未知节点 A、B 向邻居节点发送定位请求信息;

(2)A 节点接收到 n 个信标节点的应答信息,A 节点通过比较接收功率,记录距其距离相同(接收功率相同)的信标节点的 id,列为可疑 Sybil 节点,A 节点存储并与邻居节点 B 交换可疑 Sybil 节点 id 信息;B 节点行为同 A 节点;

(3)通过邻居间的信息交换,A、B 节点对比选择具有相同 id 的可疑 Sybil 节点,列为 Sybil 节点,丢弃该信标节点所发送的定位参数,并向邻居节点广播;

(4)邻居节点收到 Sybil 节点 id 列表,丢弃该信标节点所发送的定位参数。

该检测方法只需要两个未知节点即可完成检测过程,但是如果两个合法信标节点恰好位于以两个检测节点为圆心、距检测节点距离为半径的两个圆的交点上时,合法节点将被误判为 Sybil 节点。如图 4 所示,B_1、B_2为合法信标节点,S、S_1分别为两个检测节点,B_1、B_2被误认为 Sybil 节点。可以通过增加检测节点的个数减小误判的可能性。在无线传感器网络的应用过程中,由于节点的布置大都是随机的,况且任何一个在恶意节点通信范围的未知节点都可以承担检测的任务,所以误判发生的可能性对本文提出的检测正确率影响不大。

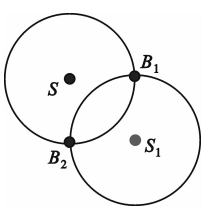

图 4　误判为 Sybil 节点

Fig.4 An illustration for misjudging

3.2.2　信标节点作为检测节点

恶意节点的攻击目的是使得未知节点不能得到正确的定位参数,从而使定位误差增大或者定位失效。所以恶意节点在发起攻击的同时,必将为每个虚拟的 Sybil 节点分别伪造一个坐标值。如图 2 所示,恶意节点发起攻击虚拟了 3 个 Sybil 节点 id_1、id_2、id_3,同时将为 3 个节点分配 3 个位置坐标$\{(x_1,y_1),(x_2,y_2),(x_3,y_3)\}$。针对恶意节点的这种篡改坐标值的欺骗攻击,利用信标节点验证距离是否满足一致性即可检测 Sybil 节点。

令(x_B,y_B)为承担检测任务信标节点的坐标,图 2 中 Sybil 节点 id_1、id_2、id_3的坐标值应该满足

$$\sqrt{(x_B-x_1)^2+(y_B-y_1)^2}=\sqrt{(x_B-x_2)^2+(y_B-y_2)^2}=\sqrt{(x_B-x_3)^2+(y_B-y_3)^2}=\sqrt[\alpha]{\frac{cP_{tx}}{P_{rcv}}} \tag{2}$$

式中,P_{tx}为恶意节点的发送功率,P_{rcv}为检测节点接收到的功率。检测节点通过验证距其距离相同的节点的坐标是否满足式(2)判断攻击是否存在。检测步骤如下:

(1)信标节点 C 伪装成未知节点承担检测任务,C 向邻居节点发送定位请求信息;

(2)C 节点接收到 n 个信标节点的应答信息(其中可能包含 Sybil 节点),C 节点通过比较接收功率,记录距其距离相同的信标节点的 id;

(3)C 节点验证 n 个信标节点的坐标是否满足公式(2),将不满足公式的节点列为 Sybil 节点;

(4)C 节点向邻居广播 Sybil 节点 id 列表;

(5)邻居节点收到由 C 发出的 Sybil 节点 id 列表,丢弃该信标节点所发送的定位参数。

4　仿真实验分析

本节以 OPNET Modeler[12] 为仿真平台对本文所提出的女巫攻击检测方法的性能进行分析。实验中未知节点的定位采用 RSSI 定位机制。仿真配置:节点天线为全向天线,通信半径为 20 m,节点分布范围为 100 m × 100 m,信标节点密度为 0.002 ~ 0.005 个/平方米,未知节点密度为 0.015 ~ 0.050 个/平方米。

图 5 显示了无攻击时网络节点的平均定位误差、存在攻击的情况下网络节点的定位误差以及采用检测方法后节点的定位误差。从图中可以看出,在存在攻击的情况下,节点的定位误差较无欺骗攻击存在时

节点的定位误差大很多。在采用本文提出的 Sybil 节点检测的方法后,定位精度提高了 9 ~ 11.64 m,节点的定位误差逼近于无攻击时的定位误差。

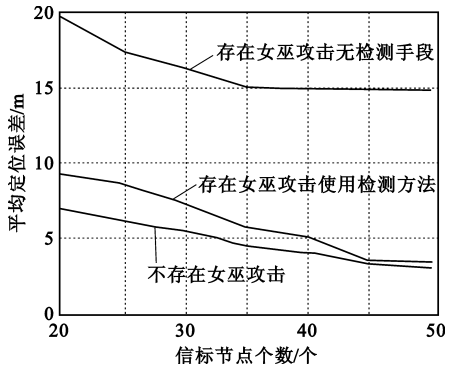

图 5 平均定位误差曲线

Fig.5 Estimation location error varying with the number of beacon nodes

信标节点和未知节点都具有检测攻击的能力,所以能明显提高检测成功率。如图 6 所示,成功检测欺骗攻击的概率随着承担检测任务的节点数目的增多而增大,检测节点布置密度为 0.03 个/平方米时,检测成功的概率能达到 95%,充分证明了本文提出的用来检测女巫攻击方法的有效性。

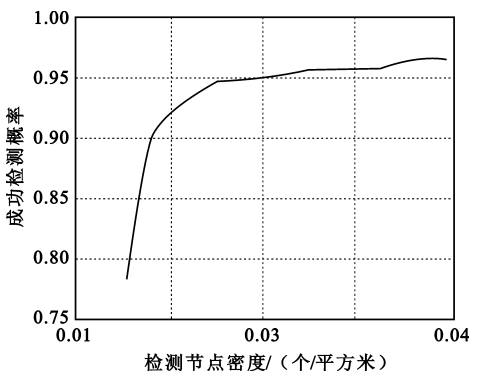

图 6 成功检测攻击概率图

Fig.6 The probability of successfully detection

5 结束语

针对无线传感器网络节点定位系统中存在的女巫攻击,本文剖析了女巫攻击的实质,提出了基于接收功率验证的攻击节点检测方法。利用核对距离的一致性寻找 Sybil 节点,通过理论分析和实验,得到如下结论:

(1)恶意节点能够发起女巫攻击的必要条件是其所虚拟的所有 Sybil 节点到此恶意节点通信范围内的任意节点的距离均相等;

(2)如果 Sybil 节点的个数大于等于 3,仅需要两个检测节点就能够检测出 Sybil 节点;当 Sybil 节点的个数等于 2 时,需要 3 个检测节点才能完成检测攻击节点的任务;

(3)检测节点的布置密度是影响检测成功率及定位精度的重要因素,信标节点和未知节点都具有检测攻击的能力,能提高检测成功率。

本文所提出的安全定位机制能有效检测出女巫攻击节点,在攻击存在的情况下能明显提高节点的定位精度。女巫攻击将改变其邻居节点的相似性,为此,今后将针对节点邻居关系做进一步研究。

参考文献:

[1] 朱博,陈曙.一种无线传感器网络质心定位改进算法[J].传感技术学报,2010,23(6):868 - 872.
ZHU Bo,CHEN Shu.An Improved Centroid Localization Algorithm for Wireless Sensor Network[J]. Chinese Journal of Sensors and Actuators,2010,23(6):868 - 872.(in Chinese)

[2] KUANG Xing - hong, SHAO Hui - he, FENG Rui. A New Distributed Localization Scheme for Wireless Sensor Networks [J]. Acta Automatica Sinica, 2008, 34(3):344 - 348.

[3] Sukhyun Yun,Jaehun Lee,Wooyong Chung,et al. A soft computing approach to localization in wireless sensor networks[J]. Expert Systems with Applications,2009,36(4):7552 - 7561.

[4] 肖硕,魏学业,王钰.基于信标优化选择的无线传感器网络定位方法研究[J].电子测量与仪器学报,2009,23(3):65 - 69.
XIAO Shuo, WEI Xue - ye, WANG Yu. Study of localization algorithm in wireless sensor networks based on optimal beacon selection[J]. Journal of Electronic Measurement and Instrument, 2009, 23(3): 65 - 69. (in Chinese)

[5] 张正勇,梅顺良.用于无线传感器网络的抗攻击节点定位算法[J].清华大学学报(自然科学版),2008,48(10):1602 - 1604.
ZHANG Zheng - yong, MEI Shun - liang. Attack - resistant node localization algorithm for wireless sensor networks[J]. Journal of Tsinghua University (Science and Technology), 2008,48(10):1602 - 1604. (in Chinese)

[6] 任秀丽,江超.基于分层网格的 Sybil 攻击检测方案[J].计算机工程,2010,36(11):159 - 163.
REN Xiu - li, JIANG Chao. Sybil Attack Detection Scheme Based on Hierarchical Grid [J]. Computer Engineering, 2010,36(11): 159 - 163. (in Chinese)

[7] Douceur J. The Sybil Attack[C]//Proceedings of International Workshop on Peer - To - Peer Systems. Cambridge: Springer, 2002:251 - 260.

[8] Levine B N, Rwiter M K, Wang C. Timing attacks in low - latency mix - based systems[C]//Proceedings of the 8th International Conference on Financial Cryptography. Key West: Springer, 2004:251 - 265.

[9] 黄晓,程宏兵,杨庚.基于身份的无线传感器网络定位认证方案[J].通信学报,2010,31(3):115 - 122.
HUANG Xiao, CHENG Hong - bing, YANG Geng. Identity - based authentication localization scheme for wireless sensor network[J]. Journal on Communications,2010, 31(3): 115 - 122. (in Chinese)

[10] Haifeng Yu, Michael Kaminsky, Phillip B Gibbons. SybilGuard: Defending Against Sybil Attacks via Social Networks [C]//Proceedings of the ACM SIGCOMM Conference on Computer Communications. Pisa: ACM, 2006:267 - 278.

[11] Demirbas M, Song Y. An RSSI - based Scheme for Sybil Attack Detection in Wireless Sensor Networks[C]//Proceedings of 2006 International Symposium on Wireless, Mobile and Multimedia Networks. Buffalo: IEEE, 2006:564 - 570.

[12] Mohd Nazri Ismail, Abdullah Mohd Zin. Network Analyzer Development: Independent Data OPNET Simulation Tool and Real Network Comparison[J]. Management and Technology, 2010,1(1):97 - 105.

作者简介:

程海青(1977—),男,山西朔州人,2006 年获硕士学位,现为博士研究生、工程师、CCF 会员,主要从事无线传感器网络研究;

CHENG Hai - qing was born in Shuozhou, Shanxi Province, in 1977. He received the M.S. degree in 2006. He is now an engineer and CCF member, and currently working toward the Ph.D. degree. His research concerns wireless sensor networks.

Email: chqwhlily@163.com

王　华(1978—),女,河北邯郸人,2006 年获硕士学位,现为讲师、ACM 会员,主要研究方向为计算机仿真技术;

WANG Hua was born in Handan, Hebei Province, in 1978. She received the M.S. degree in 2006. She is now a lecturer and ACM member. Her research concerns network simulation.

王华奎(1946—),男,山西襄垣人,1981 年获硕士学位,现为教授、博士生导师,主要从事无线传感器网络及超宽带无线电的研究。

WANG Hua - kui was born in Xiangyuan, Shanxi Province, in 1946. He received the M.S. degree in 1981. He is now a professor and also the Ph.D. supervisor. His research concerns wireless sensor networks and ultra-wideband radio.

本刊加入“万方数据 - 数字化期刊群”等数据库的声明

为了适应我国信息化建设的需要,扩大作者学术交流渠道,实现科技期刊编辑、出版发行工作的电子化,推进科技信息交流的网络化进程,本刊现已加入“万方数据 - 数字化期刊群”、“中国学术期刊(光盘版)”、“中国期刊全文数据库”、“中国学术期刊网”、“中文科技期刊数据库”、“中国期刊网”、“教育阅读网”等本刊目次页上著录的数据库,本刊录用发表的论文,将由编辑部统一纳入上述数据库,进入因特网或光盘提供信息服务。本刊所付稿酬已包含著作权使用费和刊物内容上网服务报酬,不再另付。凡有不同意者,请事先声明,本刊将作适当处理。

《电讯技术》编辑部