|  |  |  |
| --- | --- | --- |
|  | Available online at www.sciencedirect.com |  |
| **ScienceDirect** |
| AASRI Procedia 5 ( 2013 ) 62 – 66 |
| 2013 AA ASRI Conf ference on P Parallel and Distributed d Computing g and Syste ems  Co-SR RL: A Co onvex O Optimiza ation Alg gorithm f for Anch hor  Localiz zation in n Wireles ss Senso or Netwo orks  Wu Liu 1) ), Donghon ng Sun 1), P Ping Ren 2), , Yihui Zha ang 3)  *1) N Network Research h Center of Tsing ghua University, B Beijing, China*  *2)College of f Mathematics Sci ience, Chongqing g Normal Univers sity, Chongqing, C China*  *3)College of Eco onomics and Man agement, North C China University of Technology, P P.R. China* | | |

**Abst tract**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| This | paper propose ed a Convex Op ptimization me ethod which is | | called Co-SRL L and is used to o localize senso or location in | |
| Wire eless Sensor Ne etworks.Co-SRL L can be used to o help the node e to localize a fr riendnode or m mobile node usin ng anchors. In | | | | |
| Co-S SRL, convex op ptimization algo orithm is used | | forthe estimati onof malicious s nodeposition.S Simulation resu ult shows that | | |
| Co-S SRL is both se ecure and robu ust, in an envir ronment withou ut colluding, C Co-SRLcan iden ntify more tha an half of the | | | | |
| malic cious nodes; a and in an envir ronment with c colluding, no m more than 15% % of malicious s nodescan esc | | | | ape from the |

ident tification of our r methods.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| © 2013 The Authors. Published by Elsevier B.V. ong, REN Ping g and ZHANG Open access under [CC BY-NC-ND license.](http://creativecommons.org/licenses/by-nc-nd/3.0/) G [Yihui.Publis shed by](http://creativecommons.org/licenses/by-nc-nd/3.0/) Elsev vier B.V.  Selection and/or peer review under responsibility of American Applied Science Research Institute Sele ection and/or p peer review un nder responsib bility of Amer rican Applied Science Rese earch Institute | | | | |
| KeyW Words: Wireless N Network; Sensor Network; Netwo | | | rk Security; Algo orithm; Mean Squ uare Error | |
| **1. In ntroduction a and Related W Works** | | | | |
| As the rapid | | developmen nt of Internet t and netwo ork technolog gies especiall ly the wirele ess network | | |
| techn nologies, now w there are m more and mor | | | e people wor rking, studyin ng and enterta ainment from | Internet via |
| wire eless network. . But as the o openness of w wireless netwo ork, there are many securi ty events occ curred which | | | | |
| lead | great loss of f money for u sers using wir reless network k. So for secu urity consider ration and bein ng served as | | | |
| the e evidence of co omputer crim es and further r to finder the e location of t he crimes, the e localization | | | | technique is |
| very y important in wireless sens or networks. | | | | |
| 2212-6716 © 2013 The Authors. Published by Elsevier B.V. | | | Open access under [CC BY-NC-ND license.](http://creativecommons.org/licenses/by-nc-nd/3.0/) | |

Selection and/or peer review under responsibility of American Applied Science Research Institute

doi: 10.1016/j.aasri.2013.10.059

*Wu Liu et al. / AASRI Procedia 5 ( 2013 ) 62 – 66*  63

Currently, there are mainly the range based localization methods and the range free localization methods in wireless networks. The rangebased localization methods as proposed in [10][8][4], localize nodeswith property measurement.On the other hand, the rangefree localizationmethods proposed in [5][2][3][9]localize anchors without property measurement. We can tolerate that the website with bad content such as sex and violence are banned for the common good of society[5], but it may be a big pity that some websites with academic disputations are banned so not reachable only for political reason. [6]Moreover, one path may be broken down resulting in some websites not available to certain people, but actually they can still visit the webs after many attempts of trying other way only if the websites have other paths. In addition, sometimes though the websites are still available to us, we can always find a best way, i.e. with the highest speed to use.In one word, we need a put up way which can make the accessibility of the wireless sensor network more robust with better performance.

In fact, there are many papersthat study the localizationproblems in sensor networks using optimization method. For example,[3] described localization information distributing propagation methods.[10]gave a time a localization discovery method in wireless sensornetworks.The Co-SRL system is answer we find. In Co-SRL, there is not any center server, and only a register server generate identifications for the nodes who want to join the system, but not one is responsible for monitoring the behaviors single nodes. When strange nodes come to certain nodes and request for service, the requested nodes make their own opinions on response positively or negatively, according to their knowledge of the coming nodes.

This paper is arranged as follows: In section 2, we first introduce some basic principles of localization in wireless sensor networks and the optimization method, and then talk about the Co-SRL. In section 3, we present the simulation results of Co-SRL.And finally, we give the conclusion of this paper.

**2. The Algorithm of Co-SRL**

|  |
| --- |
| problem itself is presented. The sensor network is � � ���� � � �� � � ��randomlydeployed. ��is an anchor, and ����� � ����� ����� is the position set of ��. Both the mobile target and all communications between different  of them are malicious in a network. Our enhanced protocol, named Advanced Distance Bounding (AAD) |

protocol uses the high-speedDBtechnique.By Using of AAD, it can preventfrom many network attacks aiming at wireless sensor networks such as wormhole attacks [1],Sybil attack [1] and Distance reduction attacks etc., because in this case, malicious anchorswith faked position information will be detectedimmediately by a

|  |
| --- |
| shownabove, if there existmeasurementnegative errorsthe intersection region ���� of the disks ����� may be empty. The disk ����� corresponds to the circle drawn with the position of anchor ��being served the center and the distance between��and the target t as the radius. In this case, it will result in the increased distance estimation����node ���. Let�����circles. There must exist some malicious nodes in the non-empty region ���������Localization,it would minimize the worst case error in estimation.Where �� is the point satisfyingthat ���������center.As a result, to obtain ��,we will find the solution of the following equation (4.1). All points in������� � ��� � ��������� � �� denotes the increased bound disks, andlet ����  �may likely be the position of Malicious Node. ��of������� � ��, for any � � ��. Butit is very difficult to calculate the geometric � denotes the corresponding increased bound  �is used as the Malicious Node  � which is the intersection of |

|  |  |
| --- | --- |
| 64 | *Wu Liu et al. / AASRI Procedia 5 ( 2013 ) 62 – 66*  Where, � � � � �. In fact, it means that we use a common factor �tosimultaneously shrink������������������ � ����� ����� � ��� � � ��������������  � (all disks), as much as  � ���� � � �� � � �� �����  objective function as shown in equation (4.1) is to maximize�, and finally to minimize� which is the shrinking factor. Clearly, there existsa unique optimal solution ���� ��� for this convex optimization problem.  Where �� is the Largrangian multiplier [7]. By using the algorithm which is presented in Algorithm 1, the ������ � � � �� ���������� ��� ���� � ������ ������� (4.2)  and get the solution��(the center of ������will be served as the approximation of the localization of the Malicious Node. The �valuekeeps increasingin algorithm 1,which willresult in the reduction of ������) after sometimes of repeat when ����� has been reduced greatly. � . Finally, the itstopped  minimization.  Algorithm 1. The optimization method to obtain an approximation to the geometric center |

1: Initialize x, *LM*=*LM*(0)=1.00>0,�=10.00>0,ERR=1×10-6>0.

2: repeat

3: Beginning at x, calculate *x\*(LM) by minimizing the objective in* (4.2).

4: Update x:= *x\*(LM); LM*:= �·*LM*.

|  |
| --- |
| Algorithm 1: The optimization algorithm  anchors can perform the localization operations. In this research, it is assumed that the malicious node ��� has adequate ability to perform the |

**3. Simulation Results**

The proposed methodhas been implementedusingthe Matlab software. We apply the algorithm into the design the Co-SRLsystem which is an application overlay of the physical networks. It is constructed by the nodes and their accessible parts of the Internet. every peer in the system is a proxy which voluntarily relay the traffic of pass through it . Each node of Co-SRLis composed of 4 subsystems: The Functional-Module, the Calculation-Engine, the Friends-List and the Evaluation-Engine. Where, the Functional-Module is used for transferring traffic, registering and other functions. Our policy model for admission control is implemented in the calculation engine. When a new node comes, the calculate engine is responsible to calculate its trust value



|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *Wu Liu et al. / AASRI Procedia 5 ( 2013 ) 62 – 66*  for further calculation for the calculate engine.We construct a simulation field with ���� � ���� . ��������������������������������������and the Malicious Node was restrictedto����. We randomly deployed anchorsin the range of the Malicious Node t. We chose ������=0.1 asthe maximum value of measurement of the error proportion. ����� � �������������������value forthe lie proportion. Therefore, ������������������������������������������������������������, set its distance ������ ���� � �� � �������.  method ���������������������������������������������������������������������������� the maliciousanchors ����������������� ��������������������������������������������������   |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | Simulation Results of Co-SRL   |  |  |  |  | | --- | --- | --- | --- | | Malicious Anchors Detected | 1 |  | Without-Collude | | 0.8 | | 0.6 | | 0.4 | With-Collude | | 0.2 | | 0 | | 5 6 7 8 9 10 11 12 13 |   Total number of Anchors | | 65 |

Figure 2.Simulation result of our method

|  |  |
| --- | --- |
|  | �������������������������������������������������������[3] ���������������������������������������������� . �������������������������������������������������[6]. Figure 2 shows the simulation results of our method, �������������������������������� ������������������������������������������������������������� ���������� that in [8] and error prone measurements,  �������������������������������������������������������������that aregotten by the method proposed by us ��� � ���� |

**4. Conclusion**

This paper proposed a Convex Optimization method which is called Co-SRL and is used to localize sensor location in Wireless Sensor Networks. Co-SRLcan be used to help the node to localize a friendly target or

66  *Wu Liu et al. / AASRI Procedia 5 ( 2013 ) 62 – 66*

mobile node using anchors. Our localization methodCo-SRLestimate the malicious nodesposition using convex optimization methods.

**5. Acknowledgment**

This work gets the support of China NSFC No. 61272427, and the support of 863 Project No.2011AA010704 and 2012BAH38B03.

**References**

[1] H. Rowaihy, W. Enck, P. McDaniel, and T. La Porta. Limiting Sybil attacks in wireless networks.

Technical Report NASTR-0017-2005, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, July 2005.

[2] E. Damiani, S. D. C. di Vimercati, S. Paraboschi, P. Samarati, and F. Violante. A reputation-based approach for choosing reliable resources in wireless networks. Proceedings of the Ninth ACM Conference on Computer and Communications Security, pp.207–216, 2002.

[3] S. Ratnasamy, M. Handley, R. Karp, and S. Shenker. Topologically-Aware sensor network Construction and Server Selection. Proceedings of IEEE INFOCOM, pp. 1190–1199, Jun. 2002.

[4] Sun, Dong. Study on Anti-Attack Model for Low-Latency Anonymous Communication System, International Conference on Cloud and Green Computing,1-3 November 2012, Xiangtan, China. [5] Ping, Sunbin, and Donghong. A Data Security Protection Mechanism based on Transparent Biometric Authentication for Mobile Intelligent Terminals, 3nd Cybercrime and Trustworthy Computing Workshop(CTC2012), 29-31 November 2012, Ballarat, Australia.

[6] S. Ratnasamy, M. Handley, R. Karp, and S. Shenker. Topologically- Aware Overlay Construction and Server Selection. Proceedings of IEEE INFOCOM, pp. 1190-1199, Jun. 2002.

[7] Zhang H, Duan HX, Wu JP. RRM: An incentive reputation model for promoting good behaviors in distributed systems. SCIENCE IN CHINA SERIES F-INFORMATION SCIENCES,vol.51, no. 11, pp.

1871-1882   
[8] Chakraborty S, Ray I. TrustBAC-Integrating Trust Relationships into the RBAC Model for Access Control in Open Systems. Proceedings of ACM Symposium on Access Control Models and Technologies. Lake Tahoe. ACM Press, 2006. 49-58.

[9] Sun, Donghong,Xiong and Haibin. Mobile Intelligent Terminal Based Remote Monitoring and Management System, 3nd Cybercrime and Trustworthy Computing Workshop(CTC2012), 29-31 November 2012, Ballarat, Australia.

[10] Wu Liu, DuanHaixing, Jianping Wu. Study on Man-In-The-Middle Attack and Defending Techniques in Wireless Networks. 2012 Second International Conference on Electronics,Communications and Control (ICECC 2012), 10-12, September 2012, Zhoushan, China.