Available online at www.sciencedirect.com

ScienceDirect

AASRI Procedia 5 (2013) 62 – 66

AASRI Procedia

www.elsevier.com/locate/procedia

2013 AASRI Conference on Parallel and Distributed Computing and Systems

# Co-SRL: A Convex Optimization Algorithm for Anchor Localization in Wireless Sensor Networks

Wu Liu [1)], Donghong Sun [1)], Ping Ren [2)], Yihui Zhang [3)]

*1) Network Research Center of Tsinghua University, Beijing, China*
*2)College of Mathematics Science, Chongqing Normal University, Chongqing, China*
*3)College of Economics and Management, North China University of Technology, P.R. China*

**Abstract**

This paper proposed a Convex Optimization method which is called Co-SRL and is used to localize sensor location in Wireless Sensor Networks.Co-SRL can be used to help the node to localize a friendnode or mobile node using anchors. In Co-SRL, convex optimization algorithm is used forthe estimationof malicious nodeposition.Simulation result shows that Co-SRL is both secure and robust, in an environment without colluding, Co-SRLcan identify more than half of the malicious nodes; and in an environment with colluding, no more than 15% of malicious nodescan escape from the identification of our methods.



KeyWords: Wireless Network; Sensor Network; Network Security; Algorithm; Mean Square Error

## 1. Introduction and Related Works

As the rapid development of Internet and network technologies especially the wireless network technologies, now there are more and more people working, studying and entertainment from Internet via wireless network. But as the openness of wireless network, there are many security events occurred which lead great loss of money for users using wireless network. So for security consideration and being served as the evidence of computer crimes and further to finder the location of the crimes, the localization technique is very important in wireless sensor networks.


doi:10.1016/j.aasri.2013.10.059

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

For each of the specific sub-problems, the problem specific assumptions will be presented when the problem itself is presented. The sensor network is $\mathrm{A} = \{S_i, \mathrm{i} = 1, \cdots, \mathrm{n}\}$randomlydeployed. $S_i$is an anchor, and $s_i(s_i = (s_{ix}, s_{iy}))$ is the position set of $S_i$. Both the mobile target and all communications between different anchors are bidirectional.

This paper gave a convex optimizationbased method to help node to localize anchors, given that at most M 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 Malicious Node. Why? The reason can be seen as follows.

Basically, we use the convex optimizationtechnique for the Malicious Node position estimation. As shownabove, if there existmeasurementnegative errorsthe intersection region $\mathrm{Reg}_t$ of the disks $\mathrm{Dsk}_{ti}$ may be empty. The disk $\mathrm{Dsk}_{ti}$ corresponds to the circle drawn with the position of anchor $\mathrm{s}_i$being served the center and the distance between$\mathrm{s}_i$and the target t as the radius. In this case, it will result in the increased distance estimation$\mathrm{DE}'_{ti} = \frac{\mathrm{DE}_{ti}}{1-\mathrm{ERR}_{max}}$, if we increase a factor of$\frac{1}{1-\mathrm{ERR}_{max}}$ to the distance estimates$\mathrm{DE}_{ti}$for the malicious node $\mathrm{MN}_t$. Let$\mathrm{Dsk}'_{ti}$ denotes the increased bound disks, andlet $\mathrm{BC}'_{ti}$denotes the corresponding increased bound circles. There must exist some malicious nodes in the non-empty region $\mathrm{Reg}'_t$ which is the intersection of $\mathrm{Dsk}'_{ti}$.

All points in$\mathrm{Reg}'_t$may likely be the position of Malicious Node. $\mathrm{G}_c$of$\mathrm{Reg}'_t$is used as the Malicious Node Localization,it would minimize the worst case error in estimation.Where $\mathrm{G}_c$ is the point satisfyingthat $\max_{x\in \mathrm{Reg}'_t}\|x - \mathrm{G}_c\| \leq \max_{x\in \mathrm{Reg}'_t}\|x - y\|$, for any $\mathrm{y} \neq \mathrm{G}_c$. Butit is very difficult to calculate the geometric center.As a result, to obtain $\mathrm{G}_c$,we will find the solution of the following equation (4.1).

$$\max_{x,\alpha} \quad \alpha$$
$$subject\ to\ \|x - S_i\|^2 \le [\mathrm{r}'_{ti}\beta]^2, i = 1, \cdots, N, \quad (4.1)$$
$$x \in \mathrm{E}^2, \alpha \ge 0$$

Where, $\alpha + \beta = 1$.

In fact, it means that we use a common factor $\beta$tosimultaneously shrink$\mathrm{Dsk}'_{ti}$ (all disks), as much as possible, it only need to ensure that there exist at least one member in the intersection among the disks. The first N constraints in equation (4.1) can ensure the condition of non-empty intersectionamong the disks. The objective function as shown in equation (4.1) is to maximize$\alpha$, and finally to minimize$\beta$ which is the shrinking factor. Clearly, there existsa unique optimal solution $(x^*, \alpha^*)$ for this convex optimization problem. Here $x^*$is named as the algebraic centre AC of the non-empty region$\mathrm{Reg}'_t$. To simplify the solution of the in (4.1), wetransform it into the following equation (4.2).

$$\min_{x,\alpha} -LM \cdot \alpha - \sum_{i=1}^{N} log[(\mathrm{DE}'_{ti}\beta)^2 - \|x - s_i\|^2] - \log(\alpha) \quad (4.2)$$

Where $LM$ is the Largrangian multiplier [7]. By using the algorithm which is presented in Algorithm 1, the aboveproblem can be efficiently solved.

As shown in Algorithm 1,in Line 3,it uses the newton method [7] with toleranceERR $= 1 \times 10^{-6}$ for the minimization.

The $\alpha$valuekeeps increasingin algorithm 1,which willresult in the reduction of $\mathrm{Dsk}'_{ti}$. Finally, the itstopped and get the solution$x^*$(the center of $\mathrm{Reg}'_t$) after sometimes of repeat when $\mathrm{Reg}'_t$ has been reduced greatly. $x^*$will be served as the approximation of the localization of the Malicious Node.

Algorithm 1. The optimization method to obtain an approximation to the geometric center

1: Initialize x, $LM$=$LM^{(0)}$=1.00>0,μ=10.00>0,ERR=$1\times10^{-6}$>0.

2: repeat

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

4: Update x:= $x^*(LM)$; $LM$:= μ·$LM$.

Algorithm 1: The optimization algorithm

In this research, it is assumed that the malicious node $\mathrm{MN}_t$ has adequate ability to perform the localizationoperations in Algorithm 1. Otherwise, if it cannot perform the localization operations, then the anchors can perform the localization operations.

## 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

and reflect to the friend list to record, and when the node interact with some new node, as the functional module offers or demands the service, the evaluate engine estimate the Recommendation and record in order for further calculation for the calculate engine.We construct a simulation field with $100\text{m} \times 100\text{m}$. The communication range of the anchors and the Malicious Node was restrictedto $50\text{mm}$. We randomly deployed anchorsin the range of the Malicious Node t. We chose $\text{ERR}_{max}$=0.1 asthe maximum value of measurement of the error proportion. $LP_{max} = 1.0$ as the maximum value forthe lie proportion. Therefore, a malicious anchor$S_i$with $\text{DE}_{ti}$as its distance estimate from t, set its distance $[\text{DE}_{ti}, \text{DE}_{ti} \cdot (1 + LP_{max})]$.

We also studied the effectiveness of our method with different values of LP. When there is no measure-menterrors, the results were averaged over 100 iterations for a given total anchors number in therange of the Malicious Node. For all the runs, the number of malicious anchors is no more than M. Our method localized the Malicious Node correctly in 100% of the cases and also caught the maliciousanchors fully success. We do not present the result here because it is guaranteed by theory as well.

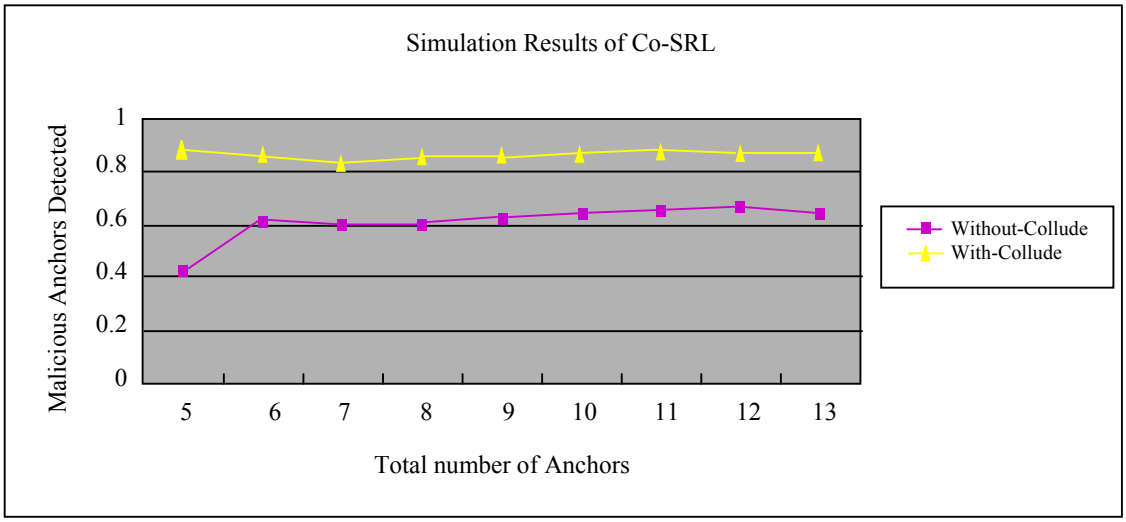


Figure 2.Simulation result of our method

When there exist error prone measurements, we compare the error in localization in our method with that in [8] and [3] to demonstrate the effectiveness of our method . Everyone knows that the methodin [3]is prone to large errors when the anchors are lying [6]. Figure 2 shows the simulation results of our method, which are averaged over 50 runs. If the number of the anchors in the range of t is given by N, the number of malicious anchors M belongs to $\left\{1, \cdots, \left[\frac{N}{2}\right] - 2\right\}$. In the simulation, the anchors number N in the range of an Malicious Node belonged to $\{5, \cdots, 13\}$. Figure 2 shows the average, fraction of malicious anchors that aregotten by the method proposed by us over 50 runs.

## 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

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.