International Journal of Information Processing, 8(3), 51-62, 2014
ISSN : 0973-8215
IK International Publishing House Pvt. Ltd., New Delhi, India

Identifying Cheating Anchor Nodes using Maximum Likelihood and Mahalanobis Distance

Jeril Kuriakose[a], Amruth V[b] Swathy Nandhini[c] Abhilash V[d]

[a]School of Computing and Information Technology (SCIT), Manipal University Jaipur, Jaipur, India, Contact: jeril@muj.manipal.edu

[b]Department of Information Science and Engineering, Bearys Institute of Technology, Mangalore, India.

[c]Department of Information Technology, Jayam College of Engineering and Technology, Dharmapuri, India.

[d]Freelancer.

Malicious anchor nodes will constantly hinder genuine and appropriate localization. Discovering the malicious or vulnerable anchor node is an essential problem in Wireless Sensor Networks (WSNs). In wireless sensor networks, anchor nodes are the nodes that know its current location. Neighbouring nodes or non-anchor nodes calculate its location (or its location reference) with the help of anchor nodes. Ingenuous localization is not possible in the presence of a cheating anchor node or a cheating node. Nowadays, it's a challenging task to identify the cheating anchor node or cheating node in a network. Even after finding out the location of the cheating anchor node, there is no assurance, that the identified node is legitimate or not. This paper aims to localize the cheating anchor nodes using trilateration algorithm and later associate it with maximum likelihood expectation technique (MLE), and Mahalanobis distance to obtain maximum accuracy in identifying malicious or cheating anchor nodes during localization. We were able to attain a considerable reduction in the error achieved during localization. For implementation purpose we simulated our scheme using ns-3 network simulator.

Keywords : Anchor Node, Distance-based Localization, Mahalanobis Distance, Maximum Likelihood Expectation, Security, Trilateration, Wireless Sensor Networks.

1. INTRODUCTION

Wireless Adhoc and sensor networks are on a steady rise in the recent decade. This is because of their reduced cost in deployment and maintenance. Advancements in radio frequency spectrum also carved way for the improvement in the data rate for communication. Many devices belong to wireless ad hoc and sensor networks; one among them is anchor node [1-8]. Anchor nodes are the nodes that know its current location. Neighbouring nodes or non-anchor nodes calculate its location (or location reference) with the help of anchor nodes, and its working is quite referable to Light House.

The location of the nodes plays a significant role in many areas as routing, surveillance and monitoring, military etc. The sensor nodes must know their location reference to carry-out location-based routing (LR) [9-12]. To find out the shortest route, the location aided routing (LAR) [13-15] makes use of the locality reference of the sensor nodes. In some industries the sensor nodes are used to identify minute changes as pressure, temperature and gas leak, and in military, robots are used to detect landmine where in both the cases location information plays a key part.

Anchor nodes can also be used to find the current location of any device (mobile phones, ob-

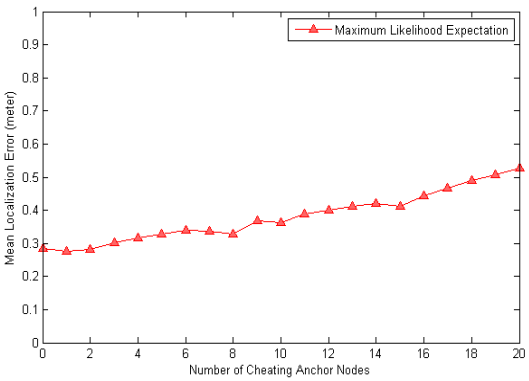

Figure 13. Mean Error after Comparing with Maximum Likelihood Function.

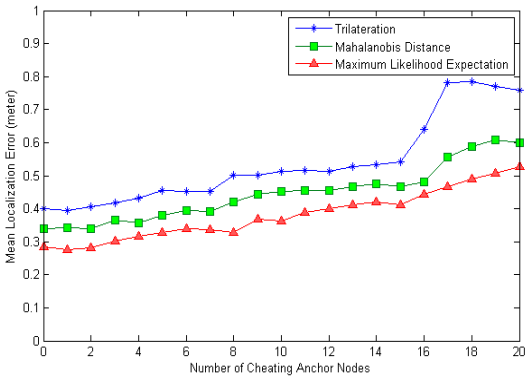

Figure 14. Result Comparison.

We have proposed a novel scheme using maximum likelihood and trilateration technique to identify malicious anchor nodes. The error can be increased if hindrance, interferences, and attenuation caused by signal fading, and noise are additional. Our scheme can also be modelled to overcome such disturbances by using some statistical distributions like Rayleigh or Rician distributions [34]. Our algorithm performed consistently for different topologies.

Our scheme can be extended for mobile sensor node with an intermittent attack type. Our framework can be extended to acoustic and ultra-wideband (UWB) technology. Using energy efficiency as a benchmark is quite challenging. Our algorithm was implemented in 2-D plane and can be extended to 3-D plane also.

7. CONCLUSIONS

For smart environments, security plays a very essential part. In this paper, we discussed about localizing malicious anchor nodes in a secured manner, using trilateration technique and comparing the results obtained with maximum likelihood expectation and Mahalanobis distance. By both the techniques way we were able to reduce the error attained during localization. However, maximum likelihood expectation outperformed Mahalanobis distance in perceiving cheating beacon nodes. By using maximum likelihood expectation and Mahalanobis distance we can obtain consistent and proficient results. Our results show that as the malicious anchor nodes increases, the simulation time and error obtained during location discovery slightly increases. The accuracy obtained in our work can be used as assistance in some wireless applications. Some imminent events for further research have been discussed.

REFERENCES

1. R Want, A Hopper, V Falcao and J Gibbons. The Active Badge Location System, *ACM Transactions on Information Systems*, 10:91–102, 1992.
2. J Liu, Y Zhang and F Zhao. Robust Distributed Node Localization with Error Management, *In Proceedings of ACM MobiHoc*, pages 250–261, 2006.
3. M W Carter, H H Jin, M A Saunders and Y Ye. SpaseLoc: An Adaptive Subproblem Algorithm for Scalable Wireless Sensor Network Localization, *SIAM Journal of Optimization*, 1102–1128, 2006.
4. P Bahl and V N Padmanabhan. RADAR: An In-Building RF Based User Location and Tracking System, *In Proceedings of IEEE INFOCOM*, 2:775–784, 2000.
5. Niculescu and B Nath. DV Based Positioning in Ad Hoc Networks, *Journal of Telecommunication Systems*, 22:267–280, 2003.
6. N Priyantha, A Chakraborty and H Balakrishnan. The Cricket Location-Support System, *In Proceedings of ACM MobiCom*, pages 32–43, 2000.
7. R Stoleru and J A Stankovic. Probability Grid:

A Location Estimation Scheme for Wireless Sensor Networks, *In Proceedings of First IEEE Conference on Sensor and Ad Hoc Communication and Networks (SECON 04)*, pages 430–438, 2004.

8. N Bulusu, J Heidemann and D Estrin. GPS-Less Low Cost Outdoor Localization for Very Small Devices, *IEEE Personal Communication Magazine*, 7(5):28–34, Oct. 2000.
9. Tracy Camp, Jeff Boleng, Brad Williams, Lucas Wilcox and William Navidi. Performance Comparison of Two Location Based Routing Protocols for Ad Hoc Networks, *IEEE Infocom*, pages 1678–1687, 2002.
10. Ljubica Blazevic, Jean-Yves Le Boudec and Silvia Giordano. A Location-Based Routing Method for Mobile Ad Hoc Networks, *IEEE Transactions on Mobile Computing*, 4(2):97–110, 2005.
11. Holger Fubler, Martin Mauve. Location Based Routing for Vehicular AdHoc Networks, *In Proceedings of ACM MOBICOM*, 7(1):47–49, 2002.
12. H Qu, S B Wicke. Co-designed Anchor-Free Localization and Location-based Routing Algorithm for Rapidly-deployed Wireless Sensor Networks, *Information Fusion*, 9(3):425–439, 2008.
13. Kuhn, R Wattenhofer and A Zollinger. Worst-case Optimal and Average-case Efficient Geometric Ad-Hoc Routing, *In Proceedings of the 4th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, pages 267–278, 2003.
14. Karim El Defrawy and Gene Tsudik. ALARM: Anonymous Location-Aided Routing in Suspicious MANETs, *IEEE Transactions on Mobile Computing,* 10(9):1345–1358, 2011.
15. Young-Bae Ko and Nitin H Vaidya. Location-Aided Routing (LAR) in Mobile Ad-Hoc Networks, *Wireless Networks*, pages 307–321, 2000.
16. Murtuza Jadliwala, Sheng Zhong, Shambhu Upadhyaya, Chunming Qiao and Jean-Pierre Hubaux. Secure Distance-Based Localization in the Presence of Cheating Anchor Nodes, *IEEE Transactions on Mobile Computing*, 9(6):810–823, 2010.
17. Z Li, W Trappe, Y Zhang and B Nath. Robust Statistical Methods for Securing Wireless Localization in Sensor Networks, *In Proceedings of Fourth International Symposium on Information Processing in Sensor Networks (IPSN 05)*, pages 91–98, 2005.
18. Liu, P Ning and W Du. Attack-Resistant Location Estimation in Sensor Networks, *in Proceedings of Fourth International Symposium on Information Processing in Sensor Networks (IPSN 05)*, pages 13–18, 2005.
19. Liu, P Ning and W Du. Detecting Malicious Beacon Nodes for Secure Location Discovery in Wireless Sensor Networks, *In Proceedings of* 25^{th} *International Conference Distributed Computing Systems (ICDCS 05)*, pages 609–619, 2005.
20. In Jae Myung. Tutorial on Maximum Likelihood Estimation, *Journal of Mathematical Psychology*, 47(1):90–100, 2003.
21. R Peng, M L Sichitiu. Angle of Arrival Localization for Wireless Sensor Networks, *In Proceedings of third Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks*, 1:374–382, 2006.
22. Niculescu and B Nath. Ad Hoc Positioning System (APS) using AOA, *In Proceedings of INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*, 3:1734–1743, 2003.
23. Nasipuri and K Li, A Directionality based Location Discovery Scheme for Wireless Sensor Networks, *ACM International Workshop on Wireless Sensor Networks and Applications*, pages 105–111, 2002.
24. P Rousseeuw and K Driessen. Computing LTS Regression for Large Data Sets, *Data Mining Knowledge Discovery*, 12(1):29–45, 2006.
25. Ravi Garg, Avinash L Varna and Min Wu. An Efficient Gradient Descent Approach to Secure Localization in Resource Constrained Wireless Sensor Networks, *IEEE Transactions on Information Forensics and Security*, 7(2):717–730, April 2012.
26. Mao, B D O Anderson and B Fidan. Path Loss Exponent Estimation for Wireless Sensor Network Localization, *Computer Networks*, 51:2467–2483, 2007.
27. R Moses, D Krishnamurthy and R Patterson. A Self-Localization Method for Wireless Sensor Networks, *Eurasip Journal on Applied Signal Processing, special issue on sensor networks*, pages 348–358, 2003.
28. Sarigiannidis. Localization for Ad Hoc Wireless Sensor Networks, *MS Thesis, Technical Uni-*

versity Delft, The Netherlands, August 2006.
29. J Xiao, L Ren and J Tan. Research of TDOA Based Self-Localization Approach in Wireless Sensor Network, *In Proceedings IEEE/RSJ International Conference on Intelligent Robots and Systems*, pages 2035–2040, 2006.
30. Jeril Kuriakose. Invalidating Vulnerable Broadcaster Nodes using Maximum Likelihood Expectation, *International Journal of Research in Engineering and Technology,* 3(7):129–136, 2014.
31. George Aggelou. Mobile Ad Hoc Networks from Wireless LANs to 4G Network, *Tata McGraw Hill Education, India,* 2009.
32. Richards John A. Remote Sensing Digital Image Analysis: An Introduction, *Springer*, 2013.
33. Jeril Kuriakose, Sandeep Joshi, Vikram Raju R and Aravind Kilaru. A Review on Localization in Wireless Sensor Networks, *Advances in Signal Processing and Intelligent Recognition System, Springer International Publishing*, pages 599-610, 2014.
34. T S Rappaport. Mobile Radio Propagation: Large-Scale Path Loss, Wireless Communications: Principles and Practice, *Second Edition, Pearson Education, Inc.,* 2003.
35. P C Mahalanobis. On the Generalised Distance in Statistics, *In Proceedings of the National Institute of Science of India*, pages 49–55.

Jeril Kuriakose received the B Tech degree from Jeppiaar Engineering College, India, in 2010, and M Tech degree from University of Mysore, India, in 2012, all in Information Technology. He is currently pursuing Ph.D in Manipal University Jaipur, India. His research interests include Mobile Computing, Mobile Ad Hoc Network, Network and Information Security and Scientific Computing.

Amruth V received B Tech Degree from Coorg Institute of Technology, India and MTech Degree from University of Mysore, India, in 2009 and 2012, respectively, all in Information Technology. At present he is working as assistant professor in Bearys Institute of Technology, Mangalore, India, in the Department of Information Science and Engineering. His research areas include Remote Sensing, Algorithms, Network and Information Security and Wireless Networking.

Swathy Nandhini N completed UG degree in KSR College of Engineering and PG degree in Varuvan Vadivelan Institute of Technology, Anna University, in India, in 2010 and 2012, respectively. Her area of interest includes Cryptography and Network Security, Computer Networks, Operating Systems and Web Technology.

Abhilash V is an Electrical an Engineer. He completed his bachelors from PES College of Engineering, Mandya. His research areas are Power Systems and Control Systems.