IMPROVED REPUTATION SYSTEMFOR WIRELESS SENSOR NETWORKS (WSNS)

[1]R.Karthikeyan, [2]C.Jothi Kumar

[1] Research Scholar, Department of Computer Science Engineering, SRM University, Chennai, Tamilnadu, India [2]
Assistant Professor, Department of Computer Science Engineering, SRM University, Chennai, Tamilnadu, India [1]
karthikjan7@gmail.com , [2] kumar.c@ktr.srmuniv.ac.in

Abstract: Reliable sensing is the important factor in the Wireless Sensors Networks (WSNs) that consist of a large number of spatially distributed autonomous sensors, which can be employed in applications ranging from environmental monitoring and battlefield surveillance to condition based maintenance. Among the tasks of these applications, target localization and classification are most frequently involved. Localization is primarily achieved by two approaches, i.e. by estimate of time delay of arrival (TDOA) or estimate of energy attenuation. Our main objective of this work is to reduce the localized sensing errors using RANSAC (Random Sampling Consensus) method and to discover the minimum dominating subset and aggregate the reliable sensing values at sink side based on greedy heuristic approach.

Keywords: Target localization, random sampling consensus (RANSAC), reputation system, sensing reliability, trust evaluation, wireless sensor networks (WSNs).

1. INTRODUCTION:

Wireless sensors networks (WSNs) are wireless networks that consist of a large number of spatially distributed autonomous sensors (generally referred to as sensor nodes) and collectively monitor environmental conditions, such as temperature, sound, vibration, and so forth. [1] WSN can be employed in applications ranging from environmental monitoring and battlefield surveillance to condition based maintenance. Among the tasks of these applications, target localization and classification are most frequently involved. [2], [3] Both tasks can be viewed as sensor fusion problems. More specifically, the target localization and classification problem is to make the best estimates with regard to the location and type of the observed targets by rationally combining information collected by relevant sensor nodes.[4] A thorough overview of these problems can be found. In the publication, a general purpose collaborative framework is proposed for localization and classification in WSN. Localization problems are overviewed. It shows localization is primarily achieved by two approaches, i.e. by estimate of time delay of arrival (TDOA) or estimate of energy attenuation. Each algorithm has its own advantages and disadvantages. Energy based localization using acoustic signatures in WSN is presented. Classification in WSN is reported. Maximum likelihood and support vector machine are used for classification. Real world experiments to classify armed vehicles with acoustic and seismic signatures are demonstrated. In WSN scenarios, the energy based localization method is preferred. The primary reason is that TDOA requires related sensors to be accurately synchronized. But accurate synchronization at present is too expensive. Localization with acoustic signatures is most desirable, because the models of acoustic energy attenuation are relatively easy to establish and less influenced by environmental changes. [5] Support vector machine is very suitable for classification in WSN because it is especially designed for small sample learning. Moreover its sparse representation of the learned classifier requires less in-network data exchange. [6].

Security breach can happen in a sensor network not only while relaying information to the end-user but also while generating information.[7] The ability of a sensor network to perform its task depends not only on its ability to communicate among the nodes, but also on its ability to sense the physical environment and collectively process the sensed data.[8] This decentralized in network decision-making, which relies on the inherent trust among the nodes, can be abused by adversaries to carry out security breaches through compromised nodes. Note that sensor nodes are envisioned to be low-cost which make it infeasible for manufactures to make them tamper-resistant; an adversary can undetectably take the control of a sensor node by physically compromising it. [9] An adversary can then potentially insert faulty data or decisions to mislead the whole network! Cryptographic and authentication mechanisms alone cannot be used to solve this problem as internal adversarial nodes will have access to valid cryptographic keys. [7] [8].Besides malicious attacks, sensornodesarealso vulnerable to system faults. Non-malicious behavior such as malfunctioning of radio/sensors can also result in the generation of bogus data, bringing equally detrimental effects to the functioning of the network. The very nature of this type of misbehavior is outside the realm of cryptography. [10][11].

2. PRELIMINARY:

Decentralized methods are considerably prevalent in most WSNs scenarios because of high robustness. However, in some cases where frequent data exchange between nodes is necessary, decentralized methods may cost more resources than centralized methods since more packet transmission may be required to make every node aware of the information in the neighborhood.[12] The performance of the MLE is generally affected by the data quality of participated sensors. The extreme readings produced by faulty sensors can possibly cause great estimation errors. There is no advantage for an entity to misbehave because any resource utilization will be forbidden and no prediction mechanism to avoid the level 2 based malicious nodes. [13] The work focuses to improve the proposed system that aggregates the correct dataset at sink node side and discover the minimum dominating senor set using greedy heuristic approach. A model is constructed by sink node. The model is predicting the sensing error of actual sensors and finds the minimum dominating sets from the actual sensors.

2.1 System Analysis:

The purpose of the System analysis is to produce the brief analysis task and also to establish complete information about the concept, behavior and the other constraints like performance measure and the system optimization. [14] The main goal of System Analysis is to completely specify the technical details for the main concept in a concise and unambiguous manner.

2.2 Existing System:

Sensor faults have been studied extensively in process control. Tolerating and modeling sensor failures was studied. [15] However, studying faults in wireless sensing systems differs from faults in process control in a few ways that make the problem more difficult. The first issue is that sensor networks may involve many more sensors over larger areas. [16] Also, for a sensor network the phenomenon being observed is often not well defined and modeled resulting in higher uncertainty when modeling sensor behavior and sensor faults. [17] Finally, in process control, the inputs to the system are controlled or measured, whereas in sensing natural phenomena this is not the case. [18].

As sensor networks mature, the focus on data quality has also increased. The many deployment experiences show that this is a major issue that needs to be addressed. [19] With the goal of creating a simple to use sensor network application, observe the difficulty of obtaining accurate sensor data. Following a test deployment, they note that failures can occur in unexpected ways and that calibration is a difficult task. [23] Using this system deployed a sensor network with the goal of examining the microclimate over the volume of a redwood tree. The authors discovered that there were many data anomalies that needed to be discarded post deployment. [20] Only 49% of the collected data could be used for meaningful interpretation. [21][22].

2.3 The RANSAC System:

The proposed RANSAC contains two steps at every sensor site, namely, hypothesis and verification. In the hypothesis step, subsets are uniformly drawn and at random from the input data set. For each subset, a model hypothesis is constructed by computing the model parameters using the subset data. In the verification step, the quality of the hypothetical models is evaluated on the full data set. Typically, the cost function for the model quality is defined to count the number of inliers. The hypothesis getting the most support from the whole data set gives the best quality.

There are four important parameters in RANSAC:

- the subset size;
- the maximum number of drawn subsets;
- a threshold that determines inliers; and
- a criterion deciding whether a model is fitted or not.

The cluster head works based on the greedy approach for finding minimum dominating set. The similarity of received datasets is computed. The error value is out of the degree means don’t send to sink node. Also eliminates the minimum dominating set send sensor from the cluster. Then valid subsets are sending to sink node and then updated into data model.

2.4 System Requirement Specification:

The purpose of the Software Requirement Specification is to produce the specification of the analysis task and also to establish complete information about the requirement, behavior and also the other constraint like functional performance and so on. [24] The main aim of the Software Requirement Specification is to completely specify the technical requirements for the software product in a concise and in unambiguous manner.[25] The hardware requirements are Processor: Pentium IV, Clock speed: 550MHz, Hard Disk: 20GB RAM: 128MB, Cache Memory: 512KB, Operating System: Windows XP/ Windows7. The software requirements include Front End: JAVA 1.6 and back end: My SQL.

2.5 Functional Requirements:

This system is done for sensing reliable data sensing using RANSAC and greedy approach. Input: The input of this project is location based sensor reading in dataset format. Behavior: The behavior this project is sensing the reliable data using Reputation based system with RANSAC method also eliminate the minimum dominating sensor set using greedy approach. Output: The output of this project is reliable sensing data from sensor. [26].

2.6 Non Functional Requirements Performance:

The performance of error correcting rate is very high. Reliability: The reliability of sensing data is very high. Implementation: NS2:

- Sensor Network Creation
- Sensor clustering
- Sensor Reading
- RANSAC based error correction
- Greedy based Data updating.

2.7 System Design Specification:

Design is a meaningful engineering of something that is to be built. Software Design sites at the technical kernel of software engineering. Software design is a process through which the requirements are translated in to a representation of the software i.e. the blue print for constructing software. Design provides us with representation of software that can be assesses for quality. Design is the only way that we can accurately translating a customer’s requirements in to a finished software product. [27] Some of the fundamental concepts of software design include Abstraction, Refinement, Modularity, Software Architecture, Control Hierarchy, Structured Portioning, Data Structure, Software Procedure and also the Information Hiding.

3. EXPERIMENTAL IMPLEMENTATION:

Ns or the network simulator (also popularly called ns-2, in reference to a popular version) is a discrete event network simulator. Ns are used in the simulation of routing protocols, among others, and are heavily used in ad-hoc networking research. Ns will supports popular network protocols, offering simulation results for wired and wireless networks alike. It is popular in research given its open source model and online documentation. However, modeling is a very complex and time-consuming task in ns-2, since it has no GUI and one needs to learn scripting language, queuing theory and modeling techniques. Of late, there have been complaints that results are not consistent (probably because of continuous changes in the code base) and that certain protocols are replete with bugs. Ns were built in C++ and provide a simulation interface through OTcl, an object-oriented dialect of Tcl. The user describes a network topology by writing OTcl scripts, and then the main ns program simulates that topology with specified parameters. Ns-2 can run either in Fedora version of Linux Operating Systems or in the surface used Windows XP with Cygwin. Ns are licensed for use under version 2 of the GNU General Public License.

4. CONCLUSION:

This project is implemented a trust evaluation-based method for energy-based acoustic target localization application in sensor networks. The proposed method is the RANSAC algorithm, which depends on sampling multiple subsets of sensor readings and exerting the MLE to examine the data quality of each drawn subset. The effectiveness of the algorithm is determined by the number of drawn subsets, which is computed by the contamination rate of the whole data. Also, a greedy based approach is effectively utilized to eliminate the minimum dominating set and update reliable dataset in sink node.

5. FUTURE WORK:

The implementation of the above work can be extended in arenas like Area monitoring, Health care monitoring, Environmental/Earth monitoring, Air quality monitoring, Air pollution monitoring, Forest fire detection, Data logging, Industrial sense and control applications, Water/Waste water monitoring, Machine health monitoring, Industrial monitoring, Natural disaster prevention, Water quality monitoring, Landslide detection, Water distribution network management, Preventing natural disaster, Irrigation management, Passive localization and tracking, Smart home monitoring.

REFERENCES

[1] P. Resnick and R. Zeckhauser, "Trust among strangers in Internet transactions: Empirical analysis of eBay's reputation system," in The Economics of the Internet and E-Commerce, vol. 11. Amsterdam, The Netherlands: Elsevier, 2002, pp. 127–157.

[2] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, "Reputation-based framework for high integrity sensor networks," ACM Trans. Sensor Netw., vol. 4, no. 3, pp. 1–37, May 2008.

[3] X. Wang, L. Ding, and D. Bi, "Reputation- enabled self-modification for target sensing in wireless sensor networks," IEEE Trans. Instrum. Meas., vol. 59, no. 1, pp. 171–179, Jan. 2010.

[4] R. A. Shaikh, H. Jameel, S. Lee, S. Rajput, and Y. J. Song, "Trust management problem in distributed wireless sensor networks," in Proc. IEEE Int. Conf. Embedded Real-Time Comput. Syst. Appl., 2006, pp. 411–414.

[5] P. Michiardi and R. Molva, "Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in Proc. IFIP Commun. Multimedia Security Conf., 2002, pp. 107–121.

[6] L. Xiong and L. Liu, "Peer Trust: Supporting reputation based trust to P2P E-communities," IEEE Trans. Knowl. Data Eng., vol. 16, no. 7, pp. 843–857, Jul. 2004.

[7] G. Gupta and M. Younis, "Fault-tolerant clustering of wireless sensor networks," in Proc. IEEE Wireless Commun. Netw., Mar. 2003, pp. 1579–1584.

[8] M. D. Krasniewski, P. Varadharajan, B. Rabeler, S. Bagchi, and Y. C. Hu, "TIBFIT: Trust index based fault tolerance for ability data faults in sensor," in Proc. Int Conf. Dependable Syst. Netw., 2005, pp. 672–681.

[9] S. Tanachaiwiwat, P. Dave, R. Bhindwale, and A. Helmy, "Secure locations: Routing on trust and isolating compromised sensors in location aware sensor networks," in Proc. SenSys, 2003, pp. 324– 325.

[10] T. Roosta, M. Meingast, and S. Sastry, "Distributed reputation system for tracking applications in sensor networks," in Proc. Int. Workshop Advances Sensor Netw., 2006, pp. 1–8.

[11] J. Hur, Y. Lee, S. M. Hong, and H. Yoon, "Trust management for resilient wireless sensor networks," in Proc. ICISC, 2005, pp. 56–68.

[12] M. Zuliani, C. S. Kenney, and B. S. Manjunath, "The multi RANSAC algorithm and its application to detect planar homo graphies," in Proc. ICIP, 2005, pp. 153–156.

[13] O. Chum and J. Matas, "Randomized RANSAC with t(d,d) test," in Proc. Brit. Mach. Vis. Conf., Cardiff, U.K., 2002, pp. 448–457.

[14] C. Meesookho, U. Mitra, and S. Narayanan, "On energy based acoustic source localization for sensor networks," IEEE Trans. Signal Process. vol. 56, no. 1, pp. 365–377, Jan. 2008.

[15] X. Wang, D. W. Bi, L. Ding, and S. Wang, "Agent collaborative target localization and classification in wireless sensor networks," Sensors, vol. 7, no. 8, pp. 1359–1386, Aug. 2007.

[16] J. C. Chen, L. Yip, J. Elson, H. Wang, D. Maniezzo, R. E. Hudson, K. Yao, and D. Estrin, "Coherent acoustic array processing and localization on wireless sensor networks," Proc. IEEE, vol. 91, no. 8, pp. 1154– 1162, Aug. 2003.

[17] X. Sheng and Y. Hu, "Maximum likelihood multiple source localization using acoustic energy measurements with wireless sensor networks," IEEE Trans. Signal Process., vol. 53, no. 1, pp. 44–53, Jan. 2005.

[18] D. Blatt and A. O. Hero, "Energy-based sensor network source localization via projection onto convex sets," IEEE Trans. Signal Process., vol. 54, no. 9, pp. 3614–3619, Sep. 2006.

[19] L. E. Parker, B. Birch, and C. Reardon, "Indoor target intercept using an acoustic sensor network and dual wave front path planning," in Proc. IEEE/RSJ Int. Conf. Intell. Robots Syst., 2003, pp. 278–283.

[20] C. Wang and L. Xiao, "Sensor localization in concave environments," ACM Trans. Sensor Netw., vol. 4, no. 1, pp. 1–31, Jan. 2008.

[21] K. Ni, N. Ramanathan, M. Chehade, L. Balzano, S. Nair, S. Zahedi, E. Kohler, G. Pottie, M. Hansen, and M. Srivastava, "Sensor network data fault types," ACM Trans. Sensor Netw., vol. 5, no. 3, pp. 1–29, Aug. 2009.

[22] Y. Xiao, V. K. Rayi, B. Sun, X. Du, F. Hu, and M. Galloway, "A survey of key management schemes in wireless sensor networks," Comput. Commun., vol. 30, no. 11/12, pp. 2314–2341, Sep. 2007.

[23] J. Deng, R. Han, and S. Mishra, "Enhancing base station security in wireless sensor networks," Dept. Comput. Sci., Univ. Colorado, Denver, CO, Tech. Rep. CU-CS-951-03, Apr. 2003.

[24] M. G. Rabbat and R. D. Nowak, "Distributed optimization in sensor networks," in Proc. 3rd Int. Symp. Inf. Process. Sensor Netw., Berkeley, CA, 2004, pp. 20–27.

[25] N. Katenka, E. Levina, and G. Michailidis, “Local vote decision fusion for target detection in wireless sensor networks,” in Proc. Joint Res. Conf. Statist. Quality Ind. Technol., Knoxville, TN, Jun. 7– 9, 2006.

[26] B. Krishnamachari and S. S. Iyengar, “Distributed Bayesian algorithms for fault-tolerant event region detection in wireless sensor networks,” IEEE Trans. Comput., vol. 53, no. 3, pp. 241–250, Mar. 2004.