This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the WCNC 2009 proceedings.

A Distributed Algorithm for Localization Error Detection-Correction, Use in In-network Faulty Reading Detection: Applicability in Long-Thin Wireless Sensor Networks

Debraj De

Department of Computer Science and Engineering
The Ohio State University
Columbus, OH 43210
Email:ded@cse.ohio-state.edu

***Abstract*—In near future, wireless sensors networks (WSN) are expected to be deployed for a vast variety of applications. For many of these applications, sensed data individually have no meaning without proper knowledge of position where the data was sensed. Although there have been proposed algorithms for localization, many of them fall short with respect to complexity, cost, security and accuracy. Some issues that still hinder the efficiency of available localization techniques are multi-path propagation, security attack (internal and external attack by faulty or malicious nodes), and sometimes specific network topologies. For example, the Long-Thin (LT) topology of WSN is highly prone to localization error due to its special distribution pattern. In many real world WSN applications, the localization is also needed to be Global Positioning Systems (GPS) free. Apart from efficient localization, another important operation in WSN application is the need to have in-network detection of faulty sensor readings, without compromising detection of important events. Looking at these critically important operations of WSN, our first contribution is proposing a self-organized distributed GPS free localization error detection and correction algorithm. Our next contribution is utilizing reliability gained in the proposed localization to construct an improved algorithm for in-network detection of faulty readings. We have also proposed a fault tolerant structure for Long-Thin (LT) WSN topology, that can well utilize both of the proposed algorithms.**

***Index Terms*—Localization, security, sensor networks, long-thin network, faulty sensor reading**

I. INTRODUCTION

Wireless sensor networks are composed of hundreds, possibly thousands of tiny low-cost devices called sensor nodes, capable of measuring various physical events, performing computations and most importantly, communicating with each other and organizing themselves in order to co-operatively achieve a desired task [1].

A fundamental challenge in wireless sensor network applications is localization, determining the location of sensor nodes. Localization information is used to detect and record events, or to route packets using geometric-aware routing, e.g. [2]. Manual configuration of location is not feasible for large-scale networks or networks where sensors may move. Providing each sensor with localization hardware (e.g. GPS [3]) is expensive in terms of cost and energy consumption, and sometimes even not feasible. A more reasonable solution to the localization problem is to allow some nodes (called seeds) to have their location information at all times, and allow other nodes to infer their locations by exchanging information with seeds. Localization algorithms can be divided into two categories: range-based and range-free. There have been plenty of research works done on forming correct localization algorithms for different application scenarios [4], [5], [6], [7], [8], [9], [10], [11], [12].

Due to their crucial role in WSNs, localization systems can be target of an attack that could compromise the entire operation of a WSN and can lead to incorrect plans and decision making. Security attack in localization can be of two fold: internal and external attack. In internal attack, a faulty node can measure and transmit wrong information. In external attack, a malicious node deceives to behave as some other node.

Another important operation in WSN is detecting sensors with faulty reading. Sensors are prone to failure in harsh and unreliable environments. Faulty sensors are likely to report arbitrary readings which do not reflect the true state of environmental phenomenon or events under monitoring. Meanwhile, sensors may sometimes report noisy readings resulted from interference [13]. Both arbitrary and noisy readings are viewed as faulty readings in this paper. The presence of faulty readings may cause inaccurate query results and hinder usefulness. Thus it is critical to indentify and filter out faulty readings so as to improve the query accuracy.

In this paper we have discussed about Long-Thin Network or LT network [14], a specific type of network topology, widely used in wireless sensor applications. The use of LT network, specifically in surveillance application, ranges from leakage detection of fuel pipes, monitoring in tunnel, stage measurements in sewer, street lights monitoring in highway systems, flood protection of rivers, vibration detection of bridges, roadside networks, pedestrian detection system and many more. In such a network, nodes may form several long backbones and these backbones extend the network to intended coverage areas. A backbone is a linear path which may contain tens or hundreds of routers.

In this paper we have discussed a simple way to achieve fault tolerance in Long-Thin network deployment. Two main algorithms are proposed in this paper: a self-organized distributed algorithm for GPS-free localization error detection and correction, and an algorithm for detection of in-network faulty reading in sensors.

Our new localization error detection and correction algorithm is distributed, self-organized and scalable. This algorithm is an anchor free scheme. It is also of very low complexity, thus good for energy constrained sensors. It has a very high degree of flexibility and scalability because no knowledge about the current network information is needed and new nodes can be added without a need to change the algorithm for existing nodes. Localization is then possible even in environments that are out of reach of GPS signal. Our algorithm is suitable not only for Long-Thin topology, but also for any possible topologies. It is also promising for secured and accurate localization

978-1-4244-2948-6/09/$25.00 ©2009 IEEE

for Ad-Hoc sensor networks. The proposed algorithm makes use of techniques based on the Received Signal Strength Indicator (RSSI) and the Angle of Arrival (AOA) [15], [16], [17], [18] and [19] to estimate the range (distance) and angle among sensors. But one thing worth mentioning is that, to some extent the proposed localization error correction algorithm at least partially relies on RSSI as an impression of distance. As RSSI is dependent on environment, it may not always be a good estimator of distance. For example, in environment full of obstacles, or in scenario of mobile nodes, RSSI can give some wrong estimation of distance. But certainly there are many topologies and application environments, where RSSI can be an inexpensive (technology and computation perspective) parameter that gives correct impression of distance.

Next, we have proposed an algorithm for in-network detection of sensors with faulty readings. This utilizes reliability information extracted from the localization algorithm, and employs distance and reliability information in a weighted voting method. This algorithm is of very low complexity with simple calculations, as opposed to highly complex and thus energy hungry correlation algorithms.

The rest of this paper is organized as follows. Section II presents the proposed fault tolerant deployment design for Long-Thin networks. Localization error detection techniques are proposed in section III. Section IV and V describes the localization error correction algorithm. Proposed faulty reading detection algorithm is presented in section VI. The experimental results and observations are in section VII. Finally we conclude in section VIII.

II. Fault Tolerant Deployment Technique for Long-Thin Wireless Sensor Networks

Due to the special kind of distribution pattern of sensor nodes in Long-Thin network, each sensor node has much lesser number of neighbors than in other topologies (for example tree). This makes it more critical for achieving fault tolerance. Failure of one or a number of closely situated nodes may cause seclusion of a part of network nodes from the cluster head node or base station. This may eventually bring down part of, or the entire network.

Here we propose a simple yet useful deployment technique for wireless sensor nodes in Long-Thin distribution. This distribution pattern is later utilized for localization error detection-correction and in-network faulty reading detection. The interesting issue with Long-Thin topology is that one sensor node cannot have too many neighbors. This is because of different issues like long thin distribution pattern, application constraint (e.g. space constraint in pipeline or tunnel) etc. On the other hand, number of neighbors cannot be too low in order to make the network fault tolerant. Looking at these contradicting requirements, we propose an optimized structure for deployment of sensor nodes in Long-Thin network. This is useful for a wide range of practical applications.

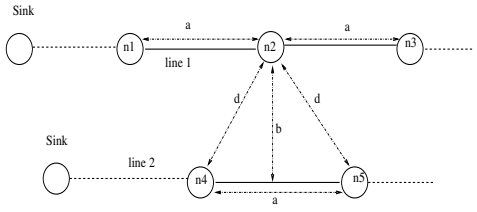

Fig. 1. Proposed fault tolerant substructure for Long-Thin network

The proposed distribution is described in Fig. 1, which shows the optimal substructure pattern that is repeated along the entire network. In the substructure, there are two parallel linear distributions or lines. There can be multiple such lines, depending on space constraint and other issues. In the Fig. 1, node *n2* on a linear distribution, is at a distance a away from its closest neighbors on the same line, and distance d away from the closest neighbors on the other line, where

$$d^2 = (\frac{a}{2})^2 + b^2 \quad (1)$$

The parameter *b* denotes separation between the two lines. Suppose the maximum range of each wireless node is *R*. Then the bounds for the parameters *a* and *b* are: (i) $a \leq R$ and (ii) $d \leq R$.

So each node in this distribution has at least four neighbors. Number of neighbors can be further increased without increasing number of lines, by reducing parameters *a* and *b*. This brings the flexibility of deployment design. One more attractive feature of this scheme is that increasing *a* and *b* also can have excellent usefulness. Even after deployment, we can select set of nodes to be awake that use larger effective values of *a* and *b*. This enables the application to switch between the sets of available active networks from time to time. This gives big benefit in elevating entire network lifetime (but obviously in lieu of deployment cost of more sensor nodes).

III. Proposed Localization Error Detection Techniques

A. Basic Concept Behind Localization Error Detection

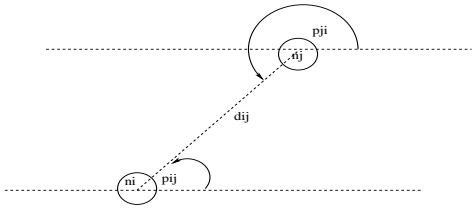

Fig. 2. Basic concept behind localization error detection

The basic idea behind the proposed localization error detection technique is simple but intuitive. It is assumed that all the sensor nodes are aligned in X-Y plane, which is quite true for most of the applications. Now as in Fig. 2, node n_i and n_j observes each other at angles p_{ij} and p_{ji} respectively. Also suppose that they are at distance d_{ij}. Then co-ordinate of node n_j with respect to n_i is $x_{ij} = d_{ij}.\cos p_{ij}$ and $y_{ij} = d_{ij}.\sin p_{ij}$. Similarly co-ordinate of node n_i with respect to n_j is $x_{ji} = d_{ji}.\cos p_{ji}$ and $y_{ji} = d_{ji}.\sin p_{ji}$.

A sensor node calculates the distance from received RSSI value, while angle of arrival is calculated mostly with a planar antenna array. Now if there is no error in measurement of distance and angle, then clearly $(x_{ji} + x_{ij}) = 0$ and $(y_{ji} + y_{ij}) = 0$.

Therefore each sensor node can detect any error in localization by checking the sum $(x_{ji} + x_{ij})$ and $(y_{ji} + y_{ij})$ each to be zero.

B. Proposed Technique for Localization Under Multi-path Propagation

The basic concept just stated, can be utilized to detect correct localization information from multiple signals received due to multi-path propagation problem. Multi-path propagation is mainly caused by reflection of radio signals from objects.

Such a scenario is shown in Fig. 3. Due to multi-path propagation problem, node n_i can see node n_j at two positions: (x_{ij}, y_{ij}) and at (x'_{ij}, y'_{ij}), but with different RSSI values: $RSSI_{ij}$ and $RSSI'_{ij}$. Similarly n_j can see node n_i at two positions: (x_{ji}, y_{ji}) and at (x'_{ji}, y'_{ji}).

Now each node, say n_i intelligently determines relative position of n_j, which gives the minimum of $(RSSI_{ij}.((x_{ij}+x_{ji})+(y_{ij}+y_{ji})))$,

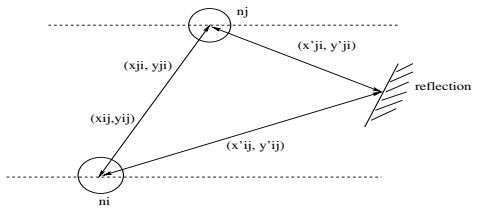

Fig. 3. Multi-path propagation causing error in localization

$(RSSI_{ij}.((x_{ij} + x'_{ji}) + (y_{ij} + y'_{ji})))$, $(RSSI'_{ij}.((x'_{ij} + x_{ji}) + (y'_{ij} + y_{ji})))$ and $(RSSI'_{ij}.((x'_{ij} + x'_{ji}) + (y'_{ij} + y'_{ji})))$, and which is within a predefined error threshold.

Validity of this technique is proved by the basic concept just mentioned, and by the fact that after reflection, the RSSI of radio signal goes down considerably.

C. Proposed Technique to Detect Internal and External Security Attack on Localization

Our proposed concept is capable of handling both kinds of security attack on localization operation - internal and external. As mentioned before, in internal attack, a bad node sends out wrong data because of faulty component. In external attack, a malicious sensor node tries to feign another node.

Suppose node n_j is a malicious node that can cause localization error in node n_i. Then applying the basic concept of detecting localization error, the node n_i can detect whether node n_j is malicious or not. For both internal and external attack, malicious node n_j can corrupt values of x_{ji} and y_{ji}, but has no control over x_{ij} and y_{ij}. So values of $(x_{ji} + x_{ij})$ and $(y_{ji} + y_{ij})$ exceeding a threshold will indicate detection of malicious node, and will save localization from erroneous interpretation.

This section dealt mainly with error detection. In the next two sections, we have proposed an algorithm for error correction.

IV. Motivation behind proposed localization algorithm design

The main motivation behind the design of proposed distributed localization algorithm comes from basic idea of Weighted Centroid Localization (WCL) [20].

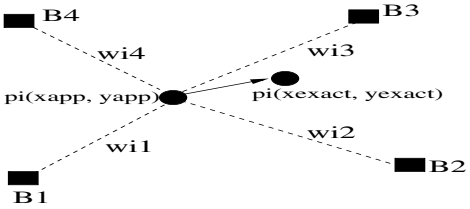

Fig. 4. Weighted Centroid Localization

The WCL technique is shown in Fig. 4, where say, four beacon nodes (having known position) B1, B2, B3 and B4 helps to calculate approximate position of a node Pi (having unknown position) with the help of weights wij. The node Pi, after gathering known positions of beacon nodes, calculates its approximate position Pi(xapp, yapp) by weighted centroid determination technique. Suppose n is the number of beacon nodes in range and $wij(d)$ is the weight between sensor node i and beacon node j.

$$p(x_i app, y_i app) = \left(\frac{\sum_{j=1}^{n}(w_{ij}(d)x_{Bj})}{\sum_{j=1}^{n}(w_{ij}(d))}, \frac{\sum_{j=1}^{n}(w_{ij}(d)y_{Bj})}{\sum_{j=1}^{n}(w_{ij}(d))} \right) \quad (2)$$

If the actual position of Pi is (xexact, yexact), then the error of this localization is

$$f_i(x, y) = \sqrt{(x_{exact} - x_{app})^2 + (y_{exact} - y_{app})^2} \quad (3)$$

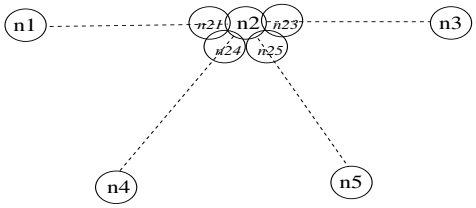

Fig. 5. Localization technique

We utilize this technique effectively to form a stochastic algorithm for localization. As shown in Fig. 5, we use the basic concept of relative position described before in section III. Suppose node $n2$'s virtual position with relative to node $n1$ is $n21$ with position $(x12 + x21, y12 + y21)$ from $n2$. Similarly there are virtual relative positions $n23$, $n24$ and $n25$. The weight functions $w21$, $w23$, $w24$, $w25$ are the RSSI value of received message at $n2$ during position information exchange.

Now the trick is that node $n2$ assumes virtual nodes $n21$, $n23$, $n24$ and $n25$ as virtual beacon nodes. Then using WCL technique, $n2$ calculates approximate new virtual position of itself. After knowing this, the node corrects the perceived positions of neighbors with respect to this new virtual position of it's own.

V. Algorithm for Localization Error Detection and Correction

A. Localization Error and Long-Thin Network

The nature of localization is static for most of Long Thin sensor network deployments (for example road, tunnel, gas pipeline, bridge, skyscraper etc.). The localization is prone to various kinds of errors, which cost the application a lot with wrong localization information. The major causes of error in localization are multipath propagation, faulty reading of sensor node, wireless channel error, security attacks (both internal and external). There are already existing localization techniques for handling error and security challenges. Still there are overhead and feasibility issues. It will be more useful to have a low-complexity, absolutely distributed, self-organizing secured localization with error correction.

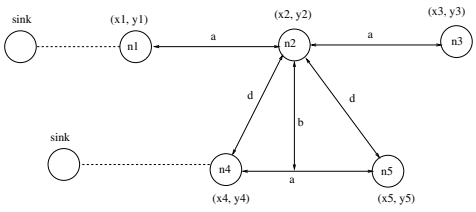

Fig. 6. Localization error correction on Long-Thin topology

Another big issue with localization error especially in Long-Thin network is the propagation of error. For example, in the Fig. 6, when the base station or head node will calculate the absolute position

of say node n_2, it will add calculated absolute position of n_1 with relative position of n_2 with respect to n_1. Now if n_1 is highly faulty or malicious, the error due to n_1 will propagate through all the position calculation of the subsequent nodes. That necessitates the localization algorithm to be highly accurate.

Here we propose a low complexity, distributed, secured localization error detection and correction algorithm. Our algorithm efficiently addresses the issues of cascaded or propagated localization error, multi-path propagation problem, as well as security threats (internal and external attack). This algorithm is suitable not only for Long-Thin networks, but also for any other topologies.

B. Proposed Algorithm

Considering the optimal substructure as shown in Fig. 6, the localization algorithm is described with respect to node n_2. Each node in the network runs the same algorithm as of node n_2. The proposed algorithm is as follows:

1) Node n_2 broadcasts a hello message or a dummy message M1, which is received by all of its neighbors (n_1, n_3, n_4 and n_5 here for n_2).
2) So n_2 in turn, receives message M1 from each of its neighbors.
3) From these messages, n_2 calculates relative position (with respect to itself) of each of its neighbors, utilizing Angle of Arrival (AOA) and Distance information. Now suppose n_2 calculates its neighbor n_j's relative position as (x_{2j}, y_{2j}) from Angle of arrival A_{2j} and distance D_{2j} information. Then:

$$x_{2j} = D_{2j}.\cos A_{2j} \tag{4}$$

$$y_{2j} = D_{2j}.\sin A_{2j} \tag{5}$$

4) Now n_2 sends feedback message M2 with calculated position information (x_{2j}, y_{2j}) to each specific neighbor n_j. Its like every node is playing a game with each of its neighbor by exchanging their positions, at which, one can observe the other.
5) Node n_2 in turn, receives feedback M2 with information (x_{j2}, y_{j2}) from each of its neighbor n_j.
6) Now ideally the value of $(x_{j2}+x_{2j})$ and $(y_{j2}+y_{2j})$ should be zero. But due to different kinds of errors, it will not always be zero. Interestingly these values capture all the possible errors that may affect accuracy of localization.
7) Detecting faulty or malicious node: if n_2 gets only one message M2 from n_j, then it saves the relative position information (x_{2j}, y_{2j}). Now n_2 calculates $(x_{j2} + x_{2j})$ and $(y_{j2} + y_{2j})$. If $(x_{j2} + x_{2j}) \leq x_{error-threshold}$ and $(y_{j2} + y_{2j}) \leq y_{error-threshold}$, then n_2 can rely node n_j, and set a confidence level of node n_j, $confidence_{2j} = trust\_val$; Otherwise n_2 can't absolutely rely on accuracy of n_j, so sets confidence level $confidence_{2j} = nontrust\_val$; Typically $trust_{val}$ and $nontrust_{val}$ can be selected as 3 and 1 respectively. In this way every node decides whether to rely its neighbor information or not. Also it sets the confidence level for the neighbors, which is utilized in in-network detection of faulty readings described later in this paper.
8) For multi-path problem, we have already proposed technique to detect accurate localization information in previous section.
9) Final position error correction: suppose the message M2 from n_j to n_2 (containing information (x_{j2}, y_{j2})) has RSSI value of $RSSI_{2j}$, then n_2 calculates the average error:

$$Ex_2 = \frac{\sum_j (RSSI_{2j} * (x_{2j} + x_{j2}))}{\sum_j (RSSI_{2j})} \tag{6}$$

$$Ey_2 = \frac{\sum_j (RSSI_{2j} * (y_{2j} + y_{j2}))}{\sum_j (RSSI_{2j})} \tag{7}$$

It is important to note that in the above two equations j belongs to nodes n_j having $(x_{j2} + x_{2j})$ within $x_{error-threshold}$ and $(y_{j2} + y_{2j})$ within $y_{error-threshold}$.
Then n_2 updates its position information about all neighbors as follows:

$$x_{2j} = x_{2j} - Ex_2 \tag{8}$$

$$y_{2j} = y_{2j} - Ey_2 \tag{9}$$

So in this fashion, all the nodes help each other to correct their perceived relative positions in a completely distributed manner. This algorithm is absolutely distributed with mostly simple algebraic computations. This less complex computation is promising for saving energy for the sensor nodes. Our algorithm efficiently eliminates the error due to multi-path propagation by averaging (based on RSSI) on the available observations. It also makes the localization more secured from internal or external attack, by testing values of $(x_{2j} + x_{j2})$ and $(y_{2j} + y_{j2})$, and setting confidence level accordingly.

VI. Proposed Algorithm for In-network Detection of Faulty Reading

Our proposed algorithm follows the weighted voting method for detection of faulty sensor reading. But the weight here is not only a function of distance, but also a function of confidence or reliability achieved during localization error detection-correction technique. The algorithm is as follows:

For a node n_i, suppose the sensor reading is s_i. Similarly s_j is the reading for each neighbor n_j of n_i. Now suppose the w_{ij} is the weight for voting from each neighbor n_j of n_i. Then we define w_{ij} as:

$$w_{ij} = confidence_{ij}/d_{ij} \tag{10}$$

Where $confidence_{ij}$ is confidence level of n_j from n_i, and d_{ij} is the distance between n_i and n_j.

Finally the vote value for the reading of n_i is as follows:

$$Vote_i = \sum_j (w_{ij}.s_j) \tag{11}$$

This algorithm does not rely nodes on closeness only, but also considers the confidence or reliability level. It efficiently removes erroneous decision due to nearby but faulty sensor node. One more point to be noted is that the proposed algorithm is not computationally expensive like correlation techniques, but gives accurate enough detection (as shown by the experimental results). It is suitable not only for Long-Thin topology, but also for any other topologies.

VII. Performance Evaluation

Extensive simulation is carried out to evaluate the performance and effectiveness of our proposed two algorithms. Comparison has been done with other existing techniques.

A. Simulation Results for Localization Algorithm

The evaluation is performed on a simulation scenario of Long-Thin network distribution having nodes from 100 to 500. The separation parameters a and b are taken as 10 meters. In the localization process, the Angle Of Arrival and Range parameters are perturbed by introducing random error within a limit. The injected errors also suffice (but not bound to limit) to the observations from practical measurement as in [15]. The algorithm is compared with default ranged based static localization technique that uses Angle Of Arrival and Range (i.e. distance) information.

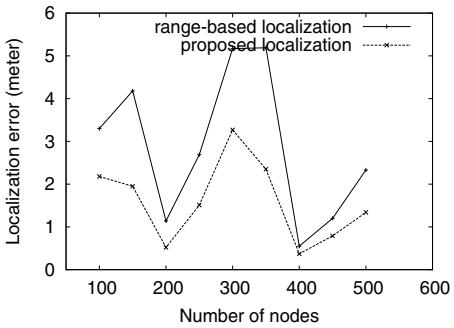

Fig. 7. Average localization error (meter)

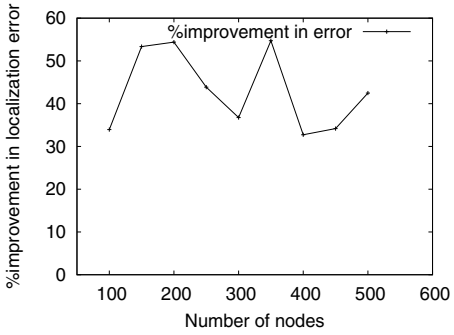

Fig. 8. %Improvement in error for proposed algorithm over range-based algorithm

From the performance plot in Fig. 7 and Fig. 8, it is observed that our proposed localization error detection and correction technique refines the localization (obtained from range-based localization technique) information efficiently and also with good scalability. The percentage improvement (reduction) in average error is quite good for any node size, from 100 to 500 and beyond. The average percentage improvement in position error is 42%, with a maximum of 54%, and a minimum of 32%.

B. Simulation Results for In-network Faulty Reading Detection

The simulation scenario is a Long-Thin network with 300 nodes. The separation parameters a and b are taken as 10 meters. The sensors are assumed to take temperature readings with range [-25, 275]. Events with unusual readings are randomly generated in the monitored field. It is assumed that the proposed localization error detection scheme has detected the faulty nodes with probability 0.7; The node failure rate is varied from as low as 0.1 to as high as 0.9; Besides failure of bad nodes, good nodes are also assumed to fail with probability 0.1; To evaluate the performance, two evaluation metrics are used: *fault detection rate* and *false positive rate*. The *fault detection rate* is the ratio of number of detected faulty nodes, to the total number of faulty nodes. The *false positive rate* is the ratio of the number of good nodes falsely detected as faulty, to the total number of good nodes.

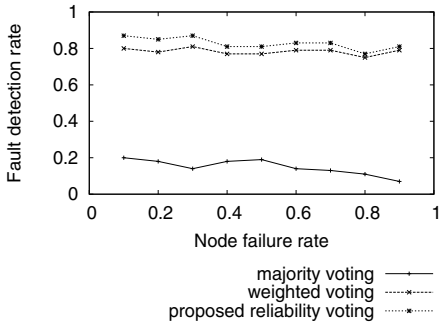

Fig. 9. Fault detection rates of the three algorithms

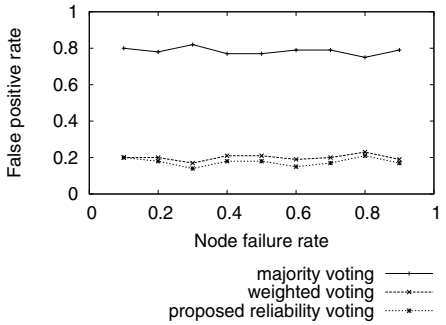

Fig. 10. False positive rates of the three algorithms

In Fig. 9 and Fig. 10 , our proposed algorithm is compared with with Majority Voting, and Weighted (distance based) Voting algorithms. The proposed algorithm is proved to perform better than the other two. Although improvement compared to Weighted Voting is not so high, but with increased number of neighbors, the performance improvement will go up even more. Even if the improvement in fault detection rate or false positive rate is low, the absolute value surely is still significant for large scale networks.

VIII. Conclusion

This work has been motivated by the need for new algorithm for: (i) localization detection and correction that can handle issuess like multi-path propagation, security attacks, faulty nodes, and (ii) low complexity in-network detection of faulty readings. We have proposed and studied the new algorithms. Our algorithms use RSSI and AOA informations of radio messages. Using RSSI as an estimator of distance is suitable for some application environments. One interesting point about these two proposed algorithms is that they can co-operate with each other. After deployment, the initial localization algorithm runs and marks the possibly faulty/malicious nodes. This information can then be utilized in the faulty reading detection algorithm. Then the detected nodes with faulty readings can be handled in the next run of localization, which in turn can again co-operate with the faulty reading detection algorithm. This mutual co-operation between localization and faulty reading detection can be even more useful in dynamic and unstable networks.

The simulation scenario and results clearly show that proposed algorithms resolve some major issues and concerns with Long-Thin wireless sensor networks. The algorithms are suitable for other topologies also. The proposed techniques are proved to be scalable and efficient, and thus quite applicable for practical use in harsh environments.

REFERENCES

[1] F. Zhao and L. Guibas, "Wireless sensor networks: An information processing approach," 2004.

[2] B. Karp and H. T. Kung, "Gpsr: Greedy perimeter stateless routing for wireless networks," in *Sixth Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom)*, 2000, pp. 243–254.

[3] B. Hofmann-WeUenhof, H. Lichtenegger, and J. Collins, "Global positioning systems, theory and practice," *Springer-Verlag*, 1993.

[4] N. B. Priyantha, H. Balakrishnan, E. Demaine, and S. Teller, "Mobile-assisted localization in wireless sensor networks," in *IEEE INFOCOM*, 2005.

[5] A. Ali, T. Collier, L. Girod, K. Yao, D. T. Blumstein, and C. E. Taylor, "An empirical study of collaborative acoustic source localization," in *IPSN*, 2007.

[6] N. Patwari and A. O. H. III, "Using proximity and quantized rss for sensor localization in wireless networks," in *WSNA*, 2003.

[7] R. Moses, D. Krishnamurthy, and R. Patterson, "Self-localization method for wireless sensor networks," *Eurasip Journal of Applied Signal Processing*, 2003.

[8] T. He, C. Huang, B. M. Blum, J. A. Stankovic, and T. Abdelzaher, "Range-free localization schemes for large scale sensor networks," in *MobiCom*, 2003.

[9] X. Sheng and Y. H. Hu, "Collaborative source localization in wireless sensor network system," in *GlobeCom*, 2003.

[10] R. Stoleru, J. A. Stankovic, and S. Son, "Robust node localization for wireless sensor networks," in *EmNets*, 2007.

[11] A. Terzis, A. Anandarajah, and K. Moore, "Slip surface localization in wireless sensor networks for landslide prediction," in *IPSN*, 2006.

[12] A. Srinivasan and J. Wu, "A survey on secure localization in wireless sensor networks."

[13] E. Elnahrawy and B. Nath, "Online data cleaning in wireless sensor networks," in *Sensys*, 2003.

[14] M.-S. Pan, H.-W. Fang, Y.-C. Liu, and Y.-C. Tseng, "Address assignment and routing schemes for zigbee-based long-thin wireless networks," in *IEEE VTC*, 2008.

[15] J. Ash and L. Potter, "Robust system multiangulation using subspace methods," in *IPSN*, 2007.

[16] D. Niculescu and B. Nath, "Ad-hoc positioning system (aps) using aoa," in *IEEE INFOCOM*, 2003.

[17] K. Chintalapudi, A. Dhariwal, R. Govindan, and G. Sukhatme, "Ad-hoc localization using ranging and sectoring," in *IEEE INFOCOM*, 2004.

[18] R. Peng and M. L. Sichitiu, "Angle of arrival localization for wireless sensor networks," in *IEEE SECON*, 2006.

[19] L. Cong and W. Zhuang, "Hybrid tdoa/aoa mobile user location for wideband cdma cellular systems," *IEEE Transactions on Wireless Communications*, vol. 1, no. 3, pp. 439–447, 2002.

[20] J. Blumenthal, F. Reichenbach, and D. Timmermann, "Precise positioning with a low complexity algorithm in ad hoc wireless sensor networks," in *PIK - Praxis der Informationsverarbeitung und Kommunikation*, 2005.