*Sensors & Transducers, Vol. 160, Issue 12, December 2013, pp. 195-201*

www.sensorsportal.com

**Sensors & Transducers**



*http://www.sensorsportal.com*

# A Trust Model for Fault Detection in Hierarchical WSN

**[1, 2] Wang NA, [3] Pang YANXIA**

[1] School of software, East China Normal University, No. 3663 North Zhongshan Rd, Shanghai, 200062, China

[2] School of Computer and information, Shanghai Second Polytechnic University, No. 2360 Jinhai Rd, Shanghai, 201209, China

[3] School of Computer and information, Shanghai Second Polytechnic University, No. 2360 Jinhai Rd, Shanghai, 201209, China

[1] Tel.: 086+18601687414, fax: 086+02150214252

E-mail:wnoffice@126.com

*Received: 18 October 2013 /Accepted: 22 November 2013 /Published: 30 December 2013*

**Abstract:** Wireless sensor networks are prone to failures and malicious attacks. A compromised node itself could report inaccurate or even forged data. So trust management is becoming a new driving force to solve challenges to WSN. In this paper, we propose a comprehensive trust model for hierarchical WSN. In this model, each node maintains a trust value according to its experience trust and social trust. Unlike previous efforts, our current design focuses on not only the node itself but also its relation with its neighbors. Results indicate the great advantage of our model to handle fault and abnormality. *Copyright © 2013 IFSA.*

**Keywords:** Abnormality, Experience trust, Fault, Hierarchical WSN, Social trust.

## 1. Introduction

Wireless sensor networks are prone to failures and malicious attacks. A compromised node itself could report inaccurate or even forged data. Trust management is becoming a new driving force to solve challenges to WSN. Generally, with trust management, each sensor node in the network is assigned a trust value to reflect its trustworthiness according to its past performance. However, as far as WSN are concerned, there are a few important issues with existing work on trust management. First, most trust research on WSN focuses on communication behavior, and data integrity is overlooked. Since data collection is the main task of WSN, the importance of data integrity should never be underestimated. Second, when recognize whether a node is integrity, several aspects should be considered rather than the node itself. Finally, different evaluation aspect may have different weight during trust value updating.

In this paper, we propose a comprehensive trust model for hierarchical WSN. In this model, each node maintains a trust value according to its experience trust and social trust. The aggregator aggregates each node's data to provide the reference to direct the trust value. Unlike previous efforts, our current design focuses on not only the node itself but also its relation with its neighbors. The results indicate the great advantage of our model to handle fault and abnormality.

The rest of the paper is organized as follows. The detailed mechanism of the experience trust model is depicted in Section 3. The detailed mechanism of the social trust model is depicted in Section 4. The analysis and evaluation of trust model are given in Sections 5. The related work and our conclusions are presented in Sections 2 and 6.

## 2. Related Work

### 2.1. Definition of Trust

Many author shave addressed the issues of trust definition in different scenarios of wireless sensor networks. Although there is no clear consensus on the definitions of trust in WSNs, most of them are generalized as follows:

Trust is a subjective opinion in the reliability of other entities or functions, including veracity of data, connectivity of path, processing capability of node and availability of service etc.

Furthermore, the concept of reputation is considered as a closed relevance measure to evaluate trust, based on the recommendations from other participants in a community. But it is clearly different with trust in definition, as illustrated by the following statements [8].

There are two key notions: reputation and direct trust. The reputation describes the node's social evaluation, and the direct trust describes the experience of one node over another. Here, Chen keeps the trustworthy networks as one-weighted digraphs, while he calls double weighted digraphs as trust-reputation networks.

The above descriptions reflect that the reputation just belongs to one of the rating methods of trustworthiness. The result depends on concrete approaches for trust evaluation. For instance, if the weight of reputation is higher, we can obtain the first results easily. Contrary to this, when the personal experience gets the upper hand, the reputation is not so important any more.

### 2.2. Trust Value

The forms of trust value may not be vital for normal networks, however, for the wireless sensor networks, the significance is completely different. In general, recording and calculating real numbers will bring much more time complexity and storage complexity. This means it spends more energy power and requires larger storage space, which, as usual, should be avoided in WSN. Thus, this issue is significant because of questions around the form of trust value to be applied, where to store those trust information, and how to process and estimate trust data in theoretical and practical terms.

### 2.3. Trust Methodologies

In recent years, a few general models have been proposed for trust management of WSNs. Ganeriwal, Balzano and Srivastava proposed a reputation-based framework for high integrity WSN named RFSN [5]. In the RFSN framework, a Bayesian formulation is employed to update reputation metrics with new transactions, density-based outlier detection discovers data outliers, and an aging mechanism is used against the sleeper attack. Other trust model studies include an agent-based trust model by Chen et al. [6] etc. As far as the hierarchical WSN are concerned, Guoxing Zhan's Sensor Trust model [7] use the Gaussian distribution of data and its mathematical analysis shows that the update protocol effectively incorporates long-term reputation and recent risk. In contrast to the aging algorithm used in RFSN, its model utilizes two parameters to gain more flexibility for different contexts. Trust Voting [4] is an efficient in-network voting algorithm to determine faulty sensor readings based on Sensor Rank by exploring Markov Chain. Compared with the distance-based weighted voting which gives more weight to closer neighbors in voting, they argue that the distance between two sensor nodes does not fully represent the correlation between readings of those two sensors. More seriously, if the nearest sensor is faulty, the voting result may be contaminated by this faulty sensor. Hence, the correlation of sensor readings rather than their distance should be considered in the voting.

But none of the above models have combined reputation (social trust) value and personal experience (experience trust) value in WSN and they only focus on personal experiences compared with former sensed value in a continuous time. When a sensor's value keeps little fluctuation, we may regard it as normal and no fault. But when the value changed significantly, we should not regard it as fault. Moreover, the reputation value must be considered for recognizing outlier as abnormal event detection but not faulty.

## 3. Experience Trust Model

The hierarchical structure has been widely accepted in designing WSN. In a hierarchical clustering WSN, child node relays data to its cluster head which is aggregator, and those aggregators forward received data to their higher level parent aggregators (cluster head), and the forwarding continues until the top layer of the hierarchy, at which point the data will be sent to the base station. Such a hierarchical structure is easy to implement, and it is known that the hierarchical structure enables more efficient use of scarce resources, such as energy.

Our model employs a Gaussian model to rate data integrity. Our goal is to establish a trust environment against faults and attacks. We first assume the aggregators are trustable, and let the aggregators evaluate the trustworthiness of their children nodes. We make the following assumption: in the same cluster, the distribution of the data collected by sensor nodes can be depicted by the well-known Gaussian model as shown in Fig. 1.

After the aggregator has get an aggregation value by the algorithm as shown in Fig. 2, each child node will has an experience trust rank.

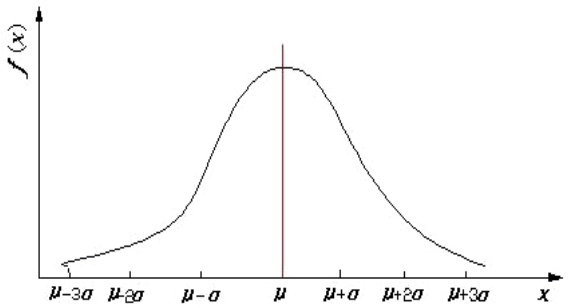


**Fig. 1.** Gaussian distribution diagram.

float Aggregation ( $D_i$):
Definition:
dist(i,j): difference between i and j;
$C_i$: ith set;
$c_i$ : average of set $C_i$;
n: number of sets
count: size of set
agg: return value
_: aggregation radius
Initialization:
min (di)⊙$C_1$;
max (di)⊙$C_2$;
for (k=1;k<m;k++)
for (i=0;i<n;i++)
{
if dist($d_k$, $c_i$)>_ then
{$d_k$⊙$C_{n+1}$; n=n+1;}
else $d_k$⊙$C_i$
}
for (i=0;i<n-1; i++)
for(j=1;j<n; j++)
{ if (($\triangleq d_k$ ⊙$C_j$) dist($d_k$, $c_i$)<_)
Then
{Merge( $C_i$,$C_j$);
n=n-1;}
}
for (i=0;i<n-1; i++)
count=max (|$C_i$|);
return $c_i$;

**Fig. 2.** Aggregation algorithm.

In the algorithm, firstly, we sort the data in D ascending and add the minimum to C1 and maximum to C2. Then calculate Ci's average implied as ci. Secondly, for arbitrary node k, if dist (dk,ci) > _ build a new set include dk. Otherwise, add it to Ci that is closest to dk and refresh the average. Repeat above procedures till the number of sets doesn't change. After the partition, we choose the average of Ci having the most members as aggregation value.

Denote X as sensor data, μ as the aggregation value received by the aggregator, and σ as the mean square deviation of sensor data in set Ci. Then we have:

$$X \sim N(\mu, \sigma), \text{ and } \sim N(0, 1), \quad (1)$$

And the experience trust can be defined as: $Te = e^{\frac{-(x-\mu)^2}{\sigma^2}}$. If a node's data is considerably deviated from μ, its experience trust will be limited to zero. The different sensor data will cause different experience trust as in Table 1.

**Table 1.** Experience trust.

| \|X-μ\| | 0 | σ | 2σ | 3σ | 4σ | … | n*σ |
|---|---|---|---|---|---|---|---|
| $T_e$ | 1 | 0.607 | 0.135 | 0.011 | 0.0003 | … | 0 |

## 4. Social Trust Model

As mentioned in section 3, when a sensor data is greatly different from aggregator value, the sensor's experience trust rank will limit to zero. In traditional method, we may consider it as a faulty node, but as an event occurs, sensors that response to the event will provide abnormal sample data. So the outlier get according to experience trust rank may be an alarm of abnormal event and we must manage such data with another method.

The method we propose in this paper called social trust which reflects a sensor's trust level with relative to its neighbors. In clustered WSNs, with different clustering algorithm, some nodes are not in the same cluster with their neighbors as shown in Fig. 3.

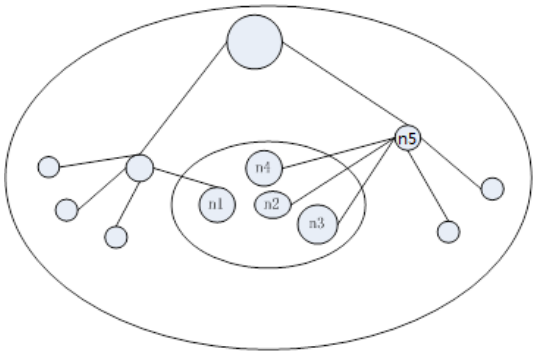


**Fig. 3.** A cluster based WSN with an event.

In Fig. 2, n1 is not in the same cluster with its neighbor n2, n3, and n4. When an event occurs, n1 may detect different data from members in the same cluster and will have a low experience trust according to section 3. In fact, n1 just report a very important abnormal event and its neighbors report approximated data at the same time which can prove n1is not fault but abnormal.

We treat nodes detecting event as follow process:

When a node's experience trust value is lower than a threshold, it sends a request to its neighbors to build a weighted connected diagram. The similarity is set as edges' weight and the social trust value is set as vertexes' weight.

Definiton 1. Dual-weighted network G:

G = (V, E, T, S) consists of vertexes V, edges E, trust weight T and similarity weight S. Each vertex is a node and each edge is the connection of two neighbors.

Definition 2. Similarity:

Once the neighbor network of sensors is constructed (and maintained), one can easily deduce the similarity among sensor nodes as: Si, j $= \frac{x_i x_j}{x_i^2 + x_j^2 - x_i x_j}$. Based on the dual-weighted network, we shall further develop an algorithm to compute social trust for each sensor node, in terms of the similarity with its neighbors.

A sensor node which has a large number of similar neighbors should have a high social trust value and a sensor node which has a large number of good references to have a high social trust value. So we can formulate social trust value of $s_i$, denoted as Ts, as follows:

$$T_{si} = \sum_{j \in nei(i)} T_{sj} * \frac{S_{i,j}}{\sum_{j \in nei(i)} S_{i,j}}, \quad (2)$$

The computation of trust value can be viewed as a random walk over the neighbor network. Several iterations are required to perform random walks until a steady state is achieved. Specially, Tsi(k) is the trust value at the k-th iteration. At the beginning, the initial Tsi (0) is set to 1. In the first round, each sensor node updates its trust value as Tsi (1) using the initial trust value of its neighbors. Now each sensor node has considered the first level neighbors to calculate its trust value. In the second round, each sensor node can indirectly obtain some information from the second level neighbors through its first level neighbors since its first level neighbors have explored their first level neighbors as well. Therefore, after the $k^{th}$ round, sensor node i has explored the kth level neighbors and up- dated trust value as Tsi(k). The algorithm computing social trust value is depicted in Fig. 4.

Input: sensor node I and iterations δ.
Output: $T_{si}$
$T_{si}^{(0)}=1$;
for k = 1 to δ do
for all j⊙nei(i) do
{
$S_{i,j}= \frac{x_i x_j}{x_i^2 + x_j^2 - x_i x_j}$;
Send $T_{si}^{(k-1)}$ to j;
Receive all $T_{sj}^{(k-1)}$ from j⊙nei(i);

$$T_{si} = \sum_{j \in nei(i)} T_{sj} * \frac{S_{i,j}}{\sum_{j \in nei(i)} S_{i,j}}$$

}

**Fig. 4.** Algorithm computing social trust value.

For example, in Fig. 5, n1 has tree neighbors and the similarity between n1 and the three other nodes is 0.9, 0.88 and 0.95 respectively. Each node has a social trust value as 0.8, 0.9, 1.0 and 0.85 in certain iteration. The social trust value of each node is as in Table 2.

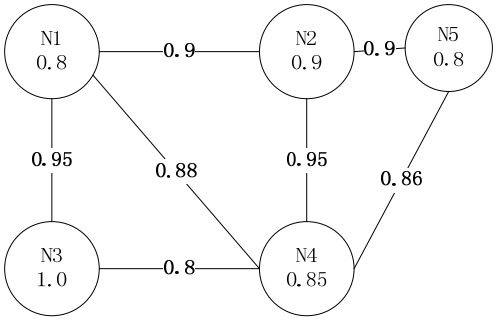


**Fig. 5.** An example of dual-weighted network.

**Table 2.** Social trust value.

| | N1 | N2 | N3 | N4 | N5 |
|---|---|---|---|---|---|
| K=h | 0.8 | 0.9 | 0.85 | 1.0 | 0.8 |
| K=h+1 | 0.919 | 0.817 | 0.88 | 0.843 | 0.876 |
| K=h+2 | 0.863 | 0.879 | 0.82 | 0.872 | 0.83 |

In this process, n5 is added as n1's indirect neighbor in iteration h+2. As there is no other node to be added, the iteration is end at the third round.

We can conclude from above table that n4 who has the most neighbors get the highest social trust value. When abnormality occurs, all normal nodes in this area will detect the abnormality and send information to its cluster. But not all nodes in one cluster can detect the abnormality because some of them may not in the abnormality area. Then node detecting the abnormality will be regarded as outlier using aggregation protocol. In fact, other nodes in the abnormality area can prove the "outlier" is a useful sensor data. In this example, n1 can be recognized as a node detecting abnormality by computing its social trust.

## 5. Trust Model and Evaluation

As introduced in section 3 and section 4, neither experience trust value no social trust value can decide whether a node is normal or fault independently. In order to get a precise decision and make lower false positive rate, we must combine both the aspects to evaluate a node's trust level. So we update trust value as follows:

$$T = \begin{Bmatrix} (1-W) * T_e + W * T_1; if T_e \le treshold \\ T_e; if T_e \ge treshold \end{Bmatrix}, \quad (3)$$

$$Stateofnode = \left\{ \begin{matrix} Fault : ifT < 0,8 \\ Normal : ifT \geq 0,8 \end{matrix} \right\}, \quad (4)$$

We analyze the efficacy of Trust model against abnormal data and fault data though generating a few abnormal nodes and faulty nodes. Firstly, we input 59 nodes and give a fixed probably faulty rate as 0.2.

The relation between iteration and social trust value can be described as in Fig. 6.

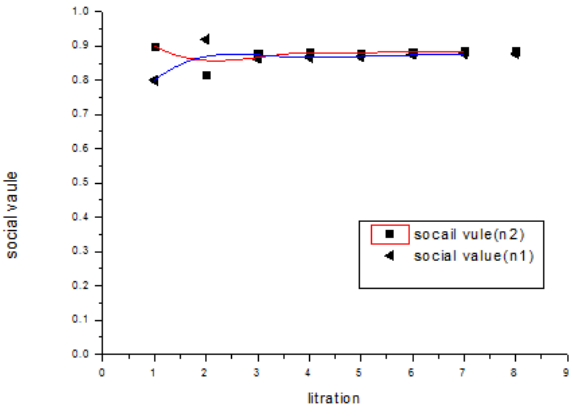


**Fig. 6.** Social trust with different iteration.

This figure shows that a node's social trust value will be invariability since it has finite neighbors and indirect neighbors.

When threshold is 0.9, 0.607 and 0.135 respectively, we select different w to compute each node's trust value that may get different result of faulty detection rate. The simulation result is as shown in Fig. 7.

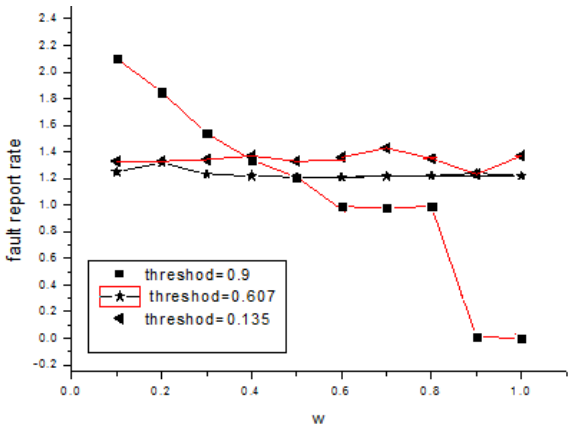


**Fig. 7.** Fault report rate with different w and threshold

The result shows that when threshold is too low, some abnormal nodes may be considered as fault and the fault report rate is above 1. Fault report rate reach to about 0 when w is between 0.9 and 1, and threshold is above 0.9.

## 6. Conclusion

With the presence of faulty readings, the accuracy of query results in wireless sensor networks may be greatly affected. So how to detect faulty is crucial in WSN. But there are still fictitious fault nodes in consideration of nodes detecting events. In this paper, we first present two types of trust that are experience trust which is deduced from its cluster members and social trust value which is deduced from its neighbors. Then we propose the method to compute these two trust values. Base on two types of trust value, we introduced the combination of two trust values. Performance evaluation shows that by exploiting our new trust model, when proper parameter (w and threshold) is set, it is able to efficiently identify faulty readings and discriminate abnormality reading with lower fault report rate.

## Acknowledgements

This work is supported by the key discipline of Shanghai second polytechnic University named software engineering (No. XXKZD1301), and Shanghai Municipal Natural Science Foundation (No. 11ZR1413700).

## References

[1]. A. Jøsang, A logic for uncertain probabilities, *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, Vol. 9, Issue 3, 2001, pp. 279-311.

[2]. W. Chunxue, Z. Fengna, Y. Hongming, A novel QoS multipath path routing in MANET, *International Journal of Digital Content Technology and its Applications*, 2010.

[3]. A. Jøsang, R. Ismail, C. Boyd, A survey of trust and reputation systems for online service provision, *Decision Support Systems,* Vol. 43, Issue 2, 2007, pp. 618-44.

[4]. X. Xiao, W. Peng, C. Hung, W. Lee, Using sensor ranks for in-network detection of faulty readings in wireless sensor networks, in *Proceeding of the 6th ACM Workshop on Data Engineering for Wireless and Mobile Access (MobiDE'07)*, Beijing, China, 2007.

[5]. S. Ganeriwal, L. Balzano, M. Srivastava, Reputation-based framework for high integrity sensor networks, *ACM Transactions on Sensor Networks*, 2008.

[6]. H. Chen, H. Wu, X. Zhou, C. Gao, Agent-based trust model in wireless sensor networks, in *Proceedings of the 8th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing*, 2007, pp. 119-124.

[7]. G. Zhana, W. Shi, J. Deng, Sensor Trust: A resilient trust model for wireless sensing systems, *Pervasive and Mobile Computing*, 2011.

[8]. Y. Chen, B. Tian-Ming, M. Zhang, H. Zhu, Measurement of Trust Transitivity in Trustworthy Networks, *Journal of Emerging Technologies in Web Intelligence*, Vol. 2, Issue 4, November 2010.

[9]. W. Chunxue; Hou Feiyue, Design and Optimization of Redundant Control Net Networking Control System, *Process Automation Instrumentation*, Vol. 32, March 2011.
[10]. Z. Yang, L. Jean, C. Wu, Y. Liu, Beyond Triangle Inequality: Sifting Noisy and Outlier Distance Measurements for Localization, *ACM Transactions on Sensor Networks*, Vol. 9, March 2013.
[11]. W. Chunxue; F. Bin, Based on Single-hop Flow Control Scheme for Wireless Sensor Networks, in *Proceedings of YET Conference on Wireless, Mobile and Sensor Networks 2007*, December 2007.
[12]. W. Chunxue, Practical models and control methods with data packets loss on NCOS, in *Proceedings of the YET International Conference on Wireless Mobile and Multimedia Networks,* January 2006.
[13]. A. R. M. Kamala, C. Bleakly, S. Dobson, Packet-Level Attestation (PAL): A Framework for In-Network Sensor Data Reliability, *ACM Transactions on Sensor Networks*, Vol. 9, March 2013.


**Organizing Committee:**

**General Chair:**
Juan Carlos Miguez, Region 9

**Technical Program Chair:**
Daniel Slomovitz, UTE Laboratory

**Technical Program Co-Chairs:**
Bernardo Tellini, University of Pisa
Wendy Van Moer, VUB Brussels

**Publications Chair:**
Pablo Thomasset, IMS Chapter Chair

**Tutorials Chair:**
Alfredo Arnaud, Universidad Catolica Uruguay

**Special Sessions Chair:**
Conrado Rossi, Universidad de la Republica Uruguay

**Important Deadlines:**

**October 15, 2013**
Submission of Extended Abstracts

**January 15, 2014**
Notification of paper acceptance

**March 15, 2014**
Deadline for Camera-ready papers

**Sponsored By:**

IEEE IEEE Instrumentation & measurement society

**Web Page:**
**imtc.ieee-ims.org**

## 2014 IEEE International Instrumentation and Measurement Technology Conference

### *Montevideo, Uruguay May 12-15*

I²MTC 2014 spans research, development and applications in the field of instrumentation and measurement science and technology. This includes Industrial Tracks, where research merges with practical applications in industrial technology used every day. The Conference fosters the exchange of know-how between industry and academia. Paper contests will include a Conference Best Paper Award and Student Best Poster Awards. In addition to papers, the conference will also have Tutorials and Exhibits covering the entire range of Instrumentation and Measurement Technology.

The Conference focuses on all aspects of instrumentation and measurement science and technology-research, development and applications. The program topics include:

- Advances in Instrumentation and Measurement Developments and Techniques
- Biomedical Systems
- Data Acquisition Systems and Techniques
- Energy and Power Systems
- Industrial Process Control
- Measurement and Instrumentation for Industrial Applications
- Measurement Applications
- Measurement of Electric and Magnetic Quantities
- Measurement of Materials and Mechanical Quantities
- Measurement, Instrumentation and Methodologies Related to Healthcare Systems
- Measurement Systems and Theory
- Non-invasive Measurement Techniques and Instrumentation
- Real-Time Measurement
- Robotics and Controls
- Sensors and Sensor Fusion
- Signal & Image Processing Techniques
- Software Development for Measurement and Instrumentation Support
- Techniques related to Instrumentation
- Transducers
- Virtual Measurement Systems
- Wireless Sensors and Systems

Given that the 2014 conference's theme is "**Instrumentation and Measurement for Sustainable Development**", we strongly encourage submissions in the areas of energy, communication instrumentation, measurement, system development and recent advances.

Potential authors are invited to submit extended abstracts via the I²MTC website.

Each extended abstract (3 or 4 pages in English) should report results of the original research of theoretical or applied nature. The extended abstract should, moreover, explain the significance of the contribution and contain a list of key references. It must be prepared according to the abstract preparation guidelines provided on the I²MTC website. A Student Poster Contest will be held for both graduate and undergraduate student papers, with cash awards for the best papers and travel subsidies ranging from USD 300 to USD 1000, depending on student location. Extended abstracts should be submitted by the students according to the rules posted on the website and should be identified as student papers. Check the website for detailed instructions and deadlines.

Authors of accepted papers must register for the Conference and attend to present their papers. The authors of papers presented during I²MTC 2014 will be allowed to submit expanded and extended versions of their papers to the Special Issue of IEEE Transactions on Instrumentation & Measurement on I²MTC 2014 to be published in 2015.