An Improved Distance Estimation Algorithm Based on Generalized CRT

Ping Deng, Yunhe Cui
Key Lab of Information Coding and Transmission, Southwest Jiaotong University, PR of China, 610031
Email: pdeng@swjtu.edu.cn, laker13438498169@126.com,

Abstract—**In wireless sensor and actuator network(WSAN), in order to determine the location of sensors based on the range-based location techniques, estimating accurately the distances between sensors and actuators is very important. In this paper, based on the analysis of Generalized Chinese Remainder Theorem(CRT), some improvement to the Generalized CRT was made and an improved distance estimation algorithm which can be used in WSAN was proposed. In addition, the derivation and proof of the improved algorithm were provided. The simulation results have shown the validity of this algorithm.**

Keywords-Chinese remainder theorem; reference item; distance estimation; WSAN

I. INTRODUCTION

Wireless sensor and actuator network(WSAN) is composed of a group of sensors and actuators to perform distributed sensing and acting tasks [1]. In WSAN, sensors are low-cost, low power devices with limited sensing, computation and wireless communication capabilities, while actors are resource rich nodes with better processing capabilities, higher transmission powers and longer battery life. Similar to WSN, node localization is also a key issue in WSAN. The node location message is indispensable to many applications of WSAN. In order to determine the location of sensors based on the range-based location techniques, accurately estimating the distances between sensors and actors is very important.

In recent years, Chinese remainder theorem(CRT) has been applied in many fields, such as signal processing, coding and cryptography [2]. Also, CRT has been used in the distance estimation in WSN. The traditional CRT can reconstruct the unknown integer by a group of remainders and modulus, but it is not robust in the sense that even a small error in any remainders may cause a large error in the reconstructed result [2]. The algorithm in [3] is a robust CRT and it makes preferable estimation accuracy, but it requires a complex two-dimension searching. A fast robust CRT has been proposed in [4], which only needs one-dimension searching. However, the computation complexity of this algorithm is still a problem. Recently, a closed form CRT has been proposed in [5]. Utilizing the properties of CRT, an efficient distance estimation algorithm with closed-form solution is proposed in [6]. Compared with other algorithms, this closed-form generalized CRT can get better accuracy of estimation, enhance the robustness to the noise and undertake lower computation cost. Therefore, it can be used in the distance estimation in WSAN. But in the parameter solution process of this algorithm, the first remainder is selected as the reference item randomly, which may influence the accuracy of distance estimation. Aiming at this deficiency, in this paper we propose an improved distance estimation algorithm by making improvement to the generalized CRT. In this algorithm, the more suitable reference remainder is selected. Simulation results in WSAN environments have shown the validity of this algorithm.

II. CRT AND DISTANCE ESTIMATION

A. *Distance estimation based on carrier-phase and CRT*

In WSAN, the carrier phase can be used to estimate the distance between sensors and actuators. The general process can be described as follows. First of all, actuators send k carriers with known wavelength and phase, and sensors measure the carrier phases $\theta_i \in [0, 2\pi), 1 \le i \le K$. Then, the different decimal distance can be described as: $\gamma_i = \lambda_i \bullet \theta_i / 2\pi$, and the unknown distance can be expressed by $d = n_i\lambda_i + \gamma_i$, where n_i is the integer cycle of the *ith* carrier. Because of the existence of phase ambiguity, n_i is hard to be determined accurately, and this will cause the big distance estimate error.

CRT can be used to solve the phase ambiguity problem. Simply speaking, CRT is a process that calculates the unknown integer based on a group of remainders and modulus. Compared with the carrier phase based on distance estimation, we can consider that the unknown integer, modulus and remainders in CRT correspond to the d , λ_i and γ_i respectively in the carrier phase based on distance estimation. The traditional CRT is not robust to the phase error, then a generalized CRT with better performance was proposed [6].

B. *Generalized CRT and its analysis*

Let N be a positive integer, $M_1 < M_2 < \cdots M_L$ be L module, and $r_1, r_2, \cdots r_L$ be L remainders.

$$N \equiv r_i \bmod M_i \text{ or } N = n_i M_i + r_i \qquad (1)$$

where $n_i (1 \le i \le L)$ is an unknown integer. If $0 \le N < lcm(M_1, M_2, \cdots M_L)$ and all M_i are co-prime, N can be determined by the traditional CRT. When $M_i (1 \le i \le L)$ are not co-prime, define: $M \triangleq \gcd(M_1, M_2, \cdots M_L)$.

This work was supported by the National Natural Science Foundation of China under Grant No. 61071107 and Key Grant Project of Chinese Ministry of Education under Grant No. 311031.

978-1-4673-1881-5/12/$31.00 ©2012 IEEE

Let $\Gamma_i = M_i / M$. It's easy to see that all Γ_i are co-prime. Define $\Gamma \triangleq \prod_{k=1}^{L} \Gamma_k$, and let

$$\alpha_i = (\prod_{k=1}^{L} \Gamma_k) / \Gamma_i = \Gamma / \Gamma_i \quad (2)$$

$$q_i \triangleq \lfloor r_i / M \rfloor \quad (3)$$

where $\lfloor \bullet \rfloor$ denotes the flooring operation. And then

$$r_i \triangleq q_i M + r^c \quad (4)$$

where $r^c = N \bmod M$ is the common remainder of $r_i (1 \le i \le L)$ modulo M. Define

$$N_0 \triangleq \lfloor N / M \rfloor \quad (5)$$

If $0 \le N_0 < \Gamma$, N_0 can be reconstructed by

$$N_0 = \sum_{i=1}^{L} \alpha_i \bar{\alpha}_i q_i \bmod \Gamma \quad (6)$$

where $\alpha_i \bar{\alpha}_i \equiv 1 \bmod \Gamma_i$. Let $\varepsilon_i = \alpha_i \bar{\alpha}_i$, then we find ε_i has the following property.

Property 1:

$$\sum_{i=1}^{L} \varepsilon_i = 1 (\bmod \Gamma) \quad (7)$$

For any Γ , let $q_i = 1 (1 \le i \le L)$, then $N_0 = 1$ is the only solution. From above, we have:

$$\begin{aligned} N_0 &= \sum_{i=1}^{L} \alpha_i \bar{\alpha}_i q_i \bmod \Gamma \\ &= \sum_{i=1}^{L} \varepsilon_i \bmod \Gamma \equiv 1 \bmod \Gamma \end{aligned} \quad (8)$$

Hence, property 1 is proved.

Therefore, N can be reconstructed by

$$N = M N_0 + r^c \quad (9)$$

Actually, the remainders have errors. Let the ith erroneous remainder be

$$r_i \triangleq r_{i0} + \Delta r_i \quad (10)$$

Where r_{i0} is the real value of r_i and Δr_i denotes the error or noise. With these erroneous remainders, (3) becomes

$$q_{i,1} = \lfloor r_i / M \rfloor = \left\lfloor \frac{q_{i0} M + r^c + \Delta r_i}{M} \right\rfloor = q_{i0} + \left\lfloor \frac{r^c + \Delta r_i}{M} \right\rfloor \quad (11)$$

where q_{i0} is the true value of q_i . From (4), $r^c = r_i - q_i M$. Let $r^c = r_i - q_i M = r_1 - q_1 M$ .Then the relationship between q_i and q_1 is as follows:

$$q_i = q_1 + \frac{r_i - r_1}{M} = q_1 + \frac{r_{i0} - r_{10}}{M} + \frac{\Delta r_i - \Delta r_1}{M} \quad (12)$$

It is well known that CRT can reconstruct the unknown integer only in the set of positive integers. Here we make rounding operation in (12), i.e.

$$q_i = \left[q_1 + \frac{r_i - r_1}{M} \right] = q_1 + \frac{r_{i0} - r_{10}}{M} + \left[\frac{\Delta r_i - \Delta r_1}{M} \right] \quad (13)$$

where $[\bullet]$ denotes rounding operation and q_i is expressed by q_1 . If $\left[\frac{\Delta r_i - \Delta r_1}{M} \right] = 0$, Δq_i , which is the error of q_i , is equal to Δq_1 . That is to say, all errors of q_i are equal.

Based on Property 1, the error of N_0 can be expressed as

$$\Delta N_0 = \sum_{i=1}^{L} \varepsilon_i \Delta q_1 = \Delta q_1 (\bmod \Gamma) \quad (14)$$

In general case, ε_i is a large integer. After treatment above, ΔN_0 is greatly reduced.

Based on above discussion, we know that if

$$\left[\frac{\Delta r_i - \Delta r_1}{M} \right] = 0 \text{ or } \left| \frac{\Delta r_i - \Delta r_1}{M} \right| < \frac{1}{2} \quad (15)$$

N can be reconstructed accurately by (9).

In order to determine r^c in (9), we can take the average of all remainders of r_i mod M. That is

$$r'_i = r_i - q_i \bullet M \quad (16)$$

$$r^c = \frac{1}{L} \sum_{i=1}^{L} r'_i \quad (17)$$

C. The Improvement to the generalized CRT

Based on above analysis, we notice that the remainder which is used as the reference item in (12) is the first remainder in the generalized CRT. It is a random item and the performance of generalized CRT will be greatly influenced by this item. Clearly, if we select the remainder whose error is the median of all remainder errors as the reference item, the probability of satisfying formula (15) will be larger and the unknown integer can be reconstructed more accurately because of the rounding operation,

In order to find the median of all remainder errors, we turn formula (13) into another expression. From (11), we define

$$q_j = \lfloor r_j / M \rfloor = q_{j0} + \left\lfloor \frac{r^c + \Delta r_j}{M} \right\rfloor \quad (18)$$

Then we have

$$
\begin{aligned}
q_{i,2,j} &= \left\lfloor q_j + \frac{r_i - r_1}{M} \right\rfloor \\
&= q_{j0} + \left\lfloor \frac{r^c + \Delta r_j}{M} \right\rfloor + \frac{r_{i0} - r_{j0}}{M} + \left\lfloor \frac{\Delta r_i - \Delta r_j}{M} \right\rfloor \\
&= q_{i0} + \left\lfloor \frac{r^c + \Delta r_j}{M} \right\rfloor + \left\lfloor \frac{\Delta r_i - \Delta r_j}{M} \right\rfloor
\end{aligned} \tag{19}
$$

Hence, we can get another property.

Property 2:

When we use q_j as the reference item to determine q_i, if $\Delta r_i \geq \Delta r_j$, we will get $q_{i,1} = q_{i,2,j}$. Otherwise, we will get $q_{i,1} \neq q_{i,2,j}$. This property is proved in Appendix.

In order to find the remainder whose error is the median of all remainder errors, we should find such a reference item q_j, which makes the number of $q_{i,1} = q_{i,2,j} (1 \leq i \leq L, i \neq j)$ equal to that of $q_{i,1} \neq q_{i,2,j} (1 \leq i \leq L, i \neq j)$.

Finally, the reference item can be selected based on steps below.

- **Step 1:** Using (11) to calculate $q_{i,1} (1 \leq i \leq L)$ and $q_j (1 \leq j \leq L)$.
- **Step 2:** Take the L q_j as reference item to calculate the $q_{i,2,j} (1 \leq i \leq L, 1 \leq j \leq L, i \neq j)$ using (19).
- **Step 3:** For any q_j, calculate the number as *num1* where $q_{i,2,j} = q_{i,1} (1 \leq i \leq L, 1 \leq j \leq L, i \neq j)$; otherwise calculate it as $num2$.
- **Step 4:** When L is an odd number, if $num1 = num2$, take the q_j as the reference item. When L is a even number, if $num1 = num2 \pm 1$, take the q_j as the reference item.
- **Step 5:** If there is no q_j to satisfy the condition, take q_1 as the reference item.

In the worst situation, L^2 times searching is needed to find the reference item. In carrier phase based ranging, L is usually a very small number, so the computation cost is limited.

When we find the proper q_j, we can use (13) to determine all the q_i. When all q_i are fixed, we can use (8) and (9) to reconstruct N.

D. Distance Estimation between nodes and actuators in WSAN

In order to estimate the distance between nodes and actuators in WSAN, first of all, we use L radio waves whose wavelength are $\lambda_i (1 \leq i \leq L)$ to make the carrier phase measurement based on the method in [7]. Then we get different phase measurements which correspond to the decimal distance $\gamma_i = \lambda_i \bullet \theta_i / 2\pi$. This can be expressed by $d = n_i \lambda_i + \gamma_i$. Then we can get the conclusion that the dividend in CRT, the modulus, and the remainders correspond to the distance d, the wavelength λ_i and the decimal distance γ_i respectively. Therefore, we can estimate the unknown distance based on the improved generalized CRT.

The improved distance estimation algorithm based on the improved generalized CRT to estimate the unknown distance between nodes and actuators in WSAN can be summarized as:

- **Step 1:** Quantization: Assume the quantization unit is u, then the integral decimal distance and modulus are $r_i = round(\gamma_i / u)$ and $M_i = round(\lambda_i / u)$.
- **Step 2:** Choose the reference item using the method in section □C and calculate q_i by (13).
- **Step 3:** Calculate N_0 by (8).
- **Step 4:** Calculate r'_i and r^c by (16) and (17).
- **Step 5:** Calculate N by (9). Then we can get the unknown distance: $d = N \bullet u$.

III. Simulation and Discussion

In order to validate the performance of the improved algorithm, two groups of simulation were carried out in a WSAN environment. Simulation 1 appraised the effectiveness of the method under the condition that the standard deviation of the remainder error is known. Simulation 2 compared the performance of the original and improved algorithm under different SNR.

A. Simulation 1

Five radio waves whose wavelength are [0.0250 0.0350 0.0450 0.0550 0.0650]m are used to measure the distances between sensors and actuators. Assume the unknown distances between sensors and actors are uniformly distributed in $0 \sim 225m$, and the phase errors can be considered to be $N(0, \sigma^2)$ normally distributed.

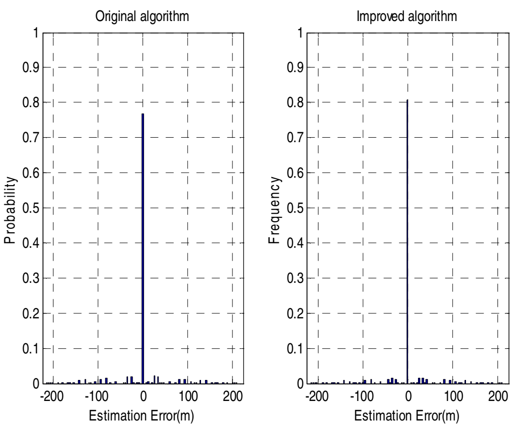

Fig.1. The distribution of estimation error when $\sigma = 10$.

Firstly, let $\sigma = 10$, the error distribution is demonstrated in Fig.1. Under this situation, the standard variance of the phase estimation error is about 6 degree and the SNR is about 3dB, and the probability of error estimation is about 18% because of the condition that $(\Delta r_i - \Delta r_j)/M < 1/2$ can not be satisfied. Compared with the original algorithm, the probability of correct estimation increases about 5%. It can be shown that the improved algorithm is more precise than the original algorithm under the same condition because of the proper selection of the reference item.

B. Simulation 2

Here the performance of the improved algorithm and the original algorithm under different SNRs are compared. Five radio waves whose wavelength are [0.0250 0.0350 0.0450 0.0550 0.0650]m are utilized, and the unknown distance is uniformly distributed in $0 \sim 225m$.

In Fig.2, the correct estimation probability of the improved algorithm and original algorithm in [6] are compared. In Fig.3, the RMSE error of the two algorithms is contrasted.

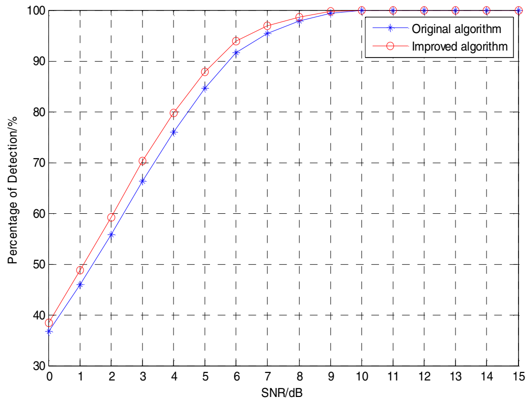

Fig.2. Percentage of correct estimation versus SNR

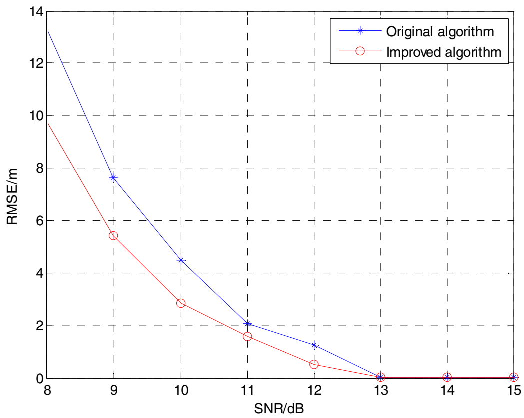

Fig.3. Estimation RMSE error versus SNR

It is shown that when SNR is low, the condition that $(\Delta r_i - \Delta r_j)/M < 1/2$ can not be met, therefore, the probability of correct estimation is small and the estimation error is unsatisfied in this situation. When SNR is improved, the probability of correct estimation is increased and the estimation error decreases with the increase of SNR. Because of the proper selection of the reference item, the performance of the improved algorithm is better than the original one. The correct estimation probability increases about 3% and the RMSE estimation error decreases about 3.0m averagely.

IV. CONCLUSION

In this paper, an improved distance estimation algorithm based on the improvement to the generalized CRT is proposed, the remainder whose error is the median of all errors is selected as the proper reference item. The simulation results under different situation have shown that the improved algorithm can remarkably improve the distance estimation performance in WSAN environments, and this algorithm can be used in other wireless network environments also.

APPENDIX

Proof of Property 2

Let

$$\left\lfloor \frac{r^c + \Delta r_i}{M} \right\rfloor \triangleq n_1 \tag{20}$$

$$\left\lfloor \frac{r^c + \Delta r_j}{M} \right\rfloor \triangleq n_2 \tag{21}$$

From (20) and (21), we have

$$r^c + \Delta r_i \triangleq n_1 M + c_i \tag{22}$$

$$r^c + \Delta r_j \triangleq n_2 M + c_j \tag{23}$$

Where $0 \le c_i < M$ .then

$$\left\lfloor \frac{\Delta r_i - \Delta r_j}{M} \right\rfloor = \left\lfloor \frac{(n_1 - n_2)M + (c_i - c_j)}{M} \right\rfloor \tag{24}$$

When $0 \le c_i - c_j < M$, (24) can be change into

$$\left\lfloor \frac{\Delta r_i - \Delta r_j}{M} \right\rfloor = \left\lfloor \frac{(n_1 - n_2)M + (c_i - c_j)}{M} \right\rfloor = n_1 - n_2 \tag{25}$$

And

$$q_{i,1} - q_{i,2,j} = \left\lfloor \frac{r^c + \Delta r_i}{M} \right\rfloor - \left\lfloor \frac{r^c + \Delta r_j}{M} \right\rfloor - \left\lfloor \frac{\Delta r_i - \Delta r_j}{M} \right\rfloor = 0 \tag{26}$$

That is, if $c_i \ge c_j$, $q_{i,1} = q_{i,2,j}$.

The same as (25), when $-M < c_i - c_j < 0$,we have

$$\left\lfloor \frac{\Delta r_i - \Delta r_j}{M} \right\rfloor = \left\lfloor \frac{(n_1 - n_2)M + (c_i - c_j)}{M} \right\rfloor = n_1 - n_2 - 1 \tag{27}$$

$$q_{i,1} - q_{i,2,j} = \left\lfloor \frac{r^c + \Delta r_i}{M} \right\rfloor - \left\lfloor \frac{r^c + \Delta r_j}{M} \right\rfloor - \left\lfloor \frac{\Delta r_i - \Delta r_j}{M} \right\rfloor = 1 \tag{28}$$

That is, if $c_i < c_j$, $q_{i,1} \neq q_{i,2,j}$.

From (22) and (23), we have

$$\Delta r_i - \Delta r_j = (n_1 - n_2)M + (c_i - c_j) \tag{29}$$

We discuss (27) in two situations: (1) $n_1 \neq n_2$ (2) $n_1 = n_2$.

- $n_1 \neq n_2$: From the definition of c_i and c_j , we know that $c_i \sim U(0,M)$ and $c_j \sim U(0,M)$. Then it is clear to see that the probability of $c_i \geq c_j$ is approximately 50% which is equal to the probability of $c_i < c_j$.
- $n_1 = n_2$: If $c_i \geq c_j$, motivated from (18) and (19), we know that $\Delta r_i \geq \Delta r_j$. Similarly, if $c_i < c_j$, we have $\Delta r_i < \Delta r_j$. In one word, if $\Delta r_i \geq \Delta r_j$, we will get $q_{i,1} = q_{i,2,j}$. Otherwise, we will get $q_{i,1} \neq q_{i,2,j}$.

Assume that the probability of $n_1 = n_2$ is p_1 , then the probability of $n_1 > n_2$ is equal to $n_1 < n_2$ which is $(1-p_1)/2$. Then we can see that if $c_i \geq c_j$, the probability of $\Delta r_i \geq \Delta r_j$ is

$$\begin{aligned} &p\{\Delta r_i \geq \Delta r_j \left| c_i \geq c_j \right.\} = p\{n_1 = n_2\} \bullet 1 \\ &+ p\{n_1 > n_2\} \bullet \frac{1}{2} + p\{n_1 < n_2\} \bullet 0 \\ &= p_1 * 1 + \frac{1-p_1}{2} * \frac{1}{2} + \frac{1-p_1}{2} * 0 \\ &= \frac{1+3p_1}{4} \end{aligned} \tag{30}$$

Similarly, we can get that if $c_i < c_j$ the probability of $\Delta r_i < \Delta r_j$ is

$$p\{\Delta r_i < \Delta r_j \left| c_i < c_j \right.\} = \frac{1+3p_1}{4} \tag{31}$$

Now we study the probability when $n_1 = n_2$.

Assume $\Delta r_i \sim N(0,\sigma^2)$, we have $\Delta r_i - \Delta r_j \sim N(0,2\sigma^2)$. Then

$$\begin{aligned} &p\{n_1 = n_2\} = p\{n_1 = n_2 = 0\} \\ &+ p\{n_1 = n_2 = 1\} + \cdots + p\{n_1 = n_2 = +\infty\} \end{aligned} \tag{33}$$

This property can still be demonstrated by simulation, here we use five radio waves whose wavelength are [0.0250 0.0350 0.0450 0.0550 0.0650]m to do the simulation, the unknown distance $d \sim U(0,225)$ m. When $SNR = 0dB$, using the algorithm in [7] and the relationship between the decimal distance and phase measured values we can get that the standard deviation of the remainder error is $\sigma = 16.2626$. Hence, from (20) and (21), we have

$$\begin{aligned} &p\{n_1 = n_2 = 0\} = p\{-r^c < \Delta r_i < M - r^c\} \\ &\bullet p\{-r^c < \Delta r_j < M - r^c\} \end{aligned} \tag{34}$$

Where $r^c = N \bmod M$. Here we take r^c as $r^c = (M-1)/2$ .Using the above parameters, we can calculate that $p\{n_1 = n_2 = 0\} = 0.8816$ .From (33), we have $p\{n_1 = n_2\} > p\{n_1 = n_2 = 0\} = 0.8816$.

Naturally, $SNR > 0dB$. Therefore, the probability when $n_1 = n_2$ is much larger than that when $n_1 \neq n_2$. Here we take $p_1 = 0.8816$, then we can get the conclusion that when $c_i \geq c_j$ which is the same as $q_{i,1} = q_{i,2,j}$, the probability of $\Delta r_i \geq \Delta r_j$ is larger than 91% and similarly, when $c_i < c_j$, which is the same as $q_{i,1} \neq q_{i,2,j}$, the probability of $\Delta r_i < \Delta r_j$ is larger than 91% .

Finally, we can believe that when $q_{i,1} = q_{i,2}$, $\Delta r_i \geq \Delta r_j$ and when $q_{i,1} \neq q_{i,2}$, $\Delta r_i < \Delta r_j$.

Thus, Property 2 is proved.

REFERENCES

[1] F. Akyildiz, I. H. Kasimoglu, "Wireless Sensor and Actor Networks: Research Challenges," Ad Hoc Networks Journal (Elsevier). vol. 2, no. 4, pp. 351-367, October 2004.

[2] G.Li, J.Xu, Y.-N.Peng, and X.-G.Xia. "Moving target location and imaging using dual-speed velocity SAR," IET Radar Sonar Navig. vol.1, no.2, pp. 158-163,2007.

[3] X.-G.Xia and G.-Y.Wang, "Phase Unwrapping and A Robust Chinese Remainder Theorem, " IEEE Signal Processing Letters. vol. 14, no. 4, pp. 247-250,April 2007.

[4] X.-W.Li and X.-G.Xia, " A Fast Chinese Remainder Theorem Based Phase Unwrapping Algorithm," IEEE Signal Processing Letters. vol. 15.,pp.665-668, 2008.

[5] W.-J.Wang and X.-G.Xia, " A Closed_form Robust Chinese Remainder Theorem and Its Performance Analysis," IEEE Transactions On Signal Processing. vol. 58, no. 11, pp. 5655-5666,2010.

[6] Wang C, Yin Q Y, Wang W J. "An efficient ranging method based on Chinese remainder theorem for RIPS measurement, " Sci China Inf Sci, vol. 53, pp. 1233–1241,2010.

[7] Qi G Q, Jia X L. "High-Accuracy Frequency and Phase Estimation of Signal-Tone Based on Phase of DFT," ACTA ELECTRONICA SINICA. vol. 29, no. 9, pp. 1164-1167, 2001.

[8] H. Chen, P. Deng, Y. Xu and X. Li, A Novel Localization Scheme Based on RSS Data for Wireless Sensor Networks, in Proc. APWeb 2006 International Workshop on Sensor Networks, LNCS 3842, pp. 315 – 320, 2006.

[9] H. Chen, P.Huang, M.Martins, H.C.So, and K.Sezaki, Novel centroid localization algorithm for three-dimensional wireless sensor networks, in Proc. 4th International Conference on WirelessCommunications, Networking and Mobile Computing (WiCOM 2008), Oct. 2008, Dalian, China.

[10] Q. Shi, C. He, H. Chen, and L. Jiang, "Distributed Wireless Sensor Network Localization via Sequential Greedy Optimization Algorithm," IEEE Transactions on Signal Processing, vol. 58, no. 6, pp. 3328-3340, Jun. 2010.