International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075, Volume-1 Issue-3, August 2012

Robust Energy-based Target Localization in Wireless Sensor Networks in the Presence of Byzantine Attacks

Zhenxing Luo

Abstract*— This paper presents a robust energy-based target localization method in wireless sensor networks (WSNs) in the presence of Byzantine attacked sensors. Byzantine attacks will cause sensors to send false information to the fusion centre and disturb the target localization method. Therefore, a robust energy-based target localization method is needed to counter the Byzantine attacks and a method is presented in this paper. The method presented in this paper assumes that the fusion centre knows the exact information about the percentage of Byzantine sensors and the attack probability. If the fusion centre does not know the Byzantine attack information, a Byzantine sensor identification scheme can be used to identify Byzantine sensors. Results showed the robust energy-based target localization method could provide better performance results than the energy-based target localizatin method, which did not consider Byzantine attacked sensors. Moreover, simulation results showed that the Byzantine sensor identificaiton scheme could identify most Byzantine attacked sensors.

Index Terms*—Byzantine sensors, Cramer-Rao lower bound, maximum likelihood estimation, *reputation value.

I. INTRODUCTION

Target localization in wireless sensor networks (WSNs) is a classic problem [1-11]. In the energy-based target localization method, sensors measure the signals from the target and send those measurements to the fusion centre using either analog data or quantized data [8]. The fusion centre, which has much more computational capacity, estimates the target position based on the measurements from sensors.

The energy-based target localization method may suffer from several problems in practice. For example, one important problem with the energy-based target localization method is that there may be Byzantine attacks in which intruders manipulate some sensors and cause these sensors to send false information to the fusion centre. The Byzantine attack problem is different from the sensor fault problem in that Byzantine attacks are from outside intruders and sensor fault is mainly due to problems within sensors. Another difference is that all sensors are subject to sensor fault while intruders usually manipulate some sensors in WSNs. The problem of Byzantine attacks in distributed detection was first discussed in [12]. A target localization method with quantized data in the presence of byzantine attacks was presented in [4]. In this method, Byzantine sensors and non-Byzantine sensors employed different thresholds, Byzantine sensors flipped decisions with probability 1, and the probability that a sensor is Byzantine sensor is α. The difference between our robust energy-based target localization method and the method in [4] is that in our method, Byzantine sensors flip decisions with probability p_a, Byzantine sensors and Non-Byzantine sensors employ the same threshold, and the fusion center knows which sensors are Byzantine sensors and which sensors are Non-Byzantine sensors.

To identify Byzantine attacked sensors, a scheme was presented for distributed detection in [13]. In this scheme, after each time step, the fusion centre makes the decision about the presence of the target based on information from the sensors. Then, a reputation value is assigned to each sensor based on how many times the decision made by that sensor is different from final decisions. Over T time steps, the reputation value is updated after each time step. If, after T time steps, the reputation value of a particular sensor is greater than a fixed threshold, this sensor is considered to be a Byzantine sensor. Similar schemes to identify Byzantine sensors have been presented, including trust management in [14], the weighted sequential probability ratio test in [15], and the outlier factor method in [16].

However, no scheme to identify Byzantine attacks has been presented for the energy-based target localization method in WSNs. A scheme to identify Byzantine sensors for the energy-based target localization method will be presented in this paper. This scheme is similar to the Byzantine identification scheme for distributed detection. First, the fusion centre estimates the target location based on the decision vector from the sensors. Then, based on the estimated target location, we calculate the fire probability and non-fire probability for each sensor. Using the fire probability and non-firing probability, the reputation value is calculated. The reputation value for each sensor is updated every time step. After T time steps, the sensors with reputation values below a certain threshold are marked as Byzantine attacked sensors.

The main contribution of this paper is a robust energy-based target localization method, which incorporates the Byzantine attack model into the energy-based target localization method. Although our method is similar to the method in [4], our method is different from the method in [4] because our method assumes the fusion center knows which sensors are Byzantine sensor and which sensors are Non-Byzantine sensors. Moreover, the Cramer-Rao lower bound (CRLB) corresponding to this method is calculated. In addition to this method, a reputation-based method to single out Byzantine sensors is presented. Simulation results showed that the robust energy-based target localization method provided better localization performance than the energy-based target localization method, which did not consider Byzantine attacks. Moreover, the results of the Byzantine sensor identification scheme will be presented.

Section II presents the robust energy-based target localization method in the presence of Byzantine attacks, followed by a scheme to identify Byzantine attacked sensors in Section III.

Manuscript received on August 2012.
Zhenxing Luo, Department of Electrical and Computer Engineering, The University of Alabama at Birmingham, Birmingham, AL, USA.

The simulation setup is discussed in Section IV. Section V presents results and analysis, followed by concluding remarks in Section VI.

II. ROBUST ENERGY-BASED TARGET LOCALIZATION IN THE PRESENCE OF BYZANTINE ATTACKS

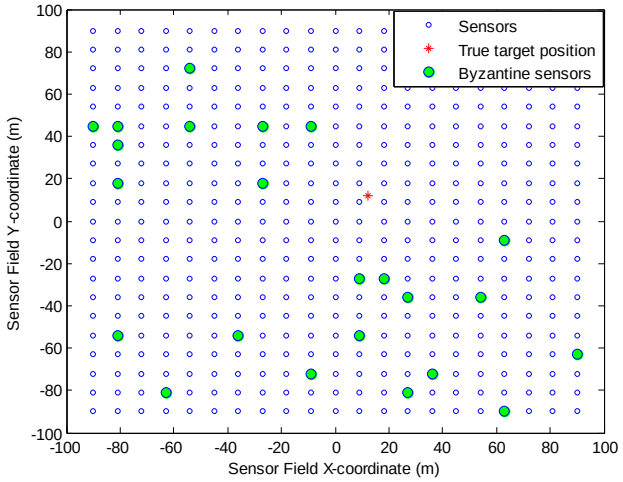

Figure 1: Sensor field with Byzantine sensors and non-Byzantine sensors

A sensor field is shown in Figure 1. Small circles indicate non-Byzantine sensors and big circles indicate Byzantine sensors. Following the derivation in [8], signals received by sensors from a target can be determined by

$$a_i^2 = \frac{G_i P_0^{'}}{\left(d_i / d_0\right)^2}, \tag{1}$$

in which P_0 is the power of the target measured at a reference distance d_0 and G_i is the gain of the ith sensor. The signal received is a function of the distance between the ith sensor at (x_i, y_i) and a target at (x_t, y_t). The distance can be calculated by

$$d_i = \sqrt{(x_i - x_t)^2 + (y_i - y_t)^2}\ . \tag{2}$$

In the paper, the minimum value of d_i is set to 1 in order to avoid numerical problems. The model in (1) can be simplified by assuming that $G_i = 1$ and $d_0 = 1$. Then, model (1) can be presented as

$$a_i^2 = \frac{P_0}{d_i^2}. \tag{3}$$

Because environmental noise will corrupt the signal received by sensors, the signal received at sensor i is

$$s_i = a_i + w_i \tag{4}$$

where w_i is a Gaussian noise with zero mean and variance σ^2.

Usually, sensors are powered by batteries. Therefore, energy is a precious resource for sensors. Moreover, bandwidth is also a scarce resource in WSNs. Therefore, information sent by sensors has to be quantized to save energy and communication bandwidth. The ith sensor quantizes s_i according to

$$m_i = \begin{cases} 0 & -\infty < s_i < \gamma_{i1} \\ 1 & \gamma_{i1} < s_i < \gamma_{i2} \\ \vdots & \vdots \\ L-2 & \gamma_{i(L-2)} < s_i < \gamma_{i(L-1)} \\ L-1 & \gamma_{i(L-1)} < s_i < \infty \end{cases} \tag{5}$$

The probability that m_i takes value m is

$$p(m_i = m|\theta) = Q\left(\frac{\gamma_{il} - a_i}{\sigma}\right) - Q\left(\frac{\gamma_{i(l+1)} - a_i}{\sigma}\right) \quad (0 \le m \le L-1) \tag{6}$$

where $Q(x)$ is defined as

$$Q(x) = \int_x^{\infty} \frac{1}{\sqrt{2\pi}} e^{-\frac{t^2}{2}} dt\ . \tag{7}$$

However, due to the presence of Byzantine attacks, decisions from Byzantine sensors can be artificially manipulated by intruders. The decisions made by sensors can be expressed in two parts: decisions made by Byzantine sensors M_a and decisions made by non-Byzantine sensors M_b. Thus, the decision vector can be expressed as

$$\mathbf{M} = [M_a, M_b]^T = [m_1\ m_2\ ...m_{N_b}\ m_{N_b+1}...\ m_N]^T. \tag{8}$$

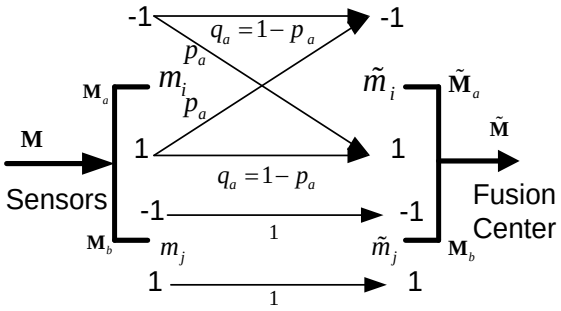

Figure 2: Decision transmission diagram

Because decisions made by Byzantine sensors can be artificially manipulated, the decisions sent by Byzantine sensors will be $\tilde{M}_a$ and decisions sent by non-Byzantine sensors will still be M_b. The decision vector received by the fusion centre is

$$\tilde{\mathbf{M}} = [\tilde{M}_a, M_b]^T = [\tilde{m}_1\ \tilde{m}_2\ ...\tilde{m}_{N_b}\ m_{N_b+1}...\ m_N]^T. \tag{9}$$

The transition relation $p(\tilde{m}_i|m_i)$ between m_i and $\tilde{m}_i$ can be determined by attack probability p_a and non-attack probability q_a.

The fusion centre estimates $\theta = [P_0\ x_t\ y_t]^T$ by maximizing

$$\ln p(\tilde{\mathbf{M}}|\theta) = \prod_{i=1}^{N_b}\left[\sum_{m_i=o}^{L-1} p(\tilde{m}_i|m_i)p(m_i|\theta)\right]\prod_{j=1}^{N-N_b}\left[\sum_{m_j=o}^{L-1} p(m_j|\theta)\right]. \tag{10}$$

The maximum likelihood estimator tries to find the θ value to maximize

$$\hat{\theta} = \max_{\theta} \ln p\left(\tilde{\mathbf{M}}|\theta\right). \tag{11}$$

If an unbiased estimate of θ exists, the Cramer-Rao lower bound (CRLB) can be derived by

$$E\{[\hat{\theta}(\tilde{\mathbf{M}})-\theta][\hat{\theta}(\tilde{\mathbf{M}})-\theta]^T\} \geq \mathbf{J}^{-1} \quad (12)$$

$$\mathbf{J} = -E\left[\nabla_\theta \nabla_\theta^T \ln p\left(\tilde{\mathbf{M}}|\theta\right)\right]. \quad (13)$$

The CRLB matrix can be derived in the following way. First we derive the (1, 1) element of $\mathbf{J}$ matrix:

$$\frac{\partial^2 \ln p\left(\tilde{\mathbf{M}}|\theta\right)}{\partial P_0^2} = \frac{\partial^2 \ln p\left(\tilde{M}_a, M_b|\theta\right)}{\partial P_0^2}$$

$$= \sum_i \sum_l \left[-\frac{\delta(\tilde{m}_i - l)}{p^2(\tilde{m}_i|\theta)} \left[\frac{\partial \ln p(\tilde{m}_i|\theta)}{\partial P_0}\right]^2 + \frac{\delta(\tilde{m}_i - l)}{p(\tilde{m}_i|\theta)} \frac{\partial^2 p(\tilde{m}_i|\theta)}{\partial P_0^2} \right]. \quad (14)$$

$$+ \sum_j \sum_l \left[-\frac{\delta(m_j - l)}{p^2(m_j|\theta)} \left[\frac{\partial \ln p(m_j|\theta)}{\partial P_0}\right]^2 + \frac{\delta(m_j - l)}{p(m_j|\theta)} \frac{\partial^2 p(m_j|\theta)}{\partial P_0^2} \right]$$

Because the expectation of the second term and the fourth term of (14) is 0, the expectation of (14) is

$$E\left[\frac{\partial^2 \ln p\left(\tilde{\mathbf{M}}|\theta\right)}{\partial P_0^2}\right] =$$

$$\sum_i \sum_l -\frac{1}{p^2(\tilde{m}_i|\theta)} \left[\frac{\partial \ln p(\tilde{m}_i|\theta)}{\partial P_0}\right]^2 \quad . \quad (15)$$

$$+ \sum_j \sum_l \left[-\frac{\delta(m_j - l)}{p^2(m_j|\theta)} \left[\frac{\partial \ln p(m_j|\theta)}{\partial P_0}\right]^2 \right]$$

In (15), $p(\tilde{m}_i|\theta)$ is defined in (10).

The derivative of $p(\tilde{m}_i|\theta)$ with respect to P_0 is

$$\frac{\partial p(\tilde{m}_i|\theta)}{\partial P_0} = \sum_{m_i=0}^{L-1} p(\tilde{m}_i|m_i) \frac{\partial p(m_i|\theta)}{\partial P_0}. \quad (16)$$

In (20), $\frac{\partial p(m_i|\theta)}{\partial P_0}$ can be obtained as

$$\frac{\partial p(m_i|\theta)}{\partial P_0} = \frac{\partial}{\partial P_0}\left[Q\left(\frac{\gamma_{il} - a_i}{\sigma}\right) - Q\left(\frac{\gamma_{i(l+1)} - a_i}{\sigma}\right)\right]$$

$$= \frac{d_i^{-\frac{n}{2}}}{2\sqrt{2\pi}\sigma_n\sqrt{P_0}} \left[e^{-\frac{-(\gamma_{il}-a_i)^2}{2\sigma_n^2}} - e^{-\frac{-(\gamma_{i(l+1)}-a_i)^2}{2\sigma_n^2}} \right] \quad (17)$$

The derivative of $p(m_j|\theta)$ with respect to P_0 is

$$\frac{\partial p(m_j|\theta)}{\partial P_0} = \frac{\partial}{\partial P_0}\left[Q\left(\frac{\gamma_{jl} - a_j}{\sigma}\right) - Q\left(\frac{\gamma_{j(l+1)} - a_j}{\sigma}\right)\right]$$

$$= \frac{d_j^{-\frac{n}{2}}}{2\sqrt{2\pi}\sigma_n\sqrt{P_0}} \left[e^{-\frac{-(\gamma_{jl}-a_i)^2}{2\sigma_n^2}} - e^{-\frac{-(\gamma_{j(l+1)}-a_j)^2}{2\sigma_n^2}} \right] \quad (18)$$

Other elements of $\mathbf{J}$ matrix can be derived similarly.

III. A SCHEME TO IDENTIFY BYZANTINE ATTACKED SENSORS

The presence of Byzantine sensors will degrade the localization performance. Even if the fusion centre has exact information about which sensor is a Byzantine attacked sensor and the attack probability of the Byzantine attacked sensor, the localization performance will still suffer. Therefore, a scheme to identify Byzantine attacked sensors is needed. We present a scheme to indentify Byzantine attacked sensors, and the detailed steps of this scheme are listed here.

1. Using the available decision vector $\mathbf{M} = [M_a, M_b]^T$ to estimate the target location
2. Calculate distance d_i between sensor i and the estimated target location for all sensors
2. Set the initial Reputation values of all sensors to 1
3. For T time steps
   For each sensor i
   If the decision of sensor i is 1
   The reputation value of sensor i = the reputation value of sensor $i + \int_{\gamma - \frac{\sqrt{P_0}}{d_i}}^{\infty} \frac{1}{\sqrt{2\pi}} e^{-\frac{t^2}{2}} dt$
   End if
   If the decision of sensor i is -1
   The Reputation value of sensor i = the reputation value of sensor $i + 1 - \int_{\gamma - \frac{\sqrt{P_0}}{d_i}}^{\infty} \frac{1}{\sqrt{2\pi}} e^{-\frac{t^2}{2}} dt$
   End if
   End for each sensor
   End for T time steps
4. If the reputation value of sensor i <0.5
   Sensor i is a Byzantine sensor
   end

IV. SIMULATION SETUP

To verify the robust energy-based target localization method, the RMS errors given by this method will be compared with the CRLB. We used the sensor layout shown in Figure 1 and binary decisions. To show the effect of the percentage of Byzantine attacked sensors on localization performance, we set (x_t, y_t)=(12, 13) , $P_0 = 10,000$, and $\gamma_1 = 4$ for all sensors. The RMS errors were calculated based on 1000 Monte Carlo simulations. The attack probability P_a was set to 0.2 and the percentage of Byzantine sensors was varied from 0 to 0.2 in Figure 3.

To show the effect of the attack probability on localization performance, we set (x_t, y_t)=(12, 13) , $P_0 = 10,000$, and $\gamma = 4$ for all sensors. The percentage of Byzantine sensors was 0.5 and the attack probability P_a was varied from 0 to 0.4. The results are shown in Figure 4.

To show the effect of the Byzantine sensor identification scheme, we set (x_t, y_t)=(12, 13) , $P_0 = 10,000$, and $\gamma = 4$ for all sensors. The percentage of Byzantine sensors was 0.5 and the attack probability P_a was 0.4. The threshold of the reputation value used to identify Byzantine sensors was set to 0.4. The results are shown in Figure 5.

V. RESULTS AND ANALYSIS

The RMS errors given by the robust energy-based target localization method were compared with the CRLB (Figure 3). The RMS errors were close to the CRLB (Figure 3). It is also clear that the RMS errors increased as the percentage of Byzantine sensors increased (Figure 3).

Similarly, when the attack probability was varied, the RMS errors were also close to the CRLB (Figure 4). The RMS errors increased as the attack probability increased (Figure 4).

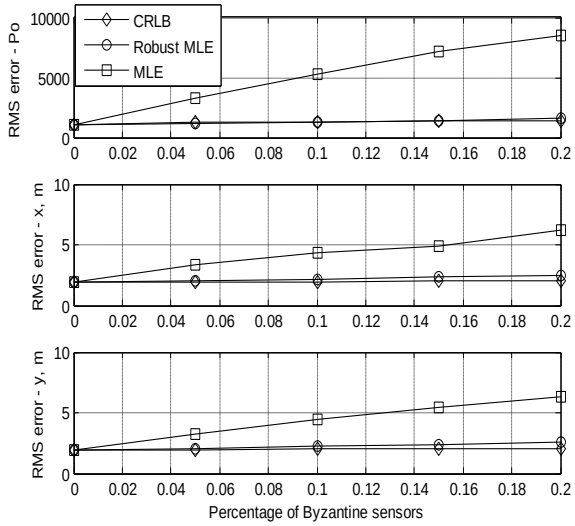

Figure 3: RMS estimation errors and the CRLB as functions of the percentage of Byzantine sensors

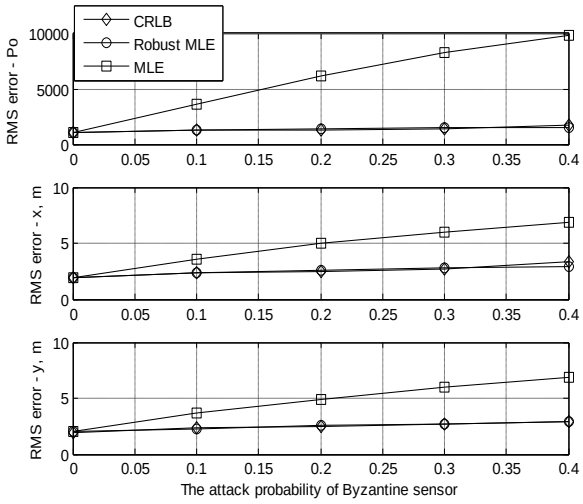

Figure 4: RMS estimation errors and the CRLB as functions of the attack probability

The results of the Byzantine sensor identificaiton scheme are shown in Figure 5. By comparing Figure 1 with Figure 5, we can see that under the setup specified in Section IV, the scheme can identify most Byzantine sensors.

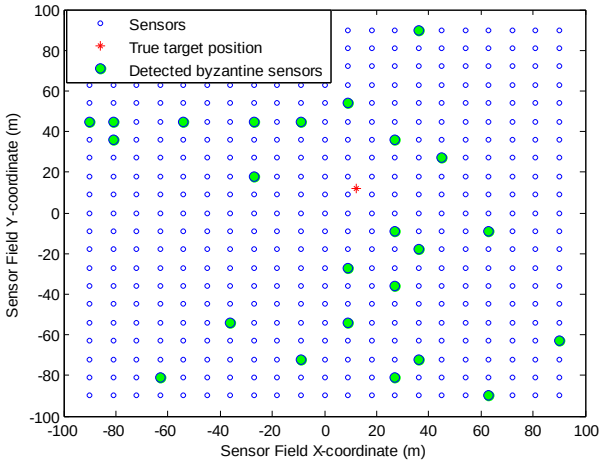

Figure 5: Results of the Byzantine sensor identificaiton scheme

VI. CONCLUSION

In this paper, a robust energy-based target localization method was presented. Simulation results showed that the RMS errors given by this method were close to the CRLB. Moreover, a Byzantine sensor identification scheme was presented in this paper. Simulation results showed that this scheme could identify most Byzantine sensors. In practice, if the fusion centre knows the exact percentage of Byzantine sensors and the attack probability, the fusion centre can improve the localization performance by including the information into the energy-based target localization method. If the fusion centre does not know this information, the fusion centre can use the Byzantine sensor identification scheme to remove the Byzantine sensors.

REFERENCES

1. D. Li, K. D. Wong, Y.H.Hu, and A. N. Sayeed, "Detection, Classification, and Tracking of Targets", *IEEE Signal Processing Magazine*, vol.19, no. 3, pp. 17-29, Mar. 2002.
2. Z. X. Luo and T. C. Jannett, "Optimal Threshold for Locating Targets within a Surveillance Region Using a Binary Sensor Network", in *Proceedings of the International Joint Conferences on Computer, Information, and Systems Sciences, and Engineering* (CISSE 09), Dec. 2009.
3. Z. X. Luo, "A censoring and quantization scheme for energy-based target localization in wireless sensor networks", To appear in *Journal of Engineering and Technology*.
4. K. Agrawal, A. Vempaty, C. Hao, and P. K. Varshney, "Target localization in Wireless Sensor Networks with quantized data in the presence of Byzantine attacks," *2011 Conference Record of the Forty Fifth Asilomar Conference on Signals, Systems and Computers* (ASILOMAR), vol., no., pp.1669-1673, 6-9 Nov. 2011
5. Z. X. Luo and T. C. Jannett, "Performance Comparison between Maximum Likelihood and Heuristic Weighted Average Estimation Methods for Energy-Based Target Localization in Wireless Sensor Networks", in *Proceedings of the 2012 IEEE Southeastcon*, Orlando, FL, Mar. 2012, in press.
6. Z. X. Luo and T. C. Jannett, "Modelling Sensor Position Uncertainty for Robust Target Localization in Wireless Sensor Networks", in *Proceedings of the 2012 IEEE Radio and Wireless Symposium*, Santa Clara, CA, Jan. 2012.
7. Z. X. Luo and T. C. Jannett, "Energy-Based Target Localization in Multi-Hop Wireless Sensor Networks", in *Proceedings of the 2012 IEEE Radio and Wireless Symposium*, Santa Clara, CA, Jan. 2012.
8. R. X. Niu and P. K. Varshney, "Target Location Estimation in Sensor Networks with Quantized Data", *IEEE Transactions on Signal Processing*, vol. 54, pp. 4519-4528, Dec. 2006.

9. Z. X. Luo and T. C. Jannett, “A Multi-Objective Method to Balance Energy Consumption and Performance for Energy-Based Target Localization in Wireless Sensor Networks”, in *Proceedings of the 2012 IEEE Southeastcon*, Orlando, FL, Mar. 2012, in press.
10. M. P. Michaelides and C. G. Panayiotou, "Fault tolerant maximum likelihood event localization in sensor networks using binary data," *IEEE Trans. Signal Process*., vol. 16, no. 5, pp. 406-409, May 2009.
11. M. P. Michaelides and C. G. Panayiotou, "SNAP: Fault tolerant event location estimation in sensor networks using binary data," *IEEE Trans. Comput.*, vol. 58, no. 9, pp. 1185-1197, Sept. 2009.
12. S. Marano, V. Matta, and Lang Tong, "Distributed Detection in the Presence of Byzantine Attacks", *IEEE Transactions on Signal Processing*, vol.57, no.1, pp.16-29, Jan. 2009
13. A.S. Rawat, P. Anand, H. Chen, and P.K. Varshney , "Collaborative Spectrum Sensing in the Presence of Byzantine Attacks in Cognitive Radio Networks", *IEEE Transactions on Signal Processing*, vol.59, no.2, pp.774-786, Feb. 2011.
14. K. Guan, L. Gharai, S. Dehnie, R. Ghanadan, and S. Kumar, “Trust management for distributed decision fusion in sensor networks,” in *Proc. of the 12th International Conference on Information Fusion Fusion*, 2009.
15. R. Chen, J. M. Park, and K. G. Bian, “Robust distributed spectrum sensing in cognitive radio networks”, in *Proc. IEEE INFOCOM*, 2008, pp. 1876–1884.
16. P. Kaligineedi, M. Khabbazian, and V. K. Bhargava, "Malicious User Detection in a Cognitive Radio Cooperative Sensing System", *IEEE Transactions on Wireless Communications*, vol. 9, pp. 2488-2497, 2010.