Anti-attack and Channel Aware Target Localization in Wireless Sensor Networks Deployed in Hostile Environments

Zhenxing Luo

Abstract—This paper discusses the attack and communication channel problems of the energy-based target localization method in wireless sensor network. An anti-attack and channel aware (AACA) target localization method is presented to address the attack problem and the problem of communication channel errors at the same time. Particularly, the AACA method proposed in this paper focuses on the Rayleigh fading channel with coherent receiver. Moreover, the AACA method was compared with the weighted average (WA) method under attack and communication channel errors. Results showed that the root mean square (RMS) errors presented by the AACA method were close to the CRLB. Moreover, the WA method, although not able to provide as good performance as the AACA method, could give results in much shorter time.

Index Terms—Cramer-Rao lower bound, Target localization, Wireless sensor networks

I. INTRODUCTION

Advances in hardware and software have enabled wireless sensor networks (WSNs) to be applied in many areas [1-6]. The basic structure of a WSN is a fusion center and a large number of cheap sensors deployed in the sensor field during the sensor layout process [7]. This paper will focus on the target localization problem in WSNs, in which the fusion centre estimates target position based on the information from sensors.

An energy-based maximum likelihood estimation (MLE) method for target localization was presented in [7]. The MLE method is easy to implement compared with the time-delay of arrival (TDOA) method because the MLE method does not require synchronization among sensors [7]. However, there are a few potential problems with the MLE method. First, the MLE method in [7] does not consider communication channel errors between sensors and the fusion centre. To address the problem caused by communication channel errors, the authors in [8] presented a channel aware MLE method in which communication channel models are incorporated into the MLE framework. Moreover, the channel aware MLE method was furthered by a multi-hop channel aware MLE method in [9]. The second problem of the MLE method is sensor fault. One method was presented in [14] to address the sensor fault and communication channel problem at the same time. The method in [14] considered binary symmetric channel (BSC) and Rayleigh fading channel with non-coherent receiver. The third problem of the MLE method in [7] is that it is prone to outsider attacks. If sensors are attacked by intruders, intruders can flip flop sensor decisions to foil the fusion centre [10][11]. Byzantine attacks in cognitive radio networks and in distributed detection were discussed in [10] and [11] respectively. If the attack problem is not taken into account by the fusion centre, the estimation performance will suffer. A robust energy-based target localization method was presented in [13] to address the Byzantine attack problem. In this paper, we will consider the Byzantine attack problem in together with the communication channel errors for the energy-based MLE target localization method. Our solution to both problems is an anti-attack and channel aware (AACA) method to address both the attack problem and the problem of communication channel errors simultaneously. The AACA method is similar to the method presented in [14]. However, the AACA method presented in this paper only considers Rayleigh fading channels with coherent receiver.

The main contribution of this paper is the use of the AACA method to counter both the sensor attack and communication channel errors at the same time. Furthermore, the AACA method is compared with the weighted average (WA) method in the context of Rayleigh communication channel with coherent receiver and hard decoder. Simulation results showed that the AACA method achieved performance close to the Cramer-Rao lower bound (CRLB). If the Rayleigh channel with coherent receiver and hard decoder is used, the AACA algorithm performed better than the weighted average (WA) method. However, the execution time of the AACA method was much longer than the WA method.

Section II presents the energy-based AACA MLE target localization method, followed by the heuristic WA method in Section III. In Section IV, we discuss the Rayleigh channel with coherent receiver and hard decoder. The simulation setup is discussed in Section V. Results and analysis are given in Section VI. Concluding remarks are provided in Section VII.

II. ENERGY-BASED ANTI-ATTACK AND CHANNEL AWARE MLE TARGET LOCALIZATION METHOD

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

Retrieval Number: F0606071612/201208BEIESP
The probability that sensor is $m_i$, however, due to attack, the decision $\tilde{m}_i$ is transmitted to the fusion centre through the Rayleigh fading channel. The relation between $m_i$ and $\tilde{m}_i$ is defined by the attack model, which is determined by the attack probability $p_a$. The attack model can be expressed as:

$$p(m_i = 0 | m_i = 0) = 1 - p_a$$

$$p(m_i = 1 | m_i = 0) = p_a$$

$$p(m_i = 0 | m_i = 1) = p_a$$

$$p(m_i = 1 | m_i = 1) = 1 - p_a$$

The decision received at the fusion centre is denoted by $\tilde{m}_i$. The values of $m_i$, $\tilde{m}_i$ and $\bar{m}_i$ can be either 1 or -1. The transition probability between $m_i$ and $\tilde{m}_i$ is defined by $p(\tilde{m}_i | m_i)$ and the transition probability of communication channel is defined by $p(\tilde{m}_i | \bar{m}_i)$.

In this paper, the communication channel is the Rayleigh fading channel. If coherent receiver and soft decoder are used, $p(\tilde{m}_i | \bar{m}_i)$ can be expressed as [8]

$$p(\tilde{m}_i | \bar{m}_i) = \frac{2\alpha}{\sqrt{2\pi(1 + 2\alpha^2)}}
\times
\frac{e^{-\frac{(\bar{m}_i - m_i)^2}{2(1 + 2\alpha^2)}}}{\sqrt{1 + \bar{m}_i^2} e^{-\frac{(\bar{m}_i - m_i)^2}{2(1 + 2\alpha^2)}}} Q(-\alpha \bar{m}_i)$$

The decision vector $\tilde{M} = [\tilde{m}_1, \tilde{m}_2, ..., \tilde{m}_n]^T$ received at the fusion centre, the fusion centre estimates $\theta = [P_x, P_y]^T$ by finding the $\theta$ value to maximize

$$Q(x) = \int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi}} e^{-\frac{x^2}{2}} \, dx$$

The decision made by the $i$th sensor is $m_i$. However, due to attack, the decision $\tilde{m}_i$ is transmitted to the fusion centre through the Rayleigh fading channel. The relation between $m_i$ and $\tilde{m}_i$ is defined by the attack model, which is determined by the attack probability $p_a$. The attack model can be expressed as:

$$p(m_i = 0 | m_i = 0) = 1 - p_a$$

$$p(m_i = 1 | m_i = 0) = p_a$$

$$p(m_i = 0 | m_i = 1) = p_a$$

$$p(m_i = 1 | m_i = 1) = 1 - p_a$$

The decision received at the fusion centre is denoted by $\tilde{m}_i$. The values of $m_i$, $\tilde{m}_i$ and $\bar{m}_i$ can be either 1 or -1. The transition probability between $m_i$ and $\tilde{m}_i$ is defined by $p(\tilde{m}_i | m_i)$ and the transition probability of communication channel is defined by $p(\tilde{m}_i | \bar{m}_i)$.

In this paper, the communication channel is the Rayleigh fading channel. If coherent receiver and soft decoder are used, $p(\tilde{m}_i | \bar{m}_i)$ can be expressed as [8]

$$p(\tilde{m}_i | \bar{m}_i) = \frac{2\alpha}{\sqrt{2\pi(1 + 2\alpha^2)}}
\times
\frac{e^{-\frac{(\bar{m}_i - m_i)^2}{2(1 + 2\alpha^2)}}}{\sqrt{1 + \bar{m}_i^2} e^{-\frac{(\bar{m}_i - m_i)^2}{2(1 + 2\alpha^2)}}} Q(-\alpha \bar{m}_i)$$

in which $\alpha$ is

$$\alpha = \frac{1}{\sigma} \sqrt{1 + 2\alpha^2}$$

If the decision vector $\tilde{M} = [\tilde{m}_1, \tilde{m}_2, ..., \tilde{m}_n]^T$ received at the fusion centre, the fusion centre estimates $\theta = [P_x, P_y]^T$ by finding the $\theta$ value to maximize
\[ \ln p(\mathbf{M}|\theta) = \sum_{i=1}^{N} \ln \left[ \sum_{s_{i} \in \{-1,1\}} \sum_{m_{i} \in \{-1,1\}} \rho(\tilde{m}_{i}, m_{i}, \rho(\tilde{m}_{i}, m_{i})) \right]. \quad (16) \]

The process is expressed as
\[ \hat{\theta} = \max_{\theta} \ln p(\mathbf{M}|\theta). \quad (17) \]

For an unbiased estimate of \( \theta \), the Cramer-Rao lower bound (CRLB) can be derived by
\[ E[\{\hat{\theta}(\mathbf{M}) - \theta\}^T (\hat{\theta}(\mathbf{M}) - \theta)] \geq \mathbf{J}^{-1} \]
\[ \mathbf{J} = -E\left[ \nabla_{\theta} \ln p(\mathbf{M}|\theta) \right]. \quad (19) \]

The derivation of the CRLB matrix is presented in Appendix.

### III. HEURISTIC WA ESTIMATION METHOD

Another method to estimate target location is the WA estimation method presented in [7][12]. The calculation of the WA method can be expressed as [7][12]
\[ \psi_i = \frac{\sum_{\tilde{m}_i} \psi_{i}}{\sum_{\tilde{m}_i}}. \quad (20) \]

In (20), the location of the \( i \)th sensor is \( \psi_i \) and the estimate of the target position is \( \psi \). If the decision \( \tilde{m}_i \) received by fusion centre from the \( i \)th sensor is 0, the decision will not be included to (20). If the decision \( \tilde{m}_i \) received by fusion centre from the \( i \)th sensor is 1, the \( \tilde{m}_i \psi_i \) value is added to the numerator of (20) and the decision \( \tilde{m}_i \) is added to the denominator of (20). The attack information or any information about the communication channels between sensors and the fusion centre is not used in the WA method.

### IV. RAYLEIGH CHANNEL WITH COHERENT RECEIVER AND HARD DECODER

The Rayleigh fading channel with soft receiver and hard decoder can be converted to a BSC model if the transmission signals are binary phase-shift keying (BPSK) signals [8][12]. The error probability \( P_e \) can be derived from channel SNR [8][12]
\[ P_e = \frac{1}{2} (1 - \frac{\sqrt{\text{SNR}}}{\sqrt{1 + \text{SNR}}}). \quad (17) \]

Therefore, if a coherent receiver and hard decoder are used, the Rayleigh channel is equal to a BSC and the crossover probability of the BSC can be determined by (21). We will use the attack model in conjunction with the Rayleigh channel with coherent receiver and hard decoder to compare the AACA method with the WA method.

### V. SIMULATION SETUP

To compare the AACA method with the CRLB, we use the Rayleigh fading channel with coherent receiver and soft decoder in conjunction with the attack model. We use 1000 Monte Carlo runs and set \( (x, y) = (12, 13) \), \( p_a = 0.01 \), \( P_0 = 10000 \), and \( \gamma' = 5 \) for all sensors. In all other simulations, we set \( \gamma' = 4 \) for all sensors, \( (x, y) = (12, 13) \), \( p_a = 0.01 \) and \( P_0 = 10000 \). All simulations involving computation times were run using a Pentium-4 computer. Results of simulation times were based on 100 runs.

### VI. RESULTS AND ANALYSIS

Because the MLE estimator is unbiased, we use RMS estimation errors as an estimation performance criterion. For the Rayleigh channel with coherent receiver and soft decoder in conjunction with the attack model as shown in Fig. 2, the RMS errors given by the AACA method were close to the CRLB (Fig. 3). As the SNR value of communication channel increased, the RMS errors become lower due to improved communication channel condition (Fig. 3).
Anti-attack and Channel Aware Target Localization in Wireless Sensor Networks Deployed in Hostile Environments

![Graph showing RMS estimation errors](image)

**Figure 4.** RMS estimation errors (solid line: AACA method, solid line+star: WA method, solid line+circle: CRLB of AACA method, solid line+square: the MLE method) Hard decoder

Table I. Computation times for aaca mle method, the mle method, and wa method (rayleigh channel with coherent receiver and hard decoder, 100 runs)

<table>
<thead>
<tr>
<th>Time (seconds)</th>
<th>SNR (dB)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0</td>
</tr>
<tr>
<td>channel aware</td>
<td>2768.409</td>
</tr>
<tr>
<td>channel unaware</td>
<td>2148.551</td>
</tr>
<tr>
<td>WA</td>
<td>5.2200</td>
</tr>
</tbody>
</table>

**VII. CONCLUSION**

In this paper, an AACA method was presented to address the attack problem and the problem of communication channel errors at the same time. Results showed that the AACA method could provide results close to the CRLB. In practice, both attack and communication channel errors are common. The AACA algorithm can effectively address both problems.

**APPENDIX**

The CRLB is given by:

\[ E(\hat{\theta}|\theta) = \mathcal{J}^{-1} \]

As we know, the Fisher information matrix (FIM) can be obtained as

\[ \mathcal{J} = -E[\nabla_\theta \nabla_\theta^T \ln p(\Theta|\theta)] \]

First we derive the (1,1) element of J matrix. According to (9), we have

\[ \frac{\partial \ln p(M|\theta)}{\partial \theta} = \sum_{i=1}^{N} \frac{1}{p(m_i|\theta)} \frac{\partial p(m_i|\theta)}{\partial \theta} \]

\[ \frac{\partial^2 \ln p(M|\theta)}{\partial \theta^2} = \sum_{i=1}^{N} \frac{1}{p^2(m_i|\theta)} \left[ \frac{\partial^2 p(m_i|\theta)}{\partial \theta^2} \right] + \frac{1}{p(m_i|\theta)} \frac{\partial^2 p(m_i|\theta)}{\partial \theta^2} \]

The expectation of (25) is

\[ E\left[ \frac{\partial^2 \ln p(M|\theta)}{\partial \theta^2} \right] = \sum_{i=1}^{N} \int_{0}^{\infty} \Delta_i d\theta_i \]

In (26), \( \Delta_i \) is defined as

\[ \Delta_i = \frac{1}{p^2(m_i|\theta)} \left[ \frac{\partial^2 p(m_i|\theta)}{\partial \theta^2} \right] - \frac{1}{p(m_i|\theta)} \frac{\partial^2 p(m_i|\theta)}{\partial \theta^2} \]

Because \( \int_{-\infty}^{\infty} \left( \frac{1}{p(m_i|\theta)} \frac{\partial^2 p(m_i|\theta)}{\partial \theta^2} \right) d\theta_i = 0 \), we have

\[ E\left[ \frac{\partial^2 \ln p(M|\theta)}{\partial \theta^2} \right] = \sum_{i=1}^{N} \int_{-\infty}^{\infty} \frac{1}{p(m_i|\theta)} \frac{\partial^2 p(m_i|\theta)}{\partial \theta^2} d\theta_i \]

In (28), \( p(m_i|\theta) \) is provided by (16), and \( \frac{\partial p(m_i|\theta)}{\partial \theta} \) is defined by

\[ \frac{\partial p(m_i|\theta)}{\partial \theta} = \sum_{m_j \in \{-1,1\}} \sum_{m_l \in \{-1,1\}} p(m_j|m_i)p(m_l|m_i) \frac{\partial p(m_l|m_i)}{\partial \theta} \]

We have

\[ \mathcal{J} = \sum_{m_j \in \{-1,1\}} \sum_{m_l \in \{-1,1\}} \frac{\partial \ln p(M|\theta)}{\partial \theta} \int_{-\infty}^{\infty} p(m_j|m_i)p(m_l|m_i) d\theta_i \]

and then \( \frac{\partial p(m_i|\theta)}{\partial \theta} \) can be expressed as

\[ \frac{\partial p(m_i|\theta)}{\partial \theta} = \frac{\partial}{\partial \theta} \left[ \frac{Q(\eta_i - a_i)}{\sigma} - \frac{Q(\eta_i + a_i)}{\sigma} \right] = \frac{1}{2\sqrt{2\pi}\sigma} \left( e^{-\frac{(\eta_i - a_i)^2}{2\sigma^2}} - e^{-\frac{(\eta_i + a_i)^2}{2\sigma^2}} \right) \]

Then, (29) can be expressed as

\[ \frac{\partial \ln p(M|\theta)}{\partial \theta} = \sum_{m_j \in \{-1,1\}} \sum_{m_l \in \{-1,1\}} \frac{\partial \ln p(M|\theta)}{\partial \theta} \int_{-\infty}^{\infty} p(m_j|m_i)p(m_l|m_i) d\theta_i \]

In (32), \( \Delta_2 \) is defined as

\[ \Delta_2 = \frac{1}{2\sqrt{2\pi}\sigma} \left( e^{-\frac{(\eta_i - a_i)^2}{2\sigma^2}} - e^{-\frac{(\eta_i + a_i)^2}{2\sigma^2}} \right) \]

Take (32) and (16) into (28), we can have the final form of (26). In (32), \( p(m_i|m_j) \) is defined in (9)-(12) and \( p(m_i|m_l) \) is defined in (14). Other elements of J matrix can be derived similarly.

**REFERENCES**


**Published By:**
Blue Eyes Intelligence Engineering & Sciences Publication

**Retrieval Number:** F0606071612/201206BEIESP


