This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE INFOCOM 2007 proceedings.

A Localization-Based Anti-Sensor Network System

Zhimin Yang†, Eylem Ekici‡, and Dong Xuan†
†Department of Computer Science and Engineering
‡Department of Electrical and Computer Engineering
The Ohio State University, Columbus, OH 43210
Email: {yangz, xuan}@cse.ohio-state.edu, ekici@ece.osu.edu

***Abstract*—In this paper, an anti-sensor network system is proposed, aiming to protect an important area from being under surveillance by an adversary's sensor nodes. The major components of the system are a set of observing points (monitors) deployed in the area of importance. The observers try to localize sensor positions using antenna arrays to measure direction of arrival (DoA) and received signal strength of the signals emitted by sensors. Once sensors are localized, additional measures are taken to physically remove or disable localized sensors. The proposed anti-sensor network system is designed to handle additional counter-measures that can be employed by sensors, including message encryption and non-uniform transmission power levels. The simulation results show the effectiveness of the proposed system and effects of counter-measures on sensor localization performance.**

I. Introduction

Wireless Sensor Networks (WSNs) have been envisioned to deliver in-situ observations from inaccessible and inhospitable areas [1]. The majority of existing WSN applications are security related applications where sensor nodes detect and report intruders and other events that my pose a threat to a given asset. A logical consequence of such deployment scenarios is the use of a counter-acting system to prevent sensor networks from fulfilling their missions. Such counter-acting systems would be deployed by the owners and operators of a (potentially) target asset.

In this paper, we introduce the concept of the *anti-sensor network system* which aims to prevent the operation of a sensor network in a given area. The basic idea behind our proposed anti-sensor network system is using the observation of the sensor communication activity to find sensor node locations. We envision a set of fixed observer nodes, referred to as *monitors*, intercepting the communication of wireless sensor nodes. Based on the observations of communication events at multiple monitors, the system tries to find the location of the sensor nodes in the area to be protected. Monitors estimate the distance to the signal source using received signal strength, and the direction of arrival (DoA) using their antenna arrays. Once sensor locations are determined, additional measures are taken to physically remove or disable localized sensors.

We also envision that sensor nodes trying to avoid being detected by the anti-sensor network system. Two counter-measures that can be used by sensors are the *encryption* of transmitted information to hide their IDs, and the *variation of transmission power* to make RSS-based distance estimations unreliable. The counter-acting functions and measures of the two systems create a challenging environment for the sensor network to maintain its presence, and for the anti-sensor network system to localize adversary sensor nodes. The localization procedures proposed in this work go beyond the standard localization methods presented in the past. Since the signal sources are hidden due to encryption, the use of multiple samples from the same source depends on the correct mapping of received signals to their actual sources. We propose a localization algorithm to accomplish this mapping and to improve the localization performance.

To the best of our knowledge, the proposed anti-sensor network is unique in that it aims to protect a given asset against sensor network-based observations. There are many potential application areas of an anti-sensor network system, ranging from protection of sensitive civilian infrastructures such as airports to the obvious military applications. The proposed anti-sensor network architecture primarily depends on processing the received signals at observation points. While the core of the proposed methods partially overlaps with the sensor localization work reported earlier [2], [3], a non-cooperative/hostile set of signal sources has not been considered in the past. To mitigate the problems arising from the non-cooperative nature of the signal sources and detectors, we design robust and resilient algorithms for location detection and signal correlation. Another important property of our proposed work is that it allows for graceful degradation of the system performance under these adverse conditions.

II. Related Work

Localization in WSNs have been studied extensively in the past to determine the locations of sensor nodes [4]. Many localization systems rely on a smaller number of higher capability landmark nodes equipped with GPS devices that emit beacons for other sensor nodes to determine their locations. The resulting solutions, referred to as *measurement-based methods*, estimate distance and/or direction of arrival of beacon signals to determine sensor locations. The distance information can be obtained through time of arrival, time difference of arrival, or received signal strength measurements. To determine the position of a sensor node in a two-dimensional coordinate system, at least three measurements from non-collinear reference points are needed. Examples of such localization methods include Cricket [3], AhLOS [5], APS [2] and, RADAR [6]. *Connectivity-based techniques* only use proximity information to derive the location of sensors.

0743-166X/07/$25.00 ©2007 IEEE

Sensor nodes only know what nodes are nearby through ordinary message exchanges, but not how far away these neighbors are or in what direction they lie. These methods, often also called range-free techniques, compute sensor locations iteratively. Examples of connectivity-based techniques include centroid algorithm [7], DV-HOP [8], MDSMAP [9], and APIT [10]. Although these and other localization methods only consider the positioning in a cooperative (or at least non-hostile) situation, these methods inspire us to solve our new problem.

III. The Anti-Sensor Network Architecture

The primary aim of an anti-sensor network is to protect a given observation area from being monitored by sensor nodes. To this end, an anti-sensor network must *identify the presence and the location of possible sensors in an observation area in a fast and accurate manner*. The general operation scenario can be regarded as a clash of two opposing systems: Sensors try to observe a protected area and collect information from the field, and the anti-sensor network tries to prevent sensors from doing so. At the same time, sensors use counter-measures to avoid (or at least delay) being detected. As in any adversarial interaction, opposing systems may utilize multiple measures and counter-measures. Within the scope of this study, we consider and analyze two easily implementable yet effective counter-measures as outlined in Section III-B.

A. System Description

The anti-sensor network is comprised of a number of fixed monitors located at known positions. We assume that the monitors do not have any resource constraints in terms of energy and processing power, and are capable of receiving messages transmitted by any potential sensor in their observation area. Monitors are also capable of communicating among themselves using separate frequencies over dedicated channels. Hence, any information collected at any monitor can be shared with other monitors reliably and at very low delays. The sensor network, on the other hand, is composed of an unknown number of sensor nodes equipped with wireless communication interfaces. Sensors are located at unknown locations in an area observed by the anti-sensor network. Although limited in power resources, sensor nodes are assumed to be able to perform basic message encryption and perform other elementary computational operations.

Monitors detect sensor locations based on the communication activity of sensors. We assume that monitors can detect and receive signals from all sensor nodes in the observation area. The observations are converted to two basic estimations, namely, distance to signal source, and the Direction of Arrival (DoA). Monitors rely on received signal strength (RSS) to estimate the distance to the signal source [6], [11]. It is also assumed that monitors are equipped with antenna arrays used to estimate the DoA of signals [12]. These estimations inherently contain errors. Through collaborative processing of individual observations, the resulting error in location estimation is minimized. Throughout the paper, we assume that the distance and DoA estimation errors have zero means.

B. Sensor Counter-Measures

To counter the detection efforts of monitors, sensors may launch counter-measures. In this work, we consider two simple yet effective counter-measures: Message encryption and location camouflaging through transmission power changes. The resulting scenarios are outlined in the following. The details of monitor actions under these scenarios are outlined in Section IV.

1) Message Encryption: Sensors try to avoid being detected by encrypting their messages. Message encryption prevents the monitors from identifying message sources directly as no explicitly ID can be extracted from the transmitted message. However, it is still possible to classify an encrypted message received by multiple monitors as belonging to the same source. For this purpose, we utilize the reception time stamps at the monitors and the encrypted bit sequence.

2) Power Level Variation: In addition to message encryption, sensors can also try to hide their location through transmission power variation. This additional defense on sensors' side involves transmission of encrypted data packets at various transmission powers. The direct consequence of this measure is that the received signal strength cannot be used to estimate the distance to the signal source. Hence, sensor location estimation needs to be performed only based on the DoA estimation.

IV. Anti-Sensor Network Operation

The localization of sensor nodes is a challenging task as sensors do not cooperate with the monitors. Under these adverse conditions, the already challenging sensor localization becomes even harder to accomplish. To this end, we propose to use localization algorithms augmented with signal classification techniques to localize sensors.

A. Basic Sensor Localization Methodology

Let the anti-sensor system be comprised of m monitors located at (x_i, y_i), $i = 1, \cdots, m$. Let each monitor observe the DoA and the received signal strength of a signal emitted by a sensor located at (x, y). Under ideal conditions, each monitor i should determine the direction of arrival (DoA) of the signal $\theta_i(x, y)$ and the distance to the emitter sensor $r_i(x, y)$ with no error:

$$r_i(x,y) = \sqrt{(x-x_i)^2 + (y-y_i)^2} \quad (1)$$

$$\theta_i(x,y) = \arctan\frac{y-y_i}{x-x_i}, \quad i = 1, \cdots, m. \quad (2)$$

However, a monitor i can only estimate the DoA $\hat{\theta}_i$ and the distance to the sensor $\hat{r}_i$ imprecisely due to measurement errors and errors introduced by the signal propagation. Let distance and DoA estimation errors be denoted by Δr_i and $\Delta\theta_i$:

$$\Delta r_i = \hat{r}_i - \sqrt{(x-x_i)^2 + (y-y_i)^2} \quad (3)$$

$$\Delta\theta_i = \hat{\theta}_i - \arctan\frac{y-y_i}{x-x_i} \quad i = 1, \cdots, m. \quad (4)$$

Input: Sample Set: X
Output: Estimated Location: EL
NLS(X):
1. Set counter j:=0
2. Compute an initial location estimate $(\hat{x}_0, \hat{y}_0)$
3. **WHILE** TRUE
4. x:=$\hat{x}_j$, y:=$\hat{y}_j$
5. **FOR** each monitor i
6. Compute Δr_i using Eq. 3
7. Compute $\Delta\theta_i$ using Eq. 4
8. Update Φ_j and A_j:
9. Compute location error Ψ_j using Φ_j and Eq. 10
10. **IF** $\Psi_j > \epsilon$
11. $[\hat{x}_{j+1}\ \hat{y}_{j+1}]^T$:=$[\hat{x}_j\ \hat{y}_j]^T + \Psi_j$
12. j:=$j+1$
13. **ELSE**
14. Return EL:=$(\hat{x}_j, \hat{y}_j)$

Fig. 1. NLS Location Estimation Algorithm

Using Taylor series expansion, we can obtain a linearized estimate for Δr_i and $\Delta\theta_i$, $i = 1, \cdots, m$, expressed in terms of the error in position $\Psi = [\Delta x\ \Delta y]^T$.

$$\Delta r_i = \frac{\partial r_i(x,y)}{\partial x}\Delta x + \frac{\partial r_i(x,y)}{\partial y}\Delta y \quad (5)$$

$$\Delta\theta_i = \frac{\partial\theta_i(x,y)}{\partial x}\Delta x + \frac{\partial\theta_i(x,y)}{\partial y}\Delta y \quad (6)$$

Defining terms a_i and b_i for $i = 1, \cdots, m$ as

$$a_i = \frac{\partial r_i}{\partial x} = \frac{x - x_i}{r_i}, \qquad a_{m+i} = \frac{\partial\theta_i}{\partial x} = \frac{-(y - y_i)}{r_i^2}, \quad (7)$$

$$b_i = \frac{\partial r_i}{\partial y} = \frac{y - y_i}{r_i}, \qquad a_{m+i} = \frac{\partial\theta_i}{\partial y} = \frac{x - x_i}{r_i^2}, \quad (8)$$

and considering the observations of all monitors $i = 1, \cdots, m$, the resulting system of equations can be expressed as $\Phi = A\Psi$, where $\Phi = [\Delta r_1 \cdots \Delta r_m\ \Delta\theta_1 \cdots \Delta\theta_m]^T$, and

$$A^T = \begin{bmatrix} a_1 & \cdots & a_{2m} \\ b_1 & \cdots & b_{2m} \end{bmatrix}. \quad (9)$$

If estimation error of all monitors Φ is known, then the estimation error in location Ψ can be computed as follows:

$$\Psi = A^{+}\Phi, \quad (10)$$

where $A^{+} = \left(A^T A\right)^{-1} A^T$ is the pseudo inverse of A.

With this introduction, we can use the well-known nonlinear least square (NLS) [14] algorithm to estimate the location of a sensor given observations from a set of monitors if every observation can be associated with its correct source. The NLS location estimation algorithm is outlined in Fig. 1. In NLS, the initial location estimate can be obtained using only the observations of a single monitor or a combination of observations via multi-lateration or triangulation.

B. Localization with Encrypted Messages

When sensors use encryption to hide their identities, monitors need to find alternative ways to associate received signals with their sources. To this end, we propose to use a single packet transmission to extract multiple samples. The resulting estimates are then used by localization algorithms. In these localization algorithms, observing multiple transmissions from the deployment area, we cluster the individual location estimations as belonging to a set of sources. Then, the clustered observations are jointly processed to yield our final estimation for the signal sources.

1) Classification of a One-Time Transmission: Under encryption, sensor IDs cannot be extracted from transmitted information packets to connect transmissions with sources. However, monitors can associate a given packet transmission received by multiple monitors to the same source, although the identity of the source would remain unknown. Such transmissions are referred to as *one-time transmissions*. This association is performed using time stamps and signal signatures.

2) Using One-Time Transmissions for Location Estimation: We define a *sample* as the set of m distance and/or DoA estimations obtained by different monitors based on a one-time transmission, where m is the number of monitors.

Assuming that the transmission rates of sensor nodes is low and the packet transmission time is sufficiently long, it is possible to obtain multiple independent observations (samples) by each monitor during one packet transmission. We define a *sample set* S_i consisting of N_p samples s_j^i gathered during j^{th} packet transmissions, where $i = 1, \cdots, N_p$ denotes the sample number during the packet transmission. Each sample set S_i consists of $m \times N_p$ distance and/or angle estimates. When S_i processed by a location estimation algorithm, the resulting location estimation is referred to as *sample point* SP_i.

3) Batch Localization Algorithm: The sample points may still contain inaccuracies. To increase the number of observations for localization, we need to group sample points according to their probable sources. We propose a Batch Localization algorithm (B_LOC) that processes the results of a large set of observations jointly. First, sample sets obtained from one-time transmissions are processed by the non-linear least square (NLS) localization algorithm, producing sample points. Then, sample points are clustered using the Quality Threshold (QT) clustering algorithm [13]. For each cluster of sample points, we re-estimate the final location of the sensor using the NLS algorithm with the sample sets of all sample points in the cluster. The outline of the algorithm is given in Fig. 2.

The clustering is done using a variation of the Quality Threshold (QT) [13] algorithm given in Fig. 3. The minimum cluster size is included in this procedure to eliminate the outliers. In our computations, we typically use 1% of the number sample sets as the minimum cluster size. We use the maximum variance value computed over the entire deployment area $\mathbb{A}$ as the cluster diameter limit R.

C. Localization with Power Level Variations

In addition to message encryption, sensors can also change their transmission power levels to affect monitors' estimations. While the algorithms outlined in Section IV-B can be used

Input: N Sample Sets: S_i; Cluster Diameter: R;
Minimum Cluster Size: CS_{min}
Output: Number of Sensors: EN; Estimated Locations EL_j
B-Loc(S_i,R):
1. **FOR** every sample set S_i, $i = 1, \cdots, N$
2. Compute sample point $SP_i := NLS(S_i)$
3. Cluster SP_i using QT algorithm:
4. Determine the number of clusters:
5. EN:=QT(SP_i,R,CS_{min}).N
6. Determine sample point clusters:
7. C_j:=QT(SP_i,R,CS_{min}).C_j, $j = 1, \cdots, EN$
8. **FOR** every sample point cluster C_j
9. Determine all sample sets of samples points in C_j:
10. $SP_i \in C_j \Rightarrow S_i \in cs_j$
11. Compute EL_j:=NLS(cs_j)

Fig. 2. Batch Localization Algorithm

Input: Sample Points: SP_i; Cluster Diameter: R;
Minimum Cluster Size: CS_{min}
Output: Number of Clusters: N; Cluster Member Sets: C_i
QT(SP_i,R):
1. Set Cluster Number N:=0
2. **WHILE** $S_i \neq \emptyset$
3. Reset temporary cluster sets $TC_j = \emptyset$
4. **FOR** every sample point j in SP_i
5. Add all neighboring sample points within R to TC_j
6. Determine the largest temporary cluster TC_k
7. **IF** $\mid TC_k \mid < CS_{min}$
8. **RETURN**
9. Increment number of clusters: N:=$N + 1$
10. Store TC_k in C_N
11. Update SP_i by removing all sample points in C_N:
12. $SP_i := SP_i \backslash C_N$

Fig. 3. QT Algorithm

without modification, the basis of the NLS estimation method must be changed slightly since distance estimations are unreliable. The estimation error vector Φ and the transformation matrix A are re-defined as Φ' and A' by removing all distance estimation-related terms as shown below:

$$\Phi' = \begin{bmatrix} \Delta\theta_1 \\ \vdots \\ \Delta\theta_m \end{bmatrix}, \text{ and } A' = \begin{bmatrix} a_{m+1} & b_{m+1} \\ \vdots & \vdots \\ a_{2m} & b_{2m} \end{bmatrix}. \quad (11)$$

V. Performance Evaluation

In this section, simulation results reflecting the performance of the proposed anti-sensor localization system are presented. We use the mean and standard variance of the localization error as well as false positive and negative alarm ratios as metrics. Unless otherwise stated, we consider a $100m \times 100m$ deployment area with 20 randomly placed sensors and four monitors located in the corners. We assume that all monitors have estimation errors uniformly distributed in the range of $[-5, +5]m$ for Δx and $[-0.04, +0.04]rad$ for $\Delta\theta$. Reported results reflect the average of 200 independent runs. We also assume that packet transmissions of sensors are long enough to be sampled up to five ($N_p = 5$) times to produce statistically independent observations. The performance evaluation of the proposed localization algorithms is performed for three cases. Case 1 involves no encryption or transmission power variations and serves as our baseline under which the best performance is achieved. Case 2 corresponds to the scenario where sensors encrypt their messages. Finally, in case 3, sensors both encrypt their messages and also change their power levels.

A. Sensitivity Analysis of Localization Algorithms

The algorithm sensitivity is evaluated by changing the number of samples processed to obtain the location information. We observe the false positive alarm ratio (i.e., ratio of the number of nodes falsely identified to exist to the total number of sensors), false negative alarm ratio (i.e., the ratio of the number of sensor nodes not found to the total number of sensors), the mean error, and the standard variance of the error.

The false positive alarm ratio is almost 3%, which tapers off quickly when more samples are obtained (Fig. 4(a)). As shown in Fig. 4(b), Case 2 has a much smaller false negative alarm ratio, than for Case 3, which is expected since the amount of information contained in Case 2 is larger than in Case 3.

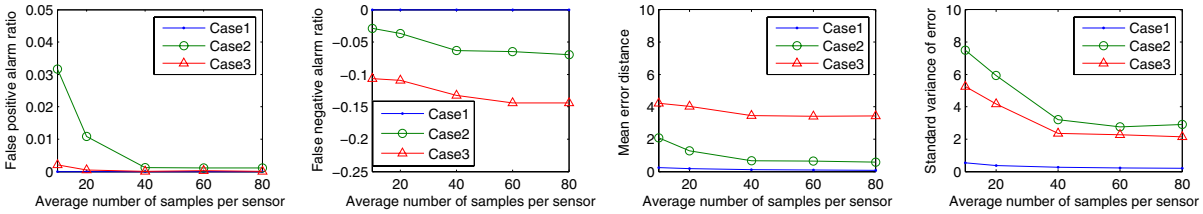
We also observe the mean and the standard variance of the error for the same scenarios as shown in Fig. 4(c) and Fig. 4(d). When the number of samples is increase, the error means stabilize, indicating that additional observations do no improve the average error performance.

B. Effect of Number of Monitors and Signal Samples

We have observed the effect of the number of monitors (equally spaced along the perimeter) and the number of samples on the estimation error mean and the standard variance as shown in Fig. 5. As expected, as the number of samples per sensor and the number of monitors increase, the mean error decreases for all cases with diminishing returns. For standard variance, the performance improvement is negligible for Cases 1 and 2 for high number of samples or monitors. In Case 3, the performance becomes slightly worse for very high number of samples due to misclassifications during clustering. This classification error can be explained by the cumulative effect of higher number of insufficient samples distorting the performance of the clustering efficiency of the localization algorithm. Hence, it can be overall stated that the performance behavior of the proposed localization algorithms depends on the initial accuracy of the sample sets. Therefore, it may not be possible to observe the benefits of an always increasing accuracy with higher number of samples.

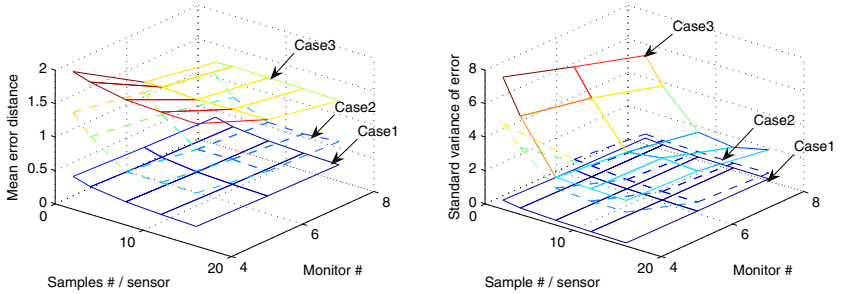
C. Effect of Estimation Errors in Monitors

In this experiment, we observe the effect of estimation error ranges on the mean and the standard variance of the localization error. We change the distance estimation error range from ± 1 to ± 10m and DoA estimation range from ± 0.01 to $\pm 0.1rad$. The results are not graphically presented due to space constraints. Our results show that the localization error mean and standard variance increase as the estimation error range increases.



(a) False Positive (b) False Negative (c) Mean Error (d) Standard Variance

Fig. 4. Sensitivity Analysis



(a) Mean Error (b) Standard Variance

Fig. 5. Error Mean and Standard Variance vs. Number of Samples and Monitors

VI. Conclusions and Future Work

In this paper, the anti-sensor network system is proposed that aims to protect a given asset from being observed by a sensor network. The system relies on fixed set of monitors nodes to observe wireless transmissions in the protected area. With these observations, sensor locations are estimated through collective processing. Once localized, sensors are physically removed from the observation area. To the best of our knowledge, this is the first work to protect assets against sensor networks. To do so, we also develop new localization methods to be used in non-cooperative environments. Our simulation results also support our design principles: Longer observation times improve the localization performance and produce accurate location estimations with diminishing returns. In our future work, we plan to study optimal monitor positioning in convex and concave observation areas. We will also focus on extending the deployment of anti-sensor networks to areas larger than the observation area of monitors.

Acknowledgment

This research was partially supported by NSF grants under contract number ACI-0329155, CCF-0546668 and CNS-0509175. This research does not reflect the views of NSF.

References

[1] I. Akyildiz, W. Su, Y. Sankarasubramaninam, and E. Cayirci, "Wireless Sensor Networks: A Survey," *Computer Networks Journal (Elsevier)*, vol. 38, pp. 393–422, March 2002.

[2] D. Niculescu and B. Nath, "Ad hoc positioning system (aps) using aoa," *Proceedings of IEEE Infocom 2003*, Apr. 2003.

[3] N. Priyantha, A. Chakraborty, and H. Balakrishnan, "The cricket location-support system," *Proceedings of ACM Mobicom 2000*, Aug. 2000.

[4] N. Patwari, J. Ash, S. Kyperountas, A. I. Hero, R. Moses, and N. Correal, "Locating the nodes: Cooperative localization in wireless sensor networks," *IEEE Signal Processing Magazine*, vol. 2, pp. 54–69, July 2005.

[5] A. Savvides, C. Han, and M. B. Srivastava, "Dynamic fine-grained localization in ad-hoc networks of sensors," *Proceedings of ACM Mobicom 2001*, July 2001.

[6] P. Bahl and V. N. Padmanabhan, "Radar: An in-building, rf-based user location and tracking system," *Proceedings of IEEE Infocom 2000*, Mar. 2000.

[7] K. C. A. D. R. Govindan and G. Sukhatme, "Ad-hoc localization using ranging and sectoring," *Proceedings of IEEE Infocom 2004*, Mar. 2004.

[8] D. Niculescu and B. Nath, "Dv-based positioning in ad hoc networks," *Journal of Telecommunication Systems*, vol. 22, no. 1-4, pp. 267–280, 2003.

[9] Y. Shang, W. Rumi, and Y. Zhang, "Localization from mere connectivity," *Proceedings of ACM MobiHoc 2003*, June 2003.

[10] T. He, C. Huang, B. Blum, J. Stankovic, and T. Abdelzaher, "Localization from mere connectivity," *Proceedings of ACM MobiCom 2003*, Aug. 2003.

[11] M. Sichitiu and V. Ramadurai, "Localization of wireless sensor networks with a mobile beacon," *Proceedings of IEEE MASS 2004*, pp. 174–183, Oct. 2004.

[12] R. Schmidt, "Multiple emitter location and signal parameter estimation," *IEEE Transactions on Signal Processing*, vol. 34, pp. 276–280, Mar. 1986.

[13] L. Heyer, S. Kruglyak, and S. Yooseph, "Exploring expression data: Identification and analysis of coexpressed genes," *Genome Research*, vol. 9, pp. 1106–1115, Nov. 1999.

[14] D. Bates and D. Watts, *Nonlinear Regression and Its Applications*. New York: Wiley, 1988.