An Intrusion Detection System for Wireless Sensor Networks

Christiana Ioannou, Vasos Vassiliou and Charalampos Sergiou
Networks Research Laboratory (NetRL)
Department of Computer Science
University of Cyprus

Email: {cioannou,vasosv,sergiou}@cs.ucy.ac.cy

***Abstract*—Attacks in Wireless Sensor Networks (WSNs) aim in limiting or even eliminating the ability of the network to perform its expected function. WSNs are networks with limited resources and often deployed in uncontrollable environments that an intruder can easily access. WSN attacks target specific network layer's vulnerabilities but normally affect other layers as well. Local sensor activity at multiple sensor network layers should be monitored and evaluated to detect possible malicious intervention. In this work we propose a general methodology of an anomaly-based Intrusion Detection System (IDS), named mIDS, that uses the Binary Logistic Regression (BLR) statistical tool to classify local sensor activity to either benign or malicious. We evaluate the proposed system using routing layer attacks and we show that mIDS is able to detect malicious activity within the range of 88%-100%.**

***Index Terms*—Security, Wireless Sensor Network, Selective Forward Attack, Blackhole Attack, Binary Logistic Regression**

I. Introduction - Related Work

The unique features of Wireless Sensor Networks (WSNs) render them attractive for use in harsh environments, which would have been otherwise difficult or impossible to operate into [1], [2]. However, as any other type of networks, WSNs suffer from a variety of security attacks. Security is a critical subject for WSNs. Compromised nodes may result in inaccurate and/or misleading information, thus failing in achieving the network's goal. Security techniques for wired networks have been considered for use in WSNs, but they invariably require significant memory and CPU power, a fact that renders their use infeasible in low-power, low-scale devices, such as wireless sensor nodes. A typical TmoteSky/TelosB wireless sensor module has 8 MHz CPU power, 10 kB of RAM and 48kB of program flash memory [3], which is a huge deviation from traditional personal computer specifications.

Research has been conducted in developing customized security methods for WSNs to establish confidentiality, integrity, and availability. Security techniques can be classified as offering either prevention or detection [4]. The first line of defense are the prevention techniques, which use low-overhead cryptography in key exchange, and hash methods to ensure integrity and confidentiality [5], [6], [7]. The second line of defense are the Intrusion Detection Systems (IDS) that are responsible to detect the presence of malicious intervention in the network. Furthermore, an IDS is classified based on the detection algorithm it applies. Many detection techniques have been proposed either in the field of WSNs [8], [9] and in IoTs [10]. Some of them employ misuse detection methods (also referred to as signature- or pattern-based), but the majority uses anomaly detection [11].

The misuse detection method detects known attacks with high success rate, but has significant drawbacks as that it requires prior knowledge of the attack and its pattern or signature. Those, are stored in a database and are used to compare the ongoing network activity with known malicious traffic patterns.

On the other hand, the anomaly detection method detects novel attacks, thus decreasing the false negative rate, but has more false positive alarms. It requires offline training to determine the normal behavior of the network and the setting of certain markers or limits, that characterise the normal behavior. Upon deployment, network activity is compared with the preset thresholds and any deviation from what is considered normal, is classified as abnormal. Setting the thresholds too high may raise high false negative alerts, while setting the threshold too low may raise high false positive alerts.

Malicious behavior is defined as the network behavior created by compromised nodes with the intend to disrupt and/or compromise WSNs goal. Attacks frequently target network layer vulnerabilities. Selective Forward and Blackhole attacks are examples of network layer attacks as they are designed to take advantage of possible vulnerabities of the routing protocol. Regardless of the network layer they are targeting, they also affect other local sensor network layers [12]. It is our belief that multilayer monitoring and detection schemes should be considered when designing an IDS.

In this work we present an anomaly-based Intrusion Detection System (IDS), called mIDS. The mIDS employs Binary Logistic Regression (BLR) statistical modeling as a classification algorithm to identify the nature of the local activity, malicious or benign. BLR defines the nature of sensor activity using both malicious and benign activity. The derived detection model uses few local sensor parameters thus confining the memory overhead imposed to a few monitored parameters.

We present a preliminary evaluation of the BLR anomaly detection method focusing on routing-related attacks. At predefined time intervals, a run-time monitoring tool (RMT) [13]

978-1-5386-0643-8/17/$31.00 ©2017 IEEE

provides local sensor activity from multiple layers in the stack, which can be used as input to the classification algorithm. We have two types of scenarios, the benign and malicious scenario. At the benign scenario, every sensor node within the network is executing its application as intended. In a malicious scenario, one node within the network is under the influence of a routing attack. Local sensor activity from each scenario and each node, retrieved at each predefined interval from RMT, is used to derive the detection models and evaluate them. When BLR detection models are evaluated, they can achieve accuracy levels within the ranges 88% - 100%.

The rest of the paper is structured as follows: Section II describes our proposed methodology. Section III layouts our experimental framework and Section IV presents our results. Section V concludes our work.

II. The mIDS Methodology

A. Anomaly Detection technique

An anomaly detection mechanism has the advantage of detecting novel attacks. If the security system is aware of the normal behavioral patterns of the node, then, when an unknown behavior is detected, it is classified as malicious and an alert is raised. Before WSN deployment the profile of the specific network is compiled and a threshold is provided. Any behavior that exceeds this threshold is classified as malicious.

Anomaly detection requires offline analysis, which is frequently called “the training phase”. For each specific network, a period is used for monitoring and data collection, that are going to be used for training. The challenge of the training phase is to simulate the exact environment that the WSN will eventually be deployed into, or use the same environment whenever possible. The training phase should take place in a controlled environment that has to be viral-free.

The disadvantage of anomaly detection is that it may have high false alarm rates. Anomaly detection bases its findings on predictions, thus increasing the possibility of having high false rates, named false positives or false negatives. False positives are the false alarms raised by IDS where there is no malicious intervention. Contrary to that, false negatives are the missed alarms (the cases that IDS failed to identify malicious interventions). The ideal situation, is the elimination of false alarms. High false positive alarms may create mistrust to the WSN administrator, while high false negative alarms may end up compromising the whole network.

B. Collecting Data

In our system the data are collected from logs that record metrics from the routing layer for each run per node using the RMT (Run-Time Monitoring Tool) [13]. In the resulting data set, a run per node, non-malicious and malicious is represented by a vector consisting of five values. We use the five metrics (independent variables) shown in Table I.

TABLE I: Parameters Monitored

Routing Layer Parameters	
Data Packets Received	Data Packets Send
Packets Forward	**Packets Dropped**
Announcements Received	

The set of the data collected is based on the work proposed in [12]. We refer to the set of benign vectors as B and the set of the viral vectors as V. The vector representation of benign and viral vectors is the following:

$$\mathbf{b}_i = \{b_{i,1}, b_{i,2}, \ldots, b_{i,j}\}^T \tag{1}$$

where $\mathbf{b}_{i,j}$ represents the metric j made by a benign sensor node at the monitoring time interval i.

$$\mathbf{v}_k = \{v_{k,1}, v_{k,i}, \ldots, v_{k,j}\}^T \tag{2}$$

where $\mathbf{v}_{k,j}$ represents the metric j made by viral sensor node at the monitoring time interval k.

For the data analyzed per experimental run we have $i = 1, 2, \ldots, 25$, $k = 1, 2, \ldots, 25$, and $j = 1, 2, \ldots, 5$. The set B_i is used to develop a template of benign behavior for node i. The set V_i is used to see if each $\mathbf{v} \in V$ can be distinguished from each $\mathbf{b} \in B$.

C. Binary Logistic Regression

Logistic Regression is a statistical method that allows to analyze and predict a dichotomous outcome. It predicts a binary dependent variable based on a set of independent variables. In this study, the dependent variable that has to be predicted, is whether the network activity is caused by a viral sensor node or not. The independent variables are the set of network activity parameters in Table I. The set of significant independent variables used for the current analysis are the subset shown in bold.

There are two phases in this approach, the training and the evaluation phase. The training phase establishes a regression model to be used in the evaluation phase. It determines whether the method can be used to identify viral activity and which independent variables are the most significant [14]. The evaluation phase tests the model against a different data set.

For the training set the independent variables are used as gathered to avoid any complicated data. The dependent variable has two values: 0, which means benign, and 1 which means viral. Equation (3) shows the calculation of probability P (the probability that the network activity is viral).

$$P = \frac{e^{\alpha+\beta_1 x_i+\beta_2 x_i+\cdots+\beta_n x_n}}{1+e^{\alpha+\beta_1 x_i+\beta_2 x_i+\cdots+\beta_n x_n}} \tag{3}$$

where n is the number of significant independent variables. Each x_i represents the value of i^{th} independent variable, α is constant, β is the regression coefficient.

The challenge of logistic regression is to fit the mathematical data with the actual data, so as to maximize the goodness of fit. The mathematical tool for computing the goodness of fit is called the ”maximum likelihood”, which is the condition probability of the dependent variable, given the set of independent variables $P\left(DependentVariable|X\right)$.

To select the most appropriate set of independent variables such as to achieve a high degree of likelihood, is a matter of trial and error. For this research the p-value is used to evaluate the independent variable significance. An independent variable is considered significant when it has a p-value more than 0.05.

The BLR model will return values between the range of 0-1. If the result is more than 0.5 then the activity is classified as malicious.

III. Experimental Framework

A. Weighed Shortest Path Routing protocol

The attacks are evaluated using an in-house implemented routing protocol called Weighed Shortest Path (WSP) that is based on the widest-shortest path concept. It takes into consideration the distance of the sensor node from the Sink node and the signal strength.

The WSP protocol we implemented requires that each sensor node has a neighbor table, which is created when the network is formed and is updated when there is change in the table or at predefined periods. A table entry includes the neighbor's node id, the number of hops and the RSSI value. A sensor node located within the transmission range of the Sink, advertises that it is one hop away from the Sink. When a sensor node receives an announcement, it updates its neighbor table. A sensor node chooses a relay node, initially based on the distance from the Sink and then according to the lowest RSSI.

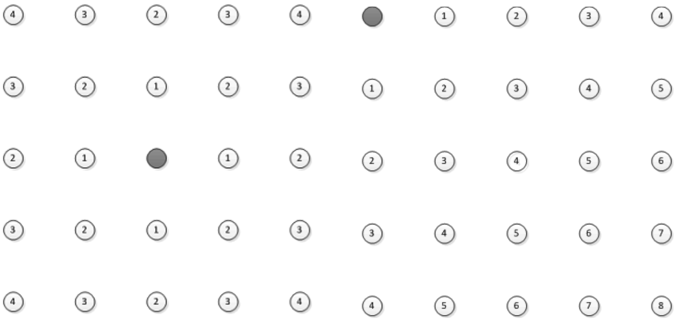
B. Routing Layer Attacks

A fundamental WSN characteristic is the fact that each sensor node relies on the cooperation of other nodes to forward its packets. The intruders can take advantage of this hop-by-hop communication to create their routing attacks. A compromised node with the Selective Forward attack, selectively chooses which packets to forward [15] [9] [16]. To examine this attack, we have implemented two variations of it based on the WSP routing protocol, the Forwarding Ratio and the Block Node attacks. The selection of the packets to be forwarded can be either randomly selected, based on a percentage of successfully transmitted packets employed by the infected node, or it can be sensor based, where the infected node denies the forwarding of packets of a specific node [12]. The percentage of successfully transmitted packets in the Forwarding Ratio attack is set to 50%. The Block Node sensor-based Selective Forward attack, randomly chooses a sensor node to drop its packets at predefined time intervals, to make it more difficult to be detected.

We have also implemented the Blackhole attack. The Blackhole attack, lures traffic toward the compromised node by advertising that it is the closest one to the Sink (one hop away) [12].

IV. Results

The aforementioned attacks have been implemented within the Contiki O/S and we tested the results using the associated COOJA simulator. All sensor nodes are equivalent to TelosB nodes and have a 25m radio range. Each node transmits one data packet of 48 bytes every second.



(a) Sink in the middle of the grid (b) Sink on top left corner of the grid

Fig. 1: Network Topology and placement of the Sink node

We gather WSP information from every sensor node within the network, as shown in Table I. Two topologies as of Fig. 1a and Fig. 1b consisting of 25 nodes including the Sink (the Sink is the node shown in darker colour) are employed for the evaluation of our BLR model. The nodes are marked with their number of hops away from the Sink. In Fig. 1a, the Sink is in the middle, making the impact of the attack less evident for Selective Forward since sensor nodes can find other routes to send their packets. In Fig. 1b, the Sink is located at the top left corner of the grid so as to communicate directly with just two nodes.

For each topology we defined two types of scenarios: a malicious scenario in which a compromised node is placed in the network, and a benign scenario in which all nodes are benign. For every attack, we run in total 24 malicious scenarios, for each topology. We also make the assumption that the Sink node is never compromised.

The total execution time for each scenario is set to 15 minutes. We allow a 2-minute period at the beginning of the simulation for the network to be connected and reach a steady state. The monitoring time period (called epoch) is set to 30 seconds, having in total 26 monitoring periods for each sensor node and for each scenario. The last monitoring period is disregarded as some nodes may not successfully completed their last monitoring period; the nodes start execution at random times. The total number of epochs for each attack are 14400 (24 malicious scenarios with each malicious scenario resulting to 600 epochs).

The BLR model is trained and evaluated on the local sensor activity gathered at every epoch. Specifically, it takes as input the averaged values of independent parameters per epoch by all nodes that are at the same distance from the Sink. Therefore, for each attack 25 averaged malicious monitoring periods are used. In the resulting data set, non-malicious and malicious nodes are represented by a vector consisting of 5 values. These are the 5 metrics (the independent variables).

A. Training Stage

For the training set all of the independent variables are used as gathered from the RMT, and averaged offline. To classify the vectors, whether they are taken from benign or malicious nodes, we include the dependent variable, 0 and

1 respectively. The classification process allows the logistic regression to evaluate the significance of each independent variable, in identifying the nature of the activity.

The metrics for the B are extracted from the benign scenario of each topology, in which no compromised node is present. The metrics for the V are extracted from the corresponding malicious scenario where a compromised node exists in the network.

$$\underline{T}_{training} = \{t_{i,1}, t_{i,2}, \dots, t_{i,j}\} \tag{4}$$

$$\underline{U}_{training} = \{u_{k,1}, u_{k,i}, \dots, u_{k,j}\} \tag{5}$$

We created two data sets $T_{training}$ by using 80% of the metrics from B and $U_{training}$ by using 80% of the metrics from V. The final training set is defined as:

$$\underline{X}_{training} = \{t_{i,1}, t_{i,2}, \dots, t_{i,j}, \dots, u_{k,1}, u_{k,i}, \dots, u_{k,j}\} \tag{6}$$

The vectors in the set $X_{training}$ are used as the input of independent variables to BLR, to derive the model.

We derived BLR models targeting each specific attack and a more general model that aims in detecting routing layer attacks. The BLR models for each attack, used as training input data taken from the malicious scenario with the respective attack.

According to [12], the location of the malicious sensor node can define the level of impact a malicious node may have on the network. To eliminate the node's placement within the network as a deterministic factor we trained our models using the training set with sensor activity from all nodes within the network, regardless of their position. We created a model for each of the attacks we implemented.

B. Evaluation Stage

For the rest of the paper, we used the following abbreviations for each attack: SF-Selective Forward, BH-Blackhole, BN-Block Node, and FR-Forwarding Ratio. The objective of this stage is to evaluate whether the BLR model captured at the training stage can achieve a high overall correct prediction percentage.

$$\underline{T}_{evaluation} = \{t_{i,1}, t_{i,2}, \dots, t_{i,j}\} \tag{7}$$

$$\underline{U}_{evaluation} = \{u_{k,1}, u_{k,i}, \dots, u_{k,j}\} \tag{8}$$

We created two evaluation sets $T_{evaluation}$ and $U_{evaluation}$, which included 20% of the corresponding B and V and were not used at the training stage. The evaluation metric $X_{evaluation}$ is defined as:

$$\underline{X}_{evaluation} = \{t_{i,1}, t_{i,2}, \dots, t_{i,j}, \dots, u_{k,1}, u_{k,i}, \dots, u_{k,j}\} \tag{9}$$

The results are displayed in the form of a Confusion Matrix that shows the false alarms and correct predictions. An activity is considered to be benign when the probability according to (3) is less than 0.5, otherwise, the sensor activity is classified as viral.

We also use the Accuracy value (ACC) as an indicator of the effectiveness of our model. The equation for ACC is shown in (10)

$$ACC = \frac{\sum TruePositives + \sum TrueNegatives}{\sum TotalPopulation} \tag{10}$$

The True Positive/Negative values are the correct predictions of the model. True positive means that the model was given an activity that was benign and was correctly identified, the same applies to true negative values when given a viral activity and the model correctly identifies it.

C. Selective Forward

In the training stage we created two BLR models, a model for Selective Forward Forwarding Ratio (SF - FR) and a BLR model for the Selective Forward Block Node (SF - BN). The training and evaluation epoch data was taken from the network topology where the Sink is placed in the middle of the grid. The significant independent variables that were used were the *number of packets forward* (P_{FR}), *data packets received* (P_{RC}) and the *number of packets dropped* (P_{DR}). The resulting probability model is shown in (11).

The evaluation result of our SF-FR and SF-BN models are shown in Table II.

TABLE II: Confusion Matrices for Selective Forward

Evaluation Set		True diagnosis		Percentage
		Benign	Viral	Correct
SF-FR	Benign	20	0	100%
	Viral	5	15	75%

Accuracy ratio(ACC)= 0.88

Evaluation Set		True diagnosis		Percentage
		Benign	Viral	Correct
SF-BN	Benign	20	0	100%
	Viral	5	15	75%

Accuracy ratio(ACC)= 0.88

The evaluation results are the same for both models. The number of parameters taken from 20 benign epochs were correctly classified as benign; whereas out of 20 malicious epochs, 5 of them were wrongly classified as benign. The 25% false negatives was expected, since the compromised nodes that are placed the furthest away from the Sink, in this case four hops away from the Sink, are not chosen to forward any packets. Therefore, even though they are compromised, they do not have any impact on the compromised sensor activity.

$$P = \frac{e^{\alpha+\beta_{fr}P_{FR}i+\beta_{rc}P_{RC}+\beta_{dr}P_{DR}}}{1+e^{\alpha+\beta_{fr}P_{FR}i+\beta_{rc}P_{RC}+\beta_{dr}P_{DR}}} \tag{11}$$

D. Selective Forward and Blackhole

We followed the same principle of training and evaluation for Selective Forward and Blackhole. We derived two BLR models and evaluated them with their corresponding evaluation sets. The results are shown in Table III. The BLR models have successfully detected all attacks having 100% accuracy.

TABLE III: Confusion Matrices for Selective Forward and Blackhole

Evaluation Set		True diagnosis		Percentage
		Benign	Viral	Correct
SFBH-FR	Benign	20	0	100%
	Viral	0	20	100%

Accuracy ratio(ACC)= 1

Evaluation Set		True diagnosis		Percentage
		Benign	Viral	Correct
SFBH-BN	Benign	20	0	100%
	Viral	0	20	100%

Accuracy ratio(ACC)= 1

E. Network Topology and multiple attacks

Our next objective was to evaluate the importance of network topology in detecting attacks and detecting multiple attacks. We derived a BLR model using all data from the network topology when the Sink is positioned in the middle of the grid and evaluated it against data taken from the network topology where the Sink is at the top of the grid. The evaluation and training sets consisted with data from all attacks. With the training set we computed our constant and coefficients to use in our BLR model (see table IV).

TABLE IV: BLR model

Variables	**Estimated Values**
α	6.931e-01
β_{fr}	-1.321e+00
β_{rc}	-6.161e-10
β_{dr}	1.458e+01

We evaluated our BLR model using our evaluation set from a different network topology and we achieved 91% accuracy according to Table V. There are 9% of false negatives, out of which 72% are caused by the sensor nodes positioned the furthest away from the Sink, which are under the influence of Selective Forward attacks and do not have any impact on the sensor activity.

TABLE V: Confusion Matrix for multiple attacks

Evaluation Set - Sink on Top		True diagnosis		Percentage
		Benign	Viral	Correct
Sink in the middle	Benign	175	25	88%
	Viral	69	731	91%

Accuracy ratio(ACC)= 0.91

V. Conclusions

In this paper we proposed a general methodology of an anomaly-based Intrusion Detection System (IDS), named mIDS, that uses the Binary Logistic Regression (BLR) statistical tool to classify local sensor activity to either benign or malicious to detect a malicious behavior within a sensor node. We have shown that when BLR is trained for a specific attack it has an accuracy level between the range 88% and 100%. Our model's accuracy better than the detection rate of other proposed works, but with the basic difference that we monitor only three parameters and we monitor local sensor activity [9], [10].

We have evaluated our model using Selective Forward and Blackhole attacks that were implemented within the Contiki O/S. We created a model that took into consideration both attacks and evaluated in different network topologies. The results were promising as the BLR model was 91% accurate for detecting two types of attacks at the same time. The next steps to take are to evaluate our model with more attacks, implement our detection model within the Contiki O/S, and install the mIDS at the constrained nodes.

References

[1] G. Werner-Allen, K. Lorincz, M. Welsh, O. Marcillo, J. Johnson, M. Ruiz, and J. Lees, "Deploying a Wireless Sensor Network on an Active Volcano," *IEEE Internet Computing*, vol. 10, Mar. 2006.

[2] A. Mainwaring, J. Polastre, R. Szewczyk, D. Culler, and J. Anderson, "Wireless Sensor Networks for Habitat Monitoring," in *Proceedings of the 1st ACM International Workshop on Wireless Sensor Networks and Applications*, WSNA '02, (New York, NY, USA), ACM, 2002.

[3] Moteiv, "tmote sky low power sensor module," 2006. original document from Harris Semiconductor.

[4] K. R. Ahmed, K. Ahmed, S. Munir, and A. Asad, "Abnormal Node Detection in Wireless Sensor Network by Pair Based Approach using IDS Secure Routing Methodology," *Int J Comput Sci Netw Sec*, 2008.

[5] J. Deng, R. Han, and S. Mishra, "Defending against path-based DoS attacks in wireless sensor networks," in *Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks*, ACM, November 2005.

[6] J. Deng, R. Han, and S. Mishra, "Limiting DoS Attacks During Multihop Data Delivery in Wireless Sensor Networks," *International Journal of Security and Networks*, 2006.

[7] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil Attack in Sensor Networks: Analysis & Defenses," in *Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks*, IPSN '04, (New York, NY, USA), ACM, 2004.

[8] N. Aschenbruck, J. Bauer, J. Bieling, A. Bothe, and M. Schwamborn, "A Security Architecture and Modular Intrusion Detection System for WSNs," in *Networked Sensing Systems (INSS), 2012 Ninth International Conference on*, June 2012.

[9] A. P. R. da Silva, M. H. T. Martins, B. P. S. Rocha, A. A. F. Loureiro, L. B. Ruiz, and H. C. Wong, "Decentralized Intrusion Detection in Wireless Sensor Networks," in *Proceedings of the 1st ACM International Workshop on Quality of Service &Amp; Security in Wireless and Mobile Networks*, Q2SWinet '05, ACM, 2005.

[10] S. Raza, L. Wallgren, and T. Voigt, "SVELTE: Real-time intrusion detection in the Internet of Things," *Ad hoc networks*, 2013.

[11] R. Mitchell and R. Chen, "A Survey of Intrusion Detection in Wireless Network Applications," *Computer Communications*, 2014.

[12] C. Ioannou and V. Vassiliou, "The Impact of Network Layer Attacks in Wireless Sensor Networks," in *The International Workshop on Secure Internet of Things 2016 (SIoT 2016)*, September 2016.

[13] C. Ioannou, V. Vassiliou, and C. Sergiou, "RMT: a Wireless Sensor Network Monitoring Tool," in *Thirteen ACM International Symposium on Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Networks (PE-WASUN)*, (Malta), ACM, November 2016.

[14] C. Ioannou and G. Marin, "The Hunt for Viral Processes," Master's thesis, Florida Institute of Technology, Melbourne, Florida, USA, 2003.

[15] S. Kaplantzis, A. Shilton, N. Mani, and Y. Sekercioglu, "Detecting Selective Forwarding Attacks in Wireless Sensor Networks using Support Vector Machines," in *Intelligent Sensors, Sensor Networks and Information, 2007. ISSNIP 2007. 3rd International Conference on*, Dec 2007.

[16] A. D. Wood and J. A. Stankovic, "A Taxonomy for Denial-of-Service Attacks in Wireless Sensor Networks," *Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems*, 2004.