2007 International Conference on Sensor Technologies and Applications

Analysis of Anomalies in IBRL Data from a Wireless Sensor Network Deployment

Sutharshan Rajasegarar[1], James C. Bezdek[2], Christopher Leckie[3], Marimuthu Palaniswami[4]
ARC Special Research Center for Ultra-Broadband Information Networks (CUBIN)
[1,4]Department of Electrical and Electronic Engineering
[3]NICTA Victoria Research Laboratory
[2,3]Department of Computer Science and Software Engineering
University of Melbourne, Australia.
Email: {r.sutharshan, swami}@ee.unimelb.edu.au, caleckie@csse.unimelb.edu.au, jbezdek@uwf.edu

Abstract

Detecting interesting events and anomalous behaviors in wireless sensor networks is an important challenge for tasks such as monitoring applications, fault diagnosis and intrusion detection. A key problem is to define and detect those anomalies with few false alarms while preserving the limited energy in the sensor network. In this paper, using concepts from statistics, we perform an analysis of a subset of the data gathered from a real sensor network deployment at the Intel Berkeley Research Laboratory (IBRL) in the USA, and provide a formal definition for anomalies in the IBRL data. By providing a formal definition for anomalies in this publicly available data set, we aim to provide a benchmark for evaluating anomaly detection techniques. We also discuss some open problems in detecting anomalies in energy constrained wireless sensor networks.

1 Introduction

Wireless sensor networks are formed using large numbers of tiny sensor nodes which are resource constrained. These sensors have on-board processing and wireless communication capabilities [1]. These sensors are usually battery powered, and hence, extremely energy constrained. Wireless sensor networks can be deployed for remote monitoring and actuation purposes.

Sensor networks deployed for monitoring purposes may have to detect and report unusual behavior in the network or in the environment where they are deployed. Compared to wired networks, inherent limitations in a sensor network make it more vulnerable to faults and malicious activities such as denial of service attacks or flooding attacks, which can cause all or part of the network to be inoperative [2, 3]. These activities can cause anomalous behavior in the network or in the measurements it collects. Therefore it is vital to identify anomalous behavior in the sensor network for reliable, secure functioning and reporting events of interest to the user.

An *anomaly* or *outlier* in the data measurements or network traffic is an observation that appears to be inconsistent with the remainder of the data set [4]. A key challenge in sensor networks is to identify anomalies with high accuracy while consuming minimal energy in the network. In sensor networks, a majority of the energy is consumed in communication activity compared to computation activity [5]. Hence, we want to minimise the communication overhead while performing in-network processing for the anomaly detection process. This necessitates a distributed approach for anomaly detection, which performs detection at the local nodes and communicates only summary information over the network to reach a global decision about the anomalies. This approach is much more energy efficient in terms of communication overhead, as opposed to a *centralised approach* wherein all the node data are communicated to a central node in the network for processing.

Several real wireless sensor network deployments have been used for testing and monitoring purposes. The Great Duck Island Project [6] in the USA, the Intel Berkeley Research Laboratory (IBRL) deployment [7], farm monitoring [8] in Australia, and the proposed sensor network for the Great Barrier Reef [9] in Australia are examples. In this note, we analyse a four hour period of data for fifty-four nodes, gathered in the IBRL deployment project [7, 10]. We perform multivariate statistical analysis on this data and provide a formal definition for *anomalies* in the data set. In particular, we introduce the concept of an elliptical anomaly, which is capable of modeling a wide variety of normal behavior in sensor networks. To the best of our

0-7695-2988-7/07 $25.00 © 2007 IEEE
DOI 10.1109/SENSORCOMM.2007.29

knowledge, this is the first time such an analysis has been performed for the IBRL data for anomaly detection (refer to Section 2).

Several studies of anomaly detection in sensor networks have recently appeared in the literature. Loo et al. [11] used a data clustering approach to detect routing attacks in sensor networks, without co-operation among the nodes. Subramanium et. al. [12] proposed a distributed approach for intrusion detection based on kernel density estimators. Ngai et. al. [13] used a statistical technique for detecting sink hole attacks in sensor networks. Rajasegarar et. al. proposed a distributed cluster based approach [14], and distributed support vector machine based approach [15] for anomaly detection in sensor networks.

While many methods have been proposed to search for anomalous measurements in sensor networks, an impediment to systematic progress in this field is the lack of a clear definition for what constitutes anomalous measurements. In this paper we provide a formal definition for anomalies in a subset of the IBRL data. By providing a formal definition for anomalies on a publicly available data set, we believe that this provides a valuable benchmark for evaluating anomaly detection research. We conclude by discussing some open questions in detecting anomalies in the sensor network environment.

The rest of the paper is organised as follows. We introduce the Intel Berkeley Research Laboratory (IBRL) data, and analyse and define anomalies in Section 2. We discuss some open issues and future research options in Section 3.

2 Intel Berkeley Research Laboratory Data

We consider a data set gathered from a wireless sensor network deployment at the Intel Berkeley Research Laboratory (IBRL) [7, 10]. A wireless sensor network consisting of 54 *Mica2Dot* sensor nodes was deployed in the IBRL for a 30 day (720 hour) period between 28th Feb 2004 and 5th April 2004 [10]. Figure 1 shows the deployed node locations in the laboratory. The sensors collect five measurements: light in Lux, temperature in degrees celsius, humidity (temperature corrected relative humidity) ranging from 0% to 100%, voltage in volts and network topology information in each 30 second interval. Node 0 is the gateway node. Other nodes transmit their data in multiple hops to the gateway node. The furthest node in the network is about 10 hops away from the gateway node. During the 30 day period, the 54 nodes collected about 2.3 million readings.

For our analysis of the IBRL sensor data, we define the following notation. The sampling window is four hours. Each sensor M_j in a set of sensor nodes $M = \{M_j : j = 1...N\}$ measures a data vector x_i^j. Each data vector is composed of attributes (or features) x_{ik}^j, where $x_i^j = \{x_{ik}^j : k = 1...d\}$ and $x_i^j \in \Re^d$. At the end of sampling, each sensor M_j has collected a set of measurements $X^j = \{x_i^j : i = 1...n_j\}$. Let M_c denote a *hypothetical node* with data vectors $X = \bigcup_{j=1..N} X^j$. We call M_c a *centralised* node.

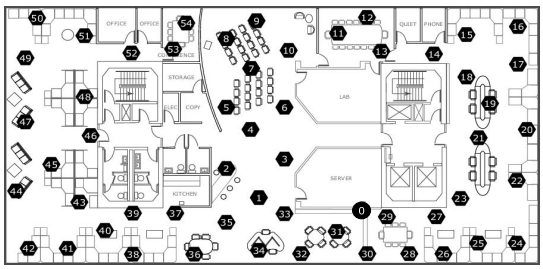


Figure 1. Sensor nodes in IBRL deployment. Nodes are shown in black with their corresponding node-IDs. Node 0 is the gateway node [10].

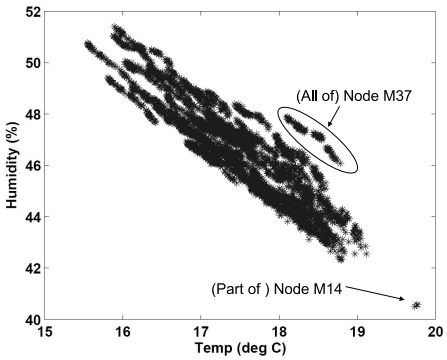
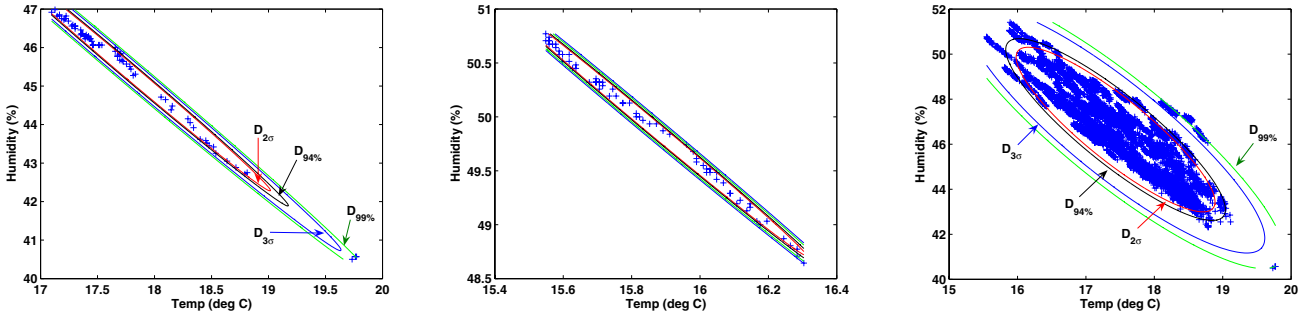


Figure 2. Scatter plot of centralised node M_c

In this paper we consider the IBRL data set obtained from 54 nodes, namely node IDs from 1 to 54, during the 4 hour period collected on 1th March 2004 during the time interval from 00:00am to 03:59am. While the lab in Figure 1 has a total of 55 sensors (including the gateway node), only 52 of them provided data during the four hour time window examined in this paper. Nodes M_5 and M_{15} did not contain any data during this time window. We consider two features, namely temperature and humidity, and we call this data set the *IBRL Data*. Figure 2 shows scatter plot of the data vectors at centralised node M_c. We do not provide scatter plots of other nodes due to space constraints.

In Figure 2, note especially that some data vectors differ significantly from the mass of data in the center. A small collection of data vectors can be seen in the lower right hand corner of the graph in Figure 2. These points come from node M_{14}. These vectors are good candidates to be anomalies; we call these points A^{14}. A^{14} is only a small portion of the node data X^{14}, $A^{14} \subset X^{14}$. Another collection of data vectors visually apparent in Figure 2 come from node M_{37}. Specifically we refer to the three "islands"



(a) M_{14} (b) M_{50} (c) M_c

Figure 3. Ellipses at nodes (a) M_{14}, (b) M_{50} and (c) M_c

marked M_{37} in Figure 2. While A^{14} is but a small portion of M_{14}, it appears that *all* of M_{37} are good candidates for anomalies. Thus it appears that $A^{37} = X^{37}$.

2.1 Statistical Analysis for IBRL Data

We perform multivariate statistical analysis on this data to see whether we can detect the anomalies mentioned above. In order to ease the notation burden, we drop the *superscript j* that denotes the *data vectors* at sensor node M_j, but we keep superscript *j* for all other quantities associated with node *j*. For each node we compute the following [16]:

- Sample mean vector $m_j = \{m_k^j : k = 1...d\}$, and $m_k^j = \frac{1}{n_j}\sum_{i=1}^{n_j} x_{ik}$
- Sample covariance matrix $S_j = \{s_{lk}^j : l,k = 1...d\}$, trace $tr(S_j)$ and determinant $|S_j|$, where $s_{lk}^j = \frac{1}{n_j - 1}\sum_{i=1}^{n_j}(x_{li} - m_l)(x_{ki} - m_k)$
- Eigen decomposition [16] of the sample covariance matrix $S_j = P_j \Lambda_j P_j^T$, where P_j is a 2×2 matrix with column vectors as the eigenvectors, and Λ_j is a 2×2 diagonal matrix with eigenvalues $\{\lambda_k^j : k = 1, 2\}$ as diagonal elements. We shall assume $\lambda_1^j \geq \lambda_2^j > 0$ for each node pair.
- Mahalanobis distances [16] of the data vectors $D_j = \{D_i^j : i = 1...n_j\}$, where $(x_i - m_j)S_j^{-1}(x_i - m_j)^T = (D_i^j)^2$ and S_j^{-1} is the inverse of the sample covariance matrix S_j. We use Mahalanobis distance because it accounts for linear correlation between pairs of features, and we know that all data vectors having the same Mahalanobis distance lie on a hyperellipsoidal surface.

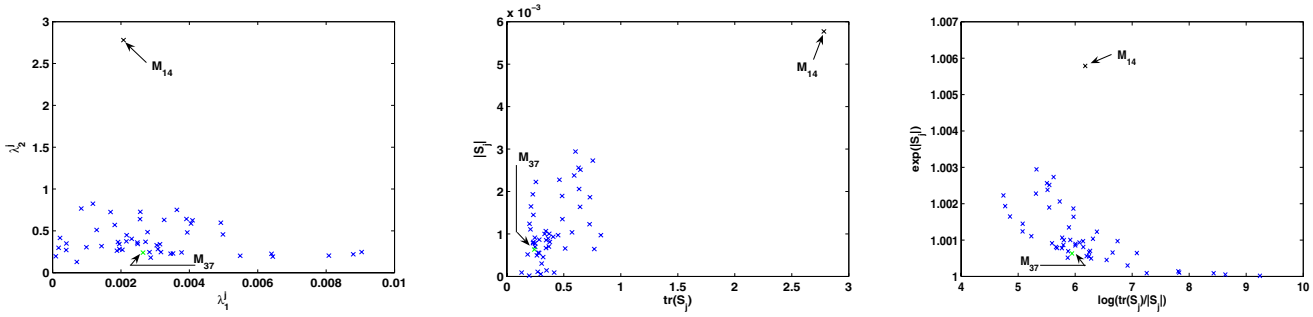
If we adopt some *threshold* Mahalanobis distance, it defines a hyperellipsoidal boundary which encompasses some fraction of data vectors at a node. A chosen ellipsoid can be uniquely represented by its center (mean vector) m_j, covariance matrix S_j and a *threshold* (known as the effective radius). We use an ellipse as it is capable of adusting to many shapes, depending on the eigen structure of the covariance matrix, from a spherical structure to a linear structure.

Having adopted level sets of the ellipse defined by the eigenvalue-eigenvector structure of the sample covariance matrix at any node, it only remains to choose a particular level set (an ellipse of constant effective radius) to define the anomalies at a node. Several definitions appeal to us.

- *94% cardinality anomalies*: Consider the threshold Mahalanobis distance $D_{94\%}^j$ beyond which 6% of the data vectors (i.e.,$\lfloor 6n_j/100 \rfloor$) lie further away than $D_{94\%}^j$. We define the 94% cardinality anomalies as those data vectors that lie further away than $D_{94\%}^j$. Similarly, the *99% cardinality anomalies* are those 1% of the data vectors that lie further away than $D_{99\%}^j$.
- 2σ *anomalies*: These are the data vectors that lie further away from the threshold Mahalanobis distance $D_{2\sigma}^j = 2$. Similarly 3σ *anomalies* are computed using $D_{3\sigma}^j = 3$.

Henceforth, we will indicate the observations at M_j that lie *outside* the ellipse $(x_i - m_j)S_j^{-1}(x_i - m_j)^T = (D_*^j)^2$ as A_*^j, where $(*)$ can be 94%, 99%, 2σ or 3σ. Thus, for example, $A_{2\sigma}^{14}$ are the 2σ elliptical anomalies at node M_{14}.

Table 1 shows the results of statistical analysis for the IBRL data set for each node $M_1, M_2, ..., M_{54}$ (except M_5 and M_{15}) and the centralised node M_c. Figures 3(a) and 3(b) show the above defined ellipses for the data vectors of nodes M_{14} and M_{50} respectively. For node M_{50}, the four ellipses are very similar, indicating observations that are very compact. For node M_{14}, all the ellipses except $D_{99\%}^{14}$ separate the A^{14} anomalies in the figure. In other words, $A_{94\%}^{14} = A_{2\sigma}^{14} = A_{3\sigma}^{14} = A^{14}$, but $A_{99\%}^{14} \neq A^{14}$. This



(a) λ_2^j Vs λ_1^j (b) $|S_j|$ Vs $tr(S_j)$ (c) $exp(|S_j|)$ Vs $log_e(tr(S_j)/|S_j|)$

Figure 4. Eigenvalues (λ_1^j, λ_2^j), determinant ($|S_j|$) and trace ($tr(S_j)$) of covariance matrix for each sensor node except nodes M_5, M_{15} and M_c

happens because M_{14} has only $n_{14} = 72$ points, so $A^j_{99\%}$ can contain only $1\% \approx 1$ of the 3 points in A^{14}. Figure 3(c) shows the ellipses for the centralised node M_c, and the ellipse $D^c_{3\sigma}$ clearly separates the A^{14} anomalies and A^{37} anomalies.

Figure 5 shows the normal and anomalous data vectors identified for the hypothetical centralised node M_c. It has four plots for the four scenarios of anomaly detection, namely (i) 94% cardinality anomalies ($D_{94\%}$) (ii) 2σ anomalies ($D_{2\sigma}$) (iii) 99% cardinality anomalies ($D_{99\%}$) (iv) 3σ anomalies ($D_{3\sigma}$). The blue dots represent the data vectors that are identified as normal and the red stars represents the identified anomalous data vectors. $A^c_{3\sigma}$ captures both node (A^{14}) and network (A^{37}) anomalies without false detection.

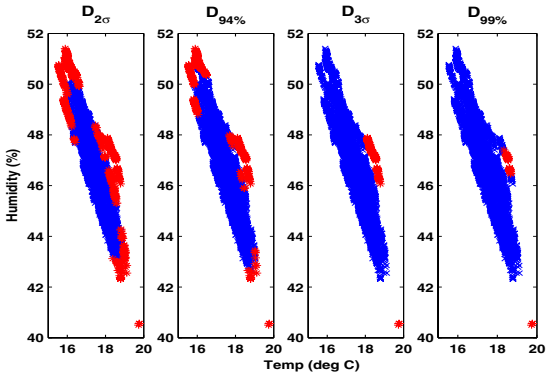


Figure 5. Scatter plots for M_c using various anomaly detection scenarios: 2σ anomalies ($D_{2\sigma}$), 94% cardinality anomalies ($D_{94\%}$), 3σ anomalies ($D_{3\sigma}$) and 99% cardinality anomalies ($D_{99\%}$). Blue dots represent *normal* data and red stars represents *anomalous* data.

2.2 Types of Anomalies in Distributed Sensor Networks

So far, we have used the ellipses $(x_i - m_j)S_j^{-1}(x_i - m_j) = (D^j_*)^2$ to isolate sets of elliptical anomalies A^j_* at an individual node M_j. When we apply this strategy to M_c, however, we see *two* types of anomalies: A^{14}, which are anomalous points *at a node*; and A^{37}, which is an anomalous node *in the network*. This leads to the idea that distributed sensor networks have different types of anomalies. We will call node anomalies such as A^{14} *first order anomalies*; and network anomalies such as A^{37} *second order anomalies*. Figure 5 shows that D^c_* may identify both first and second order anomalies, while we can only hope to find first order anomalies at a single node. This is one reason to investigate the "centralised" node M_c.

Unfortunately, building M_c for second order anomaly detection requires transmission of all $NN = \sum_{j=1}^{N} n_j$ data vectors from the nodes $\{M_j\}$ to a centralised processor, and this entails a heavy communication burden on the network.

We need an alternative to the method for second order detection represented in Figure 5. We are currently investigating a number of possibilities, one of which is to use the eigenstructure at each node to represent it. Figures 4(a), 4(b) and 4(c) are scatter plots, respectively of the pairs $\{(\lambda_1^j, \lambda_2^j)\}$, $\{(|S_j|, tr(S_j))\}$ and $\{(exp(|S_j|), log_e(tr(S_j)/|S_j|))\}$. Plots of this kind represent each node in the network by new features, and are thus capable of revealing second order anomalies. Unfortunately the first order anomalies at M_{14} are so severe that they cause M_{14} to look like a second order anomaly in Figures 4(a), 4(b) and 4(c). This begs the question: at which point does the severity of a first order anomaly cause us to declare the whole node faulty?.

Plots such as Figures 4(a), 4(b) and 4(c) are useful *only* for second order detection, and further, do *not* isolate A^{37}

from the other nodes. Thus, we need different features, or a different method of using the node parameters we have, $\{m_j, S_j, \lambda_1^j, \lambda_2^j\}$, to replace the anomalies represented by Figure 5. Before embarking on a quest for such a representation, we may ask: is A^{37} really a second order anomaly, or is this conclusion simply an artifact of our definitions of elliptical anomalies?

Referring back to Figure 1, we see that M_{37} is closer to the door of the kitchen than any other node in the network. We conjecture that the physical location of M_{37} is responsible for the elevation of its (Temperature, Humidity) pairs which in turn causes it to appear as a second order anomaly in Figure 5. We expect higher humidity and temperature around the kitchen area, which would explain this anomaly. As for A^{14}, these points are clearly first order anomalies at M_{14}, and our method successfully isolates them in all but the 99% case.

The authors of the IBRL deployment [7] observed that nodes $M_{11}, ..., M_{20}$ have seen the lowest percentage of successful transmissions, and they believe that the corner of the lab where these nodes are located is subjected to unusual interference. We believe this may be the cause for the anomalies A^{14} at node M_{14}.

3 Conclusions and Future Research

In this paper we used a real sensor network data set deployed at the Intel Berkeley Research Laboratory (IBRL) and analysed a four hour period of data for fifty-four nodes. We performed several types of multivariate statistical analysis on this data and developed formal definitions for *elliptical anomalies* in the *IBRL data*.

We conclude with a short list of open questions suggested by this initial analysis of the IBRL data. How will the elliptical anomaly analysis hold up over time? We will divide the remaining 20 hours of 1^{st} March 2004 into 4 hour windows to study this question. Can we apply the definitions of elliptical anomalies to plots such as Figures 4(a), 4(b) and 4(c) to identify second order anomalies? At what point do first order anomalies at a node push that node to become a second order anomaly in the network? If we assume normality for the observations at each node, can we substitute statistical theory for the method of Figure 5 to detect second order anomalies? If we use all $d = 4$ measurements for the IBRL nodes, will the results be the same, different, or contradictory? Our immediate plan is to attack one or more of these open questions.

Acknowledgment

We thank the ARC Research Network on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), and DEST International Science and Linkage Grant. This work was supported by the Australian Research Council (ARC).

References

[1] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: A survey," *Comp. Networks*, vol. 38, no. 4, pp. 393–422, 2002.

[2] A. Perrig *et al.*, "Security in wireless sensor networks," *CACM*, vol. 47, no. 6, pp. 53–57, 2004.

[3] N. R. Prasad and M. Alam, "Security framework for wireless sensor networks," *Wireless Personal Comm.*, vol. 37, no. 3-4, 2006.

[4] V. Barnett and T. Lewis, *Outliers in Statistical Data*. John Wiley and Sons, 3rd ed., 1994.

[5] G. J. Pottie and W. J. Kaiser, "Wireless integrated network sensors," *CACM*, vol. 43, no. 5, pp. 51–58, 2000.

[6] R. Szewczyk *et al.*, "Habitat monitoring with sensor networks," *CACM*, vol. 47, no. 6, pp. 34–40, 2004.

[7] P. Buonadonna *et al.*, "Task: sensor network in a box," in *Proc. of Second European Workshop on Wireless Sensor Networks*, pp. 133–144, 2005.

[8] P. Sikka *et al.*, "Wireless ad hoc sensor and actuator networks on the farm," *IPSN*, pp. 492– 499, 2006.

[9] S. Kininmonth *et al.*, "Sensor networking the great barrier reef," *Spatial Science Qld journal*, pp. 34–38, Spring 2004.

[10] 2006, "http://db.lcs.mit.edu/labdata/labdata.html," in *[online]*, Accessed on 07/09/2006.

[11] C. Loo *et al.*, "Intrusion detection for routing attacks in sensor networks," *Inl. Journal of Distributed Sensor Networks*, vol. 2, no. 4, pp. 313–332, Oct-Dec 2006. ISSN 1550-1329.

[12] S. Subramaniam *et al.*, "Online outlier detection in sensor data using non-parametric models," in *VLDB*, pp. 187–198, VLDB Endowment, 2006.

[13] E. Ngai *et al.*, "On the intruder detection for sinkhole attack in wireless sensor networks," in *ICC'06*, 2006.

[14] S. Rajasegarar *et al.*, "Distributed anomaly detection in wireless sensor networks," in *ICCS'06*, 2006.

[15] S. Rajasegarar *et al.*, "Quarter sphere based distributed anomaly detection in wireless sensor networks," in *ICC'07*, 2007.

[16] R. A. Johnson and D. W. Wichern, *Applied Multivariate Statistical Analysis*. Printice Hall, 1982.

Table 1. Statistics of the IBRL data of sensor nodes (except node M_5 and M_{15}). $D_{2\sigma} = 2$ and $D_{3\sigma} = 3$

Node	n_j	λ_1^j $\times 10^{-3}$	λ_2^j $\times 10^{-3}$	$\lvert S_j \rvert$ $\times 10^{-3}$	$tr(S_j)$ $\times 10^{-3}$	m_1^j	m_2^j	$D_{94\%}^j$	$A_{94\%}^j$	$A_{2\sigma}^j$	$D_{99\%}^j$	$A_{99\%}^j$	$A_{3\sigma}^j$
M_1	97	2.834	245.3	0.695	248.1	18.1	44.3	2.030	6	7	2.717	1	0
M_2	125	3.775	241.8	0.913	245.6	18.5	44.6	2.275	7	15	3.044	1	2
M_3	119	2.87	180.0	0.517	182.9	18.4	44.0	2.146	7	9	2.590	1	0
M_4	115	6.403	226.3	1.449	232.7	18.8	43.9	2.030	7	9	2.611	1	1
M_6	86	8.794	219.8	1.933	228.6	18.3	44.2	2.222	5	8	2.733	1	0
M_7	151	9.039	246.2	2.225	255.3	18.4	43.8	2.065	9	13	2.575	2	2
M_8	102	5.488	201.9	1.108	207.4	18.1	44.4	2.028	6	8	2.232	1	1
M_9	117	8.082	203.9	1.648	212.0	18.2	45.4	2.068	7	9	2.376	1	0
M_{10}	105	6.442	192.4	1.239	198.8	18.1	45.4	2.176	6	9	2.516	1	0
M_{11}	108	2.559	640.2	1.638	642.8	17.3	48.0	2.257	6	10	2.821	1	0
M_{12}	50	0.841	767.0	0.645	767.8	17.0	47.4	2.306	3	7	2.609	0	0
M_{13}	82	1.289	510.6	0.658	511.9	17.4	47.2	2.236	5	11	3.131	1	2
M_{14}	**72**	**2.076**	**2779.7**	**5.771**	**2781.7**	**17.8**	**45.4**	**2.252**	**4**	**9**	**3.405**	**1**	**3**
M_{16}	129	1.179	824.2	0.972	825.4	17.0	48.0	2.577	8	12	2.899	1	0
M_{17}	131	1.697	724.9	1.230	726.6	17.6	45.4	2.092	8	11	2.872	1	1
M_{18}	181	3.917	641.5	2.513	645.4	18.0	44.6	2.011	11	14	3.501	2	4
M_{19}	119	2.78	485.0	1.348	487.8	17.9	44.7	1.954	7	7	2.600	1	1
M_{20}	163	1.82	570.0	1.038	571.9	17.5	47.1	2.055	10	14	2.355	2	1
M_{21}	152	4.094	625.4	2.560	629.5	18.1	44.2	2.203	9	13	3.150	2	3
M_{22}	174	4.923	597.4	2.941	602.3	17.4	45.8	2.158	10	16	2.731	2	2
M_{23}	179	4.05	587.3	2.378	591.3	18.2	44.5	1.932	11	10	3.147	2	3
M_{24}	122	2.566	726.9	1.866	729.5	17.4	46.2	1.966	7	7	4.006	1	2
M_{25}	153	3.94	481.1	1.895	485.0	17.3	45.9	2.256	9	14	2.722	2	1
M_{26}	141	3.265	630.8	2.059	634.0	17.1	48.6	2.187	8	12	2.649	1	1
M_{27}	112	4.983	456.8	2.277	461.8	17.5	47.2	2.180	7	10	3.168	1	3
M_{28}	163	3.635	750.8	2.729	754.4	16.4	50.2	2.107	10	17	2.593	2	0
M_{29}	115	1.885	262.8	0.495	264.7	17.3	47.1	2.494	7	10	2.835	1	0
M_{30}	93	3.083	281.0	0.866	284.1	16.8	48.9	2.077	6	9	3.074	1	2
M_{31}	151	3.454	227.0	0.784	230.5	17.4	47.3	2.135	9	13	2.447	2	1
M_{32}	69	3.523	230.0	0.810	233.5	17.2	47.3	1.941	4	4	3.429	1	2
M_{33}	49	2.481	360.8	0.895	363.3	18.0	44.7	2.196	3	4	2.400	0	0
M_{34}	79	3.046	328.6	1.001	331.6	17.4	47.2	2.006	5	6	2.495	1	0
M_{35}	149	3.17	245.7	0.779	248.9	18.3	46.2	2.353	9	15	2.996	1	1
M_{36}	141	1.959	281.8	0.552	283.7	17.7	47.7	2.063	8	11	2.533	1	0
M_{37}	**137**	**2.646**	**239.3**	**0.633**	**242.0**	**18.4**	**47.2**	**2.340**	**8**	**11**	**2.535**	**1**	**0**
M_{38}	127	3.141	339.6	1.067	342.7	17.6	45.8	2.025	8	9	3.422	1	2
M_{39}	82	2.042	273.8	0.559	275.8	18.1	46.3	1.881	5	4	2.368	1	1
M_{40}	111	2.49	343.2	0.855	345.7	17.6	46.6	1.870	7	3	3.554	1	3
M_{41}	120	1.953	342.2	0.668	344.2	17.2	47.2	2.312	7	13	2.530	1	0
M_{42}	114	2.312	404.4	0.935	406.7	16.2	50.3	2.077	7	9	2.382	1	0
M_{43}	136	2.721	369.3	1.005	372.0	17.1	47.2	2.113	8	9	3.274	1	3
M_{44}	149	1.916	366.9	0.703	368.8	16.3	49.4	2.145	9	14	3.050	1	2
M_{45}	180	2.167	448.1	0.971	450.2	16.7	47.5	2.177	11	18	2.988	2	2
M_{46}	188	2.16	375.1	0.810	377.2	16.9	47.3	2.164	11	17	2.749	2	0
M_{47}	165	1.434	317.3	0.455	318.8	16.6	49.2	1.996	10	10	2.854	2	1
M_{48}	187	0.991	304.5	0.302	305.5	17.0	46.9	2.132	11	18	2.319	2	0
M_{49}	115	0.406	348.6	0.142	349.0	16.1	48.6	2.116	7	11	2.453	1	0
M_{50}	74	0.219	415.4	0.091	415.6	15.9	49.9	2.231	4	8	2.667	1	0
M_{51}	122	0.4	270.6	0.108	271.0	17.1	46.3	2.208	7	16	2.539	1	0
M_{52}	87	0.711	129.0	0.092	129.8	17.1	46.9	2.198	5	9	2.549	1	0
M_{53}	81	0.097	196.5	0.019	196.6	16.5	48.3	2.159	5	7	2.654	1	0
M_{54}	93	0.178	297.0	0.053	297.2	16.4	48.4	2.240	6	9	3.159	1	2
M_c	6362	106.311	3762.0	399.944	3868.3	17.4	46.6	2.209	382	658	3.378	64	140