Sensors & Transducers, Vol. 175, Issue 7, July 2014, pp. 88-94

www.sensorsportal.com

Sensors & Transducers

© 2014 by IFSA Publishing, S. L.
http://www.sensorsportal.com

Improving Accuracy of Dempster-Shafer Theory Based Anomaly Detection Systems

[1, 2] Ling Zou, [2] Liming Zheng, [2] Xianghua Zeng

[1] State Key laboratory of Virtual Reality Technology and Systems, Beihang University, Beijing 100191, China

[2] School of Electronic Science and Engineering, National University of Defense Technology, Changsha 410073, China

[1] Tel.: 0731-84575763

[1] E-mail: zouling@vrlab.buaa.edu.cn

Received: 24 March 2014 /Accepted: 30 June 2014 /Published: 31 July 2014

Abstract: While the Dempster-Shafer theory of evidence has been widely used in anomaly detection, there are some issues with them. Dempster-Shafer theory of evidence trusts evidences equally which does not hold in distributed-sensor ADS. Moreover, evidences are dependent with each other sometimes which will lead to false alert. We propose improving by incorporating two algorithms. Features selection algorithm employs Gaussian Graphical Models to discover correlation between some candidate features. A group of suitable ADS were selected to detect and detection result were send to the fusion engine. Information gain is applied to set weight for every feature on Weights estimated algorithm. A weighted Dempster-Shafer theory of evidence combined the detection results to achieve a better accuracy. We evaluate our detection prototype through a set of experiments that were conducted with standard benchmark Wisconsin Breast Cancer Dataset and real Internet traffic. Evaluations on the Wisconsin Breast Cancer Dataset show that our prototype can find the correlation in nine features and improve the detection rate without affecting the false positive rate. Evaluations on Internet traffic show that Weights estimated algorithm can improve the detection performance significantly.
Copyright © 2014 IFSA Publishing, S. L.

Keywords: Anomaly detection system, Dempster-Shafer theory, Feature, Weight, Correlation.

1. Introduction

Anomaly detection refers to the problem of identifying patterns in audit data generated from monitoring the system's activities that do not conform to expected behavior. These non-conforming patterns are often referred to anomalies. Anomaly detection System (ADS) finds extensive use in a wide variety of applications such as fraud detection for credit cards, health care, and intrusion detection for cyber-security. While ADS have been shown to be effective in protecting our system against attacks, there are some issues with them. The issues include high false alarm rate, limited types of anomalies the system can detect, and that such system can't perform real-time detection. To improve the detection accuracy of ADS, some scholars try to apply Dempster-Shafer Theory of Evidence (D-S) to ADS [1, 2]. D-S based ADS have the ability to add the notions of uncertainty and ignorance in the system and the quantitative measurement of the belief and plausibility in our detection results. It is an

effective attempt to use D-S evidence theory to resolve uncertainty inferring problem of anomaly detection.

While D-S based ADS is an effective solution to detection anomalies, there are some drawback of D-S based ADS:

First, the D-S combining rule implies that we trust observers equally. This assumption normally does not hold in distributed-sensor ADS that spans domains. The same kind of sensors installed at different locations may have different detection capabilities since that raw anomalies captured by these sensors are different. The different kinds of sensors detect the same type of anomalies with a different level of accuracy. Moreover, many features have been suggested as candidates for anomaly detection, but there has been little work in understanding the detection capabilities provided by a set of features used in conjunction with one another.

Second, the D-S is based on the hypothesis that observers are independent. This assumption normally does not hold in multi-sensor ADS that spans features. For each future observation, we compute an anomaly scores: *score*=|*Observation-Mean*|/*Stddev*. This score captures how far away from the mean value a particular observation is, expressed relative to the standard deviation. Anomaly scores time series of some features show strong correlations. Some others show moderate correlation or no correlation. Therefore, it is not clear if the different features proposed so far complement each other in their detection capability or if they provide redundant functionality.

In order to overcome these drawbacks, some algorithms have been proposed in this paper. It can achieve better detection performance.

2. Case Study

2.1. Correlations in Anomaly Deviation Scores

Multi-sensor detection or distributed-sensor detection such as D-S based ADS is proposed to combine data from multiple and diverse sensors and sources in order to make inferences about anomalies. However, D-S combining evidence theory regards all kinds of source data as the same importance and neglects the correlation of data. D-S can make correct detection if all observes are independent. But when observes are correlative, there may lead to false alert.

In this case study, we suppose there are three persons: expert, practiced worker and student worker. They diagnose the same fault. Suppose A is sensor error, B is anomaly, and C is normal. The basic probability of expert (*e*): $m_e(A)$=0.7, $m_e(\Omega)$=0.3. Due to the authority of expert, the others have the same diagnosis with him: practiced worker (*p*): $m_p(A)$=0.7, $m_p(\Omega)$=0.3, student worker (*s*): $m_s(A)$=0.7, $m_s(\Omega)$=0.3. The result of instrument test: $m_i(B)$=0.7, $m_i(\Omega)$=0.3. According to D-S combining rule, we fuse their diagnosis results: $m(A)=m_e(A) \oplus m_p(A) \oplus m_s(A) \oplus m_i(A)$=0.273, $m(B)=m_e(B) \oplus m_p(B) \oplus m_s(B) \oplus m_i(B)$=0.063, $m(\Omega)=m_e(\Omega) \oplus m_p(\Omega) \oplus m_s(\Omega) \oplus m_i(\Omega)$=0.027, $m(\Phi)$=0. The disagreement coefficient of evidence is K=0.637. Standardize the focal element by divided coefficient (1-K): $m(A)$=0.76, $m(B)$=0.17, $m(\Omega)$=0.07. Then the confidence of A is [0.76, 0.83], and the confidence of B is [0.17, 0.24].

With the support of practiced worker and student worker, though the expert is uncertainty of his diagnosis, the result is certainty. Though the result of instrument test is opposition with the expert's diagnosis, the fusion result is the same with the export. According to the D-S combining theory, the result of fusion is always decided by majority supports. It is obviously that the fusion result is unreliable if evidences are fused regardless of the correlation between them.

2.2. Detection Capabilities Difference

Different kinds of sensors or ADS (we use sensor and ADS exchangeable) which detect the same type of anomalies may do so with a different level of accuracy. Sensors usually use a single metrics which results in that they are better in detecting certain types of attacks and let others unaware.

The network traffic anomaly detection is fine case. Our case study is based on 24 *h* traffic traces published by MAWI [3]. The MAWI traffic traces are collected from the WIDE backbone networks since 1999. Traffic traces used in this case study were captured at a trans-Pacific link (sample point-F, 150 Mbps link) between Japan and the United States on 2008.03.19. The 24 *h* long traces contain more than 1 M unique IP addresses and various kinds of anomalies indicated by alphabetical labels in Fig. 1 (Some anomalies span multiple windows). Therefore, those traffic traces have strong representation. Moreover, this traffic traces have used in a lot of papers to evaluate ADS [4].

In this case study, we focus on network-based ADS: EWMA, Entropy [5], KL [6], OCSVM [7]. Most of these detectors are quite popular and used frequently for performance comparison and benchmarking in traffic anomaly detection. Fig. 1 shows the anomaly scores time series values over the entire *24 h* trace. The KL based and OCSVM based ADS detect the anomaly B with high accuracy but detect the anomaly A with moderate accuracy. The EWMA based ADS detection the anomaly A with high accuracy but detect the anomaly B with very low accuracy. We would therefore expect to place greater confidence in the anomaly B generated by the KL based and OCSVM based ADS but have less confidence in its reported the anomaly A. In contrast, we would trust more on the anomaly A generated by the EWMA based ADS.

This figure also shows correlations between the time series of different anomaly scores. The KL

based anomaly scores and OCSVM based anomaly scores appear strongly correlation. Additionally, we observe that many of the spikes and deviations in the time series plots are also highly correlated.

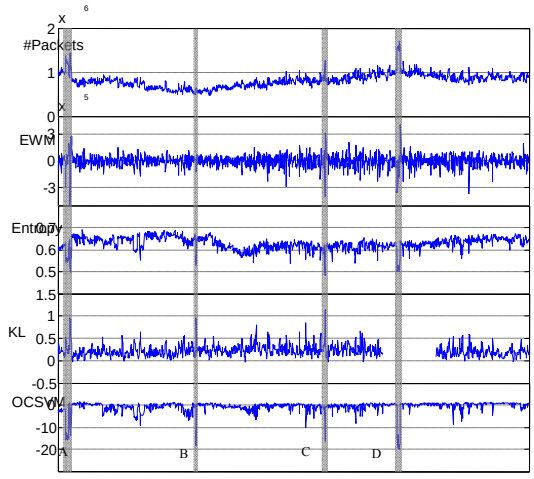

Fig. 1. Time series of anomaly scores about four traffic anomaly detection systems.

3. Architecture and Algorithms

3.1. System Architecture

The architecture of our proposed system is demonstrated in Fig. 2. There are various ADS deployed on actual environment and the different systems may use different data formats and features. Features Selection Algorithm is used to select some suitable ADS or features to detection anomaly. The selected ADS uses training process to derive thresholds from the training data, and detects an event as normal of abnormal based on the observed anomaly scores. The *bpa* functions are built based on these thresholds for the purpose of assigning mass values. The data from various ADS are processed and set to corresponding *bpa* assignment functions. The mass values for each hypothesis are generated and sent to D-S combination component. The component assigns a weight to every evidences according to the detection accuracy of them producer. The component uses the weighed Dempster's rule of combination to combine all mass values. Then the component generates the overall mass values for each hypothesis. We can determine whether there is an anomaly or not according to these results.

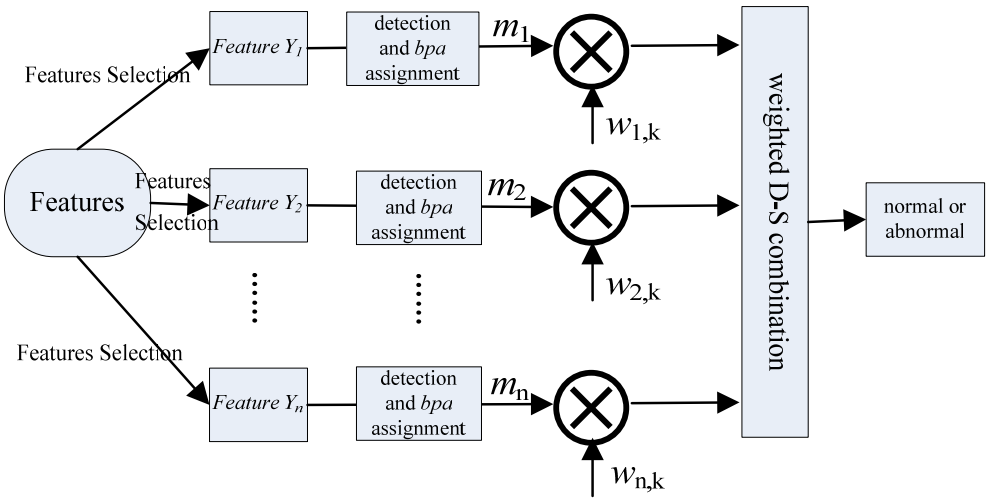

Fig. 2. System architecture.

3.2. Features Selection Algorithm

Suppose there are N sensors deployed. Each sensor has only one feature. There are T measured values collected from T different times. We set $X_{N\times T}=(X_1,X_2,\ldots,X_T)\in R^T$. Then the correlation among these features can be described by the dependence or independence of random variables.

In order to make the computation easier, we suppose the distribution of these random variables are Gaussian distribution. Then the distribution of $X_{N\times T}$ is regarded as multivariate Gaussian Graphical Models (GGM).

Finding the correlation in data is transformed into finding the conditional independence among random variables in GGM. Moreover, the precision matrix M encodes all the conditionally independent or dependent relations among all random variables. The algorithm proposed in [8] is adopted to obtain the estimation of the precision matrix M. Therefore, dependence or independence of random variables is given by GGM. When there is dependence between two or more variables, the variable with the biggest weight is selected. A group of features according to the selected variables are the used to detection anomaly.

3.3. Weights Estimated Algorithm

Suppose U is frame of discernment which is a finite set about mutually exclusive hypotheses. ADS focus on whether there is an anomaly, so we define $U_i=\{A_i,\neg A_i\}$ in every window i, and A_i is the hypotheses that there is an anomaly in this window and $2^{U_k}=\{\varnothing,\{A_k\},\{\neg A_k\},\{A_k,\neg A_k\}\}$ denotes their power set. The purpose of D-S theory is to infer the most probable finally state of system from some observations evidence, which we do not have an explicit model. We use the basic probability assignment *bpa* to measure the belief of the evidences and the belief function and plausibility function to measure the uncertainly of propositions. The *bpa* is defined as Eq. 1:

$$m\colon 2^U \rightarrow [0,1], \text{ and } m(\varnothing)=0,\ \sum_{A\subseteq U} m(A)=1, \tag{1}$$

The more details of D-S evidence theory can be found in [1] and [2].

We add a weighted to every ADS, and then can better to solve the problem of evidence conflict and improve the accuracy of detection [2]. In order to evaluate the effectiveness or accuracy of each detection systems for the final detection, the information gain [9] is introduced. In this context, the anomaly scores of every ADS defined as attributes and we use information gain as a measure of the effectiveness of an attribute in classifying the traffic data. Information gain denoted by *Gain*(*S*, *A*) is the expected reduction in entropy caused by classifying the samples according to this attribute. *Gain*(*S*, *A*) of an attribute *A* relative to a collection of examples *S* is defined as the following equation:

$$Gain(S,A)\equiv Entropy(S)-\sum_{v\in Values(A)}\frac{|S_v|}{|S|}Entropy(S_v), \tag{2}$$

Values(*A*) is the set of all possible values for attribute *A*, and S_v is the subset of *S* for which attribute *A* has value *v*(i.e. $S_v=\{s\in S|A(s)=v\}$). The first term is just the entropy of the original collection *S*, and the second term is the expected value of the entropy after *S* is classified using attribute *A*. The expected entropy described by this second term is simple the sum of the entropies of each subset S_v, weighted by the fraction of samples that belong to S_v. *Gain*(*S*, *A*) is therefore the expected reduction in entropy caused by knowing the value of attribute *A*. In this paper, the weight of every ADS is assigned as the expected reduction entropy caused by classifies the training data according to the anomaly scores of them.

Suppose $m_1,m_2,\ldots,m_n$ is the *n* basic probability assignment of ADS, The weighted D-S theory provides a rule to combine them into a single and more informative hint, and $m=m_1\oplus m_2\oplus\cdots\oplus m_n$ denotes this combining, we define it as Eq. 3:

$$\begin{aligned} &\text{m}(\varnothing)=0,\\ &m(A)=K^{-1}\sum_{\cap_i A_i=A}\prod_{1\le i\le n}[m_i(A_i)]^{w_i}\\ &K=\sum_{\cap_i A_i\neq\Phi}\prod_{1\le i\le n}[m_i(A_i)]^{w_i}. \end{aligned} \tag{3}$$

If K=0, then there is contradictions between $m_i(A_i)$. So we merge the new evidence constantly and update the confidence of detection.

4. Experimental

We implemented the proposed system and applied it to one standard benchmark problems of the UCI dataset [10], Wisconsin Breast Cancer Dataset (*WBCD*), and the internet traffic dataset introduced in 2.2. The standard benchmark dataset are chosen to compare our approach with the performance of basic D-S and to investigate whether it is possible to achieve good results by choosing more suitable features and estimating the weights for each evidences. The internet traffic dataset is chosen, because it is in our interested application area.

4.1. Experiment for the *WBCD* Dataset

The *WBCD* dataset contains 699 observed items: 241 malignant items (abnormal data), and 458 benign items (normal data). It has nine features. All features are normalized integers in the range between 1 and 10. We used A, B, C, D, E, F, G, H and I to present the biological features: A: clump thickness, B: Uniformity of cell size, C: Uniformity of cell shape, D: marginal Adhesion, E: single epithelial cell size, F: bare nuclei, G: bland chromatin, H: Normal nucleoli, and I: Mitoses. There are 16 items which contains a single missing attribute value. The unavailable values are not combining.

In this experiment, we define the function of *bpa* as Eq. 4:

$$\begin{cases} m(A_k)=(1+e^{(\overline{Y}_k-threshold)})^{-1}\\ m(\neg A_k)=1-m(A_k) \end{cases}, \tag{4}$$

where $\overline{Y}_k$ is the standardized anomaly scores

We use a training process to derive thresholds from the training data. The forepart 630 observed items are used as training data and the other 69 item are used as test data. The proportional distribution of normal vs. abnormal in the *WBCD* dataset is 65.5 % vs. 34.5. Therefore, the 413th small value of one feature is chosen as the threshold. If the *bpa* value of the 'abnormal' hypothesis is bigger than the *bpa*

value of the 'normal' hypothesis, then it is classified as abnormal; otherwise it is classified as normal.

All of the 699 data items are used to construct multivariate GMM. The output of the Features Selection Algorithm is that: A, B, D, E, F, G, H, I are a suitable group of features. The values of feature C are dependent of the value of feature B.

The weights of all of the eight selected features is show in the Table 1. The feature I give the smallest weight. The feature B give the biggest weight.

The result of detection accuracies when bombing all the nine features using the basic D-S is 97.6 %. The result of detection accuracies when bombing selected eight features using the proposed system is 98.1 %. Therefore, the proposed system is better than the D-S based ADS.

Table 1. The weights of nine features.

No.	Weight
A	0.122
B	0.137
D	0.122
E	0.127
F	0.130
G	0.129
H	0.121
I	0.112

4.1. Experiment for the Traffic Dataset

The internet traffic dataset had introduced in 2.2. Because those traces are taken on links used in real backbone networks, the ground truth is not always known about the ways and when for some specific events. The ADS proposed and involved in [11] are used to identify anomalies and carefully inspect the results. Although we cannot create ground truth of these datasets, it does mention several attacks. There are four abnormal periods on 2008.03.19 as show in Fig. 1.

In this experiment, we focus on network-based ADS: RRDtools, EWMA, Entropy, KL, OCSVM. Most of these detectors are quite popular and used frequently for performance comparison and benchmarking in the AD research community. The Entropy, KL and OCSVM are computed in the *dstport* feature.

Let $X(t) \in \mathbb{R}^n$,(X in short) be an n-dimensional random feature vector at time $t \in [0,t]$. There are two underlying states of a network, ω_k, i=0,1 in the simplest scenario, where ω_0=0 corresponds to normal state, and ω_1=1 corresponds to anomalous state. Detecting anomaly can be considered as deciding whether a given observation x of random feature vector X is a symptom of an underlying network state ω_0 or ω_1. Let f be the model for any given AD and ε is the threshold. $Y=f(X)$ is the output of this model which is named anomaly scores. When $|Y|>\varepsilon$, an alarm is reported. Due to space constraints, we do not proved detailed descriptions of evaluated ADs. Readers are referred to [5-7] for details of those ADs. For techniques operating on fixed-sized time windows, we use a window of 1 minute. All other parameters not mentioned in the paper are the same as those described in the ADS' respective papers.

We first run the Features Selection Algorithm in this dataset. The output is that: RRDtools, EWMA, Entropy, and KL. The values of OCSVM are dependent of the value of feature KL. The accuracy of OCSVM is better than KL, however, the compute complex of training OCSVM is very high. Then, The KL is selected for anomaly detection.

The weights of all of the four selected ADS is show in the Table 2. The RRDtools based ADS give the smallest weight. The KL based ADS give the biggest weight.

Table 2. The weights of four ADS.

ADS	Weight
RRDtools	0.081
EWMA	0.164
Entropy	0.373
KL	0.382

When come to traffic anomaly detection, a true positive alone is insufficient for a discussion of accuracy due to base-rate fallacy. A ROC (Receiver Operating Characteristics) curve is a graphical plot concerning the balance of the true positive rate (TPR) versus the false positive rate (FPR). ROC curves have been used as the defacto method to evaluate the accuracy of ADs. ROC curves are generated by applying a range of detection thresholds to any ADs' anomaly scores and then plotting the TPR versus the FPR for each threshold. These points make up a convex curve which is named the ROC curve. For a meaningful comparison, we normalize all of thresholds used in these five ADs so that they have the same absolute value. When we plot the ROC curve for D-S based ADS, we set the same threshold for all the selected ADS and this threshold is give to D-S based ADS. Therefore, the lower limit of threshold is located at (1,1) in the ROC space, and the upper limit is located at (0,0). Points that represent the optimum thresholds lie on the upper convex hull of the ROC curve near (0,1). An accurate ADs tends to draw the ROC curve toward the upper left corner in the ROC space. The broader an integral area of ROC curves is drawn, the more accurate a corresponding algorithm is. The integral area of the ROC curve is denoted as the area under curve (AUC).

For a comparative evaluation of anomaly detectors, we plot ROC for our algorithm by setting different values of false alarm and detection rate.

We run the four ADS, the basic D-S based ADS, and the proposed system on the internet traffic traces. The basic D-S based ADS fused the four ADS' result using the basic D-S theory. The result is show in the Fig. 3. The RRDtools based ADS given the poorest detection accuracy when using one ADS. The standard deviation of the packets number is very large in normal showing in Fig. 1. When we run the RRDtools based ADS, a larger threshold should be given to detect the anomaly B which leads to many false alerts. The OCSVM based ADS given the best detection accuracy when using one ADS. The anomaly scores series is flat in all windows. But, the ROC curve of Entropy and the ROC curve of KL are crossed. When we analyzed the detection process, we found that the KL based ADS is efficient in detection early anomaly in a long anomaly period and the Entropy based ADS is efficient in detection late anomaly in a long anomaly period.

As analysis in the previous, the basic D-S based ADS combining the results from four ADS should give the best performance. However the result is not. The basic D-S based ADS only given moderate accuracy. We found that RRDtools based ADS give many fault alerts with large basic probability value to the D-S engine. When we set the weight of RRDtools based ADS as 0.081, the performance is better than all of other ADS. Therefore, we achieve the conclusion that Weights Estimated Algorithm can improve detection accuracy significantly.

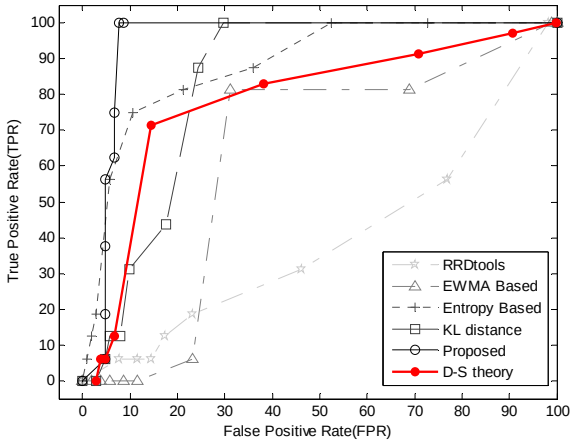

Fig. 3. ROC curves of six systems over Backbone traffic traces on 2008.03.19.

5. Related Works

Anomaly detection is a well-established field of research. D-S theory have the ability to add the notions of uncertainty and ignorance and the quantitative measurement of the belief and plausibility in our detection results. It is an effective attempt to use D-S evidence theory to resolve uncertainty inferring problem of anomaly detection. Magnus [12] use the model of multi-sensor to fusion the alerts which produced by various ADS. Qi [1] implement an ADS using D-S theory. They show that by combining multiple signals it is possible to achieve better results than by using a single signal in some benchmark problems. Dong [2] utilize the weighted D-S theory to fusion the various intrusion detection results, and improve the confidence of detection results. Alexandros [13] utilized the D-S theory to fuse outputs of local algorithms to detect physical layer jamming attacks in wireless networks. They found Dempster–Shafer algorithm when combined with the simple algorithms can increase their performance by more than 80 %. By employing D-S theory, Genge [14] detecting cyber-physical anomalies in NCIs by combine knowledge from the cyber and physical dimension of NCIs ADS.

6. Conclusions

While the Dempster-Shafer theory of evidence has been widely used in anomaly detection, there are some issues with them. In order to overcome these drawbacks, we propose improving by incorporating two algorithms. A group of suitable ADS were selected to detect and detection result were send to the fusion engine by employing Gaussian Graphical Models to discover correlation between some candidate features. A weighted Dempster-Shafer theory of evidence combined the detection results to achieve a better accuracy. We evaluate our detection prototype through a set of experiments that were conducted with *WBCD* dataset and real Internet traffic. Evaluations show that our algorithms can improve the detection performance significantly.

Acknowledgements

This research is partially supported by the National Natural Science Foundation of China (No. 61303265).

References

[1]. Qi Chen, U. Aickelin, Anomaly detection using the Dempster-Shafer method, in *Proceedings of the International Conference on Data Mining (DMIN'06)'*, Las Vegas, USA, 26-29 June 2003, pp. 232-240.

[2]. D. Yu, D. Frincke, Alert confidence fusion in intrusion detection systems with extended Dumpster-Shafer theory, in *Proceedings of the 43rd Annual Southeast Regional Conference (ACM-SE'05)*, Alabama, USA, 18-20 March 2005, pp. 142-147.

[3]. Measurement and Analysis on the WIDE Internet (MAWI) Working Group Traffic Archive, (http://mawi.wide.ad.jp/mawi/).

[4]. Y. Himura, K. Fukuda, K. Cho, H. Esaki, An evaluation of automatic parameter tuning of a statistics-based anomaly detection algorithm, *International Journal of Network Management*, Vol. 20, Issue 5, 2010, pp. 295-316.

[5]. G. Nychis, V. Sekar, D. G. Andersen, H. Kim, H. Zhang, An empirical evaluation of entropy-based traffic anomaly detection, in *Proceedings of the 8th ACM SIGCOMM Conference on Internet Measurement (IMC'08)*, Vouliagmeni, Greece, 20-22 October 2008, pp. 151-156.

[6]. M. Almgren, U. Lindqvist, E. Jonsson, D. Brauckhoff, X. Dimmitropoulos, A. Wagner, K. Salamatian, Anomaly extraction in backbone networks using association rules, in *Proceedings of the 9th ACM SIGCOMM Conference on Internet Measurement (IMC'09)*, Chicago, USA, 4-6 November 2009, pp. 28-34.

[7]. L. Zheng, P. Zou, Y. Jia, W. Han, Traffic anomaly detection in backbone networks using classification of multidimensional time series of entropy, *China Communications*, Vol. 9, Issue 7, 2012, pp. 108-120.

[8]. J. Friedman, T. Hastie, R. Tibshirani, Sparse inverse covariance estimation with the graphical lasso, *Biostatistics*, Vol. 9, Issue 3, 2008, pp. 432-441.

[9]. T. Mitchell, Machine Learning, *McGraw Hill*, 1997.

[10]. UC Irvine machine learning repository, (http://archive.ics.uci.edu/ml/).

[11]. R. Fontugne, P. Borgnat, P. Abry, K. Fukuda, MAWILab: combining diverse anomaly detectors for automated anomaly labeling and performance benchmarking, in *Proceedings of the ACM Conference on Emerging Networking Experiments and Technology (ConExt'10)*, Philadelphia, USA, 30 November – 3 December 2010, Article No. 8.

[12]. M. Almgren, U. Lindqvist, E. Jonsson, A multi-sensor model to improve automated attack detection, in *Proceedings of the International Symposium on Recent Advances in Intrusion Detection (RAID'08)*, Boston, USA, 15-17 September 2008, pp. 291-310.

[13]. B. Genge, C. Siaterlis, G. Karopoulos, Data fusion-based anomaly detection in networked critical infrastructures, in *Proceedings of the 43rd IEEE/IFIP International Conference on Dependable Systems and Networks (DSN'13)*, Budapest, Hungary, 24-27 June 2013, pp. 1-8.

[14]. A. G. Fragkiadakis, V. A. Siris, N. E. Petroulakis, A. P. Traganitis, Anomaly-based intrusion detection of jamming attacks, local versus collaborative Detection, *Wireless Communications and Mobile Computing*, Published online in Wiley Online Library (wileyonlinelibrary.com), 2013.

2014 Copyright ©, International Frequency Sensor Association (IFSA) Publishing, S. L. All rights reserved. (http://www.sensorsportal.com)