QUALITY AND RELIABILITY ENGINEERING INTERNATIONAL
Qual. Reliab. Engng. Int. 2007; **23**:545–553
Published online 7 November 2006 in Wiley InterScience (www.interscience.wiley.com). DOI: 10.1002/qre.830

Research

Attack–Norm Separation for Detecting Attack-induced Quality Problems on Computers and Networks

Nong Ye*,† and Qiang Chen

Department of Industrial Engineering, Arizona State University, Box 875906, Tempe, AZ 85287, U.S.A.

Cyber attacks on computer and network systems induce system quality and reliability problems, and present a significant threat to the computer and network systems that we are heavily dependent on. Cyber attack detection involves monitoring system data and detecting the attack-induced quality and reliability problems of computer and network systems caused by cyber attacks. Usually there are ongoing normal user activities on computer and network systems when an attack occurs. As a result, the observed system data may be a mixture of attack data and normal use data (norm data). We have established a novel attack–norm separation approach to cyber attack detection that includes norm data cancelation to improve the data quality as an important part of this approach. Aiming at demonstrating the importance of norm data cancelation, this paper presents a set of data modeling and analysis techniques developed to perform norm data cancelation before applying an existing technique of anomaly detection, the chi-square distance monitoring (CSDM), to residual data obtained after norm data cancelation for cyber attack detection. Specifically, a Markov chain model of norm data and an artificial neural network (ANN) of norm data cancelation are developed and tested. This set of techniques is compared with using CSDM alone for cyber attack detection. The results show a significant improvement of detection performance by CSDM with norm data cancelation over CSDM alone. Copyright © 2006 John Wiley & Sons, Ltd.

Received 5 September 2005; Revised 23 December 2005

KEY WORDS: cyber attack detection; attack–norm separation; chi-square distance monitoring; artificial neural network

*Correspondence to: Nong Ye, Professor of Industrial Engineering, Arizona State University, Box 875906, Tempe, AZ 85287, U.S.A.
†E-mail: nongye@asu.edu

Contract/grant sponsor: Air Force Office of Scientific Research; contract/grant number: F49620-99-1-0014

1. INTRODUCTION

Cyber attacks on computer and network systems induce system quality and reliability problems, and present a significant threat to the computer and network systems that we are heavily dependent on. Although many attack prevention mechanisms (firewalls, authentication and authorization, access control, etc.) exist, there will still be cyber attacks that break into computer and network systems due to the many known and/or unknown vulnerabilities of those complex systems. Therefore, cyber attack detection, which monitors system data and detects the attack-induced quality and reliability problems of computer and network systems caused by cyber attacks, is an important part of protecting computer and network systems from cyber attacks.

Usually there are normal user activities, or normal data (norm data), being processed by a computer or network when a cyber attack occurs. Hence, the observed system data are a mixture of attack data and norm data resulting from both attack activities and normal use activities when a cyber attack occurs. Ye and Farley[1] described a new approach to cyber attack detection, called attack–norm separation. This approach has the following steps:

(1) define the data model of a given attack (attack model) and the data model of a given norm (norm model);
(2) cancel or reduce the data effect of the norm from the observed data (the mixed data of both attack and norm activities when the attack occurs and the norm data only when there is no attack), using the norm model, to obtain the residual data; and
(3) detect and identify the attack in the residual data, using the attack model.

In contrast, other existing work on cyber attack detection is based mainly on two conventional approaches: signature recognition, and anomaly detection[1,2]. The signature recognition approach first builds the attack model representing the signature patterns of attacks, and then uses those signatures to find a match in the observed computer and network data for cyber attack detection. The anomaly detection approach first builds the norm model representing the norm behavior of computers and networks, and then considers large deviations of the observed computer and network data from the norm model as indicators of cyber attacks.

The two conventional approaches of signature recognition and anomaly detection use either the attack model or the norm model to directly analyze the mixed attack–norm data collected from computers and networks when an attack occurs, whereas our new attack–norm separation approach first cancels or reduces the effect of the norm data from the mixed attack–norm data and then performs the attack detection on the residual data. The mixed data or the presence of the norm data in the attack data may weaken or distort the characteristic captured either in the attack model or the norm model, thus lowering the detection accuracy (as shown in our previous study[3]). Hence, it is crucial to first cancel or reduce the data effect of normal activities using the norm model for an improved attack–norm data ratio before performing the attack detection. In contrast, the two existing approaches of signature recognition and anomaly detection do not perform norm data cancelation.

In this study, we investigate a technique of norm data cancelation and examine how the technique helps improve the detection performance of an anomaly detection technique, the chi-square distance monitoring (CSDM) method, which we presented in earlier issues of this journal[4,5] and also in other journals[2,6]. In the following sections of this paper, we first give a brief review of applying CSDM to cyber attack detection. We then present the technique of norm data cancelation. Finally, we present the testing results of CSDM with the norm data cancelation technique and CSDM alone.

2. APPLICATION OF CSDM TO CYBER ATTACK DETECTION

In this section, we first describe the computer and network data used in this study for cyber attack detection. Then we present CSDM and the application of CSDM to such computer and network data for cyber attack detection.

DOI: 10.1002/qre

2.1. Computer and network data

As in our previous studies[2–6], we use computer audit data, specifically basic security module (BSM) audit data of the Solaris operating system on Sun workstations. BSM is a security facility provided by the Solaris operating system to monitor the activities on a host computer and record security-related events. From the audit record for each event, we extract and use the information that indicates the type of audit event for cyber attack detection. There are 284 types of audit events defined in BSM for the Solaris 2.5 operating system.

In this study, we use the audit data generated in 2000 by the MIT Lincoln Laboratory under the sponsorship of the Defense Advanced Research Agency (DARPA) and the Air Force Research Laboratory (AFRL) for evaluating intrusion detection systems (http://ideval.ll.mit.edu/). This data set is called the DARPA 2000 data in this paper. There are two sets of BSM audit data collected from two UNIX-based host machines (Sun SPARC 10 Workstation with Solaris 2.5), 'Mill' and 'Pascal'. The settings of UNIX machines 'Mill' and 'Pascal' and the normal activities on them are similar. There are 104 907 events in the 'Mill' data set. Among them, there are 36 036 attack events and all others are normal events. There are 114 082 events in the 'Pascal' data set. Among them, there are 32 327 attack events and all others are normal events. In this study, the data collected from 'Mill' are used as the training data and the data collected from 'Pascal' are used as the testing data.

We obtain an observation data vector, $(x_{1,n}, \ldots, x_{K,n})$, for audit event n, to measure the exponentially weighted moving average (EWMA) smoothed frequency distribution of K event types for a moving window including audit event n and the preceding events in the recent past. Specifically, the following equation is used to obtain the measure[2,5,6]:

$$x_{i,n} = \lambda \times o_i + (1 - \lambda) \times x_{i,n-1}, \quad \text{where } x_{i,0} = 0,\ i = 1, \ldots, K,\ n = 1, \ldots, N \tag{1}$$

where $x_{i,n}$ is the smoothed frequency value for event type i, o is a value for the current event or event n (if event type i is present in the current event, o is 1; otherwise it is 0), $X_{i,n-1}$ is the previous smoothed frequency value, and λ is the smoothing constant ($0 < \lambda < 1$). In this study, we let $\lambda = 0.3$ as in previous studies[2,5,6]. Hence, an observation for the current event is a multivariate vector with K variables for the smoothed frequencies of K event types.

2.2. Application of CSDM to cyber attack detection

The test statistic of CSDM has the following form[4,5]

$$\chi^2 = \sum_{i=1}^{p} \frac{(x_i - \overline{x_i})^2}{x_i} \tag{2}$$

where p is the number of variables in the observation data vector, $X = (x_1, \ldots, x_p)$, $p \geq 1$, and $\overline{x_i}$ is the sample average of the observations of x_i in the normal (in-control) condition. The statistic in Equation (2) measures the distance of a data point from the estimated center of the in-control data population. Using a sample of χ^2 values, the mean and standard deviation of the χ^2 population can be estimated from the sample mean $\overline{\chi^2}$ and the sample standard deviation S_{χ^2}. The control limits to detect out-of-control anomalies can be set to 3σ control limits as determined by $[\overline{\chi^2} - 3S_{\chi^2}, \overline{\chi^2} + 3S_{\chi^2}]$. As discussed in previous studies[2,5,6], we are interested in detecting significantly large χ^2 values for cyber attack detection. Hence, we set only the upper control limit to $\overline{\chi^2} + 3S_{\chi^2}$ as the signal threshold. That is, if χ^2 for an observation is greater than $\overline{\chi^2} + 3S_{\chi^2}$, we signal an out-of-control anomaly.

CSDM is an anomaly detection technique for cyber attack detection. The norm profile is obtained from the training data of normal events and is represented by $\bar{\mathbf{X}}$. The distance of the observation vector $\mathbf{X}$ for an audit event in the testing data from the norm profile, represented by $\bar{\mathbf{X}}$, and is computed as the χ^2 value. The larger the χ^2 value, the larger deviation the observation vector $\mathbf{X}$ of the audit event is from the norm profile, and the more likely the audit event is a part of an attack. For a given signal threshold, if the χ^2 value of an audit event is greater than the signal threshold, the audit event is signaled as an attack; otherwise, the audit event

DOI: 10.1002/qre

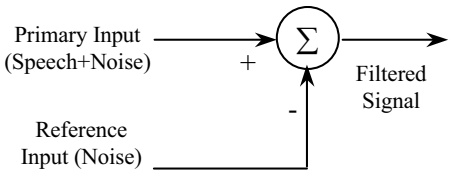

Figure 1. Simplified fixed-parameter noise cancelation

is considered as a norm. As a result, we classify the χ^2 value of each audit event in the testing data as being the result of either attack or norm activities.

The procedure of applying CSDM to the BSM data for cyber attack detection is provided below.

- *Training*:
  (1) select only the sequence of the normal events from the training data;
  (2) extract the event type of each audit event;
  (3) generate the observation vector for each audit event using formula (1);
  (4) compute the mean vector, $\bar{\mathbf{X}}$, of the observations for those normal events.
- *Testing*:
  (1) extract the event type of each audit event in the testing data;
  (2) generate the observation vector, $\mathbf{X}$, for each audit event using formula (1);
  (3) calculate the chi-square distance value, χ^2, for each audit event using formula (2) based on the $\bar{\mathbf{X}}$ characterization of the norm profile.

3. A NORM DATA CANCELLATION TECHNIQUE

If we consider attack events as signals we want to detect in the cyber domain and normal events as noise[2], cyber attack detection is similar to signal detection in the physical domain. Noise cancelation has been widely studied in the physical domain. For example, noise cancelation is used for speech enhancement. An interesting problem in speech enhancement is '*Captain Voice Enhancement*', capturing the speech of a captain in the noisy cockpit of an airplane. The primary speech input in this problem is the noise-corrupted speech. A reference input collecting a background noise signal from a microphone located in the cockpit but far enough away from the captain so as not to record his speech. Since the reference input approximately matches the noise in the primary input of the noise-corrupted speech, the reference input is used to cancel the noise in the primary input and thus enhance the quality of speech as shown in Figure 1 (Gannot *et al.*[7], Haykin[8], Lee and Jung[9], and Widrow and Stearns[10]). A matched filter with the primary input of signal and noise and the noise-only reference input collected separately but in a synchronized manner is the foundation of many noise cancelation techniques in the physical domain. That is, the noise-only reference input must be available to provide information about noise and cancel noise in the primary input.

However, in the cyber domain we can hardly collect the reference input of norm data separately when both attack events and normal use events are occurring on computers and networks since there may not be a location—a computer or network resource—in the cyberspace that is sensitive to normal user events (noise in cyberspace) but not attack events (signals in cyberspace). Any computer or network resource can be affected by both attack events and normal use events. Considering the difficulty in collecting the reference input of norm events directly from computers and networks, we propose to build a mathematical model of norm events and then use this model to generate the reference input of norm events. Specifically, we build a mathematical model of norm events using the training data of norm events. In testing, the primary input is the testing data that contain a stream of mixed attack and norm events. We use the model of norm events to generate a stream

DOI: 10.1002/qre

of norm events which is in turn used to cancel their effect in the primary input before performing CSDM for cyber attack detection. In the following sections, we first describe the mathematical modeling of norm events. Then we present two norm data cancelation techniques.

3.1. A Markov chain model of norm events to generate the reference input

In previous studies[3,11], we investigated the Markov chain model of audit events and demonstrated the effectiveness of modeling audit events as a Markov chain model. Hence, in this study, a Markov chain model of normal events is built from the stream of normal events in the training data.

As described in the previous section, each audit event is represented by its event type. To build a Markov chain model of normal events, we take the event type of an audit event at a given time as the system state at that time with uncertainty. In general, we assume that a system state at a discrete time point n, s_n, takes one of the K states (K is an integer and $K > 1$) and the probability that s_n is at state j depends on the past only through the most recent state s_{n-1}:

$$P\{s_n \mid s_{n-1}, \ldots, s_{n-k}\} = P\{s_n = state_j \mid s_{n-1} = state_i\} = p_{ij} \tag{3}$$

Such a process is described as a K-state Markov chain with transition probabilities $\{p_{ij}\}_{i,j=1,2,\ldots,K}$ (see Buttorp[12] and Winston[13]). The transition probability is the probability that state i at time $n-1$ will be followed by state j at time n. If n_{ij} represents the number of state transitions from state i to state j in the sequence of normal events in the training data, and N_i represents the total number of state transitions from state i to all of the states (including state i), then p_{ij} can be obtained from the sequence of normal events in the training data:

$$p_{ij} = \frac{n_{ij}}{N_i} = \frac{n_{ij}}{n_{i1} + n_{i2} + \cdots + n_{iK}} \tag{4}$$

The sum of all the probabilities that state i transmits to other states is 1:

$$\sum_{j=1}^{j=K} p_{ij} = 1 \tag{5}$$

It is often convenient to represent the transition probabilities in a $K \times K$ matrix, $\mathbf{P}$, known as the *transition probability matrix*:

$$\mathbf{P} = \begin{bmatrix} p_{11} & p_{12} & \cdots & p_{1K} \\ p_{21} & p_{22} & \cdots & p_{2K} \\ \vdots & \vdots & \ddots & \vdots \\ p_{K1} & p_{K2} & \cdots & p_{KK} \end{bmatrix} \tag{6}$$

The row j column i element of $\mathbf{P}$ is the transition probability p_{ij}. In our study, $K = 60$ for the total of 60 event types that appear in the training and testing data of this study.

In addition to the transition probability matrix, the Markov chain model of normal events also has the *initial probability distribution* $\mathbf{P}_0 = [p_{01}\, p_{02} \ldots p_{0K}]^{\mathrm{T}}$, where

$$p_{0j} = \frac{n_{0j}}{N} \tag{7}$$

where p_{0j} is the initial probability of event type j, n_{0j} is the number of occurrences of event type j in the sequence of normal events in the training data, and N is the total number of normal events in the training data. Provided with the observations of the system state, $s_1, s_2, \ldots, s_N$ at time $n = 1, \ldots, N$, the transition probability matrix and the initial probability distribution of a Markov chain model can be learned from the observations of system state in the sequence of the normal events in the training data using formulas (4) and (7).

DOI: 10.1002/qre

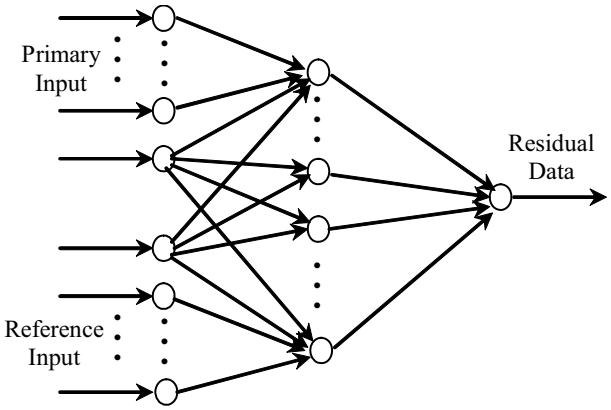

Figure 2. Norm data cancelation using an ANN

In testing, the Markov chain model of normal events is used to generate the events in the reference input. When generating the event sequence as the reference input, the first event in the reference input is generated based on the initial probability distribution of event types. The second event is generated based on the transition probabilities from the event type of the first event to 60 possible event types. The transition probabilities are also used to generate the third event, the fourth event, and so on.

3.2. Norm data cancelation

It is difficult to perform norm data cancelation directly on audit events by removing those audit events in the reference input produced by the Markov chain model from the testing data of audit events because the event sequence in the reference input and the event sequence in the testing data are not necessarily synchronized. Hence, we need to perform norm data cancelation on a more general feature of audit event data rather than directly on audit events. In this study, we perform norm data cancelation on the EWMA vector of the smoothed event frequency distribution. We propose a norm data cancelation technique using an artificial neural network (ANN).

Figure 2 shows the ANN noise cancelation on the EWMA vectors. The observation vectors from the primary input and the reference input are used directly as the inputs to the ANN. The ANN is a multi-layer perceptron with one hidden layer of 25 hidden units, 2×60 inputs, and 60 output units (there are only 60 event types rather than all 284 event types appearing in both the training data and the testing data). The ANN is implemented using Matlab. Each unit in each layer uses the linear postsynaptic potential function (PSP) transfer function and the logistic activation function. The back-propagation learning algorithm is used to train this ANN. The training of the ANN attempts to minimize the sum of squared errors between the actual outputs and the target outputs. Both the learning rate and the momentum are set to 0.6. The echo is set to 500.

The training procedure and the testing procedure of the ANN norm data cancelation are described below. In training, we first learn the Markov model of normal events using the sequence of the normal events in the training data. The training data with both attack events and normal events are used as the primary input for the ANN training. To generate the reference input for the ANN training, the following method is used. If the nth audit event in the primary input is a normal event, the corresponding event in the reference input is generated using the Markov chain model. If the nth audit event in the primary input is an attack event, the corresponding event in the reference input is blank as no event occurs. To generate the target output as the filtered data for the ANN training, the following method is used. If the nth audit event in the primary input is a normal event, the corresponding target event is blank as no event happens. If the nth audit event in the primary input is an attack event, then the corresponding target event has the same event type as that of the primary event. The training procedure and the testing procedure of the ANN norm data filtering are described below.

DOI: 10.1002/qre

- *Training:*

(1)–(4) same as training (1)–(4) for CSDM alone;

(5) learn the transition probability matrix and the initial probability distribution in the Markov chain model from the sequence of the normal events in the training data using formulas (4) and (7);

(6) use the training data as the primary input, and generate the reference input and the target output using the method described above;

(7) generate the EWMA vectors for the primary input, the reference input, and the target output;

(8) train the ANN using the EWMA vectors for the primary input, the reference input, and the target output.

- *Testing:*

(1) use the Markov chain model to generate the sequence of totally N normal events, where N is the number of the audit events in the testing data, such that the total number of the audit events in the reference input is the same as the total number of the audit events in the testing data—the primary input with both normal and attack events;

(2) extract the event type of each audit event in the primary input and the reference input;

(3) generate the EWMA vector for each audit event in the primary input and the EWMA vector for each audit event in the reference input using formula (1);

(4) obtain the residual data for each audit event in the primary input using the trained ANN and the EWMA vectors for that event in the primary input and the corresponding event in the reference input;

(5) calculate the χ^2 value for each audit event in the primary input using formula (2) with the residual data for that event as X, and the $\bar{\mathbf{X}}$ characterization of the norm profile.

4. RESULTS

The testing results are evaluated using a receiver operating characteristic (ROC) chart[14]. A *hit* is a term used to refer to a true attack event in the testing data that is correctly signaled as an attack event by a given detection technique. The hit rate is the ratio of the signaled attack events to the total number of the true attack events in the testing data. A *false alarm* is used to refer to a true normal event that is signaled as an attack event. The false-alarm rate is the ratio of the falsely signaled normal events to the total number of true normal events in the testing data. The hit and the false-alarm rates give the performance of a given detection technique. Given different signal thresholds, different pairs of hit and the false-alarm rates can be obtained and plotted in a ROC chart. A ROC chart shows the trade-off between the false alarm and the hit rates for signal detection by plotting pairs of the hit and the false-alarm rates for varying signal thresholds in a two-dimensional space. The closer the ROC curve is to the point (the top-left corner of the ROC chart) representing the pair of the 100% hit rate and the 0% false-alarm rate, the better the detection performance.

For a given detection technique, the minimum and maximum of the χ^2 values from the testing data are first obtained. The signal threshold is first set to a value smaller than the minimum of the χ^2 values from the testing data. The signal threshold is gradually increased with one increment in each step, until the signal threshold reaches a value greater than the maximum of the χ^2 values from the testing data. For each signal threshold, the hit and false-alarm rates are calculated. The pair of the hit and false-alarm rates is plotted in the ROC chart. Finally, all of the points for the pairs of the hit and false-alarm rates are connected to form the ROC curve. The curve shows the change of the hit rate as the signal threshold varies to produce more or less false alarms.

Figure 3 shows the ROC chart with a ROC curve for CSDM alone and another ROC curve for CSDM with the ANN norm data cancelation technique. The detection performance of CSDM alone is not satisfactory since the hit rate is over 99% only when the false-alarm rate is about 45%. CSDM with the ANN norm data cancelation technique shows a significant performance improvement as the ROC curve gets much closer to the top-left corner (representing the 100% hit rate and the 0% false-alarm rate) of the ROC chart than the ROC curve of CSDM alone, with an improvement in the false-alarm rate from about 45% to about 5%. Therefore, the testing results demonstrate that our technique of norm data cancelation significantly improves the detection performance of CSDM.

DOI: 10.1002/qre

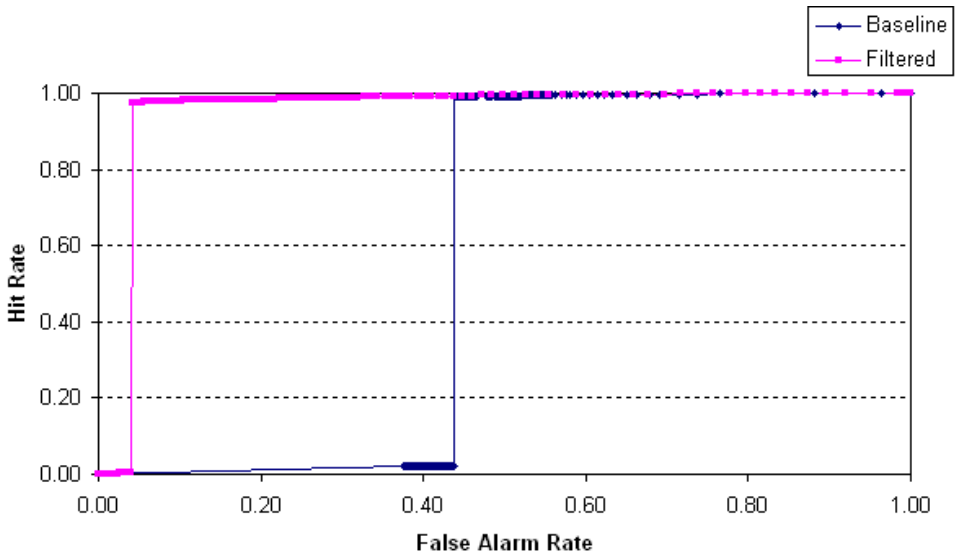

Figure 3. The ROC chart with the ROC curve for CSDM alone (baseline) and CSDM with ANN norm data cancelation (filtered)

5. SUMMARY

In this paper, a norm data cancelation of improving the performance of a cyber attack detection method—CSDM—has been presented. This technique can improve the data quality and lead to an improvement in the attack detection performance by canceling the effect of the norm data in the mixed attack and norm data observed from computers and networks. The testing results show that our norm data cancelation technique provides a significantly large performance improvement in cyber attack detection. Hence, the results of this study show that the performance of an existing cyber attack detecting technique, such as CSDM, can be improved by first applying norm data cancelation to computer and network data to improve the data quality.

Acknowledgement

This work is sponsored by the Air Force Office of Scientific Research (AFOSR) under grant number F49620-99-1-0014. The U.S. Government has the authority to reproduce and distribute reprints for governmental purpose notwithstanding any copyright annotation thereon. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either express or implied, of the AFOSR or the U.S. Government.

REFERENCES

1. Ye N, Farley T. A scientific approach to cyberattack detection. *IEEE Computer* 2005; **38**(11):55–61.
2. Ye N, Li X, Chen Q, Emran SM, Xu M. Probabilistic techniques for intrusion detection based on computer audit data. *IEEE Transactions on Systems, Man, and Cybernetics* 2001; **31**(4):266–274.
3. Ye N, Zhang Y, Borror CM. Robustness of the Markov-chain model for cyber-attack detection. *IEEE Transactions on Reliability* 2004; **53**(1):116–123.
4. Ye N, Borror C, Parmar D. Scalable chi square distance versus conventional statistical distance for process monitoring with uncorrelated data variables. *Quality and Reliability Engineering International* 2003; **19**(6):505–515.
5. Emran SM, Ye N. Robustness of chi-square and Canberra techniques in detecting intrusions into information systems. *Quality and Reliability Engineering International* 2002; **18**(1):19–28.

DOI: 10.1002/qre

6. Ye N, Emran SM, Chen Q, Vilbert S. Multivariate statistical analysis of audit trails for host-based intrusion detection. *IEEE Transactions on Computers* 2002; **51**(7):810–820.
7. Gannot S, Burshtein D, Weinstein E. Iterative and sequential Kalman filter-based speech enhancement algorithms. *IEEE Transactions on Speech and Audio Processing* 1998; **6**(4):373–385.
8. Haykin S. *Adaptive Filter Theory*. Prentice-Hall: Upper Saddle River, NJ, 1996.
9. Lee KY, Jung S. Time-domain approach using multi Kalman filters and EM algorithm to speech enhancement with nonstationary noise. *IEEE Transactions on Speech and Audio Processing* 2000; **8**(3):282–291.
10. Widrow B, Stearns SD. *Adaptive Signal Processing*. Prentice-Hall: Upper Saddle River, NJ, 1985.
11. Ye N, Ehiabor T, Zhang Y. First-order versus high-order stochastic models for computer intrusion detection. *Quality and Reliability Engineering International* 2002; **18**(3):243–250.
12. Buttorp P. *Stochastic Modeling of Scientific Data*. Chapman and Hall: London, 1995.
13. Winston WL. *Operations Research: Applications and Algorithms*. Duxbury Press: Belmont, CA, 1994.
14. Egan JP. *Signal Detection Theory and ROC Analysis*. Academic Press: New York, 1975.

Authors' biographies

Nong Ye is a Professor of Industrial Engineering and an Affiliated Professor of Computer Science at Arizona State University, Tempe, Arizona. She received a BS degree in Computer Science from Peking University, Beijing, a MS degree in Computer Science from the Chinese Academy of Sciences, Beijing, and a PhD degree in Industrial Engineering from Purdue University, West Lafayette, Indiana. Her research interest is in information and systems assurance. She serves as an Associate Editor for *IEEE Transactions on Reliability*, *IEEE Transactions on Systems, Man, and Cybernetics*, and *Information, Knowledge, and Systems Management*. She is a senior member of the Institute of Industrial Engineers and a senior member of IEEE.

Qiang Chen received a PhD degree in Industrial Engineering from Arizona State University and a BS degree and a MS degree from the Manufacturing Engineering Department at Beijing University of Aeronautics and Astronautics (BUAA), Beijing, People's Republic of China, in 1993 and 1999, respectively. From 1993 to 1996, he worked as an information management engineer in Beijing Aircraft Maintenance and Engineering Co.

DOI: 10.1002/qre