International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, November 2011

STATISTICAL QUALITY CONTROL APPROACHES TO NETWORK INTRUSION DETECTION

Rohitha Goonatilake[1], Rafic Bachnak[1], and Susantha Herath[2]

[1]Department of Engineering, Mathematics, and Physics
Texas A&M International University, TX 78041, USA
E-mails: harag@tamiu.edu and rbachnak@tamiu.edu
[2]Department of Information Systems, St. Cloud State University, MN 56301, USA
E-mail: sherath@stcloudstate.edu

ABSTRACT

In the study of network intrusion, much attention has been drawn to on-time detection of intrusion to safeguard public and private interest and to capture the law-breakers. Even though various methods have been found in literature, some situations warrant us to determine intrusions of network in real-time to prevent further undue harm to the computer network as and when they occur. This approach helps detect the intrusion and has a greater potential to apprehend the law-breaker. The purpose of this article is to formulate a method to this effect that is based on the statistical quality control techniques widely used in the manufacturing and production processes.

KEYWORDS

Anomalies, control charts, false alarm, intrusion, network system, and quality control

1. INTRODUCTION

The rapid growth of Internet use in public and private enterprises has increased cyber-crimes. Conventional mechanisms for secured networks include firewalls, virtual private networks, and authentication tools. These provide a protective layer, but are vulnerable to more sophisticated attacks. However, completely preventing intrusions and attacks on systems is impossible. Hence, intrusion detection is considered to be the next step in providing defense to systemsas the prevention is given much greater attention accordingly. The objective of current research is to explore advances for the benefits tothe general public. This is essential as the consequences can be enormous as vulnerabilities could be exploited to obtain authority, to disrupt service, to inject additional damages into the system, or to deny service to the legitimate users [1]. Online intrusion detection provides the architecture that uses the comparison of outputs from diverse applications to provide a significant and novel approach to preventing intrusion attacks.

In order to detect intrusions and have a secured network, Network Intrusion Detection Systems (NIDS) have been introduced. Network security architectures, such as NIDS and firewalls, will attempt to detect break-ins by monitoring the incoming and outgoing trafficof the network. According to the Computer Crime Research Center survey, new threats are on the rise [6]. There has also been an increase in reported cases of cybercrimes in recent years, with one major difference being that the motives for breaches have multifaceted. Apart from viruses and worms, a varied number of unauthorized activities play a role in disturbing both computer and breaching network security. Another aspect of risks to any network activity distinguishes

DOI : 10.5121/ijnsa.2011.3608

between risks occurring internally and externally to the organization. Internal sources can be people inside a firm working against policies and taking over privileges to access confidential files, etc. External sources include threats and attacks from outside the organization's access to the information for monitory and private uses. Quiet internal attacks can result in substantial financial losses to an organization [9].

2. PRELIMINARIES

Major attacks include denial of service, sniffing, spoofing, SYN (synchronized) flooding, viruses, and worms. Denial of service attacks try to prevent legitimate users from accessing the network by sending huge numbers of data packets to the network. Since the Internet has limited resources, it is hard to cope with heavy traffic, thereby, denying access to legitimate users [4]. In SYN flooding, the attacker sends SYN packets to the server using fake IP addresses, but does not acknowledge the server's messages. If a legitimate user sends a message, it does not get acknowledgement from the server since the server's resources have been used up by the attacker. Yahoo, Amazon, e-Bay, and other popular websites have been exposed to denial of service attacks [2 & 9]. Worms and viruses are the programs when injected, spread through emails and Internet packets and begin toreplicate themselves and send copies to other nodes in the network. For example, the SQL Slammer worm replicated once every eight seconds; within ten minutes, it had spread to almost all parts of the world. It created chaos, hampered credit card transactions, interrupted airline reservations, and did many other related activities of disruption [4]. An IDS detects intrusions and misuses by collecting and analyzing the information from different variety of network sources. The IDS compares the signatures of the received packets with the known signatures in the database. If the same signature is found, it treats it as an attack and filters it. For unknown signatures, the data is sent to the anomaly detection unit. This unit builds models of normal data. It checks for patterns that deviate from normal behavior to be suspected as a possible intrusion. One of the many advantages of anomaly detection is that it does not require a database of signatures. On the basis of network protection, an IDS is classified into either a host-based intrusion detection systems (HIDS) or network-based intrusion detection systems (NIDS). IDS tools use data from a single host in HIDS [5].

A situation can warrantee us to determine intrusions of the network in real-time to prevent further harm to the computer network as they occur. This possibility will help detect the intrusion and has a greater potential to apprehend the law breaker.There are other applications, as well. For example, mobile communication networkstransmit a large amount of data that can be used in identifying the place of an emergency that requires immediate attention and it can be disrupted from intrusions. Accordingly, the abilityto quickly identify anomalous data in real-time is paramount important[8]. Another approach in this effortis multivariate statistical analysis of audit trails for host-based intrusion detection [11]. The performance of this test is not as good as that of the Chi-square test that detects only mean shifts [14]. However, the results show that the multivariate statistical techniques based on the Chi-square test statistic achieved the 0% false alarm rate and the 100% detection rate [12].

3. TECHNIQUE AND IMPLEMENTATION

Among all statistical techniques, control charts appear to be the most widely used to maintain the quality of products in manufacturing processes. Samples of the packetsare collected successively in order for this technique to work. A set of commands in a network system

consists of strings used to specify the goals for each of the virtual performer agents running on the individual computers and are sent using the UDP protocol. Anomalous traffic in the network system is generally identified as a potential intrusion. Traffic analysis does not deal with the payload of a measure (not available for analysis) but with other characteristics such as source, destination, routing, length, duration, and frequency of the communication [13]. Traffic may be encrypted to analyze the packet payload. Traffic behavior in the network is characterized by statistical measures to capture the behavior. Means and standard deviations of anomalies are referred to in the corresponding measures of the distribution of data so obtained.It is assumed that the anomalies that belong to each sampleare independent and identically distributed with mean, μ, and standard deviation, s.

In order to construct control charts, reliable historical data is not available. As mean,μ, and standard deviation,σ, would not be known, the three-standard-deviation-rule cannotbe employed. Since the statistic,s, is not an unbiased estimator of σ,transforming the same to an unbiased estimator requires some work.Let $X_1, X_2, \ldots$ denote the measures of the communications successively obtained from the network system. Items are collected periodically in some fixed size, n. The average of the i[th] sample is denoted by $\overline{X}_i$. That is, $\overline{X}_1 = \frac{X_1 + X_2 + \cdots + X_n}{n}$, $\overline{X}_2 = \frac{X_{n+1} + X_{n+2} + \cdots + X_{2n}}{n}$, $\overline{X}_3 = \frac{X_{2n+1} + X_{2n+2} + \cdots + X_{3n}}{n}$, and so on. It is appropriate to estimate μ by $\overline{\overline{X}}$, the average of these sample averages. Let s_i denote the sample standard deviation of the i[th]collection. That is, letting $s_k = \sqrt{\sum_{i=1}^{n} \frac{(X_{(k-1)n+i} - \overline{X}_k)^2}{n-1}}$ for $i = 1, 2, \ldots, k$ so that $\overline{s} = (s_1 + s_2 + \cdots + s_k)/k$. It follows that $\overline{s}/c(n)$ is an unbiased estimator of σ, where $c(n) = \frac{\sqrt{2}\,\Gamma\left(\frac{n}{2}\right)}{\sqrt{n-1}\,\Gamma\left(\frac{n-1}{2}\right)}$ and $\Gamma(\cdot)$ is the gamma function [6]. Now, the corresponding upper and lower control limits for $\overline{X}$ are:

$$\overline{\overline{X}} - \frac{3\overline{s}}{\sqrt{n}\,c(n)} \leq \overline{X} \leq \overline{\overline{X}} + \frac{3\overline{s}}{\sqrt{n}\,c(n)}$$

andthe upper and lower control limits for s are:

$$\overline{s}\left[1 - 3\sqrt{{}^{1}/_{c(n)^2} - 1}\right] \leq s \leq \overline{s}\left[1 + 3\sqrt{{}^{1}/_{c(n)^2} - 1}\right], \text{ respectively.}$$

The lower and upper control limits for $\overline{X}$ and s play a significant role in the determination of whether the intrusion detection system will work normally as expected. The control charts for variability of the measures can also be plotted. If the distribution of breaking strength is normally distributed with mean equals μ and standard deviation equals σ, we can construct a control chart for the variance or standard deviation. If s^2 is the sample variance, then $n\,s^2/\sigma^2$

has a χ^2 −distribution with $(n-1)$ degrees of freedom. Unfortunately, the mean, μ, and standard deviation, σ, would not be available. So, the LCL and ULC derived abovefor $s$are used.

An IDSplays an important role in network security process and provides a peace of mind for those who continue to work on innovative and advancement of cyber applications. This technique requiresperforming a set of calculations using the data obtained from the network system periodically. This would include intrusion modeling, detection, prevention and advancements in IDS; a comparison of these techniques will be made with other IDS tools. Several intrusion detection systems have recently enjoyed the limelight as they improve the efficiency of intrusion detection [1, 2,& 3]. It has proved to be efficient in diagnosing misuses and other anomalies which were not detected otherwise.

As an illustration, let us assume that a sample of fivecommunications is collected from the network successively. As such, the value of $c(5) = 0.9399851$. Let us assume that the successive thirtysamples of five network communications collected have yielded the means and standard variations as listed in Table 1.

Table 1: Means ($\overline{X}$) and standard variations (s) collected for thirty samples of fixed size

Sample	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\overline{X}$	13.01	12.97	13.12	12.99	13.03	13.02	13.10	13.14	13.09	13.20	14.88	13.03	13.00	13.04	12.99
s	1.12	1.14	1.08	1.11	1.09	1.08	1.15	1.25	1.16	1.13	1.16	1.17	1.23	1.11	1.10
Sample	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
$\overline{X}$	12.98	13.05	13.02	13.03	13.04	13.11	11.65	12.98	14.10	13.02	13.04	13.09	13.00	13.03	11.03
s	1.13	1.12	1.08	1.07	1.10	1.11	1.03	1.11	0.97	0.99	1.13	1.11	1.02	1.01	1.12

The necessary calculations of the control limits for $\overline{X}$ and s provide whether there would be anomalies or suspicious activities in the network system. These estimations can be computed periodically to ensure new $\overline{X}$ and s are within these limits. For data listed in Table 1, the lower and upper control limits (LCLs & UCLs) for $\overline{X}$ and s are $(11.405, 14.650)$ and $(-0.101, 2.310)$. Since $s \geq 0$, these estimates are corrected to be read as $(11.405, 14.650)$ and $(0.0000, 2.310)$ for $\overline{X}$ and s, respectively. The calculations are continued beyond the thirtieth samples in order to secure the system is in complete control. Network systems will be investigated if at any time the values of $\overline{X}$ and s go outside the limits of the intervals. From Figure 1, two instances are seen where the values of $\overline{X}$ went outside the control limits of $\overline{X}$;at the same time, the values of s stayed within the control limits of $s$due to larger variation seen in the data set. This now provides that an anomaly has occurred.

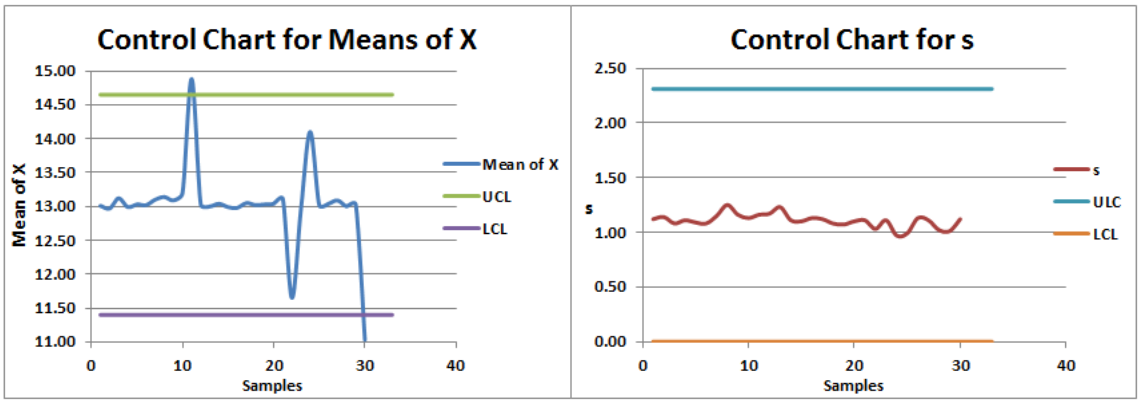

Figure 1: Control charts for $\overline{X}$ and s

The effectiveness of this technique depends on frequency of updates and nature of monitoring by collecting samples of fixed size necessary to plot control charts for $\overline{X}$ and s as provided in Figure 1.

4. SAMPLING INSPECTION

Among many methods employed for sampling inspection to meet the demands of network provider and the user, the single sample plan is considered a commonly used technique [10]. Given a sample of N packages, only n of them will be tested for anomalies. Among $n$items, if d or fewer anomalies are found,the sample will be accepted and rejected otherwise. The user insisted that the fraction of anomalies is no more than p_t called "sample tolerance fraction anomaly" in each accepted sample. There can be a situation that this value can only be achieved when the complete sampling that involves higher cost of inspection is done. The user position needs to be modified depending on meeting the fraction. The probability of user's risk of accepting a samplethat has fraction $p_t$of anomalies, $P_C$is given by

$$P_C = \sum_{x=0}^{d} \frac{\binom{N_{pt}}{x}\binom{N - N_{pt}}{n - x}}{\binom{N}{n}}.$$

It is assumed that n items are to be tested from among the collection of N communications that contain N_{pt} anomalies. It appears that x anomalies in the sample so that $0 \le x \le N$. For$N$ is sufficiently large compared to n, we obtain,

$$P_C \approx \sum_{x=0}^{d} \binom{n}{x} p_t^x (1 - p_t)^{n-x}.$$

Suppose that we want to estimate some possible values of n and d. For $P_C = 0.06$, $p_t = 0.02$, we will have the smallest possible choice of n by setting $d = 0$. If N is large, we have the equation, $\binom{n}{0}(0.02)^0(0.98)^n = 0.06$, thus giving $n \approx 140$.

Revision to this number may be required due to the cost of testing such a large number of anomalies. There are instances that the network provider has given additional thought to their own risk. The Copula model provides a framework to quantify the risk associated with online

business transactions as a result of a security breach [7]. They now insist on a probability of invoking this risk, $P_{R,}$of rejecting the sample if the mean fraction of anomaly is$\overline{p}$.The network provider is willing to adjust p_t and $P_C$on the demand by the userwho is now willing to propose$\overline{p}$ to the network provider. This can now be regarded as the choice forthe random sampledrawn from the process (conceptually infinity) producing a mean fraction of anomalies, $\overline{p}$.Assuming the statistical process corresponds to $n$independent Bernoulli trails of an event with probability $\overline{p}$ is:

$$P_R = \sum_{x=d+1}^{n} \binom{n}{x} \bar{p}^x (1-\bar{p})^{n-x},$$
$$= 1 - \sum_{x=0}^{d} \binom{n}{x} \bar{p}^x (1-\bar{p})^{n-x}.$$

The network provider's risk, $P_{R,}$ can also be defined as the probability that the sample will be rejected if the fraction p of anomalies of this sample is $p = \overline{p}$.Accordingly, we now have two equations to be solved for n assuming N is sufficiently large.

$$\sum_{x=0}^{d} \binom{n}{x} {p_t}^x (1-p_t)^{n-x} = P_C, \text{ and}$$
$$\sum_{x=0}^{d} \binom{n}{x} \bar{p}^x (1-\bar{p})^{n-x} = 1 - P_{R.}$$

Obviously, we need to have $\bar{p} < p_t$ since it is presumed that $1 - P_R > P_C$given x and $np$are small relative to n,whilst$p$ (either$\overline{p}$or p_t) is very small to calculate $n$and p using Poisson probability approximation to the binomial probability. The values should be modified thereafter to meet the interest of the network provider and the user in the single sampling plan. The sequential testing (sampling) of hypotheses results in statistical cost-cutting measuresis introduced to reduce the number of samples required to arrive at a specific precision in the quality control process. The idea is naturally analogous to testing hypothesis. After each sample is collected the network provider decides to continue the process before the user decides to reject the null hypothesis or the alternative hypothesis(appropriately defined).

5. OPERATING CHARACTERISTIC CURVE

The risk associated with a sampling inspection plan can be investigated from the operating characteristic curve (OCC) showing the probability of acceptance of the sample for different quality levels. The OCC of a single sampling plan is a curve obtained from the probability of accepting the sample when it contains a fraction,p, of anomalies as it varies. For large N,the OCC is obtained by plotting the graph of $P(p) = \sum_{x=0}^{d} \binom{n}{x} p^x (1-p)^{n-x}$ as a function of p.

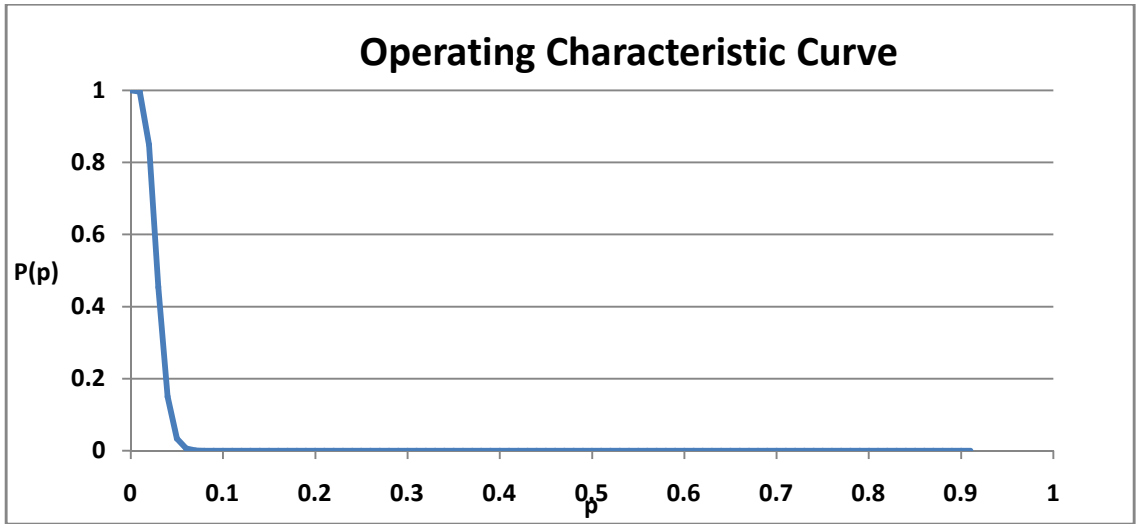

Figure 2: Operating characteristics curve, $P(p)$ as a function of p (for$N$ is large, $N = 300$, and $d = 8$)

The network user may now demand at least worry-free ongoing network activities. Accordingly, the user insists that no matter what fractions of anomalies in the samples before, the average fraction of anomalies per sample finally accepted should not exceed the user's average ongoing quality limitations. An alternative is always available for the network provider. Instead of specifying the maximum allowable probability of rejecting a sample, if the process is under a control,the network providerprefers to minimize the average number of inspections subject to other requirements of the user. Let W denote the number of packetsto be inspected before an acceptable sample is turned over to the user. If d or fewer anomalies are found, the value of W will be n; the probability, $Pr\{W = n\}$, is:

$$Pr\{W = n\} = \sum_{x=0}^{d} \frac{\binom{N_p}{x}\binom{N - N_p}{N - x}}{\binom{N}{n}},$$

whereN_p is the actual number of anomalies. If more than $d$anomalieswere found, then N packets must be inspected, the probability of this event, $Pr\{W = n\}$, is equal to $1 - P(p)$.

Let Y be the number of items expectedfor inspection prior to accepting the samplethat is returned over to the user. Consequently the expected number of inspections is,

$$E(Y) = nP(p) + N[1 - P(p)] = n + (N - n)[1 - P(p)].$$

If $P(p) = 0.5$,then$E(Y) = \frac{N+n}{2}$. That is, the expectation equals to the average of two sample sizes in this case. However, there can be a method that can be formulated to meet the expectation of the network provider. These methods and ideas are applicable in acceptance sampling implementation, with the exception that the inspection is still carried out by the network provider. They can neglect the user's point of view, and have their own choice of values for n and d to safeguard user's risk and minimum inspectionrequired for theongoing

quality limitations. Discussion of other plans such as double sampling and sequential sampling can be carried out as detailed in the literature [15, 16, & 17].

6. FALSE ALARM RATE AND SPECIFICITY

In probability models, there are two kinds of properties worth considering. One is that the probability of calculating changes when none have occurred(the power of the model), and the other is the probability of calculating changes incorrectly occurred, (false alarm rate or more precisely, the false positive probability), respectively. The latter is the probability that the values are not falling between the lower control and upper control limits. For $\overline{X}$control charts of normally distributed random variables, the probability that the values are not falling between the lower control and upper control limits, provided the system remains in statistical control, can be calculated using the standard normal random variable, Z, as follows.

$$\text{False alarm probability} = \alpha = Pr\{\overline{X} < \text{LCL}\} + Pr\{\overline{X} > \text{UCL}\}$$

$$= Pr\left\{Z < -\frac{3}{\sqrt{n}c(n)}\right\} + Pr\left\{Z > +\frac{3}{\sqrt{n}c(n)}\right\}$$

$$= Pr\{Z < -1.42730\} + Pr\{Z > +1.42730\} \approx 2 \times 0.0764 = 0.1528.$$

The specificity for $\overline{X}$ control charts is (1- False alarm probability)$\approx 1 - 0.1528 = 0.8472$, thus enabling to conclude that almost all sample means should be between the LCL and ULC if the system remains to be in control. False alarm events occur infrequently, at the rate of approximately 1.5 per 10 successive samples. This rate can be further improved by choosing larger sample sizes. Of course, this depends on the distribution of the data providing a high level of specificity. If the threshold is set on this value, then false alarms would be generated within the obtained interval [13]. Natural expectationsare thatfewer false alarms can compromise the method that tolerates greater possible malicious traffics. The existing methods may not ensure the inclusion or exclusion of unnecessary quality controls. However, choosing a novel approach for evaluating information security controls can help decision-makers to select the most effective techniques in the resource-constrained being the focus. The proposed approach quantifies the desirability of each information security control taking into account benefits and restrictions associated with the technique [18].

7. CONCLUSIONS

Learningabout online attacks, correcting the situations, and generalizingthe techniques are part of the online testing to positively identify attacks, eliminating false positives, and rule-base similarity reasoning to avoid further vulnerabilities. The policy issues need to be periodically reviewed or revisedto safeguard both public and private interest in this regard. This also evaluates the ability to detect outliers in a data set and to describe how it can be used as an indicator of an emergency response management system. Generally, outliers are removed to calculate modified set of control limits for $\overline{X}$ and s as the process is being continued. This article provided an introduction to the use of statistical quality control methods for intrusion detection assuming the availability and accuracy of sufficient data at the necessary level of breadth and intensitywhilst a risk and cost comparison isyet to be undertaken.

In this article, an initial attempt also has been made to the study of emerging attacks, detection and prevention techniques, intrusion detection systems, and how they have advanced in recent

times using quality control techniques. Naturally, the next steps would be to extend these techniques to more sophisticated ones based on moving-average, exponentially weighted moving-average, and cumulative sum control charts. It is hoped that the recent approaches and comparative studies willcomplement the preliminary results of this topic and the extensions proposed by the work of this paper.

ACKNOWLEDGEMENTS

The authors would like to thank the reviewers for their suggestions that greatlyimproved this manuscript.

REFERENCES

[1] James C. Reynolds, James Just, Larry Clough, and Ryan Maglich, ”On-Line Intrusion Detection and Attack Prevention Using Diversity, Generate-and-Test, and Generalization,” Proceedings of the 36th Hawaii International Conference on System Sciences (HICSS’03), 2002, pp. 1-8

[2] L. Ertoz, E. Eilertson, A. Lazarevic, P. Tan, P. Dokas, V. Kumar, and J. Srivastava, "Next Generation Data Mining,” The MINDS - Minnesota Intrusion Detection System, MIT Press, 2004

[3] Vipin Kumar, “Parallel and Distributed Computing for Cybersecurity,” IEEE Distributed Systems Online, 2005, Vol. 6, No. 10

[4] William Stallings “Cryptography and Network Security: Principles and Practice,”3rdEdition, Prentice Hall, 2003

[5] http://www.kernelthread.com/publications/security/intrusion.html

[6] Sheldon M. Ross, “Introduction to Probability and Statistics for Engineers and Scientists,” Fourth Edition, Elsevier Academic Press, 2009

[7] ArunabhaMukhopadhyay, Samir Chatterjee, DebashisSaha, AmbujMahanti, and Samir K. Sadhukhna, “e-Risk Management with Insurance: A Framework using Copula aided Bayesian Belief Networks,” Proceedings of the 39th Hawaii International Conference on System Sciences, 2006, pp. 1-6

[8] Alec Pawling, Nitesh V. Chawla, and Greg Madey, “Anomaly Detection in a Mobile Communication Network,” Comput Math Organ Theory, 2007, Vol. 13, pp. 407-422

[9] Paul E. Proctor “The Practical Intrusion Detection Handbook”, Prentice Hall,2001

[10] H. D. Brunk, “An introduction to Mathematical Statistics,” Ginn and Co, New York, 1960

[11] Nong Ye, Syed MasumEmran, Qiang Chen, and Sean Vilbert, “Multivariate Statistical Analysis of Audit Trailsfor Host-Based Intrusion Detection,” IEEE Transactions on Computers, 2002, Vol. 51, No. 7

[12] Nong Ye and Qiang Chen, “An Anomaly Detection Technique Based On a Chi-Square Statistic for Detecting Intrusions into Information Systems,” Quality and Reliability Engineering International, 2001, Vol. 17, pp. 105–112

[13] PetarČisar and SanjaMaravićČisar, “Quality Control in Function of Statistical Anomaly Detection in Intrusion Detection Systems,” 4th Serbian-Hungarian Joint Symposium on Intelligent Systems (SISY 2006), 2006, pp. 209-220

[14] Rohitha Goonatilake, Ajantha Herath, Suvineetha Herath, Susantha Herath, and Jayantha Herath, “Intrusion Detection Using the Chi-Square Goodness-of-Fit Test for Information Assurance, Network, Forensics and Software Security,” The Journal of Computing Sciences in Colleges (JCSC), Vol. 23, No. 1, 2007, pp. 255-263

[15] CengizKahraman, "Fuzzy Applications in Industrial Engineering," Springer-Verlag, 2006

[16] P. Rama Murthy, "Production and Operations Management," Revised Second Edition, New Age International Publisher, 2007

[17] CengizKahraman and MesutYavuz, "Production Engineering and Management under Fuzziness," Springer, 2010

[18] Angel R. Otero, Carlos E. Otero, and AbrarQureshi, "A Multi-Criteria Evaluation of Information Security Controls Using Boolean Features," International Journal of Network Security & Its Applications (IJNSA), Vol.2, No.4, 2010

Authors:

Rohitha Goonatilake received a Ph.D. in applied mathematics from Kent State University, Kent, Ohio in 1997 and is currently working as an associate professor of mathematics in the Department of Engineering, Mathematics, and Physics at Texas A&M International University. He was a Co-PI for two grants funded by the Texas Higher Education Coordinating Board for the Engineering Summer Programs held in 2010 and 2011 to provide enrichment for area middle and high school students to enter into careers in engineering. He is a member of American Mathematical Society, Mathematical Association of America, Institute of Mathematical Statistics, and The Honor Society of Phi Kappa Phi.

Rafic Bachnak is Professor and Chair of the Department of Engineering, Mathematics, and Physics at Texas A&M International University (TAMIU). He received his B.S., M.S., and Ph.D. degrees in Electrical from Ohio University in 1983, 1984, and 1989, respectively. Prior to joining TAMIU in 2007, Dr. Bachnak was on the faculty of Texas A&M University-Corpus Christi, Northwestern State University, and Franklin University. His experience includes several fellowships with NASA and the US Navy Laboratories and employment with Koch Industries. Dr. Bachnak is a registered Professional Engineer in the State of Texas, a senior member of IEEE and ISA, and a member of ASEE. During the 2009-2010 academic year, he was a Fulbright Scholar at Notre Dame University, Lebanon.

Susantha Herath is a Professor and Chair of the Information Systems Department at St. Cloud State University, Minnesota. Before moving to St. Cloud, Dr. Herath worked as an Associate Professor of Computer Science at Aizu University, Japan and as an Assistant Professor of Computer Science at Southwest Texas State University, San Marcos, TX. Also, he worked as a visiting researcher at George Mason University, Fairfax, VA, and Electrotechnical Laboratory, Japan. He received his Ph.D. in Computer Engineering from Keio University, M.S. in Industrial Engineering Management from the University of Electrocommunications, Japan and B.S. in Business Administration from the Sri JayawardenapuraUniversity, Sri Lanka. His current research interests are in Information Assurance and Security. He taught numerous courses related to security and has published many papers. Dr. Herath is a Senior Member of the IEEE.