Application of Change Point Outlier Detection Methods in Real Time Intrusion Detection

Naveen N.C. ,
Associate Professor, Department of ISE,
R V College of Engineering, Bangalore
and Research Scholar, Dept of CSE,
SRM University, Chennai, India
naveennc@rvce.edu.in

Dr Natarajan.S,
Professor,
Department of ISE
P E S I T,
Bangalore, India
snatarajan44@gmail.com

Dr Srinivasan.R,
Professor Emeritus,
Department of Computer Science
and Engineering,
M S R I T, Bangalore , India
rsv38@yahoo.co.in

Abstract - **Recent years has shown a growing interest in the development of change detection techniques for the analysis of Intrusion Detection. Current research shows that change detection methods can be used for a wide range of real time applications. Detecting the changes by observing data collected at different times is one of the most important applications of network security because they can provide analysis of short interval on global scale. Research in exploring change detection techniques for medium/high network data can be found for the new generation of very high resolution data. The advent of new technologies has greatly increased the ability to monitor and resolve the details of changes in order to analyze better. Analyzing large amount of data is still a new challenge. The data need to be analyzed and corrected for registration and classification errors for identifying frequently changing trend. In this research paper we have proposed a unified and novel approach for Intrusion Detection System (IDS) which embeds a Change Detection Algorithm with Data Mining (DM) technique. IDS are considered as a system integrated with intelligent subsystems, which completes the distributed solution procedure on the basis of exchanging large data and information. The goal is to learn more effectively from the model. The knowledge developed automatically adjusts to the changes as well as threshold while minimizing the false alarm rate and timely detection. A hybrid approach for improving the performance of detection algorithm by building more intelligence to the system is proposed using Support Vector Machine (SVM). The results are properly substantiated for better effectiveness, system security and flexibility.**

Keywords: Network Intrusion, Anomaly Detection, Change Detection, Threshold Algorithms, Performance Evaluation, Outlier Detection

I. INTRODUCTION

Reasonable level of security is provided by static defense mechanisms such as firewalls and software updates. Dynamic mechanisms can also be used to achieve security such as IDS and Network Analyzers (NA). The main difference between IDS and NA is the IDS aims to achieve the specific goal of detecting attacks whereas NA aims to determine the changing trends in network of computers [1].

IDS involve automatic identification of unusual activity by collecting data, and comparing it with reference data. An assumption of IDS is that a networks' normal behavior is distinct from abnormal or intrusive behavior, which can be a result of various attack/s. There are several approaches for Intrusion Detection which will differ in the features they consider for identifying abnormal activity. Identifying the metrics to be monitored is an important research as the amount of monitored data differ, it affects the detection performance. Data can be particularly large and hence its collection can consume a significant amount of resources.

Intrusion Detection procedures are classified into three categories [2] and they differ in the reference data that is used for detecting unusual activity. Signature based or Misuse detection considers signatures of unusual activity for detection. Anomaly Detection mechanism considers a profile of normal system activity and Protocol-Based (or Specification based) detection considers constraints that characterize the normal behavior of a particular protocol or a program.

In this paper a novel approach for improving the performance of detection algorithm by building additional intelligence to the system is proposed. In this direction Change Point (CP) detection is considered for discovering change points if the properties of network behavior change. CP is the change in characteristics that occur very fast with respect to the sampling period of the measurements, if not instantaneously. The detection of changes refers to tools that help to decide whether such a change has occurred in the characteristics or not. Outlier Detection is a major step in DM problem which discovers abnormal or deviating data points with respect to distribution in data. Outliers are often considered as an error or noise although they may carry very important information.

1.1 Machine Learning versus Statistical Techniques

A wide range of real world applications are discussed in the community of Statistical Analysis and DM [3]. Statistical techniques usually assume an underlying distribution of data and require the elimination of data instances containing noise. Statistical methods though computationally intense can be applied to analyze the data [4]. Statistical methods are widely used to build

978-0-7695-4959-0/13 $25.00 © 2013 IEEE
DOI 10.1109/ACSAT.2012.36

behavior-based IDS. The behavior of the system is measured by a number of variables sampled over time such as the resource usage duration, the amount of processor-memory-disk resources consumed during that session etc. The model keeps averages of all the variables and detects whether thresholds are exceeded based on the standard deviation of the variable.

Earlier work emphasized that data can be obtained by three ways; by using real traffic, using sanitized traffic and also, using simulated traffic [5]. But in real time fast response to external events within an extremely short time is demanded and expected. Therefore, an alternative algorithm to implement real time learning is imperative for critical applications for fast changing environments. Even for offline applications, speed is still a need, and a real-time learning algorithm that reduces training time and human effort to nearly zero would always be of considerable value. Mining data in real time is a big challenge.

II. RELATED WORK

Recent research shows that there are two broad issues relevant to network security: Detection and Prevention. Recently a third type of mechanism namely Response is added. In recent years there is a growing interest in the development of change detection techniques for the analysis of issues pertaining to network security. These developments can also be applied to a wide range of applications like geospatial monitoring, agriculture and monitoring of forests [6].

Coefficient of Variation (CV): The behavior of certain type of data increases proportionally to the average and the average shifts upwards at least by 50% so as the standard deviation. Common examples include filling the process, systems measurements and accuracy of systems. CV can be used for such processes to better characterize by the ratio of the standard deviation to the average [7].

Chauvenet's Criterion [8]: From the mean value of a given sample of N measurements a scatter is defined from this criterion. All data points that fall within a band around the mean that corresponds to the probability of (1-(1/2N)) should be retained. Data points are considered for rejection only if the probability of the deviation obtained from the mean is less than 1/2N.

Peirce's criterion [2, 9]: This technique applies a rigorous method based on probability theory which can be used to eliminate data “outliers” or spurious data in a better way. However, Peirce's criterion can be applied more generally to a data set in Gaussian distributions. A piecewise segmented function as proposed by Stephen M Ross [9] caters for time-dependent data where the change points are qualified as the points between successive segments. A CP may be detected by discovering the point such that all errors of local model fittings of segments to the data before and after that point are minimized. However, it is computationally expensive to converge to such a point as the local model fitting is required as many times as the number of points between the successive points whenever the data is given as an input.

CUSUM (CUmulative SUM) [10]: CUSUM charts can be used to detect deviations from a given predetermined values. This method computes the standard deviation of the observed data from the desired process mean. This is accumulated over time to compute the CUSUM at each given point. The basic rules for interpreting a CUSUM values are 1) if the data is above the overall average - CUSUM value increases 2) if the data is below the overall average - CUSUM value decreases and 3) if values have shifted it means a there is a sudden change in direction.

GLR (Generalized Likelihood Ratio) [11]: This is an intuitive approach for handling the testing problems based on discrepancy measures. The logarithmic value of the likelihood ratio between two consecutive intervals in time-series data will be monitored for detecting change points. The above premise has been extensively explored in the DM community in connection with real world applications.

Direct Density-Ratio [12, 13]: This is an estimation that has been actively explored in the Machine Learning (ML) community, e.g., Kernel Mean Matching which avoids density estimation and directly gives an estimate of the importance at test points.

Research shows that if a malicious activity is detected their statistical properties will no longer remain constant and the network parameters need to be changed. In [14], Chan et al. use a non parametric CUSUM algorithm to identify specific worms which use a hit list of potential target IP addresses to propagate through the network. Each incoming source address is weighted based on heuristics and the total weight in a given time window is calculated. A non-parametric CUSUM is then applied on the total (weighted) source address count. If the current weighted value is greater than a predefined percentage of the mean then the calculated CUSUM score is subjected to a threshold test in order to identify a worm outbreak.

In [4], Bo et al. identifies worm attacks by applying the non-parametric CUSUM algorithm. Similarly in [6], Fabio Pacifici has used the non-parametric CUSUM algorithm to detect Denial of Service (DoS) attacks based on SYN flooding. A framework is provided in [7] by Chen et al. to detect Distributed Denial of Service (DDoS) attack using a distributed change detection algorithm based on the nonparametric CUSUM.

Siris et al. [10] shows that a parametric CUSUM change detection algorithm can be used to detect TCP SYN flooding attack. Different design parameters are calculated using two data sets containing both high and low intensity attacks. Synthetically generated attacks are generated and the real network traffic is used as background noise. The authors have compared two CP detection techniques namely the adaptive threshold and parametric CUSUM algorithms. In both

these techniques results were subject to a threshold that is fixed and is tested to identify the change points. Low, medium and high intensity attacks were used to analyze the performance of the algorithm. Duration and frequency that varies the attack characteristics were not considered. It is also shown that these methods can detect anomalies that cause abrupt changes in the network traffic parameters. Timely detection of an attack is critical in any field and hence identification of an end to the anomalous activity is equally important. The main challenge is to successfully detect attack patterns and reduce the false alarms. Use of a static threshold, for detection of CP results in a higher false alarm in the event of different and diverse attack patterns [15].

The problem of detecting attacks can be formulated and solved as a CP detection problem: detect changes in the distributions (models) with fixed delays (batch approach) or minimal average delays (sequential approach). Choosing the relevant network flow and resource usage characteristic that are to be observed represents a crucial aspect of the development. The observables used for our experiments are discussed in Section III [16]. There are two main approaches for change detection problem namely supervised and unsupervised. Application of these methods depends on the problem. Supervised technique can analyze data can be carried out on temporal data with multiple dimensions as in maps of land-cover transitions etc. Unsupervised techniques can be used to analyze data maps that are associated with damages caused by natural disasters.

Outlier detection is an active research area and is useful in applications developed on Statistics, ML, and DM. Many techniques are proposed in the literature for detecting and identifying outliers [17]. The previous methods are not very effective in detecting outliers and may require too much data analysis time if the data set is large. In the proposed research work CP and Outlier Detection is combined which has improved the detection performance.

Intrusion Detection using Data Mining Technique (IDDM) is one of the real-time Network Intrusion Detection System (NIDS) for misuse and anomaly detection. The architecture uses Association Rules, Meta Rules and Characteristic Rules for Intrusion Detection. DM techniques are employed to produce description of network data collected and the information generated is used for deviation analysis. Mining Audit Data for Automated Models for Intrusion Detection (MADAM ID) is a leading DM project in Intrusion Detection and Prevention.

SVM is a supervised learning algorithm that is used increasingly in IDS. The classification performance of SVM model is better than the classification methods, such as ANN [18]. The benefits of SVM are that they learn very effectively with high dimensional data. A SVM maps input feature vectors into a higher dimensional feature space through some nonlinear mapping. SVMs can learn a larger set of patterns and are able to scale better, because the classification complexity does not depend on the dimensionality of the feature space. SVMs also have the ability to update the training patterns dynamically whenever there is a new pattern detected during classification.

III. METHODOLOGY

Over 90% of Internet traffic has been shown to use the Transmission Control Protocol (TCP). Because of its widespread use and its impressive growth, the research focuses on the detection of anomalous behavior within TCP traffic.

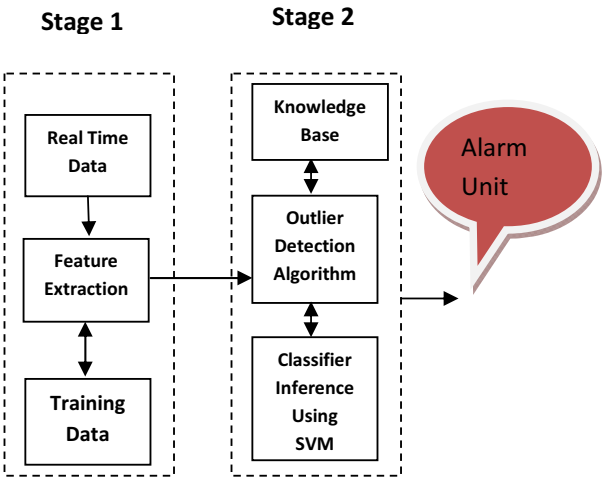

Figure 1: Architecture of the model

3.1 Dataset Description

The process of detecting outliers using Outlier Detection Algorithm is depicted in Figure 1. The first stage of the implementation involves in training the system. For the present problem data is collected from our campus network datasets to measure the accuracy and attacks of different types. Data such collected is preprocessed and used to detect change point in Network performance characteristics. Traffic in the network results in continuous change as the user's login and make use of Internet. For capturing the packets in real time JPCAP and WINPCAP tool is used to collect the information that is being transmitted. JPCAP provides facilities to capture and save raw packets live. It can automatically identify packet types and can generate corresponding Java objects for Ethernet, IPv4, IPv6, ARP/RARP, TCP, UDP, and ICMPv4 packets. Packets can also be filtered according to the user requirement. JPCAP is developed on LIBPCAP / WINPCAP, which is implemented in C and Java and is the industry-standard tool for link-layer network access. In Windows environment WINPCAP allows applications to capture and transmit network packets bypassing the protocol stack.

The network data is collected from the interface which is capable of capturing information flowing within the

local network. For example, anomalies can be detected on a single machine, a group of network a switch or a router. For the current research work the TCP/IP packet is collected in real time from the research lab network and dumped for further process.

The Feature Extraction handles the conversion of raw packet or connection data into a format that DM algorithms can utilize and store the results in the knowledge base. Rather than operating on a raw network dump file, the algorithm uses summary information to perform the analysis. Data is preprocessed to generate summary lines about each connection found in the dump file. The resulting summary file is then parsed and processed by the algorithm to give a gain to each data/each time point, with a higher gain indicating a high possibility of being an outlier/a change point.

The Knowledge Base stores the data as rules produced by the detection algorithm for further mining process. It may also hold information for the preprocessor, such as patterns for recognizing attacks and conversion templates.

The Training Data is responsible for generating the initial rule sets that needs to be used for deviation analysis. It can be triggered automatically based on time or the amount of pre-processed data available.

The proposed Outlier Detection Algorithm examines the network data and creates a description of differences and stores in the knowledge base for further reference. If a deviation is detected it signals the alarm unit. A strategy for invoking the deviation analyzer is by querying periodically the knowledge base for the new profiles. Also the profiler may signal when a new profile is added to the knowledge base.

The Alarm Unit is responsible for informing the administrator when the deviation analyzer reports unusual behavior in the network stream. This can be in the form of SMS, e-mails, console alerts, log entries etc.

IV. PROPOSED ALGORITHM

Change Point Outlier Detection (CPOD): To illustrate the problem, network data collected is observed with threshold values in the college local area network at regular intervals of time window for a certain period of time. In the analysis it is found that the threshold variations are statistically regular most of the time. Once in a while there may be a point that deviates from the normal pattern that can be marked as outlier point. Detection of such outliers is very important as they may be due to an anomaly within the network or from an external environment.

The following are the requirements of CPOD algorithm. The statistics should be on-line meaning an outlier has to be detected as it appears. A CP has to be detected within some constant number of observations after the change happens. Specific assumptions regarding distributions are not considered and hence the detection can be adaptive to a non-stationary time series and robust to a wide variety of distributions.

The major theme of this research is to demonstrate a unified solution for detecting outliers and change points whilst taking care of the above requirements. This algorithm satisfies the on-line requirement as it computes an outlier classification gain for a data point immediately at the time at which it occurs without waiting. CP's are detected after a constant number of successive outliers. As sliding window technique is used the algorithm satisfies the adaptive requirement. This technique overwrites the old data and adapts the thresholds after CP's are detected.

The CPOD Algorithm

The algorithm considers a real time data sequence $\{x_i : i = 1, 2,... N\}$, where i denotes the time window variable. CPx_i denotes the data point in the time series that is currently being considered for analysis. t and s are the thresholds for CP and OD respectively. Threshold value is the mean magnitude of fluctuation allowed in the data points within which they won't be classified that is user defined. The mean and median is computed for window size w and v respectively. When a median over a small window is chosen it is found that it less sensitive to outliers and the deviations are localized. When $w < v$ it is found that selecting $(w/v) < 0.6$ is optimal. A vector maintained that signifies the classification state of each data point that is selected. States could be {A,B,C,D} where 'A' means neither outlier nor change point, 'B' means outlier, 'C' means outlier and high probability that previous point was the change point, and 'D' means the CP done from previous two observations.

If the thresholds are well tuned, CPOD can detect maximum outliers and change points in a time series.

CPOD Algorithm (Input : p,s,t,w,v)

Step 1: The iteration for all data points is done after initializing i=p+1

Step 2: The median and mean over the windows v, w is computed respectively as in Eq. 1 and Eq. 2

$$\pi_i = \tilde{x}_{i-1}^{i-w} \qquad (1)$$

Mean of values in window 'v'

$$\mu_i = \bar{x}_{i-1}^{i-v} \qquad (2)$$

Step 3: $\mathbf{Gain_1}$ is the ratio of absolute difference between the current data point from the median to the mean amplified by the threshold and calculated as

$$\mathbf{Gain_{1i} = (|\mu_i - \pi_i| * t) / \mu_i \text{ and}} \qquad (3)$$

$\mathbf{Gain_2}$ is the ratio that is normalized between two distance magnitudes.

$$\mathbf{Gain_{2i} = (|\pi_i - \mu_i|)/ (|\mu_i - \pi_i|) * 100} \quad \mathbf{(4)}$$

The median that is calculated is over the short term window w. Similarly the mean is calculated over the longer term window v. This ratio makes $Gain_2$ much more robust to fluctuations that may happen in the long terms μ. Using Brute Force method is found that selecting (w/v < 0.5) would be the best choice as this depends on the performance of detection of outliers. If $Gain_1 > Gain_2$, the data point is classified as an outlier. $Gain_2$ is used as a data dependent threshold that classifies $Gain_1$ as outlier or not. $Gain_1$ is always sensitive to the mean and to the variation of current data point from median. $Gain_2$ is always sensitive to deviation of current data point from mean and to variation of mean from median. In the presence of outliers in window v, $Gain_1$ will be greater than $Gain_2$.

Step 4: A stronger possibility of current data point being an outlier or CP is indicated if $Gain_1$ is higher than $Gain_2$. To classify the current data point as CP an additional check is made to find if the point lies beyond a certain band around the median represented as LL_i and UL_i. The classification state is then saved in vector V.

$$\mathbf{Gain_{1i}} \begin{cases} > Gain_{2i} \wedge (CPx_i < LL_i \vee CPx_i > UL_i) : GV_i = B \\ \leq Gain_{2i} \vee (LL_i > CPx_i > UL_i) : GV_i = A \end{cases} \quad \mathbf{(5)}$$

Step 5: Gain information in vector GV is used to classify outlier and CP. If the current point has a higher $Gain_1$ as indicated in GV_i the past three states is considered for classification. Vector GV_{si} is the sum state of GV_i,GV_{i-1} and GV_{i-2} which stores state of the past two data points with respect to the selected current data point. If the value of GV_{si} is 3 it indicates that outliers were detected in the past and current point could be the change point. We test the previous states to make sure there was no change point detected in the past two data points. If detected then the CP is inferred as an outlier. Similarly if the value of GV_{si} is 1 then it is possible that current point is an outlier as shown in Eq. 6 and Eq. 7.

$$\mathbf{GV}_i \begin{cases} = \mathbf{B} \ : \ \mathbf{GV_{si}} = (GV_i + GV_{i-1} + GV_{i-2}) & \mathbf{(6)} \\ = \mathbf{A} \ : \ \mathbf{GV_{si}} = \mathbf{0} & \mathbf{(7)} \end{cases}$$

$$\mathbf{GV_{si}} \begin{cases} = \mathbf{D} \wedge (GV_{s\,i-1} = \mathbf{D} \vee GV_{s\,i-2} = \mathbf{D}) \ : \ GV_{s\,i} = \mathbf{B} \\ = \mathbf{B} \wedge (GV_{s\,i-1} = \mathbf{B} \vee GV_{s\,i-2} = \mathbf{B}) : GV_{s\,i} = GV_{s\,i} + GV_{s\,i} - \mathbf{1} \end{cases}$$

Finally CPx_i is classified depending on the values of GV_{si}. If the value of the current point is 0, then it is inferred that there is no significant deviation. If the current point is 1 or 2 and the current data point deviates more than t% threshold it is inferred as an outlier and signifies a higher possibility of CPx_i - 1 being a CP. If the state of current point is 3, with accuracy it is inferred that two points prior to current one is the CP.

$$\mathbf{GV_{si}} \begin{cases} = \mathbf{A} : \mathbf{No\ change\ ,\ adjust\ LL,\ UL\ to\ } \pi_i \\ = (\mathbf{B} \vee \mathbf{C}) \wedge (\ CPx_i > (CPx_i + t\ \%\ CPx_i\ )\ ) : \mathbf{Outlier} \\ > \mathbf{2} : \mathbf{Change\ point,\ adjust\ LL,\ UL} \end{cases}$$

Step 6: The classification of outliers and CP as signified in the GV_{si} vector is reported. The Gains and state elements of vector GV, GV_s for past data points N, N-1 and N-2 are persisted. Persistence of median and mean over the window sizes while classifying current data point enables online implementation.

V. EXPERIMENTAL RESULTS

The log file contains four weeks of training data and one week of testing data. Table 1 lists the statistics of IP addresses and their count observed in our research laboratory for a time period of 30 minutes specified as window 'w_1', 'w_2', 'w_3'. The values shown is the count to each data/each time point, with a higher gain indicating a high possibility of being an outlier/a change point. The number of source/destination IP addresses (nSrcs; nDsts; nSrcPorts; nDstPorts) and average packet size (avgPktsSize) features are used to calculate the IP address count for DoS attack.

TABLE I . REAL TIME DATA COLLECTED

IP Address	Time Window 'w_1'	Time Window 'w_2'	Time Window 'w_3'
172.16.30.28	2110	2011	2140
172.16.30.91	86	88	90
172.16.30.75	425	462	512
172.16.30.108	140	140	140
172.16.30.70	24	24	24
172.16.30.92	58	58	58
172.16.30.68,	175	175	179
172.16.30.69	14	14	14
172.16.30.96	14	14	14
172.16.30.35	7	7	7
172.16.30.95	101	120	110

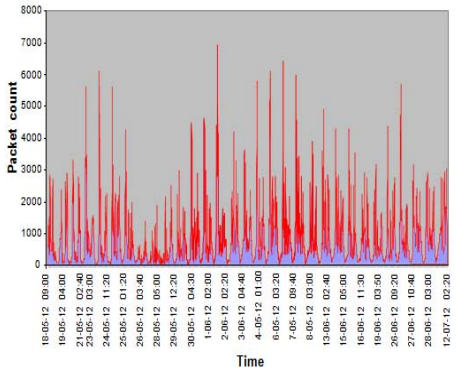

Figure 2: Plot of real time data collected for 4 weeks

For the real time statistics the data was collected for one week and the graph is as shown in Figure 2.

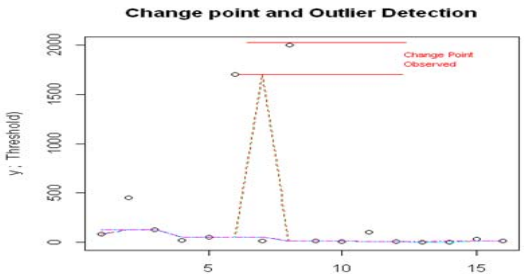

Figure 3: Plot of real time data and detection of change point and outliers

As Figure 3 shows outliers and change points that were detected. The test data consists of small, medium and large magnitude of changes and also outliers in each segment. The algorithm was able to detect all outliers as well as classify change points.

Experiments were done using R statistical framework. Performance of the process at each level is measured. In order to train the SVM, unique IP addresses with 19 different feature and 3043 training instances that contains 375 and 459 test instances for normal and attack were used respectively.

Table II. Error obtained by the SVM with different parametric values

Poly Kernel	Degree 1	Degree 2	Degree 3	Degree 4
Error Rate	**0.102**	**0.093**	**0.081**	**0.052**
RBF Kernel	**σ =1**	**σ =4**	**σ=6**	**σ=9**
Error Rate	**0.094**	**0.072**	**0.051**	**0.043**

Table II summarize the training results where the generalization error obtained by the classifier is listed under different parametric values. SVM achieved the best error level with a degree 5 polynomial kernel.

VI. CONCLUSION

In this research a solution for classifying outliers and change points from real time data is proposed which is addressed in two parts gain and classification. Gain is computed that reflects outliers and incrementally discovers to keep the state of outliers in data series. The algorithm is characterized in its aspect to address outliers and change points at the same time. This enabled to deal with frequently and fast changes in the source. The current implementation and usage indicates the success of the algorithm. This gave a unifying view of OD and CP detection in real time network data. The proposed method uses mathematical, statistical and SVM techniques to rank the participation of individual features into the detection process. The results empirically confirm that the proposed model can successfully be applied to mine new features in the detection process.

Future research in this area can be on applying other DM methods. Problem of classifying rarely seen attack types is still a major work. Studies could be conducted on addressing more attack types which are totally new, or variations on existing types. The important work is to identify the exact source of a given attack. It is possible to reduce the complexity of carefully tuning the thresholds and window sizes by adding a prediction layer. The core future idea is to develop a layer that predicts next data point with some probability.

REFERENCES

[1] Olin Hyde, Machine Learning For Cyber Security at Network Speed & Scale, 1st Public Edition: AI-ONE INC. October 11, 2011

[2] Amitabh Mishra, Ketan Nadkarni, and Animesh Patcha, Virginia Tech, Intrusion Detection in Wireless Ad Hoc Networks, IEEE Wireless Communications, February 2004

[3] Ben-Gal I., Outlier Detection, Data Mining and Knowledge Discovery Handbook: A Complete Guide for Practitioners and Researchers," Kluwer Academic Publishers, 2005, ISBN 0-387-24435-2.

[4] G. Mohammed Nazer, A. Arul Lawrence Selvakumar, Current Intrusion Detection Techniques in Information, European Journal of Scientific Research, Euro Journals Publishing, Inc. 2011, pp. 611-624

[5] Iftikhar Ahmad, Azween Abdullah and Abdullah Alghamdi, Towards the Selection of Best Neural Network System for Intrusion Detection, International Journal of the Physical Sciences Vol. 5(12), October, 2010, pp. 1830-1839

[6] Fabio Pacifici, Change Detection Algorithms: State of the Art, v1.2, Earth Observation Laboratory, Tor Vergata University, Rome, Italy, Feb 28, 2007

[7] Jo.ao B. D. Cabrera, Jaykumar Gosar, Wenke Lee_and Raman K. Mehra, On the Statistical Distribution of Processing Times in Network Intrusion Detection, Proceedings of the 43rd IEEE Conference on Decision and Control, Bahamas, December 2004

[8] N. P. Olewuezi, Some Basic Tests on Time Series Outliers, Federal University of Technology Owerri, Nigeria, Journal of the Nigerian Association of Mathematical Physics Volume 15 (November, 2009), pp 101 – 106

[9] Stephen M. Ross, Peirce's Criterion for the Elimination of Suspect Experimental Data, Journal of Engineering Technology, Fall 2003

[10] Basseville, M. and Nikiforov, V., Detection of Abrupt Changes: Theory and Applications, Prentice-Hall, Inc., Englewood Cliffs, N. J., 1993.

[11] Gustafsson, F., Adaptive Filtering and Change Detection, John Wiley & Sons Inc., 2000.

[12] Yoshinobu Kawahara, Masashi Sugiyama , Sequential Change Point Detection Based on Direct Density Ratio Estimation, Statistical Analysis and Data Mining, vol.5, no.2, 2012, pp.114 - 127.

[13] Shohei Hido , Yuta Tsuboi , Hisashi Kashima , Masashi Sugiyama , Takafumi Kanamori , Statistical Outlier Detection Using Direct Density Ratio Estimation, Knowledge and Information Systems. vol.26, no.2, 2011, pp.309-336

[14] Jeffrey Chan, Christopher Leckie, Tao Peng, Hitlist Worm Detection using Source IP Address History, NICTA Victoria Research Laboratory, The University of Melbourne, Australia

[15] Ejaz Ahmed, Andrew Clark, George Mohay, A Novel Sliding Window Based Change Detection Algorithm for Asymmetric Traffic, IFIP International Conference on Network and Parallel Computing, 2008

[16] Alexander G. Tartakovsky, Boris L. Rozovskii, Rudolf B. Bla˘zek, and Hongjoong Kim, A Novel Approach to Detection of Intrusions in Computer Networks via Adaptive Sequential and Batch Sequential Change-Point Detection Methods, IEEE Transactions On Signal Processing, Vol. 54, No. 9, September 2006, pp 3372- 3382

[17] G. Buzzi-Ferraris, F. Manenti, "Interpolation and Regression Models for the Chemical Engineer: Solving Numerical Problems", Wiley-VCH, Weinheim, Germany 2010.

[18] Moguerza Javier M., Munoz A., "Support Vector Machines with Applications", Statistical Science, Vol. 21, No. 3, pp 322 – 336, 2006