# Network Anomaly Detection System: The State of Art of Network Behaviour Analysis

Shu Yun Lim[1], Andy Jones[2]
[1]British Telecommunications plc., Malaysia Research Centre, Kuala Lumpur, Malaysia
shuyun.lim@bt.com
[2]British Telecommunications plc., Security Research Centre, Ipswich, United Kingdom
andrew.28.jones@bt.com

## Abstract

*This paper presents a taxonomy of anomaly detection techniques that is then used to survey and classify a number of research prototypes and commercial products. Commercial products and solutions based anomaly detection techniques are beginning to establish themselves in mainstream security solutions alongside firewalls, intrusion prevention systems and network monitoring solutions. These solutions are focused mainly on network-based anomaly detection, thus creating a new industry buzzword that describes it: Network Behavior Analysis. This classification is used predictably, pointing towards a number of areas of future research in the field of anomaly detection.*

## 1. Introduction

There is an urgent need for a solution that can actively defend networks against the growing sophistication and damage potential of network threats. This is where network Intrusion Detection System (IDS) comes in to offer security in addition to that provided by traditional anti-threat applications such as firewalls, antivirus software and spy-ware detection software. Network IDS can be categorized into anomaly detection and misuse detection. Anomaly detection is carried out based on the desired or positive behaviour of users and processes. Based on this normative specification of positive behaviour, attacks are identified by observing deviations from the established normal usage profiles. It does not require prior knowledge of intrusions and can thus detect new intrusions. Conversely, misuse detection is based on the specification of the undesirable or negative behaviour of users and processes. It tries to detect patterns of known attacks and weak spots in a system. It performs a pattern match between audit data streams and an attack signature and generates alarms if the match is successful.

For the last decade, misuse detection has been the dominant strategy for intrusion detection systems. Misuse detection prevailed for the reasons that it is easier for the developer to implement and easier for the analyst to understand. However, anomaly detection is not dead. Implementing this heuristic detection technique has the advantage of detecting novel intrusions without any prior knowledge as the intrusion is attempted. The anomaly detector monitors network segments to compare their state to the normal baseline and look for anomalies. The architecture of a generic anomaly detection system consists of three components namely the sensor subsystem, modeling subsystem and the detection subsystem [1]. The sensor subsystem is responsible for monitoring the input traffic to the anomaly detection system, the modeling subsystem is responsible for generating the profile of normal traffic usage and the detection subsystem is for tracking network characteristics in real time and flag anomalous activity if a strange event that could indicate a threat is presence. Generally, baseline behavioral model construction and detection operations are carried out separately. The process begins with the training of the anomaly detection sensor. This is accomplished by observing specific events in the monitoring environment such as network traffic over a designated time period. The appliances are left for a few days or weeks to monitor the network and gradually build up a picture of all hosts, how they interact with each other and general traffic flows. When the interval expires, a profiling method is used to generate a measure for the observed data. The result is a baseline for some variable of a system's behavior for instance the normal state of the network's traffic load, protocol, and typical packet size. Therefore the essential component of an anomaly detector is the behaviour model of the system which serves as a pattern of correctness. Nevertheless, if there are loop-holes in the profile generated, such that the profile is learnt under abnormal traffics which has been presumed as normal background traffic, malicious attacks that conform to that abnormal profile will go unnoticed by the anomaly detection system.

The growing interest in the research and development of anomaly-based detection systems raised a need for an up-to-date and thorough survey of the research in the network anomaly detection field.

978-0-7695-3328-5/08 $25.00 © 2008 IEEE
DOI 10.1109/ICHIT.2008.249

This paper presents such a survey, focusing on network anomaly behavior analysis and surveyed systems according to taxonomy.

## 2. A Taxonomy of Network Anomaly Behaviour Analysis

There are many anomaly detection algorithms proposed in the literature that differ according to the information used for analysis and according to techniques that are employed to detect deviations from normal behavior. In this section, we provide classification of anomaly detection techniques based on employed techniques into two groups: *2.1 learnt model method* and *2.2 specification model*. Although anomaly detection algorithms are quite diverse in nature, and thus may fit into more than one proposed category, this classification attempts to find the most suitable category for all described anomaly detection algorithms. In any case, anomaly detection is still considered to be a 'hard' problem in several domains. This taxonomy is expected to continuously evolve before achieving a solid maturity for its implementation.

We have two approaches for building the behaviour model which are *learning-based* and *specification-based*. The former is based on the application of machine learning techniques, in order to automatically obtain a representation of normal behaviours from the analysis of system activity. The latter requires that someone manually provide specifications of correct behaviour. All the approaches that concern the model construction are presented in Figure 1.

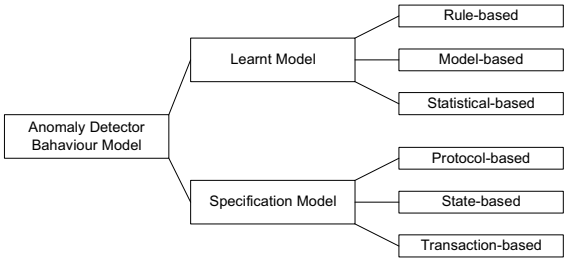


Figure 1. Taxanomy of anomaly detector behavioral model.

### 2.1. Learnt Model

An anomaly detection model must be trained on the specific network or host to be monitored. In the training phase, the behaviour of the system is observed and machine learning techniques are used to create a profile of such normal behaviours. In the process of creating an effective anomaly detection model, *rule-based*, *model-based*, and *statistical-based* approaches have been adopted to create the baseline profile.

#### 2.1.1. Rule-based

Rule-based systems used in anomaly detection characterize the normal behaviour of users, networks and/or computer systems by a set of rules. These predefined rules typically look for the high-level state change patterns observed in the audit data compared to predefined penetration state change scenarios.

**Expert System**

The expert system is an extension of rule-based systems. The system state is represented in a *knowledge base* consisting of a *fact base* and a *rule base*. A fact base is a collection of assertions that can be made on accumulated data from the audit records or directly from system activity monitoring. The rule base contains the rules that describe known intrusion scenario or generic techniques. When a pattern of a rule's antecedent matches the asserted fact, a rule-fact binding is created. After this binding is made, if all the patterns of the rule have been matched, then a binding analysis is performed to make sure that all the associated variables with the rule are consistent with the binding.

Probably the best known rule-based anomaly detection system is the expert system whose rules fire when audit records that are parsed appear to be of suspicious activity [2]. This technique first identifies expected behaviour at the user, group, remote host, target system levels, and then trigger rules in the expert system rule base if observed behaviour deviates significantly from normal behaviour.

SRI International's Next-generation Intrusion Detection Expert System (NIDES) [3] is an innovative statistical algorithm for anomaly detection, as well as an expert system that encodes known intrusion scenarios. The features considered by NIDES are related to user activity, for instance CPU usage and file usage. The usage rate or intensity features derived are used to match with the long term profile and deviations for the system are learned and then summarized in a chi-squared statistic. The system learned an empirical distribution rather than referring to a standard table. A variant of incorporating expert system in anomaly detection is presented in [4]. S. Owens et. al. presented an adaptive expert system for intrusion detection that utilises fuzzy sets. Fuzzy sets are sets whose elements have degrees of membership. This theory permits the gradual assessment of the membership of elements in a set and it is described with the aid of a membership function valued in the real unit interval 0 and 1. Therefore, this system has the ability to adapt to the type and degree of threat, and it is relatively simple to implement it in anomaly detection system which has a high degree of uncertainty and ambiguity.

These rule-based systems rely heavily on the expertise of the network manager and do no adapt well to the evolving network environment. T.D. Ndousse and T. Okuda [5] describes an expert system model using fuzzy cognitive maps (FCM) to overcome this limitation. FCMs are constructed with the nodes of the FCM denoting managed objects such as network nodes and the arcs denoting the fault propagation model. FCM can be used to obtain an intelligent modelling of propagation and interaction of network faults.

### 2.1.2. Model-based

As opposed to rule-based intrusion detection, model based intrusion detection attempts to model intrusions at a higher level of abstraction than audit records. The model-based technique differs from current rule-based techniques, which simply attempts to bind audit records to expert rules. A model-based anomaly detector restricts execution to a pre-computed model of expected behaviour. In this approach more data can be processed, because the technique allows you to narrow the focus of the data selectively. Besides, more intuitive explanations of intrusion attempts are possible whereby the system can actually predict the intruder's next action. Constructing a model that balances the competing needs of detection ability and efficiency is a challenging task.

Many researchers have used different types of models to characterize the normal behaviour of the monitored system. In the model-based approaches, anomalies are detected as deviations from the model that represents the normal behaviour. Very often, researchers have used approaches like *data mining*, *neural networks*, *pattern matching, etc.* to build predictive models.

**Data Mining**

Data mining generally refers to the process of automatically extracting models from a large amount of data. Since many current IDSs require frequent updates as new attack methods are continuously being discovered, data mining techniques that can adaptively build intrusion detection models have a great deal of utility. The central idea is to utilize auditing programs to extract an extensive set of features that describe each network connection or host session, and apply a data mining program to learn rules that accurately capture the behaviour of intrusions and normal activities.

By applying data mining techniques, W. Lee et. al. [6] proposed a framework consisting of meta classification for learning correlation between intrusion evidence, association rules for link analysis and frequent episodes for sequence analysis, as well as supporting an environment that enables system builders to interactively construct detection models. The key idea is to mine network audit data then use the patterns to compute inductively learned classifiers that can recognize anomalies and known intrusions.

**Neural Networks**

Neural networks are known for good performance in learning system-call sequences. The basic approach here is to train the neural net on a sequence of information units, each of which may be at a more abstract level than an audit record. Once the neural net is trained on a set of representative command sequences of a user, the net constitutes the profile of the user, and the fraction of incorrectly predicted events then measures, in some sense, the variance of the user behaviour from his profile.

A Neural Network Intrusion detector (NNID) is a back propagation neural network trained to identify users based on what commands they use during a day. The system administrator runs NNID at the end of each day to see if the users' sessions match their normal pattern. If not, an investigation can be launched. This neural network can generalise from past observed behaviour to recognise similar future behaviours. In the work of Ryan, J et. al. [7] the NNID model was implemented in a UNIX environment and consisted of keeping logs of the commands executed, forming command histograms for each user, and learning the users' profiles from these histograms. NNID provides an elegant solution to off-line monitoring utilizing these user profiles.

Anup K. Ghosh et. al. [8] describe process-based intrusion detection approaches that provide the ability to generalize from previous observed behaviour in order to recognise future unseen behaviour. This approach employs artificial neural networks (ANN) and can be used for both anomaly detection to detect novel attacks and misuse detection to detect known attacks and even with variations of known attacks. S. J. Han et. al. [9] had proposed an evolutionary neural network (ENN). ENN does not require trial-and-error cycles for designing network structures and the near-optimal structure can be obtained automatically. This means that better classifiers can be acquired in shorter time periods.

Modeling networking trends for a simple representation of a neural network shows great promise, especially on an individual attack basis. Once trained, the neural network can make decisions quickly, facilitating real-time detection. Neural networks using both supervised and unsupervised learning have many advantages in analysing network traffic trends and will be a continuing area of research.

**Pattern Matching**

This approach attempts to deal with the variability in the network environment and describes anomalies as deviations from normal behaviour. In this approach, online learning is used to build a traffic profile for a given network. Traffic profiles are built using symptom-specific feature vectors such as link utilization, packet loss, and number of collisions. Normal behaviour of time series data is captured as templates and tolerance limits are set, based on different levels of standard deviation. These profiles are then categorised by time of day, day of week and so on. When newly acquired data fails to fit within some confidence interval of the developed profiles then an anomaly is declared. The efficiency of this pattern matching approach depends on the accuracy of the traffic profile generated. Given a new network, it may be necessary to spend a considerable amount of time building traffic profiles and this method might not scale well with the evolving network topologies and traffic conditions.

### 2.1.3. Statistical-based

Denning and Neumann [10] presented a detailed discussion of statistical-based anomaly detection for the first time in 1985. The anomaly detector observes the activity of subjects and generates profiles for them that represent their behaviour. These profiles are designed to use little memory to store their internal state, and to be efficient in updating because every profile may potentially be updated for every audit record. As audit records are processed, the system periodically generates a quantitative measure of the normal profile.

The well-studied techniques in statistics can often be applied. For example, data points that lie beyond a multiple of the standard deviation on either side of the mean might be considered anomalous. The integral of the absolute difference of two functions over time might also be used as an indicator of the deviation of one function with respect to the other. There are more statistical technique like *Bayesian statistics*, *covariance matrices and Chi-square statistics* [11] for the profiling of anomaly detection. Nevertheless, statistical approaches have their disadvantages as statistical measures are insensitive to the order of occurrence of events. Sequential interrelationships among events should be considered for more accurate detection. It is also difficult to determine a threshold above which an anomaly should be considered intrusive. Imprecise thresholds usually lead to either false positive or false negative intrusions.

## 2.2. Specification Model

The specification approach depends less on mathematics and more on human observation and expertise. It was first proposed by C. Ko et. al. [12] and it uses a logic based description of expected behaviour to construct a base model. This specification-based anomaly detection system monitors multiple system elements, ranging from application to network traffic.

### 2.2.1. Protocol-based

Instead of training models on normal behaviour, protocol anomaly detectors build models of TCP/IP protocols using their specifications [13]. Statistical anomaly detection is overwhelmed by the inherent inability to create a normal model of network traffic statistics. Protocol anomaly detection is much easier because protocols are well defined and a normal use model can be created with greater accuracy.

A protocol anomaly filter as proposed by E. Lemonnier [13] is able to specifically analyse a protocol and model the normal usage of a specific protocol. This technique can be seen as a filter looking for protocol misuse. ‘Protocol’ in this sense should be interpreted as any official set of rules describing the interaction between the elements of a computer system. Protocols always have theoretical rules governing their usage. The rules can either refer to their official description in documents such as RFCs or the practical area of usage of this protocol. Therefore, any use of this protocol outside the defined area can be considered as a protocol anomaly. Protocol anomaly filters are thus able to detect all attacks by deviations from the normal usage of the protocols, including novel attacks that are unknown to any authorities. Accordingly, this ability of detecting new attacks added to the fact that they do not require signature database updates and has as long a lifetime as the protocol they are monitoring, makes it superior to signature filters.

### 2.2.2. State-based

All connection oriented protocols have a state. Certain events must take place at certain times. As a result, many protocol anomaly detectors are built as state machines [14]. Each state corresponds to a part of the connection, such as a server waiting for a response from client. The transitions between the states describe the legal and expected changes between states. Besides, Z. Shan et. al. [21] uses network state based model approach to describe intrusion sand attacks. The model which uses FA theory and can detect unknown attacks, the attacks and intrusions are described by the states and state transitions of network protocols and operating systems.

#### 2.2.3. Transaction-based

The transaction based approach formally describes positive behaviour. It specifies the desired actions and sequence of actions by the definition of transactions. This explicit definition makes the transaction an integral part of security policy.

Transactions are a well known concept originating from the field of database management systems and now widely applied in other environments such as distributed systems. This generally consists of a sequence of Read/Write operations. In the research proposed by R. Buschkes et. al. [15] the detection of anomalies is based on the definition of correct transactional behaviour. This definition of correct, desired behaviour defines the system's multi-level security policy, which is monitored during runtime by the IDS. In contrast to classical database and other transactional systems it does not enforce the distinct transactions to be executed. Instead, it monitors the system only for potential conflicts.

Anomaly detection, while already well established, is in fact a continuing flow of techniques and concepts that are moving from research and development into production and application. Since vendors are working to associate the detection techniques with their products, the line separating academic research and commercial product is increasingly blurred. In the next section we outline the key anomaly detection products currently available in the computer security industry.

## 3. Commercial Products

The findings in this section are based on product information gathered primarily from vendors' web sites. Table 1 depicts the broadening functionality of the commercial network anomaly detection products.

Table 1. Anomaly Detection Products and Characteristics

| Product name | Target Network | Behavioral analysis | Sampling method | Threat analysis |
|---|---|---|---|---|
| Peakflow SP/X (Arbor network) | Enterprise/ Service provider | Rule-based | Packet/Flow | ATF[a] ASERT[b] |
| Proventia ADS (IBM-ISS) | Enterprise | Rule-based, Model-based, Statistical-based | Packet/Flow | ATF[c] |
| Esphion | Enterprise/ Service provider | Neural network | Packet | - |
| CounterStorm | Enterprise | Statistical-based | Flow | ART[d] |

a. Active Threat Feed by Arbor Network
b. Arbor Security Engineering and Response Team by Arbor Network
c. Active Threat Feed by IBM-ISS
d. Active Recognition Technology by CounterStorm

### 3.1. Peakflow

Arbor Networks [16] is an early NBA pioneer, providing network security visibility in service provider and enterprise networks. There is the Peakflow X series targeted for enterprise networks, and the Peakflow SP series aimed at carrier class service providers. Peakflow works by collecting network data from different network devices; then analyses the data to produce meaningful network security information for operators. The behaviour of the Peakflow system is determined by policies containing multiple rules. System rules detect host and port scans along with flood attacks whilst Active Threat Feed (ATF) rules use fingerprints to detect threats such as known DDOS attacks, malware, worms, botnet traffic and P2P protocols. User defined rules allow you to define traffic that you specifically want to watch. Peakflow X can also integrate with Active Directory and Novell's eDirectory allowing it to track users based on their login credentials.

False positives and false negatives also exist for this product. For example, a sudden surge in network traffic due to legitimate requests for live Olympics video streaming may fire off anomalies (false positive); or low intensity hack attacks that do not deviate enough to affect the normal behaviour of the network (false negative). To minimise these occurrences, the product also combines both misuse detection and anomaly detection techniques. The misuse detection technique is based on Arbor Networks' ASERT (Arbor Security Engineering and Response Team) initiative. ASERT combines suspicious network information collected from honeypots and Peakflows installed at participating service providers around the world, and then creates signatures of emerging threats. These signatures are then used by Peakflows to detect emerging threats, lower "security alert events noise" (known threats can be identified more accurately, hence reducing false positives and reducing overwhelming security alert events) and may also lower false negatives (similar low intensity attacks detected elsewhere can be used to flag an alert when detected locally).

### 3.2. Proventia Network ADS

IBM-ISS has been recognized as the world leader in the intrusion detection (IDS) and intrusion prevention (IPS) market in 2007 in a new research service report by global growth consulting company, Frost & Sullivan. IBM-ISS was also the pioneering force behind commercial Intrusion Detection Systems (IDS) offerings in late 1990's and early 2000's. Today, ISS offers a comprehensive array of security products that cover host security, network security and centralised security management.

IBM Proventia Network Anomaly Detection System [17] is designed for enterprise users to monitor and analyse network information within the enterprise. This network behavior analysis system enhances network intelligence and security by auditing network flow data from existing infrastructure devices. It goes beyond basic Cisco NetFlow [18] collection to perform full reassembly of all disparate flow information, converting raw flow into actionable security information. Proventia Network ADS uses patented technology to model networks and understand internal threats. This product leverages six unique detection engines to constantly monitor for threats, network abnormalities and misuse. Using rate-based (statistical-based) anomaly detection, it detects sudden shifts from baseline traffic levels over time. Proventia network ADS also uses Active Threat Feed (ATF) which contains the latest network and security behavioral intelligence. Once updated, it immediately begins analyzing network-wide flow data for these new behaviors.

### 3.3. Esphion

Esphion [19] appliances detect, in real-time, network anomalies and threats such as denial of service attacks (DDoS), worm outbreaks, and other threats in enterprise and service provider network. Both Esphion EX and SP appliances use neural network to continuously profile the behaviour of network traffic to learn normal traffic behaviour. Neural network technologies rapidly detect the emergence of previously unseen and unknown threats. The intelligent neural agent is incorporated in the controller to detect anomalies without relying on out-of-date signature databases. In addition, this product builds a 'normal' profile of the network with packet-based analysis, thus eliminates reliance on weaknesses of flow-based systems.

### 3.4. CounterStorm

CounterStorm [20] is a leading provider of modular threat detection and mitigation software development kits (SDKs) to security and infrastructure companies, as well as sophisticated government and commercial end users. Its core intellectual property consists of Active Recognition Technology (ART) a distributed, modular and signatureless threat detection architecture, an integrated correlation engine, and an extensible software platform on which all of these capabilities are delivered. Its multi-engine architecture provides comprehensive exploit detection such as low and slow stealthy surveillance detection, fast-scanning worm detection, packet header anomaly detection, traffic flow anomaly detection, e-mail flow anomaly detection and statistical payload anomaly detection.

CounterStorm's Statistical Payload Analysis (SPA) Engine is the first and only application layer anomaly detection solution in the market. SPA dynamically builds a model for each application, flow direction and packet size that identifies normal content usage. Deviations from the normal model indicate an anomaly and a possible application layer exploit. Not based on signatures or rules, SPA does not rely on prior application knowledge, like protocol anomaly detection. It operates at a per packet level to learn the normal content profile of any application on the network. SPA was developed specifically to detect the low profile, slow and stealthy behavior characteristic of targeted attacks. SPA enhances security infrastructures with a signatureless deep packet inspection solution capable of accurately identifying application layer exploits, botnet activity and rootkits. It runs at the lowest level of the machine and typically intercepts API calls. For instance, it can intercept requests to a file manager such as Explorer and cause it to keep certain files hidden from display and can even report false file counts and sizes to the user.

## 4. Challenges to Network Anomaly Detection

Current network behaviour anomaly detection does not provide a true security solution against threats, especially for larger deployments. The ingredients required to provide adequate defence against attacks include speed, accuracy and the ability to actively block attacks from spreading to other machines, systems and networks. Anomaly detection falls short as it is too slow to detect fast-spreading virus and worm attacks. In many cases, whole networks can be infected in a matter of minutes. Anomaly detection relies on network flow data, which is often reported at intervals of 15 to 45 minutes. This latency can translate into hundreds of machines being compromised before an attack is detected. It is necessary to envisage a method to handle high volume of data with less information loss.

The efficiency of ADS is dependent on the network normal behavior modeling. Various techniques, as addressed in Section II, have been researched to improve on the efficiency of the generated profile. However, network normal behavior can be subjective and anomalies may not be well defined since the normal profile is subject to the current state of normality in the network, which may be compromised by very low intensity attacks. Moreover, with the advent of new technologies it is common to see the introduction of new protocols, application usage

models or changes of network topologies. These legitimate changes will be marked as anomalous if this new traffic and usage patterns do not match with the initially generated baseline profile. From time to time, the baseline profile should be rebuilt to adapt to the evolving network environment and usage patterns. Hence, the accuracy of the generated profile and the adaptiveness of the profile is one of the most significant catalyses in determining the success or failure of anomaly detection system in an evolving environment.

Network ADS is also challenged to reduce the number of false alarm. It normally gives users a false sense by producing enormous number of false positives. Because anomaly detection is looking for an anomalous event rather than an attack, it is frequently plagued by time-consuming false positives. Besides, anomaly detection systems are unable to mitigate slow, stealthy and sophisticated attacks. Hackers are using this method, essentially spreading an attack over a longer time, to fly under the radar of anomaly detection engines and other security devices. From the theoretical point of view, it is essential for ADS to improve the accuracy of anomaly detection, react in real-time to avert an intrusion or to limit potential damage.

## 5. Conclusions

Anomaly detection will continue to play a key role in advancing the capabilities of security technology. Thankfully, as the techniques and tools move from research and development into production and application, the products and services that are available are increasing in number and capability. Anomaly detection will continue to be used in conjunction with firewalls and intrusion detection systems to create a robust defence for networks and hosts. In time, components of all three will be used to transparently enforce policy, report misuse and protect against unknown threats. ADS will focus on integrating solutions such as network access control, intrusion prevention and behavioral anomaly detection to create an intelligent network. By pulling all of these solutions together, this evolution in the technology cycle will help to obtain unprecedented level of security.

## 6. References


[1] J.M. Estevez-Tapiador, P. Garcia-Teodoro and J.E. Diaz-Verdejo, “Anomaly detection methods in wired networks: a survey and taxonomy”, Computer Communications 27,pp. 1569-1584, 2004.

[2] Ilgun, Koral, "USTAT: A Real-time Intrusion Detection System for UNIX”, Proceedings of the 1993 Computer Society Symposium on Research in Security and Privacy. Oakland, California, 1993.

[3] D. Anderson, Thane Frivold, A. Valdes “ Next-generation Intrusion Detection Expert System (NIDES)”, 2005.

[4] S. Owens, R. Levary, “An adaptive expert system approach for intrusion detection”, International Journal of Security and Networks, Volume 1, Numbers 3-4, 2006.

[5] T.D. Ndousse, T. Okuda, “Computational intelligence for distributed fault management in networks using fuzzy cognitive maps,” in Proc. IEEE ICC, Dallas, TX, 1996.

[6] W. Lee, S. J. Stolfo, “Data mining approaches for intrusion detection”, In Proceedings of the 7th USENIX Security Symposium, 1998.

[7] J. Ryan, M. Lin, R. Miikkulainen, "Intrusion Detection with Neural Networks”, Advances in Neural Information Processing Systems, Vol. 10, 1998.

[8] Anup K. Ghosh and Aaron Schwartzbard, “A Study in Using Neural Networks for Anomaly and Misuse Detection”, Proceedings of the 8th USENIX Security Symposium, Washington, D.C., USA, 1999.

[9] Sang-Jun Han and Sung-Bae Cho, “Evolutionary Neural Networks for Anomaly Detection Based on the Behaviour of a Program”, IEEE Transactions on Systems, Man and Cybernetics, 2006.

[10] D. Denning, P. Neumann,"Requirements and Model for IDES--A Real-Time Intrusion-Detection Expert System," SRI Project 6169, SRI International, Menlo Park, CA, 1985.

[11] S. Masum, E.M. Ye, Q. Chen, K. Noh, “Chi-square statistical profiling for anomaly detection”, Proceedings of the 2000 IEEE Workshop on Information Assurance and Security, 2000.

[12] C. Ko, M. Ruschitzka. K, Levitt, “Execution monitoring of security-critical programs in distributed systems: a specification-based approach”, Proceedings of IEEE Symposium on Security and Privacy, Oakland, CA, USA. 1997.

[13] E. Lemonnier, “Protocol Anomaly Detection in Network-based IDSs”, Defcom white paper, 2001.

[14] R. Sekar, A. Gupta, J. Frullo, T.Shanbag, A. Tiwari, H. Yang, S. Zhou, “Specification-based anomaly detection: A New Approach for Detecting Network Intrusions”, ACM Computer and Communication Security Conference, Washington, DC, USA, 2002.

[15] R. Buschkes, M. Borning, D. Kesdogan, “Transaction-based Anomaly Detection”, Proceedings of the Workshop on Intrusion Detection and Network Monitoring, Santa Clara, Calfornia, USA, 1999.

[16] Arbor Network, “Peakflow: Pervasive Networki Visibility, Deep Application Insight, Security and Managed Services” [website], Available: http://www.arbornetworks.com/en/peakflow-sp.html

[17] IBM-ISS, “IBM Proventia Network Anomaly Detection System” [website], Available: http://www-935.ibm.com/services/us/iss/pdf/ proventia-network-anomaly-detection-system-ss.pdf

[18] Cisco Systems Inc, “Cisco IOS NetFlow” [website], Available: http://www.cisco.com/en/US/products/ps6601/products_ios_protocol_group_home.html

[19] Esphion, “A new approach to network disaster protection” [website], Available: http://www.esphion.com/solutions-technology.html

[20] CounterStorm, “CounterStorm-1: The Most Effective Defense Againt Known, Zero-Day and Targeted Attacks” [website], Available: http://www.counterstorm.com/solutions.html

[21] Zheng Shan, Peng Chen, Ying Xu, Ke Xu, “A Network State Based Intrusion Detection Model”, Proceedings of the 2001 International Conference on Computer Networks and Mobile Computing (ICCNMC'01), 2001.