© 2015 IJSRSET | Volume 1 | Issue 6 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

A Survey on Intrusion Detection Systems

Prof. Shivendu Dubey, Neha Tripathi
Gyan Ganga Institute of Technology & Science, Jabalpur, Madhya Pradesh, India

ABSTRACT

With the advent of anomaly based intrusion detection systems, many approaches and techniques have been developed to track novel attacks on the systems. Though anomaly based approaches are efficient, signature based detection is preferred for mainstream implementation of intrusion detection systems. As a variety of anomaly detection techniques were suggested, it is difficult to compare the strengths, weaknesses of these methods. The reason why industries don‟t favor the anomaly based intrusion detection methods can be well understood by validating the efficiencies of the all the methods. To investigate this issue, the current state of the experiment practice in the field of anomaly based intrusion detection is reviewed and survey recent studies in this. This paper contains summarization study and identification of the drawbacks of formerly surveyed works.

Keywords : Intrusion Detection, Anomaly-based Detection, Signature-based detection

I. INTRODUCTION

Network intrusion detection systems (NIDS) are most efficient way of defending against network-based attacks aimed at computer systems [13, 14]. These systems are used in almost all large-scale IT infrastructures [15]. Basically, there are two main types of intrusion detection systems: signature-based (SBS) and anomaly-based (ABS). SBS systems (e.g. Snort [16, 7]) rely on pattern recognition techniques where they maintain the database of signatures of previously known attacks and compare them with analyzed data. An alarm is raised when the signatures are matched. On the other hand ABS systems (e.g. PAYL [18]) build a statistical model describing the normal network traffic, and any abnormal behavior that deviates from the model is identified. In contrast to signature-based systems, anomaly-based systems have the advantage that they can detect zero-day attacks, since novel attacks can be detected as soon as they take place. Whereas ABS (unlike SBS) requires a training phase to develop the database of general attacks and a careful setting of threshold level of detection makes it complex. In this paper focus is on anomaly-based systems, in particular on a specific kind of this ABS payload-based. These payload-based systems are particularly suitable to detect advanced attacks, and we describe the most prominent and the most recent of them in detail: respectively Wang and Stolfo‟s PAYL [18] and our POSEIDON [19].

II. METHODS AND MATERIAL

A. Categories of Intrusion Detection Systems

1.1 Signature Based Detection

1.2

Signature detection involves searching network traffic for a series of malicious bytes or packet sequences. The main advantage of this technique is that signatures are very easy to develop and understand if we know what network behavior we are trying to identify. For instance, we might use a signature that looks for particular strings within exploit particular buffer-overflow vulnerability. The events generated by signature- based IDS can communicate the cause of the alert. As pattern matching can be done more efficiently on modern systems so the amount of power needed to perform this matching is minimal for a rule set. For example if the system that is to be protected only communicate via DNS, ICMP and SMTP, all other signatures can be ignored.

Limitations of these signature engines are that they only detect attacks whose signatures are previously stored in database; a signature must be created for every attack; and novel attacks cannot be detected.

This technique can be easily deceived because they are only based on regular expressions and string matching. These mechanisms only look for strings within packets transmitting over wire. More over signatures work well against only the fixed behavioral pattern, they fail to deal with attacks created by human or a worm with self-modifying behavioral characteristics.

Signature based detection does not work well when the user uses advanced technologies like nop generators, payload encoders and encrypted data channels. The efficiency of the signature based systems is greatly decreased, as it has to create a new signature for every variation. As the signatures keep on increasing, the system engine performance decreases. Due to this, many intrusion detection engines are deployed on systems with multi processors and multi Gigabit network cards. IDS developers develop the new signatures before the attacker does, so as to prevent the novel attacks on the system. The difference of speed of creation of the new signatures between the developers and attackers determine the efficiency of the system.

Anomaly Based Detection

The anomaly based detection is based on defining the network behavior. The network behavior is in accordance with the predefined behavior, then it is accepted or else it triggers the event in the anomaly detection. The accepted network behavior is prepared or learned by the specifications of the network administrators.

The important phase in defining the network behavior is the IDS engine capability to cut through the various protocols at all levels. The Engine must be able to process the protocols and understand its goal. Though this protocol analysis is computationally expensive, the benefits it generates like increasing the rule set helps in less false positive alarms.

The major drawback of anomaly detection is defining its rule set. The efficiency of the system depends on how well it is implemented and tested on all protocols. Rule defining process is also affected by various protocols used by various vendors. Apart from these, custom protocols also make rule defining a difficult job. For detection to occur correctly, the detailed knowledge about the accepted network behavior need to be developed by the administrators. But once the rules are defined and protocol is built then anomaly detection systems works well.

If the malicious behavior of the user falls under the accepted behavior, then it goes unnoticed. An activity such as directory traversal on a targeted vulnerable server, which complies with network protocol, easily goes unnoticed as it does not trigger any out-of-protocol, payload or bandwidth limitation flags.

The major advantage of anomaly based detection over signature-based engines is that a novel attack for which a signature does not exist can be detected if it falls out of the normal traffic patterns. This is observed when the systems detect new automated worms. If the new system is infected with a worm, it usually starts scanning for other vulnerable systems at an accelerated rate filling the network with malicious traffic, thus causing the event of a TCP connection or bandwidth abnormality rule.

B. Network Intrusion Detection System

CIDF (Common Intrusion Detection Framework) integrated with IETF and labeled as IDWG (Intrusion Detection Working Group) has achieved considerable progress in defining the frame work, the group defined a general IDS architecture based on the consideration of four types of functional modules

E-Modules (Event-Modules): Combination of Sensor elements that monitor the target system, thus acquiring information events to be analyzed by following modules.

D-Modules (Database-Modules): The information from E- Modules are stored for further processing by following modules.

A-Modules (Analysis-Modules): The Analysis of events and detecting probable aggressive behavior, so that some kind of alarm will be generated if necessary.

R-Modules (Response-Modules): The main function of this type of block is the execution, if any intrusion occurs, of a response to perplexing the detected threat

Normally, Anomaly based Network intrusion detection systems (ANIDS) have following functional stages.

Attribute Formation: Here, the observed forms of the target system are depicted in a pre-established form.

Observation stage: A model is built on based on behavioral characteristics of the system. This can be

done in many distinct ways, automatically or manually (depending on the type of ANIDS considered).

Espial stage: If the model of the system is available, it is matched with the experiential traffic.

C. Anomaly Detection Techniques

Anomaly detection is based on a host or network. Many distinct techniques are used based on type of processing related to behavioral model. They are: Statistical based, Operational or threshold metric model, Markov Process or Marker Model, Statistical Moments or mean and standard deviation model, Univariate Model, Multivariate Model, Time series Model, Cognition based, Finite State Machine Model, Description script Model, Adept System Model, Machine Learning based, Baysian Model, Genetic Algorithm model, Neural Network Model, Fuzzy Logic Model, Outlier Detection Model, Computer Immunology based, User Intention based

a. Statistical Models

Operational Model (or) Threshold Metric:

The count of events that occur over a period of time determines the alarm to be raised if fewer then „m" or more than „n" events occur. This can be visualized in Win2k lock, where a user after „n" unsuccessful login attempts here lower limit is „0" and upper limit is „n". Executable files size downloaded is restricted in some organizations about 4MB.The difficulty in this sub-model is determining „m" and „n".

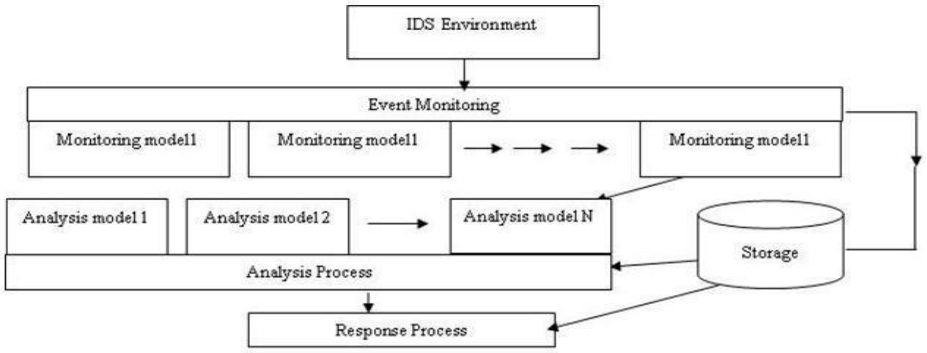

Figure1: Common Intrusion Detection Framework Architecture

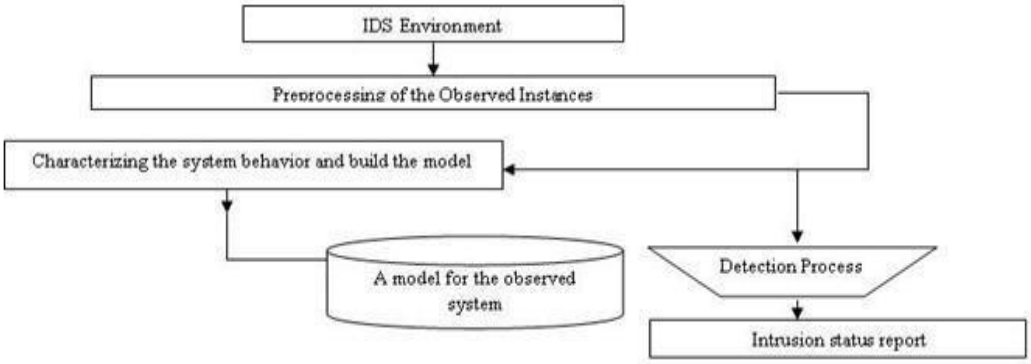

Figure 2: Common Anomaly Based Network Intrusion detection System

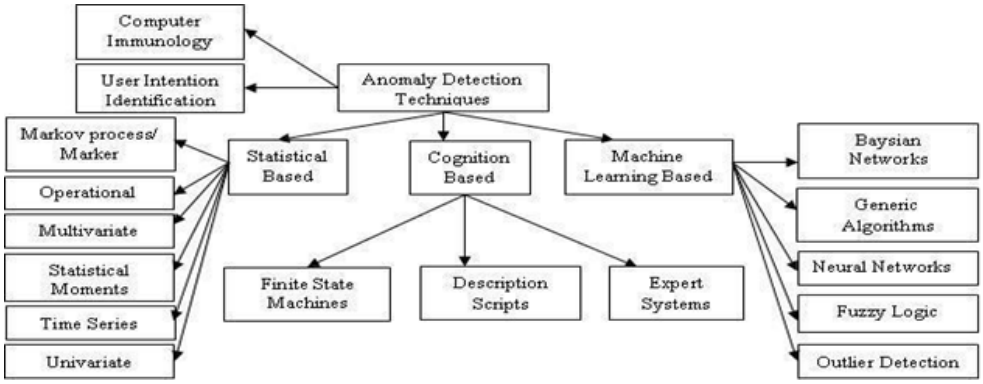

Figure 3 : Classification of Anomaly Based Intrusion Detection

Markov Process or Marker Model:

The Intrusion detection in this model is done by investigating the system at fixed intervals and keeping track of its state; a probability for each state at a given time interval Is. The change of the state of the system occurs when an event happens and the behavior is detected as anomaly if the probability of occurrence of that state is low. The transitions between certain commands determine the anomaly detection where command sequences were important.

Statistical Moments or Mean and Standard Deviation Model:

In statistical mean, standard deviation, or any other correlations are known as a moment. If the event that falls outside the set interval above or below the moment is said to be anomalous. The system is subjected to change by considering the aging data and making changes to the statistical rule data base. There are two major advantages over an operational model. First, prior knowledge is not required determining the normal activity in order to set limits; Second, determining the confidence intervals depends on observed user data, as it varies from user to user. Threshold model lacks this flexibility. The major variation on the mean and standard deviation model is to give higher weights for the recent activities.

Multivariate Model:

The major difference between the mean and standard deviation model is based on correlations among two or more metrics. If experimental data reveals better judicious power can be achieved from combinations of related measures rather than treating them individually.

Time Series Model:

Interval timers together with an event counter or resource measure are major components in this model. Order and inter- arrival times of the observations as well as their values are stored. If the probability of occurrence of a new observation is too low then it is considered as anomaly. The disadvantage of this model is that it is more computationally expensive.

- **Markov Process or Marker Model:**

The Intrusion detection in this model is done by investigating the system at fixed intervals and keeping track of its state; a probability for each state at a given time interval Is. The change of the state of the system occurs when an event happens and the behavior is detected as anomaly if the probability of occurrence of that state is low. The transitions between certain commands determine the anomaly detection where command sequences were important.

- **Statistical Moments or Mean and Standard Deviation Model:**

In statistical mean, standard deviation, or any other correlations are known as a moment. If the event that falls outside the set interval above or below the moment is said to be anomalous. The system is subjected to change by considering the aging data and making changes to the statistical rule data base. There are two major advantages over an operational model. First, prior knowledge is not required determining the normal activity in order to set limits; Second, determining the confidence intervals depends on observed user data, as it varies from user to user. Threshold model lacks this flexibility. The major variation on the mean and standard deviation model is to give higher weights for the recent activities.

- **Multivariate Model:**

The major difference between the mean and standard deviation model is based on correlations among two or more metrics. If experimental data reveals better judicious power can be achieved from combinations of related measures rather than treating them individually.

b. Cognition Models:

- **Finite State Machine:**

A finite state machine (FSM) or finite automation is a model of behavior captured in states, transitions and actions. A state contains information about the past, i.e. any changes in the input are noted and based on it transition happens. An action is a description of an activity that is to be performed at a given moment. There are several action types: entry action, exit action, and transition action

- **Description Scripts:**

Numerous proposals for scripting languages, which can describe signatures of attacks on computers and networks, are given by the Intrusion Detection community. All of these scripting languages are

capable of identifying the sequences of specific events that are indicative of attacks.

- **Adept Systems:**

Human expertise in problem solving is used in adept systems. It solves uncertainties where generally one or more human experts are consulted. These systems are efficient in certain problem domain, and also considered as a class of artificial intelligence (AI) problems. Adept Systems are trained based on extensive knowledge of patterns associated with known Perkins presented an algorithm using support vector regression. Ihler et al. present an adaptive anomaly detection algorithm that is based on a Markov modulated Poisson process model, and use Markov Chain Monte Carlo methods in a Bayesian approach to learn the model parameters [45].

c. Cognition Based Detection Techniques:

Cognition-Based (also called knowledge based or expert systems) Detection Techniques work on the audit data classification technique, influenced by set of predefined rules, classes and attributes identified from training data,set of classification rules, parameters and procedures inferred.

- **Boosted Decision Tree**

Boosted Tree (BT), that uses ADA Boost algorithm [2] to generate many Decision Trees classifiers trained by different sample sets drawn from the original training set, is implemented in many IDS successfully[20, 21, 22]. All hypotheses, produced from each of these classifiers, are combined to calculate total learning error, thereby arriving at a final composite hypothesis.

- **Support Vector Machine**

Support vector machines (SVM)) [4], reliable on a range of classification tasks, are less prone to over fitting problem, and are effective with unseen data. The basic learning process of the SVM includes two phases: 1) Mapping the training data from the original input space into a higher dimensional feature space, using kernels to transform a linearly non separable problem into a linearly separable one, 2) Finalizing a hyper plane within the feature space, with a maximum margin using Sequential Minimal Optimization (SMO) [22] or Osuna‟s method [26].

- **Artificial Neural Network**

$$\delta t = \min_a \left[\sum_{j-1}^{M} aj \,.\, \emptyset(xi) - \emptyset(xt)\right]^2 < v$$

Artificial Neural network (ANN) architectures (popular one being , Multilayer Perceptron (MLP), a layered feed forward topology in which each unit performs a biased weighted sum of their inputs and pass this activation level through a transfer function to produce their output [7]), are able to identify not readily observable patterns, however MLP is ineffective with new data. For general signal processing and pattern recognition problems, another branch of ANN that makes use of radial basis function, called The Modified Probabilistic Neural Network (related to General Regression Neural Network (GRNN) classifier [29] and generalization of Probabilistic Neural Network (PNN)), was introduced by Zaknich [28]. It assigns the clusters of input vectors rather than each individual training case to radial units.

d. Machine Learning Based Detection Techniques

Machine learning techniques to detect outliers in datasets from a variety of fields were developed by Gardener (use a One-Class Support Vector Machine (OCSVM) to detect anomalies in EEG data from epilepsy patients [8A]) and Barbara (proposed an algorithm to detect outliers in noisy datasets where no information is available regarding ground truth, based on a Transductive Confidence Machine (TCM) [3]).Unlike induction that uses all data points to induce a model, transduction, an alternative, uses small subset of them to estimate unknown attributes of test points. To perform online anomaly detection on time series data in [4], Ma and

e. Kernel Based Online Anomaly Detection (KOAD):

A set of multivariate measurements $\{x\}\ t=1^T$ is considered. The features corresponding to the normal traffic measurements must come together in a suitably selected space F with an associated kernel function k(xi, xj).The region of normality using a relatively small dictionary of nearly linearly independent elements $\{\varphi(x_j)\}_{j\ 1}^{M}$ [19A] can be defined. $\{x_j\}_{j\ 1}^{M}$ are those $\{x_t\}_{t\ 1}^{T}$ that Are entered into the dictionary (size of the dictionary (M) is much less than T) , thereby computational and storage overhead is reduced. If the projection error δt satisfies the following criterion:

Where a = $\{a_j\}_{j=1}$ is the optimal coefficient vector, feature vector $\varphi(x_t)$ is nearly linearly dependent on $\{\varphi(x_j)\}_{j=1}^{m}$ with approximation threshold ν.

The Kernel based Online Anomaly Detection (KOAD) algorithm, working at each time step t on a measurement vector x_t, begins by evaluating the error δ_t in forecasting the coming x_t onto the current dictionary (in the feature domain) and then weighs the two thresholds v1 and v2 where $v1<v2$. x_t is inferred to be sufficiently linearly dependent on the dictionary and represents normal traffic if $\delta_t < \nu_1$ while x_t is far away from the realm of normal behavior, and immediately raise a "Red1" alarm to signal an anomaly, if $\delta_t > \nu_2$. Old and unused elements are deleted from the dictionary by the KOAD algorithm basing on whether the region of normality expands or migrates. Also it incorporates exponential forgetting so that the impact of past observations is gradually reduced.

f. Detection Models Based on Computer Immunology

Inspired by the ideas taken from the concept of immunology, the computational technique, Artificial Immune System (AIS) is developed in developing adaptive systems that are capable of solving problems from various domains. This has now become a tool for research which studied well and applied in solving problems in the computer security field and particularly to detect the viruses [7] in computers and also network intruders [3]. It is also applied to give a solution to the scheduling problem [4], to build support systems in taking decisions or to solve function optimization and combinatorial optimization problems [2].

Applying immunology to the basic computational model is the subject of research; the widely applied basic notions are antigen and antibody. The invaders which are foreign to the system and attack it in some way are antigens. A part of system, and which help in detecting and eliminating the antigens are called antibodies. The detection of antigens is done by matching them. The number of antigens is much higher than the number of antibodies in the system, so a perfect matching can never occur. To keep a less number of antibodies, that reliably detect large number of antigens that were never seen before, AIS-based system is used

g. Models Based on User Intention

Building the profile of normal behavior and attempting to identify certain pattern or activity deviations from normal profile. Anomaly detection is used to find unknown attacks by using the concept of profiling normal behaviors. But, significant false alarm may be caused because it is difficult to obtain complete normal behaviors.

Intrusion detection can be built upon multiple levels in a real computer network system. It will be a choosing the features that characterize the user or the system usage patterns in the best way, such that distinguishing abnormal activities from normal activities is done clearly. Data sources like Unix shell commands, audit events, keystroke, system calls and network packages can be used. The first crucial step in building a profiling method for intrusion detection is selecting a data source. During the early study on anomaly detection, the main focus was on profiling system or user behaviors from monitored system log or accounting log data.

h. Current State of Art

A new method that could achieve more accuracy than the existing six classification patterns (Gaussian Mixture, Radial Basis Function, Binary Tree Classifier, SOM, ART and LAMASTAR),called Hierarchical Gaussian Mixture Model[HMM] for IDM was put forward by M.Bahrololum et al[1].

Jiankun Hu and Xinghuo Yu et al [2] studied development of host-based anomaly intrusion detection, focusing on system call based HMM training. This was later enhanced with the inclusion of data pre-processing for recognizing and eliminating redundant sub-sequences of system calls, resulting in less number of HMM sub models. Experimental results on three public databases indicated that training cost can be reduced by 50% without affecting the intrusion detection performance. False alarm rate is higher yet reasonable compared to the batch training method with a 58% data reduction.

R. Nakkeeran et al [3] proposed an anomaly detection system comprising of detection modules for detecting anomalies in each layer. The anomaly detection result of the neighbor node(s) is taken by the current node and its result in turn is sent to the neighbor node(s).

Experimental results revealed increased detection rate and reduced false alarm positives, compared to other methods.

Jiong Zhang et al [4] proposed a new framework of unsupervised anomaly NIDS based on the outlier detection technique in random forests algorithm. The framework builds the patterns of network services over datasets labeled by the services. With the built patterns, the framework detects attacks in the datasets using the modified outlier detection algorithm, reducing the calculation complexity. This approach is independent of attack-free training datasets, but assumes that each network service has its own pattern for normal activities.

Ahmed Awad E. Ahmed et al [5] proposed a biometrics-based intrusion detector model to provide a lightweight and self-contained module for detecting user identities misuse. System-calls and network traffic monitoring systems have to be combined to this detector to achieve the best solutions.

Vijay Bhuse et al [6] proposed a technique to detect anomalies at all layers of a network stack in a sensor network, segregating the service at various levels. Physical layer intrusion is detected by using RSSI values of neighbors (dependant on background noise, weather conditions etc). Targeting MAC layer will work for schedule based and sleep/wake-up based MAC protocols while IASN protocol is aimed at the routing layer. Experiments show that IASN can be used for source initiated routing protocols, table driven routing protocols and data dissemination mechanisms like directed diffusion. The probability of detection increases linearly with the number of nodes running IASN. Nodes guard each other from masquerade at application layer. Depending on the resource availability, any combination of the above methods can be employed, as they are independent of one another. All techniques are energy efficient as they have very low false positive rates(except RSSI and round trip time) and low overhead.

Using information theory measures, a model was put forward by Hossein M. Shirazi et al [7] that ranked 41 connection features performing normalization on each attack class. The main features of this are, ranking (relevant features for each attack class are selected and computing complexity is decreased) and features selection (detection rate preserved, yet detection time decreased). Noisy and irrelevant features can be eliminated by running some detection models like SF-5NN and SUS-5NN using only selected features. A combination of two detection engines(SF-KNN,SUS-KNN) based on best selected features and KNN algorithm was proposed, that was much better(notably in detecting attacks like U2R, R2L) than approaches like traditional 5-NN, C4.5,C5. Experimentally, engines gave classification rates of 92.56%, 92.84% and false positive rates 2% and 4.52% respectively.

Dayu Yang et al [8] introduced a method to apply Auto Associative Kernel Regression (AAKR) empirical modeling and the SPRT for SCADA system intrusion detection. In detecting anomalous behavior, this model is limited by two requirements - different indicators for different intrusion methods and managing a number of highly valuable variables. Identifying the optimal set of indicators for known and potential abnormalities is the future of this research.

Combining multiple independent data sources and studying combined traditional intrusion attack and anomaly intrusion, the anomaly intrusion traffic detection work carried out by M.Thangavel et al[9], provided the statistical wavelet based detection mechanism.The properties such as attack duration, packet count, packet rate, and dominant protocol type match with the two data sets, as is indicated by attack structure. At lean and heavy traffic scenarios, the demand capacity of the server was observed to give better clarity of anomaly intrusion detection although server uptime. Analysis of several traffic anomaly properties which is impossible using traditional intrusion measurements can be performed by a new model that used anomaly intrusion attack measurements. Small businesses seem to be the most common targets of attacks. Traditional measures in understanding and detecting of anomaly intrusion is no more reliable given the current trends of attacking using spoofed address sources.

Miao Wang, et al [10], proposed a method suitable for Windows Host Anomaly Detection System, which is used as a supplement for other security mechanisms under windows. It can only detect intrusions which invoke an anomaly sequence by programs. One of the

general situations such as an unauthenticated use of normal programs cannot be detected.

Constantine Manikopoulos et al [11], proposed a statistical. anomaly detection technology called HIDE with hierarchical multitier multi-observation window system to monitor network traffic parameters simultaneously, using a real-time probability distribution function(PDF) for each parameter, collected during the observation window. The similarity measurements of measured PDF and reference PDF are combined into an anomaly status vector classified

by a neural network. This methodology detects attacks and soft faults with traffic anomaly intensity as low as 3 to 5 percent of typical background traffic intensity, thereby generating an early warning.

Jeyanthi Hall et al[12], proposed an anomaly based intrusion detection system for mobile networks, based on simulation results of mobility profiles for enhancing ABID in mobile wireless networks. If the mobility behavior of users has not been accurately found, the selection of specific values for key parameters, such as sequence length and cluster size is absurd. One possible strategy for enhancing the characterization of users and dealing with concept drift (keeping UMP up to date), is to maintain a window of the newly observed sequences (analogous to the exponential weighted moving average) that can then be used to update the training patterns periodically and hence reduce the false positives.

An intrusion detection algorithm and its architecture (two- layered, global central layer and a local layer, together performing data collection, analysis and response), based on test the limits in accuracy and robustness in existing systems and showed that some data mining and useful in real time for network security, is proposed be HAZEM M. EL-BAKRY et al [3].By filtering

out the known traffic behavior (intrusive and normal) this IDS focuses on analysis on unknown data thereby reducing false alarm rates.

Tich Phuoc Tran et al [6] proposed an approach called "A Multi-Expert Classification Framework with Transferable Voting for Intrusion Detection". This model, aimed to improve the strategies to detect different anomalies and intrusions emphasized on different attribute selection strategies, defined a new multi expert classification system to learning algorithms that use certain set of features can provide superior detection capability for a given attack category. A set of five local classifiers, created to detect five different classes including Normal, Probe, DoS, U2R and R2L and outputs from these experts are then integrated by different voting methods. Finally concluded that

a) the weighted voting strategies outperform simple majority voting, b) with Transferable voting approach, the model achieved noticeable performance improvement compared with other conventional techniques, in terms of detection accuracy and system robustness, misclassification cost and processing overheads for “unknown” instances. This may not be an ultimate choice for security, but is effective on different situations.

Min Yang et al [9] discussed a model based on contiguous expert voting algorithm. Although early methods detect most anomalies, unsuccessful match doesn‟t mean an abnormity, as normal rules may not cover all normal data. Detection rate in this is not commendable but it has vast future scope for improvement.

The One Class Neighbor Machine (OCNM) algorithm proposed by Munoz and Moguerza, assumes a sample set S T comprising T, F-dimensional data points, {xt} t=1 and estimates minimum volume sets [4]. The algorithm requires the choice of a sparsity measure(like choices of a sparsity measure are the k nearest neighbor Euclidean distance and the average of the first k nearest-neighbor distances) denoted by g, whose values are sorted by a set of points S. The points that lie inner to the minimum volume set (MVS) with minimum sparsity measure g, till a specified number of points μ are obtained. The distance from every point xt to every other point in the sample set has to be found out along with OCNM algorithm ,when the sparsity measure used is kth neighbor distance function. The complexity her is of the order 2 O(T F) as every point is F-dimensional.

III. RESULTS AND DISCUSSION

Table1: Summary of the anomaly detection techniques

Layer	Protocols / Techniques for Anomaly Detection	Use	Overhead	Drawbacks
Physical	RSSI value	Detects masquerade	Calibration of RSSI value for each neighbour	Large number of positives
MAC	TDMA: Check if adversary follows TDMA Schedule	Detects masquerade	Keep track of TDMA Schedule of other nodes	None
	S-MAC: Check if sender is supposed to be sleeping	Detects masquerade	Keep track of sleep-wake of schedule of other nodes	None
Routing	For any routing protocol, check if neighbour and the expected information matches	Guarantees information authentication	Constructiong ADTs. Updating previous hop in a packet	None
Application	Use triangulation to detect Intrusions	Detects masquerade	Nodes always have to listen	Overhearing
	Round trip time	Detects masquerade	Precise calibration of range of round trip time for each neighbour	Large number of positives

In recent literature, anomaly detection through a Bayesian Support Vector Machine by Vasilis A. Sotiris et al[2] is found as interesting machine learning model for anomaly detection. Use of a SVM with one-class to detect the system anomalies at their early stage is studied along with drift output classification probabilities. Experimentally, absence of failure

training data under one-class SVM leads to quick detection of unknown anomalies. Initially dividing the training data into multiple unrelated lower dimensional models, the test data will be evaluated on each model separately thereby revealing outliers in different capacities (as is used to evaluate the posterior class probabilities in Bayesian framework).

A Machine Learning (ML) based anomaly detection scheme is proposed by Zhenghong Xiao et al [3], where Bayesian classification algorithm is used to detect anomalous nodes with respect to the characteristics of Wireless Sensor Networks (WSN). While the traditional models failure is attributed to the use of specific characteristics of WSN, this scheme achieves relatively highly accurate detection rate and lower false positive rate The WSN characteristics, such as limited power, limited communication capacity, and limited computational capabilities of nodes are retained in the current model. Establishment of detection rules is also possible after the completion of few samples learning.By making use of the simulation model the authors of the paper tried to provide a proof that the model proposed will be able to retrieve vital association rules and can be able to differentiate normal connection, called intrusion and the intrusion which is unknown with high degree of accuracy.

Li-li Liu et al[5] proposed a method which is used for detecting anomalies which used the construction of a Wavelet Neural Network(WNN) that makes use of changed quantum- behaved particle swarm optimization(MQPSO) algorithm. In this model, MQPSO will be used to train WNN. The learning algorithm multidimensional vector that has WNN parameters as components will be considered as particle. The vector of parameters will search the value globally. Experiments were performed by the authors on well-known KDD Cup 1999 Intrusion Detection Data Set.

A result was published by the author that explains that the learning algorithm has more rapid convergence, improved global convergence ability when compared with the traditional quantum-behaved particle swarm optimization (QPSO), thus enhancing the accuracy of anomaly detection.

Jian Xu et al[6], inspired by immunology, proposed an approach for detecting system performance anomalies that combines the negative selection algorithm(NSA) and the genetic algorithm. This generated B set of fuzzy rules that will characterize the normal and the abnormal.

To remove the invalid detections and to reduce the space required for search, NSA serves as filter. The problem of anomaly detection was derived as two-class classification problem by the authors, the goal being classifying the patterns of the system to two categories as self and non-self, that uses a set of samples which include self and non-self. The idea was to make use of the fuzzy rules in the place of crisp rules. Various concepts of fuzzy logic are used to find a solution to this problem of classification. Taking a set of samples, that include self and non-self, fuzzy detector rules must be generated in the non- self-space that will help find a new sample belongs to which category: self or non-self. Making use of the fuzzy rules, the accuracy of detection is improved and these rules, like any other approach do not use hyper-rectangles for representation.

Following are the advantages:

Many times, the negative selection algorithm acts as a filter. It is added to the Genetic Algorithm (GA) particularly as a filter operator that efficiently eliminates the bad solutions to get low False Positives (FP).

A new partial match of chromosome, used to calculate the distance of two different individuals is adopted by the algorithm. A better characterization of the boundaries for the two categories self and non-self is provided by fuzzy rules and they help in reducing the search space.

An adaptive approach to modeling user's behavior in computer anomaly detection systems was proposed by Artem M.Sokolov et al[3].Markov chains with variable memory length were used as a base model. Considering the changes in user‟s behaviour an adaptive version of the algorithm constructing a model was introduced. An application of adaptive version of Markov model with variable memory length to the anomaly detection task was discussed by the authors.

Based on the demonstrations from the experimental results it was claimed that the modified model can be applied in modeling various sequences. It was possible for the approach to capture more subtle peculiarities of users' behavior and to continuously refine their models only with use of adaptive adjustment procedure. Since the anomaly criteria cannot be precisely formalized, it is a better option to use a set of techniques from which the conclusion will be drawn on the presence of intrusion. Threshold classification and cross test technique are the two possible techniques of anomaly detection, proposed in this work along with their experimental testing.

Based on the mobility patterns of mobile users, who make use of public transportation Jeyanthi Hall et al [4] examined the feasibility of using profiles. A novel framework, which makes use of an instance based learning technique, for classification purposes was presented by them

It was concluded by the authors that it is feasible to use mobility profiles for Anomaly Based Intrusion Detection in mobile wireless networks, based on the simulation results. It is a challenge to accurately characterize the mobility behavior of users. To incorporate the missing parameter sequences into the training patterns, which enhances the characterization of users and increases the detection rate at a minimal cost (low percentage of FAs) is one of the simple strategies. Concept drift, that accommodates variability in mobility sequences over time can also be addressed by continuously monitoring the false alarm rate and incorporating the observed mobility sequences into the training patterns selectively, using a window trhat will be shifted in time. The basis for the selection can be pre-established thresholds, like the frequency of all new sequences encountered over a time period.

An approach for generating the data was proposed by Ramkumar Chinchani et al [9] that is based on customizable templates, where a user profile is represented by each template. The templates can be user-defined or can be created from known data sets. The tools that have been developed is RACOON, that generated generates large amounts of user command data rapidly from a given template. Several statistical similarity tests were performed to test their reliability and to explain that this technique will produce realistic data.

To generate the user command data, two paths are there, in the first path, a template specified by the user will be created and provided as the input to the module that generates data. To assist the user, the authors have implemented a front end because the manual specification can be a onerous process. An available

data set can be processed for creating the template and the second process, and later it follows the first path. Parameters like data size which are controlled by the user allow the data generation that is of the required size and quality.

A new Non-negative Matrix Factorization (NMF) based model to profile program and user behaviors for anomaly intrusion detection was proposed by Wei Wang, et al [5]. The information source in this method is the audit data stream obtained from sequences of system calls and commands. The audit data is divided into segments of fixed length. The frequencies of individual system calls or commands embedded in each segment of the data are the measures for program and user behaviors and are to extract the features from the blocks of audit data associated with the normal behaviors, NMF is used. Based on these features the model describing the normal program and user behaviors is built, deviation from the normal program and user behaviors above a predetermined threshold is considered as anomalous. Unlike many other methods which use transition property, this method considers the frequency property of system calls and commands. It is proven by the simulation results published by the authors that there is no need to consider individual system calls or commands, thus it can be concluded that the computational cost of NMF method is economical and suits real-time intrusion detection.

IV. CONCLUSION

This paper explains the primary's establishment's abnormality based system interruption discovery advancements alongside their operational architectures furthermore exhibits a grouping in view of the kind of preparing that is identified with the "behavioral" model for the objective framework. This concentrate likewise portrays the principle components of a few ID‟s frameworks/stages that are presently accessible in a brief way. The most noteworthy open issues with respect to Anomaly based Network Intrusion Detection frameworks are recognized, among which evaluation is given specific accentuation. The introduced data constitutes a vital point to begin for tending to Research and Development in the field of IDS. Countermeasures which are speedier and more successful are expected to adapt up to the assaults always developing. We find that the greater part of reviewed works don't meet these necessities. Overall, the discoveries affirm a typical pattern in the trial software engineering.

V. REFERENCES

[1] M. Bahrololum and M. Khaleghi, "Anomaly Intrusion Detection System Using Hierarchical Gaussian Mixture Model" IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.8, August 2008

[2] Jiankun Hu and Xinghuo Yu, "A Simple and Efficient Hidden Markov Model Scheme for Host-Based Anomaly Intrusion Detection" IEEE Network Journal, Volume 23 Issue 1, January/February 2009

[3] R. Nakkeeran, T. Aruldoss Albert and R.Ezumalai, "Agent Based Efficient Anomaly Intrusion Detection System in Ad-hoc networks" IACSIT International Journal of Engineering and Technology Vol. 2, No.1, February, 2010

[4] Jiong Zhang and Mohammad Zulkernine, "Anomaly Based Network Intrusion Detection with Unsupervised Outlier Detection" IEEE International Conference on Communications, 2006.

[5] Ahmed Awad E. Ahmed, and Issa Traore, "Anomaly Intrusion Detection based on Biometrics", IEEE Workshop on Information Assurance 2005

[6] Vijay Bhuse, Ajay Gupta, "Anomaly Intrusion Detection in Wireless Sensor Networks" ACM Journal of High Speed Networks, 2006

[7] Hossein M. Shirazi,"Anomaly Intrusion Detection System Using Information Theory, K-NN and KMC Algorithms", Australian Journal of Basic and Applied Sciences, 3(3): 2581-2597, 2009

[8] Dayu Yang, Alexander Usynin, and J. Wesley Hines, "Anomaly-Based Intrusion Detection for SCADA Systems" IAEA Technical Meeting on Cyber Security of NPP I&C and Information systems, Idaho Fall, ID, Oct. 2006

[9] M.Thangavel, Dr. P.Thangaraj and K.Saravanan, "Defend against Anomaly Intrusion Detection using SWT Mechanism" IACSIT, 2010

[10] Miao Wang, Cheng Zhang and Jingjing, "Native API Based Windows Anomaly Intrusion Detection Method Using SVM" IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, 2006

[11] Manikopoulos.C and Papavassiliou.S, "Network Intrusion and Fault Detection: A Statistical Anomaly Approach" IEEE Communications, 2002.
[12] Jeyanthi Hall, Michel Barbeau, Evangelos Kranakis, "Using Mobility Profiles for Anomaly-based Intrusion Detection in Mobile Networks" IEEE Conference, 2005.
[13] Hazem M. El-Bakry, Nikos MastorakisA, "Real-Time Intrusion Detection Algorithm for Network Security,WSEAS Transactions on communications, Issue 12, Volume 7, December 2008.
[14] Debar.H, Dacier.M and Wespi.A, "A Revised Taxonomy of Intrusion-Detection Systems" Annales des Telecommunications 55(7–8) (2000) 361–378
[15] Allen.J, Christie.A, Fithen.W, McHugh.J, Pickel.J, Stoner.E, "State of the practice of intrusion detection technologies" Technical Report CMU/SEI-99TR- 028, Carnegie-Mellon University - Software Engineering Institute (2000).
[16] Roesch.M, "Snort - Lightweight Intrusion Detection for Networks" 13th USENIX Conference on System Administration, USENIX Association (1999) 229–238
[17] Sourcefire: Snort Network Intrusion Detection System web site (1999) URL http://www.snort.org.
[18] Wang. K and Stolfo.S.J, "Anomalous Payload-Based Network Intrusion Detection" 7th Symposium on Recent Advances in Intrusion Detection, Volume 3224 of LNCS., Springer-Verlag (2004) 203–222
[19] Bolzoni.D, Zambon.E., Etalle.S, Hartel.P, "POSEIDON: a 2-tier Anomaly based Network Intrusion Detection System"IEEE International Workshop on Information Assurance, IEEE Computer Society Press (2006) 144– 156.
[20] B.Pfahringer, "Winning the KDD99 Classification Cup: Bagged Boosting," in SIGKDD Explorations, 2000.
[21] I. Levin, "KDD-99 Classifier Learning Contest: LLSoft‟s Results Overview" SIGKDD Explorations, 2000.
[22] V. Miheev, Vopilov.A and Shabalin.I., "The MP13 Approach to the KDD‟99 Classifier Learning Contest" SIGKDD Explorations, 2000.