4: ANOMALY DETECTION APPROACHES FOR INTRUSION DETECTION IN WI-FI
CHAPTER 4: ANOMALY DETECTION APPROACHES FOR INTRUSION DETECTION IN WI-FI

4.1 OVERVIEW

In any concept of understanding, identifying an anomaly is a challenge, not because of its inherent nature, but the intent it carries. Technology in general, and software technology in particular has remained the biggest victim of anomaly intrusion. No matter how secured and advanced the technology may offer to wireless software networks, completely isolating it from anomaly intrusion is not realistically possible. Such aberrations are bound to happen, although time and again preventing measures have been conceptualized, developed and re-designed to neutralize, defuse and overcome such anomalies. Thinkers, policy makers, engineers and scientists have always come-up with newer solutions to make the Wi-Fi more reliable and secure.

Anomalies with regard to intrusion detection in Wi-Fi have remained a major concern today. Perhaps no other approach in any technology has suffered as badly as WLANs because of anomaly. The subject under discussion rejuvenates understanding all the views and approaches of this, which are principally in practice. Through this study, a broader perspective to identify the intrusion detection mechanisms that prevents such malaise that disrupts the whole system in a multifaceted wireless network are examined. Particularly the present chapter will focus on studying all the approaches of anomaly detection in force, and try to redefine the mechanisms from
architectural point of view to operating system in the wireless network environment. Considering the inherit nature as being difficult to detect and respond to misuse detection systems, the anomaly detection system has been given such importance. An attempt has been made to examine the most frequently exploited vulnerabilities identified, and how far these wireless IDS solutions have been able to defend such networks are presented.

There are existing studies on anomaly detection approaches, having extensive research in the same domain, accordingly techniques developed either in generic form or a particular kind to detect such anomalies. This chapter will try to offer a constructive overview on the subject under discussion. A technical report of 2009 while re-defining anomaly detection, and the challenges, says: “problem of finding patterns in data that do not conform to expected behavior,” and goes on to say that those “non-conforming patterns are …… outliers, discordant observations, exceptions, aberrations, surprises, peculiarities or contaminants in different application domains.” [23] Because of the characteristics of Wi-Fi networks and its growing popularity in use, introduction of intrusion detection systems both in wired and wireless networks are in place. The science has so developed now that these intrusion detection systems can fight attacks, and neutralize their intentions without referring to the previous and thorough characterization. There are in-built mechanisms like anomaly based triggering which can alarm if there are any anomalies. The other one is ‘user group profile’, which is also a popular concept in IDS; all these will be subsequently discussed. [33]
4.2 **Anomaly Detection System**

This application primarily identifies anomalies from unseen data, or from any deviations of the normal patterns. One of the best advantages of anomaly detection is that it doesn’t have to refer whole history of intrusions that has taken place to detect new intrusions. Figure-4.1 below illustrates explaining the key components of Anomaly Detection Systems, followed by different kinds and aspects of this system, which will help us understand how anomaly detection systems have been working:

4.2.1 **Key Components of Anomaly Detection System**

![Diagram showing key components of Anomaly Detection System]

*Figure 4.1: Key Components of Anomaly Detection System [33]*
From the above illustration of the figure, all the components of the system can be inferred. These apparatuses are linked to all anomaly systems. There is lots of research work ongoing on this topic.

### 4.2.2 Aspects of Anomaly Detection System

It is a primary requirement to have the inputs to understand the nature of attacks, therefore data input and its labels are induced to the application to help us examine the approach, and accordingly solutions are developed considering the constraints and other limitations. [23]

#### 4.2.2.1 Nature of Input Data

From the collection of data input, data instances are segregated according to their attributes and features, like variables, characteristics and dimensions; which may be binary, categorical or continuous. Based on their relationships present among data instances, data input has been categorized into sequence data, spatial data and graph data, which will be discussed at the later stage of this chapter.

#### 4.2.2.2 Type of Anomaly

Let’s understand how and why these anomalies have been classified into different categories; Point Anomalies, Contextual Anomalies and Collective Anomalies:
(i) **Point Anomalies:** When a particular data instance is found anomalous with rest of the data, then the instance is taken into analysis, termed as a Point Anomaly. This application helps like that of detecting credit card frauds.

(ii) **Contextual Anomalies:** It is when a particular data instance is used for a specific purpose with regard to context. There are two classes of attributes:

- **Contextual Attributes:** Depending upon the location, either in spatial data sets, or in time series data, “time” is a taken as contextual attribute helping to identify the instance and the sequence. Using this method, detection of anomalies in Wi-Fi are carried out.

- **Behavioral Attributes:** These kind of attributes define non-contextual characteristics of an instance. It must be noted that a particular instance which is “contextual anomaly” may be normal in behavioral attributes in different context. Therefore, it is not easy to identify and define instances according to their attributes, and use the same effective anomaly detection.
Collective Anomalies: When a group of data instances prove to be anomalous in the whole data, it is called, collective anomaly, individually they are anomalous.

This may be noted that in any data set ‘point anomalies’ can appear but ‘collective anomalies’ can only appear when data instances are related to one-another. Interestingly, both the anomalies can be considered as ‘contextual anomalies’ when analyzing the entire set of data is required.

4.2.2.3 Data Labels

It must be noted that the labels when associated with data instances can conform to normaley, but the irony is, obtaining such labeled data is quite expensive, that conform to accuracy and representing all behavioral attributes. Because this kind of labeling is done by experts who are specially trained, moreover, manually. Considering that the anomalous behavior is often dynamic in nature, it is difficult to develop a technique according to the behavior of labels. Therefore, it is recommended to follow below three operating technique modes to detect anomalies:

(i) Supervised Anomaly Detection: In this technique, sum of both normal and anomaly data is taken together to build a
model, which is predictive in nature. By setting both the classes, a comparison is made with unseen data instances according to classes it may into. Here the issues are: first, having fewer anomalous instances in comparison with normal instances in the data, second, getting appropriate labels for anomaly class is too expensive, moreover, not easy.

(ii) **Semi-Supervised Anomaly Detection:** Under this scheme, the technique assumes that the labelled instances have been allotted for normal classes only, therefore, anomaly classes are considered. For example, spacecraft having fault detection mechanism to avoid possible accidents. It is programmed in such a way to give signal to the pilots. But developing such a program and model is a herculean task.

(iii) **Unsupervised Anomaly Detection:** Interestingly, to prepare a model under this scheme, there is no need for training data. Because it assumes that the normal instances are frequent rather than anomalies in the data.
4.2.2.4 Output of Anomaly Detection System

This kind of technique identifies and reports the anomaly through patterns of outputs in labels. This is of two types: **Scores and Labels**, the former adopts a technique to score anomalies, and the latter it looks for all instances in the data individually.

4.2.3 Benefits of Anomaly Detection System

Trigger mechanism helps detecting anomalies easily. ‘User group’ profiles are similar to that of ‘signature database’ approach. Application of signature-based detection is such that the moment an intruder enters into the system, the IDS system will generate an alert. But profile-based approach has the bigger advantage, because it doesn’t set pre-configured signatures or known attacks. Since the signature-based files are purchased with an IDS system, that a hacker can have an easy access, thus enabling to perform on his own IDS system to generate an alert. Reason, anomaly detection approach doesn’t use a pre-configured signature database, thus an internal attack can be detected using a compromised user account.

4.2.4 Challenges for Anomaly Detection System

As stated earlier, only then can it be called an anomaly when the pattern of instances in data does not conform to expected normal behavior. And, also there can be a possibility, that some portion of data can be normal or
abnormal in the data itself. Therefore, developing a detection mechanism according to anomalies is not easy as it sounds. This is elaborated as under:

(i) At a time the thin-line which determines an instance to be normal or abnormal is often proves critical, as both the instances are very similar in nature.

(ii) When anomalies occur due to malicious attacks, the adversaries adapt themselves to appear as normal, thus makes it even difficult to define what is normal.

(iii) It must be noted that normal behavior in each domain keeps evolving, therefore how to assume which one to be normal.

(iv) Moreover, behavior of an anomaly changes from one application to other, then applying a generic technique may not help.

(v) Availability of appropriate and correct labeled data for training.

(vi) Data containing noise appears to be anomalous.

Considering the above mentioned challenges, specific techniques are adapted depending upon the availability of data and labels, and other parameters as discussed, and accordingly anomaly detection approaches are developed.
4.2.5 Limitation of Anomaly Detection System

The limitation of this approach is that often it fails to describe the exact nature of attacks, thus offers high false positive rate, and it assumes all intrusive activities are anomalous. [16] This limitation leads to other possibilities, such as: (i) those activities which are anomalous but not intrusive are considered intrusive, and (ii) this may result into false negatives.

It must be noted that the selection of threshold levels are very critical, because their problems are either unreasonable or their features are unreasonable. The other noted problem is that this approach is very expensive to adopt, as the system requires constant up-gradation profiles. Figure 4.2 below illustrates Block Diagram, which is a typical case of anomaly detection system:

Another limitation to this application is that it heavily relies on abnormal behaviors to define normal standards, thus giving an opportunity to develop faint signs of DDoS attacks.
4.3 Anomaly Detection in Wireless Network

Having established the usage patterns in a given time gives an opportunity to the administrator to single out the anomaly. In order to recognize this anomaly behavior, it must recognize the user behavior which can be done by forming a profile, defining normal behavior in it.

The study is based on the following profile for anomaly intrusion detection.

- Under normal circumstances, from a particular AP, SNMP traffic comes between the specific time stamps XXXX, but if the time is extended from the specified time, it would significantly increase or decrease the traffic, which will establish a deviation from behavior in normal circumstances, therefore, an intrusion.

- The user connects to the network via a particular AP and Station, which is considered as normal activity of the user during working hours. But if he accesses network from another station or point then it establishes ulterior motifs.

- During working hours specific level network activities are common, therefore, traffic on the network usually remains heavy, but after working hours if the network traffic is found to be still heavy, then certainly it is an intrusion.

As novel attacks are experienced in the wireless network systems are the development of anomaly detection approach. Of all concerns, security of the network medium has remained the prime issue. This
makes even more challenging to keep a track record on every possible attacks on the network, meant either for denying service, or compromise nodes or perform any kind of malicious activity.

4.3.1 Worm Propagations

Worm propagation is a kind of attack that exploits security weaknesses, be it in an operating systems or applications. Although signature-based detection systems are taking care of it by simply scanning the identified worms, unless those are suppressed at a very early stage, it can spread to other systems. It must be noted that the packet content analysis is a time-consuming process.

Wormhole Attacks

Although the wireless network system is mobility-friendly, but has no ability to recognize participating nodes, resulting into vulnerabilities to happen. One of such vulnerabilities are ‘wormhole,’ [8] defined as an attacker, aiming to attract as much traffic as possible to a node. It pretends to other nodes as their neighbor. [11][33][23]

4.3.2 Distributed Denial of Service (DDoS) Attacks

The attacker, in this approach aims to overload resources by flooding the system with more traffic. As a result, it either denies service or prevents accessing from the network resources. [3][33]
4.3.3 Botnet

It is a collection of compromised hosts whose aim is to launch cyber-attacks by a single command, a command that is well organized through coordination, meant to cause a disaster. [23] To prevent such kind of attacks, botnet detectors use exploit pattern techniques, i.e., ‘code downloading’, ‘bot coordination communications’, and ‘patterns of outbound attacks’ to save their software network systems. [10][33]

4.4 Attack Detection Approach for Anomaly Based IDS

When wireless attack happens, it is most certain that the malicious compromised node will attract other nodes causing traffic collisions by sending a large number of packets. If anyone sets a wormhole, there will be sudden rise in the traffic. Similarly, a DDoS attack can raise the number of packet collisions when it observes botnet propagation by signaling an increase the volume of traffic in the node. Therefore, the study suggests that detecting such attacks in wireless networks are possible even by monitoring the activity of these anomalies. [33]

From the above study it reveals that anomaly detection mechanisms can be possible without any modification on range of a network. Undoubtedly, whenever an application is to be moved, it will demand some minor adjustments or thresholds, because, every network has its own peculiarities. Considering that WLANs cover a huge area, maximum APs should be deployed to enable wide signal coverage. Where a wireless AP is located, it will require a wireless
ADS solution for sensor. Therefore, most of the attacks can be identified if there is a comprehensive physical infrastructure in place along with sensors fitted with all AP locations. [33]

One of the critical components is the security architecture, as it heavily depends on Nodal and Root Agents within the architecture. The Nodal Agents are specifically designed to monitor individual network nodes corresponding to Nodal Agents in the network. At the outset, Nodal Agent works as an observer of packet distribution system to detect any untoward incident thereby alerting the Root Agent from a possible network attack. It is done through a centralized approach where APs work as the Root Agents. It may be referred to a case in 2008, when D. Brauckhoff et.al, had introduced an anomaly model named FLAME, in which a different mechanism of anomaly detection was proposed, called “flow-based-anomaly detection”. Precisely, three were three categories: i.e. Additive Anomaly, Subtractive Anomaly and Interactive Anomaly. [12][23][24][33]

First it was observed that the hierarchical detection mechanism offered a low level of analysis effort, because it could only observe packet distribution. Subsequently it was upgraded by addressing the shortcomings observed in the first stage. Then, it could only detect anomalies based on the information. Splitting anomaly detection established that in a hierarchical system, it affected less to a machine than the systems. It gave a new dimension to this approach by mixing the basic detection systems with latest mechanisms of the same. It could accommodate the desired range, had the flexibility, understood different network scenarios, offered a better architecture,
and most importantly, allowed broad security arrangements to all the network users.

The conventional architecture of anomaly detection is illustrated below in Figure 4.3, giving a clear understanding of how the approach works:

(i) **Additive Anomaly**: In the existing network ‘botnet activities’ can add network packets which will not interact with the existing traffic.

(ii) **Subtractive Anomaly**: Baseline is created for the local network data, and anomalies are observed from there to rule out any network attacks.

(iii) **Interactive Anomaly**: FLAME model is one the examples of ‘interactive anomaly.’ In this, Denial-of-service (DoS) attacks are added to have an impact on the baseline traffic.
4.5 Anomaly Detection Techniques

Classifications of this technique are: Statistical Analysis, Data Mining, and Rate Limiting Techniques as shown in Figure 4 below:

![Figure 4: Anomaly Detection Techniques](image)

A monitoring system called NOMAD was designed by Talpade et al. [11], which could detect network anomalies based on Statistical Analysis of the information it receives in packet header. It detects anomalies of local network traffic for high-bandwidth traffic aggregate without any support from distributed sources of the classifier. Cabrera et al. have offered a method, in which DDoS attacks could use Management Information Base (MIB) data from the routers having different parameters indicating routing statistics and packets. Anomalies were detected by mapping abnormalities of ICMP, UDP and TCP packets altogether through analysis. It seems to be quite effective for controlled traffic loads, and the information received can be very useful for filtering DDoS attacks.

In a real network scenario, this approach needs further evaluation. Similar to this approach, Huang and Pullen [14] has proposed a mechanism, called “congestion triggered packet sampling and filtering,” in which, congestions happening at a
dropped packets are taken for statistical analysis to find presence of anomaly. Application of Data Mining Technique used by Lee and Stolfo [16] helps detecting anomalies and intrusions by examining the patterns of system features, program and user behavior in the system. In this, host-based intrusion detection approaches are applied. Meta-Detection model, which is a much improved version offering more accurate results in anomaly detection.

Mirkovic et al. [16] has proposed a system, called DWARD for DDoS attack detection, with an understanding that as far as possible, these DDoS attacks must be stopped at the source. Therefore, DWARD was installed at the edge routers which closely monitored the traffic, if there was any asymmetry in the packet rates noticed, D-WARD could limit the packet rate. In this approach, there is a possibility of numerous false positives due to the asymmetry in short duration of the packet rates. Furthermore, some legitimate flows like real time UDP flows do exhibit asymmetry.

4.5.1 Statistical Analysis

The objective of statistical analysis is to identify traffic parameters with regard to abnormality in the network traffic. Figure 4.5 illustrates about the steps how statistical anomaly detection works. First, it must filter the given data inputs, because it significantly affects the detection performance. Second, it separates normal from anomalous, for this, a battery of analysis techniques are applied, like Wavelet, Covariance Matrix and Principal Component Analysis. It is quite challenging to identify or
develop a technique which offers anomaly detection with low false alarm rate. Third, decision theories like GLR test can be performed to ascertain worthiness of network anomaly. [18] For statistical analysis, packet length, number of packets per flow, inter-arrival time, and flow size are required; and for each parameter Mean Value, Variance and higher order moments, Distribution function and Quantiles must be considered. [17]

Let’s analyze the following techniques, and how they work in statistical analysis:

(i) **Change-Point Detection:** It is a powerful tool that helps in determining whether any change has occurred, including the subtle changes. One must note that it provides further information to control charting, but not
a replacement for it. This technique proves very effective especially while analyzing large historical data with regard to better characterization and overall error rate. Thottan et al. [49, 48] have found abrupt changes in a correlated fashion in their experimentation in MIB variable. Similarly, Wang et al. [51] have identified attacks of SYN flooding based on the differences between the number of SYN and FIN packets, then, non-parametric Cumulative Sum (CUSUM) method is used. The works cited elsewhere [1][4][5][9] where traffic dynamics are quasi-stationary, but under certain network environment, it exhibits non-stationary behaviors [3][4]. It must also be noted that all detected abrupt changes do not correspond to network anomalies, therefore, accurate characterization is critical to effective anomaly detection [4][9].

(ii) **Wavelet Analysis:** This analysis has been applied in non-stationary data series modeling, because it characterizes the scaling properties in temporal and frequency domains. Miller et al. [39] have experimented detecting anomaly in geophysical prospects. Barford et al. [5] have applied this technique both in shorter and longer versions and found that this approach isolates traffic anomaly very effectively. The IP packet header data is being taken at an egress router, and then traffic anomaly are put for detection through
wavelet analysis. One of the observations in this technique was that over a time the out-bound traffic exhibited a strong correlation with itself. However, Soule et al. have argued that this method does not perform well in residual traffic analysis compared to the simple GLR method. [45].

(iii) **Covariance Matrix Analysis:** Covariance matrix method is used for detecting flooding attacks in the software system. [54]. Yeung et al. have developed this model, establishing each element corresponding to correlate between the monitored features but at different sample sequences.

(iv) **Principal Component Analysis:** This method involves in the findings of linear combination of a set of variables, and while doing so it removes the maximum variance by repeating it, means it can separate the normal behavior from anomalies through dimensionality-reduction approach. Lakhina et al. modified the approach [30, 31, 32], arguing that the k-subspace obtained from PCA can correspond to the normal behavior of the traffic, and the remaining will correspond to either anomalies or anomalies. Ringberg et al. [41] have performed a detailed study of the feature time series to detect anomalies in two IP backbone networks (Abilene and Geant), saying that “false positive rate of the detector is sensitive,” and in small differences.
(v) **Kalman Filter:** Based on Kalman Filter, Soule et al. [45] have developed a scheme to predict the traffic matrix using Kalman filter. After prediction is done, the actual traffic matrix is estimated based on new link data.

From the above study with regard to limitations of statistical approach, it reveals that most of the tests are for a single attribute, and data distribution cannot be unknown in a high dimensional approach thus will be difficult to estimate the true distribution.

### 4.5.2 Rate Limiting

In the IDS, Rate Limiting detectors are commonly used by research community. Of all Rate Limiting detectors, some are specifically designed for portscan detection. Let’s evaluate how algorithm adaptation and other tuning parameters work for anomaly detection.

Assuming that an infected host will try to connect different machines in a short period of time, Rate Limiting detects portscans by using new connections which can exceed a certain threshold level in a queue. It means that alarm will ring when the queue length exceeds that threshold level. ROCs for endpoints are generated by varying queue length $q = \mu + k\sigma$, where $\mu$ and $\sigma$ represent the sample mean and sample standard deviation of the connection rates in the training set, and $k = 0, 1, 2, \ldots$ is a positive integer. Large values of $k$ will provide low false
alarm and detection rates, while small values will render high false alarm and detection rates. [19]

4.5.3 Data Mining

Data mining is a process, to ensure automatic model extraction from a large stores of data using a wide variety of algorithms [FPSS96]. As scientists and researchers continue experimenting with different models and approaches with regard to IDS, as and when they discover anomalies, they propose new approaches. Still, there is no foolproof mechanism to contain anomaly from attacking network systems. Therefore, as and when these scientists and researchers come across such anomalies, they negotiate with it, at a time experience with cases of false negative or false positive.

To overcome these false negative or false positive problems on network traffic, Data Mining (DM) technique provides a feasible solution. It helps developing better IDS along with NBA (Network Behaviour Analysis), as example, the CPU and I/O activities of a particular user or program can be identified for malicious activity. There are multiple data mining algorithms for IDS. The aim of this study to reduce the use of manual and ad-hoc elements from the process of building an IDS. Considering that the intrusion detection is a data analysis process, then, the data analysis may be taken on the point of data-centric view. Since objective of the research is not only to detect
anomaly but to identify and neutralize them from within the audit data by encoding and matching with the intrusion patterns. Therefore, can one get rid of this with the application of data mining techniques to IDS. Rapid development of data mining has helped us accessing variety of algorithms, mainly in statistical forms:

(i) **Classification:** Classification is a mapping technique from a large source of data with a pre-definition of "normal" and "abnormal" marking in a program. This classification algorithm determines what is normal and what is abnormal from the audit data.

(ii) **Link Analysis:** By correlating with right set of system features in audit data, analysis is done.

(iii) **Sequence Analysis:** This model works on sequential patterns, by developing an algorithm.

(iv) **Decision Tree:** It is a kind of classification algorithm of data mining, constructed taking into consideration of data being pre-classified. One of the problems in this algorithm is in selecting the attributes. [23]

4.5.3.1 **Dimensionality Reduction**

It is a technique to remove predictive information features from the original data [24]. Selection of features considerably reduces complexity in the programming for which it is meant for. It is of two
types: ‘subset selection’ and ‘feature ranking’. In the former, depending upon the suitability of features in the group, it uses genetic algorithms. In the later, based on the scores, it uses a metric to rank the features metric and removes rest of features which are unwanted. [20]

4.5.3.2 Classification Analysis

It is done by assigning objects (intrusions) into classes based on their values and features to identify ‘misuse’ and ‘anomaly detection’. [16]. In the former, SVM, NN, NB or ID3 type of data are collected from traffic, which are labeled as ‘normal’. In the latter, from the same normal data, pre-defined data are collected.

At a time using data mining plays an important role with regard to specially classification techniques. [22]. According to Kumar, “data, facts, concepts or instructions” which are easy to represent, can also be “communicated by humans” or by automation for interpretation and processing. [21] Sequential data can be classified into temporal and non-temporal. The temporal will have time stamp attached to it whereas, the non-temporal will use other dimensions such as space.
4.5.3.3 Clustering Analysis

Based on the distance between the objects (intrusions) and groups (clusters), clustering analysis assigns learning process because of non-availability of information about the data which are labelled. The role of distance or similarity measure are critical in group clustering. Therefore, accordingly metric has to be formulated to determine whether the data is normal or anomalous. For this Jaccard Similarity Measure, Cosine Similarity Measure, Euclidean Distance Measure and Longest Common Subsequence (LCS) measure are used for clustering analysis.

Jaccard Similarity coefficient helps identifying similarity between sample sets. In Cosine Similarity, a common vector is used to identify difference between two vectors. The Longest Common Subsequence (LCS) helps to differentiate between two similar sequences.

Mining models view data as a sequence of network packet, where the technique is commonly used K-Nearest neighborhood algorithm. Should algorithms like clustering and classification be efficient scalable, it can handle high volume network data, whether dimensionality or heterogeneity. [20] Detecting recurrent temporal patterns in digital media content is a first step to the
next generation of data mining. Digital media, depending on content carries a definitive structure that involves either short term interaction or long-term correlation. For example, a video capturing of model, considered for being telecast in a shorter version or long term recurrence. This is all done on temporal model approach.

4.5.3.4 Support Vector Machines

Through a technique like clustering-approach, when it relies on mapping the network connections to a hyper-plane, it is called Support Vector Machines (SVMs). SVM separates data into multiple classes by using of a hyper-plane. It is interesting to note use of same application in the works of Eskin et al. (2002), and Honig et al. (2002), where they have slightly modified the SVM algorithm to operate in unsupervised learning domain. They found the application of this approach giving a better result. For a more conventional SVM approach, Mukkamala, Sung, et al. (2002, 2003) have used five SVMs. One to identify normal traffic and the rest to identify for malicious activity independently in the KDD Cup dataset. They used seven different variations of the feature set and found that every SVM were performing with more than 99% accuracy. In comparison, with the
application of neural network (with a much longer training time) they could achieve a maximum of 87.07% accuracy. In terms of accuracy and speed, they could conclude through this experimentation and research that SVMs are superior to neural nets.

4.5.3.5 **Frequent Pattern Analysis**

It is a kind of pattern (set of items, sequence, etc.) that appears regularly in database, which helps in finding regularities of frequent features in abnormal / malicious packets. For detecting intrusions with the use of data mining approach, two phases must be followed, first: mining a repository of normal frequent itemsets for attack-free data, and second: for finding frequent itemsets in the current sliding window and comparing the patterns with the normal profile. Upon using both these techniques, one can see occurrence of frequent patterns in a data set, which can be easily captured, but the same would be difficult in data streams

4.5.3.6 **Artificial Neural Network**

It is a model based on its structures and functions similar to that of neural network in biology, the information it carries affects its structure due change in neural network, i.e., input and output. It is considered as data modeling tool,
that is nonlinear statistical in which the complex relationships between inputs and outputs are modeled or patterns are found. This neural network can learn from its surroundings by adjusting its internal structure through training process, and by using nonlinear regression, it abstracts information from the abnormal training cases. This is to predict future attacks [5]. ANNs were originally developed to study and analyze human nervous system with the complex webs of interconnected neurons built in. It is based on a set of multiple interconnected neurons, in which each unit plays a significant role for inputs and similarly for outputs. By assigning a value to any two connections helps in determining how much one unit will affect the other, thus mapping is done and stored in the network itself.

Unless there is precise training on the IDS, ANN will fail in detecting any anomaly intrusion. Therefore, it is very critical to have proper training data and adequate training methods. As any training process will obviously need a large amount of data, one must be careful to avoid overfitting. Because such overfitting can easily lead to predictions, which are beyond the range of the training data, or it can produce wild predictions in multilayer perceptron with noise-free data. On one side, process of data collection is difficult, on the other, the nature of
neural network is like that of a black box; thus networks to intrusion detection process becomes extremely challenging. It must also be noted that the connected network nodes will automatically freeze when they achieve the acceptable level of identifying the events. [27]

4.5.3.7 Other Data Mining Approaches

Some of the approaches of Han and Kamber may be referred with reference to the above mentioned approach, which are as under:

(i) Association and Correlation Analysis: This analysis helps to identify and establish based on relationships in large datasets bearing specific values and features. It usually helps in discovering hidden patterns of relationships, which are useful to select discriminating attributes for intrusion detection. At a time, there may be new attributes in the data, as mentioned below, which can also help identifying a particular pattern.

(ii) Stream Data Analysis: Based on the evidence, it is no denying of the fact that intrusions and malicious attacks in wireless software system are dynamic in nature. Though data streams often help detecting such
intrusions, considering it as normal or malicious depending upon the events occurring now and then or frequently.

(iii) **Distributed Data Mining:** Considering that intruders can attack from several different sources, these methods are applicable in detecting and preventing such attacks.

(iv) **Visualization and Querying Tools:** This method works by viewing classes and associations, clusters and outliers. Often used for viewing anomalies and their patterns, and detect them with the use of Graphical interface to analyze and understand IDS performance, which helps in deciding future course of action. [20][21][22]

At the backdrop of existing techniques, the research co-relates with different approaches taking each approach into consideration. Accordingly, the key assumptions are identified to differentiate between normal and anomalous behavior, which are invariably used by each of the techniques. By applying the given technique to a particular domain, the outcome may be measured, and its effects can be authenticated by validation. For each category, this work provides a basic anomaly detection technique, and then shows how the different existing
techniques in that category are variants of the basic technique. Then, the advantages and disadvantages of each techniques are identified in that category. The research also discusses different computational complexity of the techniques along with the limitations, considering that in real-life use, these approaches are not easy to adopt. Therefore, the study provides a wholesome understanding of different approaches it has undertaken, thus giving a clear direction as to how and where these techniques can be developed and applied in a particular domain, keeping in mind of the better and sustainable result, depending upon how it is executed. [23]

REFERENCES


2. Amardeep Singh and Gurjeet Singh (December 2010)“Vulnerabilities and Intrusion Detection in Wireless Networks” IJCST Vol. 1, Issue 2, December 2010; ISSN : 0 9 7 6 - 8 4 9 1 ( O n l i n e )


6. Michel Barbeau, Jyanthi Hall, and Evangelos Kranakis “Detecting Impersonation Attacks in Future Wireless and Mobile Networks”

7. Mei-Ling Shyu, Shu-Ching Chen, Kanosksri Sarinnapakorn and LiWu Chang “A Novel Anomaly Detection scheme based on Principal component classifier”

8. Sandeep Kumar and Eugene Spafford “A Pattern Matching Model for Misuse Intrusion Detection”


10. Amel Meddeb Makhlouf, Noureddine Boudriga (2008) “Intrusion and Anomaly Detection in Wireless Networks” Copyright © 2008, IGI Global, distributing in print or electronic forms without written permission of IGI Global is prohibited; Available At: http://www.irma-international.org/viewtitle/22041/

11. Sutharshan Rajasegarar, Christopher Leckie, Marimuthu Palaniswami “Distributed Anomaly Detection In Wireless Sensor Networks”
12. Shu Yun Lim, Andy Jones “An Anomaly-based Intrusion Detection Architecture to Secure Wireless Networks”


14. Murtaza Masalawala; “Anomaly Detection in Wireless Networks” As a M-Tech Project


19. Ayesha Binte Ashfaq (May 2009) , Muhammad Qasim Ali , Syed Ali Khayam “Accuracy improving guidelines for network anomaly detection systems” Published By : Received: 4 May


24. Marina Thottan, Guanglei Liu, Chuanyi Ji “Anomaly Detection Approaches for Communication Networks”.

25. Chris Giannella, Jiawei Han, Jian Pei, Xifeng Yan, Philip S. Yu “Mining Frequent Patterns in Data Streams at Multiple Time Granularities “

26. Discovering Recurrent Events in Multichannel Data Streams Using Unsupervised Methods

27. Lixin Wang, “Artificial Neural Network for Anomaly Intrusion Detection”

29. Bharati M. Ramageri, “Data Mining Techniques And Applications” Indian Journal of Computer Science and Engineering Vol. 1 No. 4 301-305, ISSN : 0976-5166


31. Iwan Syarif, Adam Prugel-Bennett & Gary Wills, “Unsupervised clustering approach for network anomaly detection”

32. Manh Phung “Intrusion Detection FAQ: Data Mining in Intrusion Detection “


