**Methodology :**

My research from the some books ,paper and watch the movie I use the movie for how I can do my practical work because in the movie we can clearly know .

I use for deferent tools for detecting this attack like: Signature-based IDPS, SOM-based, KDD\_TND and etc…

**Signature-based IDPS:**

These signatures are used by IDPS for attacks detection. For example, when it detects „Land‟, „Teardrop‟ attack; packet containing that attack is dropped.

After detection it performs preventive steps according to type of attack detected Signature-based IDPS is designed to detect and prevent server from Land, Pod, smurf, teardrop attacks .these attacks are considered as known DoS attacks. Neptune (SYN Flood) and two resource consumption attacks are used as Novel attacks. Originally Duration, Src\_bytes and Dst\_Bytes fields contain continuous values, but these values are not suitable for Frequent Item set identification. So these fields are converted into discrete by dividing them by 10.

This attack working:

1: Receive network traffic feature record

2: Search for network traffic feature record in KAS DB

3: If (Attack detected) Then a) Take preventive action according to type of attack detected b) Go to step 1 Else a) Insert traffic feature record in LogDB b) Go to step 1

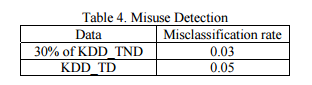
4: Go to Step 1

**ISS:**

Using ISS, we scan our network for computers with known security vulnerabilities, and then reports are sent to the system administrator. Custom scans are developed to detect other vulnerabilities where ISS is insufficient. For example, scans for the latest "named" exploit were developed and used. The administrators for all machines identified as running "named" were notified, and they either patched or disabled "named." In another case, a teardrop check was developed to allow users to test their machines and verify vulnerabilities to a teardrop attack. Review of the latest CIAC and CERT advisories, as well as frequent checks of hacker resources such as bugtraq, provide critical knowledge of the "newest" attacks. These advisories and hacker resources are often the stimulation for development of a custom scan.

**KDD\_TND and KDD\_TD :**

we use two subsets of KDD Cup 1999 data for training (KDD\_TND) and test(KDD\_TD). We consider Back, Neptune, Pod, Smurf, teardrop, Ipsweep, Nmap, Portsweep and Satan as attacks. 70% of KDD\_TND is used for training and 30% of KDD-TND and KDD-TD are used for test of anomaly detection and misuse detection. Misuse detection trains the data including normal and all considering attacks and catches intrusions in terms of the characteristics of known attacks. We train the mixture of normal and attacks and build and label the U-matrix to evaluate the performance of misuse detection in our system. Then we collect the results of BMU for Attack Classification Based on Data Mining Technique 29 test data in our system. Table 4 shows the misclassification rates in terms of the misuse detection. Since the misclassification means that our system selects the wrong BMU, the lower rate is the better. The rate of 30% KDD\_TND is lightly lower than that of KDD\_TD because 30% of KDD\_TND is familiar with 70% of KDD\_TND and U-matrix is more adjustable to the characteristics of 30% of KDD\_TND. If our system collects and train the data at the network installed, the result is similar to that of 30% of KDD\_TND.



**SOM-based:**

The SOM-based intrusion detection mechanism Figure 1 show our system with three steps as follows: Training, Labeling and Detection & Training. Training means creating the map based on the preprocessed and normalized data using SOM. Labeling means classifying clusters from the trained map based on the traffic feature correlations. Finally, Detection & Training means the real-time intrusion detection and the continuous training to adapt our system to new data.

Training The accurate training requires the modification of data because the values of traffic features have the various ranges. Our mechanism has the preprocessing stage and the normalization stage before training. Preprocessing It transforms the TCPdump data into the numeric data because SOM resolves only numerical data but the TCPdump data has some features whose data types are not numeric.

