# ENHANCED MOVING TARGET DEFENSE MECHANISMS TO HANDLE CYBER ATTACKS

## CHAPTER 2

## REVIEW OF LITERATURE

After framing the objectives of the thesis, the existing cyber attack handling methods are reviewed. Due to the increasing number of cyber attacks, cyber attack is a major challenge. According to the general approach, the signatures of the attacks are studied and a database is created and incoming traffic pattern is studied to prevent the incoming attacks. These types of attacks are called as known class of attacks. In the beginning of the literature, the known attack handling methods are reviewed. The two steps involved in the known attacks handling mechanisms are

i. Network Traffic Monitoring and
ii. Attack Detection

The existing methods are studied and compared. However, it is observed that the unknown attacks are more vulnerable due to the lack of their signatures in the database and their unpredictable behaviour. Hence, the second step focuses on the unknown attack handling mechanisms. The literatures corresponding to known and unknown attack handling methods are presented in this chapter. First, the known attack handling methods are studied and examined.

As a first step, the existing network traffic monitoring methods are studied.

## 2.1. Network Traffic Monitoring

Accurate identification and classification of network traffic according to the application that generated is the first step towards network security management. Due to the dynamic characteristic of the Netflow, it is difficult to detect the network abnormality and predict the time when the fault will happen.

There are various traffic monitoring techniques available based on many concepts. They are classified into four types namely, Based on Queuing Theory, Based on Forecasting Algorithm, Based on Statistical Method[45] and Monitoring and Analysis

Techniques. The classification of network Traffic Monitoring Techniques is given in Figure.2.1

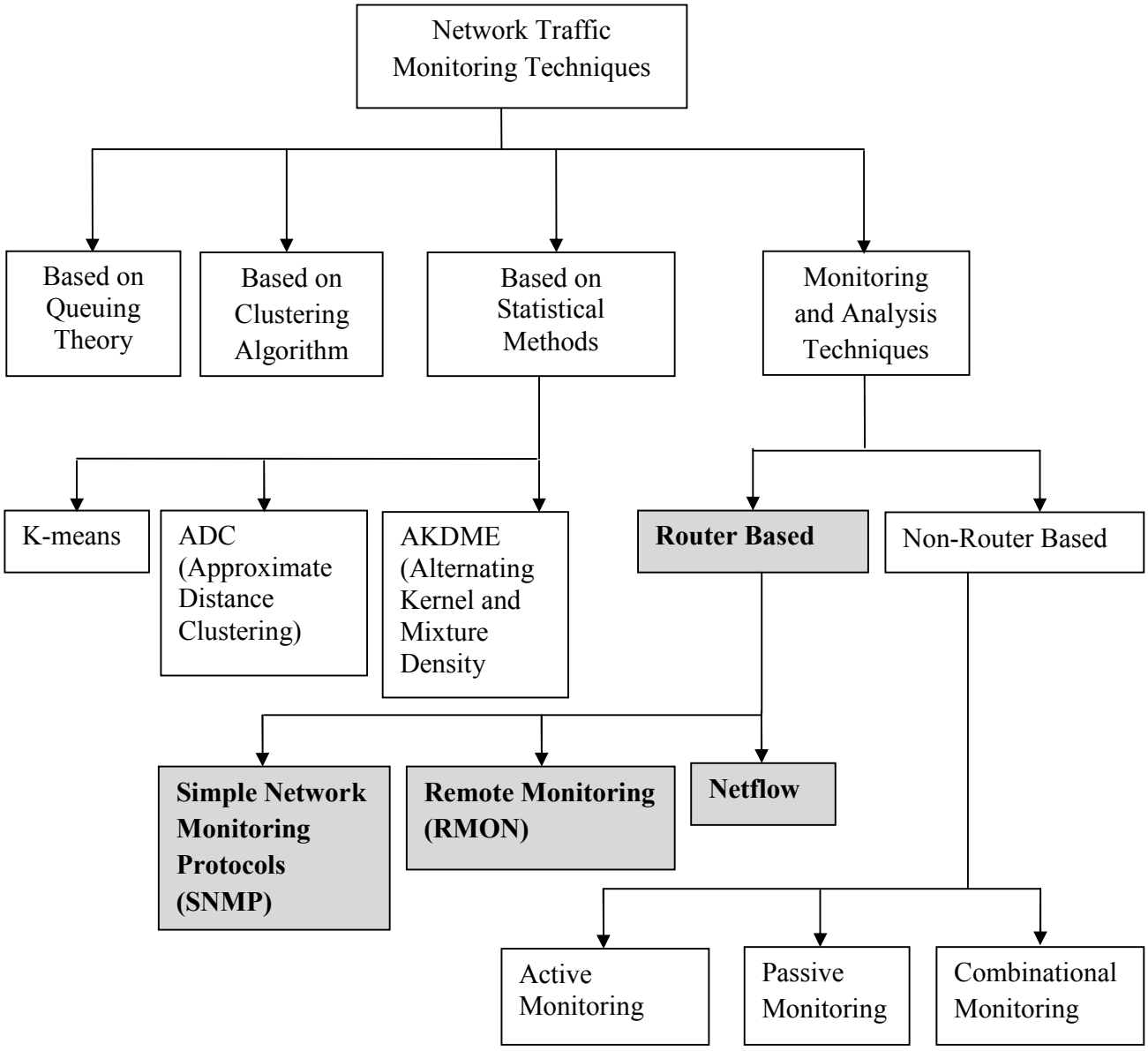


**Figure.2.1 Classification of Network Traffic Monitoring Techniques**

To handle the cyber attacks, the monitoring and analysis techniques are studied. The two types of monitoring techniques are router based and non-router based. Out of which, the router based methods are used widely to analyze the incoming traffic of network against the known cyber attacks.

**Router Based Monitoring Techniques**

The main idea behind the router based monitoring techniques is to embed the input data to the router without any requirement of hardware/software resources. Basically, these techniques are hard-coded so that they offer flexibility. Router based monitoring technique is a process of fixing the input data strongly into the router that allows for traffic flow due to profound modest agreement. The router based monitoring consisting of three methods namely

i. SNMP (Simple Network Monitoring Protocols),

ii. RMON (Remote Monitoring) and

iii. Netflow

Router based monitoring techniques have evinced keen interest in the recent times because of their ease of use, applicability for research and effectiveness in monitoring the wireless networks.

**Simple Network Monitoring Protocol (SNMP)**

SNMP uses passive sensors to collect the traffic data. The traffic data will be generated based on the flow from the router to the host. SNMP handles the entire traffic monitoring using the three components namely, Manager, Agents and Network Management Devices.

The communication between the manager and the agent will be similar to client/server communication paradigm which is shown in figure.2.2

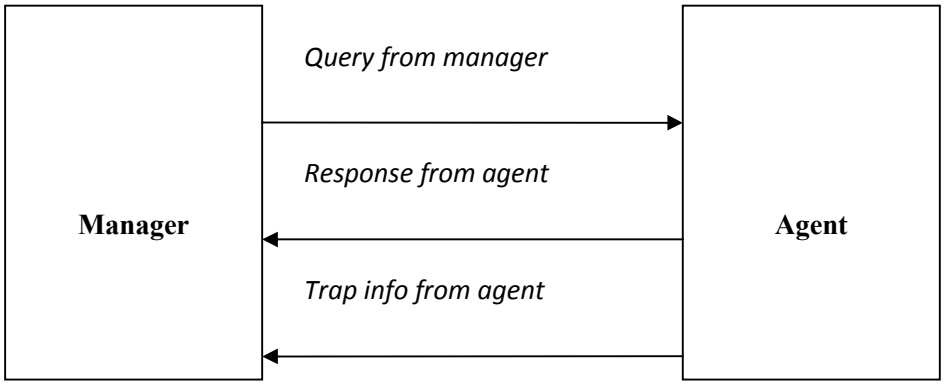


**Figure.2.2. Communication between the Manager and Agent**

The flow of SNMP consists of various steps like Command Generator, Dispatcher, Message Processing Model and Security model. They all play a major role in requesting, generating and responding to the queries by the manager to the guest. SendPdu and processResponsePdu are the two processing steps of Command Generator. The information related to the intended destination, security parameters and Pdu will be sent to the dispatcher. The dispatcher will put forward to message processing model and then the security model will bring up the message. After that, the message prepared by the security model will be forwarded to the transport layer by the dispatcher. The return primitive value will be generated by dispatcher as an indication to an unsuccessful attempt in preparing the message. The dispatcher dispenses SendPduHandle to PDU and the value will be forwarded to command generator once the message is successfully prepared. Otherwise, the message will be stored by the command generator so that it can

be used to compare with the request if there is a necessity. The processResponsePdu primitive will be used to deliver the incoming response PDU to the appropriate command generator. The algorithmic steps involved in SNMP is given in table.2.1.

**SNMP Algorithm**

**Table.2.1 Algorithmic steps of SNMP**

```
Input:S-> CommandGenerator,
R->CommandResponder
DTS-> Data Transfer Service
Msg-> Message
Pdu->Protocol data unit
repeat
  for each neighbor nodein the network
     if route exists then
                  send Pdu to dispatcher
                 send DTS outgoing Msg prepared to generate RequestMsg
                security model prepares requestMsg
               R registers engine ID with acknowledgement from S
               responsePdu processed  { The Command responder Sends ResponseMsg back}
          else
               response Pdu is returned by R then
              security model generates responseMsg
             dispatcher prepares response Msg
     end if
until end of the node in the list
```

**Remote Monitoring (RMON)**

RMON is an extension of the SNMP Management Information Base (MIB) which helps to monitor the network. Remote Monitoring (RMON) supports the administrator to monitor and to inspect the network without much difficulty. Based on some standards, RMON helps to set the alarm which helps to monitor the network. RMON monitors local

network and remote locations from one central place. RMON has two components such as the probe and the client. It also helps the administrator to analyze the fault, plan and regulate the performance of the information gathered in that network. The Client and the Server are the working characteristic of RMON. It is otherwise called as flow based management. It does not concentrate on any of the devices connected with that particular network; rather it focuses on the pattern of the network traffic. RMON consists of the few goals such as offline operation, proactive monitoring, problem detection and reporting. In remote monitoring, there are nine monitoring groups which are used to gather information. The algorithmic steps involved in RMON is given in table.2.2.

**Table.2.2 Algorithmic steps of RMON**

```
Procedure:
HostTopN- Number of Host
repeat for each node
        collect network statistics
 do
    if a € { token ring, ethernet, host and conversation statistics}
                token ring and ethernet monitored
                history controlled
                host monitored
               HostTopN and matrix passed to network manager
       elseif
                captured data within group
           then
                generate alarm
           else
                generate event
       end if
    endif
  capture packet
  sent to network manager
until end of the node
```

## Netflow

In order to collect the IP traffic information, Cisco system developed a network protocol called Netflow. It is termed as the standard of industries for monitoring the traffic. It is a tool used to evaluate the process of the network. It also deals with traffic monitoring, to clarify the elegant flow, accumulate and estimate the statistics, maintain details about the source and destination IP addresses and protocols. Apart from that, if any unusual movement is found in the network, the Netflow analyzer will accord with those activities. A network administrator can determine things such as the source and destination of the traffic, class of service, and the cause of congestion by analyzing the data that is provided by Netflow. The three components of Netflow include Flow caching, Flow Collector, and Data Analyzer.

The IP data flows that enter an interface are collected by flow caching and prepared for data exportation. The first packet of a flow through the standard switching path is processed to create the cache. Packets with similar flow characteristics are used to create a flow record which is kept in the cache for all active flows. The flow record tracks the packet sent bytes per flow. The cache information is then periodically exported to the Flow Collector. Data collection, filtering, and storage are done by the flow collector which contains a history of flow information. The presentation of data is done by data analyzer. The processing of Netflow is given as algorithm in Table.2.3.

**Table.2.3 Algorithm for Netflow**

```
Procedure:
a->Server
UDP-> User Datagram Protocol
SCTP –> Stream Control Transmission Protocol
repeat
for each netflow exporter
do
if a € { netflow records} then
    netflow probes generates
    netflow server stores
     transmits data using UDP and SCTP
     records statistical information of packets
end if
    filter activated
```

Some of the existing literatures of router based network traffic monitoring methods are discussed below.

**Chia-Mei Chen and Chuan-Pi Wei (2007)** developed a network monitoring mechanism based on Netflow for larger networks. The proposed system consisting of three phases namely, Collecting Module, Statistic Analysis Module and Rule Based Analysis Module. This method is adapted for real time traffic flow as well. This system is specially designed to detect DDoS(Distributed Denial of Service) attacks. The simulation result shows that the solution suggested by the author efficiently monitors the large sized network and detects denial of service attacks, port scans and worm propagation.

**Frederic Beck (2007)** presented a deployment of Netflow and RMON in a testbed [25]. The network is deployed similar to Cisco network. While deploying the network, the flow of the network, Netflow record is completely like Cisco's deployment procedure. For RMON overview, RMON agent implementation, RMON groups are clearly defined. The authors summarize all the required information from the different official Cisco

documentations which enable to understand what Cisco Network Analysis Module is and how it works.

**Aiko Pras et al., (2004)** present a generic formula to calculate SNMP's bandwidth requirements; the bandwidth consumption of prototypes is compared. Bandwidth usage, CPU time, memory requirements and round trip delay are implemented to evaluate the performance of SNMP. The authors have concluded their study saying that SNMP is capable of retrieving single object from web services, but not that much capable of retrieving many objects from web services.

**Paul Barford et al., (2002)** presented a signal analysis of both short and long-lived network traffic anomalies in IP flow and SNMP. The authors have collected data at University of Wisconsins' border router. To isolate the anomalies, various time frequency analysis techniques are used for the data. Based on high and medium frequency bands, they have developed a concept of deviation score. This method is enormously valuable in isolating the anomalies and for generation of threshold-based alerts that can be used willingly.

After the literature study, it is observed that SNMP performs better than the other two router based monitoring techniques. Though it outperforms the other two methods, it needs to be enhanced to reduce the processing time as it involves more processing steps.

After network traffic monitoring, the next step is detection of known cyber attacks using the dimensionality reduction techniques. Many related literatures are reviewed.

## 2.2. Detection of known cyber attacks using Dimensionality Reduction Techniques

Dimensionality reduction techniques are used to transform the original high dimensional data into consequential description of reduced data. The dimensionality reduction techniques are mainly classified as linear and non-linear techniques. The process of assuming that the data will be placed on or near a linear subspace of higher

dimensional space is termed as linear technique [4]. Figure.2.3 shows the classification of dimensionality reduction techniques.

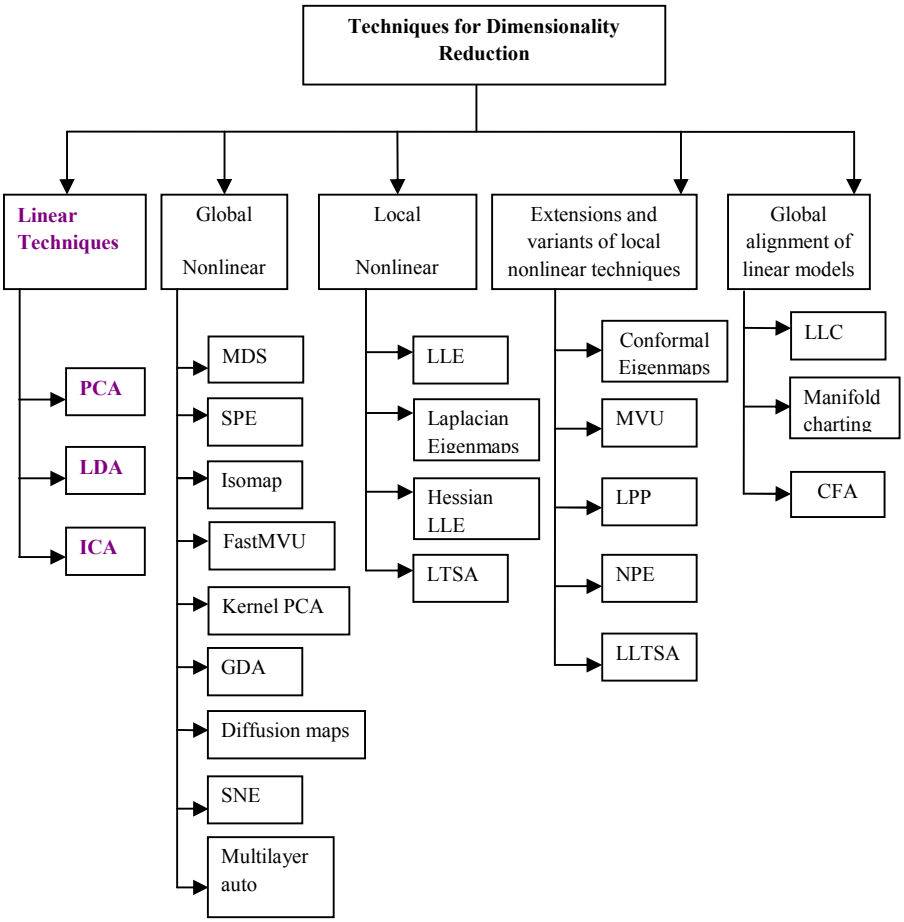


**Figure.2.3 Dimensionality Reduction Techniques**

Following are the linear dimensionality reduction techniques applied to reduce the dimension of the traffic data.

i.Principal Component Analysis

ii. Linear Discriminant Analysis

iii.Independent Component Analysis

**Principal Component Analysis (PCA)**

PCA is considered as competent scheme for identifying any type of attacks. It helps to check the similarities and differences among the data. The processing steps of PCA is fully dependent on comparatively reconstructing the huge numeral variables into lesser of uncorrelated variables where the data will be retained as it is**.** PCA produces a set of principal components, which are orthonormal eigenvalue/ eigenvector pairs. It is considered the most efficient analysis tool as it helps to reduce the data in certain outline without losing the data. Steps Involved in PCA are given below:

Transform an N x d matrix X into an N x m matrix Y:

- Centralize the data (subtract the mean)
- Calculate the d x d covariance matrix: $C = \frac{1}{N-1} X^T X$
  - $c_{i,j} = \frac{1}{N-1} \sum_{q=1}^{N} X_{q1} . X_{qj}$
  - $C_{i,i}$ (diagonal) is the variance of variable i.
  - $C_{i,j}$ (off-diagonal) is the covariance between variables i and j
- Calculate the eigenvectors of the covariance matrix
- Select ‘m’ eigenvectors that correspond to the largest ‘m’ eigenvalues to be the new basis

| |
|---|
| m –length of the vector |
| N – data size |
| d – dimensional data vector |
| $X_{nxm}$ – representation of dataset |

The principal component produces the results in component values according to the number of original variable. The first linear variable will be calculated by replacing the original variable with new principal component. Principle component values can be calculated using the following mathematical equation:

$$X_{nxm} = \begin{bmatrix} x_{11}.....x_{1m} \\ x_{21}.....x_{2m} \\ ..... \\ x_{n1}.....x_{nm} \end{bmatrix} = [x_1,...,x_n]$$

$x_1$, $x_2$ are the observations which will be exhibited as vector of length 'm' and the entire dataset will be reproduced as matrix $X_{nxm}$.

**Linear Discriminant Analysis (LDA)**

Linear Discriminant Analysis[68] is one of the linear dimensionality reduction techniques that helps in sorting biased information in to groups to the maximum to execute the dimensionality reduction operation. It aims to locate the directions [3]. It is a promising strategy developed recently to detect attacks from network traffic [5]. The following equation is used to detect the anomalies.

$$S_w = \sum_c P_c \underset{x^c - x^c}{\text{cov}}$$

$$S_b = \sum_c \underset{\bar{x}^c}{\text{cov}} = \underset{x - \bar{x}}{\text{cov}} - S_w$$

$p_c$ is priori of class label c

cov $x^c - \bar{x}^c$ Covariance matrix of the zero mean data point

cov $\bar{x}^c$ Covariance matrix of the cluster

cov $x - \bar{x}$ covariance matrix of the zero means data x

$S_w$ within class scatter

$S_b$ between class scatter

## Independent Component Analysis (ICA)

Linear transformation is performed in order to split multivariate signal into subcomponents and it is the basic process of ICA[1][2]. ICA has wide area of applications in data analysis, compression, audio and image processing, feature extraction, signal separation, detecting the hidden components, Noise diminishing from Images and telecommunications [6]. The process involved in this method relates the process of blind source separation [7]. It helps for redundancy reduction. The following equation is used for detection of hidden components.

$$X_j = a_{j1}s_1 + a_{j2}s_2 + ..... + a_{jn}s_n \ , \quad \text{for all j.}$$

$x_j$ _ random vector

$s_1$ ……. $s_n$ - random variables

$a_{j1}$ …… $a_{jn}$ - matrix with elements

**Annie George (2012)** conducted an experiment using Principal Component Analysis for dimensionality reduction and Multi-class Support Vector Machine for classification of cyber attacks. The experimental results have been analyzed based on precision and recall values for each class and it shows that classification using dimensionality reduction is more accurate depending on the new subspace where the features are combined together according to maximum variance which enhances classification using discriminating plane. The algorithms can be used for anomaly detection.

**Shailendra Singh et al., (2011)** presented an algorithm which is efficient and scalable to classify the cyber attacks. In order to classify the cyber attacks, the author introduced an iSVM (improved Support Vector Machine) algorithm. The iSVM algorithm is compared with SVM which helps in evaluating the accuracy rate in detection using false alarm rate, testing time and training time. The author claims that iSVM gives 100% accuracy.

**Shilpa lakhina et al., (2010)** developed a new hybrid algorithm namely PCANNA (Principal Component Analysis Neural Network Algorithm) which helps in reducing usage of resources, memory and CPU time requirement for detection. The author declares that the algorithm developed gives better results in terms of 80% in feature reduction, 40% training time and 70% testing time. In this method, the classification accuracy is improved. This method is observed to be more reliable in intrusion detection.

**Huizhong Sun et al., (2008)** developed a PCA based defense system for denial of service attacks which helps in analyzing the traffic data. According to the violation of nominal traffic intrinsic dependency, the attacks are identified. The data set used is from the Internet traces of WIDE project. Principal Component Analysis (PCA) and Conditional Legitimate Probability (CLP) methods are experimented against both static and dynamic attacks. The PCA with statistical filtering rule scanning reduces the false positive against adaptive Distributed Denial-of-Service (DDoS) attacks.

**Almotairi et al., (2008)** proposed the use of principal component analysis (PCA) on the traffic flows of low interaction honeypots. PCA is observed to be a very powerful tool in detecting the structure of attackers' activities and the decomposition of the traffic into seven dominant clusters. The author proves that principal component analysis could provide administrative level security with a very simple and efficient way of summarizing honeypot traffic and monitoring activities. The entire study is done in

offline mode which can be followed for real time model for monitoring honeypot traffic and provides security alerts for Internet threats.

**Huizhong Sun et al., (2008)** developed a defense system against DDoS with statistical filtering rules scanning. Packet Score, a statistical filtering rules-based scheme and PCA-based scheme effectively differentiate attack packets from legitimate ones, when defending against various static, dynamic, and adaptive attacks.

**Dayu Yang (2008)** applied Independent Component Analysis for feature extraction for network intrusion detection. The author says that the method developed outperforms Principal Component Analysis (PCA). To increase the accuracy level, the author used decision fusion method to aggregate the results. The experimental results show that ICA based feature extraction method is able to reduce computational burden for classification of attacks, and at the same time maintaining the level of detection accuracy significantly.

**L.J.P. Van der Maaten et al., (2008)** have presented a review and comparative study on dimensionality reduction techniques[41] and concluded that non-linear techniques for dimensionality reduction are not yet capable of outperforming traditional PCA.

**V. Venkatachalam and S. Selvan (2007)** developed an Intrusion Detection System using LAMSTAR neural network to learn patterns of normal and intrusive activities. For classification of observed activities of the system, the author has used three classifiers. Based on the performance comparison the author says that LAMSTAR IDS performs better than the other classifiers they have taken for study. The author also used PCA for reduction of dimension of data which helps in reducing the computational complexity, training time and testing time.

**Wei Wang and Roberto Battiti (2006)** introduced a novel method for intrusion identification in computer networks based on Principal Component Analysis (PCA). The

method developed is capable of identifying different types of attacks. It is also capable of giving intimation if it detects any attacks so that necessary steps can be taken. This method is modeled to transform each network connection as data vector with the help of feature extracted after the dimension is reduced using PCA. Thus it is an effective model to process a high quantity of audit data in real-time with low overhead and it is suitable for real-time intrusion identification.

**Khaled Labib and V. Rao Vemuri (2004)** present a method for detecting Denial-of-Service attacks and Network Probe attacks using Principal Component Analysis as a multivariate statistical tool. In this work, the authors study about the nature of attacks, Principal component analysis and also discussed about the merits of using it in intrusion detection. The proposed method helps in extracting the Principal Components and the related statistics. The results are obtained from the proposed threshold value for detecting the subject intrusions. The study also presented a graphical method for interpreting the results obtained based on the Bi-plots.

**Wei Wang et al., (2004)** presented a new method for intrusion detection method based on Principle Component Analysis (PCA) with low overhead and high efficiency. To validate the new method, system call data and command sequences data are used as information sources. PCA is used for dimensionality reduction of data vectors, Distance between vectors and its projection onto the subspace is used for anomaly detection. The method is evaluated based on detection accuracy, computational expenses and implementation for real-time data.

Due to the literature study, it is very clear that the Principal Component Analysis is the most popular method among all other methods and it performs better in all circumstances and it is well suited for detecting the known cyber attacks.

In the next section, the detailed study on moving target defense mechanisms is done. The four moving target defense mechanism is analysed for improvement in detecting the unknown cyber attacks.

## 2.3. Moving Target Defense Mechanisms

Four Moving Target Defense Mechanisms are taken for research work and they are examined. They are:

i. **Smart Motion Adaptation/Management – Game Theory**
ii. **Robust Cryptographic Authentication – Mouse Dynamics**
iii. **Data Chunking and Decentralization**
iv. **Decoys**

### 2.3.1 – Smart Motion Adaptation/Management – Game Theory

Game theory[6] [62][75][82][90] is a kind of a concept used for decision making. it helps in determining the co-operation and differences among the decision makers using the mathematical models. Recently, game theory is used almost in all fields like security[51][53][55], economics, political science, and psychology, logic and biology. game theory is fully based on mathematical object. It consists of players, moves, payoffs, etc.

**Xiannuan Liang and Yang Xiao (2013)**, they have done a study on game theoretic approach for providing security for networks. In their analysis they classified application scenario in two categories namely, Attack-defense analysis and Security measurement. The solution is summarized into two as co-operative game models and non-cooperative game models. Players, Actions, Payoff, Strategies are the basic elements needed to play a game are clearly stated by the authors. The defense attack interactions are abstracted into the following group such as System, Attacker, Attack target, IDS, Virtual sensor and

Defender. Various models of co-operative and non-cooperative are discussed in detail. In this paper, they have clearly stated that the game theoretic approach is a powerful tool for network security.

**Ramona Trestian et.al, (2012)** presents an overview of network selection decision problems, challenges, also the classification of game theoretic approaches and applications are discussed in detail. Monitoring, Network selection/Handover(HO) decision and Call setup or HO execution are the three main steps involved in network selection process. The key elements of network selection problem discussed in this paper help the researcher and engineers who are unfamiliar with. Basic concepts of game theory are well defined and mapping network selection with game theory is also stated in this paper. Various game theoretical models that suit for network selection are also given briefly and a range of classification of game theory approaches is also given in this paper. At the end, the challenges of game theory for 4G are well defined.

**Jaeok Park and Mihaela van der Schaar (2012)** developed a game theoretic framework for the design and analysis of the new class of incentive schemes called intervention schemes[31]. The proposed framework is applied for resource sharing scenarios in wireless communications. Resource sharing scenario of intervention has two types and they have discussed in a better manner called as Intervention equilibrium

**DejunYang et.al, (2012)** have done a detailed study on existing game theoretic approaches based on cooperation incentives in cooperation communications. The cooperation communication is suitable for cellular networks, ad-hoc networks and cognitive radio network environment. The topologies of cooperative communications are one-to-one, one-to-many and many-to-one are also discussed in this paper. In this survey, cooperative incentives of cooperative communications say reputation-based mechanism, resource-exchange mechanism and pricing-based mechanism are given in detail.

Selections of the utility function, Mechanism design, Efficiency of Nash Equilibrium, Computation of Nash Equilibrium are the challenges in applying game theory.

**Samuel N. Hamilton et.al, (2008)** discuss major challenges of information warfare that are analysed in this research work. Fundamental issues such as only restricted examples can be represented, multiple and concurrent moves, timing for moves, well-known legal moves may change in times, different end goals, etc are analysed in detail.

**Tansu Alpcan and Tamer Basar (2004)** discuss about a game-theoretic approach for intrusion detection in access control systems is analysed in this research work. Both finite and continuous-kernel versions are investigated for security game between the attacker and the intrusion detection have been done and specific cost functions will be associated with the players in continuous-kernel versions. Distributed virtual sensor network based on software agents with imperfect detection capabilities are also introduced in this model. Dynamic characteristics of the sensor network are also taken into consideration as an extended work of the model presented. A quantitative mathematical framework is established that offers the approach in addressing the wide range of intrusion detection's resource allocation problem. Every moment of communication of the players will be analysed using repeated games.

**Kong wei Lye and Jeannette Wing (2002)** proposed a game strategy in Network Security. They have modeled a stochastic game between the attacker and the administrator. To compute the Nash equilibrium for both players and administrator non-linear program NLP-1 is used. Network state, Actions, State transition probabilities and costs and rewards are discussed in detail. The Nash Equilibrium is briefly explained as each player's responsibility. Attacker's view of the game and administrator's view of the game are clearly stated by the authors. The above works are shown in Table.2.4.

**Table.2.4 State of the art – Game Theory**

| Year | Author | Method | Parameters used | Results/ Inferences |
|---|---|---|---|---|
| 2013 | Xiannunan Liang | Co-operative and Non-cooperative models | ------- | Powerful Tools |
| 2012 | Romona Trestian | Co-operative and Non-cooperative models | ------ | Open issues that further investigations, computational complexity important issue |
| 2012 | Jaeok Park | Intervention schemes | Payoff | |
| 2012 | Dejun Yang | Co-operative communication | ------ | Can be extensively apply, more challenges for research |
| 2004 | Tansu Alpcan | Finite and continuous-kernel non-cooperative games Dis-crete time system model | Nash equilibrium cost, Time | -------- |
| 2002 | Kong-Wei Lye | Non-linear program | Nash equilibria state values | Best attack strategies, more realistic |

### 2.3.2. Robust Cryptographic Authentication – Mouse Dynamics

**Bassam Sayed et.al (2013),** introduce a new framework for static authentication for mouse dynamics. Vector quantization neural network classifier is used to capture the gestures in this research work. The evaluation of the proposed system is conducted for 39 users based on false acceptance ratio and false rejection ratio. Accuracy and validation is improved using the proposed system as this is the first method which provides the relatively accurate static authentication scheme.

**Chao Shen et.al (2013)** proposed a simple and efficient user authentication approach based on a fixed mouse-operation task. To get the accuracy and mouse behavior fine-grained characterization of every user traditional holistic feature and feature newly introduced in proposed system are also extracted. To increase the efficiency of the mouse

feature, space distance-measurement and eigen space-transformation techniques are used and for distance-based feature eigen space for the authentication one-class learning algorithm is applied. The dataset used is 5550 mouse-operation samples from 37 subjects. Authentication time is also analyzed based on false-acceptance rate and false-rejection rate is also calculated to ensure the efficiency of the proposed system.

**Cheng-Jung Tsai et.al (2012)**, in their research work captured the clicking and pressing of mouse button based on time. Down-Up, Down-Down, Up-Down, Up-Up and Down-Up2 are the five features analyzed and experimentation is done with 25 users. Imitate samples and non-imitate samples are used to extract those five features for 25 users. The weight scores are calculated using three statistical methods. False Acceptance Rate, False Rejection Rate, Average False Rate and Equal Error Rate are the four performance metrics used to evaluate the proposed system. The authors have concluded that the system proposed increases the portability and the same system can be applied in electronic devices. To improve the security level, this system can also be used as standby identifiable factor of the keystroke-dynamics based authentication. Finally they have declared that error rate of the system is high and reducing the error rate is given as future scope.

**Harini Jagadeesan and Michael S. Hsiao (2009)** proposed a user re-authentication system which is application independent, continual, non-intrusive, fast and easily deployable based on user behavioral biometrics of keyboard and mouse operations. Mouse-to-keyboard interaction ratio and interaction quotient are proposed to extract the attributes of the user. Behaviour of the user will be captured every time and it will be with the existing behavior which is stored already. The accuracy and application independency of the proposed is improved comparatively. The performance metrics

sensitivity, specificity, false acceptance rate, false rejection rate and accuracy are used to evaluate the proposed system.

**Ahmed Awad et.al (2007)** introduced a new technique to capture the mouse behavioral characteristics of the user using artificial neural network. The first experiments are conducted for 22 participants, mouse movements are collected randomly for 284 hours, 45 sessions for every user and 998 sessions for entire users. The second experiments were conducted for 7 participants. The proposed system is evaluated using the performance metrics such as receiver operating characteristic (ROC), confusion matrix, false acceptance rate and false rejection rate.

**Adam Weiss et.al (2007)** focused a detailed study on data collection, feature metrics, and classification. New software is developed for capturing the data, feature extraction, creation of user profile and classification of patterns. Leave-one out method of next Nearest Neighbor is used for implementation and the success rate achieved is 92%. Experimentation is done with five users for 25 sample data to train and test the software developed.

**Ross A.J. Everitt and Peter W. McOwan (2003)** introduced a new concept for security using biometric authentication. Proposed is a novel method which combines two different biometrics to make sure that the system provides authenticity. The experiments are conducted for 41 participants and the dataset collected are trained using back propagation algorithm and stored for future verification. False acceptance rate, false rejection rate, latency time and hold time are the performance metrics used to evaluate the system developed. It is concluded that better results are achieved for FAR and FRR by the proposed system and suggested that the system can be applied for heterogeneous networks. Table.2.5. shows all the above works.

## Table.2.5 State of the Art – Mouse Dynamics

| Year | Author | Method | Parameters used | Results/ Inferences |
|---|---|---|---|---|
| 2013 | Bassam Sayed | Vector quantization neural network classifier | Accuracy, Validation | First method provides relatively accurate static authentication scheme |
| 2013 | Chao Shen | Distance-based feature, Eigen-space transformation techniques, one-class learning algorithm | Accuracy, Fine-grained, Efficiency FRR, FAR | |
| 2012 | Cheng-Jung Tsai | Rhythm click-dynamic authentication system | Down-Up, Down-Down, Up-Up Up-Down, Down-Up2, FRR, FAR AFR, EER | Increase probability, It can be applied for all electronic devices |
| 2011 | Nan Zheng | Support Vector Machines | Direction, Angle of Curvature, Curvature Distance, Speed, Pause-and-Click, False Reject Rate, False Accept Rate | Techniques is robust across different operating platforms, no specialized hardware is required, verifies user in accurate and in time, induced system overhead is minor. |
| 2009 | Harini Jagadeesan | Feed forward network with back propagation algorithm, K-NN algorithm | Sensitivity, Specificity, FAR, FRR Accuracy | Accuracy – 96.4% Application based model – 82.2% |
| 2007 | Ahmed Awad | Artificial Neural Network | Receiver Operating Characteristic (ROC), Confusion Matrix, False Acceptance Rate and False Rejection Rate. | Explores multiple sets of conditions, |
| 2007 | Adam Weiss et.al | Leave-one out method | | Success rate achieved is 92%. |
| 2003 | Ross A.J. | Back Propagation Algorithm | False acceptance rate, | Better results is achieved |

| | | | | |
|---|---|---|---|---|
| | Everitt | | false rejection rate, latency time and hold time | for FAR and FRR<br>Can be applied for heterogeneous networks |

### 2.3.3 – Data Chunking and Decentralization

Data chunking[84] is a process of split the files into chunks. The size of the chunks will be determined well in advance. Data chunking consists of thousands of rows and columns. In order to improve the performance of Input and Output operations the chunks should be applied correctly which helps to reduce the redundancy[8][22][36][37][46][83][94] of reading and writing to a scientific dataset. The process involved in chunking is reading and writing in scientific data set. Since it is an efficient way of storing there are some issues related to reading and writing are compressed, subsetting, chunk sizing, chunk cache sizing and compression and chunk cache sizing respectively.

**Diego Perino et al., (2012)** proposed a novel framework to eliminate the redundancy of data storage and the technique bridges the Information-Centric Networking (ICN). The author analyzed in detail about Named Data Networking (NDN), Redundancy Elimination (RE), identifying the redundancy, data chunking. Bandwidth, hardware and software suitability is comparatively enhanced with the existing system called vanilla ICN. Complexity in traffic saving is much simpler in ICN-RE when compared to the existing techniques SmartRE and EndRE. Delay is reduced and bandwidth is increased using this method than the existing method.

**Punyada M. Deshmukh (2012)** developed an application which ensures the data storage security using a distributed scheme. Set of master servers are responsible to process the user requests. File chunking process will be executed with file recovery and data backup. The proposed system will benefit android users and chatting applications as well.

**Seiichi Ozawa (2008)** proposed an extended work of IPCA (Incremental Principal Component Analysis) called *chunk* IPCA. Three eigenspace models, Fixed Eigenspace, IPCA and Batch PCA are compared to evaluate the proposed system. Classification accuracy and testing time are the two performance metrics used in this research work. The author says that the training time is lower while using chunk IPCA than the IPCA even for high attributes of input. Seven large-scale data sets with a large number of data samples and attributes are used to evaluate the scalability and learning of the proposed system. Learning scheme of the proposed method executes well though the sample data set is given at any size of chunks.

**Mark W. Storer, et al., (2008)** proposed a secure data Deduplication for efficient spacing as well as for protecting the data. They have developed two models for secure storage such as authenticated and anonymous. Once the data is chunked, the key generation is done in order to encrypt the data and also designed a map to reconstruct the chunked data to its original form.

**Deborah S. Carstens (2006)** suggested a technique to evaluate the authentication of password crash[20]. Two levels of experiments were conducted to create password which is pertinent, consequential password and it ensures that it is not easily reachable by the public. A password chunking theory is introduced in this research work. 7-Character Password Level, Two-Chunk Password Level, Three-Chunk Password Level, Four-Chunk Password Level are the various levels of chunking used in this research work. Recall rates and paper rates are the two performance metrics used to evaluate the proposed method.

**Hong Shen (2004)** developed a combinational approach using trigram Hidden Markov Model (HMM) and Data Representation (DR) voting techniques. The analysis is done for Multiple Data Representations and Multiple Learning Models. It is observed that the

chunker is faster, simpler and very accurate in training and decoding. CoNLL-2000 dataset is used for this research work. The above works are compared and the summary is given in table.2.6.

**Table.2.6 State of the art – Data Chunking**

| Year | Author | Method | Parameters used | Results/Inferences |
|---|---|---|---|---|
| 2012 | Diego Perino et.al | Information-Centric Networking, Redundant Elimination | Bandwidth, processing probability | Improves bandwidth efficiency by 15-40%. Delay reduced |
| 2012 | Punyada M. Deshmukh | Cloud computing | ------ | Effective working environment Quick updates |
| 2008 | Seiichi Ozawa | IPCA | Classification accuracy, Testing time | Reduced training time, Learning scheme executes well |
| 2008 | Mark W. Storer | anonymous and authenticated models | -------- | -------- |
| 2006 | Deborah S Carstens | trigram Hidden Markov Model DR voting technique | Precision Recall | 94.01 score |

### 2.3.4 – Decoys

The concept behind decoys is to place a fake system to capture the attack and its pattern. Almost it performs like a sensor nodes, which predicts the attacks and the pattern of attacks during the beginning period itself. Decoys have the capability of emulating the system, virtual machine, applications, data, network, sensors and actuators.

### Time Triggered Approach

In the time triggered[66] schemes, the link state updates are generated periodically, based on a specified interval of time between two successive link state updates originated at a given node. The clock synchronization algorithm is used for

simulating the WLAN environment to provide proper security. Deterministic transfer, synchronized clock, efficiency and membership service are some of the advantages of using time triggered approach. It also has some disadvantages like to interrupt messages, flexibility and synchronized clock.

**Event Triggered Approach**

The transmission of messages in event-triggered communication systems is initiated by the occurrence of events. A new link state update is generated based on a specified unreserved bandwidth variation on a given link. Each node uses its local information to determine when making a transmission. Interrupt messages and flexibility are the merits of event triggered approach and deterministic transfer, delay and missing features are some of the demerits of event triggered approach.

The literature study on time triggered and event triggered approaches are analysed in detail in this section.

**Frank Bohdanowicz (2010),** developed Routing with Metric-based Topology Investigation (RMTI) protocol that uses event-triggered updates. To compare the convergence time of routing protocols, a new test environment has been developed. Online data capturing facility is used to collect characteristic data during a test run. Offline statistical analysis tool is used to visualize the results of a test run using plots and graphs. Convergence properties of RMTI are compared with the Routing Information Protocol (RIPv2) under the impeded condition of provoked Counting-to-Infinity (CTIs). The RMTI protocol is implemented on top of the Routing Information Protocol (RIP). Thus, RMTI-protocol is downward-compatible to RIP. As the RMTI extension does not change the message structure but only the processing algorithm, the RMTI technique can also enhance other distance vector routing protocols as well. The RMTI algorithm shows

two important advantages: the possibility to avoid CTI situations and to converge much faster than other distance vector algorithms in case of a topology change. The ability of RMTI to choose whether to optimize fast topology change detection or a traffic reduction (or a mixture of both) makes the test environment adaptable to the specific needs of many different networks.

**Thomas Fuhrer (2009),** In this research work, all the messages are transferred as the priority is given to the mechanism. Time master will allot specific time for sending and receiving the messages. Message A is sent if the system clock reaches 3 and 6 while message c is sent at 5. All these details will be maintained in a timetable and all the processes will be made according to that. The primary goal of using the time triggered is to ensure the successful communication on the bus, to avoid the latency and also to increase the usage of bandwidth efficiently in the network. Time triggered approach helps the communication for TTCAN more conceptual and also it fits for potential applications. Presently it does not cover all the security aspects such as redundancy or data transmission rate of TTCAN and that is given as future directions.

**Robert Leidenfrost and Wilfried Elmenreich (2009)**, use the time triggered approach for a 'priori' known transmission events. These events must be globally coordinated with the use of rounds and stored in a file called Round Description List (RODL) file. In their research work, round corresponds to a cycle of the synchronization algorithm. Many slots will be formed with a round. Every node in a network must have its own RODL file and it statically assigns a communication activity. To every slot in every round, a probabilistic wireless sensor network simulator called JProwler is used. Several experiments were conducted based on all-to-all topology that shows that it is possible to achieve a synchronization precision. Unfortunately, the test bed system suffered from an unexpected delay jitter and an additional communication delay. For this reason, the test

bed results considering highly multi-hop topologies were worse compared to the simulation results with a low delay jitter.

**Christopher Szilagyi (2009),** introduces an approach for authentication in time-triggered applications which prevent both masquerade and replay attacks. In this research work, consideration is given only to time-triggered applications which define a real-time system communications and processing activities are initiated at predetermined points in time from an a priori designated clock tick. This method is developed as an approach to authenticate time-triggered communications by validating truncated MACs across multiple packets. This approach enables per-message authentication of reactive control messages and delayed authentication of state changes at a slight increase in the probability of induced failures. This approach also enables a tradeoff among per-packet authentication cost, application level latency, tolerance to invalid MACs to provide flexibility for system designers.

**Ahmed Helmy (2000)**, in this research work presents a new methodology for developing a systematic and automatic test generation algorithms for multipoint protocols. These algorithms attempt to synthesize network topologies and sequences of events that stress the protocol's correctness or performance. One goal of this work is to circumvent the state space explosion problem utilizing knowledge of network and fault modeling, and multipoint protocols. He has Introduced the concept of transition classification and completion to distinguish between transient and stable states and identified two types of transitions; externally triggered (ET) and internally triggered (IT) transitions. The former is stimulated by events external to the system, whereas the latter is stimulated by events internal to the system. Two algorithms for test generation are done namely, the fault-independent test generation (FITG) and the fault-oriented test generation (FOTG). FOTG is a better fit for robustness studies since it targets faults directly. The complexity for

FOTG was quite manageable for the case study. Corrections to errors captured in the study were proposed with the aid of the method and integrated into the latest PIM-DM specification.

**Venugopalan Ramasubramanian[2002]**, introduces Sharp Hybrid Adaptive Routing Protocol (SHARP), which automatically finds the balance point between proactive and reactive routing by adjusting the degree to which route information is propagated proactively versus the degree to which it needs to be discovered reactively. SHARP enables each node to use a different application-specific performance metric to control the adaptation of the routing layer. This model provides an accurate estimate of the routing overhead of the proactive component and an approximate analysis of the overhead of the reactive routing component. He has analyzed the probability distribution of link-failure events and derive expressions to compute the following: the average frequency of route-failures in AODV and the average frequency of event-triggered updates in SPR (SHARP Proactive Routing protocol). A Node running SPR, generates an event-triggered updates upon the failure of its downstream links. A SHARP node running SPR may lose a downstream link for two reasons, namely, the failure of the downstream link due to mobility, and reversal of the downstream link due to an event-triggered update at the downstream node. It is obvious that there is no combined time and event triggered robust system with computational intelligence techniques for wireless network security.

Table.2.7. presents all the techniques discussed above.

## Table.2.7 State of the Art – Decoys

| Year | Author | Method | Parameters used | Results/ Inferences |
|---|---|---|---|---|
| 2010 | Frank Bohdanowicz | Routing with Metric-based Topology Investigation | convergence time,<br>diameter of network topology | possibility to avoid CTI situations<br>to converge much faster than other distance vector algorithms |
| 2010 | Liqi Shi,<br>et.,al | time division multiple access | energy consumption<br>frame length | does not impose a limit on the frame length |
| 2009 | Robert Leidenfrost | Reachback Firey Algorithm | time to sync, 50th- percentile, 90th- percentile<br>Maximum deviation, Standard deviation | collision-free communication<br>reduction of power consumption |
| 2009 | Christopher Szilagyi | Time Division Multiple Access | successful attack rate, history buffer size, authentication bits per packet | approach enables per-message authentication of reactive control messages<br>delayed authentication |
| 2008 | Christian Seifert, et. al | Divide and Conquer | Buffer Size, Bandwidth, Server Response Time | Improvement Appro., 72% |
| 2008 | S. Almotairi, et.,al | Principal Component Analysis | Total number of basic flows<br>Total number of open<br>TCP ports targeted<br>Total number of distinct open TCP ports targeted<br>Total number of closed TCP ports targeted<br>Total number of distinct closed TCP ports targeted | very powerful tool in detecting<br>the structure of attackers'<br>activities |
| 2007 | Andre Gregio, et., al | Data Mining | False Positive, False Negative, Correctness, Effectiveness | Best and Interesting |
| 2000 | Ahmed Helmy | Fault-independent test generation (FITG) and the fault-oriented test generation (FOTG). | packet loss<br>machine crashes | FOTG is a better fit for robustness studies since it targets faults directly |
| 2002 | Venugopalan Ramasubramanian | Sharp Hybrid Adaptive Routing Protocol | Total packet overhead<br>routing protocol overhead<br>mobility for multiple destinations<br>zone radius for multiple destinations | Efficient mechanisms for dynamically<br>manipulating the zone size performs<br>Fine-grained adaptation with low overhead. |

## 2.4. Observation due to literature

It is observed that, though the detection technique of unknown attacks is efficient it has some limitations. New and efficient cyber attack detection technique is essential in the cyber world. The moving target defense mechanisms are analysed and four methods are considered for this research work as suggested in the Co-Chair's report of National Cyber Leap Year Summit 2009. The four moving target defense mechanisms are

(i). Smart Motion Adaptation/Management - Game Theory

(ii). Robust Cryptographic Authentication - Mouse Dynamics

(iii). Data Chunking and De-centralization

(iv). Decoys

Smart Motion Adaptation/Management is another Moving Target Defense Mechanism suggested as a defense mechanism to handle cyber attacks. Game theory is one of the methods of this mechanism. As a result of literature survey it is found, secure hash based puzzle in the standard model is still an open problem.

The Third moving Target Defense Mechanism is Robust Cryptographic Authentication. Biometric authentication is refered as a category under this method. In the literature study, it is clearly known that various distance measurement techniques are used to calculate the similarity of the mouse operations of user which is already available in the database. Though there is a requirement of efficient similarity measure, an efficient anytime algorithm to increase the accuracy in detecting the unknown cyber attacks is a must.

Data Chunking and Decentralization is the first moving target defense mechanism, which is used for storing the data in a decentralized manner. So far, Mark.W.Storer has used data chunking for secured storage but used only the traditional way of storing the chunked files into the database. The traditional way of storing is more vulnerable to the

hackers, so still there is a need for efficient method for secured storage. As a result of literature survey it is necessary to develop a Improved Data Chunking method.

Decoys, is a next moving target defense mechanism which confuses the attacker by placing the fake target. Time triggered and Event triggered approaches are analysed in detail and observed that both the approaches are efficiently protecting the data or information. Integration of both these approaches will increase the accuracy in detecting the unknown cyber attacks.

Robust security mechanism based on Moving Target Defense Mechanisms is still a challenging, unexplored research challenge.

## 2.5. Chapter Summary

Cyber attacks are vulnerable due to huge usage of internets. various attack handling mechanisms are discussed in the literature. The traditional methods use traffic monitoring methods along with dimensionality reduction techniques to handle some of them used based on their signatures. However, the present attacks need better mechanisms to handle the same. Moving Target Defense Mechanism is a one of the game changing approaches. Currently discussed to handle cyber attacks. Four such mechanisms are taken for further study to improve the accuracy of detection of cyber attacks. The proposed methodology and the research design are discussed in the next chapter.