Optimizing Network Security Considerations with Transition to IPv6 in University of Baghdad, A Prototype

[1]Eman H. Khudhair, [2]Imad J. Mohammed
[1,2]University of Baghdad, College of Science, Dep. Of computer science Baghdad, Iraq
Emails:[1]emanhatem32@yahoo.com, [2]Dr.imadjm@scbaghdad.edu.iq

***Abstract*—It is believed that Organizations around the world should be prepared for the transition to IPv6 and make sure they have the "know how" to be able to succeed in choosing the right migration to start time. These papers focus on thetransition to IPv6 mechanisms.Also, this paper proposes and tests a deployment of IPv6 prototype within the intranet of the University of Baghdad (BUniv) using virtualization software. Also, it deals with security issues, improvements and extensions of IPv6 network using firewalls, Virtual Private Network (VPN), Access list (ACLs). Finally, the performance of the obtainable intrusion detection model is assessed and compared with three approaches.**

***Keywords* —IPv4, IPv6, security aspect, transition mechanisms**

I. INTRODUCTION

THE main InternetProtocol standard is IPv4, which periods back to the 1970s. Conversely, the exponential growing of the Internet gets new stresses that IPv4 cannot achieve in a suitable approach [1]. Some of this problem is the following: a shortage of address space, the speedy expansion of routing tables, essential for a sample configuration, request aimed at a real-time data transmission and then improved necessities considering security. To remove some of the stated limitations a new version of Internet protocol (IPv6) was established in the 1990s [2]. Through the next insufficient years, the original IPv6 protocol must switch an olds IPv4 protocol. Internet Protocol Next Generations (IPngs) or IPv6 distributes a supple besides flexible architecture mounted to vanquish the limits of IPv4. It offers a flexible design upon which network applications as well as services can deploy [2]. Furthermore to meeting the anticipated future request for globally unique IP addresses, IPv6 provides the greater address space for global reachability and scalability, Furthermore, IPv6 moreover affords strong QoS supports with theassistance of Flow-Label and Traffics-Class in the headers of the packets. IPv6 have an easy packets header which supports in quicker convergences of routing packages. The employment of IPsec had been made binding in the formula of extensions-header [3][4]. IPsec actualities inherent components of IPv6 achieve end-to-end securities and offers for privacy, integrity, and verification with thesupport of Encapsulating a Security Protocols and Authentications Headers. Hence, during next years, both IPv6 and IPv4 will coexist. Since security, particularly difficult is the transitions time through which every IPv6 and IPv4 coexists. Throughout transition time, security networks can affect via security issues exact for IPv6 and IPv4 networks. Farther, altered transition mechanism get different, formerly unknowns, security problems can possibly offer novel potentials of interruption and misuse of system linked to the network. Subsequently, the transitions time will not be shorts,

security threats payable to transition mechanisms must be extremely occupied into considerations. Usually, IPv6 is unaffected to many security dangers than the IPv4, nonetheless, there are many threats beside IPv4 network that strength similarly affects an IPv6 network [4][5][6].

This paper is organized as: in Sections II background information is provided. Related works are discussed in Sections III. Also, the security topic due to transition mechanisms is presented in Section IV. The proposed prototype performance evaluation and security validation, the Simulated scenario are discussed in Section V. Section VI summarizes the results of validation. And in section VII proposed IDS with K-mean clustering and the dataset used also the performance of the obtainable intrusion detection model is assessed and compared with three approaches. Section VIII concludes this paper.

II. BACKGROUND

Firewall is a system designed to avoid unauthorized access from or to a private network, can be applied in both software and hardware, or a blend of both. The hardware firewall is a device that can connect at the point where the network links to the Internet. Also, the firewall has to be talented to respond to any request pending either through IPv6 or IPv4. It has to be designed to process IPv6 packets with the related thoroughness of IPv4 packets. Consequently, need to configure rules to allow traffic to permit over the firewall [7].

ACLs are lists of instructions applying to a router's interface to express the router what types of packets to accept and what kinds to deny. ACLs used to limit traffic and increase the performance of the network, basic level of security for network access, traffic sorts forwarded or blocked controller access to areas and deny or permit host access to the network segment.

A *Virtual Private Network*(VPN) is a kind of a connection that links remote users to their central office by the internet. VPN are extremely encrypted and secure connections.

An Intrusion is a method of including confidentiality, veracity, and availability scalability of network resources. The intrusion detection in the environment of IPv6 or IPv4 is an important security technology laterally with a firewall in

system security, which can be used for actual detection and monitoring of the organization in the complete process of system invasion [8].

K-means-clustering the simple step is to determine the number of clusters (K) and adopt the centroid of this cluster, take random objects as the primary centroids or the first (K) object serve as the centroid. Then prepare the steps below till convergence. Iterate until stable; a. Determine the centroid organize b. Regulate the distance of the every object to the centroid c. Assembly the object founded on lowest distance (discovery the closest centroid) [9].

Expectation-Maximization (EM) cluster is an irregular of K-Means clustering and is mostly use for density estimate of data opinions in an unsupervised cluster. In IDS firstly, this algorithm learns the framework and recognizes the encroached data. It absorbs both the means and the covariance of the typical distributions [10].

In density-based (DB) cluster, the cluster isdefinite as areas of advanced density than the rest of the data-sets. Matters in theses spare areas are obligatory to distinct clusters are typically considered to stand noise plus boundary point.In difference to many newer approaches, it features a well-defined cluster model so-called "density reachability". Comparable to linkage based clustering; it is based on relating points within certain distance thresholds . The cluster contains of all density-connected substances (which can form a cluster of an arbitrary shape, in contrast to many other methods) and above all objects that are inside these objects' scope [11].

III. RELATED WORK

Authors in [12] summarized and compared the IPv6 transitions methods like Dual-Stack (DSTM), Tunneling issues, the IPv6 transitions situations, IPv6 transitions security problem, highlights IPv4 and IPv6 threat through automatics tunneling and construction tunneling consideration. They suggested a provisional threat models for an automatic tunneling, in addition, a structure tunneling that might be accompanied by the University of Mysore (UoM), to evaluated manually configured tunnelings and automatic tunneling risk problems. Moreover, they test vary tunneling mechanisms like IPv6 over IPv4, Tunnel broker also described a lot of identified dangers against IPv6 besides it compared and difference how these threated might have an effect on an IPv6 network.

Analyses and comparisons of IPv4 and IPv6 threats using two phases are discussed in [13], The First part considerations on attacks with IPv6 and IPv4 similarities. And the second part is emphases on the attacks with new thoughts in IPv6. Yet IPv6 offers better security, the protocols moreover raises new security tasks. Intended for an enhanced protection in IPv6 network also mentioned implementing security device for packet filtering (firewall) and IDS. Nonetheless, security of IPv6 protocols and IPv6 network still is better, nonetheless, this point would not be a difficulty to its receipt, practice and more improvement.

In [14] Pointing of the issues for asmooth transition from IPv4 to IPv6 and interoperability in technological coexistence time about campus networks. The OPNET and GNS3 simulator combined with the position of faintness of IPv6 technology implemented the simulations to create a network of IPv6 and IPv4 to attain the knowledge research such as topology scheme, network testing, and configuration. Network performance strategy and assessment of IPv6 campus network under the low-cost conditions.

IV. SECURITY ISSUES DUE TO TRANSITION MECHANISMS

The transition mechanisms to IPv6 present new, previously unidentified security dangers. So, it is very significant for networks engineers and managers to recognize safety insinuations of transition mechanism so as to apply correct security machines, as IDS and firewalls.

1)Dual Stack: A plausible approach to presenting IPv6 is the dual stack approach, hosts and routers run both IP protocol in parallel. The main security issue for the dual-stack method is simply there are two IP protocols that may be attacked, and hence must be hardened, checked, possibly patched etc. [15]. On dual-stack requests must be beset by IPv6 and IPv4 attacks. Consequently, firewall and IDS on hosts must support both IPv6 and IPv4 protocols; also definitely necessity proper filtering detections guidelines for two protocols.

2) Tunneling mechanism: likewise bring novel risk and misuses potentials. Tunneling can enable an interloper to avoid access filtering checks. Singular care should be salaried to automatics tunneling mechanisms. If tunneling approaches are in usage, a receiving node should permit decapsulation of packages that can be obtained from anyplace. And can be a thoughtful security problematic. The 6to4 mechanisms usages automatics IPv6-over-IPv4 tunneling aimed at connecting IPv6 networks. The 6to4 router accepts and decapsulates IPv4 packets from the 6to4 routers that take packages from IPv6 nodes. Addresses in the IPv6 and IPv4 header might be spoofed and can use for Denial of Service (DoS) attack. [16][17][18].

3) Translation mechanisms: needed to permit IPv4-only hosts to connect with IPv6-only hosts. This includes converting IPv6 packets to IPv4 packets, and vice versa. Translation techniques are not predictable to be used widely since they significantly slow down package flow [15]. Further, they do not permit the network to exploit exact capabilities of either protocol. The translation built methods usually might not support the end-to-end security structures that rely on the sources and endpoint addresses (e.g., IPsec); the encryption structures of DNS-SEC are easily broken. Also, the assailant can direct the translations entry some packages deceived the basis address as multicast addresses to procedure reproduce-DoS attacks. Normally, security subjects of translations can be alleviated by examination the validness of the addresses, addition authentications schema and required statically. Nonetheless, this structure will importantly consume the system's assets, besides increases the difficulty of this mechanism. Additionally, the impression on security structures cannot be healthy established currently of these arrangements along with the manuscript.

V. PERFORMANCE EVALUATION AND SECURITY VALIDATION OF THE PROPOSED IPv6

A. Testing environment

Due to space and equipment limitations, a virtual network is generated to simulate the real one using (Graphical NetworkSimulator) GNS3 [19]. Different scenarios designed

run on a Lenovo laptop running Windows 7 Enterprise 64-bit with having a core-i7 processor with 8 GB of RAM based on infrastructure identified by University of Baghdad (BUniv) intranet network.

For experimental purposes, a dual-stack (IPv6 and IPv4) network had been recognized (as shown in Fig. 1). The network contains two routers, four switches, and data center with four servers managed by two administers. All the experiments of security aspect in IPv6 network have been achieved and described in this following subsection.

B. Firewall testing

All firewall configurations (listed below) must be replicated for both IPv4 and IPv6 for the sake of dual stack security.

Firewall Configuration of IPv4

Setup Firewall for IPv4

```
ASA5505 (configr)# interface Vlan1
ASA5505 (configr-if)# nameif inside
ASA 5505 (configr-if)# security --level 100
ASA 5505 (configr-if)# ip address 192.168.1.1 255.255.255.0
ASA 5505 (configr)# interface Vlan 2
ASA 5505 (configr-if )# nameif outside
ASA 5505 (configr-if)# security-- level 0
ASA 5505 (configr-if)# ip address 200.200.200.1 255.255.255.0
ASA 5505 (configr)# interface Ethernet0/0
ASA 5505 (configr- if) # switchport access vlan 12
ASA 5505 (configr )#object network NAT-LAN
ASA 5505 (configr-network-1object )# subnet 192.168.0.0 255.
255.255.0
ASA5505 (configr-network -object )# nat (inside ,outside ) dynamic
interface
```

Firewall Configuration of IPv6

Creating the new rules is just like creating rules for IPv4, and below shows the steps of configuration using IPv6.

Setup Firewall for IPv6

```
ASA 5505 (configr)# interface Vlan1
ASA 5505(configr-if)# nameif inside
ASA 5505(configr-if)# security-level 100
ASA 5505 (configr-if)# ipv6 enable
ASA 5505 (configr-if )# ipv6 address 2001 :5:80/64
ASA 5505(configr)# interface Vlan 2
ASA 5505 (configr-if )# nameif outside
ASA 5505 (configr-if)# security -level 0
ASA 5505 (configr-if)#ipv6 enable
ASA 5505 (configr-if)# ip address 2001:5::70/64
ASA 5505(configr)# interface Ethernet0/0
ASA 5505(configr-if )# switchport access vlan 2
ASA 5505 (configr)# object network NAT- LAN
ASA 5505 (configr-network-object)# subnet 2001:5:00/6 4
ASA 5505 (configr-network-object)# nat (inside ,outside)
dynamic interface
```

C. Access lists (ACLs) testing

The following ACLs commands are used to protect each LAN connected to the data center of intranet from the access of the rest LANS. In another meaning, it prevents the cross reference/access between LANs across the data center.

Setup Access list for IPv4

```
R1(configr)# ip access -list 1
R1(configr)# access-list permit 192.168.5.1 255. 255.255 .0
R1(configr)# access- list deny 192. 168.4.1 255.255 .255.0
R1(configr)# access- list d eny 192.168.3.1 255 .255.255.0
R1(configr)# access- list deny 192.168.2.1 255.255 .25 5.0
```

Apply this ACL to an interface:

```
R1(configr)# interface Fa0/1
R1(configr-if)#ip access-group 1 IN
```

Setup Access list (ACL) for IPv6

```
R1(configr)# ipv6 access- list CISCO
R1(configr-ipv6-acl)# deny tcp2000:20:: 1/64 2000:30::1/64
R1(configr-ipv6-acl)# deny tcp 2000:20::1/64 2000:40::1/64
R1(configr-ipv6-acl)# deny tcp 2000:20::1/64 2000:50::1/64
R1(configr-ipv6-acl)# permit 2000:20::1/64 2003:: 1/64
```

Apply this ACL to aninterface:

```
R1(configr)#interface Fa0/1
R1(configr-if)# ipv6 traffic-filter CISCO IN
```

D. VPN testing

VPN configuration is used to secure site to site connection of Intranet between the main campus BUniv (Al-Jadriya campus) associations with the network branches outside the main campus like Bab Al-Muadham campusas shown in figure 1

VPN Setup

```
R1 (configr)#crypto isakmp enable
R1 (configr)#crypto isakmp policy 10
R1(configr-isakmp)#authentication pre-share
R1 (configr-isakmp)#hash sha
R1(configr-isakmp)#encryption aes 256
R1 (configr-isakmp)#group 5
R1(configr-isakmp)#lifetime 3600
R1(configr)#crypto isakmp key 0 KEYTOOR address ipv6
2001:bd9:7 7:1::1/64
R1 (configr)#crypto isakmp keepalive 10 2 periodic
R1(configr)#crypto ipsec transform-set MYTSETNAME esp-
aes 256 esp-sha- hmac
R1(cfg-crypto-trans)#mode tunnel
R1(configr)#access- list 101 permit ip 2001:bd9:77:1::1/64
20 01:bd9:77:1::2/6 4
R1(configr)#crypto map LEFTY_TO_RIGHTY 10 ipsec-
isakmp.
R1(configr-crypto-map)#set transform- set MYTSETNAME
R1(configr)#crypto isakmp profile 3des
R1(conf-isa-prof)#self-identity address ipv6
R1(conf-isa-prof)#match identity address ipv6
2001 :bd9:77:1::1/64
R1(conf-isa-prof)#keyring default
R1(configr)#intfastEthernet 1/0
R1(configr-if)#crypto map LEFTY_TO_RIGHTY
```

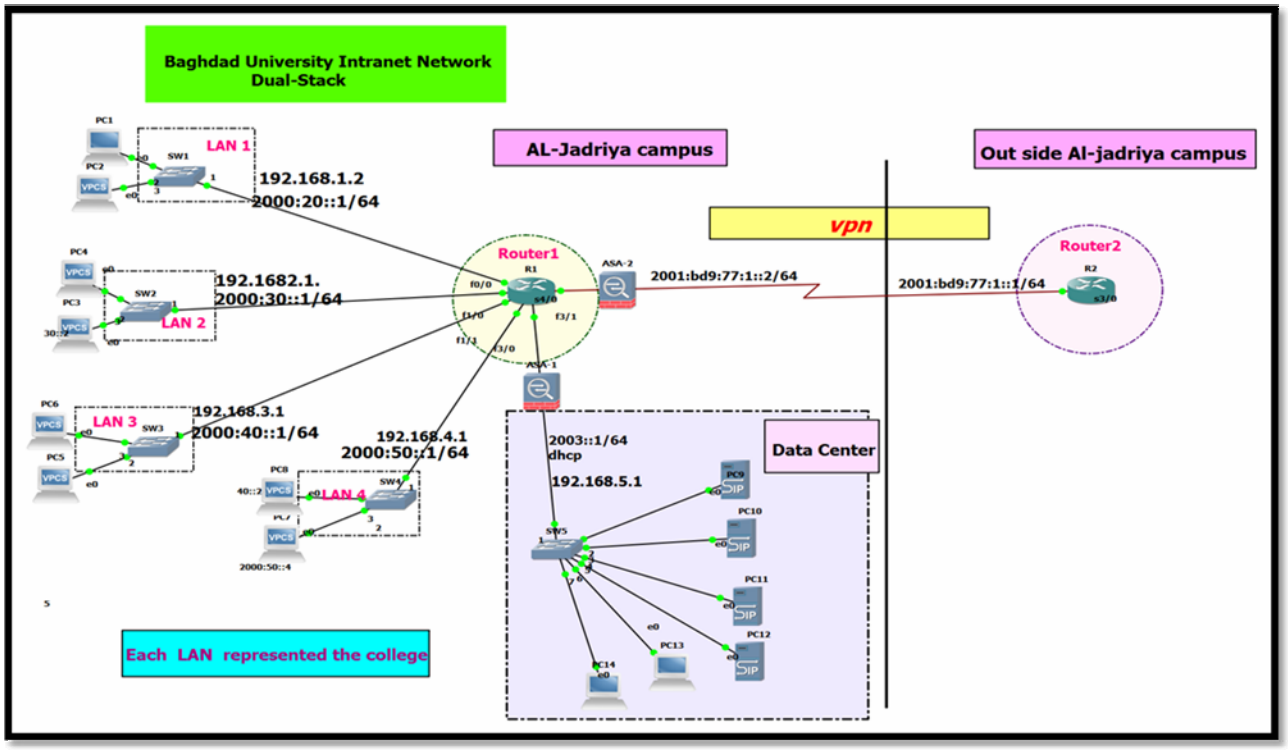

Fig .1: Dual-Stack Network (BUniv)

VI. CONFIGURATION RESULT AND DISCUSSION

This section introduces the configuration validation and the security legal and illegal access. The communication is verified using "ping" command as shown in Fig (2) which depicts the successful or deny aconnection from LAN 1 to the data center or to another LAN respectively. Fig 3 shows the VPN connectivity results using theping command.

Fig. 2: Shows the Result after Setup Access list in LAN1

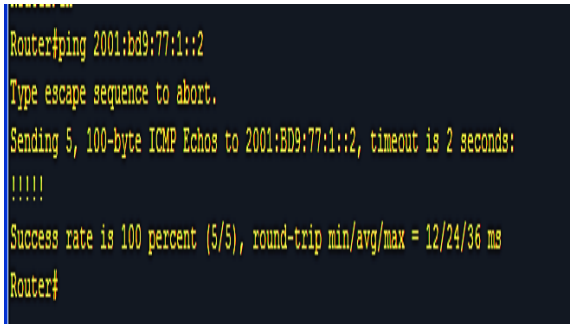

Fig. 3: Show Result when Connect R1 with R2 (via VPN).

VII. INTRUSION DETECTION ALGORITHM BASED ON DATA CLUSTERING USING K-MEAN

In this section, a K-Mean Data Clustering Algorithm designed and implemented to provide the networkIntrusion DetectionSystem (IDS) of the proposed IPv6 network. The next subsections discuss: the used data set, proposed an IDS clustering Algorithm to cluster the network traffic into normal and abnormal objects, the performance metrics, and finally explains the results comparisons to other algorithms.

A. Dataset description (NSL-KDD)

The IPv6 dataset, at the instant, there is no accessible hence so-called labeleddataset for IPv6 network as comparable to the NSL-KDD dataset of IPv4. NSL-KDDdataset was formed to produceto be a platform to test and evaluate the recognition techniques. This datasetwas conceived built on the IPv4 network situation. Towards the greatest of our

knowledge, there is no comparable dataset was produce created on theIPv6network environment. The closest IPv6-dataset accessible is dataset created by CAIDA. Yet, this dataset is just as a raw besides unlabeled which is not appropriate to use as a stage for more investigation in IPv6 IDS realm. Thus NSL-KDD dataset is promoted for our paper experiments. It includes 41features and 5 classes that are considered normal and the rest are abnormal with 4 types of attacks: Dos, R2L, Probe, and U2R[20].
The proposed model uses NSL-KDD benchmark dataset as an evaluationdata. It involves three different datasets: the complete dataset, 20% of the complete dataset for training and KDD full testing dataset. This work uses 20% training dataset that contains 25192 normaland attack instances.

B. Proposed IDS clustering Algorithm

K-MEAN based Clustering Algorithm

Input: N dataset of m object
Output: Desired set of thenormal and abnormal cluster.
Begin

Step1: normalize the dataset in order to scope the feature value to suitable range. The attributes were normalized using theexpression (1).

$$X^{P}_{norm} = \left(\frac{x^{P} - min^{P}}{max^{P} - min^{P}}\right) \quad \text{.....(1)}$$

Where: X^{P} is the value of the p[th] attribute of instance$X$ .max^{P} andmin^{P} correspond, congruently, to maximum and minimum value of the P[th] attribute in the dataset.

Step2: Select initial Cluster mean and aimed at that the formulation of Euclidean distance for variation measure had been used. **C** object is particular as the initial cluster center having the smallest value.

Step3: Assistant each objects to its nearby cluster and compute the optimum value as the sum of distances from the entire objects to their clusters.
Step4: Switch the existing cluster center in every cluster by the item which minimizes the total distance to other items in the clusters.

Step5: Over associate, every object to the nearby centroid and calculate the new value as in **step3.**
If the new value is similar as previous one then break the algorithms else repeat **step4.**

End

C. Adopted Performance metrics

The following are measurements used for performance evaluation applied on NSL-KDD dataset.

True positives (TP): number of attacks represents data objects that are correctly classified as an intrusion. True negatives (TN): numbers of normal denotes data objects that are correctly classified as a normal. False positives (FP): numbers of normal represents data objects that are incorrectly classified as attacks. False negatives (FN): numbers of data objects that are incorrectly classified as an intrusion.
To evaluate the efficiency of the proposed K-mean data clustering algorithms using NSL-KDD datasets, the results are described using two main factors called Detection Rate (DR) and Accuracy (ACC) [22].

Detection Rate (DR): The DR is definite as the ratios of the numbers of properly detected attacks relative to total numbers of attacks. As shown in equation (2)

Detection Rate (DR) =TP/ (TP+FN) ……. (2)

Accuracy (ACC): accuracy evaluated how the IDS works besides measuring the ratioof number of truly classified connections to a total number of connections (i.e. the proportion of true results in the population) as shown in equation(3).

Accuracy= (TP+TN)/ (TP+TN+FP+FN) ……. (3)

D. Result and discussion of IDS

This segment discusses and studies the results of the NSL-KDD dataset using proposed K-means clustering algorithm. The performance of the K-Means algorithm is evaluated using Euclidean distance measure.

The proposed algorithm is being run to get the desired cluster and later choose the cluster to label them as normal or intrusions.

Intrusion detection dataset has been clustered in two modes: normal data and anomaly data. Results of the proposed clustering algorithms have been compared and time complexity to build the cluster model is evaluated

Detection rate and accuracy factors are calculated for the proposed K-mean clustering algorithms as shown in Table(1) which offers the ratio of accuracy, detection rate and required time to form the cluster.

The results show that the proposed intrusion detection model satisfied the ACC and DRup to 90.27% and 91.23% respectively and reduced the required time to 1.44 to form the cluster.

Table 1: Experiment Results of Proposed Algorithm

Parameters	The Proposed Algorithm
Accuracy (ACC)	90.27
Time (Sec.)	1.44
DetectionRate(DR)	91.23

E. Comparative analyses and results

WEKA [22] is used as a test platform in our experiments for the sake of performance evaluation and comparisons

conducted using 20% (or (25192 objects) of NSL-KDD dataset.

Weka permits the input data set to be in numerous file formats like CSV (comma separated values: *.csv), Binary Serialized Instances (*.bsi) etc. However, the most preferred and the most convenient input file format is the attribute relation file format (arff). So the first step in Weka always is taking an input file and making sure that it is in ARFF.Three of the symbolic data attributes (protocol_ type, flag , and service) are removed as non-contributing. Clustering is performed over (25192 x39) metrics.

In terms of initialization, maximum iterations set to 100 and number of clusters is set to 2. Our proposed algorithm compared to three standard algorithms: K-Means, DBC, and EM implemented on the same NSL-KDD dataset.

Fig.(4)-(6) demonstrate the detection rate (DR), Accuracy (ACC) and the required time to build the clusters of the four algorithms.

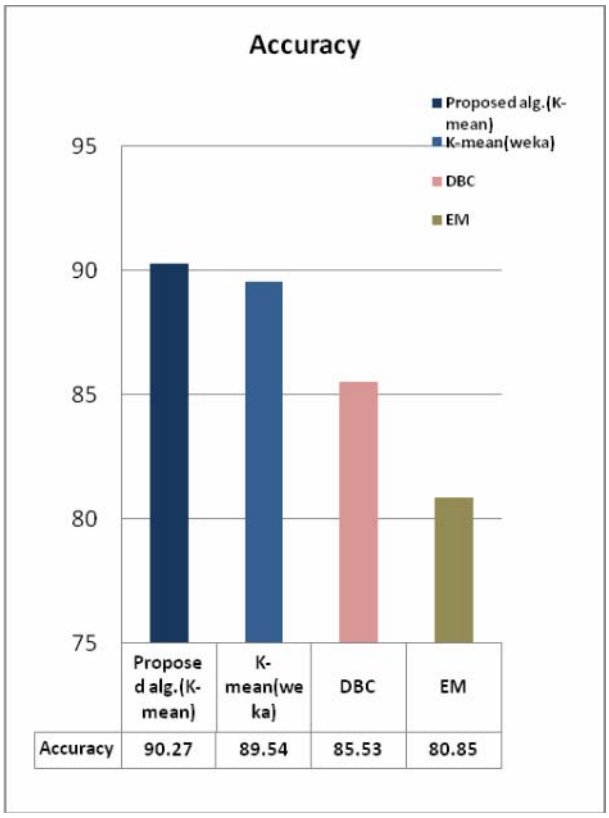

Fig.4: Result of Accuracy

As observed from the fig.4, when comparing (ACC) for proposed K-mean algorithms with supplementary three algorithms k-mean standard, EM, and DBC, the proposed algorithm illustrations better results than other algorithms.

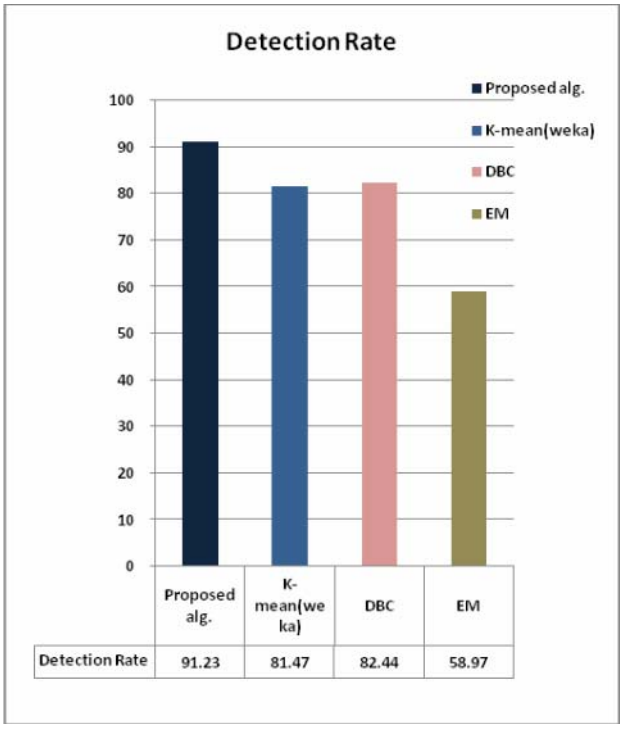

Fig.5: Result of Detection Rate

In fig 5, when comparing (DR) for proposed K-mean algorithms with k-mean standard, EM and DBC, the proposed algorithm gives higher results 91.23% as compared with alternative algorithms.

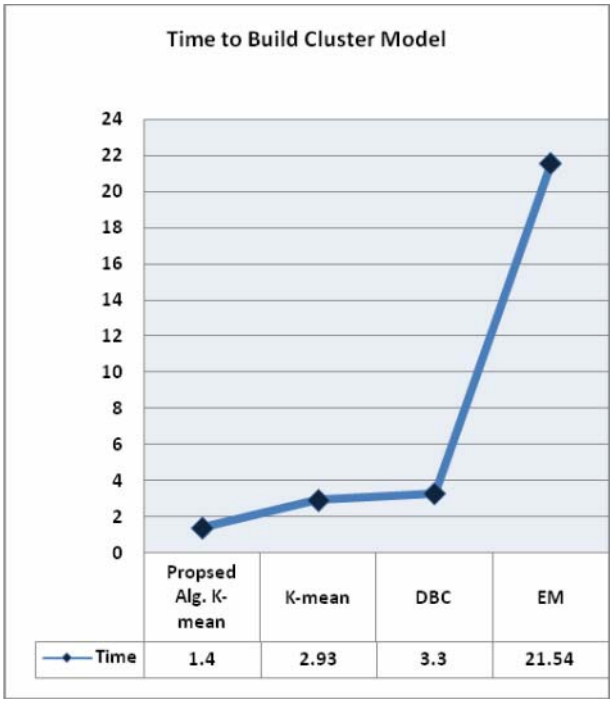

Fig.6: Time Taken to Build Cluster Model

The required time to build the clusters model seen in fig 6 Shows that the required time to build the clusters for proposed K-mean is lower as compared to other approaches

The obtainable ID model provides a good accuracy up to 90.27% that outperforms the EM and DBC and increases the DR to 91.23% furthermore the time taken in building the clusters is lower as compared to other algorithms (1.44 second). The improvement satisfied due to the features of the proposed algorithms is having numerous benefits over the present algorithm which mostly overwhelms the drawbacks of dependence on initial centroids, dependence on the number of cluster and immaterial clusters. K-means it minimalize a sum of pairwise variations using Euclidean distance.

F. CONCLUSION

Nexta certain periods of existence the IPv6 protocol will exchange the IPv4 protocols. IPv6 affords many enhancements in association to IPv4. Certain weaknesses and misuses potentials identified in IPv4 networks persevere, besides new transitions associated and IPv6 exact security subjects appeared. Successful resolving of security subjects will surely contributes to broader receipt of IPv6protocols. Because of the being of many security matters in IPv6 networks, it is essential to assume totally probable stages for realizing the maximum potential security levels. Aimed at an enhanced protection in the network, it is suggested to implemented security devices for packets filtering (firewalls) and intrusions detections (IDS) and also implements VPN and ACLs.

REFERENCES

[1] Durand, A., "Deploying IPv6"., IEEE Internet Computing, Vol.5, No.1, pp.79-81, 2003.

[2] RFC 2460. "Internet Protocol Version 6 (IPv6) Specification"

[3] Caicedo, C. E., Joshi, J.B. and Tuladhar, S.R.,. "IPv6 Security Challenges". IEEE Computer , Vol.42 ,No. 2, pp.36-42 , 2009.

[4] Zagar D, Vidakovic S. "IPv6 Security: improvements and implementation aspects". , In: Proceedings of the Eighth International Conference on Telecommunications, Contel . Zagreb, 2005

[5] RFC 4301. "Security Architecture for the Internet Protocol".

[6] RFC 4303. "IP Encapsulating Security Payload (ESP)".

[7] Lai, Y., Jiang, G., Li, J. and Yang, Z.,"Design and implementation of distributed firewall system for IPv6". In Communication Softwareand Networks , 2009,.International Conference on IEEE ,pp. 428-432, 2009.

[8] Denning ,D. E., "An intrusion -detection model,", IEEE Transactions on Software EngineeringVol.13 ,No.2, pp. 222-232 , 1987 .

[9] Velmurugan T., and Santhanam T., "Performance Evaluation of K-Means and Fuzzy C- Means Clustering Algorithms for Statistical Distributions of Input Data Points," European Journal of Scientific Research , Vol. 46, No. 3, pp. 320-33 0. 2010.

[10] Dempster ,A. P., Laird, N. M., and Rubin , D. B., " Maximum Likelihood from Incomplete Data via the EM Algorithms," Journal of the Royal Statistical Society. Series B. (Methodological), Vol. 39, No. 1, pp. 1-38, 1977.

[11] Kriegel ,H.P.,Kröger ,P.,Sander ,J., and Zimek, A., "Density- based Clustering ," WIREs Data Mining and Knowledge Discovery Vol. 1, No. 3, pp. 231-240, 2011.

[12] Hanumanthappa , J., and Manjaiah.DH., "IPv6 and IPv4 Threat reviews with Automatic Tunneling and Configuration Tunneling Considerations Transitional Model : A Case Study for University of Mysore Network". (IJCSIS) International Journal of Computer Science and Information Security, Vol. 3, No.1, 2009.

[13] Durdağı, E. and Buldu, A., "IPV4//IPV6 security and threat comparisons ". Procedia-Social and Behavioral Sciences, Vol.2 ,No.2, pp .5285-5291, 2010 .

[14] Zhaoa, L., Yangb, F. and Zhaob, Y.," The Simulation Research of Campus Network Technology Based on IPv6". Journal of Computational Science and Engineering, Vol4, pp.190- 195,2013.

[15] RFC 2893. "Transition Mechanisms for IPv6 Hosts and Routers".

[16] Zagar D., Martinovic G., Rimac -Drlje S. "Security Analyses of IPv4/IPv6 Tunneling Tool". WSEAS Trans Compute;Vol. 5 ,No.1, pp.194–201, 2006

[17] Tatipamula , M., Grossetete, P., & Esaki, H,." IPv6 integration and coexistence strategies for next- generation networks ". IEEE Communications Magazine,Vol. 42, No. 1 ,pp. 88-96, 2004.

[18] RFC 3964. "Security Consideration for 6to4".

[19] Kaplan , G, "Simulating networks," Spectrum , IEEE , Vol.38, No. 1, pp.74-76 , 2001 .

[20] Zulkiflee , M., Haniza, N., Shahrin, S. and Ghani, M.K.A,"A framework of IPv6 network attack dataset construction by using test-bed environment " . International Review on Computers and Software (IRECOS), Vol. 9, No. 8, pp .1434-1441, 2014.

[21] Garg, T. and Khurana, S.S., ." Comparison of classification techniques for intrusion detection dataset using WEKA". In Recent Advances and Innovations in Engineering(ICRAIE) IEEE, pp . 1-5, 2014.

[22] WEKA : Data Mining Machine Learning Software,Machine Learning Group at the University of Waikato.http://www.cs.waikato.ac.nz/ml/weka/