Distributed Denial of Service (DDoS) attack prevention using Fuzzy Logic

Harmeet Kaur[1], Jashanpreet Singh[2]

[1]Research Scholar, Department of CSE, Chandigarh Engineering College, Mohali, India

[2]Assistant Professor, Department of CSE, Chandigarh Engineering College, Mohali, India

Abstract: This paper is concentrated on detecting and analyzing the Distributed Denial of Service (DDOS) attacks in cloud computing climates. This type of attacks is often the source of cloud services disruptions. Our solution is to combine the evidences obtained from Intrusion-Detection-Systems (IDSs) set up in the cloud system. This paper discusses the various DDOS attacks and the defense mechanisms that can be employed to secure the cloud. In proposed work, we developed AODV routing protocol for route discovery within the cloud system. We are implementing two types of environment for detection and preventions from DDOS attack. First one is based on only AODV routing protocol but in next part we implement detection and preventions from the DDOS attack using fuzzy logic with AODV routing protocol. Fuzzy logic is used for the optimization purpose, with the help of fuzzy logic. We can detect exact location of attackers and after that we can prevent from this type of attacker. For implementation of this proposed work we use data acquisition and communication toolboxes within MATLAB software.

Keywords: Cloud Computing, Cloud Security, Distributed Denial of Service (DDOS) Attacks, Intrusion Detection Systems, Optimization Techniques and Fuzzy Logic.

I. INTRODUCTION

Web applications are similar to e-business, internet banking, enterprise coordinated effort and supply chain management suites and presume that at the least 92% of Web applications are helpless against some type of assault. The detection of DDOS attack is very important for management of security in web services. Security has to be take care in web log files to deliver high level data rate in network.

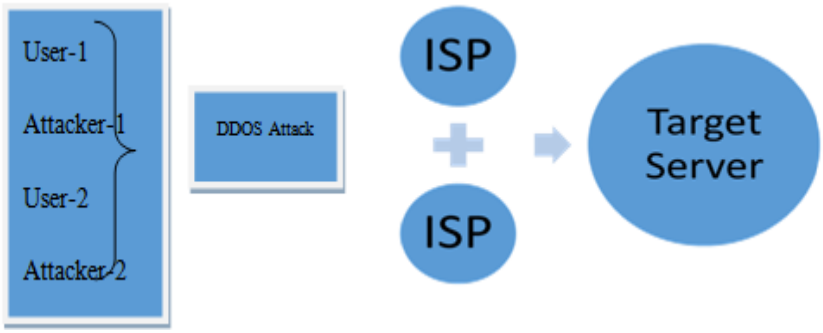

Figure 1. DDOS attack in Cloud

Web has transformed into a fundamental bit of our lives nowadays, so the frameworks which are helpful in extricating the information show on the web is a captivating area of investigation. Content information is the social event of actualities a site page is intended to contain. It may contain content, pictures, sound, video, or organized records, for instance, records and tables. Exploration activities on this subject have drawn intensely on strategies grew in different disciplines for example, Information Retrieval (IR) and Natural Language Processing (NLP). Web structure mining is the procedure of

finding structure data from the web. This can be further isolated into two sorts in view of the sort of structure data utilized.

A Web log file is a record which records data of action when the web server discovers the solicitation from the web client. Web access log is the primary wellspring of crude information which we should exchange to as log record. As log files are at first compensated for debugging purposes.

An intrusion detection system (IDS) inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system.

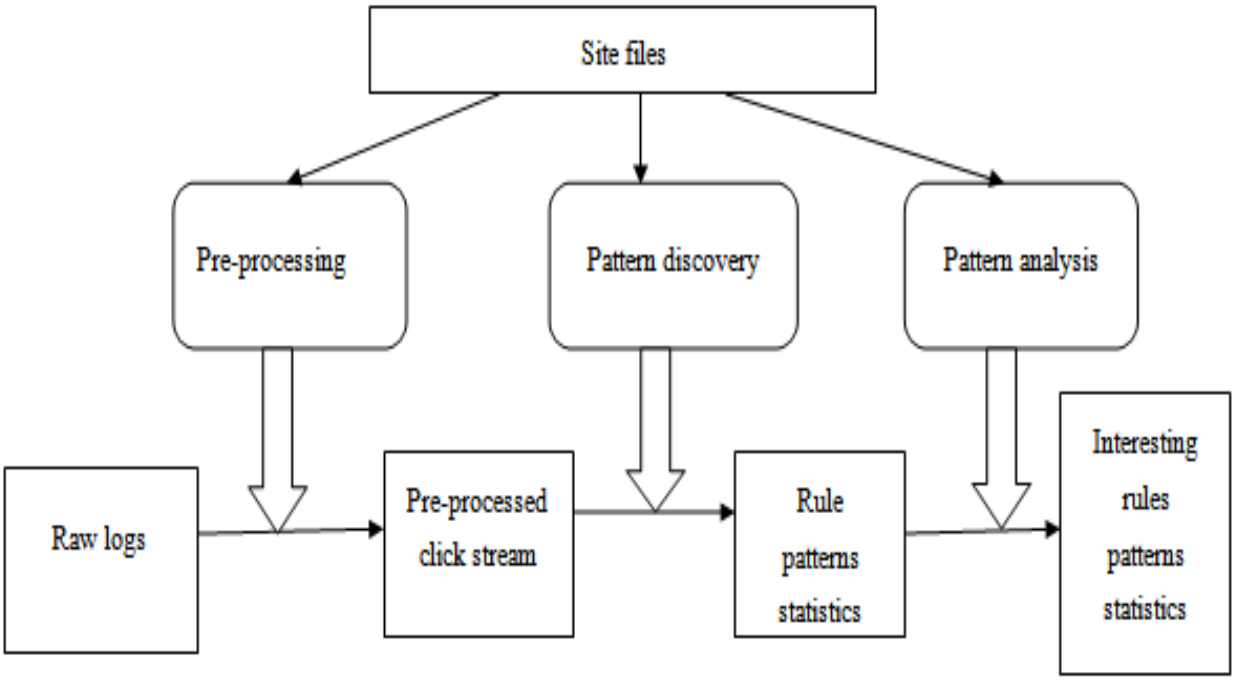

Figure 2. Web log mining process

Dos is the type of attack in which attacker gets the access to denied resources and then made chnges accordingly [6].

There are different ways to launch DoS attacks:

- Abusing the computers legitimate features.
- Targeting the implementations bugs.
- Exploiting the system's misconfigurations.

DoS attacks are classified based on the services that an attacker renders unavailable to legitimate users.

Fuzzy Model is the generalized model of previous classic models. As the output is not limited to only 0 and 1, so the theory of fuzzy logic is introduced. It is also known as diffuse logic. Difference between fuzzy logic and classical model is introduced using membership functions. Consider a finite set [10, 11],

C= {c1, c2, c3….cn}

It is the universal set. Now according to graphical representation, suppose fuzzy sets has only two elements c1 and c2. So the degree of fuzzification can be called as entropy. Therefore, entropy can

be shown as:
E=$\frac{f1}{f2}$; Where f1 and f2 are the distances

II. RELATED WORK

Bridges et.al proposed genetic algorithm and fuzzy based IDS system.Li et.al proposed IDS system based on genetic algorithm. Genetic algorithm worked by using fitness function. Dilpreet kaur et al [27], presented the overview of various atatcks in web log files. RimmyChuchra et al [28] focused on Web agents identifying online attack with itsintroduction. S.Mirdula et al. [29]dealt with the significance of web application and its security is expanding step by step, yet conventional systems neglects to give security to web application. Diallo Abdoulaye Kindy et al. [30] depicted a detailed survey on various aspects of sql injection in web application. This research also deals with vulnerabilities related to SQL injection, innovative attacks and remedies. PallaviAsrodia et al. [31] analyzed that amount of network traffic flowing over their nodes has increased day by day. This paper focused on the concept of packet sniffer, its working principle which used for analyzing network traffic. Sokratis et al. [34] proposed the network Intrusion Detection System.

III. SIMULATION MODEL

In proposed work detection and prevention of dos attack is done using GA and fuzzy logic.

NodesNum = input('Enter the number of Nodes');

TotalPackets = 1000;

rounds = input('Enter the number of Rounds');

SourceNode = inputdlg('Enter the Source Node');

DestinationNode = inputdlg('Enter the Destination Node');

SourceNode = str2double(cell2mat(SourceNode));

DestinationNode = str2double(cell2mat(DestinationNode));

Plot network

Get coverage set for source and destination.

Evaluate metric values

Do optimization

Again, get values for parameters

end

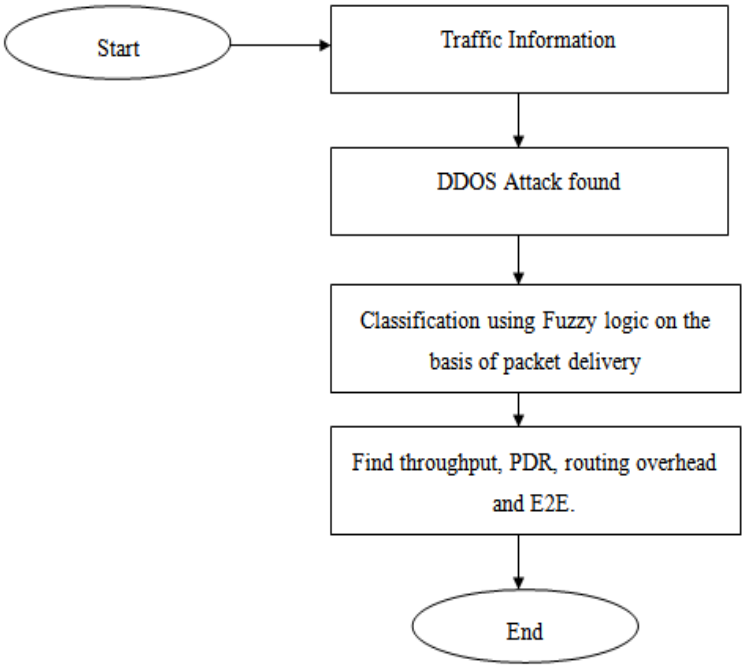

Figure 3. Methodology Flowchart

Simulation parameters:

```
 for u=1:nodes
errornormal(u)=2*rand;
errorattack(u)=20*rand;
energynormal(u)=10*rand;
delaynormal(u)=rand;
delayattack(u)=20*rand;
PDRN(u) = 10*rand;
end
end
```

IV. SIMULATION RESULTS

Throughput for three scenarios like normal network, without optimization and with optimization using fuzzy logic has been seen and it has been concluded that for normal network the obtained value for throughput is 600, without optimization is 200 and with optimization is 230. Similarly, it has been seen that for normal network the obtained value for delay is .4, without optimization is 13 and with optimization is 3 and for normal network the obtained value for PDR is 45, without optimization is 90 and with optimization is 45.

A. With attack

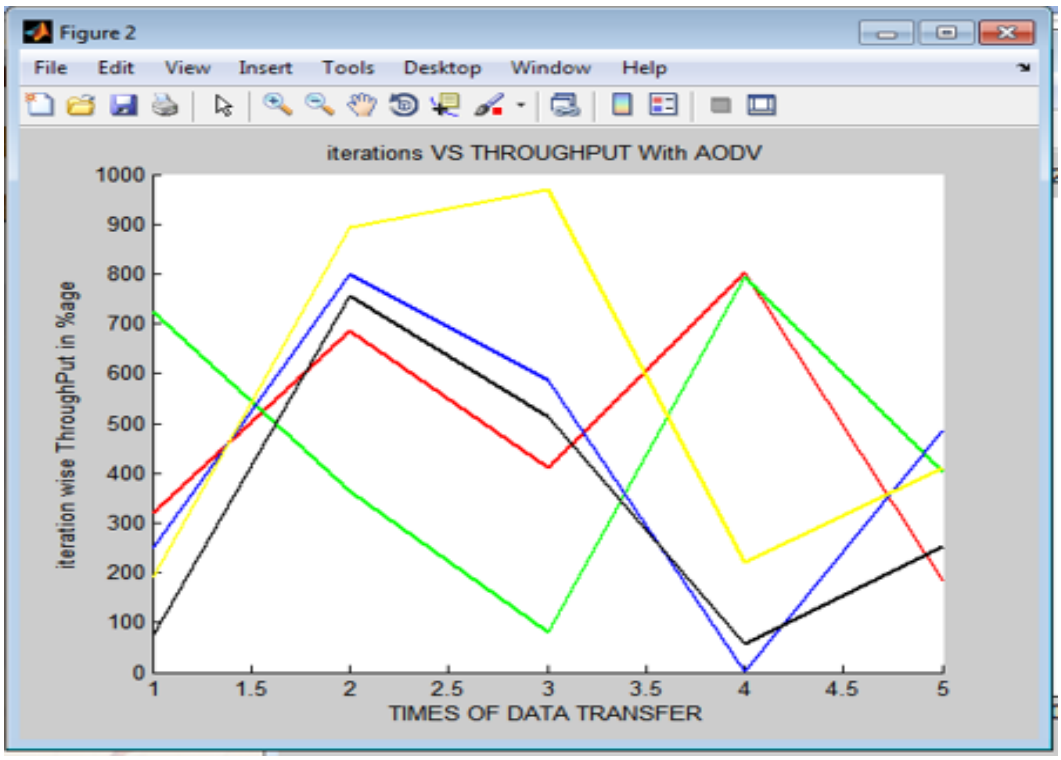

Figure 4. Iteration V/S Throughput

Above figure, shows the graph between iteration V/S throughputs. In this, five iteration has been taken which is shown by blue, green, yellow, black and red colour. For 5 time of data transfer, the five different iteration values of throughput are 190, 200, 450, 430 and 500.

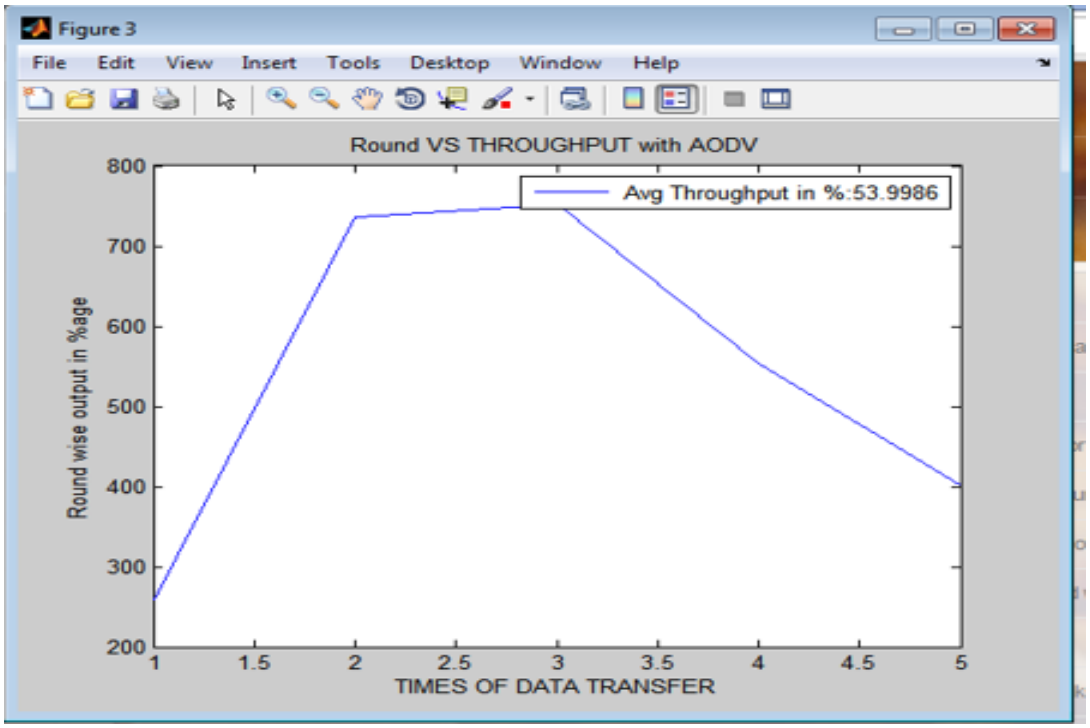

Figure **Error! No text of specified style in document.**. Round V/S Throughput

Above figure, shows the graph between round wise output V/S times of data transfer for throughput for 5 rounds. From graph the average value of throughput for 5 times= 400. Also the average throughput value = 53%.

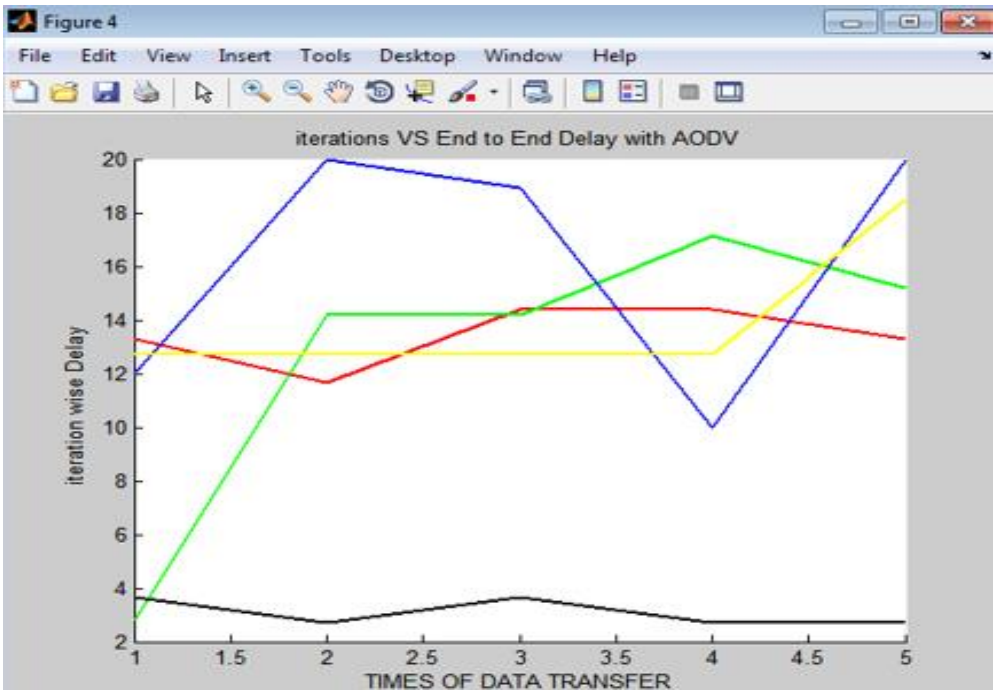

Figure 6. Iteration V/S Delay

Above figure, shows the graph between iteration V/S delay. In these five iterations, has been taken which is shown by blue, green, yellow, black and red colour. For 5 time of data transfer, the five different iteration values of delay are 3.5, 14, 14.5, 18 and 20.

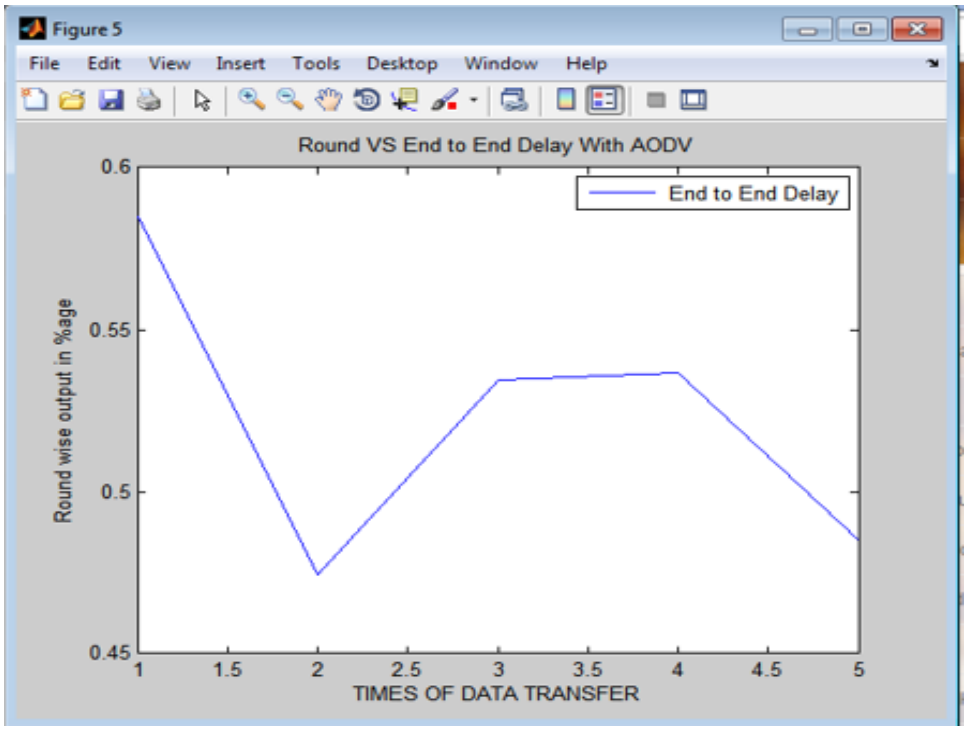

Figure 7. Round versus Delay

Above figure, shows the graph between round wise output V/S times of data transfer for delay for 5 rounds. From graph the average value of delay for 5 times= .5.

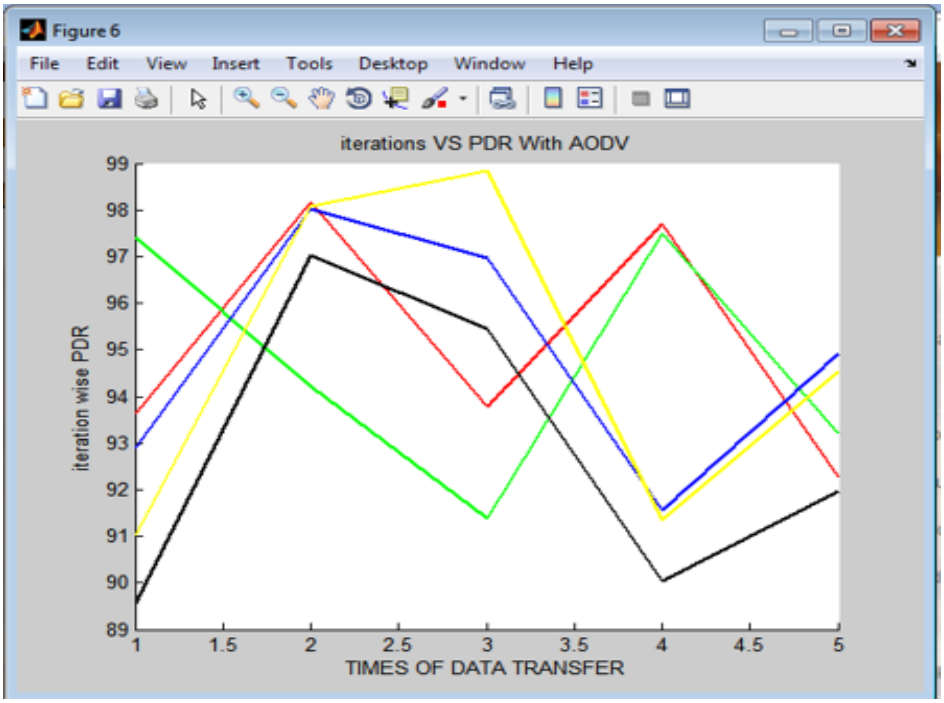

Figure 8. Iteration V/S PDR

Above figure, shows the graph between iteration V/S PDR. In this five iteration has been taken which is shown by blue, green, yellow, black and red colour. For 5 time of data transfer, the five different iteration values of delay are 3.5, 14, 14.5, 18 and 20.

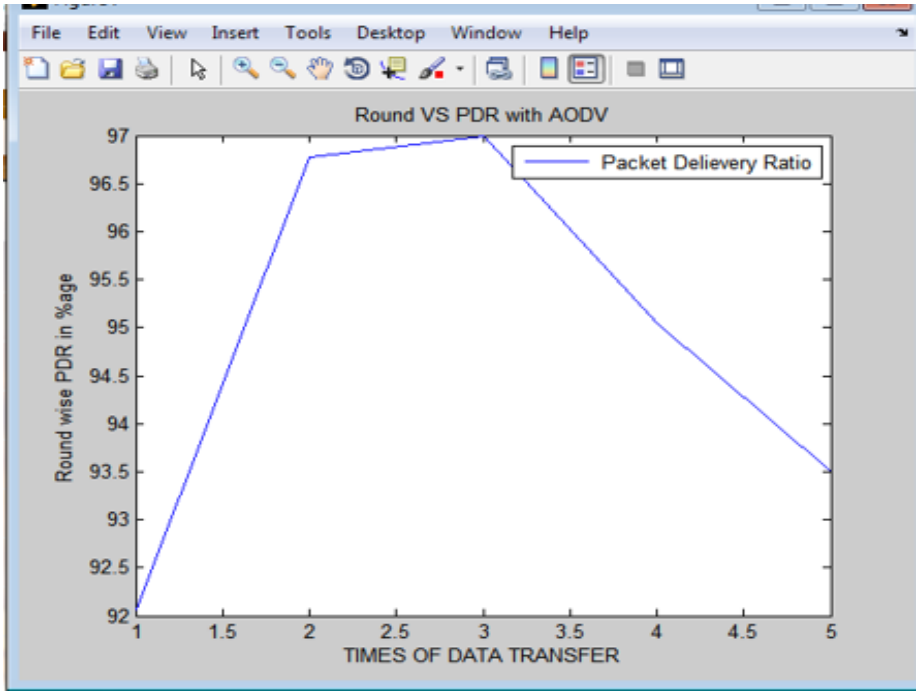

Figure 9. Round versus PDR

Above figure, shows the graph between round wise output V/S times of data transfer for PDR for 5 rounds. From graph the average value of PDR for 5 times= 94. Also the average PDR value = 94%.

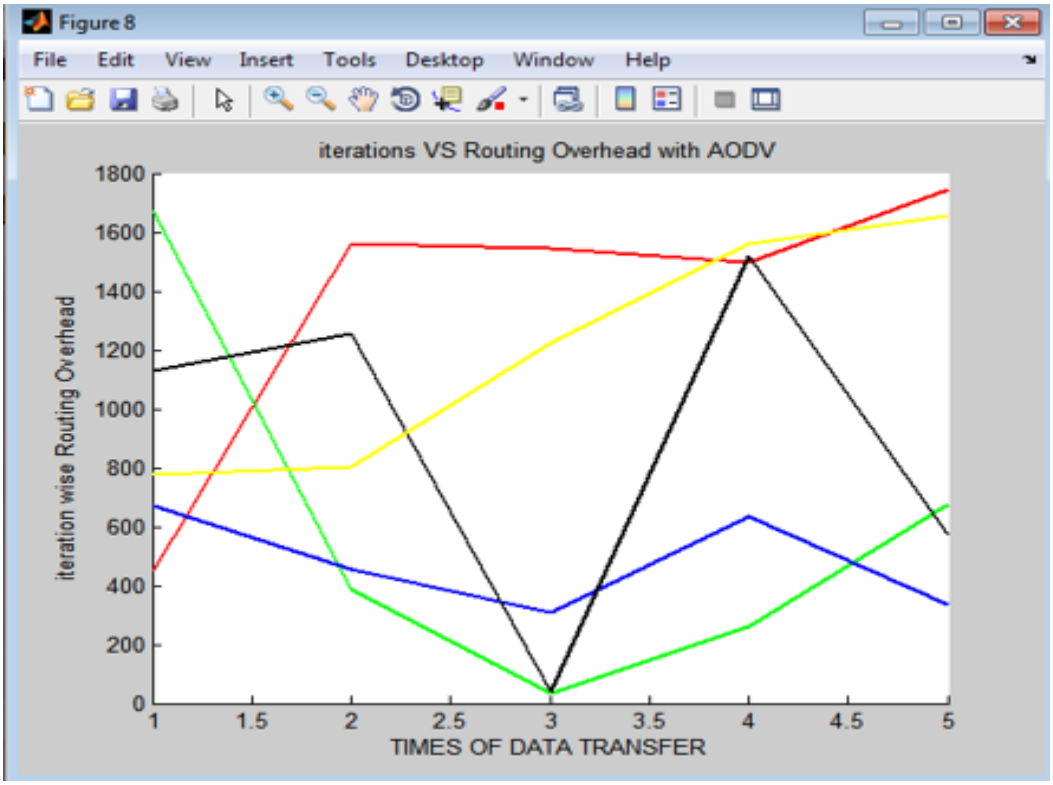

Figure 10. Iteration V/S Routing Overhead

Above figure, shows the graph between iteration V/S Overhead. In this five iteration has been taken which is shown by blue, green, yellow, black and red colour. For 5 time of data transfer, the five different iteration values of routing overhead are 400, 600, 550, 1600 and 1650.

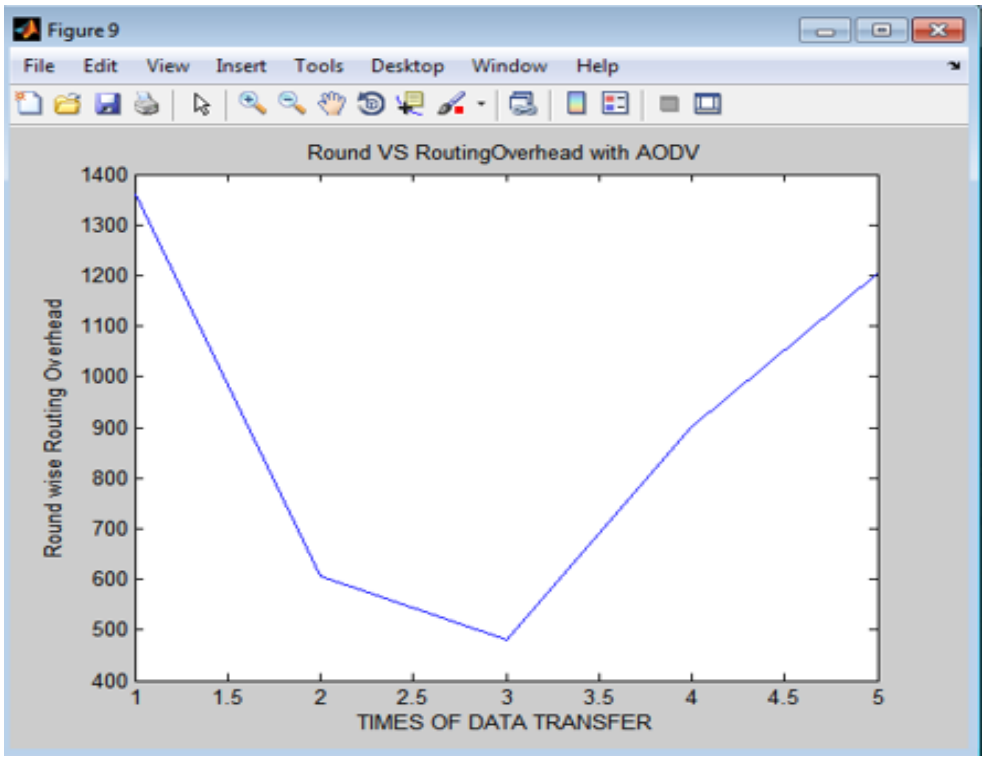

Figure 11. Round versus Routing Overhead

Above figure, shows the graph between round wise output V/S times of data transfer for routing overhead for 5 rounds. From graph the average value of routing overhead for 5 times= 120.

B. With optimization using fuzzy logic

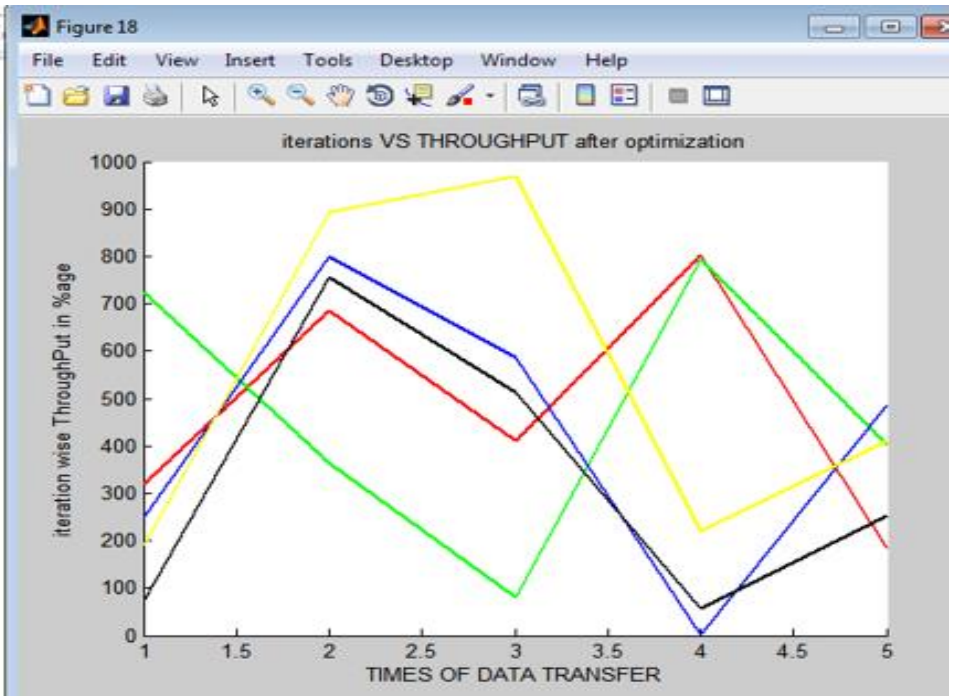

Figure 12. Iteration V/S Throughput after optimization

Above figure, shows the graph between iteration V/S throughput using optimization method. In this five iteration has been taken which is shown by blue, green, yellow, black and red colour. For 5 time of data transfer, the five different iteration values of throughput using optimization are 100, 200, 400, 430 and 500.

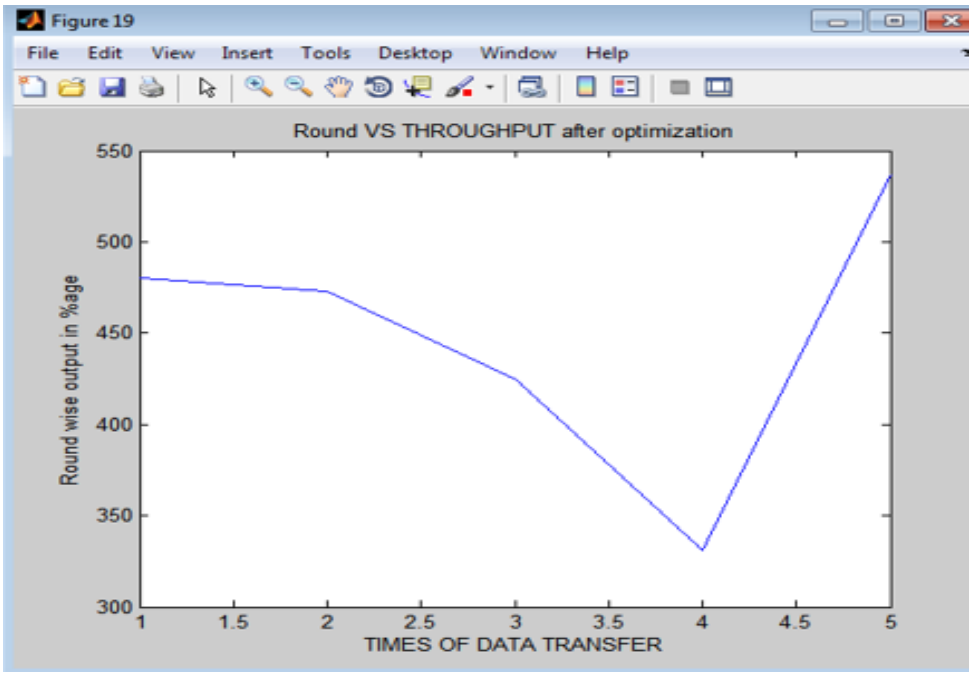

Figure 13. Round versus Throughput using Optimization

Above figure, shows the graph between round wise output V/S times of data transfer for throughput for 5 rounds using optimization method. From graph the average value of throughput using optimization method for 5 times= .540.

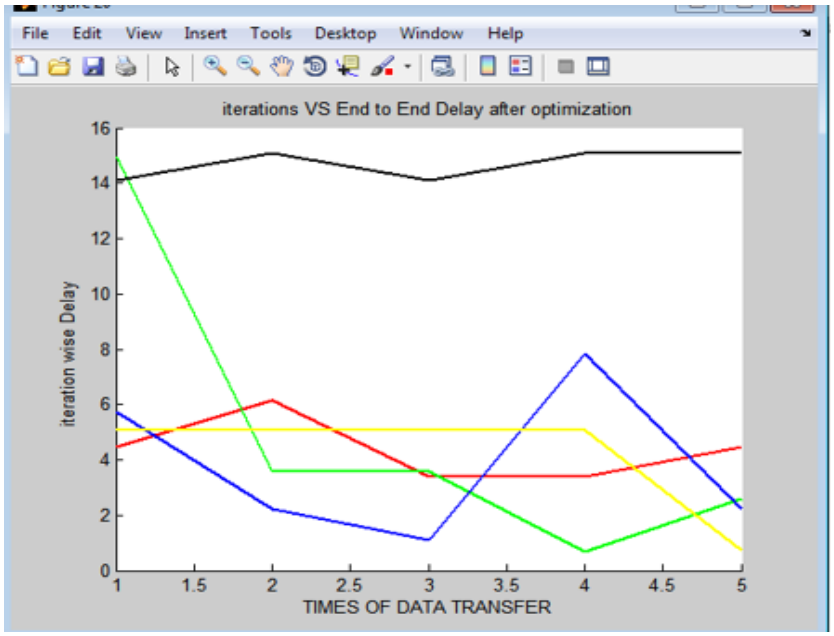

Figure 14. Iteration V/S Delay after optimization

Above figure, shows the graph between iteration V/S delay using optimization method. In these five iterations, has been taken which is shown by blue, green, yellow, black and red colour. For 5 time of data transfer, the five different iteration values of delay using optimization are 1.3, 2.3, 3.1, 4.1 and 14.1

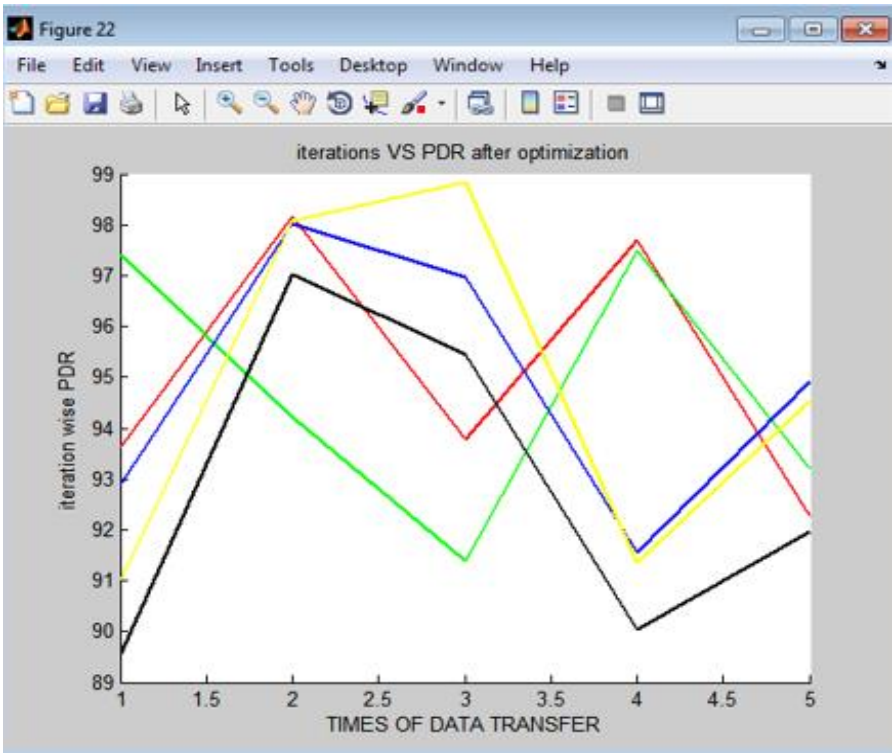

Figure 15. Iteration V/S PDR after optimization

Above figure, shows the graph between iteration V/S PDR using optimization method. In these five iterations, has been taken which is shown by blue, green, yellow, black and red colour. For 5 time of data transfer, the five different iteration values of PDR using optimization are 100, 200, 400, 430 and 500.

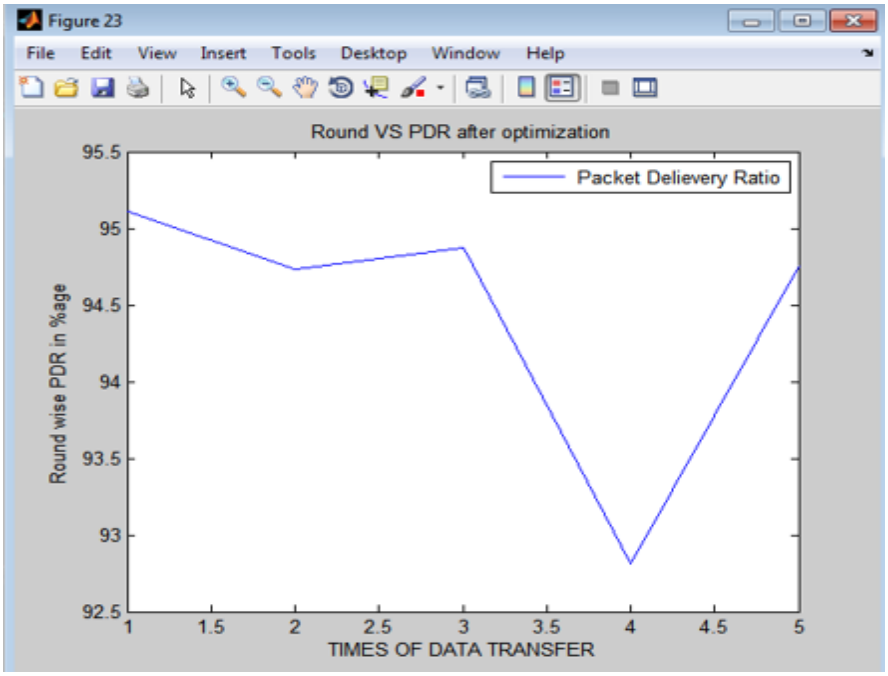

Figure 16. Round versus PDR using Optimization

Above figure, shows the graph between round wise output V/S times of data transfer for PDR for 5 rounds using optimization method. From graph the average value of PDR using optimization method for 5 times= 94.9.

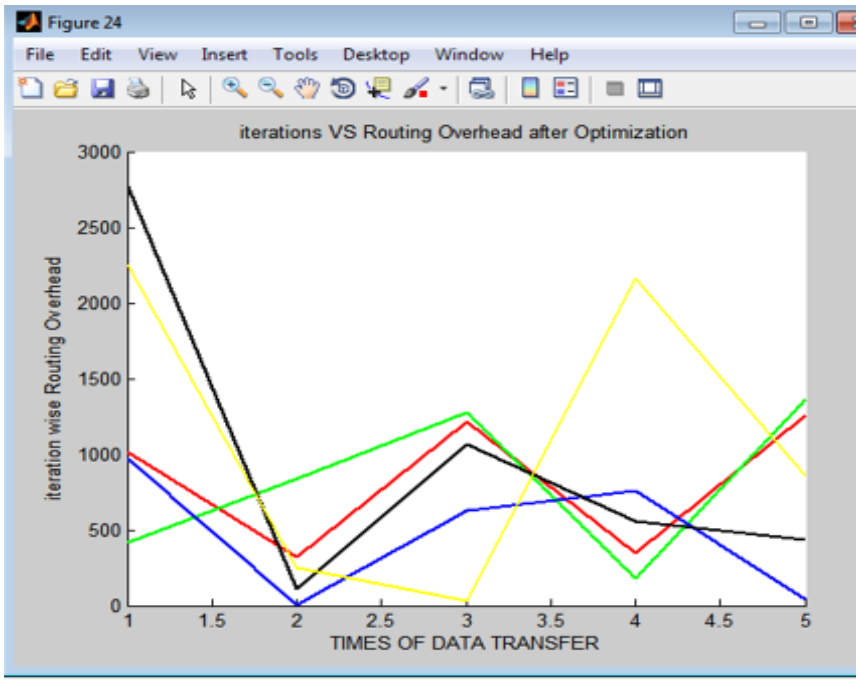

Figure 17. Iteration V/S routing overhead after optimization

Above figure, shows the graph between iteration V/S routing overhead using optimization method. In these five iterations, has been taken which is shown by blue, green, yellow, black and red colour. For 5 time of data transfer, the five different iteration values of routing overhead using optimization are .1, 500, 850, 1100 and 1200.

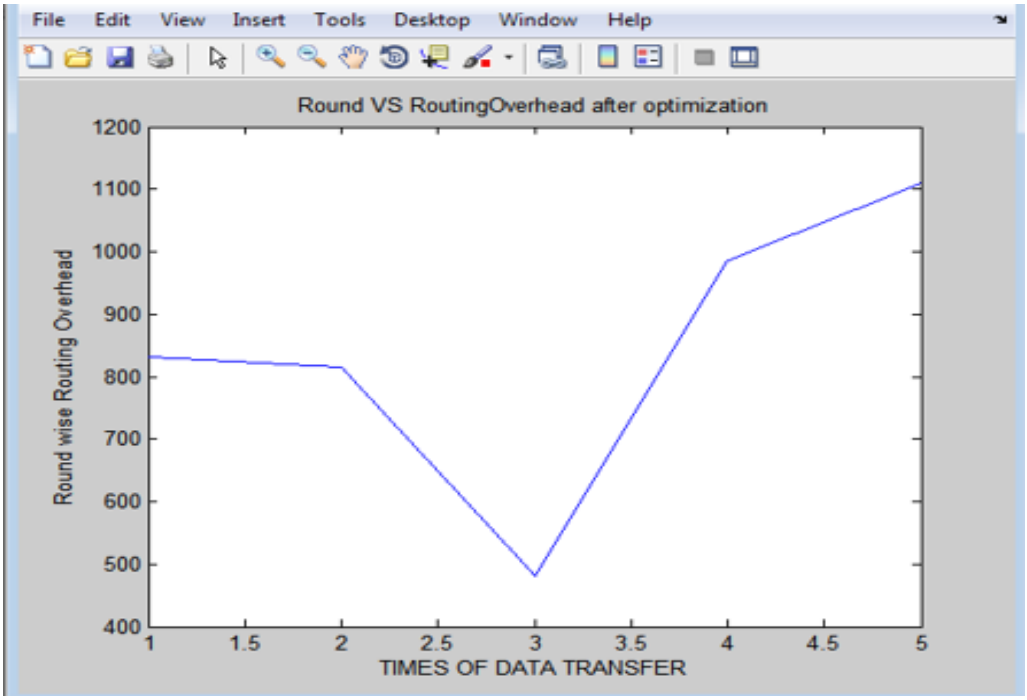

Figure 18. Round versus Routing Overhead using Optimization

Above figure, shows the graph between round wise output V/S times of data transfer for routing overhead for 5 rounds using optimization method. From graph the average value of routing overhead using optimization method for 5 times= 1100.

Table I. Throughput (%)without optimization:

S. No.	*A/C to Iteration*	*A/C to Round*
1	76	53
2	74	53.5
3	76	54
4	77	53
5	76	52.8

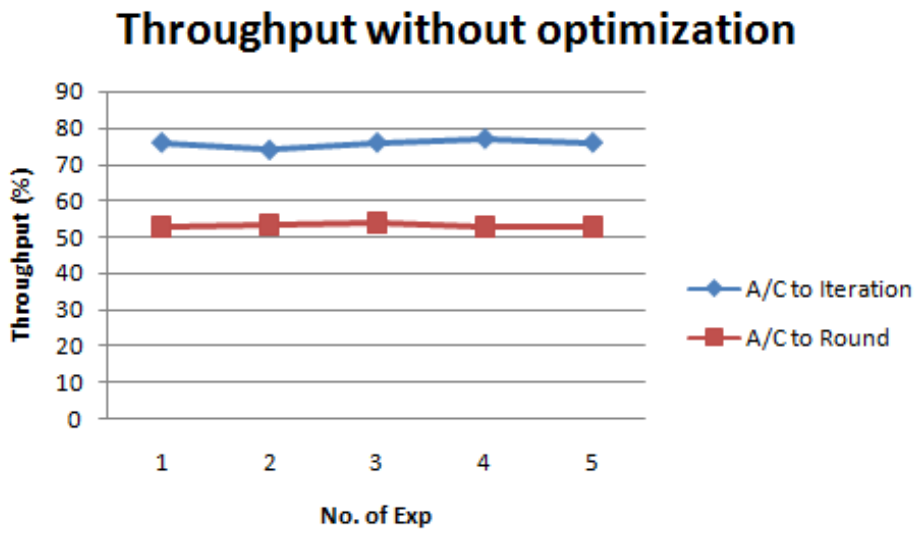

Figure 18. Throughput without optimization

Above table and graph show the throughput comparison between throughput according to iteration and throughput according to round for without optimization. Blue color line show the throughput according to the iteration and red color line show the throughput according to the round.

Table II. Throughput (%) with optimization:

S. No.	*A/C to Iteration*	*A/C to Round*
1	81	57
2	78	58
3	82	53
4	79	56
5	81	55

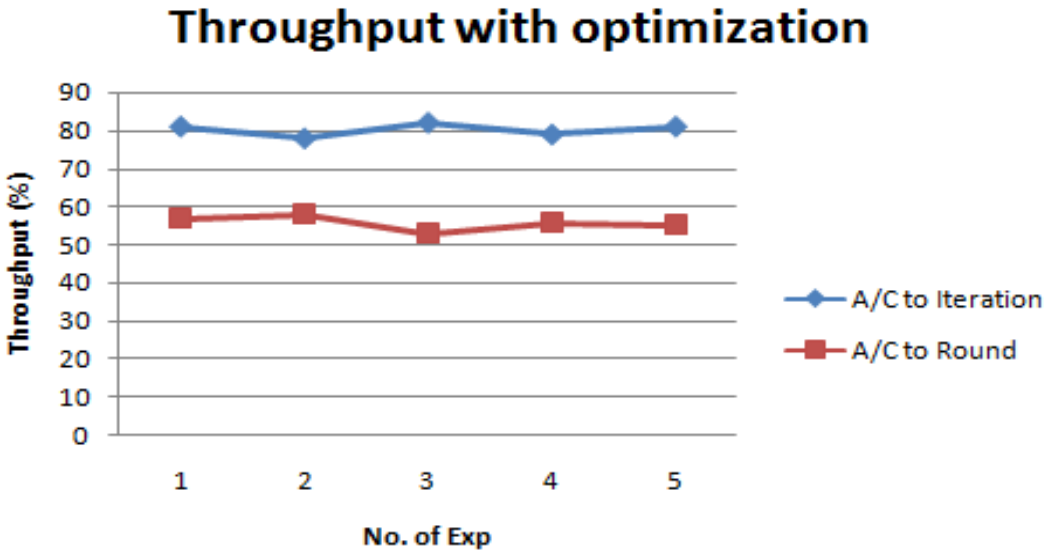

Figure 19. Throughput with optimization

Above table and graph show the throughput comparison between throughput according to iteration and throughput according to round for with optimization. Blue color line show the throughput according to the iteration and red color line show the throughput according to the round.

Table III. Delay (ms) without optimization:

S. No.	*A/C to Iteration*	*A/C to Round*
1	14.5	0.5
2	14	0.56
3	13.8	0.51
4	15.6	0.62
5	16	0.58

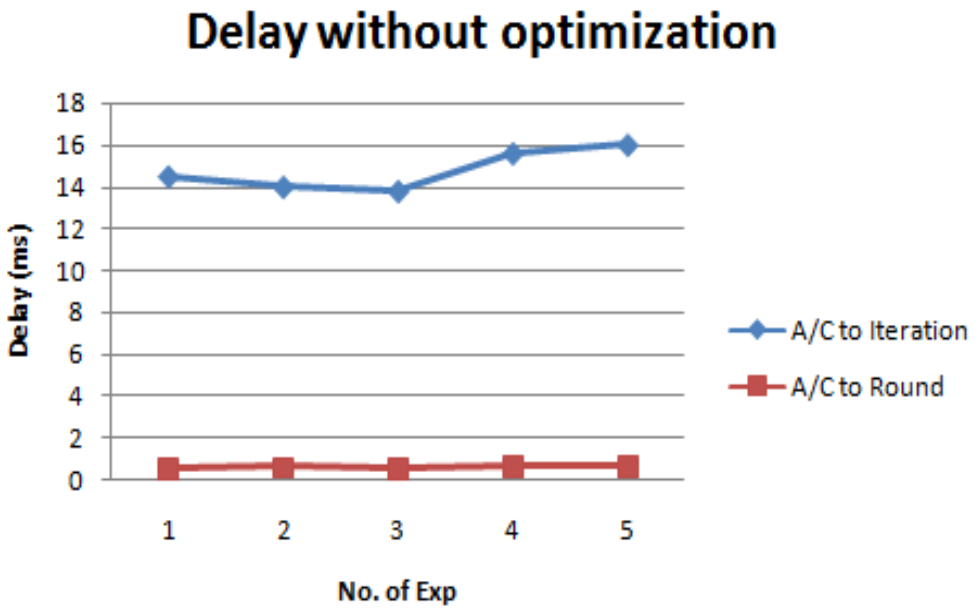

Figure 20. Delay without optimization

Above table and graph show the delay comparison between delay according to iteration and delay according to round for without optimization. Blue color line show the delay according to the iteration and red color line show the delay according to the round.

Table IV. Delay (ms) with optimization:

S. No.	*A/C to Iteration*	*A/C to Round*
1	5.7	0.4
2	6	0.4
3	4.3	0.38
4	5.5	0.42
5	5.8	0.36

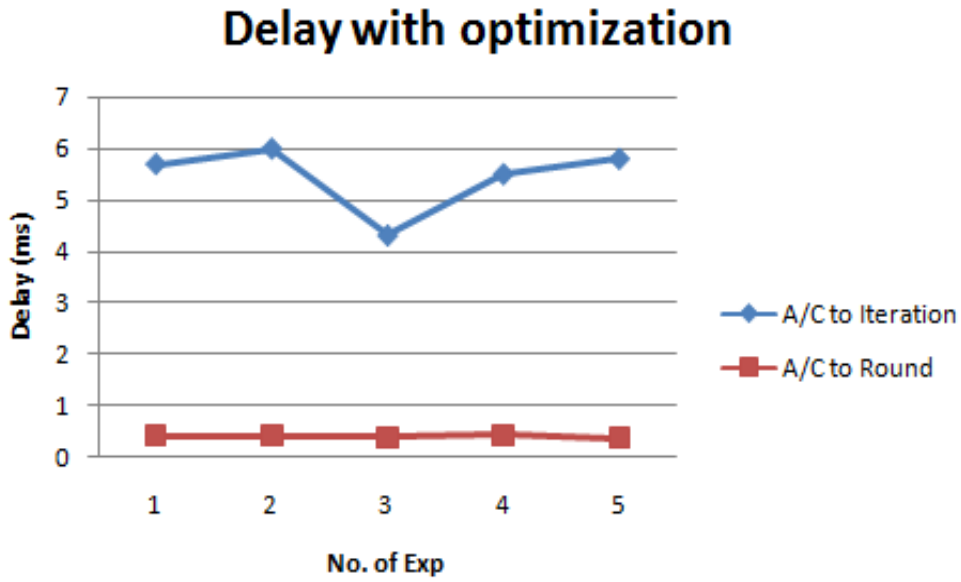

Figure 21. Delay with optimization

Above table and graph show the delay comparison between delay according to iteration and delay according to round for with optimization. Blue color line show the delay according to the iteration and red color line show the delay according to the round.

Table V. PDR (%) without optimization:

S. No.	*A/C to Iteration*	*A/C to Round*
1	97.5	96.4
2	98	95.3
3	97	96
4	96.8	96.8
5	98.4	95.4

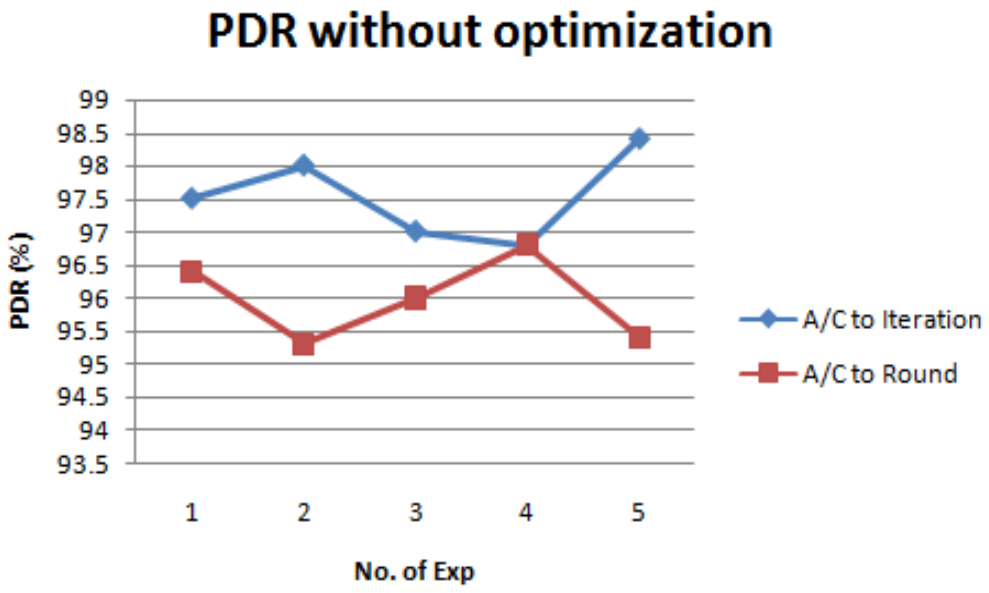

Figure 22. PDR without optimization

Above table and graph show the packet delivery ratio comparison between packet delivery ratio according to iteration and packet delivery ratio according to round for without optimization. Blue color line show the packet delivery ratio according to the iteration and red color line show the packet delivery ratio according to the round.

Table VI. PDR (%) Table with optimization:

S. No.	*A/C to Iteration*	*A/C to Round*
1	98	96
2	98.6	97.1
3	97.8	96.7
4	98.8	96.2
5	99.2	97.6

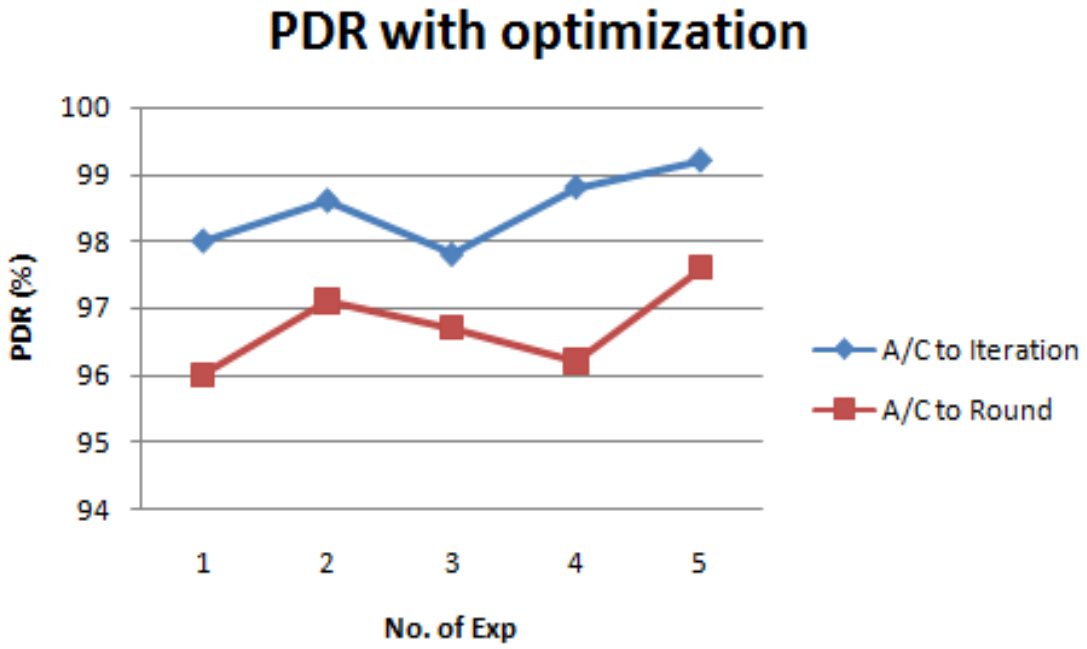

Figure 23. PDR with optimization

Above table and graph show the packet delivery ratio comparison between packet delivery ratio according to iteration and packet delivery ratio according to round for with optimization. Blue color line show the packet delivery ratio according to the iteration and red color line show the packet delivery ratio according to the round.

Table VII. ROH without optimization:

S. No.	*A/C to Iteration*	*A/C to Round*
1	1400	1302
2	1460	1380
3	1520	1460
4	1380	1320
5	1470	1240

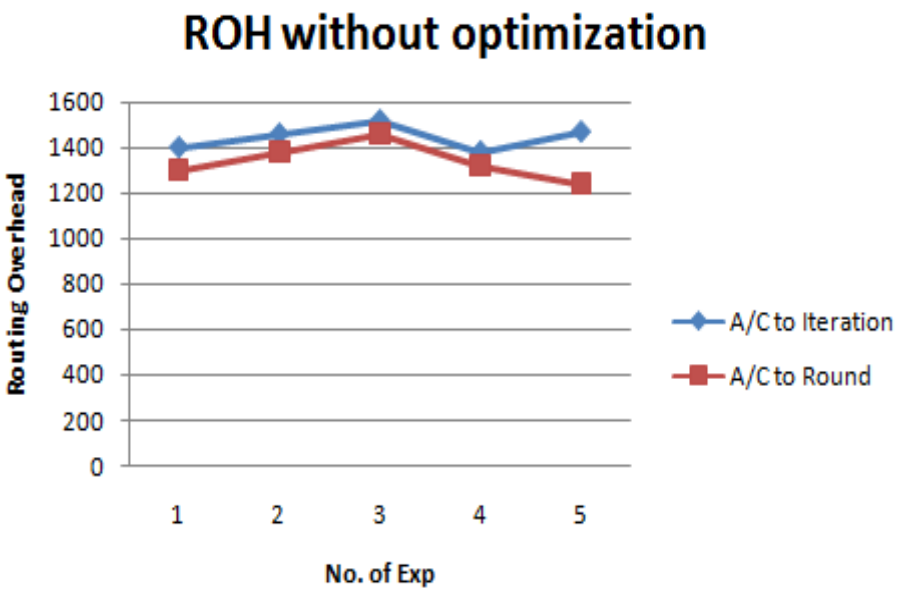

Figure 24. ROH without optimization

Above table and graph show the routing overhead comparison between routing overhead according to iteration and routing overhead according to round for without optimization. Blue color line show the routing overhead according to the iteration and red color line show the routing overhead according to the round.

Table VIII. ROH with optimization:

S. No.	*A/C to Iteration*	*A/C to Round*
1	600	644
2	540	345
3	720	380
4	450	410
5	930	340

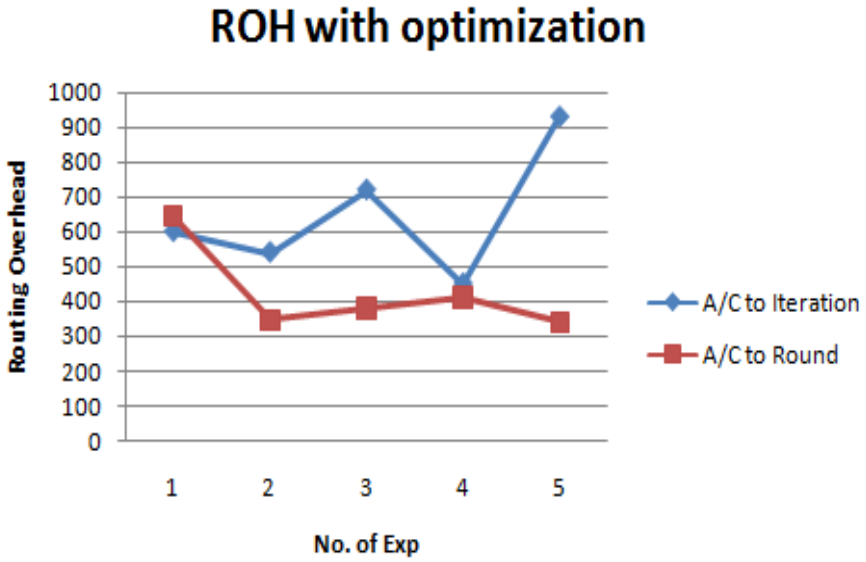

Figure 25. ROH with optimization

Above table and graph show the routing overhead comparison between routing overhead according to iteration and routing overhead according to round for with optimization. Blue color line show the routing overhead according to the iteration and red color line show the routing overhead according to the round.

V. CONCLUSION

AI methods are gaining more interest in providing security and they are very good in learning process. As it is known fact that cyber security has lots of attacks so they must be prevented. In this work usage of genetic algorithm with fuzzy rule set has been implemented for detection as well as prevention of attacks in the network. It has been concluded that the proposed algorithm has good rate of accuracy.

ACKNOWLEDGMENT

I wish to express my sincere gratitude to Mr. Jashanpreet Singh, Assistant Professor for his guidance and encouragement in my work. I would also like to thank my fellow mates Manpreet Singh and Hardavinder Singh for their suggestions throughout the work.

Conflict of interest: The authors declare that they have no conflict of interest.

Ethical statement: The authors declare that they have followed ethical responsibilities**.**

REFERENCES

[1] Ravi Sharma (2012). Study of Latest Emerging Trends on Cyber Security and its challenges to Society. International Journal of Scientific & Engineering Research, Vol. 3.

[2] Abraham D. Sofaer, David Clark andWhitfield Diffie (1997). Proceedings of a Workshop on Deterring Cyber Attacks. Informing Strategies and Developing Options for U.S. Policy http://www.nap.edu/catalog/12997.htmlCyber Security and International Agreements ,Internet Corporation for Assigned Names and Numbers, pp. 185-205.

[3] Pallavi Asrodia and Hemlata Patel (2012). Network Traffic Analysis Using Packet Sniffer. International Journal of Engineering Research and Applications(IJERA), Vol. 2, Issue 3, pp.854-856.

[4] Maryam Jafari, Shahram Jamali and Farzad Soleymani Sabzchi (2013). Discovering Users` Access Patterns for Web Usage Mining from Web Log Files. Journal of Advances in Computer Research.

[5] Roop Ranjan, Sameena Naaz and Neeraj Kaushik (2013). Web Miner: A Tool for Discovery of Usage Patterns from Web Data. Volume 5 ,Issue 5.

[6] L.Feinstein, D.Schnackenberg and R. Balupari,D. Kindred (2003). Statistical approaches to DDoS attack detection and response. In DARPA Information Survivability Conference and Exposition, Washington DC, Vol. 1, pp. 303-314.

[7] J. Choi, C. Choi, ByeongkyuKo, D. Choi and P. Kim (2013). Detecting Web based DDoS Attack using MapReduce operations in Cloud Computing Environment. Journal of Internet Services and Information Security, Vol. 3, no. 3/4, pp. 28-37.

[8] Loren Paul Rees, Jason K. Deane , Terry R. Rakes and Wade H. Baker. Decision support for Cyber security risk planning. Department of Business Information Technology, Pamplin College of Business, Virginia Tech., Blacksburg, VA 24061. United States b Verizon Business Security Solutions, Ashburn, VA 20147, United States.

[9] SamanehRastegari, M. Iqbal Saripan and MohdFadlee A. Rasid (2009). Detection of Denial of Service Attacks against Domain Name System Using Neural Networks. IJCSI International Journal of Computer Science Issues, Vol. 6, No. 1.

[10] C.Balarengadurai and S Saraswathi (2013). Fuzzy logic-based detection of DDoS attacks in IEEE 802.15.4 low rate wireless personal area network. Int. J. Trust Management in Computing and Communications, Vol. 1, Nos. 3/4, pp: 243- 260.

[11] Carr, V and J.H.M. Tah (2001). A fuzzy approach to construction Project management system. J. Adv. Eng. Software, Vol.32, pp. 847-857.

[12] Maryam Jafari, ShahramJamali and FarzadSoleymaniSabzchi (2013). Discovering Users` Access Patterns for Web Usage Mining from Web Log Files. Journal of Advances in Computer Research.

[13] T. Xiao, G. Qu, S. Hariri, and M. Yousif (2005). An Efficient Network Intrusion Detection Method Based on Information Theory and Genetic Algorithm. Proceedings of the 24th IEEE International Performance Computing and Communications Conference (IPCCC „05), Phoenix, AZ, USA. Proceedings of the Sixth International Conference on Software Engineering, Artificial Intelligence, Net.
[14] W. Li (2004). Using Genetic Algorithm for Network Intrusion Detection. A Genetic Algorithm Approach to Network Intrusion Detection. SANS Institute, USA.
[15] Bridges, Susan and Rayford B. Vaughn (2000). Intrusion Detection via Fuzzy Data Mining. In Proceedings of 12th Annual Canadian Information Technology Security Symposium, Ottawa, Canada, pp. 109-122.
[16] Crosbie, Mark and Gene Spafford (1995). Applying Genetic Programming to Intrusion Detection. In Proceeding of 1995 AAAI Fall Symposium on Genetic Programming, Cambridge, Massachusetts, pp. 1-8.
[17] Selvakani S and R.S. Rajesh (2007). Genetic Algorithm for framing rules for Intrusion Detection. IJCSNS, Vol.7, No.11.
[18] W. Lu and I. Traore (2004). Detecting new forms of network intrusion using genetic programming. Computational Intelligence Vol.20, Issue 3, pp. 475-494.
[19] J. Cannady (1998). Artificial Neural Networks for Misuse Detection. In Proceedings of National Information Systems Security Conference.
[20] B.C. Rhodes, J.A. Mahaffey, and J. D. Cannady (2000). Multiple Self-Organizing Maps for Intrusion Detection. In Proceedings of 23rd National Information Systems Security Conference.
[21] AbdelhakimHerrouz, ChabaneKhentout and MahieddineDjoudi (2014). Overview of Web Mining Contents: IJIRCCE.
[22] Daxin Jiang Jian Pei Hang Li (2013). Mining Search and Browse Logs for Web Search. ACM.
[23] JianliDuan and Shuxia Liu (2012). Research on web log mining analysis. IEEE.
[24] Sivakumar J and Ravichandran K.S (2013). Review on Semantic-Based Web Mining and its Applications. IJET.
[25] Maryam Jafari, ShahramJamali and FarzadSoleymaniSabzchi (2013). Discovering Users` Access Patterns for Web Usage Mining from Web Log Files. Journal of Advances in Computer Research.
[26] Roop Ranjan, Sameena Naaz and Neeraj Kaushik (2013). Web Miner: A Tool for Discovery of Usage Patterns from Web Data. Volume 5 ,Issue 5.
[27] Dilpreet kaur and Sukhpreet Kaur (2013). Study on User Future Request Prediction Methods Using Web Usage Mining. IJCER.
[28] Rimmy Chuchra, Bharti Mehta and Sumandeep Kaur (2013). Use of web Mining in Network Security. IJETAE.
[29] S.Mirdula and D.Manivannan (2013). Neural Network Approach for Web Usage Mining. IJRTE.
[30] Diallo Abdoulaye Kindy and Al-Sakib Khan Pathan (2012). A Detailed Survey on Various Aspects of SQL Injection in Web Applications: Vulnerabilities, Innovative Attacks, and Remedies.
[31] Pallavi Asrodia and Hemlata Patel (2012). Network Traffic Analysis Using Packet Sniffer. International Journal of Engineering Research and Applications (IJERA). Vol. 2, Issue 3, pp.854-856.
[32] Wei Lu et. al (2013). Detecting New Forms of Network Intrusion Using Genetic Programming. IEEE.
[33] ZU Wang (2011). Complement of an Extended Fuzzy Set. International Journal of Computer Applications (0975 – 8887) Volume 29– No.3.
[34] Sokratis et.al. Intrusion Detection Using Evolutionary Neural Networks. IEEE.
[35] Tridivet. Al (2009). A Real-time Intrusion Detection System Based on PSO-SVM. IEEE.
[36] Tridiv et.al (2011). Complement of an Extended Fuzzy Set. International Journal of Computer Applications (0975 – 8887) Volume 29– No.3.
[37] Gomez et. al (2002). Evolving Fuzzy Classifiers for Intrusion Detection. IEEE.
[38] Karen et.al (2007). Guide to Intrusion Detection and Prevention Systems. IDPS.
[39] Tao et.al (2205). An Efficient Network Intrusion Detection Method Based on Information Theory and Genetic Algorithm. IEEE.
[40] T. Xia, G. Qu, S. Hariri and M. Yousif (2005). An Efficient Network Intrusion Detection Method Based on Information Theory and Genetic Algorithm. Proceedings of the 24th IEEE International Performance Computing and Communications Conference (IPCCC ’05), Phoenix, AZ, USA.

[41] T. Hashni and T.Amudha (2012). Relative Study of CGS with ACO and BCO Swarm Intelligence Techniques. Int.J.Computer Technology &Applications. Vol 3 (5), pp.1775-1781.
[42] Hardavinder Singh Kairon & Manpreet Singh Sohal (2016), "A Review on gestures to control car functions", International Journal of Advanced Engineering Research and Applications, Volume – 2, Issue – 3, pp.168-173.