Global Journal

of Computer Science and Technology: E

Network, Web & Security

Efficient Clustering in WSN

Genetic Algorithm in MANET

Highlights

The Wireless Networks

Biometric Template Security

Discovering Thoughts, Inventing Future

VOLUME 14 ISSUE 7 VERSION 1.0

Global Journal of Computer Science and Technology: E
Network, Web & Security

Global Journal of Computer Science and Technology: E
Network, Web & Security

Volume 14 Issue 7 (Ver. 1.0)

Open Association of Research Society

Incorporation No.: 0423089
License No.: 42125/022010/1186
Registration No.: 430374
Import-Export Code: 1109007027
Employer Identification Number (EIN):
USA Tax ID: 98-0673427

Global Journals Inc.

*(A Delaware USA Incorporation with "Good Standing"; **Reg. Number: 0423089**)*

Sponsors: *Open Association of Research Society*
Open Scientific Standards

Publisher's Headquarters office

Global Journals Headquarters
301st Edgewater Place Suite, 100 Edgewater Dr.-Pl,
Wakefield MASSACHUSETTS, Pin: 01880,
United States of America
USA Toll Free: +001-888-839-7392
USA Toll Free Fax: +001-888-839-7392

Offset Typesetting

Global Journals Incorporated
2nd, Lansdowne, Lansdowne Rd., Croydon-Surrey,
Pin: CR9 2ER, United Kingdom

Packaging & Continental Dispatching

Global Journals
E-3130 Sudama Nagar, Near Gopur Square,
Indore, M.P., Pin:452009, India

Find a correspondence nodal officer near you

To find nodal officer of your country, please email us at *local@globaljournals.org*

eContacts

Press Inquiries: *press@globaljournals.org*
Investor Inquiries: *investors@globaljournals.org*
Technical Support: *technology@globaljournals.org*
Media & Releases: *media@globaljournals.org*

Pricing (Including by Air Parcel Charges):

For Authors:
22 USD (B/W) & 50 USD (Color)
Yearly Subscription (Personal & Institutional):
200 USD (B/W) & 250 USD (Color)

Integrated Editorial Board
(Computer Science, Engineering, Medical, Management, Natural Science, Social Science)

Dr. Bart Lambrecht
Director of Research in Accounting and FinanceProfessor of Finance
Lancaster University Management School
BA (Antwerp); MPhil, MA, PhD (Cambridge)

Dr. Carlos García Pont
Associate Professor of Marketing
IESE Business School, University of Navarra
Doctor of Philosophy (Management), Massachusetts Institute of Technology (MIT)
Master in Business Administration, IESE, University of Navarra
Degree in Industrial Engineering, Universitat Politècnica de Catalunya

Dr. Fotini Labropulu
Mathematics - Luther College
University of ReginaPh.D., M.Sc. in Mathematics
B.A. (Honors) in Mathematics
University of Windso

Dr. Lynn Lim
Reader in Business and Marketing
Roehampton University, London
BCom, PGDip, MBA (Distinction), PhD, FHEA

Dr. Mihaly Mezei
ASSOCIATE PROFESSOR
Department of Structural and Chemical Biology, Mount Sinai School of Medical Center
Ph.D., Etvs Lornd University
Postdoctoral Training,
New York University

Dr. Söhnke M. Bartram
Department of Accounting and FinanceLancaster University Management SchoolPh.D. (WHU Koblenz)
MBA/BBA (University of Saarbrücken)

Dr. Miguel Angel Ariño
Professor of Decision Sciences
IESE Business School
Barcelona, Spain (Universidad de Navarra)
CEIBS (China Europe International Business School).
Beijing, Shanghai and Shenzhen
Ph.D. in Mathematics
University of Barcelona
BA in Mathematics (Licenciatura)
University of Barcelona

Philip G. Moscoso
Technology and Operations Management
IESE Business School, University of Navarra
Ph.D in Industrial Engineering and Management, ETH Zurich
M.Sc. in Chemical Engineering, ETH Zurich

Dr. Sanjay Dixit, M.D.
Director, EP Laboratories, Philadelphia VA Medical Center
Cardiovascular Medicine - Cardiac Arrhythmia
Univ of Penn School of Medicine

Dr. Han-Xiang Deng
MD., Ph.D
Associate Professor and Research
Department Division of Neuromuscular Medicine
Davee Department of Neurology and Clinical NeuroscienceNorthwestern University
Feinberg School of Medicine

Dr. Pina C. Sanelli
Associate Professor of Public Health
Weill Cornell Medical College
Associate Attending Radiologist
NewYork-Presbyterian Hospital
MRI, MRA, CT, and CTA
Neuroradiology and Diagnostic Radiology
M.D., State University of New York at Buffalo,School of Medicine and Biomedical Sciences

Dr. Roberto Sanchez
Associate Professor
Department of Structural and Chemical Biology
Mount Sinai School of Medicine
Ph.D., The Rockefeller University

Dr. Wen-Yih Sun
Professor of Earth and Atmospheric SciencesPurdue University Director
National Center for Typhoon and Flooding Research, Taiwan
University Chair Professor
Department of Atmospheric Sciences, National Central University, Chung-Li, TaiwanUniversity Chair Professor
Institute of Environmental Engineering, National Chiao Tung University, Hsin-chu, Taiwan.Ph.D., MS The University of Chicago, Geophysical Sciences
BS National Taiwan University, Atmospheric Sciences
Associate Professor of Radiology

Dr. Michael R. Rudnick
M.D., FACP
Associate Professor of Medicine
Chief, Renal Electrolyte and Hypertension Division (PMC)
Penn Medicine, University of Pennsylvania
Presbyterian Medical Center, Philadelphia
Nephrology and Internal Medicine
Certified by the American Board of Internal Medicine

Dr. Bassey Benjamin Esu
B.Sc. Marketing; MBA Marketing; Ph.D Marketing
Lecturer, Department of Marketing, University of Calabar
Tourism Consultant, Cross River State Tourism Development Department
Co-ordinator , Sustainable Tourism Initiative, Calabar, Nigeria

Dr. Aziz M. Barbar, Ph.D.
IEEE Senior Member
Chairperson, Department of Computer Science
AUST - American University of Science & Technology
Alfred Naccash Avenue – Ashrafieh

Contents of the Issue

Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 14 Issue 7 Version 1.0 Year 2014
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Stochastic Approach for Energy-Efficient Clustering in WSN

By Manpreet Kaur, Er. Rohit Bhullar & Er. Lokesh Pawar
Chandigarh University, India

Abstract- Wireless sensor networks are self-organizing networks in which sensor nodes with limited resource are scattered in an area of interest to gather information. WSNs need to have effective node's energy management methods for stable and seamless communication. Power efficient clustering is done in WSN to prolong the life of the network. In WSN, many algorithms are developed to save energy of sensor nodes and to increase the lifetime of the network. This paper provides an energy efficient clustering algorithm inspired by prophet routing protocol to enhance the cluster based operation of the nodes. Adaptive learning is implemented for head selection for efficientcommunication. Simulation results confirm the efficiency of the mechanism.

Keywords: *WSN, ELEACH, EBCH, and CELEACH.*

GJCST-E Classification : *H.3.3, I.5.3*

Strictly as per the compliance and regulations of:

Stochastic Approach for Energy-Efficient Clustering in WSN

Manpreet Kaur [α], Er. Rohit Bhullar [σ] & Er. Lokesh Pawar [ρ]

Abstract- Wireless sensor networks are self-organizing networks in which sensor nodes with limited resource are scattered in an area of interest to gather information. WSNs need to have effective node's energy management methods for stable and seamless communication. Power efficient clustering is done in WSN to prolong the life of the network. In WSN, many algorithms are developed to save energy of sensor nodes and to increase the lifetime of the network. This paper provides an energy efficient clustering algorithm inspired by prophet routing protocol to enhance the cluster based operation of the nodes. Adaptive learning is implemented for head selection for efficient communication. Simulation results confirm the efficiency of the mechanism.

Keywords: WSN, ELEACH, EBCH, and CELEACH.

I. Introduction

Wireless Sensor Networks in which sensors behaves as a substitute of humans consists of small devices with very limited capabilities, called wireless sensor nodes that collect information from the environment by sensors, process the information, locally make decisions and wirelessly communicate with other nodes in the network. In wireless sensor networks, the large number of sensors is deployed over a wide range to inspect and collect the information regarding their environmental performance. Generally, the most important responsibility of those device nodes in WSN is to notice and collect WSN's environmental knowledge and to send its knowledge into WSN network's external finish users [1]. To detect and collect the data many routing protocols have been proposed which reduce load from network and extend the network lifetime. In WSN load can be balanced by using clustering algorithm. Most of the load maintaining algorithms assumes similar parameters like energy, load at nodes and clustering overhead. Thus, Cluster formation and cluster election is very important for data gathering, and clustering phenomenon is an essential part of the organizational structure.

LEACH is one of the first cluster-based routing protocols. But LEACH causes unequal partition of clusters in the network and don't allow reselection of cluster head during 1/p rounds. To overcome the drawbacks of LEACH new cluster head algorithms are introduced such as EBCHS introduces residual energy which is an important parameter in WSN to threshold calculation of cluster head selection. It allows reselection of cluster head during 1/p rounds. EBCHS increases lifetime of network better than the LEACH. Many other energy efficient algorithms are proposed to prolong the life of the network such as ELEACH, PEGASIS, PEACH, HEEP, HEED, etc. In routing algorithms, Multiple-sink topologies are also chosen due to limited battery power, capabilities and low communication range sensor nodes suffer from some disadvantages in single sink networks. Moreover, in WSN multi-sinks are used to increase the lifetime and enhance the performance of the network. EMCA, MRMS, and PBR such algorithms use the concept of multi-sinks to increase the lifetime of the network.

In our case, packet count between the sensors in a cluster is an important parameter: as it comes longer, the radio signal to communicate between two nodes must be more powerful, and more energy is consumed. Eventually, our goal is to save energy and to enable the WSN to live longer. The rest of the paper is organized as follows. Section II introduces some related work of clustering algorithms. In Section III we describe the clustering-related method of our CELEACH. Section IV describes various algorithms for proposed methodology and pseudo code. Section V presents network simulations and assumptions. Then we show simulation evaluation and performance comparison in Section VI and Section VII concludes this paper.

II. Related Work

Wireless Sensor Network consists of sensor nodes and many algorithms have been proposed to select a suitable cluster head for clusters, for communicating cluster headers with each other, etc. by many researchers. Ye XiaoGuo, Lv KangMeng, Wang RuChuan, and Sun Lijuan begin with the introduction of traditional routing protocols, classifications of routing protocols and proposed a novel adaptive load-balanced routing algorithm (ALB) based on minimum interference and cross-layer design principle in [3] and introduced the least interference path algorithm principle briefly, and the implementation of adaptive load-balanced routing algorithm is elaborated in detail. ALB algorithm could realize the prediction of network congestion and TCP can adjust the congestion window size self-adaptive according to the real-time status of link. The

Author α: Research Scholar, CSE Dept. CGC Gharuan, Mohali. e-mail: manpreet15dec@gmail.com.
Author σ ρ: Assistant Professor, CSE Dept.Chandigarh University, Mohali. e-mails: rohitbhullar.cu@gmail.com, lokeshpawar.cu@gmail.com

simulation results show that packet loss rate had been greatly improved and throughput rate had got a large scale enhancement (PP). It is not only avoiding the occurrence of link overload phenomenon, but also increased the network resource utilization rate and ensured data transmission reliable.

Tejal Irkhede, and Prachi Jaini begin with wireless sensor networks, frequently occurrence of failures in WSN and stated that load balancing is of great importance in wireless sensor networks because of the limited resource constraint and by keeping dynamic metrics such as network load, load balancing can be achieved and congestion can be avoided in [4]. They also stated that multipath routing decision in network layer has an important impact on the performance of WSN. The approach they take is to combine the ideas of clustering first and then traffic is evenly distributed in network. In clustering, each node takes part in cluster head formation. For load balancing in the network they improved the traffic splitting protocol. This approach helps in enhancing the total energy consumption. Common WSN experience shows that link congestion node failure frequently occur. This is because using single route in WSN would deplete the energy resources of involved nodes. Communication in WSN is depending on different parameters. Proposed method is considering two parameters load balancing and energy. Proposed protocol provides the better result than exiting E-leach protocol for total energy consumption. In future work, they will explore load balancing technique to avoid the congestion at nodes. They will evaluate more metrics like delay, jitter, bandwidth, packet delivery ratio.

In paper [1], Authors begin with the needs of WSN such as self Organizing Mechanism, Low-Powered Communication, Data Aggregation Mechanism and CH Rotational Selection and propose the CH self-selection mechanism based on nodes' energy value comparison algorithm to migrate these problems. In this paper authors compare energy consumed in LEACH, EACH and their propose algorithm EBCH. The first node dies at 357 in the case of LEACH and the spherical of initial node dead is 379 within the case of EACHS. Conversely, the spherical of FND is 478 within the case of EBCHS. However, Nodes square measure dead systematically when 490 rounds thanks to unequal energy consumption in LEACH and EACHS. But, EBCHS will maintain a standard network higher than alternative mechanisms by employing a minimum of 530 rounds.

Z. Xu, Yue Yin, Jin Wang and Jeong-Uk Kim proposed an Energy-efficient Multi-sink Clustering Algorithm (EMCA) for wireless sensor networks in [8] and stated that wireless sensor networks with single sink; the energy consumption of sensors near the sink or on the critical paths is too fast besides other disadvantages. In EMCA, residual energy plays a big role within the procedure of choosing cluster heads. Simulation results show that their projected rule consumes abundant less energy and owns longer network time period than the normal routing rule LEACH. For LEACH, the primary node that becomes invalid seems in 390th spherical, whereas EMCA has the primary inactive node in 503rd spherical. It is owing to the changes of cluster head roles considering nodes' residual energy, additionally because the main concentrate on diminution of energy consumption in EMCA that with efficiency prolongs the network time period.

A.Y. Al-Habashneh, M.H. Ahmed, and T. Husain had proposed three MAC protocols for the forest fire detection using WSN: P-CSMA/CA and Per-Hop Synchronization CSMA/CA are contention-based MAC protocols and the third one called Sensor-TDMA is a TDMA-based protocol in [2]. In paper [4], Author begins with brief introduction of clustering algorithms and their usage in many domains. Subsets are clusters of groups which share the similarities. The authors suggest that these algorithms are particularly use full in wireless sensor networks where there is data aggregation and energy cuts. In this paper clusters are assigned base stations of the network to spare energy and they can detect forest fire. A new approach of clustering in WSNs based on FFUCA method and on a metric measure of energy consumption. This algorithm can process large network easily with same cost and simple to use and clear organisation of nodes.

Andrei Gagarin and Sajid Hussain begin with transient introduction concerning WSN and provides a brand new heuristic approach to look for balanced and little weight routing spanning trees in an exceedingly network in [9]. This approach could be a modification of Kruskal's minimum spanning tree (MST) search rule and relies on a distributed search by graded clusters. It provides spanning trees with a lower most degree, an even bigger diameter and may be used for balanced energy consumption routing in wireless sensing element networks. In this, Author assumes that every link is employed specifically once in each directions in each of the information gathering or distribution communication rounds, consumed receiving energy of every node will be neglected with reference to its transmission energies in each of the communication rounds and every one transmissions over the links square measure assumed to possess knowledge packets of constant size. The approach will be enforced in parallel yet as a straightforward regionally distributed rule. Simulations of a sensible situation WSN square measure done supported the transmission energy matrix. The simulation results show that the proposed approach can extend the functional lifetime of a WSN in 3-4 times in terms of sensor transmission energy.

Ting Yang, ChunJian Kang, and Guofang Nan states that the simple graph theory is commonly employed in wireless sensor networks topology control

but an inherent problem of small- granularity algorithms is the high computing complexity and large solution space needed when managing large-scale WSNs. So, they use hyper-graph theory to solve these practical problems and propose a spanning hyper-tree algorithm (SHTa) to compute the minimum transmitting power delivery paths set for WSNs converge cast. Variable scale hyper-edges represented as computing units limit solution space and reduce computing complexity in. Mutual backup delivery paths in one hyper-edge improve the capability of fault tolerance. With experiment results, SHTa computes short latency paths with low energy consumption, compared with previous algorithms. Furthermore, in dynamic experiments scenes, SHTa retains its robust transmitting quality and presents high fault tolerance.

There are three main contributions of [10]:

1. They present a novel hyper-graph model to abstract large-scale and high connectivity WSNs into a robust hyper-tree infrastructure.
2. They present a precise mathematical derivation that solves the "hyper-tree existence" problem.
3. SHTa is proposed to compute the delivery paths set, which is the minimum power transmitting converge cast hyper-tree.

III. Proposed Methodology

In the proposed methodology, the prime focus was on reducing the load on node which will in turn provide a good platform to improve upon a number of things such as better performance and long life of the network.

Now we had two major schemes to discuss and implement. Firstly EBCH i.e. Load distributing protocol in which residual energy is an important parameter and threshold calculations are used for cluster head selection. It allows reselection of cluster head during 1/p rounds and secondly CELEACH in which we combine the ideas of clustering first and then traffic is evenly distributed in network. For clustering, the concept of EBCH algorithm is used and for load balancing in the network we use prophet routing protocol's concept on the improved the E-leach protocol for total energy consumption proposed in [4].

Hereby, an energy efficient algorithm CELEACH is proposed to enhance the cluster based operation of the nodes and balance traffic load. First step of proposed work is deployment of the network that consists of 50 nodes equally divided in five clusters. Each cluster elects cluster head for efficient communication. In our proposed methodology, we assume that:

1. Network area is 400*400 sq.units
2. Number of nodes are 50
3. Initial energy of all the nodes is 500mj
4. Delay between subsequent 0.2 unit Packet, and
5. Packet Size is 5 bit.

In the paper that we taken as our base of work for tsp the Load distribution is done. But contrastingly the load distributed is not balanced as evident in the figure above that the data is split in different paths of equal capacity but if that data if not balanced it will cause congestion.

Figure 1

In figure 1, the green part is the travelling data, the blue part is empty slots and the red ones are which are waiting for slots to be free. This red part is the one which hinders the performance of the system. The problem is evident enough from the above scenario that the traffic that is distributed needs to be balanced immediately and for that purpose we have used CELEACH as explained in brief above in which our focus is on removing this unbalanced load on paths. EBCH improves the problem single path but the scope of improvement is still there in the multipath mechanism. For fulfilling the above stated purpose and for full filling the CELEACH mechanism we simulated the situation with equal distribution while EBCH was undertaken.

In figure 2, the packets which were earlier waiting for the slots to get free for the communication now are assigned to different paths which intern give the right solution for their communication over same paths which faced heavy congestion earlier, reduced but still prominent in case of EBCH but with now the situation is under control.

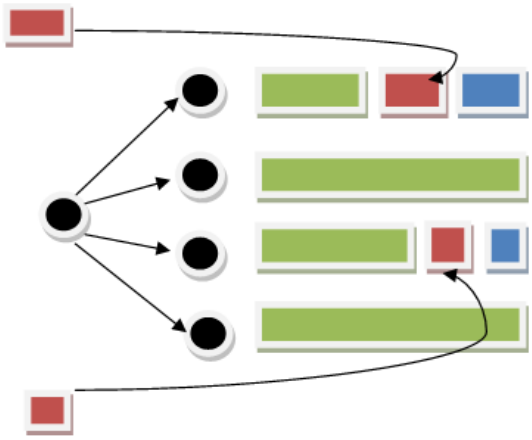


Figure 2

We also calculate average load, throughput, end to end delay, power left and power consumption in ELEACH and CELEACH algorithms. Description of calculations in brief is as given below:

- *Average load* is simply calculated by taking averages of all paths of *CELEACH* and *ELEACH*.
- *Throughput* is calculated by counting the number of packets needed for transmitting the same information.
- *End to End delay* is calculated by taking the sum of delay needed to send each packet.
- *Power left* is calculated as the power required to transmit one packet is known and number of packet send helps to calculate to total power in each case. Also the sleeping of nodes is considered.
- *Power consumed* is *100 - Power left*.

IV. Algorithm for Proposed Methodology

Three algorithms are designed for proposed methodology. First algorithm describes the whole procedure used to the cluster heads for clusters till the network is alive, second algorithm describes how the data is transferred from nodes to cluster head and from cluster head to base station, and third algorithm shows how the load is managed on the paths in the proposed methodology.

Algorithm 1: Election of CH

1. Deploy n nodes at random for the network.
   for n=1:50 // n is number of nodes
   k= randint (1, 2, [53,348]); // equation for node
   // deployment
2. Choose uniformly a part of nodes as cluster and elect one CH(Cluster Head) for each cluster as:
   ✓ let ***bcno*** is battery capacitor of each node and *c* is battery capacitor of CH.
   ✓ ***c= max(bcno)*** // node with maximum // battery power elected as CH
3. Repeat step 2 for each cluster to elect their CH.
4. CH will hold its position till its battery power is maximum than the threshold value.
5. Next CH will be elected by repeating step 2 to 5.

Algorithm 2: Data transfer

1. Both nodes send data to CH and CH transfer data to base station using multi paths.
2. Initially packet count is zero on each path.
3. If load on path is less than or equal to threshold

```
{
  Packet count increased by one
  Energy consumed (de)      //  de  is  assumed
  energy
                            // used to transfer
                            // one packet count
  }

Else

  {
   Algorithm 3
  }
```

Algorithm 3: Load Balancing

1. If load is less than or equal to threshold
   {
   // Do nothing
   }

   Else
   {
   Calculate extra load by subtracting threshold value
   from load

   Adjust extra load on the minimum loaded path
   {

   If extra load did not adjusted on other path
   Then: Send extra load on same path in next term
   Its packet count increased by two and
   Double of energy consumed (2de)
   }

   }

Pseudo code

Step 1: let load at 4 paths be L1, L2, L3 and L4.
Step 2: Start for loop path 1 >=4
Step 3: if (L1 > T) \\ T is the load threshold
Step 4: find difference in load D= L1 - T;
Step 5: if (L2 ' < T)
Step 6: put extra load to this path L2 = L2 ' + D; \\ L2 & L2 ' are the current and previous loads.
Step 7: end if condition;
Step 8: if (L3 ' < T)
Step 9: put extra load to this path L3 = L3 ' + D; \\ L3 & L3 ' are the current and previous loads.
Step 10: end if condition;
Step 11: if (L4 ' < T)
Step 12: put extra load to this path L4 = L4 ' + D; \\ L4 & L4 ' are the current and previous loads.
Step 13: end if condition;
Step 14: end if condition;

REPEAT THE STEPS 2 TO 14 FOR L2, L3 & L4 also.

V. Network Setup for Simulation

In this section, we mainly describe the simulations that are used to analyze and evaluate the performance of the proposed methodology. MATLAB was used to evaluate the ELEACH, EBCH and CELEACH algorithms via simulations. In wireless sensor networks, there are a lot of parameters to evaluate a clustering algorithm. In this paper, the packet count and average remaining energy of all nodes are chosen to compare the performance of the improved algorithm with ELEACH and EBCH.

We simulate E-LEACH, E-LEACH using EBCH and E-LEACH using CELEACH protocols by using the parameters defined in Table 1.

Table 1: Parametr of simulation

S.No.	Parameters	Values
1	Network size	400m X 400m
2	Initial Energy	500 mJ
3	Pd	100 mJ
4	Data Aggregation Energy cost	50pj/bit j
5	Number of nodes	50
6	Packet size	4000 bit
7	Transmitter Electronics	50 nJ/bit
8	Receiver Electronics	50 nJ/bit

VI. Simulation Analysis

During simulation, we compare the performance of our proposed algorithm with the performance of LEACH and EBCH algorithms. During deployment we divide 50 nodes in five clusters and each cluster is represented by different colors as shown in figure 3:

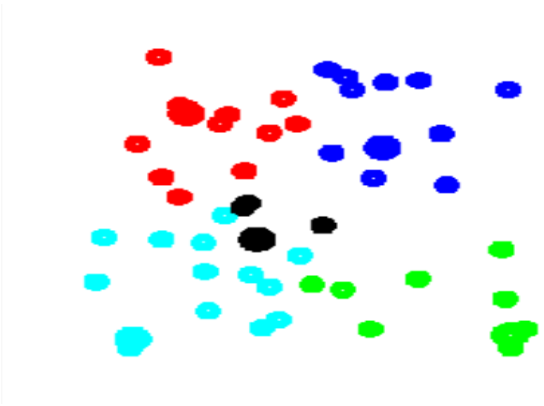
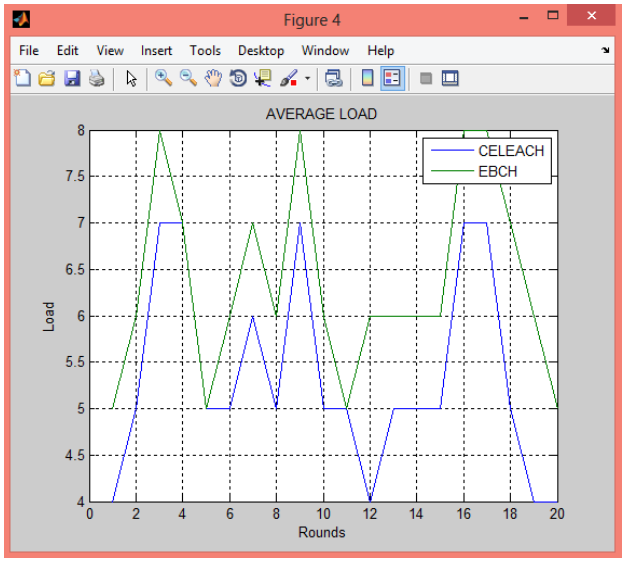


Figure 3

Simulations of E-LEACH using CELEACH in comparison with LEACH and E-LEACH using EBCH is being performed to observe the average load, power left, power consumption, end-to-end delay, average jitter and overall PDR or throughput.

Figure 4 shows that average load of E-LEACH using EBCH (Traffic splitting protocol) & CELEACH (Adaptive load balancing). Here the figure shown that the total no. of average load in E-LEACH using EBCH is higher than the total no. of average load in E-LEACH using CELEACH.

Figure 4



As CELEACH algorithm adaptively balanced the load in the network & gives better results in terms of network lifetime, end-to-end delay and throughput too.

Figure 5 shows that end to end delay comparison is higher in EBCH, lower in CELEACH and lowest in LEACH,

Figure 5

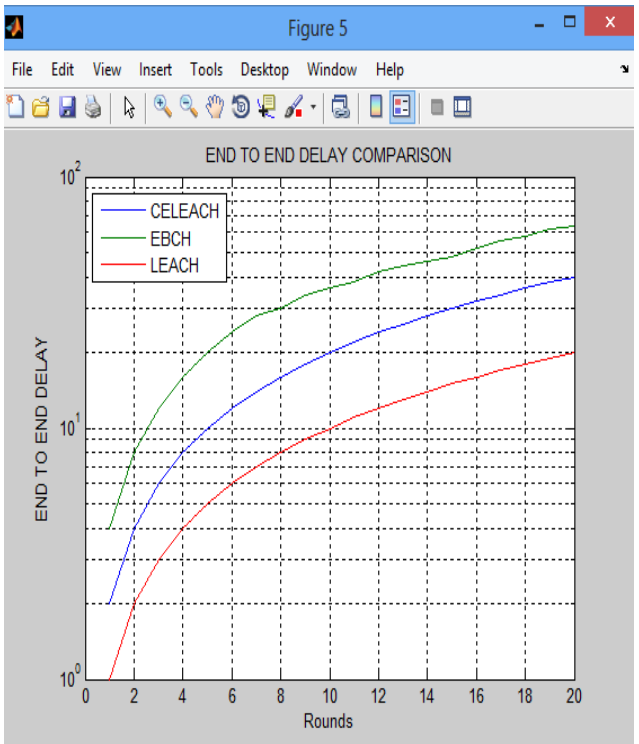


Figure 6 shows that throughput of E-LEACH using CELEACH is significantly greater as compared to LEACH and E-LEACH using EBCH. From this graph we see that the throughput of E-LEACH using CELEACH is more than the other two protocols because of adaptively load balancing in clustering and provide congestion free network,

Figure 6

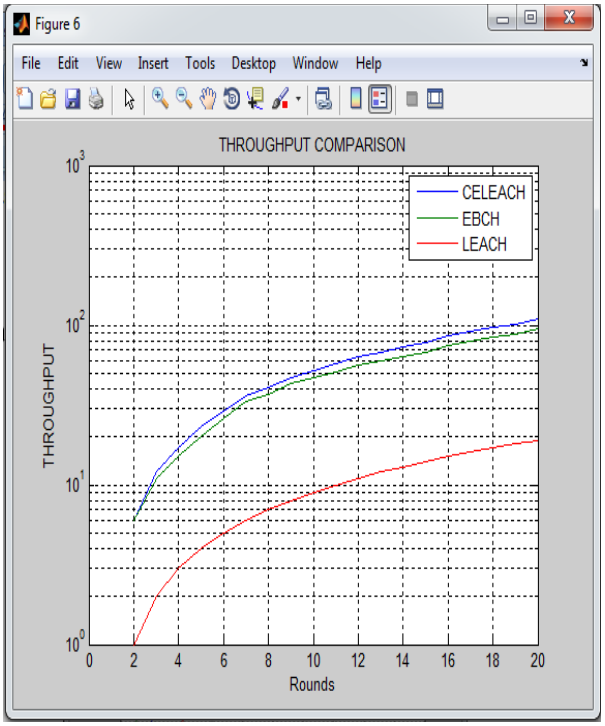
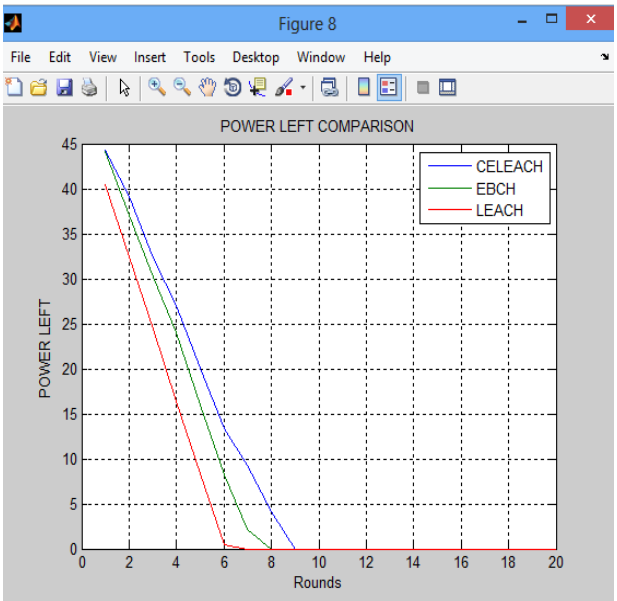


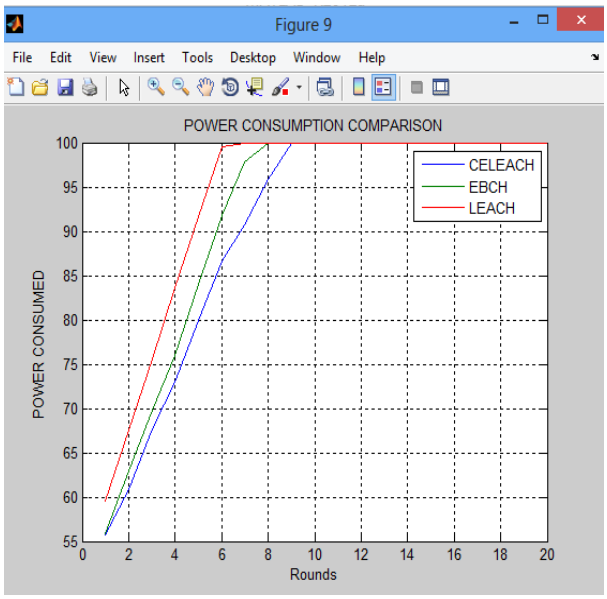
Figure 7 shows that power left comparison is less in LEACH as compare to CELEACH and EBCH,

Figure 7



and figure 8 also shows that the power consumption comparison is higher in LEACH as compare to CELEACH and EBCH.

Figure 8



Simulation results of LEACH, E-LEACH using EBCH and E-LEACH using CELEACH protocols by using the parameters defined in Table 1 are briefed in *Table 2:*

Algorithm	Network Survival Time	Through put (Max)	Jitter (Max)	E2E Delay (Max)
LEACH	7 rounds	10 bps	10 u	10 ms
EBCH	8 rounds	40 bps	6 u	30 ms
CELEACH	9rounds	50 bps	4 u	20 ms

Simulation results of LEACH, EBCH and CELEACH for various parameters while variation in nodes of the network.

a) Throughput Comparison

Table 3 compares throughput parameter in LEACH, EBCH and CELEACH and shows that the performance of CELEACH is getting better by increasing the number of nodes.

Table 3 : Throughput Comparison

No. of Nodes	LEACH	EBCH	CELEACH
50	10 bps	40 bps	50 bps
100	10 bps	40 bps	60 bps
150	10 bps	50 bps	70 bps

b) Jitter Comparison

Table 4 compares jitter parameter in LEACH, EBCH and CELEACH and shows that the performance of EBCH is getting better by increasing the number of nodes.

Table 4 : Jitter Comparison

No. of Nodes	LEACH	EBCH	CELEACH
50	10 u	6 u	4 u
100	10 u	5 u	4 u
150	10 u	5 u	4 u

c) Comparison of End to End Delay

Table 5 compares End to End Delay parameter in LEACH, EBCH and CELEACH and shows that there is no change by increasing the number of nodes.

Table 5 : Comparison of End to End Delay

No. of Nodes	LEACH	EBCH	CELEACH
50	10 ms	30 ms	20 ms
100	10 ms	30 ms	20 ms
150	10 ms	30 ms	20 ms

d) Comparison of Network Survival Time

Table 6 compares Network Survival Time in LEACH, EBCH and CELEACH and shows that the performance of CELEACH is getting better by increasing the number of nodes.

Table 6 : Network Survival Time's comparison

No. of Nodes	LEACH	EBCH	CELEACH
50	7 rounds	8 Rounds	9 Rounds
100	7 Rounds	8 Rounds	10 Rounds
150	7 Rounds	8 Rounds	11 Rounds

VII. Conclusion

In this paper, we proposed an optimized routing scheme for WSNs. The main focus was to provide the congestion free protocol. In our proposed scheme, Adaptive Load balancing is used in clustering. In E-LEACH using CELEACH, cluster heads are selected in each cluster on the basis of residual node energy. The E-LEACH using CELEACH scheme decrease the congestion in the network which make the WSN communication more energy efficient. The stability period of network and network lifetime have been optimized in our proposed strategy. Simulation results show that when compared with existing routing protocols CE-LEACH and ELEACH using EBCH, there is significant improvement in all these parameters.

References Références Referencias

1. C. Nam, Y. Han, and D. shin, "The Cluster-Heads Selection Method considering Energy Balancing For Wireless Sensor Network", International Journal of Distributed Sensor Network, 269215, 2013.
2. A.Y. Al-Habashneh, M.H. Ahmed, and T. Husain, "Adaptive MAC Protocols for Forest Fire Detection Using Wireless Sensor Networks", IEEE, 978-1-4244-3508, 2009.

3. Ye XiaoGuo, Lv KangMeng, Wang RuChuan, and Sun Lijuan, "Adaptive Load-Balanced Routing Algorithm", IEEE, 978-0-7695-4455-7, 2011.
4. Tejal Irkhede, and Prachi Jaini, "Cluster and Traffic Distribution Protocol for Energy Consumption in Wireless Sensor Network", IEEE, 978-1-4673-5630-5, 2013.
5. M.M. Sathik, M.S. Mohamed, and A. Balasubramanian, "Fire Detection Using Support Vector Machine in Wireless Sensor Network and Rescue Using Pervasive Devices", IJANA, 2010.
6. S. Fouchal, Q. Monnet, D. Mansouri, L. Mokdad, and M. Loualslen, "A clustering method for wireless sensors networks", IEEE, 978-1673-2713-8, 2010.
7. Y. Singh, S. Singh, U. Chugh, and C. Gupta, "Distributed Event Detection in Wireless Sensor Networks for Forest Fires", IEEE, 978-0-7695-4994-1, 2013.
8. K. Bouabdellah, H. Noureddine, and S. Larbi, "Using Wireless Sensor Networks for Reliable Forest Fires Detection", The 3rd International Conference on SEIT, 1877-0509, 2013.
9. M. Hefeeda and M. Bagheri, "Wireless Sensor Networks for Early Detection of Forest Fires", IEEE, 1-4244-1455-5, 2007.
10. Z. Xu, Yue Yin, Jin Wang and Jeong-Uk Kim "An Energy-Efficient Clustering Algorithm in WSN with Multiple Sinks", International Journal of Distributed Sensor Network, 429719, 2012.
11. Andrei Gagarin and Sajid Hussain, "Distributed search for balanced energy consumption spanning trees in Wireless Sensor Networks",
12. Ting Yang, ChunJian Kang, and Guofang Nan, "An Energy-Efficient and Fault-Tolerant Converge cast Protocol in Wireless Sensor Networks", International Journal of Distributed Sensor Networks, 429719, 2012.

Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 14 Issue 7 Version 1.0 Year 2014
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Energy Efficient QoS Routing Protocol based on Genetic Algorithm in MANET

By M. L. Ravi Chandra & Dr. P. Chandra Sekhar Reddy
Netaji institute of engineering & Technology, JNTUH, India

Abstract- In mobile ad-hoc networks (MANETs), providing quality of service is more challenging than wired networks, because of multi hop communication, node connectivity and lack of central co-ordination. Mobile ad-hoc networks need sure distinctive characteristics which might cause difficulties providing QoS in such network. Coming up with of multi constrained QoS routing protocols remains troublesome. As a result of routing protocols must satisfy the numerous QoS metrics at a time. Genetic algorithm based routing protocol will give the solution for multi constrained QoS routing problem. In existing genetic algorithm based routing, achieving energy efficiency is the major drawback. To overcome this drawback, in this paper, we have proposed genetic algorithm based energy efficient QoS routing for MANET. Proposed GA based routing algorithm discovered the shortest path from source to destination, which can consumes less energy compare to existing algorithms. In this paper TCP,CBR and video sources are applied at a time then energy consumption of proposed algorithm is compared with existing normal GA based and AOMDV. Simulation results show that proposed algorithm consumes less energy towards given scenario. Simulations are performed in NS-2.

Keywords: *multi constrained, genetic algorithm, energy consumption.*

GJCST-E Classification : *C.2.2*

Strictly as per the compliance and regulations of:

Energy Efficient QoS Routing Protocol based on Genetic Algorithm in MANET

M. L. Ravi Chandra [α] & Dr. P. Chandra Sekhar Reddy [σ]

Abstract- In mobile ad-hoc networks (MANETs), providing quality of service is more challenging than wired networks, because of multi hop communication, node connectivity and lack of central co-ordination. Mobile ad-hoc networks need sure distinctive characteristics which might cause difficulties providing QoS in such network. Coming up with of multi constrained QoS routing protocols remains troublesome. As a result of routing protocols must satisfy the numerous QoS metrics at a time. Genetic algorithm based routing protocol will give the solution for multi constrained QoS routing problem. In existing genetic algorithm based routing, achieving energy efficiency is the major drawback. To overcome this drawback, in this paper, we have proposed genetic algorithm based energy efficient QoS routing for MANET. Proposed GA based routing algorithm discovered the shortest path from source to destination, which can consumes less energy compare to existing algorithms. In this paper TCP,CBR and video sources are applied at a time then energy consumption of proposed algorithm is compared with existing normal GA based and AOMDV. Simulation results show that proposed algorithm consumes less energy towards given scenario. Simulations are performed in NS-2.

Keywords: multi constrained, genetic algorithm, energy consumption.

I. Introduction

a) MANET

A Mobile Ad hoc Network (MANET) consists of a collection of mobile nodes that are communicated in a multi-hop manner without any fixed infrastructure. Due to the characteristics like easy deployment and self-organizing capability, MANET has great potentials in many civil and military applications [1] [3].

MANETs have become an important medium of present day communication, and is easily deployable and infrastructure less. These networks are particularly suitable for emergency situations like warfare, floods and other disasters where infrastructure networks are not possible to operate [3]. In order to enable the data transfer, they communicate through single hop or through multiple hops with the help of intermediate nodes [9]. Nodes in MANETs are small radio devices with Limited computational capacity and memory. Routes are mostly multi-hop because of the limited radio propagation range [10]. In this regard multicasting protocol plays a critical role in the MANETs than uni cast protocols and are faced with the challenge of producing multi-hop routing under host mobility and band width constraint.

Author α: Associate Professor, ECE Dept, NIET, Hyderabad, India. e-mail: mlravigates@gmail.com

Author σ: Professor-coordinator, ECE Dept, JNTUH, Kukatpally, Hyderabad, India. e-mail: drpcsreddy@gmail.com

b) QoS Routing

Quality of Service (QoS) routing algorithms is different from the conventional routing algorithms. In QoS routing, the path from the source to the destination must satisfy the multiple constraints simultaneously (e.g., bandwidth, reliability, end-to-end delay, jitter and cost), while in conventional routing, routing decisions are made based only on a single metric [2]. The main purpose of QoS routing is to find a feasible path that has sufficient resources to satisfy the constraints. A main problem in QoS routing is to find a path between the source and destination that satisfies two or more end-to-end QoS constraints [4]. In MANET, providing QoS is more challenging than in wired networks, mainly due to node mobility, multi hop communication, contention for channel access, and lack of central coordination [5] [6]. The basic function of QoS routing is to find a network path, which satisfies the given constraints and optimize the resource utilization [7]. The role of QoS routing strategy is to compute paths that are suitable for different type of traffic generated by various applications while maximizing the utilizations of network resources [8].

The important objectives of QoS routing are:

- To find a path from source to destination while satisfying user's requirements.
- To optimize the usage of the network resource.
- To degrade the network performance when unwanted things like congestion, path breaks appear in the network [8].

c) Energy Efficiency in MANET

The two important characteristics of multi-hop wireless networks are:

- Available battery power on the constituent lightweight mobile nodes (such as sensor nodes or smart phones) is quite limited.
- Communication costs (in terms of requirement of transmission energy) are much higher than computing costs (on individual devices).

The insufficient lifetime of battery imposes a limitation on the network performance. To take the complete advantage of lifetime of nodes, traffic should be routed to minimize the energy consumption [5].

Energy-aware routing protocols for such networks usually select routes that minimize the total transmission power. When the transmission power is fixed, each link has the same cost and the minimum hop path is selected. When the transmission power can vary with the link, as the link cost is higher for longer hops, the energy-aware routing algorithms select a path with large number of small-distance hops [6].

II. Literature Review

Jinhua Zhu and Xin Wang [11] have proposed an accurate analytical model to track the energy consumption. Then, they proposed a simple energy-efficient routing scheme called PEER to improve the performance of the routing protocol during route discovery and in mobility scenarios. Simulation results have indicated that PEER protocol reduces path discovery overhead and delay up to 2/3, and transmission energy consumption about 50 percent.

Gabriel Ioan Ivascu et al [14] have presented a new approach called Quality of Service Mobile Routing Backbone over AODV (QMRB-AODV) for supporting QoS using a mobile routing backbone to dynamically distribute the traffic and to select the route that can support the best QoS connection. Nodes in real-life MANET are heterogeneous and have different characteristics. Based on these characteristics, their solution classifies nodes as either QoS routing nodes, simple routing nodes that route the packets through the network without providing special service provisions or transceiver nodes, that send and receive the packets but cannot relay them. Simulation result shows that QMRB-AODV gives the best result in terms of packet delivery ratio and bandwidth utilization. The drawback of this paper is that this protocol cannot perform well when the number of route requests increased. Since it increases the average queuing time for packets, which leads to higher end-to-end delay.

In [13], a GA based QoS routing algorithm is proposed for solving the MCP problem. It is able to produce multiple feasible paths, which makes the algorithm more robust when the actual state information in the network changes. In GA, multiple feasible paths can be created by iterating the algorithm until multiple feasible paths are found. This process increases the success of finding feasible path that can fulfill the QoS requirement.

The drawbacks of this paper are:

Increase in end-to-end delay in the network.

- Lack of energy efficiency constraints.
- Less efficient utilization of bandwidth.
- Decrease in packet delivery ratio.

In [12], the minimum bandwidth, end-to-end delay and connectivity metrics are considered for fitness function. But, it does not consider the energy efficiency. Then various constraints like end-to-end delay, available bandwidth, and node connectivity index and resource availability are combined into a single constraint. In GA based routing algorithm, the fitness function is modified by incorporating the combined metric in such a way that it satisfies the set of QoS requirement. In this, we have given the preference for dynamic aspects of node while determining its performance in the network.

By implementing this method, we are minimizing the QoS values on links from source to destination and increasing the possibility for the path to satisfy the given QoS requirement and hence we can overcome the MCP problem.

III. Proposed Solution

Initially, a minimum energy shortest path is discovered. Several paths may exist between the source and the destination. Among them, the minimum energy shortest path (energy-efficient) is selected using this method.

For example, in an 802.11 network, the energy consumption by the RTS,CTS and Ack packets accounts for a significant part of the total energy consumption without considering such energy consumption, these protocols may tried to used a larger number of intermediate nodes. These resulting in more energy consumption, a lower throughput and /or a higher end to end packet error rate.

To address the deficiencies of the existing approach, in this section more accurate energy consumption model is applied, which uses minimum energy routing scheme.

a) Determining Average Power For Transmission

There are two types of MAC schemes in IEEE 802.11: Distributed Coordination Function (DCF) and Point Coordination Function (PCF). In our proposed protocol we will implement DCF as PCF is a centralized protocol.

DCF is actually based on Carrier Sensing Multiple Access with Collision Avoidance (CSMA/CA) mechanism that consists of two carriers sensing schemes: physical carrier sensing and virtual carrier sensing. The virtual carrier sensing scheme is implemented along with Network Allocation Vector (NAV). If a node receives a packet (such as RTS, CTS, and DATA packet) it updates NAV along with the duration included in the received packet. The NAV value indicates while the on-going transmission session ends. When a node wants to send data packet to another node, it first checks its NAV. If the NAV is larger than 0, it has to wait till NAV reaches 0. After this only, sender transmits RTS packet when the channel is available for a period greater than DCF InterFrame Space (DIFS) or when the backoff timer reaches zero. The receiver responds along with a CTS packet after receiving The RTS packet. After receiving the CTS, sender sends out the data packet and receiver reply with ack packet after

receiving the data packet successfully. If the sender doesn't receive the ACK packet within the time defined, the entire process is repeated again.

Based on the above defined DCF protocol, the total power required for transmission can be estimated as follows:

Notations Used:

N	data size
N_{hdr}	802.11 header size
N_{rts}	RTS packet size
N_{cts}	CTS packet size
N_{ack}	ACK packet size
N_{phy}	size of physical layer overhead
$P_{r,i,j}$	packet error rate of RTS packet
$P_{c,i,j}$	packet error rate of CTS packet
$P_{i,j}$	packet error rate of DATA packet
$P_{a,j,i}$	packet error rate of ACK packet

The total transmission power PT required to transmit a packet from node i to node j is given by

$$P_T(i,j) = \frac{P_m(N_r + N_c p_{r,i,j})}{p_{r,i,j} p_{c,j,i} p_{i,j} p_{a,j,i}} + \frac{P_{i,j} N_K + P_{j,i} N_a p_{i,j}}{p_{i,j} p_{a,j,i}} \quad (1) \quad [11]$$

Average total receiving power PR to receive a packet from node i to node j is given by

$$P_R(i,j) = \frac{\frac{N_r}{N_K} + \left(\frac{N_c}{N_K} + p_{i,j} + \frac{N_a}{N_K} p_{i,j} p_{a,i,j}\right) p_{c,i,j}}{p_{c,i,j} p_{i,j} p_{a,i,j}} \quad (2) \quad [11]$$

where $N_K = N + N_{hdr} + N_{phy}$

$N_r = N_{rts} + N_{phy}$

$N_c = N_{cts} + N_{phy}$

$N_a = N_{ack} + N_{phy}$

Here the network considers the transmission power PT and receiving power PR to estimate the link cost in the network. We assume that there are I-1 intermediate nodes between source and destination. Also the nodes along the path from source to destination are numbered from 0 to I.

Then, the total power required for reliable transmission along the path from source to destination is given by

$$P_m = \sum_{i=0}^{I-1} P_T\left((i, i+1) + P_R(i, i+1)\right) \quad (3) \quad [11]$$

b) Minimum Energy Shortest Route Discovery Process

Using the minimum energy shortest route discovery process, multi-route is selected. The main route is selected based on the QoS metric. The combined QoS constraint consists of end-to-end delay, bandwidth, packet loss rate, and node connectivity index (Ni) and dynamic resources availability. In this paper, we present simulation results only for energy consumption for TCP, CBR and video sources.

Proposed Genetic algorithm based energy efficient routing protocol (GAEEQR) discovered the optimized energy route from source to destination.

IV. Simulation Results

a) Simulation Model and Parameters

The Network Simulator (NS2) [16] is used to simulate the proposed architecture. In the simulation, the mobile nodes move in a 1250 m x 1250 m region for 50 seconds of simulation time. All available nodes have the same transmission range of 250 meters. The traffic used for simulation is Constant Bit Rate (CBR), Video and TCP.

The parameters used for simulation are summarized in table.

Table 1 : SIMULATION PARAMETERS

No. of Nodes	30,50,70,90 and 110
Area Size	1250 X 1250
Mac	IEEE 802.11
Transmission Range	250m
Simulation Time	50 sec
Traffic Source	CBR,Video and TCP
Packet Size	512
Routing Protocol	AOMDV,GA,GAEEQR
Speed	10,20,30,40 and 50m/s
Rate	50,100,150,200 and 250kb
Initial Energy	10.3 J
Transmission Power	0.660
Receiving power	0.395

The proposed Genetic Algorithm based QoS Routing is compared with the GA based QoS Routing technique [13] and AOMDV. The performance is evaluated mainly, energy consumption between the source and destination.

b) Results

Simulation experiments were conducted by varying

- Nodes
- Speed
- Rate

i. *Based on Nodes*

In this simulation experiment, we may vary the number of nodes as 30, 50, 70, 90 and 110.

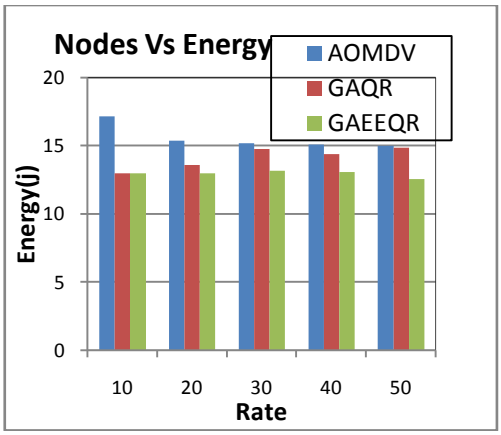


Figure 1 : Nodes Vs Energy consumption

Fig1 shows the energy consumption of all the 3 protocols for different number of nodes scenario. We can observe that the energy consumption of GAEEQR is 7% less than GAQR and 17% less than AOMDV.

ii. *Based on Speed*

In this experiment, we may vary the mobile speed as 10, 20, 30, 40 and 50 m/s

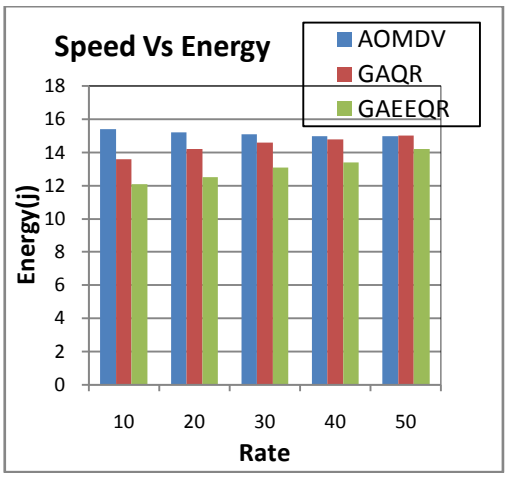


Figure 2 : Speed Vs Energy Consumption

Fig 2 shows the energy consumption of all the 3 protocols for different speed scenario. We can observe that the energy consumption of GAEEQR approach is 6.4% less than GAQR and 12% less than AOMDV.

iii. *Based on Rate*

In this experiment, by varying the rate as 50,100,150,200 and 250kbits then Energy consumption has calculated for three algorithms.

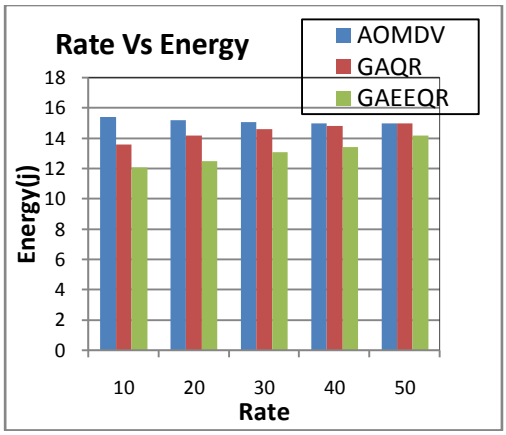


Figure 3 : Rate Vs Energy consumption

Fig 3 shows the Energy consumption of GAEEQR, GAQR and AOMDV protocols for different rates scenario. By observing above scenario it can conclude that, GAEEQR algorithm is giving better results, means it can consume less energy than AOMDV and GAQR.

V. Conclusion

In this paper, we have proposed GA based Energy Efficient QoS routing and Optimization Protocol in MANET. There are several paths between the source and destination, among them, the minimum energy shortest path (energy-efficient) is selected. Using the Minimum Energy Shortest Route Discovery Process, multiple routes are selected. The main route is selected based on the QoS metric. By observing above simulation results, it is conclude that,the proposed GA based energy efficient QoS routing protocol consumes less energy compare to existing GA based algorithm and AOMDV.

References Références Referencias

1. Wendong Xiao, Boon Hee Soong, Choi Look Law, Yong Liang Guan, "QoS Routing Protocol for Ad Hoc Networks with Mobile Backbones", 2005.
2. Zhenjiang Li • J.J. Garcia-Luna-Aceves, "Finding multi-constrained feasible paths by using depth-first search", July 2006.
3. Vinod Kone and Sukumar Nandi, "QoS Constrained Adaptive Routing Protocol For Mobile Adhoc Networks", 2006.
4. R. Asokan, A. M. Natarajan and A. Nivetha, "A Swarm-based Distance Vector Routing to Support Multiple Quality of Service (QoS) Metrics in Mobile Adhoc Networks", 2007.
5. LAJOS HANZO, RAHIM TAFAZOLLI, "A SURVEY OF QOS ROUTING SOLUTIONS FOR MOBILE AD HOC NETWORKS", 2007.
6. L. Hanzo, R. Tafazolli, "A Survey of QoS Routing Solutions for Mobile Ad hoc Networks", 2007.

7. Saida Ziane, Abdelhamid Mellouk, "AMDR: A Reinforcement Adaptive Mean Delay Routing Algorithm for MANET", 2007.
8. P. Deepalakshmi, Dr. S. Radhakrishnan, "Ant Colony Based QoS Routing Algorithm For Mobile Ad Hoc Networks", May 2009.
9. G. Santhi and Alamelu Nachiappan, "A SURVEY OF QOS ROUTING PROTOCOLS FOR MOBILE AD HOC NETWORKS", August 2010.
10. D.S. Thenmozhi, Dr. R. Lakshmipathi, " Highly Ensured QOS Routing in Mobile Ad Hoc Networks Based on Multiple Constraints", October 2010.
11. inhua Zhu and Xin Wang," Model and Protocol for Energy-Efficient Routing over Mobile Ad Hoc Networks", IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 10, NO. 11, NOVEMBER 2011.
12. Jiwa Abdullah, M. Y. Ismail, N. A. Cholan, S. A. Hamnzah, "GA-based QoS route Selection Algorithm for Mobile Ad-Hoc Networ:ks", Proceedings of IEEE 2008 6th National Conference on Telecommunication Technologies and IEEE 2008 2nd Malaysia Conference on Photonlis, 26-27 August 2008, Prjaya, Malaysia .
13. Salman Yussof, Ong Hang See, "A Robust GA-based QoS Routing Algorithm for Solving Multi-constrained Path Problem", JOURNAL OF COMPUTERS, VOL. 5, NO. 9, SEPTEMBER 2010.
14. Ivascu, Gabriel Ioan, Samuel Pierre, and Alejandro Quintero. "QoS routing with traffic distribution in mobile ad hoc networks" Computer Communications 32.2 (2009): 305-316.
15. Floriano De Rango, Francesca Guerriero and Peppino Fazio," Link-Stability and Energy aware Routing Protocol in Distributed Wireless Networks", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, 2012.
16. Network simulator: ///http:www.isi.edu/nsnam

This page is intentionally left blank

Global Journal of Computer Science and Technology: E Network, Web & Security
Volume 14 Issue 7 Version 1.0 Year 2014
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

DoS and DDoS Attacks: Defense, Detection and Traceback Mechanisms -A Survey

By K. Munivara Prasad, A. Rama Mohan Reddy & K.Venugopal Rao
JNTUH University, India

Abstract- Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks are typically explicit attempts to exhaust victim's bandwidth or disrupt legitimate users' access to services. Traditional architecture of internet is vulnerable to DDoS attacks and it provides an opportunity to an attacker to gain access to a large number of compromised computers by exploiting their vulnerabilities to set up attack networks or Botnets. Once attack network or Botnet has been set up, an attacker invokes a large-scale, coordinated attack against one or more targets. Asa result of the continuous evolution of new attacks and ever-increasing range of vulnerable hosts on the internet, many DDoS attack Detection, Prevention and Traceback mechanisms have been proposed, In this paper, we tend to surveyed different types of attacks and techniques of DDoS attacks and their countermeasures. The significance of this paper is that the coverage of many aspects of countering DDoS attacks including detection, defence and mitigation, traceback approaches, open issues and research challenges.

Keywords: denial of service (DoS), distributed denial of service (DDoS), detection mechanisms and trceback approaches.

GJCST-E Classification : D.4.6

Strictly as per the compliance and regulations of:

DoS and DDoS Attacks: Defense, Detection and Traceback Mechanisms - A Survey

K. Munivara Prasad [α], A. Rama Mohan Reddy [σ] & K. Venugopal Rao [ρ]

Abstract- Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks are typically explicit attempts to exhaust victim's bandwidth or disrupt legitimate users' access to services. Traditional architecture of internet is vulnerable to DDoS attacks and it provides an opportunity to an attacker to gain access to a large number of compromised computers by exploiting their vulnerabilities to set up attack networks or Botnets. Once attack network or Botnet has been set up, an attacker invokes a large-scale, coordinated attack against one or more targets. As a result of the continuous evolution of new attacks and ever-increasing range of vulnerable hosts on the internet, many DDoS attack Detection, Prevention and Traceback mechanisms have been proposed, In this paper, we tend to surveyed different types of attacks and techniques of DDoS attacks and their countermeasures. The significance of this paper is that the coverage of many aspects of countering DDoS attacks including detection, defence and mitigation, traceback approaches, open issues and research challenges.

Keywords: denial of service (DoS), distributed denial of service (DDoS), detection mechanisms and trceback approaches.

I. Introduction

Denial-of-service (DoS) attacks exploit internet to target critical Web services [1, 2, 3, 4, 5,6]. This type of attack is intended to prevent legitimate users from accessing a specific network resource or degrade normal services for legitimate users by sending huge unwanted traffic to the victim (machines or networks) to exhaust services and connection capacity or the bandwidth. Increasing flow of these DoS attacks has made servers and network devices on the internet at greater risk.

Denial of service attack programs are around for several years. Previous single source attacks are currently countered simply by several defense mechanisms and therefore the source of those attacks will be simply rejected or blocked with improved tracing capabilities. However, with the amazing growth of the internet throughout the last decade, an increasingly large amount of vulnerable systems are currently available to attackers. Attackers will currently use a huge range of those vulnerable hosts to launch an attack rather than employing a single server, an approach that is not terribly effective and detected easily.

A distributed denial of service (DDoS) attack [7, 12] is a large-scale, coordinated attack on the provision of services of a victim system or network resources, launched indirectly through a large number of compromised computer agents on the internet. Before applying an attack the attacker takes large number of computer machines under his control over the internet and these computers are vulnerable machines. The attacker exploits these computers weaknesses by inserting malicious code or some other hacking technique so that they become under his control. These vulnerable or compromised machines can be hundreds or thousands in numbers and these are commonly termed as 'zombies.' The group of zombies usually formed the 'botnet.' The magnitude of attack is depends on the size of botnet, for larger botnet, attack is more severe and disastrous.

DDoS attacks in the Internet can be launched using two main methods. In the first method the attacker send some malicious packets to the victim to confuse a protocol or an application running on it (i.e., vulnerability attack [8]). The Second method essentially include the network/transport-level/ application-level flooding attacks [8], in which an attacker to do one or both of the following: (i) interrupt a legitimate user's connectivity by exhausting bandwidth, network resources or router processing capacity or (ii) disrupt services of a legitimate user's by exhausting the server resources such as CPU, memory, disk/database bandwidth and I/O bandwidth.

Nowadays, DDoS attacks are often launched through well organized, remotely controlled, and widely distributed Zombies or Botnet computers of a network, that are continuously or simultaneously sending a huge amount of traffic or service requests to the target system. The attack results the target system either responds so slowly, unusable or crashes completely [8],[9] [10]. Zombies of a botnet are usually recruited through the use of Trojan horses, worms, or backdoors [11]–[13]. It is very difficult for the defense mechanisms to identify the original attacker because of the use of spoofed IP addresses by zombies under the control of the attacker with botnet [14].

Earlier DDoS attacks were manual, in which attacker had to implement many steps before the launch of final attack, which includes port scanning, identifying compromised machines or zombies in the internet to

Author α: Research scholar, Department of CSE, JNTUH, Hyderabad. e-mail: prasadkmv27@gmail.com
Author σ: Professor, Department of CSE, SVUCE,SV University, Tirupati
Author ρ: Professor and Head, Department of CSE, GNITS, Hyderabad.

create botnet, deploying malware etc. Nowadays, sophisticated and automated DoS or DDoS attack tools been developed to assist attackers in implementing all or some steps automatically with minimal human effort to launch these attacks. The attackers can just configure desired attack parameters for a specified attack and the rest is managed by automated tools. Some of the common automated attack tools available are TFN (Tribe Flood Network), Trinoo, TFN2K, Shaft, Stacheldraht, Knight and Trinity. Many of them work on IRC (Internet Relay Chat) in which handlers and zombies communicate indirectly without revealing their identities. The others are agent based where handlers and zombies know each other's identity and communicate direct [9].

II. DDoS Attacks Classification and Architectures

a) *DDoS Motivation*

DDoS attackers are usually motivated by various reasons. We categorized these DDoS attacks based on the motivation of the attackers into seven main classes:

1. *Financial/economical gain:* Attacks launched for financial gain are often, the most dangerous and difficult to stop. These are mainly concern of corporations and require more technical skills and experience.
2. *Invariably slow network performance:* The attacker launches an attack to block the resources of victim system, which slowdowns the performance of the system and intern to the network.
3. *Revenge:* Attackers of this kind are normally with lower technical skills and are frustrated individuals, carry out these as a response to a perceived injustice.
4. *Ideological belief:* Attackers in this category are inspired by their ideological beliefs to attack their targets. This category is currently one of the major incentives for the attackers to launch DDoS attacks.
5. *Intellectual Challenge:* In this, attack the targeted systems for experiment and learn how to launch various attacks. They are usually young hacking enthusiasts who want to show off their competencies.
6. *Service unavailability:* In this attacker overloads the services offered by the victim system through unwanted or fake traffic.
7. *Cyberwarfare:* Attackers of this class is normally belong to the military or terrorist organizations of a country and they are politically motivated to attack a wide range of critical sections of another country.

b) *Classification*

Various classifications of DDoS attacks have been proposed in the literature, when DDoS attacks are classified based on the degree of automation, they are defined as Manual, Semi-automatic and Automatic attacks. In manual approach the attacker had to complete many steps before the launch of final attack, such as port scanning, identifying available machines in the public or private network to build botnet, inserting malware etc. For Semi-automatic or Automatic attacks, various sophisticated attack tools have been developed to support attackers in carrying out all or some steps automatically to reduce human effort. The attackers can configure desired attack parameters and the rest is done by automated tools.

Another classification of DDoS attacks by attack rate i.e., how the rate of attack varies with respect to the time. The classes are Continuous Rate and Variable Rate attacks. The attack has constant flow in continuous rate after it is executed. But as in, variable rate attack changes its impact and flow with time, making it more difficult to detect and respond. Within variable rate, the attack rate can further be applied as Fluctuating or Increasing. Additionally, based on the data rate of attack, traffic in a network is also categorized as high rate and low rate DDoS attacks.

DDoS attacks further classified as 'by impact' i.e., in which the normal service is completely unavailable to users known as Disruptive, or it can be Degrading the services of victim system in which it is not completely unavailable or decrease in the efficiency.

In direct attacks, agents or zombie machines directly attack the victim system as shown in the in Figure. 1. But in reflector attacks, zombies send request packets to a number of other compromised machines (PCs, routers etc.) called Zombies or Bots and the reply generated Zombies is targeted towards the victim system for an impact desired by the attacker. Example for this attack is sending huge amount of traffic as 'ping' request with spoofed IP address to the victim system to saturate bandwidth.

The main classification of DDoS attacks is 'by exploited vulnerability' through which an attacker launches attack on the victim. The classification is given in Fig. 2 .In this classification, flood attack is used to block the victim's machine or network's bandwidth. This can be performed as TCP flood, UDP flood and ICMP flood. In general, all flooding attacks generated through DDoS can as direct attacks or reflector attacks.

c) *DDoS attacks architectures*

DDoS attack networks uses three types of architectures: the Agent-Handler architecture, Internet Relay Chat (IRC)-based architecture and the Web based architecture.

i. *Agent-Handler Architecture*

The Agent-Handler architecture is also referred as Botnet based architecture, in which the attacker uses the botnet to launch an attack. Generally a group of

zombies or bots that are controlled by an attacker (also called as bot Master) form a botnet. Botnets consist of masters, handlers, and bots as shown in Figure 3. The handlers are means of communication that attackers use to command and control indirectly the bots. The handlers can be programs installed by the attackers on a collection of compromised systems (e.g.,Network servers) to send commands to carry out the attack. Bots are devices that have been compromised by the handlers and that will carry out the attack on the victim's system. Figure 4 shows all the elements of a botnet. The owners and users of the bot systems are generally unaware of the situation.

ii. *IRC-based architecture*

The bot master or controller launches an attack through the bots by sending the commands to them which intern behave according to the master instructions. At the other end the bot sends the response or the status information to the master. Their communication is done through public chat systems instead of doing these with their original addresses. If they use the original identity or private channels, the detection system easily track and block the location and system. Internet relay chat (IRC) is the one which allows the users to communicate without performing any authentication check and no security to user communications. IRC provides a text-based command syntax protocol to define the rules and regulations to the users and that is installed widely across the network. There is huge number of existing IRC networks available in the internet and which can be used as public exchange points, but the majority IRC networks doesn't contain any strong authentication. The wide variety of tools in the internet is available to provide anonymity on IRC networks. Therefore, IRC provides simple, low-latency, widely available, and anonymous command and control channel for botnet communication. An IRC network is a collection of one or more IRC servers as depicted in figure 4.

iii. *Web-based architecture*

Botnets are using HTTP as a communication protocol to send commands to the bots making it more difficult to track the DDoS command and control structure. Like IRC-based botnets web-based botnets do not maintain connections with command and control servers or handlers. The Web bots downloads the instructions using web requests periodically. Web-based botnets are stealthier since they hide themselves within legitimate HTTP traffic. Advanced web development languages (PHP, ASP, JSP, etc.) through encrypted communication over HTTP or HTTPS protocol are used to configured and control the bots.

d) DDoS Strategy

A Distributed Denial of Service (DDoS) attack consists of several elements as shown in Figures 1. There are four steps in launching a DDoS attack. These are shown in Figure 5.

1. *Discover vulnerable hosts or agents:* The attacker selects the agents to perform the attack. Any systems which is running with no antivirus software or pirated copies of software in internet is vulnerable and operated as a compromised system. Attackers utilized these compromised hosts or bots for further scanning and compromises .Attacker generates the attack stream by using the abundant resources of these compromised machines.
2. *Compromise:* The attacker exploits vulnerabilities and security holes of the agent machines and installs the attack code.
3. *Communication:* The attacker communicates with the handlers to identify the active agents, to schedule attacks or to upgrade agents. The communication among the attackers and handlers

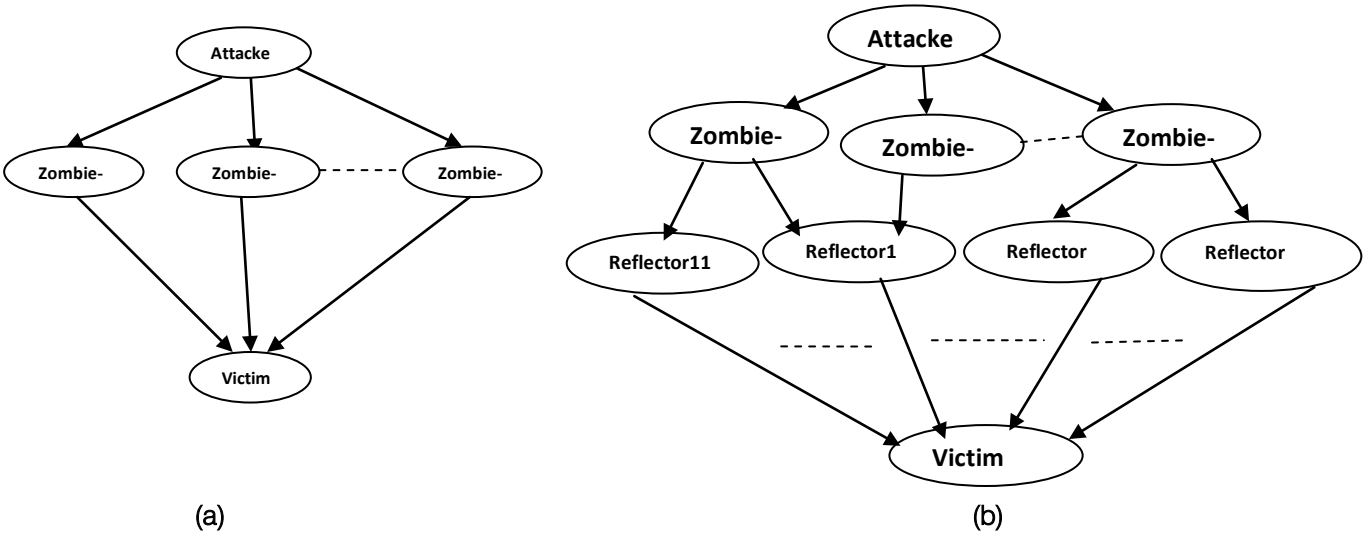


Figure 1 : (a).Direct attack, (b).Indirect attack

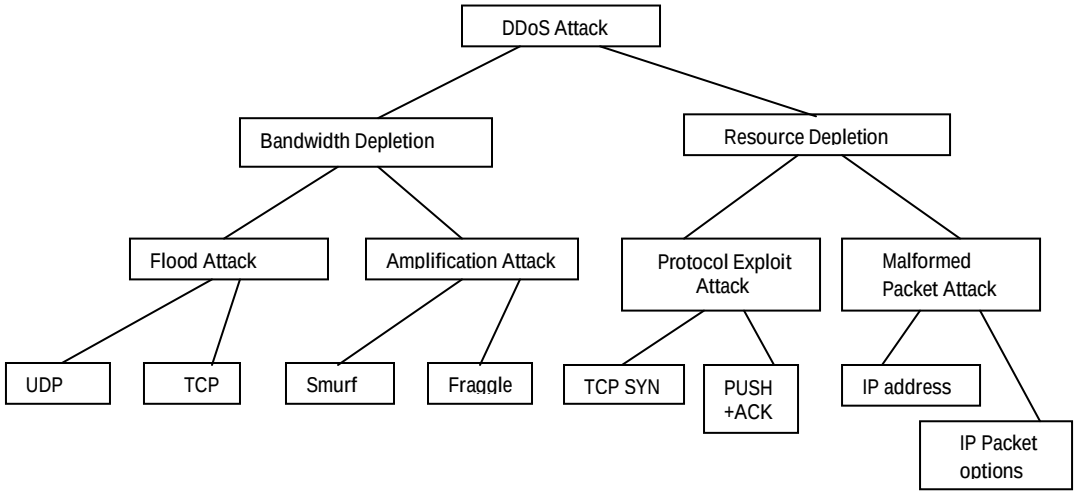


Figure 2 : DDoS attacks Classifications

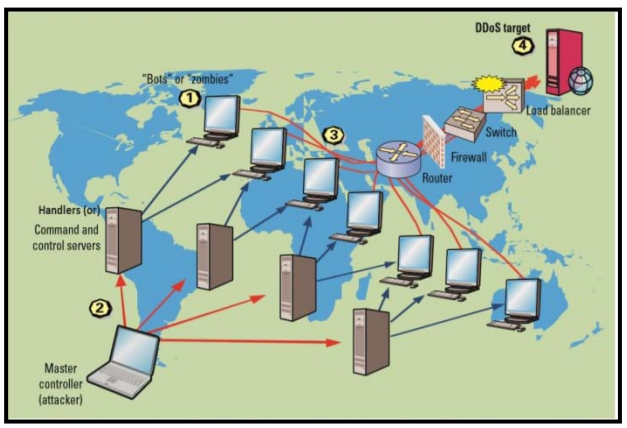


Figure 3 : Agent handler Architecture Figure

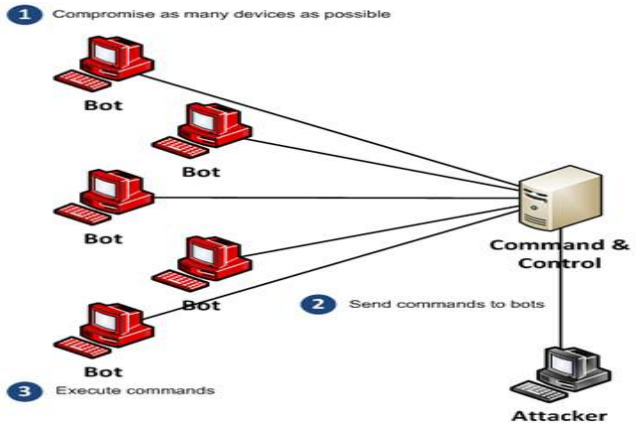


Figure 4 : IRC- based Architecture

can be done through various protocols such as TCP,UDP or ICMP and based on the network configuration with single handler or multiple handlers.

4. *Launching an Attack:* The attacker launches an attack by selecting the victim system, attack duration and adjusting the features of the attack

such as the type, length, Time to Live(TTL), and port numbers.

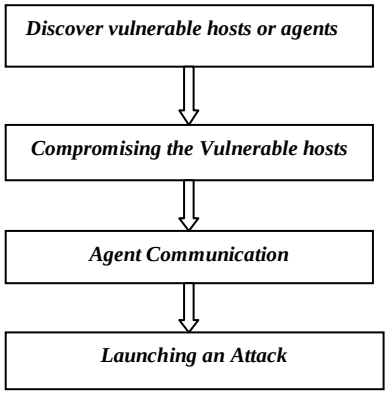


Figure 5 : Phases of performing DDoS attacks

III. DDoS Defense, Detection and Mitigation

a) DDoS Defense Architectures

When a DDoS attack is detected, there is nothing that can be done except manually fix the problem and disconnect the victim system from the network. DDoS attacks blocks a lot of resources such as CPU power, bandwidth, memory, processing time, etc., on the paths that lead to the targeted system. The main goal of any DDoS defense mechanism is to detect DDoS attacks as soon as possible and stop them as near as possible to their sources. DDoS defense schemes are divided into four classes based on the locality of deployment: source-end, victim- end, Core-end or intermediate router and Distributed or Hybrid defense mechanisms. The advantages and disadvantages of all these approaches are given in the table1.

i. *Source-end defense mechanism*

Source-end defense mechanisms are deployed at the sources of the attack to prevent network users from generating DDoS attacks. In this approach, source devices identify malicious packets in outgoing traffic and filter or rate-limit the traffic. Detecting and stopping a DDoS attack at the source is the best possible defense as minimum damage is done on legitimate traffic.

ii. *Victim-end defense mechanism*

In the victim-end defense mechanism, the victim system detects, filter or rate-limit malicious incoming traffic at the routers of victim networks, i.e., networks providing Web services. The legitimate and attack traffic can clearly be distinguished from either online or offline, using either misuse based intrusion detection or anomaly based intrusion detection. However, attack traffic reaching the victim may denied or degraded services and bandwidth saturation.

iii. *Core-end or Intermediate router defense mechanism*

In core-end or intermediate network defense scheme, any router in the network can independently attempt to identify the malicious traffic and filter or rate-limit the traffic. It also balances the trade-offs between detection accuracy and attack bandwidth consumption. Detection and traceback of attack sources becomes easy, due to collaborative operation. In this point of defense, the traffic is aggregated i.e., both attack and legitimate packets arrive at the router and it is a better place to rate-limit all the traffic.

iv. *Distributed-end or Hybrid Defense architecture*

Attack detection and mitigation at distributed ends can be the best strategy against DDoS attacks. The hybrid defense mechanisms are deployed at (or their components are distributed over) multiple locations such as source, Victim or intermediate networks and there is usually cooperation among the deployment points. The core-end is best to rate-limit all kinds of traffic whereas the victim-end can accurately detect the attack traffic in a combination of legitimate and attack packets. Therefore, distribution of methods of detection and mitigation at different ends of the network can be more beneficial.

b) DDoS Detection and Mitigation Strategies

In this section, we present a summary of existing methods on DDoS attack detection and mitigation. These methods are based on the architectures discussed above namely source-end, Victim-end, Core-end and Hybrid mechanisms in the network. We classify methods for DDoS attack detection into four major classes as shown in Figure 6.

i. *Statistical Methods*

Statistical properties of normal and attack patterns can be exploited for detection of DDoS attacks. Generally a statistical model for normal traffic is calculated and then a statistical inference test is applied to determine if a new instance of the traffic or flow belongs to this model. Instances that do not follow the learnt model, based on the applied test statistics results, traffic or flows are classified as anomalies.

Chen et al. [19] develop a distributed change point (DCP) detection architecture using change aggregation trees (CATs). The pre-change and post-change network traffic was described using non-parametric CUSUM approach. The cumulative deviation is higher than random increase when a DDoS flooding attack is launched and CAT mechanism is designed to detect abrupt changes in traffic flows work at router level. The traffic change patterns were detected at the domain server uses attack-transit to construct the CATs, which represent the attack flow pattern.

D-WARD [20] detects an attack based on constant monitoring of bidirectional traffic flows between

the network and the Internet and based on the periodic deviation analysis with the normal flow patterns. Abnormal flows are rate limited in proportion to their arrival rate. D- WARD offers a good detection rate along with the reduction of DDoS attack traffic significantly. It uses a predefined model for normal traffic and detects anomalies in the two-way traffic based on the deviation statistics. Finally, D-WARD notices the traffic for either confirmation of the attack or refutation. If confirmed, D-WARD further controls the rate limit. However, if refuted, it gradually allows increased traffic rate.

Saifullah [21] proposes a defense mechanism by using distributed algorithm that performs weight-fair throttling at upstream routers. The throttling is weight-fair because the traffic intended for the server is controlled (increased or decreased) by using leaky buckets at the routers based on the number of users connected, directly or indirectly to the routers. In the beginning of the algorithm, the survival capacity is underestimated by the routers so as to protect the server from any sudden initial attack. The survival capacity is initialized to minimal or normal values at the beginning of the algorithm and the rate is updated (increased or decreased), based on the server's feedback sent to its child routers and ultimately propagated downward to all routers, in the successive rounds of the algorithm with an assessment to converging the total server load to the acceptable capacity range.

Peng et al. [22] describe a new approach to detect bandwidth attacks by observing the arrival rate of new source IP addresses. The detection system is based on an advanced non-parametric change detection scheme, CUSUM. Cheng et al. [23] propose the IP Flow Feature Value (FFV) algorithm using the vital features of DDoS attacks, such as flow dissymmetry, abrupt traffic change, distributed source IP addresses and concentrated target IP addresses. ARMA prediction model is established for normal network flow using a linear prediction technique. Then a DDoS attack detection scheme based on anomaly detection techniques and linear prediction model (DDAP) is used.

Udhayan and Hamsapriya [24] defines a Statistical Segregation Method (SSM), by sampling the flow in consecutive intervals and compares the samples with the attack state condition and sorts them based on the mean parameter. Attack flows from legitimate flows are segregated using correlation analysis.

In [25], a generic DoS detection scheme was introduced based on maximum likelihood criterion with random neural networks (RNN). This approach initially selects a set of traffic features in offline mode to obtain pdf estimates and to evaluate the probability ratios. It measures the features of incoming traffic and attempts to decide according to each feature to take decision. Lastly, it obtains an overall decision using both feed-forward and recurrent architectures of the RNN. A brief summary of these methods is given in Table 1.

In [26], authors present a lightweight tunnelling protocol called LOT, to prevent network traffic against IP spoofing and flooding attacks. It is deployed at network's communication gateways. Two gateways with LOT implementation can detect each other and create the tunnel between them to secure communication. The protocol allows the gateway to discard spoofed IP packets which specify source addresses in other gateway and vice versa and communication can be protected from any type of DDoS attacks. The use of per-flow quotas to identify flooding of packets from different networks mitigation the DDoS attacks. The LOT protocol not only passes restricts spoofed packets to destination and also filter packets based on filtering rules determined by destination gateway.

In [27], authors attain DDoS detection with enhanced time limits through non-asymptotic fuzzy estimators. The estimator is deployed on mean packet inter-arrival times. The problem is divided into two parts; one is actual DDoS detection and the other is identification of victim IP addresses. The first part is achieved using strict real time limits for DDoS detection. The second part i.e., identification of victim IP addresses is attained through comparatively relaxed constraints. The goal is to identify victim IP addresses in a timely manner to launch added anti intrusion applications on offended hosts using packet arrival time as the main statistic of DDoS attack determination.

A game theoretic approach is followed in [28] to offer defense against DoS/DDoS cyber-attacks. The DDoS attack is modelled as a one-shot & zero-sum game with non-cooperation. To perform an attack, multiple features are investigated in terms of cost with malicious traffic distribution and number of attackers. It is validated in analytical terms that a single optimal strategy of defense is available to defender in which upper boundaries are set to attacker payoff depending upon the rational or irrational attackers. Table 2 presents a brief summary of the Statistical based DDoS detection methods.

ii. *Soft computing based methods*

Learning paradigms, such as Artificial Neural Networks (ANNs), radial basis functions and genetic algorithms are widely used in DDoS attack detection because of their ability to classify intelligently and automatically. Soft computing is a method of describing a set of optimization and processing techniques that are tolerant of imprecision and uncertainty.

Artificial Neural Networks (ANNs) are widely used learning models with their ability to cope with demands of a changing environment [32]. These ANNs are self-learning and self-organizing models with the features like robustness, fault tolerance and parallelism. ANNs are good to identify and resist unknown disturbances in a system because of its self-learning characteristic.

In [33], authors use Linear Vector Quantization (LVQ) model of ANN. It is same as self-organizing maps and applied the techniques of pattern recognition, multi-layer classification and data compression. In supervised learning, it knows the target output against different forms of various input patterns. After testing the system with LVQ model, authors use the same dataset with Back propagation (BP) model of ANN for comparative study. On the basis of comparison results, they claim that LVQ is more accurate in determining DDoS attacks than BP. They show that LVQ is 99.723% accurate on average against tested dataset whereas the average accuracy of BP is 89.9259% for the same dataset. Accuracies are computed on the basis of percentages of obtained false positives and false negatives against each sample of testing data. There are 10 samples used to test the systems for each of the LVQ and BP models.

In [34], authors train the BP neural network with a traffic entropy variations dataset as inputs and DDoS strengths as outputs. 20 different samples in the dataset are used for training with 10Mbps attack strength as the lowest and 100Mbps being the highest in the dataset. The entropy variations are calculated based on an assumption that the attack traffic is seen different in the network from normal traffic. The model is tested with random inputs of four entropy variations and calculated attack strengths respectively as 20, 50, 70 and 95Mbps. The BP neural network's output is obtained with little errors. False positives and false negatives are very less and also the system is tested with variations in network size i.e., number of neurons in processing layer but in real cases, increasing the network size also increases both training time and implementation cost.

In [35], authors propose Time Delay Neural Network (TDNN) to acquire early warning system against DDoS attacks. TDNN is a neural network in which time delay factor is hidden inside the representative signal. The authors created a Demilitarized Zone (DMZ) and TDNN is implemented in two-layer pattern. The node action is monitored by neighboring nodes and attack information is sent to the expert module for integrated analysis. The layered structure enables the system to ensure some appropriate actions as a proactive strategy against DDoS attacks. The detection results on deployed architecture show that proposed scheme is able to give 82.7% correct detection rate as compared to 46.3% with general Intrusion Detection System (IDS).

Jalili et al. [36] introduce SPUNNID as DDoS attack detection system based on a statistical pre-processor and unsupervised artificial neural network. It use statistical pre-processing to extract features from the traffic, and uses an unsupervised neural network to analyse and classify traffic as an attack or normal traffic.

Karimazad and Faraahi [37] propose an anomaly-based DDoS detection method using Radial Basis Function (RBF) neural networks based on features of attack packets analysis. It is applied to classify data as normal or attack categories. If the incoming traffic is identified as attack traffic, the attack packets source IP address are sent to the Filtering Module and the Attack Alarm Module performs further actions. Otherwise, if the traffic is normal, it is directed to the destination.

Gavrilis and Dermatas [38] present a detection method for DDoS attacks in public networks based on statistical features estimated in short-time window analysis of incoming data packets. A small number of statistical parameters are used to define the behavior of the DDoS attacks. An accurate classification is achieved using Radial Basis Function neural networks than this.

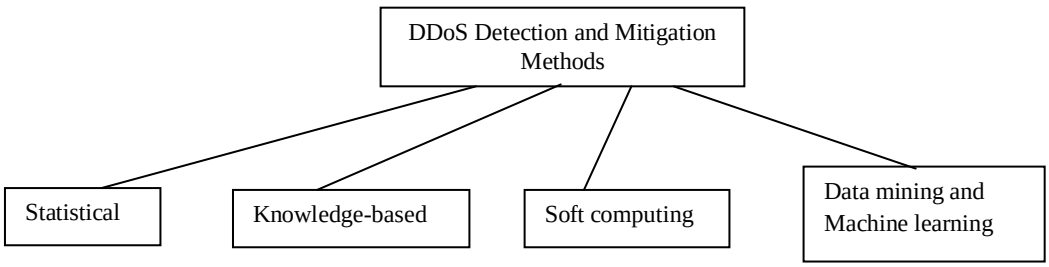


Figure 6 : DDoS Detection and Mitigation methods

Table 1 : Comparison of DDoS attack Defense architectures

Defense Method	Advantages	Disadvantages
Source-end Defense Architecture	• Detecting and stopping a DDoS attack at the source provides best possible defense as minimum damage is done on legitimate traffic. • Minimum amount of traffic to be checked at source point for which fewer resources are required by the detection & mitigation mechanism.	• Detecting DDoS attacks at source end is difficlut because sources are widely distributed across the network and a single source behaves like a normal traffic. • The difficulty of deploying system at the source end.
Victim-end Defense Architecture	• Detecting DDoS attacks in victim routers is relatively easy because of the high rate consumption of resources. • Best practically applicable type of defense scheme as Web servers providing critical services always try to secure their resources for legitimate users.	• During DDoS attacks, victim resources, e.g., network bandwidth, often gets over- whelmed and these approaches cannot stop the flow beyond victim routers. • Detect the attack only after it reaches the victim and detecting an attack when legitimate clients have already been denied is not useful.
Core-end Defense Architecture	• Detection and traceback of attack sources are easy in this approach due to collaborative operation. • The traffic is aggregated i.e., both attack and legitimate packets arrive at the router and it is a better place to rate-limit all the traffic.	• Deployment is the main difficulty with this approach. • To attain full detection accuracy, all routers on the Internet will have to follow this detection scheme, because unavailability of this scheme in one router may cause failure to the detection and traceback process. • Full practical implementation is extremely difficult because it requires the reconfiguration of all the routers on the Internet.
Distributed-end or Hybrid Defense architecture	• Detection can be done at the victim side and the response can be initiated and distributed to other nodes by the victim. • Distribution of methods of detection and mitigation at different ends of the network can be more beneficial.	• Strong cooperation among the deployment points is required. • Complexity and overhead because of the cooperation and communication among distributed components scattered all over the Internet.

Wu et al. [39] proposes detection of DDoS attacks using decision trees and grey relational analysis. The detection of the attack from the normal state is defined as a classification problem. They use 15 attributes, to monitor the incoming/outgoing packet/byte rate, and also collect the TCP, SYN, and ACK flag rates, to define the traffic flow pattern. The decision tree method is used to develop a classifier to detect abnormal traffic flow and also use a novel traffic pattern matching procedure to identify traffic flow similar to the attack flow and to trace back the origin of an attack.

In [42] the authors proposes ensemble of classifiers which uses the Resilient Back Propagation (RBP) neural network as the base classifier for DDoS Detection. They are mainly focussed on improvement of the performance of the base classifier. The RBPBoost combines the output of the ensemble of classifier outputs and Neyman Pearson cost minimization strategy [43], for final classification decision. Table 3 presents a brief summary of the soft computing.

Table 2 : Statistical based DDoS Detection methodsReference

Reference	Objective	Deployment	Working Mode	Remarks
Mirkoviac al. et[20]	Attack prevention	Source side	Centralized	Statistical traffic modelling is used to Detect DDoS attacks and blocks the attack traffic when it is detected at source end.
Akella.et al.[31]	Attack detection	Source and victim side	Distributed	A profile is constructed from normal traffic and detects anomalies in the traffic using stream sampling. In general this approach used in the network routers.
Prasad, ARMReddy, KVGRrao[41]	Attack detection	victim side	Distributed	Modeling and Counter measures of Flooding attacks to ITM using Botnet and Group Testing.
Peng.et al.[22]	Detecting bandwidth attacks	Victim side	Centralized	Sequential nonparametric change point detection method is used to improve the detection accuracy and employed at victim end.
Chen.et al.[19]	Attack detection and Traceback	Between source and destination network	Distributed	Hybrid approach which is used to detect and trace back the attack source.
Oke and Loukas [25]	Attack detection	Victim side	Centralized	Defines a set of attack specific input features that captures the behavior and the long term statistical properties of the traffic during detection.
Saifullah[21]	Attack prevention	Between source and destination network	Distributed	Prevention method which protects Internet servers and routers from DDoS attacks using distributed weight-fair throttling from the upstream routers.
Chen[29]	Attack detection	Victim side	Centralized	Detects DDoS attacks using two-sample t-test by integrating the statistics of SYN arrival rate.
Zhang.et al.[30]	Attack detection	Victim side	Centralized	Uses an Auto Regressive Integrated Auto Regressive (ARIMA) model for protecting servers from DDoS attacks.
Cheng.et al.[23]	Attack detection	Victim side	Centralized	Activities four flow features: asymmetry of the flow, burst in the traffic volume, distributed source IP destination IP address while detecting DDoS attacks.
Udhayanand Hamsapriya[24]	minimize false alarm	Victim side	Centralized	Statistical segregation method is used to detect DDoS attacks based on sampling of traffic flow in consecutive time interval.

Table 3 : Soft computing based DDoS Detection methods

Reference	Objective	Deployment	Working Mode	Remarks
Jalili.et al[36]	Attack detection	Victim side	Centralized	Statistical preprocessor and unsupervised neural network classifier methods were used for DDoS attack detection.
Gavrilis &Dermatas[38]	Attack detection	Victim side	Centralized	Detects DDoS attacks using statistical features estimated in short time interval in public network with Radial basis function of neural network.
Nguyen and Choi[40]	Attack detection	Intermediate network	Centralized	K-nearest neighbour based technique is used to detect only known attacks.
Wu et al. [39]	Attack detection and traceback	Victim side	Distributed	Trace back to the attacker location based on traffic flow pattern matching using decision trees.

Karimazad And Faraahi[37]	Attack detection	Victim side	Centralized	Low false alarm rate can be achieved using Radial Basis Function (RBF) neural networks.
Kumar and Selvakumar[42]	Attack detection	Victim side	Centralized	High detection rate in RBP Boost can be achieved using the combination of an ensemble of classifier outputs and Neyman Pearson cost minimization strategy.

methods presented in this section. Table 3 presents a brief summary of the soft computing methods presented in this section.

iii. *Knowledge based Methods*

In knowledge-based approaches, network events or actions are tested against predefined rules or patterns of attack. In these, general representations of known attacks are called as attack signatures and these are formulated to identify actual occurrences of attacks. Knowledge-based approaches include expert systems, signature analysis, self-organizing maps, and state transition analysis.

Gil and Poletto [44] present a heuristic data structure named as MULTOPS (MUlti-Level Tree for Online Packet Statistics), that monitor traffic characteristics of network devices like routers to detect and eliminate DDoS attacks. MULTOPS is a tree of nodes which includes traffic rate statistics for subnet prefixes at different aggregation levels and was expansion and contraction of the tree occurs within a pre-specified memory size. A MULTOP of network device detects bandwidth attacks by the occurrence of a significant difference between traffic rates going to and coming from the victim or the attacker. Routers or network monitors equipped MULTOPS may fail to detect a bandwidth attack that is fixed by attackers that randomizes IP attack source addresses on malicious packets. It also fails to detect attacks that deploy a large number of attack flows to explode a victim.

Thomas et al. [45] introduces a practical approach with high performance DDoS defense mechanism called as NetBouncer. It distinguishes legitimate and illegitimate use of resources and ensuring that are made available only for legitimate use. It allows traffic to flow with respective to a long list of recognized legitimate clients and if packets are received from a source not on the legitimate list, a NetBouncer device invite administer to perform variety of legitimacy tests to test the client to prove its legitimacy. If a client proved its authorization, it is added to the legitimacy list and subsequent packets from the client are accepted.

Wang et al. [46] present a methodical way of modeling DDoS attacks using Augmented Attack Tree (AAT), and implemented an AAT-based attack detection algorithm. It explicitly captures the specific subtle incidents triggered by a DDoS attack and the corresponding state changes from the observation of the network traffic transmission on the primary victim server. With reference to the conventional attack tree (CAT) modeling method, AAT is advanced because it provides additional information like the state transition process. It overcomes the limitations of CAT modelling.

Limwiwatkul and Rungsawang [47] discover DDoS attack signatures by analysing the TCP/IP packet header against pre defined rules and conditions, and differentiating the difference between normal and abnormal traffic flow. These mainly focus on ICMP, TCP and UDP flooding attacks.

Zhang and Parashar [48] introduced a distributed approach to defend against DDoS attacks in the Internet. To detect DDoS attacks independently, defensive systems are deployed in the network, unlike traditional IDS, this method detects and stops DDoS attacks within the intermediate network. An IRC communication is used between these independent detection nodes to exchange information about network attacks and combined this information for aggregate network attacks. Individual defence nodes obtain estimated information about global network attacks and stop the attacks more effectively and accurately using the aggregated information of network. An earlier approach depends on monitoring the volume of traffic received by the victim and these are incompetent of distinguishing a DDoS attack from a flash crowd.

Lu et al. [49] defines a perimeter-based DDoS defese system, in which the traffic is analyzed at the edge routers of an Internet Service Provider (ISP) network. The DDoS defense system consists of two major components: (1) temporal-correlation based feature extraction and (2) spatial-correlation based detection. It accurately identifies and detect DDoS attacks without changing existing IP forwarding mechanisms at routers. A brief summary of these knowledge based methods is given in Table 4.

iv. *Data mining and machine learning methods*

In [50] the authors proposed an effective defensive system called as NetShield to protect client hosts, network routers and network servers from becoming victims, zombies and handlers of DDoS flood attacks. It protects any IP-based public network on the Internet and uses preventive and rate limiting to eliminate system vulnerabilities on target machines. It enforces dynamic security policies for protecting network resources against DDoS flood attacks.

Chen et al. [51] introduces DDoS Container as a comprehensive framework for DDoS attack detection. It uses a network based detection method to defense complex and simple types of DDoS attacks and works in parallel to inspect and control ongoing traffic in real time. It covers stateful inspection on traffic flow streams

and correlates actions among different sessions by continuous monitoring of both DDoS attacks and legitimate applications. It terminates the session when it detects a DDoS attack.

Lee et al. [52] propose proactive detection method for DDoS attacks by exploiting an architecture comprising of a selection of handlers and agents that communicate, compromise and attack. It performs cluster analysis. The authors presented the results using the DARPA dataset, were each phase of the attack scenario is segregated well and can detect originators of a DDoS attack as well as the attack itself.

Sekar et al. [53] inspect the design space for in-network DDoS detection and propose a triggered, multi-stage approach that addresses both scalability and accuracy. They designed and implemented the LADS (Large-scale Automated DDoS detection System), which makes effective use of the data readily available to an ISP.

Rahmani et al. [54] designed a joint entropy analysis of for DDoS attack detection using multiple traffic distributions. The time series of IP- flow numbers and aggregate traffic sizes are statistically dependant and were this occurrence of an attack affects the dependence and causes a break in the time series for joint entropy values.

A low-rate DDoS attack detection difficult compared with the Normal attacks because of its similarity with normal traffic. In [55] defined two new information metrics: (i) generalized entropy metric and (ii) information distance metric, to detect low- KK DDoS attacks. The attack is detected based on the distance between legitimate and attack traffic. The generalized entropy metric is more accurate than the traditional Shannon metric [56].

In [57] early detection of flooding DDoS attacks are defined using FireCol, which is based on information theory. It is deployed in Internet service provider (ISP) level as a part of intrusion prevention system (IPS). The IPSs create virtual protection rings around the hosts to defend and cooperate by exchanging specific traffic information.

The approach described in [58] analyses characteristics of DDoS and flash crowd attacks and provides an efficient way to distinguish between the two in VoIP networks. The authors validated the method through simulation.

In [59] the authors present a wavelet transformation and probability theory based network anomaly detection approach. It is able to identify known as well as unknown DDoS attacks.

Zhong and Yue [60] implemented a DDoS attack detection model which extracts a network traffic and a network packet protocol status models and defines the threshold for the detection model. K-Means clustering algorithm is used to build initial threshold values for network traffic of Captured network traffic values. Packet protocol status model is built using Apriori [61] and FCM [62] for captured packets. When the current network traffic exceeds the threshold value, the network packet protocol status is checked to identify abnormal packets. If there are no abnormal packets exist, a new threshold value model is build based on the current network using k-means module.

A two-stage automated detection system is proposed in [63] for DoS attacks in network traffic. It is the combination of traditional change point detection method with wavelet transforms [64]. In [65], Li and Lee present a systematic wavelet based method for DDoS attack detection. DDoS attack traffic is detected using energy distribution based on wavelet analysis. Energy distribution over time has limited variation if the traffic keeps change its behavior over time.

Gupta et al. [66] use ANN to identify the number of zombies in a DDoS attack. Sample data is used to train a feed-forward neural network created using the NS-2 network simulator. The generalization capacity of the trained network is capable and it is able to calculate the number of zombies involved in a DDoS attack with test error.

Cheng et al. [68] proposes the IP Address Interaction Feature (IAI) algorithm considering abrupt traffic changes, interactions among addresses, many-to-one asymmetries among addresses, distributed source and concentrated target addresses. The IAI algorithm is designed to describe the critical characteristics of network flow states. A support vector machine (SVM) classifier, which is trained by an IAI time series with normal and attack flows, is applied to classify the state of current network flows and identify the DDoS attacks. It has higher detection and lower false alarm rates compared to competing techniques.

The method defined in [69] identifies flooding attacks in real time and also assess the strength of the attackers based on fuzzy reasoning. This process consists of two stages: (i) statistical analysis of the network traffic time series and (ii) identification and assessment of the strength of the DDoS attack based on an intelligent fuzzy reasoning mechanism.

Zhang et al. [70] define a Congestion Participation Rate (CPR) based approach for flow level network traffic to detect

Table 4 : Knowledge based DDoS Detection methods

Reference	Objective	Deployment	Working Mode	Remarks
Gil and Po-Letto [44]	Attack prevention	Between source and destination network	Centralized	Each network device maintains a MULTOPS data structure to detect attacks that deploy a large number of DDoS attack flows using a large number of agent and IP spoofing attacks.
Thomas et al.[45]	Attack detection	Victim side	Centralized	Inline packet processing is used by the Net Bouncer to differentiate DDoS traffic from flash crowd based on network processor technology.
Limwiwatkul & Rung-Sawang[47]	Attack detection	Victim side	Distributed	Attack signature models are constructed using TCP packet headers for DDoS attack detection.
Zhang and Parashar[48]	Proactive	Intermediate network	Distributed	A gossip based scheme uses global information about DDoS attacks by information sharing to detect attacks.
Lu et al.[49]	Attack detection	Edge router	Distributed	Exploits spatial and temporal correlation of DDoS attack traffic for detecting anomalous packet.
Wang.et. al[46]	Attack detection	Victim side	Centralized	Augmented Attack Tree model is used for the detection of DDoS attacks.

Table 5 : Datamining and machine learning based DDoS Detection methods

Reference	Objective	Deployment	Working mode	Remarks
Hwang et al.[50]	Attack prevention	Victim side	Centralized	Protects network clients, routers and servers from DDoS attacks using protocol anomaly detection
Li and Lee[52]	Attack detection	Victim end	Centralized	An energy distribution based wavelet analysis technique defined for the detection of DDoS traffic.
Sekar.Et.al[53]	Attack detection	Source side	Distributed	A triggered multi-stage approach is defined to acquire scalability and accuracy for DDoS attack detection.
Gelenbe and Loukas[73]	DDoS defense	Victim end	Centralized	Detects attack by tracing back flows automatically.
Lee et al.[62]	Attack detection	Source side	Centralized	Agent handler architecture along with cluster analysis is used to Detects DDoS attack proactively.
Rahmani et al[54]	Attack detection	Victim side	Distributed	A joint entropy analysis used for multiple traffic distributions to detect DDoS attacks.
Li and Li[65]	Attack detection	Victim end	Centralized	Wavelet transformation and probability theory are used to detect DDoS attacks
Dainotti et al[63]	Detection of DoS attack anomalies	Victim end	Centralized	Detects attacks accurately using combination of traditional change point detection and continuous wavelet transformation.
Zhong and Yue[60]	Attack detection	Victim side	Centralized	Unknown DDoS attacks are detected using fuzzy c-means clustering and Apriori techniques.
Xia et al. [69]	Detects flood attack and its intensity	Victim end	Centralized	Detection of DDoS flooding attack using fuzzy logic.

Xiang et al[55]	Detects low rate flooding attacks	Victim end	Centralized	New information metrics used to detect low-rate DDoS flooding attacks.
Gupta et al.[66]	Number of zombies identification	Victim end	Distributed	Uses ANN to evaluate the number of zombies in a DDoS attack.
Francois et al.[57]	DDoS flooding attack detection	Source end	Distributed	A DDoS flooding attack detection technique supports incremental deployment in real network.
Jeyanthi and Iyengar[58]	Flash crowd Detection	Victim end	Centralized	Detects DDoS attacks using entropy based analysis.
Prasad, ARMReddy ,KVGRao[15]	Flash crowd Detection	Router/ITM level	Distributed	Detects DDoS attacks using entropy variations.

low-rate DDoS (LDDoS) attacks. A flow of higher CPR value leads to LDDoS and subsequent dropping of the packets. It identifies DDoS attacks with high detection accuracy using correlation of subset of features.

In [71], authors defined an approach to detect botnet and their activities based on traffic behaviour analysis. Machine learning strategies are used to classify traffic behaviour and proved experimentally that botnet activities can be identified in smaller time windows with high accuracy.

In [72], low-rate DDoS attacks are detected using anomaly based approach. In low-rate DDoS attacks methods, attackers send malicious traffic at lower transmission rate to mislead traditional anomaly based DDoS detection techniques. The authors proposed two information metrics, generalized entropy metric and information distance metric. These metrics are used to measure difference between legitimate traffic and attack traffic to detect DDoS attacks.

In [73], a mathematical model is proposed to provide the benefits of DDoS defence based on dropping of attack traffic. The authors used an autonomic defence mechanism based on Cognitive Packet Network (CPN) protocol to tracing back flows coming into a node automatically. A summarized presentation of these methods in this category is given in Table 5.

IV. Traceback Mechanisms

Identifying attack source(s) through some mechanism to block or mitigate the attack at origin is referred as Traceback in DDoS defense. Implementing the traceback to identify DDoS source accurately is difficult because of, easy spoofing of source IP addresses, stateless nature of IP routing without knowing the complete path, link layer or MAC address spoofing and modern attack tools provides to implement intelligent attack techniques easily [74].

In [75], authors calculated entropy variations of network traffic to implement a traceback scheme. To detect an attack the difference of entropy values between normal traffic and the DDoS attack traffic is calculated. If the attack is detected, the traceback is initiated towards its upstream routers. The proposed scheme provides an advantage over traditional traceback approaches in terms of scalability and storage requirements in victim or intermediate routers. It stores only short-term information i.e, entropy values of successive time intervals in order to detect the DDoS attack.

In [76], authors presents a method for detection and traceback of low-rate DDoS attacks ,where low-rata attacks are very much similar to normal traffic and have more ability to hide their attack related identities in the aggregate traffic. Two new information metrics were introduced to detect low-rate DDoS attacks, which are generalized entropy metric and information distance metric. In this approach, difference between legitimate and attack traffic is identified through the proposed information metrics and are capable to detect the attack in prier hops earlier than counts mentioned in proposed schemes. These information metrics increase detection accuracy of the system and is capable of identifying low-rate DDoS attacks effectively by reducing false positive rates.

In addition to entropy variation scheme, other traditional reactive methods also exist to traceback DDoS attack sources [74]. In packet marking scheme, trace the path through upstream routers towards the attack sources i.e., zombies. It is a standard technique used in traceback implementations, however contains some inherent drawbacks. There exits two types of packet marking schemes i.e., probabilistic and deterministic packet marking.

In probabilistic packet marking (PPM), every router inserts its IP address probabilistically into the packets moving from source to destination. The method relies on the assumption that attack packets more frequent than legitimate packets. Once the attack is detected, the victim requests sufficient range of packets to reconstruct the path upto the attack source through embedded information within the packets. There is no specific fields defined in an IP packet for markings. Therefore, it utilizes infrequently used 16-bit fragment ID in IP packets for the markings [78]. However, this method has some major drawbacks. For instance, it is valid just for direct attacks. It cannot detect the original location of attack source just in case of reflector attacks

because the traced location is of reflector machines and not the actual zombies. Moreover, in a well distributed attack with a reasonably sizable amount of zombies, the possibility of wrong construction of the path increases. It's additionally an acknowledged indisputable fact that nowadays, due to large number of zombies, the attackers reveal real IPs of zombie machines and hence the sources are already discovered. The packet marking scheme places computational overhead on intermediate routers when traceback is initiated. In addition that victim remains available during the process of traceback to send control messages to upstream routers. The bandwidth is saturated due to attack impacts the control messages are dropped, it leads to wrong construction or misconstruction of attack path.

Table 6 : Trceback mechanisms of DDoS attacks

Existing mechanisms	Traceback Working Principle	Advantages	Drawbacks
Hash Based IP Traceback	20 byte IP header and first 8 bytes of payload is logged for every packet by the Intermediate routers. Hashing is performed on the logged data.	It requires low storage and protects from eavesdropping.	Increases the false positives and Overhead in generating 28 byte hash for the packets.
Algebraic approach to IP traceback	Polynomial functions are used to generate traceback data and stores in unused bits of IP header.	Noise elimination and multiple path reconstruction are possible and robustness is improved.	Variations will occur in random full path tracing schemes and poor scaling.
Enhanced ICMP traceback-Cumulative path[77]	Intermediate routers generate Itrace-CP message. The victim uses this message to trace the attack path and source.	In less time it constructs an entire attack path.	A change to be made to the router and space is required to process packets.
Advanced and Authenticated scheme for IP Traceback.	Traces the origin of IP packet with 11 bit hash and distance field of 3 bits are generated using 32 bit IP address and stored in IP header.	Low overhead on router and network and computational complexity is very less.	No time synchronization between victim and the router and Secret key is shared between routers.
Fast Internet Traceback	A packet marking scheme and path reconstruction algorithms are used at routers and end hosts to receive the packet markings.	Minimal Processing time is required to traceback the attack source for less flow.	False positive rates are high.
Deterministic packet marking [78]	The source of an attack flow is identified by employing tracing information inscribed in the packet.	Traceback process requires small number of packets.	No overload prevention and Increase in packet header size.
Probabilistic packet marking [78]	Routers mark the packets with probabilistic path information and victim reconstructs the attack graph.	Efficiency and easy implementabilty over Deterministic Packet Marking.	More number of packets and computational work involved in traceback process. Probability of finding the source traced is low.
Flexible Deterministic Packet marking [74]	Large scale IP Trace back scheme which encodes the information and reconstruction the attack path using mark recognition.	Traceback process requires relatively less number of packets and minimal Computation work. Probability of finding a source is high.	Packet processing consumes more resources.
IP Traceback for Flooding attacks on Internet Threat Monitors (ITM) Using Honeypots[16]	Honeypots are used as the proxy servers and the attack source is traced through honeypot entries.	Low overhead on server and no direct damage to the server.	Processing delay and cost consuming process for honeypots.
Decision tree and grey relational	Decision trees are constructed for the traffic flow with respective upstream routers and analyses the	Upstream routers can be easily identified for attack strength.	Complicated process when for the large size network.

analysis[18]	attack strength.		
New information metrics[17]	Information distances are calculated for each flow in the network.	Less computational complexity for calculating the information distance.	Accurate detection is not possible.

In deterministic packet marking (DPM), the router inserts its IP address deterministically into the IP packets. This scheme was introduced to overcome the drawbacks of probabilistic packet marking, because it has easy implementation and needs less computational overhead on intermediate routers. However, it also has the limitations. In this scheme, packets are marked only by first ingress edge router with the information i.e., the entire is not stored as in PPM. Therefore, it needs even additional packets to reconstruct the attack path [74]. Furthermore, it additionally has some limitations similar to PPM scheme discussed above. This approach is less efficient than traditional schemes.

In packet logging scheme [74] which is also referred as Source Path Isolation Engine (SPIE), the information of each packet is stored or logged at routers through which the packet is passed. The routers in this approach are termed as Data Generation Agents (DGAs). The stored information of the packet includes constant header fields and first 8 bytes of the digests (payload hashed through many hash functions). Bloom filters are used to store these DGAs, which is a space-efficient data structure and is capable of reducing storage requirements by large magnitude.

In ICMP messaging scheme [77], routers are programmed to send ICMP messages together with the network traffic. The ICMP packets contain path information such as source address, destination address and authentication parameters etc. A typical router with this scheme normally sends one ICMP messaging packet for every 20,000 packets passing through it i.e., a traceback message is sent with the proportion of 0.005 percent of the network traffic [74]. A summarized presentation of these methods in this category is given in Table 6.

V. Conclusion and Future Work

In this paper, we have presented a broad classification of various DDoS attacks, DDoS Defensive architectures such as Source-end, Victim-end and Intermediate architectures. We have also presented various Detection and mitigation mechanisms such as Statistical based, Soft-computing based, Knowledge based and Data mining based approaches along with their advantages and disadvantages based on where and when they detect and respond to DDoS attacks. Finally, we presented an overview of traceback mechanisms of DDoS attacks such as packet marking schemes, information distance, honey pots and entropy variations. Practically it is very difficult to design and implement DDoS defense and detection. In real time networks, fulfilling all the requirements for DDoS detection is not possible and to accomplish this, various performance parameters need to be balanced against each other delicately and appropriately.

References Références Referencias

1. T. Peng, C. Leckie, , and RMrao, K. “Survey of network-based defense mechanisms countering the DoS and DDoS problems.”, ACM Computing Survey, 39, 3:1–3:42. (2007),
2. V. Chandola,, A. Banerjee, , and V. Kumar, ,“Anomaly detection: A survey. ACM Computing Survey,” 41, 15:1–15:58. (2009)
3. G. Loukas, and ¨G. Oke, “Protection against denial of service attacks: A survey.” Computer. Journal. 53, pages-1020–1037. (2010)
4. M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita “Surveying port scans and their detection methodologies.” Computer. Journal., 54, Pages-1565–1581. ,(2011)
5. H. J. Kashyap, and D. K. Bhattacharyya “,A DDoS attack detection mechanism based on protocol specific traffic features.”, Proceedings of the Second International Conference on Computational Science, Engineering and Information Technology, Coimbatore, India, 26-28 October, pp. 194–200. ACM. , (2012)
6. S.Lin, and T.C.Chiueh “A survey on solutions to distributed denial of service attacks.”, Technical Report TR201. Department of Computer Science, State University of New York, Stony Brook. ,(2006)
7. P. J. Criscuolo, “Distributed Denial of Service, Tribe Flood Network 2000, and Stacheldraht CIAC-2319,”, Department of Energy Computer Incident Advisory Capability (CIAC), UCRL-ID-136939, Rev. 1., Lawrence Livermore National Laboratory, February 14, 2000.
8. J. Mirkovic and P. Reiher, “A taxonomy of DDoS attack and DDoS defense mechanisms,” ACM SIGCOMM Computer Communications Review, vol. 34, no. 2, pp. 39-53, April 2004.
9. Ranjan. S, Swaminathan. R, Uysal. M, and Knightly. E, “DDoS-Resilient Scheduling to Counter Application Layer Attacks under Imperfect Detection”, IEEE INFOCOM’06, 2006.
10. Chang R. K. C., “Defending against flooding-based distributed denial of service attacks: A tutorial,”, Computer Journal. IEEE Communication Magazine, Vol. 40, no. 10, pp. 42-51, 2002.
11. Puri. R, “Bots and Botnet – an overview,”, Aug. 08, 2003, [online] http://www.giac.org/practical/GSEC/Ramneek Puri GSEC.eps

12. Todd B., "Distributed Denial of Service Attacks," Feb. 18, 2000, [online] http://www.linuxsecurity.com/resource files/intrusion detection/ ddos–whitepaper.html
13. CERT, "Denial of Service Attacks," June 4, 2001, [online] http://www.cert.org/tech tips/denial of service.html
14. Liu. J, Xiao. Y, Ghaboosi. K, Deng. H, and J. Zhang, "Botnet: Classification, Attacks, Detection, Tracing, and Preventive Measures,", EURASIP Journal. Wireless Communications and Networking, vol. 2009, Article ID 692654, 11 pages, 2009.
15. K Munivara Prasad, Dr. A Rama Mohan Reddy and Dr K Venugopal Rao, Discrimination of Flash crowd attacks from DDoS attacks on internet threat monitoring (ITM) using *Entropy variations*, IEEE African Journal of Computing & ICT , Vol 6. No. 2, pp- 53-62, June 2013.
16. K Munivara Prasad, Dr. A Rama Mohan Reddy , IP *Traceback for Flooding attacks on Internet Threat Monitors (ITM) Using Honeypots* , International journal of Network Security & Its Applications (IJNSA),ISSN : 0974 - 9330, Vol.4, pp 13-27, No.1,Jan 2012.
17. Y. Xiang., Li, K., and Zhou,, "Low-rate DDoS attacks detection and traceback by using new information metrics, " IEEE Transaction on Information Forensics. Vol: 6, pages: 426–437, 2011.
18. Y. C Wu,., Tseng, H. R., Yang, W., and Jan, R. H., "DDoS "detection and traceback with decision tree and grey relational analysis.,", International Journal of Ad Hoc and Ubiquitous Computing, Vol-7, 121–136.2011.
19. Y Chen,., K. Hwang,., and W. S. Ku, "Distributed change-point detection of DDoS attacks over multiple network domains.", Proceedings of the IEEE International Symposium on Collaborative Technologies and Systems, Las Vegas, NV, 14-17 May, pp. 543–550. IEEE CS. (2006),
20. J. Mirkoviac,., Prier, G., and Reiher, P. "Attacking DDoS at the source.", Proceedings of the 10th IEEE International Conference on Network Protocols, Paris, France, 12-15 November, pp. 1092–1648. IEEE CS. (2002)
21. A. M. Saifullah, ",Defending against distributed denial-of-service attacks with weight-fair router throttling." Technical Report 2009-7. Computer Science and Engineering, Washington University, St. Louis, USA. (2009)
22. T. Peng, C.Leckie, and RM Rao, K. "Detecting distributed denial of service attacks using source IP address" monitoring. Proceedings of the 3rd International IFIP-TC6 Networking Conference, Athens, Greece, 9-14 May, pp. 771–782. Springer-verlag. (2004)
23. J. Cheng, ,Yin, J., Wu, C., Zhang, and Li, Y. "DDoS attack detection method based on linear prediction model." Proceedings of the 5th international conference on Emerging intelligent computing technology and applications, Ulsan, South Korea, 16-19 September, pp. 1004–1013. Springer- Verlag. (2009)
24. J. Udhayan, and T. Hamsapriya, "Statistical segregation method to minimize the false detections during DDoS attacks." International Journal of Network Security, 13, pages 152–160. (2011)
25. G. Oke, G. and G. Loukas, G "A denial of service detector based on maximum likelihood detection and the random neural network." Computer. Journal., 50, 717–727. (2007)
26. Y. Gilad., and A. Herzberg, A., ''LOT: A defense against IP spoofing and flooding attacks,'' ACM Transaction on Information. Systems. Se, 15: (2012).
27. S. N. Shiaeles,., Katos, V., A. S Karakos, , and Papadopoulos, B. K., ''Real time DDoS detection using fuzzy estimators,'' Computer. Security., 31: pages:782–790 (2012).
28. T. Spyridopoulos, G. Karanikas, T. Tryfonas, T., and Oikonomou, G., ''A game theoretic defence framework against DoS/ DDoS cyber-attacks,'' Computer Security., DOI: 10.1016/j.cose.2013.03.014 (2013).
29. C.L. Chen "A new detection method for distributed denial-of-service attack traffic based on statistical test",. Journal of Universal Computer Science, 15, 488–504. ,(2009)
30. G. Zhang, , S. Jiang., Wei, G., and Guan, Q. A prediction-based detection algorithm against distributed denial-of-service attacks.", Proceedings of the International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly, Leipzig, Germany, 21-24 June, pp. 106–110. ACM. (2009) "
31. A. Akella, , Bharambe, M. Reiter, M., and Seshan, S "Detecting DDoS attacks on ISP networks." Proceedings of the Workshop on Management and Processing of Data Streams, San Diego, CA, 8 June, pp. 1–2. ACM. . (2003)
32. Y. Liu., B.Cukic, and Gururajan, S., ''Validating neural network-based online adaptive systems: A case study,'' Software Quality. Jounal., 15: pages-309–326 (2007).
33. Liu, Y ,Li, J. and Gu, L., "DDoS Attack Detection Based on Neural Network," Proceedings of IEEE 2nd International Symposium on Aware Computing (ISAC), 196–199 (2010).
34. P.K. Agarwal, B. Gupta, , Jain, S., and M.K. Pattanshetti, "Estimating Strength of a DDoS Attack in Real Time Using ANN Based Scheme,", Communications in Computer and Information Science (Springer), 157: 301–310 (2011).
35. T. Chang-Lung, A.Y. Chang,, and Ming Szu, H., "Early Warning System for DDoS Attacking Based

on Multilayer Deployment of Time Delay Neural Network," Proceedings of IEEE 6th International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), pages-704–707 (2010).
36. R. Jalili, F. Imani-Mehr, M. Amini, and Shahriari, H. R. (2005) "Detection of distributed denial of service attacks using statistical pre-processor and unsupervised neural networks." Proceedings of the International conference on information security practice and experience, Singapore, 11-14 April, pp. 192–203. Springer-verlag.
37. R. Karimazad, and A. Faraahi, A "An anomaly-based method for DDoS attacks detection using rbf neural networks." Proceedings of the International Conference on Network and Electronics Engineering, Singapore, pp. 44–48. IACSIT Press. . (2011)
38. D. Gavrilis, and Dermatas, E "Real-time detection of distributed denial-of-service attacks using RBF networks and statistical features." Computer Networks and ISDN Systems, 48, pages-235–245. . (2005)
39. Y. C Wu, Tseng, H. R., Yang, W., and Jan, R. H "DoS detection and traceback with decision tree and grey relational analysis.", International Journal of Ad Hoc and Ubiquitous Computing, 7, 121–136. . (2011)
40. H.Nguyen and Choi, Y "Proactive detection of DDoS attacks utilizing k-NN classifier in an Anti- DDoS framework." International Journal of Electrical, Computer, and Systems Engineering, 4, 247–252. . (2010)
41. K Munivara Prasad, Dr. A Rama Mohan Reddy ,Modelling and Counter measures of Flooding attacks to ITM using Botnet and Group Testing, Global journal of Computer Science and Technology (GJCST), Volume11, Issue 21,pp-15-24,Dec 2011,
42. P. Kumar, and S. Selvakumar, "Distributed denial of service attack detection using an ensemble of neural classifier." Computer Communication, 34, pages-1328– 1341. (2011)
43. C. Scott, and R.Nowak, A neyman-pearson approach to statistical learning." IEEE Transaction on Information Theory, 51, pages-3806–3819. (2005)"
44. T. M. Gil, and M. Poletto, "MULTOPS: a data-structure for bandwidth attack detection." Proceedings of the 10th conference on USENIX Security Symposium - Volume 10, Berkeley, CA, USA, 13-17 August 3. USENIX Association Berkeley. (2001)
45. R. Thomas, B. Mark, T. Johnson, and J. Croall, "Net Bouncer: Client-legitimacy-based high-performance DDoS filtering". Proceedings of the 3rd DARPA Information Survivability Conference and Exposition, Washington, DC, 22-24 April, pp. 111–113. IEEE CS, USA. (2003)
46. J. Wang, R. C. W. Phan, Whitley, J. N., and Parish, D. J.) "Augmented attack tree modelling of distributed denial of services and tree based attack detection method." Proceedings of the 10th IEEE International Conference on Computer and Information Technology, Bradford, UK, 29 June-1 July, pp. 1009–1014. IEEE CS. (2010
47. L. Limwiwatkul, and A. Rungsawang, A. Distributed denial of service detection using TCP/IP header and traffic measurement analysis." Proceedings of the IEEE International Symposium Communications and Information Technology, Sapporo, Japan, 26-29 October, pp. 605–610. IEEE CS. (2004)"
48. G. Zhang, and Parashar, M. "Cooperative defence against DDoS attacks." Journal of Research and Practice in Information Technology, 38, 1–14. (2006)
49. Wu, D., Lu, K., Fan, J., Todorovic, S., and Nucci, A "Robust and efficient detection of DDoS attacks for large-scale internet." Computer Networks, 51, 5036–5056. . (2007)
50. Hwang, K., Dave, P., and Tanachaiwiwat, S. "Net Shield: Protocol anomaly detection with datamining against DDoS attacks". Proceedings of the 6th International Symposium on Recent Advances in Intrusion Detection, Pittsburgh, PA, 8-10 September, pp. 8–10. Springer-verlag. (2003)
51. Chen, Z., Chen, Z., and Delis, A. "An inline detection and prevention framework for distributed denial of service attacks." Computer. Journal. 50, 7–40. (2007)
52. Lee, K., Kim, J., Kwon, K. H., Han, Y., and Kim, S."DDoS attack detection method using cluster analysis. Expert Systems with Applications, "34, 1659– 1665. (2008)
53. Sekar, V., Dueld, N., Spatscheck, O., van der Merwe, J., and Zhang, H. "LADS: large-scale automated DDoS detection system." Proceedings of the annual conference on USENIX Annual Technical Conference, Boston, MA, 30 May-3 June, pp. 16–29. USENIX Association. (2006)
54. H. Rahmani, N. Sahli, and Kammoun, F "Joint entropy analysis model for DDoS attack detection." Proceedings of the 5th International Conference on Information Assurance and Security - Volume 02, Xian, China, 18-20 August, pp. 267–271. IEEE CS. . (2009)
55. Y. Xiang, , K. Li, and Zhou, W. "Low- rate DDoS attacks detection and traceback by using new information metrics." IEEE Transactions on Information Forensics and Security, 6, 426–437. (2011)
56. Shannon, C. E. (1948) "A mathematical theory of communication." Bell system technical journal, 27, 397– 423.

57. J. Francois, Aib, I., and Boutaba, R. "Fire Col: A collaborative protection network for the detection of flooding DDoS attacks." IEEE/ACM Transaction on Networking, 20, pages-1828–1841. (2012)
58. N. Jeyanthi, and N.C.S.N. Iyengar, "An entropy based approach to detect and distinguish DDoS attacks from flash crowds in VoIP networks." International Journal of Network Security, 14, 257–269. (2012)
59. Li, M. and Li, M. "A new approach for detecting DDoS attacks based on wavelet analysis." Proceedings of the 2nd International Congress on Image and Signal Processing, Tianjin, China, 17-19 October, pp. 1–5. IEEE. (2009)
60. R. Zhong, and G. Yue DDoS detection system based on data mining." Proceedings of the 2nd International Symposium on Networking and Network Security, Jinggangshan, China, 2-4 April, pp. 062–065. Academy Publisher. (2010)"
61. R. Agrawal, and R. Srikant, "Fast algorithms for mining association rules in large databases." Proceedings of the 20th International Conference on Very Large Data Bases, Santiago de Chile, Chile, 12-15 September, pp. 487–499. Morgan Kaufmann. (1994)
62. J.C. Dunn "A Fuzzy Relative of the ISODATA Process and Its Use in Detecting Compact Well-Separated Clusters." Journal of Cybernetics, 3, 32–57. (1973)
63. A. Dainotti, A. Pescap´e, and Ventre, G. (2009) "A cascade architecture for DoS attacks detection based on the wavelet transform." Journal of Computer Security, 17, 945–968.
64. A. Haar, A. (1910) Zur "Theoriederorthogonalen Funktionensysteme." Mathematische Annalen, 69, 331– 371.
65. Li, L. and Lee, G. "DDoS attack detection and wavelets." Proceedings. of the 12th International Conference on Computer Communications and Networks, Dallas, Texas, USA, October 20-22, pp. 421–427. IEEE. (2003)
66. B. B.Gupta, R. C. Joshi, and Misra, M. "ANN based scheme to predict number of zombies in DDoS attack." International Journal of Network Security, 14, pages:36–45. (2012)
67. R. Yan, Q. Zheng, Niu, G., and Gao, S "A new way to detect DDoS attacks within single router." Proceedings of the 11th IEEE Singapore International Conference on Communication Systems, Guangzhou, China, 19-21 November, pp. 1192–1196. IEEE CS. . (2008)
68. J. Cheng, Yin, J., Y. Liu,, Cai, Z., and Wu, C. "DDoS attack detection using IP address feature interaction." Proceedings of the 1st International Conference on Intelligent Networking and Collaborative Systems, Barcelona, Spain, 4-6 November, pp. 113–118. IEEE CS. (2009)
69. Xia, Z., Lu, S., Li, J., and Tang, J. "Enhancing DDoS flood attack detection via intelligent fuzzy logic." Informatics (Slovenia), 34, pages-497–507. (2010)
70. C. Zhang, Z. Cai, W. Chen, Luo, X., and Yin, J. "Flow level detection and filtering of low-rate DDoS. Computer Networks," 56, pages:3417–3431. (2012)
71. D. Zhao, I. Traore, B. Sayed, W. Lu, Saad, S., Ghorbani, A., and Garant, D., ''Botnet detection based on traffic behaviour analysis and flow intervals,'' Computer Security, DOI: 10.1016/j.cose.2013.04.007 (2013).
72. P. C. Senthil mahesh, S. Hemalatha, P. Rodrigues, and A. Shanthakumari, "DDoS Attacks Defense System Using Information Metrics," Proceedings of 3rd International Conference on Trends in Information, Telecommunication and Computing, Lecture Notes in Electrical Engineering (Springer, New York), 25–30 (2012).
73. E. Gelenbe, and G. Loukas,. "A self-aware approach to denial of service defence." Computer Networks, 51, pages:1299–1314. (2007)
74. K. Kumar, A.L. Sangal, and A. Bhandari, "Traceback Techniques Against DDoS Attacks: A Comprehensive Review," Proceedings of IEEE 2nd International Conference on Computer and Communication Technology (ICCCT), 491–498 (2011).
75. Yu, S., Zhou, W., Doss, R., and Jia, W., ''Traceback of DDoS Attacks Using Entropy Variations,'' IEEE Transactions on Parall. Distr., 22: pages:412–425 (2011).
76. Y. Xiang, Li, K., and Zhou, W., ''Low-rate DDoS attacks detection and traceback by using new information metrics,'' IEEE T Inf. Foren. Sec., 6: 426–437 (2011).
77. H.F. Lipson, "Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues," CERT Coordination Center, Special Report: CMU/SEI-2002-SR-009 (2002).
78. K. Subhashini, and G. Subbalakshmi, ''Tracing sources of DDoS attacks in IP networks using machine learning automatic defence system,'' International. Journal. Electron. Commun. Comput. Eng., 3: 164–169 (2012).

Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 14 Issue 7 Version 1.0 Year 2014
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Integrated Biometric Template Security using Random Rectangular Hashing

By Madhavi Gudavalli Dr. D. Srinivasa Kumar & Dr. S. Viswanadha Raju
JNTU Kakinada, India

Abstract- Large centralized biometric databases, accessible over networks in real time are especially used for identification purposes. Multimodal biometric systems which are more robust and accurate in human identification require multiple templates storage of the same user analogous to individual biometric sources. This may raises concern about their usage and security when these stored templates are compromised since each person is believed to have a unique biometric trait. Unlike passwords, the biometric templates cannot be revoked and switch to another set of uncompromised identifiers when compromised. Therefore, fool-proof techniques satisfying the requirements of diversity, revocability, security and performance are required to protect stored templates such that both the security of the application and the users' privacy are not compromised by the impostor attacks. Thus, this paper proposes a template protection scheme coined as random rectangular hashing to strengthen the multimodal biometric system. The performance of the proposed template protection scheme is measured using the fingerprint FVC2004 and PolyU palmprint databases.

Keywords: biometric cryptosystems, cancellable biometrics, feature level fusion, multimodal biometric systems, random rectangular hashing, template protection.

GJCST-E Classification : C.2.0

Strictly as per the compliance and regulations of:

Integrated Biometric Template Security using Random Rectangular Hashing

Madhavi Gudavalli [α] Dr. D. Srinivasa Kumar [σ] & Dr. S. Viswanadha Raju [ρ]

Abstract- Large centralized biometric databases, accessible over networks in real time are especially used for identification purposes. Multimodal biometric systems which are more robust and accurate in human identification require multiple templates storage of the same user analogous to individual biometric sources. This may raises concern about their usage and security when these stored templates are compromised since each person is believed to have a unique biometric trait. Unlike passwords, the biometric templates cannot be revoked and switch to another set of uncompromised identifiers when compromised. Therefore, fool-proof techniques satisfying the requirements of diversity, revocability, security and performance are required to protect stored templates such that both the security of the application and the users' privacy are not compromised by the impostor attacks. Thus, this paper proposes a template protection scheme coined as random rectangular hashing to strengthen the multimodal biometric system. The performance of the proposed template protection scheme is measured using the fingerprint FVC2004 and PolyU palmprint databases.

Keywords: biometric cryptosystems, cancellable biometrics, feature level fusion, multimodal biometric systems, random rectangular hashing, template protection.

I. Introduction

A biometric system automatically recognizes the person based on his/her physiological or behaviour characteristics [1]. As the biometric features are distinct to each person, it establishes direct connection between users and their identity. These systems are more ease and secure as they are not needed to remember any password or carry any token to gain access to the applications. The biometric systems which rely on the evidence of a single source of information for authentication (e.g., single fingerprint, iris, palm-print, retina, voice, ear *or* face) are known as *Unimodal biometric systems*. They often suffer from enrolment problems due to non-universal biometric traits, susceptibility to biometric spoofing or insufficient accuracy caused by noisy data. One of the methods to overcome these problems is to make use of multimodal biometric systems, which combines information from multiple inputs of one or more modalities to arrive at a decision [2]. Depending on the level of information that is fused, the fusion scheme can be classified as sensor level, feature level, match score level and decision level fusion. The sensor level and the feature level are referred to as pre-mapping fusion while the matching score level and the decision level are referred to as post-mapping fusion [3]. The acquisition and processing sequence of these systems can be either serial or parallel. In the serial or cascade or sequential architecture, the acquisition and processing of the different sources take place sequentially and the outcome of one matcher may affect the processing of the subsequent sources. In the parallel design, different sources are processed independently and their results are combined using an appropriate fusion scheme [4].

The security of the system will be determined by the integrity of the biometric database. The conventional biometric systems elevate privacy and protective problems to the users [6]. A stolen template yields ruinous issues to the biometric system i.e an attacker recapitulates the seized template to the matching module to get admitted or the snatched template can be misused across other biometric systems for cross-matching that uses the same biometric modality[5]. Therefore, if the stored template is compromised, it becomes useless forever. A compromised template cannot be revoked because of the significant link between a biometric trait and its template. Thus, template protection has come into existence due to the intrinsic weaknesses of traditional biometric systems.

In general, a template protection scheme must fulfil the following requirements [5]:

- *Diversity:* The user's templates should differ from each other. The same biometric data should not be used in more than one application.
- *Revocability:* A compromised template should be easily cancelled and the new template has to be reconstituted such that it does not alter the existing system performance.
- *Security:* It should be computationally tough for the template to remake its original biometric data. Thereby, confirming the source data security.
- *Performance:* The implementation of template protection method should not lower the biometric system performance which is computed in terms of

Author α: Research Scholar of JNTU Hyderabad & Assistant Professor Department of IT, JNTUK-UCEV, Vizianagaram, Andhra Pradesh, India. e-mail: madhavi.researchinfo@gmail.com .
Author σ: Principal & Professor, Department of CSE, Hosur Institute of Technology and Science, Errandapalli Village, Hosur Taluk, Krishnagiri, India. e-mail: srinivaskumar_d@yahoo.com.
Author ρ: Professor & Head Department of CSE, JNTUH CEJ, JNT University Hyderabad, Telangana, India. e-mail: svraju.jntu@gmail.com.

False Rejection Rate (FRR) or False Acceptance Rate (FAR) or Equal Error Rate (EER).

In literature, *Cancellable Biometrics* [17] known as *Transformation-based Approach* and *Biometric Cryptosystems* [7] known as *Helper Data Methods* are the two approaches to secure stored single biometric template. Cancellable Biometrics facilitates the template to operate like a password which can be cancelled and reinstated if required. This approach assures the privacy and security of the actual biometric template by employing an irreversible transformation. Thus, the transformed biometric data is stored in the database instead of original template. This approach is furthermore organized as *biometric salting* and *non-invertible transform*. In [8] Soutar et al. suggested biometric encryption method. Three non-invertible transformation functions were proposed for cancellable fingerprint template generation by Ratha et. al. in [9] namely Cartesian transformation, surface folding transformation and polar transformation. In [10], Teoh et. al. proposed Bio-Hashing technique to produce cancellable fingerprint templates. A new token will be reissued in the case of compromised template. Biometric Cryptosystems circumscribe the template protection design by including biometric data into cryptographic bounds. This method stringent the template security by employing the biometrics data to determine an encrypted template. In [13] Dodis et al. introduced *secure sketch* and *fuzzy extractor* concepts in key generation from biometrics. A two-level quantization method was introduced by Li and Chang in [14] to obtain secure sketches. The practical issues in secure sketch construction and secure sketch quantization for face biometric were discussed by Sutcu et al. [15]. Buhan et al. in [11] addressed the problem of generating fuzzy extractors from continuous distributions. The secure sketch construction is proposed for fingerprints in [12] and for multimodal systems (face and fingerprint) in [16].

This paper proposes a well-defined key-based transformation technique for integrated template of fingerprint and palmprint obtained by combining their respective feature vectors at feature level. In the proposed scheme, it is difficult to reconstruct the original template form the transformed template without submitting the distinctive secret key. A different key can be assigned to the biometric template for the generation of new one if the transformed template is compromised.

II. Proposed System

The proposed scheme analyses the performance of multimodal biometric system that integrates extracted feature vectors of fingerprint and palmprint at feature level. This fusion level is preferred as it contains much richer information on the source data. The acquisition and processing sequence employed for this system is *serial* i.e each biometric source is obtained and processed independently with a short time interval between their successive acquisitions and processing.

a) Methodology

The following steps show the process of proposed template protection scheme.

Step 1: The user U_i with identity ID_i inputs fingerprint and palmprint data to get registered in the system.

Step 2: Feature Extraction- The acquired fingerprint and palmprint data are pre-processed and enhanced by adopting a two dimensional discrete wavelet transform (2D-DWT). The mutual attributes such as ridges of fingerprint and palmprint images are preserved using 2D Gabor filter.

$$G(x, y, f, \theta) = \exp\left(-\frac{x'^2+y'^2}{2\sigma^2}\right)\cos(2\Pi f x')$$

Where $x' = x\cos\theta + y\sin\theta$ and $y' = -x\cos\theta + y\sin\theta$, f is the frequency of the sinusoidal plane wave along the direction θ from the x-axis, σ^2 is the standard deviation of the Gaussian envelope. The values considered for experiment are f= 10, $\sigma^2=16$, and $\theta=\Pi/8$.

Step 3: Normalization- As the intensity domains of filtered palmprint and fingerprint are different, they are normalized to the same domain by employing Gaussian normalization.

$$G(x,y) = \frac{I(x,y) - \mu_I}{\sigma_I}$$

Where I(x, y) denotes the pixel intensity at coordinate (x, y), μ_I denotes the intensity mean, and σ_I denotes the intensity standard deviation.

Step 4: Feature Level Fusion- The normalized LL sub-band images are combined at feature level using Daubechies Wavelet.

Step 5: Random Tiling- A set of rectangles with random characteristics of the user U_i are generated from the fused feature using random tiling. The magnitude of each rectangle is obtained by computing the standard deviation. These magnitudes are concatenated to generate a feature vector. The random tiling is a function *'f'* which accepts two parameters and returns a feature vector *'V'*. $V = f(I_{fused}, K)$, Where I_{fused} represents the fused feature, and 'K' is the user specific key to obtain the rectangles' characteristics. A set of random numbers $r_w, r_h \in [-1,1]$ are generated using 'K' as the seed. A new set of features can be extracted from the fused feature in the case of a compromise using newly generated key 'K'.

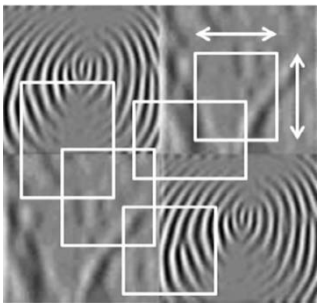


Figure 1 : Random rectangular blocks of fused feature

Step 6: Cryptographic Key Generation- The biometric secret key 'k' is generated using AES algorithm which is the variableness origin to select the random rectangular regions. Thus, every user has a distinct fused template depending on the different unique keys generated.

Step 7: Helper Data Generation- Cancellable biometric features are generated through Bio-hashing using MD5 (Message Digest) from the random rectangle region. This hashing is a transformation function which represents the ridges in the form of a decimal vector. The number of ridges falling within the rectangle region is counted. The numbers in the decimal vector form the basis for generating template bit-string. The same process is repeated for remaining rectangular regions. The hash vector is obtained by combining all the 8-digit fixed-length vectors produced from each rectangular region. This hash vector acts as the *helper data* and is stored in the database. The bit-string representing the biometric features is generated by utilising the hash vector. The process of cryptographic key, *'k'* is formulated from the encoded Bio-hash is as follows.

$$Key\ Binding: b_c \oplus$$

$$Key\ Retrieval: \gamma \oplus b'_c = \mathrm{k}'$$

where γ is called Biokey, b_c and b_c refer to the encoded Bio-hash and decoded Bio-hash respectively, while $\oplus$ denotes bitwise XOR operation.

Step 8: Bit-String Generation-The integer hash vector produced is insecure and occupies much of the database. The integer values are transformed to binary bit-string using the bit-block coding technique. This technique first initializes a fixed binary block with zeros. This block values will be reset to ones corresponding to the integer in the hash vector. This process is iterated for the remaining blocks of the hash vector to generate the binary bit-string.

III. Experimental Results

The databases fingerprint FVC2004 [18] and PolyU palmprint [19] are used for performance analysis of the proposed integrated template security approach. The experiments were conducted on the randomly selected 10 samples of fingerprint and palmprint images of respective databases. The present work assumes that each user is allotted with a secret key which is stored in the database and these keys are lost by no means. The enrolled and query binary vectors are produced based on the secret keys and the scores for identification between the enrolled bit-strings (*e*) and query bit-strings (*q*') were computed using the formula:

$$Score(i,j) = \frac{\sum_{r=1}^{d}(e_{j,r} \oplus q_{i,r})}{L}$$

where $\oplus$ represents the XOR operation, while $e_{j,r}$, and $q_{i,r}$ corresponds to the r-th bit in e_j and q_i,. L denotes the length of e_j and q_i.

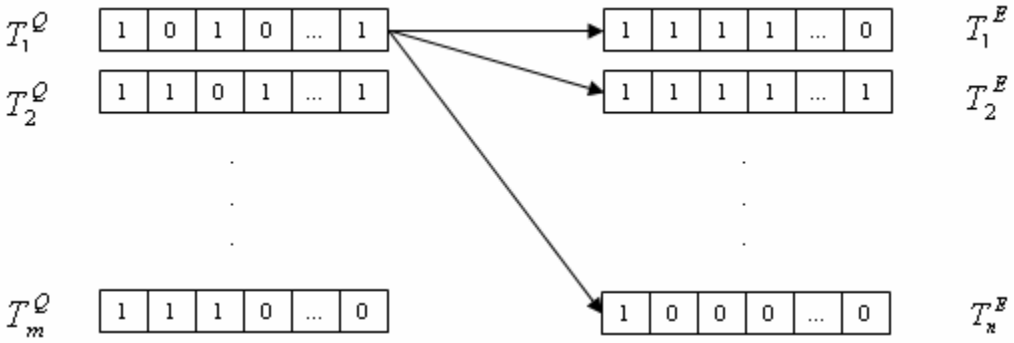


Figure 2 : Collation between the query and the enrolled template

The collation between the enrolled and query binary templates is shown in Figure 2. The performance in terms of equal error rate (EER) with various random rectangles is listed in Table 1. It is observed that the rise in random rectangles lowers the EER. The root cause is that more features can be extracted with more number of random rectangles there by features more distinct. The recognition rate obtained is lower than 1% when tested on public databases of FVC2004 [18] and PolyU palmprint [19].

Table 1: Equal Error Rate (EER) of varied random rectangles

Number of Random Rectangles	EER
10 Random Rectangles	2.81%
15 Random Rectangles	0.32%
20 Random Rectangles	0.20%

IV. Conclusions

A novel scheme based on key based hashing with randomized rectangle is presented in this paper that produces short hash strings for integrated templates. These hashes cannot reproduce the original template without knowledge of the unique key. Further, the use of Bio-hash as the mixing process provides the one-way transformation and deters exact recovery of the biometric features when compromised. When the template is compromised, it is difficult to construct the original hash vector because the impostors cannot figure out the exact location of each ridge as the count of number of ridges is only contained in the random rectangle. In the current work, the performance attained is lower than 1%. The diversity property of proposed scheme is examined by evaluating the correlation of the bit-strings obtained by using different user specific keys as seed in random tiling process. In this case, a high positive correlation indicates that the old bit-string falls into the region of acceptance of the refreshed bit-string. Thus, the proposed scheme satisfies all the four requirements of template protection scheme namely, revocability, security, performance and diversity. The future work signifies the stolen-token scheme, where the attacker grabs the secret key to get access to the system.

V. Acknowledgement

We would like to express our gratitude to all the referees' authors of the papers who have helped directly or indirectly the possibility to complete this research work.

References Références Referencias

1. Anil K. Jain, Patrick Flynn, and Arun A. Ross, *"Handbook of Biometrics",* Secaucus, NJ, USA: Springer-Verlag New York, Inc., 2007.
2. Madhavi Gudavalli, Dr. S. Viswanadha Raju, Dr. A. Vinaya Babu and Dr. D. Srinivasa Kumar, *"MultiModal Biometrics- Sources, Architecture & Fusion Techniques: An Overview",* IEEE-International Symposium on Biometrics and Security Technologies (ISBAST'12), Taipei, Taiwan, pp. 27-34, March 26-29, 2012, DOI 10.1109/ISBAST. 2012.24.
3. C. Sanderson and K. K. Paliwal, "*Information Fusion and Person Verification Using Speech and Face Information,*" IDIAP-RR 02-33, 2003.
4. Karthik Nandakumar, *"Multibiometric Systems: Fusion Strategies and Template Security",* Ph.D Thesis 2008.
5. Anil K. Jain, Karthik Nandakumar, and Abhishek Nagar, "*Biometric Template Security,*" EURASIP Journal on Advances in Signal Processing, vol. 2008, p. 17, 2008.
6. Madhavi Gudavalli and Dr.S.Viswanadha Raju et.al, *"A Template Protection Scheme for Multimodal Biometric System with Fingerprint, Palmprint, Iris and Retinal Traits",* CUBE 2012 International IT Conference, Pune, Maharashtra, India, September 3-5, 2012, ACM 978-1-4503-1185-4/12/09, PP. 102-107.
7. Uludag, U., Pankanti, S., Prabhakar, S., Anil, K.J, *"Biometric Cryptosystems: Issues and Challenges",* Proceedings of the IEEE 92(6), 948–960 (2004).
8. Roberge C. S. D., Stoianov A., Gilroy R., Kumar B. V.: Biometric encryption. ICSA Guide to Cryptography, Chapter 2 (1999).
9. N.K. Ratha, S. Chikkerur, and J.H. Connell, "Generating Cancelable Fingerprint Templates," in IEEE Pattern Analysis and Machine Intelligence, vol.29, no.4, pp. 561-572, 2007.
10. A. B. J. Teoh, D. C. L. Ngo, and A. Goh, "BioHashing: Two factor authentication featuring fingerprint data and tokenised random number," Pattern Recognition, vol. 37, pp. 2245-2255, 2004.
11. I. R. Buhan, J. M. Doumen, P. H. Hartel, and R. N. J. Veldhuis. Fuzzy Extractors for Continuous Distributions. In *Proceedings of ACM Symposium on Information, Computer and Communications Security,* pages 353–355, Singapore, March 2007.
12. A. Arakala, J. Jeffers, and K. J. Horadam. Fuzzy Extractors for Minutiae-Based Fingerprint Authentication. In *Proceedings of Second International Conference on Biometrics,* pages 760–769, Seoul, South Korea, August 2007.
13. Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. Technical Report, Cryptology ePrint Archive, February 2006. A preliminary version of this work appeared in EUROCRYPT 2004.
14. Q. Li and E. C. Chang. Robust, Short and Sensitive Authentication Tags Using Secure Sketch. In *Proceedings of ACM Multimedia and Security Workshop,* pages 56–61, Geneva, Switzerland, September 2006.

15. Y. Sutcu, Q. Li, and N. Memon. Protecting Biometric Templates with Sketch: Theory and Practice. *IEEE Transactions on Information Forensics and Security,* 2(3):503–512, September 2007.
16. Y. Sutcu, Q. Li, and N. Memon. Secure Biometric Templates from Fingerprint- Face Features. In *Proceedings of CVPR Workshop on Biometrics,* Minneapolis, USA, June 2007.
17. Ratha, N.K., Chikkerur, S., Connell, J.H., Bolle, R.M, *"Generating Cancelable Fingerprint Templates",* IEEE Transactions on Pattern Analysis and Machine Intelligence, Special Issue on Biometrics 29(4), 561–572 (2007).
18. FVC2004 Fingerprint Database, http://bias.csr.unibo.it/fvc2004/.
19. PolyU Palmprint Database, http://www4.comp.polyu.edu.hk/ ~biometrics/.

This page is intentionally left blank

Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 14 Issue 7 Version 1.0 Year 2014
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

A Comparative Study on Performance Evaluation of Intrusion Detection System through Feature Reduction for High Speed Networks

By V. Jyothsna & V. V. Rama Prasad
JNTUH University, India

Abstract- The rapid growth in the usage of the internet had led to many serious security issues in the network. The intrusion detection system (IDS) is one of the sophisticated defensive systems used to detect the malicious activities happening in the network services across the world.Hence, more advanced IDS are been developed in past few years. To improve the performance of the IDS, the system has to be trained effectively to increase the efficiency and decrease the false alarm rate. To train the system the attributes selection plays the major role.This paper evaluates and compares the performance of the intrusion detection systems for different feature reduction techniques in high speed networks.

GJCST-E Classification : C.2.1 C.2.3

Strictly as per the compliance and regulations of:

A Comparative Study on Performance Evaluation of Intrusion Detection System through Feature Reduction for High Speed Networks

V. Jyothsna [α] & V. V. Rama Prasad [σ]

Abstract- **The rapid growth in the usage of the internet had led to many serious security issues in the network. The intrusion detection system (IDS) is one of the sophisticated defensive systems used to detect the malicious activities happening in the network services across the world. Hence, more advanced IDS are been developed in past few years. To improve the performance of the IDS, the system has to be trained effectively to increase the efficiency and decrease the false alarm rate. To train the system the attributes selection plays the major role. This paper evaluates and compares the performance of the intrusion detection systems for different feature reduction techniques in high speed networks.**

I. Introduction

Internet is a global public network. In today's world, with the rapid increase in the potentials of the Internet, business model adopted in the organizations has subsequent change. Every day the people connecting to the Internet are also drastically increased. Today's a very critical business model popularly used is E-Business.

With the internet, business organizations are having incredible approach of reaching the end users. But in the internet there will be both harmless and harmful users that may lead to lots of risk to the business organizations. The information availability to the end users is one of the main services adopted by every organization. At the same time the information becomes available to the malicious users also. Malicious users or hackers will use different techniques on organization's internal systems to exploit vulnerabilities and compromise the system to access the sensitive information available in the system [1].

Every organization needs to adopt a security measure to overcome the accessing of data from the hackers. Many organizations across the world deployed firewalls to protect their private network from the Public network. Firewall protects the internal system by controlling the incoming and outgoing network traffic based on rule set. As the business organizations needs some kind of access permissions to the internal systems for the Internet users. These permissions may cause some vulnerabilities in the Private network through which the malicious users will have a change to get in to the system. So, the firewalls will not provide the 100% guarantee of the organization in securing the sensitive data present in the system.

One of the remedy to defence against the attacks in the network is intrusion detection system (IDS) [2]. An intrusion detection system (IDS) is used to monitor suspicious activities in the network traffic and alerts the system or network administrator. In some cases the IDS is not only used to detect the anomalous or maliceousstraffic but also for taking action such as blocking the user or source IP address from accessing the network.

Initially, Intrusion Detection Systems [3, 4] were implemented to run on individual hosts or network devices to monitor the inbound and outbound packets from the device and alert the user or administrator about suspicious activity. This sort of detection is called host based (HIDS) intrusion detection systems. But the gradual evolution of the network led to focus on network based (NIDS) intrusion detection systems which is used to monitor traffic to and from all devices in the network by scanning all inbound and outbound traffic that would affect the overall speed of the network.

Depending upon the type of analysis used to detect the anomalies, IDS are classified as Signature based and Anomaly based detection systems [5]. Signature based detection system also called misuse detection will monitor the network packets and check the availability of signatures in the database. If the pattern matches it specifies as attack. It is similar to the most antivirus software. The main limitation is it will only detect the attack whose attack patterns are already present in the database i.e., known malicious threats. It is unable to predict the new attacks. But the other type of analysis technique so called Anomaly based detection system will analyse the behaviour of the network and establish the baseline. If the activities in the network deviate from the baseline it will consider as malicious threat.

Author α: Research Scholar, Department of CSE, JNTUH, Hyderabad e-mail: jyothsna1684@gmail.com.
Authorσ: Professor, Department of CSE, Sree Vidyanikethan Engineering College, Tirupati.

The benchmark dataset usually adopted by the research community of intrusion detection is KDD99 [6]. Each record in the dataset is labelled as normal or attack. Each record in the dataset will consist of 41 features. The features are categorized into four clusters. They are Basic Features, Content Features, Time-based Traffic Features and Host-based Traffic Features. The data records labelled as attack falls in one of the following four types:

- DoS: It denotes the denial of service attack. By denial of service attack, the legitimate user will not be able to access the services for which he has the access permissions. Some of the categories of DoS attack are Apache2, Back, Land, Mail bomb, etc.
- U2R: U2R means user to root attack. In this class of attack user subscribe the service as normal user and then slowly tries to exploiting various vulnerabilities of the system. Some of the types of U2R are Eject, Ffbconfig, Fdformat, Load module, etc.
- R2L: R2L is remote to local attack. In this kind of attack a remote user gains access of the local user account through network communication and tries to access the sensitive information in the system. Some of the kinds of R2L attacks are Sendmail, Xlock, Xsnoop, etc.
- Probe: A Probe attack is used to scans the network to find the vulnerabilities of the system through which the hacker or attacker can peep into the system for further attacks.

In this paper the performance of IDS is evaluated by comparing different feature reduction techniques such as Correlation-based feature reduction (CFS), Gain ratio (GR), Information gain (IR), Principal component analysis (PCA), Gini Index (GI) and Optimized Least Significant Particle based Quantitative Particle Swarm Optimization (OLSP-QPSO). Rest of the paper is organised as follows: Section 2 provides the various feature selection techniques applied for IDS. Section 3 presents the comparison of feature selection techniques. Section 4 focuses on the Performance Evaluation by different feature selection techniques. Finally, Section 4 concludes and provides suggestions for future scope.

II. Feature Selection Techniques

Feature selection also called attribute selection or variable subset selection. It is used to select the subset of relevant features needed for the model. The data set used in the constructed model will consists of relevant, redundant or irrelevant features [7]. So, the key assumption used in the feature selection technique is removing the data which are redundant or irrelevant. The attribute or feature which does not provide any more information than the currently selected features then such type of features are called as Redundant and if the feature does not consist of useful information in any context then they are called as irrelevant features. Feature selection is also useful as part of the data analysis process, as it shows which features are important for prediction, and how these features are related [8, 9].

A feature selection technique provides the following benefits for analytical models:

- Improves the performance of the system.
- Increases the accuracy of prediction
- Need short time for training through which overall time of execution can be reduced.

The performance of the system will depend on detection rate and the false alarm rate also called as false positive rate. The detection rate is defined as the number of malicious packets detected by the system (True Positive) divided by the total number of malicious packets present in the data set. False Alarm Rate is defined as the number of normal packets detected as malicious packets (False Positive) divided by the total number of normal packets. Normally the IDS need to have high detection rate and low false alarm rate. To retrieve have high detection rate and low false alarm rate training the system plays a vital role. To train and improve the performance of the system all the parameters of the packet is not needed. So, an appropriate feature selection technique has to be used to select the relevant features by removing the redundant and irrelevant features through which overall performance of the system can be increased by decreasing the training time and increasing the accuracy of detecting the attacks in the network [10,11].

a) Correlation-based feature reduction (CFS)

The Correlation Feature Selection (CFS) [12, 13] is a simple filter algorithm for evaluating and ranks subset of features based on correlation evaluation function. By observing the ranks for the attributes we can predict the correlation of the features. The features with high correlation will be considered as relevant features and low correlation can be ignored as Irrelevant features.

The following equation gives the correlation of features consisting k features:

$$r_{zc} = \frac{k\overline{r_{zi}}}{\sqrt{k + k - (k-1)\overline{r_{ii}}}}$$

Where

r_{zc} = Correlation between the features.

k = Number of features.

$\overline{r_{zi}}$ = Average of the correlations between all features.

$\overline{r_{ii}}$ = Average inter-correlation between features.

b) Information gain (IR)

Information gain [14, 15] determines the importance of the attribute in the total training dataset by analysing the information content of attributes. It is also used to predict the ordering of the nodes in the decision tree where nodes are considered as attributes. The highest information gain attribute is chosen as the splitting attribute for node N. This attribute minimizes the information needed to classify the list of attributes in the resulting partitions. By this approach, the needed expected number of tests can be minimized to classify a given list of attributes and guarantees that a simple tree is found.

The information gain of the each attribute is calculated as follows:

$$\text{Gain (A)} = \text{Info (D)} - \text{Info}_A\text{(D)}$$

Where,

A→Attribute

Info (D) → Information content of the total dataset

Info_A(D) →Information content of the Attribute A

Information content of the total dataset is calculated as

$$Info(D) = -\sum_{i=1}^{m} P_i \log_2(P_i)$$

Where,

D → Total dataset

i→ Total number of class labels in the data set

P_i→ Probability of class label i in the data set

Information content of the Attribute A in the total dataset is calculated as

$$Info_A(D) = \sum_{j=1}^{v} \frac{|D_j|}{|D|} \times Info(D_j)$$

Where,

A → Attribute in the dataset D

j→ Total number of different category values present in the attribute A

|Dj| → Total number of j^{th} category values in the attribute A

|D| → Total number of records in the dataset D

Info (D_j) → Information content of j^{th} category values of the attribute A

c) Gain ratio (GR)

Gain ratio [16, 17] is also a method which is used to define the importance of the attributes. It is a modified version of the information gain that reduces its bias on high-branch attributes. The values of the Gain ratio will be Large when data is evenly spread and it is small when all data belongs to one branch. It will take Gain ratio takes into account the number and size of branches when choosing an attribute. It has modified the information gain by taking into account the essential information of a split. It is based on how much information is needed to tell which branch an instance belongs to.

Gain ratio is calculated as follows

$$\text{Gain Ratio (A)} = \text{Gain (A)} / \text{SplitInfo (A)}$$

Where,

Gain (A) →The information gain of the attribute A

Split Info (A) →The splitting information of the attribute A

The splitting information is calculated as follows

$$SplitInfo_A(D) = -\sum_{j=1}^{v} \frac{|D_j|}{|D|} \times \log_2\left(\frac{|D_j|}{|D|}\right)$$

Where,

A → Attribute in the dataset D

j→ Total number of different category values present in the attribute A

|Dj| → Total number of j^{th} category values in the attribute A

|D| → Total number of records in the dataset D

d) Principal component analysis (PCA)

Principal components analysis (PCA) [18] also known as the Karhunen-Loeve or K-L method is a useful statistical technique which is used to reduce the number of attributes or dimensions in the dataset without much loss in the information needed to analyse the data.

The basic procedure is as follows [19, 20]:

1. Select the dataset for which the attributes or dimensions has to be reduced.
2. The dataset is normalized such that each attribute falls within the same range.
3. Initially calculate the covariance between one attribute with the other and derive the covariance matrix.

Covariance is calculated as

$$cv(X,Y) = \frac{\sum_{i=1}^{n}(X_i - \bar{X})(Y_i - \bar{Y})}{n-1}$$

Where,

X → Independent variable

Y → Dependent variable

n→ Number of attributes in the dataset

$\bar{X}$→Mean of the independent variable X

Y_i →Mean of the dependent variable Y

Covariance matrix (for example X, Y, Z are the 3-dimensional dataset) is derived as

$$C_{max} = \begin{bmatrix} cv(X,X) & cv(X,Y) & cv(X,Z) \\ cv(Y,X) & cv(Y,Y) & cv(Y,Z) \\ cv(Z,X) & cv(Z,Y) & cv(Z,Z) \end{bmatrix}$$

4. Calculate the Eigen values (λ) and for the λ values derive the Eigenvectors from the covariance matrix
5. Choosing components and forming a feature vector

After calculating the eigenvectors of the covariance matrix, then order the eigen values by highest to lowest. These values give the importance of the attributes. The attributes with lesser eigen values can be ignored and higher eigen values will be considered. The attributes after leaving out the lesser Eigen values is considered as feature vector.

6. Derive the final data set

Final dataset = Row feature vector * Row data adjust

Where,

Row feature vector → The transposed eigenvectors matrix with most important features at the top.

Row data adjust → The transposed mean-adjusted matrix (Attribute values in each column, with each row holding a separate dimension).

e) Gini index (GI)

The Gini index [21] is used to extract the attributes mainly needed to analyse the data set to detect the attacks. It measures the impurity of data set D. The attribute with highest gini index is treated as the unimportant attributes and the lowest gini index is treated as important attributes to detect the attacks.

Gini index for the attribute A is calculated as

$$\text{Gini (A)} = \text{Gini (D)} - \text{GiniA (D)}$$

Where,

Gini (D) → impurity of the total dataset

$Gini_A$ (D) → impurity of the Attribute A

Impurity of the total dataset is calculated as

$$\text{Gini (D)} = 1 - \sum_{i=1}^{m} P_i^{\,2}$$

Where,

D → Total dataset

i→ Total number of class labels in the data set

P_i→ Probability of class label i in the data set

Impurity of the Attribute A in the total dataset is calculated as

$$Gini_A(D) = \frac{|D_1|}{|D|} \times Gini(D_1) + \frac{|D_2|}{|D|} \times Gini(D_2)$$

Where,

A → Attribute in the dataset D

|D| → Total number of records in the dataset D

$|D_1|$ → Total number of subset pair category values of attribute A

$|D_2|$ → Total number of another subset category values of attribute A

Gini (D_1) → Impurity of subset pair category values of the attribute A

Gini (D_2) → Impurity of another subset category values of the attribute A

f) Optimized Least Significant Particle based Quantitative Particle Swarm Optimization (OLSP-QPSO)

OLSP-QPSO [22] is an optimizing technique used to replace the QPSO. This technique is used to calculate the best swarm particles by applying a quadratic polynomial model. This process is an iterative process until the best swarm particles are been identified to analyse the attacks. The procedure for optimized QPSO algorithm is as follows

1. Swarm is initialized.
2. mbest is calculated
3. Update the position of the attributes
4. Estimate the fitness value for each attribute
5. If the present fitness value is better than the best fitness value in past, then update the existing fitness value by the current fitness value.
6. Update global best
7. Find the new attribute
8. If the new attribute is better than the worst attribute in the swarm, then replace the worst attribute by the new attribute
9. Repeat step 2 until maximum iterations is reached.

III. Comparison Between the Different Feature Selection Techniques

Feature selection plays a major role for achieving the high performance intrusion detection system. Many feature selection techniques were proposed to select the relevant attributes from the data set. Some of the feature selection techniques mainly used was discussed in the previous section. The standard data set mainly used to experiment the intrusion detection system is KDD cup 1999. The KDD cup 1999 [23] consists of approximately 5 million training set records and 3 million test set records. The records are classified as normal or anomaly. The anomalies are broadly classified as four categories such as DoS, U2R, R2L and Probe. Only 19.86 % of the total training records are normal traffic and remaining are the attack traffic. Among the test set, 19.45 % is normal traffic and remaining is attack traffic. Each record in the data set will consists of 41 features. All the attributes in the data set is not needed to analyse the attacks in the network. So, appropriate technique has to be chosen to reduce the features for the data set. Selected feature reduction should not affect the performance of the system. The selected technique should increase the detection rate and decrease the false positives [24].

In this study, all the records in the training and test data set are considered. The number of attributes considered for each record in the training set is 41. The following table shows the comparison between the different feature selection technique and the number of attributes obtained after applying the technique.

Table 1 : The number of attributes selected for each feature selection techniques

Feature selection methods	Number of attributes selected
Correlation-based feature reduction (CFS)	10
Gain ratio (GR)	14
Information gain (IR)	20
Principal component analysis (PCA)	12
Gini Index (GI)	18
Optimized Least Significant Particle based Quantitative Particle Swarm Optimization (OLSP-QPSO)	**8**

From the above table it is observed that among the specified feature selection techniques more number of attributes is reduced using the Optimized Least Significant Particle based Quantitative Particle Swarm Optimization (OLSP-QPSO).

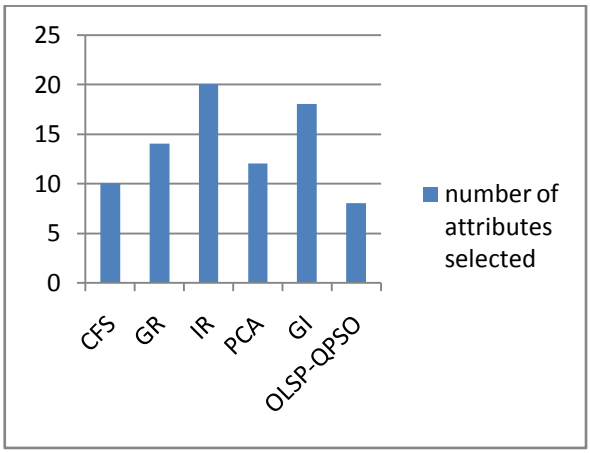


Figure 1 : Number of attributes selected

IV. Performance Evaluation by Different Feature Selection Techniques

The performance of the system will depend on detection rate and the false alarm rate [25]. The detection rate is defined as the number of malicious packets detected by the system (True Positive) divided by the total number of malicious packets present in the data set. False Alarm Rate also called as false positive rate is defined as the number of normal packets detected as malicious packets (False Positive) divided by the total number of normal packets. Normally the IDS need to have high detection rate and low false alarm rate. This can be done by selecting the appropriate features needed to detect the attacks.

The general formulae used for detection rate and false alarm rate is calculated as follows

$$\text{Detection rate} = \frac{Total - anomalies\ - detected}{Total - attacks} * 100$$

False alarm rate or false positive rate =

$$\frac{Total - misclassified - attacks}{Total - normal - \ attacks} * 100$$

Table 2 : Detection rate

Statistical results / Feature selection methods	Number of attributes selected	Detection rate
Correlation-based feature reduction (CFS)	10	97.78%
Gain ratio (GR)	14	96.56%
Information gain (IR)	20	96.30%
Principal component analysis (PCA)	12	97.20%
Gini Index (GI)	18	96.42%
Optimized Least Significant Particle based Quantitative Particle Swarm Optimization (OLSP-QPSO)	**8**	**98.33%**

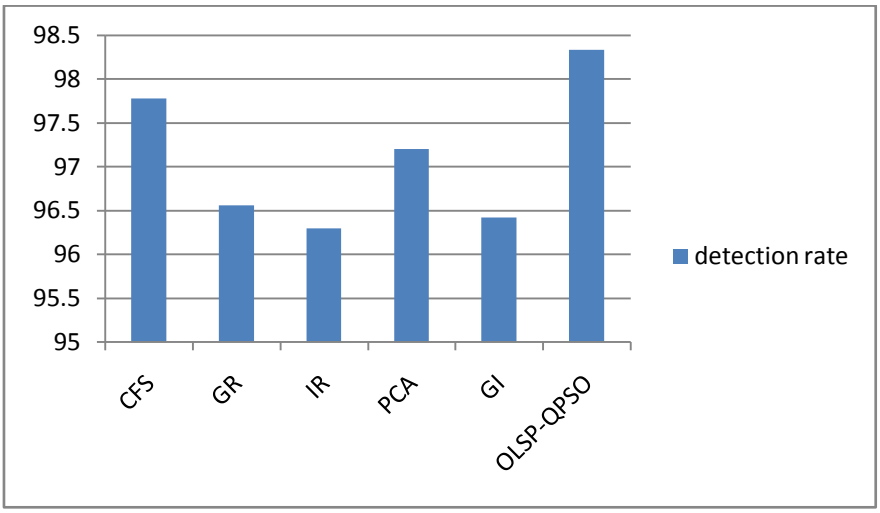


Figure 2 : Detection Rate

Table 3 : False positive rate for attack categories

Feature selection methods / Attack categories	Correlation-based feature reduction (CFS)	Gain ratio (GR)	Information gain (IR)	Principal component analysis (PCA)	Gini Index (GI)	Optimized Least Significant Particle based Quantitative Particle Swarm Optimization (OLSP-QPSO)
DoS	0.003	0.004	0.002	0.001	0.002	**0.002**
R2L	0.002	0.004	0.01	0.003	0.008	**0.001**
U2R	0.001	0.005	0.006	0.002	0.004	**0.003**
Probe	0.015	0.036	0.028	0.013	0.024	**0.01**

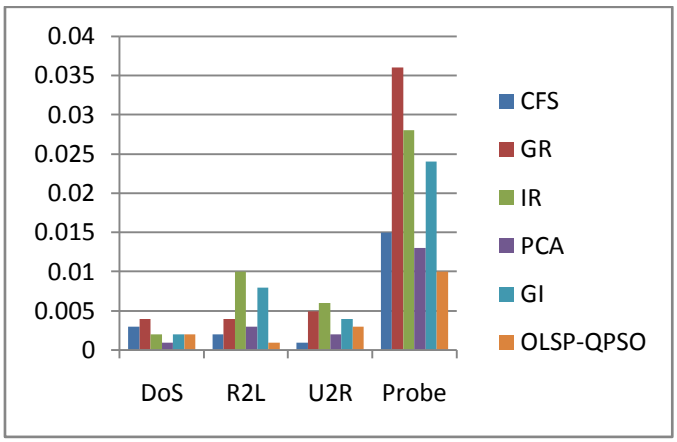


Figure 3 : False positive rate for attack categories

V. Conclusion and Future Work

This paper mainly focuses on the different feature selection techniques used to detect the attacks in the network. Feature selection techniques will decreased the training time of the network. By training the system by the appropriate feature selection technique will increases the performance of the system.

The detection rate can be increased and the false alarm rate can be decreased. The above results shows that the Optimized Least Significant Particle based Quantitative Particle Swarm Optimization (OLSP-QPSO) techniques has more number of attribute reduction and high detection rate and low false alarm rate when comparing with the remaining feature selection techniques. In the above categories of attacks the detection rate of probe is high when compare to Dos, R2L and U2R. In future, the feature selection techniques are more refined to decrease the false alarm rate of the Probe attack.

References Références Referencias

1. Kendall, K, "A Database of Computer Attacks for the Evaluation of Intrusion Detection Systems", Master's Thesis, Massachusetts Institute of Technology, 1998.
2. V. Jyothsna, V. V. Rama Prasad, "A Review of Anomaly based Intrusion Detection Systems", International Journal of Computer Applications (0975 – 8887) Volume 28– No.7, August 2011, pp. 26 – 35.
3. Debar, H., Dacier, M., and Wespi, A., "A Revised taxonomy for intrusion detection systems", Annales des Telecommunications, Vol. 55, No. 7–8, 361–378, 2000.
4. Mukkamala, S., Sung, AH,"A Comparative Study of Techniques for Intrusion Detection", Proceedings of 15th IEEE International Conference on Tools with Artificial Intelligence, IEEE Computer Society Press; (2003) 570-579.
5. P. García-Teodoro , J. Díaz-Verdejo , G. Maciá-Fernández , E. Vázquez , "Anomaly-based network intrusion detection: Techniques, systems and challenges", Elsevier Computers & Security, Volume 28, Issues 2, March 2009, Pages 18–28.
6. Xin Xu, "Adaptive Intrusion Detection Based on Machine Learning: Feature Extraction, Classifier Construction and Sequential Pattern Prediction", International Journal of Web Services Practices, Vol.2, No.1-2, 2006, pp. 49-58.
7. Isabelle Guyon, Andre Elisseeff, "An Introduction to Variable and Feature Selection", Journal of Machine Learning Research, March 2003.
8. H. Sung, S. Mukkamala.," The Feature Selection and Intrusion Detection Problems", in Proceedings of the 9th Asian Computing Science Conference, Lecture Notes in Computer Science, Springer 2004.
9. S Zaman, F Karray, "Features selection for intrusion detection systems based on support vector machines", CCNC'09 Proceedings of the 6th IEEE Conference on Consumer Communications and Networking Conference 2009.
10. S Chebrolu, A Abraham, J P. Thomas, "Feature deduction and ensemble design of intrusion detection systems", Computers & Security, Volume 24, Issue 4, June 2005, Pages 295-307.
11. T. S. Chou, K. K. Yen, and J. Luo "Network Intrusion Detection Design Using Feature Selection of Soft Computing Paradigms", International Journal of Computational Intelligence, 2008.
12. H Nguyen, K Franke, S Petrovic, "Improving Effectiveness of Intrusion Detection by Correlation Feature Selection", International Conference on Availability, Reliability and Security, IEEE 2010, Pages-17-24.
13. Mark A. Hall, Correlation-based Feature Selection for Machine Learning, Dept of Computer Science, University of Waikato. http:// www.cs. waikato.ac.nz/ ~mhall/thesis.pdf.
14. Jasmina Novakovic, "Using Information Gain Attribute Evaluation to Classify Sonar Targets", 17th Telecommunications forum TELFOR 2009 Serbia, Belgrade, November 24-26, 2009.
15. B. Azhagusundari, Antony Selvadoss Thanamani, "Feature Selection based on Information Gain ", International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-2, Issue-2, January 2013.
16. R. Puttini, Z. marrakchi, and L. Me, "Bayesian classification model for Real time intrusion detection", Proc. of 22nd. International workshop on Bayesian inference and maximum entropy methods in science and engineering, 2002.
17. Hesham Altwaijry, Saeed Algarny, "Basesian based intrusion detection system", Journal of King Saud University – Computer and Information Sciences, 2012, pp. 1–6.
18. Xin Xu, X.N. Wang, "Adaptive network intrusion detection method based on PCA and support vector machines", Lecture Notes in Artificial Intelligence, ADMA 2005, LNAI 3584, pp. 696 – 703, 2005.
19. Lindsay I Smith, "A tutorial on Principal Components Analysis", February 26, 2002.
20. I Ahmad, A B Abdulah, A S Alghamdi, K Alnfajan, M Hussain, "Feature Subset Selection for Network Intrusion Detection Mechanism Using Genetic Eigen Vectors" , Proc .of CSIT vol.5, 2011
21. Jiawei Han, Micheline Kamber, "Data mining: Concepts and Techniques", Morgan Kauffmann Publishers, 2006.
22. V. Jyothsna, V. V. Rama Prasad, "HFO-ANID: Hierarchical Feature Optimization for Anomaly based Network Intrusion Detection" Third International Conference on Computing Communication & Networking Technologies (ICCCNT), July 2012 Published in IEEE Xplore digital library, pp 1-11.
23. Tavallaee M, Bagheri E, Lu W and Ghorbani AA., "A detailed analysis of the KDD Cup datasets", in proceedings of IEEE Symposium on computational

intelligence in security and defence applications, 2009.
24. Saman M. Abdulla, Najla B. Al-Dabagh, Omar Zakaria, "Identify Features and Parameters to Devise an Accurate Intrusion Detection System Using Artificial Neural Network", World Academy of Science, Engineering and Technology 2010.
25. Dr. Saurabh Mukherjeea, Neelam Sharmaa, "Intrusion Detection using Naive Bayes Classifier with Feature Reduction", Published by Elsevier Procedia Technology,2012, pp. 119 – 128.
26. NSL-KDD dataset for network –based intrusion detection systems" available on http://iscx.info/NSL-KDD/

Global Journals Inc. (US) Guidelines Handbook 2014

www.GlobalJournals.org

FELLOW OF ASSOCIATION OF RESEARCH SOCIETY IN COMPUTING (FARSC)

Global Journals Incorporate (USA) is accredited by Open Association of Research Society (OARS), U.S.A and in turn, awards "FARSC" title to individuals. The 'FARSC' title is accorded to a selected professional after the approval of the Editor-in-Chief/Editorial Board Members/Dean.

- The "FARSC" is a dignified title which is accorded to a person's name viz. Dr. John E. Hall, Ph.D., FARSC or William Walldroff, M.S., FARSC.

FARSC accrediting is an honor. It authenticates your research activities. After recognition as FARSC, you can add 'FARSC' title with your name as you use this recognition as additional suffix to your status. This will definitely enhance and add more value and repute to your name. You may use it on your professional Counseling Materials such as CV, Resume, and Visiting Card etc.

The following benefits can be availed by you only for next three years from the date of certification:

FARSC designated members are entitled to avail a 40% discount while publishing their research papers (of a single author) with Global Journals Incorporation (USA), if the same is accepted by Editorial Board/Peer Reviewers. If you are a main author or co-author in case of multiple authors, you will be entitled to avail discount of 10%.

Once FARSC title is accorded, the Fellow is authorized to organize a symposium/seminar/conference on behalf of Global Journal Incorporation (USA).The Fellow can also participate in conference/seminar/symposium organized by another institution as representative of Global Journal. In both the cases, it is mandatory for him to discuss with us and obtain our consent.

You may join as member of the Editorial Board of Global Journals Incorporation (USA) after successful completion of three years as Fellow and as Peer Reviewer. In addition, it is also desirable that you should organize seminar/symposium/conference at least once.

We shall provide you intimation regarding launching of e-version of journal of your stream time to time. This may be utilized in your library for the enrichment of knowledge of your students as well as it can also be helpful for the concerned faculty members.

The FARSC can go through standards of OARS. You can also play vital role if you have any suggestions so that proper amendment can take place to improve the same for the benefit of entire research community.

As FARSC, you will be given a renowned, secure and free professional email address with 100 GB of space e.g. johnhall@globaljournals.org. This will include Webmail, Spam Assassin, Email Forwarders, Auto-Responders, Email Delivery Route tracing, etc.

The FARSC will be eligible for a free application of standardization of their researches. Standardization of research will be subject to acceptability within stipulated norms as the next step after publishing in a journal. We shall depute a team of specialized research professionals who will render their services for elevating your researches to next higher level, which is worldwide open standardization.

The FARSC member can apply for grading and certification of standards of their educational and Institutional Degrees to Open Association of Research, Society U.S.A. Once you are designated as FARSC, you may send us a scanned copy of all of your credentials. OARS will verify, grade and certify them. This will be based on your academic records, quality of research papers published by you, and some more criteria. After certification of all your credentials by OARS, they will be published on your Fellow Profile link on website https://associationofresearch.org which will be helpful to upgrade the dignity.

The FARSC members can avail the benefits of free research podcasting in Global Research Radio with their research documents. After publishing the work, (including published elsewhere worldwide with proper authorization) you can upload your research paper with your recorded voice or you can utilize chargeable services of our professional RJs to record your paper in their voice on request.

The FARSC member also entitled to get the benefits of free research podcasting of their research documents through video clips. We can also streamline your conference videos and display your slides/ online slides and online research video clips at reasonable charges, on request.

The FARSC is eligible to earn from sales proceeds of his/her researches/reference/review Books or literature, while publishing with Global Journals. The FARSC can decide whether he/she would like to publish his/her research in a closed manner. In this case, whenever readers purchase that individual research paper for reading, maximum 60% of its profit earned as royalty by Global Journals, will be credited to his/her bank account. The entire entitled amount will be credited to his/her bank account exceeding limit of minimum fixed balance. There is no minimum time limit for collection. The FARSC member can decide its price and we can help in making the right decision.

The FARSC member is eligible to join as a paid peer reviewer at Global Journals Incorporation (USA) and can get remuneration of 15% of author fees, taken from the author of a respective paper. After reviewing 5 or more papers you can request to transfer the amount to your bank account.

MEMBER OF ASSOCIATION OF RESEARCH SOCIETY IN COMPUTING (MARSC)

The ' MARSC ' title is accorded to a selected professional after the approval of the Editor-in-Chief / Editorial Board Members/Dean.
The “MARSC” is a dignified ornament which is accorded to a person’s name viz. Dr. John E. Hall, Ph.D., MARSC or William Walldroff, M.S., MARSC.

MARSC accrediting is an honor. It authenticates your research activities. After becoming MARSC, you can add 'MARSC' title with your name as you use this recognition as additional suffix to your status. This will definitely enhance and add more value and repute to your name. You may use it on your professional Counseling Materials such as CV, Resume, Visiting Card and Name Plate etc.

The following benefitscan be availed by you only for next three years from the date of certification.

MARSC designated members are entitled to avail a 25% discount while publishing their research papers (of a single author) in Global Journals Inc., if the same is accepted by our Editorial Board and Peer Reviewers. If you are a main author or co-author of a group of authors, you will get discount of 10%.

As MARSC, you will be given a renowned, secure and free professional email address with 30 GB of space e.g. johnhall@globaljournals.org. This will include Webmail, Spam Assassin, Email Forwarders, Auto-Responders, Email Delivery Route tracing, etc.

We shall provide you intimation regarding launching of e-version of journal of your stream time to time. This may be utilized in your library for the enrichment of knowledge of your students as well as it can also be helpful for the concerned faculty members.

The MARSC member can apply for approval, grading and certification of standards of their educational and Institutional Degrees to Open Association of Research, Society U.S.A.

Once you are designated as MARSC, you may send us a scanned copy of all of your credentials. OARS will verify, grade and certify them. This will be based on your academic records, quality of research papers published by you, and some more criteria.

It is mandatory to read all terms and conditions carefully.

AUXILIARY MEMBERSHIPS

Institutional Fellow of Open Association of Research Society (USA)-OARS (USA)

Global Journals Incorporation (USA) is accredited by Open Association of Research Society, U.S.A (OARS) and in turn, affiliates research institutions as "Institutional Fellow of Open Association of Research Society" (IFOARS).

The "FARSC" is a dignified title which is accorded to a person's name viz. Dr. John E. Hall, Ph.D., FARSC or William Walldroff, M.S., FARSC.

The IFOARS institution is entitled to form a Board comprised of one Chairperson and three to five board members preferably from different streams. The Board will be recognized as "Institutional Board of Open Association of Research Society"-(IBOARS).

The Institute will be entitled to following benefits:

The IBOARS can initially review research papers of their institute and recommend them to publish with respective journal of Global Journals. It can also review the papers of other institutions after obtaining our consent. The second review will be done by peer reviewer of Global Journals Incorporation (USA) The Board is at liberty to appoint a peer reviewer with the approval of chairperson after consulting us.

The author fees of such paper may be waived off up to 40%.

The Global Journals Incorporation (USA) at its discretion can also refer double blind peer reviewed paper at their end to the board for the verification and to get recommendation for final stage of acceptance of publication.

The IBOARS can organize symposium/seminar/conference in their country on behalf of Global Journals Incorporation (USA)-OARS (USA). The terms and conditions can be discussed separately.

The Board can also play vital role by exploring and giving valuable suggestions regarding the Standards of "Open Association of Research Society, U.S.A (OARS)" so that proper amendment can take place for the benefit of entire research community. We shall provide details of particular standard only on receipt of request from the Board.

The board members can also join us as Individual Fellow with 40% discount on total fees applicable to Individual Fellow. They will be entitled to avail all the benefits as declared. Please visit Individual Fellow-sub menu of GlobalJournals.org to have more relevant details.

We shall provide you intimation regarding launching of e-version of journal of your stream time to time. This may be utilized in your library for the enrichment of knowledge of your students as well as it can also be helpful for the concerned faculty members.

After nomination of your institution as "Institutional Fellow" and constantly functioning successfully for one year, we can consider giving recognition to your institute to function as Regional/Zonal office on our behalf.
The board can also take up the additional allied activities for betterment after our consultation.

The following entitlements are applicable to individual Fellows:

Open Association of Research Society, U.S.A (OARS) By-laws states that an individual Fellow may use the designations as applicable, or the corresponding initials. The Credentials of individual Fellow and Associate designations signify that the individual has gained knowledge of the fundamental concepts. One is magnanimous and proficient in an expertise course covering the professional code of conduct, and follows recognized standards of practice.

Open Association of Research Society (US)/ Global Journals Incorporation (USA), as described in Corporate Statements, are educational, research publishing and professional membership organizations. Achieving our individual Fellow or Associate status is based mainly on meeting stated educational research requirements.

Disbursement of 40% Royalty earned through Global Journals : Researcher = 50%, Peer Reviewer = 37.50%, Institution = 12.50% E.g. Out of 40%, the 20% benefit should be passed on to researcher, 15 % benefit towards remuneration should be given to a reviewer and remaining 5% is to be retained by the institution.

We shall provide print version of 12 issues of any three journals [as per your requirement] out of our 38 journals worth $ 2376 USD.

Other:

The individual Fellow and Associate designations accredited by Open Association of Research Society (US) credentials signify guarantees following achievements:

- The professional accredited with Fellow honor, is entitled to various benefits viz. name, fame, honor, regular flow of income, secured bright future, social status etc.

- In addition to above, if one is single author, then entitled to 40% discount on publishing research paper and can get 10%discount if one is co-author or main author among group of authors.
- The Fellow can organize symposium/seminar/conference on behalf of Global Journals Incorporation (USA) and he/she can also attend the same organized by other institutes on behalf of Global Journals.
- The Fellow can become member of Editorial Board Member after completing 3yrs.
- The Fellow can earn 60% of sales proceeds from the sale of reference/review books/literature/publishing of research paper.
- Fellow can also join as paid peer reviewer and earn 15% remuneration of author charges and can also get an opportunity to join as member of the Editorial Board of Global Journals Incorporation (USA)
- • This individual has learned the basic methods of applying those concepts and techniques to common challenging situations. This individual has further demonstrated an in–depth understanding of the application of suitable techniques to a particular area of research practice.

Note :

"

- In future, if the board feels the necessity to change any board member, the same can be done with the consent of the chairperson along with anyone board member without our approval.
- In case, the chairperson needs to be replaced then consent of 2/3rd board members are required and they are also required to jointly pass the resolution copy of which should be sent to us. In such case, it will be compulsory to obtain our approval before replacement.
- In case of "Difference of Opinion [if any]" among the Board members, our decision will be final and binding to everyone.

"

Process of submission of Research Paper

The Area or field of specialization may or may not be of any category as mentioned in 'Scope of Journal' menu of the GlobalJournals.org website. There are 37 Research Journal categorized with Six parental Journals GJCST, GJMR, GJRE, GJMBR, GJSFR, GJHSS. For Authors should prefer the mentioned categories. There are three widely used systems UDC, DDC and LCC. The details are available as 'Knowledge Abstract' at Home page. The major advantage of this coding is that, the research work will be exposed to and shared with all over the world as we are being abstracted and indexed worldwide.

The paper should be in proper format. The format can be downloaded from first page of 'Author Guideline' Menu. The Author is expected to follow the general rules as mentioned in this menu. The paper should be written in MS-Word Format (*.DOC,*.DOCX).

The Author can submit the paper either online or offline. The authors should prefer online submission.Online Submission: There are three ways to submit your paper:

(A) (I) First, register yourself using top right corner of Home page then Login. If you are already registered, then login using your username and password.

(II) Choose corresponding Journal.

(III) Click 'Submit Manuscript'. Fill required information and Upload the paper.

(B) If you are using Internet Explorer, then Direct Submission through Homepage is also available.

(C) If these two are not convenient, and then email the paper directly to dean@globaljournals.org.

Offline Submission: Author can send the typed form of paper by Post. However, online submission should be preferred.

Preferred Author Guidelines

MANUSCRIPT STYLE INSTRUCTION (Must be strictly followed)

Page Size: 8.27" X 11'"

- Left Margin: 0.65
- Right Margin: 0.65
- Top Margin: 0.75
- Bottom Margin: 0.75
- Font type of all text should be Swis 721 Lt BT.
- Paper Title should be of Font Size 24 with one Column section.
- Author Name in Font Size of 11 with one column as of Title.
- Abstract Font size of 9 Bold, "Abstract" word in Italic Bold.
- Main Text: Font size 10 with justified two columns section
- Two Column with Equal Column with of 3.38 and Gaping of .2
- First Character must be three lines Drop capped.
- Paragraph before Spacing of 1 pt and After of 0 pt.
- Line Spacing of 1 pt
- Large Images must be in One Column
- Numbering of First Main Headings (Heading 1) must be in Roman Letters, Capital Letter, and Font Size of 10.
- Numbering of Second Main Headings (Heading 2) must be in Alphabets, Italic, and Font Size of 10.

You can use your own standard format also.
Author Guidelines:

1. General,

2. Ethical Guidelines,

3. Submission of Manuscripts,

4. Manuscript's Category,

5. Structure and Format of Manuscript,

6. After Acceptance.

1. GENERAL

Before submitting your research paper, one is advised to go through the details as mentioned in following heads. It will be beneficial, while peer reviewer justify your paper for publication.

Scope

The Global Journals Inc. (US) welcome the submission of original paper, review paper, survey article relevant to the all the streams of Philosophy and knowledge. The Global Journals Inc. (US) is parental platform for Global Journal of Computer Science and Technology, Researches in Engineering, Medical Research, Science Frontier Research, Human Social Science, Management, and Business organization. The choice of specific field can be done otherwise as following in Abstracting and Indexing Page on this Website. As the all Global

Journals Inc. (US) are being abstracted and indexed (in process) by most of the reputed organizations. Topics of only narrow interest will not be accepted unless they have wider potential or consequences.

2. ETHICAL GUIDELINES

Authors should follow the ethical guidelines as mentioned below for publication of research paper and research activities.

Papers are accepted on strict understanding that the material in whole or in part has not been, nor is being, considered for publication elsewhere. If the paper once accepted by Global Journals Inc. (US) and Editorial Board, will become the copyright of the Global Journals Inc. (US).

Authorship: The authors and coauthors should have active contribution to conception design, analysis and interpretation of findings. They should critically review the contents and drafting of the paper. All should approve the final version of the paper before submission

The Global Journals Inc. (US) follows the definition of authorship set up by the Global Academy of Research and Development. According to the Global Academy of R&D authorship, criteria must be based on:

1) Substantial contributions to conception and acquisition of data, analysis and interpretation of the findings.

2) Drafting the paper and revising it critically regarding important academic content.

3) Final approval of the version of the paper to be published.

All authors should have been credited according to their appropriate contribution in research activity and preparing paper. Contributors who do not match the criteria as authors may be mentioned under Acknowledgement.

Acknowledgements: Contributors to the research other than authors credited should be mentioned under acknowledgement. The specifications of the source of funding for the research if appropriate can be included. Suppliers of resources may be mentioned along with address.

Appeal of Decision: The Editorial Board's decision on publication of the paper is final and cannot be appealed elsewhere.

Permissions: It is the author's responsibility to have prior permission if all or parts of earlier published illustrations are used in this paper.

Please mention proper reference and appropriate acknowledgements wherever expected.

If all or parts of previously published illustrations are used, permission must be taken from the copyright holder concerned. It is the author's responsibility to take these in writing.

Approval for reproduction/modification of any information (including figures and tables) published elsewhere must be obtained by the authors/copyright holders before submission of the manuscript. Contributors (Authors) are responsible for any copyright fee involved.

3. SUBMISSION OF MANUSCRIPTS

Manuscripts should be uploaded via this online submission page. The online submission is most efficient method for submission of papers, as it enables rapid distribution of manuscripts and consequently speeds up the review procedure. It also enables authors to know the status of their own manuscripts by emailing us. Complete instructions for submitting a paper is available below.

Manuscript submission is a systematic procedure and little preparation is required beyond having all parts of your manuscript in a given format and a computer with an Internet connection and a Web browser. Full help and instructions are provided on-screen. As an author, you will be prompted for login and manuscript details as Field of Paper and then to upload your manuscript file(s) according to the instructions.

To avoid postal delays, all transaction is preferred by e-mail. A finished manuscript submission is confirmed by e-mail immediately and your paper enters the editorial process with no postal delays. When a conclusion is made about the publication of your paper by our Editorial Board, revisions can be submitted online with the same procedure, with an occasion to view and respond to all comments.

Complete support for both authors and co-author is provided.

4. MANUSCRIPT'S CATEGORY

Based on potential and nature, the manuscript can be categorized under the following heads:

Original research paper: Such papers are reports of high-level significant original research work.

Review papers: These are concise, significant but helpful and decisive topics for young researchers.

Research articles: These are handled with small investigation and applications.

Research letters: The letters are small and concise comments on previously published matters.

5. STRUCTURE AND FORMAT OF MANUSCRIPT

The recommended size of original research paper is less than seven thousand words, review papers fewer than seven thousands words also.Preparation of research paper or how to write research paper, are major hurdle, while writing manuscript. The research articles and research letters should be fewer than three thousand words, the structure original research paper; sometime review paper should be as follows:

Papers: These are reports of significant research (typically less than 7000 words equivalent, including tables, figures, references), and comprise:

(a)Title should be relevant and commensurate with the theme of the paper.

(b) A brief Summary, "Abstract" (less than 150 words) containing the major results and conclusions.

(c) Up to ten keywords, that precisely identifies the paper's subject, purpose, and focus.

(d) An Introduction, giving necessary background excluding subheadings; objectives must be clearly declared.

(e) Resources and techniques with sufficient complete experimental details (wherever possible by reference) to permit repetition; sources of information must be given and numerical methods must be specified by reference, unless non-standard.

(f) Results should be presented concisely, by well-designed tables and/or figures; the same data may not be used in both; suitable statistical data should be given. All data must be obtained with attention to numerical detail in the planning stage. As reproduced design has been recognized to be important to experiments for a considerable time, the Editor has decided that any paper that appears not to have adequate numerical treatments of the data will be returned un-refereed;

(g) Discussion should cover the implications and consequences, not just recapitulating the results; conclusions should be summarizing.

(h) Brief Acknowledgements.

(i) References in the proper form.

Authors should very cautiously consider the preparation of papers to ensure that they communicate efficiently. Papers are much more likely to be accepted, if they are cautiously designed and laid out, contain few or no errors, are summarizing, and be conventional to the approach and instructions. They will in addition, be published with much less delays than those that require much technical and editorial correction.

The Editorial Board reserves the right to make literary corrections and to make suggestions to improve briefness.

It is vital, that authors take care in submitting a manuscript that is written in simple language and adheres to published guidelines.

Format

Language: The language of publication is UK English. Authors, for whom English is a second language, must have their manuscript efficiently edited by an English-speaking person before submission to make sure that, the English is of high excellence. It is preferable, that manuscripts should be professionally edited.

Standard Usage, Abbreviations, and Units: Spelling and hyphenation should be conventional to The Concise Oxford English Dictionary. Statistics and measurements should at all times be given in figures, e.g. 16 min, except for when the number begins a sentence. When the number does not refer to a unit of measurement it should be spelt in full unless, it is 160 or greater.

Abbreviations supposed to be used carefully. The abbreviated name or expression is supposed to be cited in full at first usage, followed by the conventional abbreviation in parentheses.

Metric SI units are supposed to generally be used excluding where they conflict with current practice or are confusing. For illustration, 1.4 l rather than 1.4 × 10-3 m3, or 4 mm somewhat than 4 × 10-3 m. Chemical formula and solutions must identify the form used, e.g. anhydrous or hydrated, and the concentration must be in clearly defined units. Common species names should be followed by underlines at the first mention. For following use the generic name should be constricted to a single letter, if it is clear.

Structure

All manuscripts submitted to Global Journals Inc. (US), ought to include:

Title: The title page must carry an instructive title that reflects the content, a running title (less than 45 characters together with spaces), names of the authors and co-authors, and the place(s) wherever the work was carried out. The full postal address in addition with the e-mail address of related author must be given. Up to eleven keywords or very brief phrases have to be given to help data retrieval, mining and indexing.

Abstract, used in Original Papers and Reviews:

Optimizing Abstract for Search Engines

Many researchers searching for information online will use search engines such as Google, Yahoo or similar. By optimizing your paper for search engines, you will amplify the chance of someone finding it. This in turn will make it more likely to be viewed and/or cited in a further work. Global Journals Inc. (US) have compiled these guidelines to facilitate you to maximize the web-friendliness of the most public part of your paper.

Key Words

A major linchpin in research work for the writing research paper is the keyword search, which one will employ to find both library and Internet resources.

One must be persistent and creative in using keywords. An effective keyword search requires a strategy and planning a list of possible keywords and phrases to try.

Search engines for most searches, use Boolean searching, which is somewhat different from Internet searches. The Boolean search uses "operators," words (and, or, not, and near) that enable you to expand or narrow your affords. Tips for research paper while preparing research paper are very helpful guideline of research paper.

Choice of key words is first tool of tips to write research paper. Research paper writing is an art.A few tips for deciding as strategically as possible about keyword search:

- One should start brainstorming lists of possible keywords before even begin searching. Think about the most important concepts related to research work. Ask, "What words would a source have to include to be truly valuable in research paper?" Then consider synonyms for the important words.
- It may take the discovery of only one relevant paper to let steer in the right keyword direction because in most databases, the keywords under which a research paper is abstracted are listed with the paper.
- One should avoid outdated words.

Keywords are the key that opens a door to research work sources. Keyword searching is an art in which researcher's skills are bound to improve with experience and time.

Numerical Methods: Numerical methods used should be clear and, where appropriate, supported by references.

Acknowledgements: Please make these as concise as possible.

References

References follow the Harvard scheme of referencing. References in the text should cite the authors' names followed by the time of their publication, unless there are three or more authors when simply the first author's name is quoted followed by et al. unpublished work has to only be cited where necessary, and only in the text. Copies of references in press in other journals have to be supplied with submitted typescripts. It is necessary that all citations and references be carefully checked before submission, as mistakes or omissions will cause delays.

References to information on the World Wide Web can be given, but only if the information is available without charge to readers on an official site. Wikipedia and Similar websites are not allowed where anyone can change the information. Authors will be asked to make available electronic copies of the cited information for inclusion on the Global Journals Inc. (US) homepage at the judgment of the Editorial Board.

The Editorial Board and Global Journals Inc. (US) recommend that, citation of online-published papers and other material should be done via a DOI (digital object identifier). If an author cites anything, which does not have a DOI, they run the risk of the cited material not being noticeable.

The Editorial Board and Global Journals Inc. (US) recommend the use of a tool such as Reference Manager for reference management and formatting.

Tables, Figures and Figure Legends

Tables: Tables should be few in number, cautiously designed, uncrowned, and include only essential data. Each must have an Arabic number, e.g. Table 4, a self-explanatory caption and be on a separate sheet. Vertical lines should not be used.

Figures: Figures are supposed to be submitted as separate files. Always take in a citation in the text for each figure using Arabic numbers, e.g. Fig. 4. Artwork must be submitted online in electronic form by e-mailing them.

Preparation of Electronic Figures for Publication

Even though low quality images are sufficient for review purposes, print publication requires high quality images to prevent the final product being blurred or fuzzy. Submit (or e-mail) EPS (line art) or TIFF (halftone/photographs) files only. MS PowerPoint and Word Graphics are unsuitable for printed pictures. Do not use pixel-oriented software. Scans (TIFF only) should have a resolution of at least 350 dpi (halftone) or 700 to 1100 dpi (line drawings) in relation to the imitation size. Please give the data for figures in black and white or submit a Color Work Agreement Form. EPS files must be saved with fonts embedded (and with a TIFF preview, if possible).

For scanned images, the scanning resolution (at final image size) ought to be as follows to ensure good reproduction: line art: >650 dpi; halftones (including gel photographs) : >350 dpi; figures containing both halftone and line images: >650 dpi.

Color Charges: It is the rule of the Global Journals Inc. (US) for authors to pay the full cost for the reproduction of their color artwork. Hence, please note that, if there is color artwork in your manuscript when it is accepted for publication, we would require you to complete and return a color work agreement form before your paper can be published.

Figure Legends: Self-explanatory legends of all figures should be incorporated separately under the heading 'Legends to Figures'. In the full-text online edition of the journal, figure legends may possibly be truncated in abbreviated links to the full screen version. Therefore, the first 100 characters of any legend should notify the reader, about the key aspects of the figure.

6. AFTER ACCEPTANCE

Upon approval of a paper for publication, the manuscript will be forwarded to the dean, who is responsible for the publication of the Global Journals Inc. (US).

6.1 Proof Corrections

The corresponding author will receive an e-mail alert containing a link to a website or will be attached. A working e-mail address must therefore be provided for the related author.

Acrobat Reader will be required in order to read this file. This software can be downloaded

(Free of charge) from the following website:

www.adobe.com/products/acrobat/readstep2.html. This will facilitate the file to be opened, read on screen, and printed out in order for any corrections to be added. Further instructions will be sent with the proof.

Proofs must be returned to the dean at dean@globaljournals.org within three days of receipt.

As changes to proofs are costly, we inquire that you only correct typesetting errors. All illustrations are retained by the publisher. Please note that the authors are responsible for all statements made in their work, including changes made by the copy editor.

6.2 Early View of Global Journals Inc. (US) (Publication Prior to Print)

The Global Journals Inc. (US) are enclosed by our publishing's Early View service. Early View articles are complete full-text articles sent in advance of their publication. Early View articles are absolute and final. They have been completely reviewed, revised and edited for publication, and the authors' final corrections have been incorporated. Because they are in final form, no changes can be made after sending them. The nature of Early View articles means that they do not yet have volume, issue or page numbers, so Early View articles cannot be cited in the conventional way.

6.3 Author Services

Online production tracking is available for your article through Author Services. Author Services enables authors to track their article - once it has been accepted - through the production process to publication online and in print. Authors can check the status of their articles online and choose to receive automated e-mails at key stages of production. The authors will receive an e-mail with a unique link that enables them to register and have their article automatically added to the system. Please ensure that a complete e-mail address is provided when submitting the manuscript.

6.4 Author Material Archive Policy

Please note that if not specifically requested, publisher will dispose off hardcopy & electronic information submitted, after the two months of publication. If you require the return of any information submitted, please inform the Editorial Board or dean as soon as possible.

6.5 Offprint and Extra Copies

A PDF offprint of the online-published article will be provided free of charge to the related author, and may be distributed according to the Publisher's terms and conditions. Additional paper offprint may be ordered by emailing us at: editor@globaljournals.org .

You must strictly follow above Author Guidelines before submitting your paper or else we will not at all be responsible for any corrections in future in any of the way.

Before start writing a good quality Computer Science Research Paper, let us first understand what is Computer Science Research Paper? So, Computer Science Research Paper is the paper which is written by professionals or scientists who are associated to Computer Science and Information Technology, or doing research study in these areas. If you are novel to this field then you can consult about this field from your supervisor or guide.

TECHNIQUES FOR WRITING A GOOD QUALITY RESEARCH PAPER:

1. Choosing the topic: In most cases, the topic is searched by the interest of author but it can be also suggested by the guides. You can have several topics and then you can judge that in which topic or subject you are finding yourself most comfortable. This can be done by asking several questions to yourself, like Will I be able to carry our search in this area? Will I find all necessary recourses to accomplish the search? Will I be able to find all information in this field area? If the answer of these types of questions will be "Yes" then you can choose that topic. In most of the cases, you may have to conduct the surveys and have to visit several places because this field is related to Computer Science and Information Technology. Also, you may have to do a lot of work to find all rise and falls regarding the various data of that subject. Sometimes, detailed information plays a vital role, instead of short information.

2. Evaluators are human: First thing to remember that evaluators are also human being. They are not only meant for rejecting a paper. They are here to evaluate your paper. So, present your Best.

3. Think Like Evaluators: If you are in a confusion or getting demotivated that your paper will be accepted by evaluators or not, then think and try to evaluate your paper like an Evaluator. Try to understand that what an evaluator wants in your research paper and automatically you will have your answer.

4. Make blueprints of paper: The outline is the plan or framework that will help you to arrange your thoughts. It will make your paper logical. But remember that all points of your outline must be related to the topic you have chosen.

5. Ask your Guides: If you are having any difficulty in your research, then do not hesitate to share your difficulty to your guide (if you have any). They will surely help you out and resolve your doubts. If you can't clarify what exactly you require for your work then ask the supervisor to help you with the alternative. He might also provide you the list of essential readings.

6. Use of computer is recommended: As you are doing research in the field of Computer Science, then this point is quite obvious.

7. Use right software: Always use good quality software packages. If you are not capable to judge good software then you can lose quality of your paper unknowingly. There are various software programs available to help you, which you can get through Internet.

8. Use the Internet for help: An excellent start for your paper can be by using the Google. It is an excellent search engine, where you can have your doubts resolved. You may also read some answers for the frequent question how to write my research paper or find model research paper. From the internet library you can download books. If you have all required books make important reading selecting and analyzing the specified information. Then put together research paper sketch out.

9. Use and get big pictures: Always use encyclopedias, Wikipedia to get pictures so that you can go into the depth.

10. Bookmarks are useful: When you read any book or magazine, you generally use bookmarks, right! It is a good habit, which helps to not to lose your continuity. You should always use bookmarks while searching on Internet also, which will make your search easier.

11. Revise what you wrote: When you write anything, always read it, summarize it and then finalize it.

12. Make all efforts: Make all efforts to mention what you are going to write in your paper. That means always have a good start. Try to mention everything in introduction, that what is the need of a particular research paper. Polish your work by good skill of writing and always give an evaluator, what he wants.

13. Have backups: When you are going to do any important thing like making research paper, you should always have backup copies of it either in your computer or in paper. This will help you to not to lose any of your important.

14. Produce good diagrams of your own: Always try to include good charts or diagrams in your paper to improve quality. Using several and unnecessary diagrams will degrade the quality of your paper by creating "hotchpotch." So always, try to make and include those diagrams, which are made by your own to improve readability and understandability of your paper.

15. Use of direct quotes: When you do research relevant to literature, history or current affairs then use of quotes become essential but if study is relevant to science then use of quotes is not preferable.

16. Use proper verb tense: Use proper verb tenses in your paper. Use past tense, to present those events that happened. Use present tense to indicate events that are going on. Use future tense to indicate future happening events. Use of improper and wrong tenses will confuse the evaluator. Avoid the sentences that are incomplete.

17. Never use online paper: If you are getting any paper on Internet, then never use it as your research paper because it might be possible that evaluator has already seen it or maybe it is outdated version.

18. Pick a good study spot: To do your research studies always try to pick a spot, which is quiet. Every spot is not for studies. Spot that suits you choose it and proceed further.

19. Know what you know: Always try to know, what you know by making objectives. Else, you will be confused and cannot achieve your target.

20. Use good quality grammar: Always use a good quality grammar and use words that will throw positive impact on evaluator. Use of good quality grammar does not mean to use tough words, that for each word the evaluator has to go through dictionary. Do not start sentence with a conjunction. Do not fragment sentences. Eliminate one-word sentences. Ignore passive voice. Do not ever use a big word when a diminutive one would suffice. Verbs have to be in agreement with their subjects. Prepositions are not expressions to finish sentences with. It is incorrect to ever divide an infinitive. Avoid clichés like the disease. Also, always shun irritating alliteration. Use language that is simple and straight forward. put together a neat summary.

21. Arrangement of information: Each section of the main body should start with an opening sentence and there should be a changeover at the end of the section. Give only valid and powerful arguments to your topic. You may also maintain your arguments with records.

22. Never start in last minute: Always start at right time and give enough time to research work. Leaving everything to the last minute will degrade your paper and spoil your work.

23. Multitasking in research is not good: Doing several things at the same time proves bad habit in case of research activity. Research is an area, where everything has a particular time slot. Divide your research work in parts and do particular part in particular time slot.

24. Never copy others' work: Never copy others' work and give it your name because if evaluator has seen it anywhere you will be in trouble.

25. Take proper rest and food: No matter how many hours you spend for your research activity, if you are not taking care of your health then all your efforts will be in vain. For a quality research, study is must, and this can be done by taking proper rest and food.

26. Go for seminars: Attend seminars if the topic is relevant to your research area. Utilize all your resources.

27. Refresh your mind after intervals: Try to give rest to your mind by listening to soft music or by sleeping in intervals. This will also improve your memory.

28. Make colleagues: Always try to make colleagues. No matter how sharper or intelligent you are, if you make colleagues you can have several ideas, which will be helpful for your research.

29. Think technically: Always think technically. If anything happens, then search its reasons, its benefits, and demerits.

30. Think and then print: When you will go to print your paper, notice that tables are not be split, headings are not detached from their descriptions, and page sequence is maintained.

31. Adding unnecessary information: Do not add unnecessary information, like, I have used MS Excel to draw graph. Do not add irrelevant and inappropriate material. These all will create superfluous. Foreign terminology and phrases are not apropos. One should NEVER take a broad view. Analogy in script is like feathers on a snake. Not at all use a large word when a very small one would be sufficient. Use words properly, regardless of how others use them. Remove quotations. Puns are for kids, not grunt readers. Amplification is a billion times of inferior quality than sarcasm.

32. Never oversimplify everything: To add material in your research paper, never go for oversimplification. This will definitely irritate the evaluator. Be more or less specific. Also too, by no means, ever use rhythmic redundancies. Contractions aren't essential and shouldn't be there used. Comparisons are as terrible as clichés. Give up ampersands and abbreviations, and so on. Remove commas, that are, not necessary. Parenthetical words however should be together with this in commas. Understatement is all the time the complete best way to put onward earth-shaking thoughts. Give a detailed literary review.

33. Report concluded results: Use concluded results. From raw data, filter the results and then conclude your studies based on measurements and observations taken. Significant figures and appropriate number of decimal places should be used. Parenthetical remarks are prohibitive. Proofread carefully at final stage. In the end give outline to your arguments. Spot out perspectives of further study of this subject. Justify your conclusion by at the bottom of them with sufficient justifications and examples.

34. After conclusion: Once you have concluded your research, the next most important step is to present your findings. Presentation is extremely important as it is the definite medium though which your research is going to be in print to the rest of the crowd. Care should be taken to categorize your thoughts well and present them in a logical and neat manner. A good quality research paper format is essential because it serves to highlight your research paper and bring to light all necessary aspects in your research.

Informal Guidelines of Research Paper Writing

Key points to remember:

- Submit all work in its final form.
- Write your paper in the form, which is presented in the guidelines using the template.
- Please note the criterion for grading the final paper by peer-reviewers.

Final Points:

A purpose of organizing a research paper is to let people to interpret your effort selectively. The journal requires the following sections, submitted in the order listed, each section to start on a new page.

The introduction will be compiled from reference matter and will reflect the design processes or outline of basis that direct you to make study. As you will carry out the process of study, the method and process section will be constructed as like that. The result segment will show related statistics in nearly sequential order and will direct the reviewers next to the similar intellectual paths throughout the data that you took to carry out your study. The discussion section will provide understanding of the data and projections as to the implication of the results. The use of good quality references all through the paper will give the effort trustworthiness by representing an alertness of prior workings.

Writing a research paper is not an easy job no matter how trouble-free the actual research or concept. Practice, excellent preparation, and controlled record keeping are the only means to make straightforward the progression.

General style:

Specific editorial column necessities for compliance of a manuscript will always take over from directions in these general guidelines.

To make a paper clear

· Adhere to recommended page limits

Mistakes to evade

- Insertion a title at the foot of a page with the subsequent text on the next page
- Separating a table/chart or figure - impound each figure/table to a single page
- Submitting a manuscript with pages out of sequence

In every sections of your document

· Use standard writing style including articles ("a", "the," etc.)

· Keep on paying attention on the research topic of the paper

· Use paragraphs to split each significant point (excluding for the abstract)

· Align the primary line of each section

· Present your points in sound order

· Use present tense to report well accepted

· Use past tense to describe specific results

· Shun familiar wording, don't address the reviewer directly, and don't use slang, slang language, or superlatives

· Shun use of extra pictures - include only those figures essential to presenting results

Title Page:

Choose a revealing title. It should be short. It should not have non-standard acronyms or abbreviations. It should not exceed two printed lines. It should include the name(s) and address (es) of all authors.

Abstract:

The summary should be two hundred words or less. It should briefly and clearly explain the key findings reported in the manuscript--must have precise statistics. It should not have abnormal acronyms or abbreviations. It should be logical in itself. Shun citing references at this point.

An abstract is a brief distinct paragraph summary of finished work or work in development. In a minute or less a reviewer can be taught the foundation behind the study, common approach to the problem, relevant results, and significant conclusions or new questions.

Write your summary when your paper is completed because how can you write the summary of anything which is not yet written? Wealth of terminology is very essential in abstract. Yet, use comprehensive sentences and do not let go readability for briefness. You can maintain it succinct by phrasing sentences so that they provide more than lone rationale. The author can at this moment go straight to shortening the outcome. Sum up the study, with the subsequent elements in any summary. Try to maintain the initial two items to no more than one ruling each.

- Reason of the study - theory, overall issue, purpose
- Fundamental goal
- To the point depiction of the research
- Consequences, including definite statistics - if the consequences are quantitative in nature, account quantitative data; results of any numerical analysis should be reported
- Significant conclusions or questions that track from the research(es)

Approach:

- Single section, and succinct
- As a outline of job done, it is always written in past tense
- A conceptual should situate on its own, and not submit to any other part of the paper such as a form or table
- Center on shortening results - bound background information to a verdict or two, if completely necessary
- What you account in an conceptual must be regular with what you reported in the manuscript
- Exact spelling, clearness of sentences and phrases, and appropriate reporting of quantities (proper units, important statistics) are just as significant in an abstract as they are anywhere else

Introduction:

The **Introduction** should "introduce" the manuscript. The reviewer should be presented with sufficient background information to be capable to comprehend and calculate the purpose of your study without having to submit to other works. The basis for the study should be offered. Give most important references but shun difficult to make a comprehensive appraisal of the topic. In the introduction, describe the problem visibly. If the problem is not acknowledged in a logical, reasonable way, the reviewer will have no attention in your result. Speak in common terms about techniques used to explain the problem, if needed, but do not present any particulars about the protocols here. Following approach can create a valuable beginning:

- Explain the value (significance) of the study
- Shield the model - why did you employ this particular system or method? What is its compensation? You strength remark on its appropriateness from a abstract point of vision as well as point out sensible reasons for using it.
- Present a justification. Status your particular theory (es) or aim(s), and describe the logic that led you to choose them.
- Very for a short time explain the tentative propose and how it skilled the declared objectives.

Approach:

- Use past tense except for when referring to recognized facts. After all, the manuscript will be submitted after the entire job is done.
- Sort out your thoughts; manufacture one key point with every section. If you make the four points listed above, you will need a least of four paragraphs.

- Present surroundings information only as desirable in order hold up a situation. The reviewer does not desire to read the whole thing you know about a topic.
- Shape the theory/purpose specifically - do not take a broad view.
- As always, give awareness to spelling, simplicity and correctness of sentences and phrases.

Procedures (Methods and Materials):

This part is supposed to be the easiest to carve if you have good skills. A sound written Procedures segment allows a capable scientist to replacement your results. Present precise information about your supplies. The suppliers and clarity of reagents can be helpful bits of information. Present methods in sequential order but linked methodologies can be grouped as a segment. Be concise when relating the protocols. Attempt for the least amount of information that would permit another capable scientist to spare your outcome but be cautious that vital information is integrated. The use of subheadings is suggested and ought to be synchronized with the results section. When a technique is used that has been well described in another object, mention the specific item describing a way but draw the basic principle while stating the situation. The purpose is to text all particular resources and broad procedures, so that another person may use some or all of the methods in one more study or referee the scientific value of your work. It is not to be a step by step report of the whole thing you did, nor is a methods section a set of orders.

Materials:

- Explain materials individually only if the study is so complex that it saves liberty this way.
- Embrace particular materials, and any tools or provisions that are not frequently found in laboratories.
- Do not take in frequently found.
- If use of a definite type of tools.
- Materials may be reported in a part section or else they may be recognized along with your measures.

Methods:

- Report the method (not particulars of each process that engaged the same methodology)
- Describe the method entirely
- To be succinct, present methods under headings dedicated to specific dealings or groups of measures
- Simplify - details how procedures were completed not how they were exclusively performed on a particular day.
- If well known procedures were used, account the procedure by name, possibly with reference, and that's all.

Approach:

- It is embarrassed or not possible to use vigorous voice when documenting methods with no using first person, which would focus the reviewer's interest on the researcher rather than the job. As a result when script up the methods most authors use third person passive voice.
- Use standard style in this and in every other part of the paper - avoid familiar lists, and use full sentences.

What to keep away from

- Resources and methods are not a set of information.
- Skip all descriptive information and surroundings - save it for the argument.
- Leave out information that is immaterial to a third party.

Results:

The principle of a results segment is to present and demonstrate your conclusion. Create this part a entirely objective details of the outcome, and save all understanding for the discussion.

The page length of this segment is set by the sum and types of data to be reported. Carry on to be to the point, by means of statistics and tables, if suitable, to present consequences most efficiently.You must obviously differentiate material that would usually be incorporated in a study editorial from any unprocessed data or additional appendix matter that would not be available. In fact, such matter should not be submitted at all except requested by the instructor.

Content

- Sum up your conclusion in text and demonstrate them, if suitable, with figures and tables.
- In manuscript, explain each of your consequences, point the reader to remarks that are most appropriate.
- Present a background, such as by describing the question that was addressed by creation an exacting study.
- Explain results of control experiments and comprise remarks that are not accessible in a prescribed figure or table, if appropriate.
- Examine your data, then prepare the analyzed (transformed) data in the form of a figure (graph), table, or in manuscript form.

What to stay away from

- Do not discuss or infer your outcome, report surroundings information, or try to explain anything.
- Not at all, take in raw data or intermediate calculations in a research manuscript.
- Do not present the similar data more than once.
- Manuscript should complement any figures or tables, not duplicate the identical information.
- Never confuse figures with tables - there is a difference.

Approach

- As forever, use past tense when you submit to your results, and put the whole thing in a reasonable order.
- Put figures and tables, appropriately numbered, in order at the end of the report
- If you desire, you may place your figures and tables properly within the text of your results part.

Figures and tables

- If you put figures and tables at the end of the details, make certain that they are visibly distinguished from any attach appendix materials, such as raw facts
- Despite of position, each figure must be numbered one after the other and complete with subtitle
- In spite of position, each table must be titled, numbered one after the other and complete with heading
- All figure and table must be adequately complete that it could situate on its own, divide from text

Discussion:

The Discussion is expected the trickiest segment to write and describe. A lot of papers submitted for journal are discarded based on problems with the Discussion. There is no head of state for how long a argument should be. Position your understanding of the outcome visibly to lead the reviewer through your conclusions, and then finish the paper with a summing up of the implication of the study. The purpose here is to offer an understanding of your results and hold up for all of your conclusions, using facts from your research and generally accepted information, if suitable. The implication of result should be visibly described. Infer your data in the conversation in suitable depth. This means that when you clarify an observable fact you must explain mechanisms that may account for the observation. If your results vary from your prospect, make clear why that may have happened. If your results agree, then explain the theory that the proof supported. It is never suitable to just state that the data approved with prospect, and let it drop at that.

- Make a decision if each premise is supported, discarded, or if you cannot make a conclusion with assurance. Do not just dismiss a study or part of a study as "uncertain."
- Research papers are not acknowledged if the work is imperfect. Draw what conclusions you can based upon the results that you have, and take care of the study as a finished work
- You may propose future guidelines, such as how the experiment might be personalized to accomplish a new idea.
- Give details all of your remarks as much as possible, focus on mechanisms.
- Make a decision if the tentative design sufficiently addressed the theory, and whether or not it was correctly restricted.
- Try to present substitute explanations if sensible alternatives be present.
- One research will not counter an overall question, so maintain the large picture in mind, where do you go next? The best studies unlock new avenues of study. What questions remain?
- Recommendations for detailed papers will offer supplementary suggestions.

Approach:

- When you refer to information, differentiate data generated by your own studies from available information
- Submit to work done by specific persons (including you) in past tense.
- Submit to generally acknowledged facts and main beliefs in present tense.

Please carefully note down following rules and regulation before submitting your Research Paper to Global Journals Inc. (US):

Segment Draft and Final Research Paper: You have to strictly follow the template of research paper. If it is not done your paper may get rejected.

- The **major constraint** is that you must independently make all content, tables, graphs, and facts that are offered in the paper. You must write each part of the paper wholly on your own. The Peer-reviewers need to identify your own perceptive of the concepts in your own terms. NEVER extract straight from any foundation, and never rephrase someone else's analysis.

- Do not give permission to anyone else to "PROOFREAD" your manuscript.

- Methods to avoid Plagiarism is applied by us on every paper, if found guilty, you will be blacklisted by all of our collaborated research groups, your institution will be informed for this and strict legal actions will be taken immediately.)
- To guard yourself and others from possible illegal use please do not permit anyone right to use to your paper and files.

Criterion for Grading a Research Paper (Compilation) by Global Journals Inc. (US)

Please note that following table is only a Grading of "Paper Compilation" and not on "Performed/Stated Research" whose grading solely depends on Individual Assigned Peer Reviewer and Editorial Board Member. These can be available only on request and after decision of Paper. This report will be the property of Global Journals Inc. (US).

Topics	Grades		
	A-B	**C-D**	**E-F**
Abstract	Clear and concise with appropriate content, Correct format. 200 words or below	Unclear summary and no specific data, Incorrect form Above 200 words	No specific data with ambiguous information Above 250 words
Introduction	Containing all background details with clear goal and appropriate details, flow specification, no grammar and spelling mistake, well organized sentence and paragraph, reference cited	Unclear and confusing data, appropriate format, grammar and spelling errors with unorganized matter	Out of place depth and content, hazy format
Methods and Procedures	Clear and to the point with well arranged paragraph, precision and accuracy of facts and figures, well organized subheads	Difficult to comprehend with embarrassed text, too much explanation but completed	Incorrect and unorganized structure with hazy meaning
Result	Well organized, Clear and specific, Correct units with precision, correct data, well structuring of paragraph, no grammar and spelling mistake	Complete and embarrassed text, difficult to comprehend	Irregular format with wrong facts and figures
Discussion	Well organized, meaningful specification, sound conclusion, logical and concise explanation, highly structured paragraph reference cited	Wordy, unclear conclusion, spurious	Conclusion is not cited, unorganized, difficult to comprehend
References	Complete and correct format, well organized	Beside the point, Incomplete	Wrong format and structuring

INDEX

save our planet

Global Journal of Computer Science and Technology

Visit us on the Web at www.GlobalJournals.org | www.ComputerResearch.org
or email us at helpdesk@globaljournals.org

ISSN 9754350