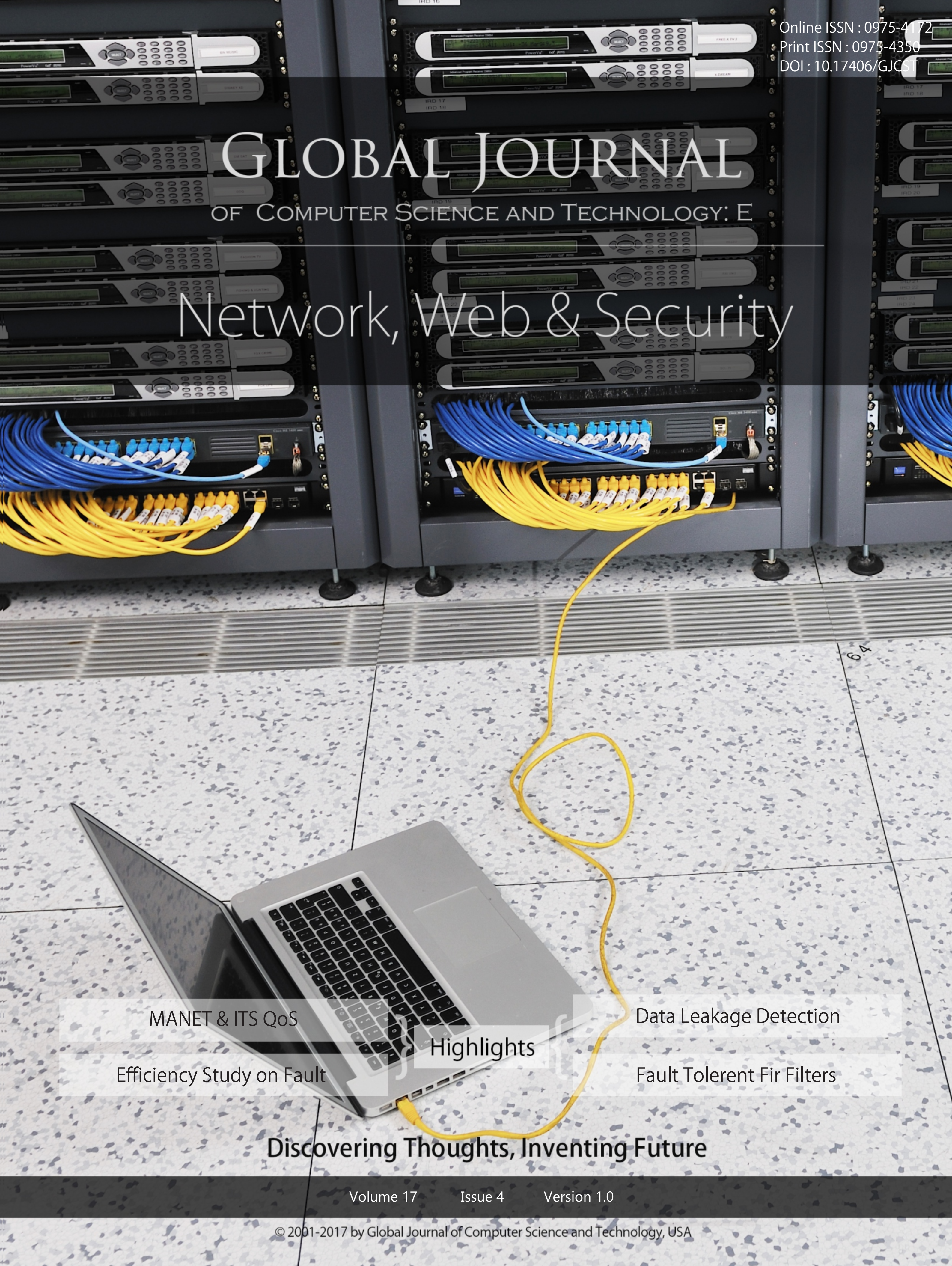
Online ISSN : 0975-4172
Print ISSN : 0975-4350
DOI : 10.17406/GJCST

Global Journal of Computer Science and Technology: E

Network, Web & Security



MANET & ITS QoS

Efficiency Study on Fault

Highlights

Data Leakage Detection

Fault Tolerent Fir Filters

Discovering Thoughts, Inventing Future

Volume 17 Issue 4 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 17 Issue 4 (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
945th Concord Streets,
Framingham Massachusetts Pin: 01701,
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 Pvt Ltd
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)

Editorial Board

Global Journal of Computer Science and Technology

Contents of the Issue

Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 17 Issue 4 Version 1.0 Year 2017
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

FREE HIT –A Novel History Based Reinforcement Approach for Fast Path Construction in Vehicular Ad Hoc Networks

By Abhilash Kumar Reddy Manchu & A. Rama Mohan Reddy
Sri Venkateswara University College of Engineering

Abstract- Vehicular ad hoc networks playing significant role in development of intelligent transport system and rise in demand for accessing fascinated applications such as entertainment and advertisements in vehicles via internet leverages to build efficient routing mechanisms. Due to rapid vehicles flow in Vanets, network often subjected to link breaks and creates delay in communication which affects overall network performance, hence to address these serious issue earlier approaches focused on parameters like rate estimation, feedback and link-expiration-time but being different from earlier our Instant Look up and Immediate Action(ILU-IA) technique uses adaptive learning thru past knowledge. ILU-IA identifies immediate neighbour (Free-Hit-Node) efficiently at point of link failure using Case-Based-Learning and Q-learning techniques. Simulation analysis shows that proposed approach performance improved in terms of throughput with negligible delay also reduces network overhead.

Keywords: *vanets, graph-attribute, case-based-learning, q-learning, path reliability, intelligent road side units.*

GJCST-E Classification: *C.2.1, G.2.2*

FREE HIT –A Novel History Based Reinforcement Approach for Fast Path Construction in Vehicular Ad Hoc Networks

Abhilash Kumar Reddy Manchu [α] & A. Rama Mohan Reddy [σ]

Abstract- Vehicular ad hoc networks playing significant role in development of intelligent transport system and rise in demand for accessing fascinated applications such as entertainment and advertisements in vehicles via internet leverages to build efficient routing mechanisms. Due to rapid vehicles flow in Vanets, network often subjected to link breaks and creates delay in communication which affects overall network performance, hence to address these serious issue earlier approaches focused on parameters like rate estimation, feedback and link-expiration-time but being different from earlier our Instant Look up and Immediate Action(ILU-IA) technique uses adaptive learning thru past knowledge. ILU-IA identifies immediate neighbour (Free-Hit-Node) efficiently at point of link failure using Case-Based-Learning and Q-learning techniques. Simulation analysis shows that proposed approach performance improved in terms of throughput with negligible delay also reduces network overhead.

Keywords: vanets, graph-attribute, case-based-learning, q-learning, path reliability, intelligent road side units.

I. Introduction

Vanets [1],[2] comprise of vehicles and road side units which offer direct information exchanges between vehicles and vehicles to and from RSU and exchanges information like current traffic and sharing high priority messages using dedicated short range protocol for communication. Now a day's vehicle on road increases phenomenally and creates more difficulty to handle all vehicles under single point of control to address this issue one way is to use hierarchical topology where vehicles are grouped into clusters and one cluster head is elected to manage group members as shown in fig 1. For inter cluster communication Cluster Head(CH) selects one node in group to act as gateway and considerable amount of work has been carried out for cluster creation, maintenance and knowledge sharing [3],[4] and clusters are internally connected to road side units in order to exchange information between clusters as well as RSUs .In existing to establish reliable routing Hashem & Owens [5] proposed SAMQ algorithm which provides routing reliability by make use of "situation awareness", routing decisions would be taken only after comprehensive analysis of current traffic patterns with stored patterns, then suitable actions will be taken to revive situation additionally SAMQ utilizes ant colony system algorithm for searching feasible paths.

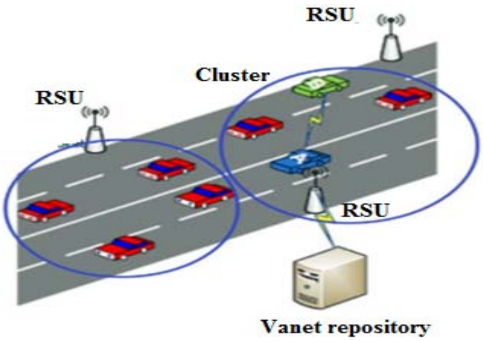


Fig. 1: Vanets Cluster Architecture

Author α: Research Scholar, Computer Science and Engineering, SVUCE, Tirupati, Andhra Pradesh.
Author σ: Professor & Head, Computer Science and Engineering, SVUCE, Tirupati, Andhra Pradesh.
e-mails: abhilash.svu@gmail.com, ramamohansvu@gmail.com

In other existing approaches [6],[7] whenever link failure occurs control signals were used to search new node or block to forward packet towards destination which increases network overhead. In another research [8] buffering technique used to store packets temporarily until new path traced out or source initiates [9] a new path from beginning again in all above approaches RREQ flooding and ACK signals were required to find new node which wastes network bandwidth here point to be consider that vanets are delay sensitive networks, sure it would consume some amount of valuable network time to search new neighbour node, assigning addresses and diverting packets results in delay. To overcome aforementioned issues in proposed system cluster head collects and sends various traffic situations information like number of vehicles in clusters their velocities, moving direction and positions etc. along with above information CH maps traffic patterns to Intelligent road side units (IRSU) .Initially Cluster Heads sends collected traffic patterns to repository later CBL and Q-learning algorithms applied for machine learning. In this paper our intention is to reduce network overhead and delay by applying "instant look up and immediate action " from past experiences , section-II shows state-of-art while section-III describes methodology and algorithms , section- IV shows performance evaluation and section-V concludes the work

II. State-Of-Art

In research [10] fuzzy logic and rate-estimation-algorithm used for finding reliable path between source and destination. Fuzzy logic is used select straight link and mostly applied to real time applications where information about things is not accurate. it uses linguistic terms to define the facts while Q-learning algorithm adjusts behavior of nodes using trial and error base. Q-Table dynamically updates its contents like action and state of vehicle environment by agent. Whenever changes occur in states immediately the same should mirror in Q-Table otherwise learning data is unused. Transfer learning is used to apply learned knowledge to another similar environment, so that decision making would be ease and faster for new arriving nodes. Finally to find reliable end to end path both route selection and rate estimation process were used. In [11] to enhance optimized link state routing author combined four metaheuristics techniques to achieve automatic optimization process. Simulated annealing for finding global best solutions to given function. Genetic algorithm (Panmictic & decentralized) used here to solve multicast routing issues also identifies best selections based on minimum time factor in local optima, particle swarm optimization at global level calculates second minimum shortest time using differential evaluation for efficient resource scheduling to minimize packet loss ratio. In[12] vehicles are grouped thru velocities so that assumption is all moving with same pace therefore stability also high. ROMSGP technique gathers group information based on Link-Expiration-Time, Stable link selections based on expiration time i.e. Long LET, whenever path goes down immediately RERR message would send to source node. One alternate is choosing next best path without link breakages accordingly routing table is then modified and another solution if there is no alternate path from break point source again initiates route discovery if no of hops from source to break point is minimum otherwise local recovery process will be initiated .So here usage of control messages were minimized and reduced communication delay but gathering vehicles with same speed, calculating LET and route discovery process would increase in more computational complexity which may not suitable for dynamic networks like Vanets. In [13] automatic rate fall back (ARF) periodically sends probes with different speed rates i.e. lower rate and higher rate, if it faces more continuous packet loss in either cases based on minimum losses it may choose higher or lower speeds but would not suitable for dynamic networks. Sample rate initially sends data with maximum rates based and based on failures (more than four packet losses) it stops sending and then chooses another rate at which capable of forwarding packets.

This technique stores total information like number of transmissions, success ratios, failure details and timings , for further transmissions algorithm analysis history stored in table and chooses best rate to accomplish maximum throughput. In research [14] Reinforcement learning (RL) is used to acquire knowledge of given space by observing behavior in order to improve machine intelligence. Combinatorial – optimization- problems (COPs) such as limited resources allocation for more requirements and dynamic search space where hard to find optimal possibilities. Distributed RL (DRL) is used for solving COPs in a simple way like what-to-do and how to map discovered states to actions, here agent selects actions based on feedback from earlier states and actions. The agent intent is to collect and summarize feedback received from initial ceremonial to final state so that machine could precisely take decisions for further created search space. In[15] Q-learning is used with AODV where all the node entries in Q-table contains distance and next hop information i.e. Q(d,x) values ranging from 0 to 1 whereas dynamic Q-table size depends on number of neighbour and destination nodes. Table information and learning information distributed to all neighbors. QL-AODV used dynamic routing to avoid route and link breaks to attain maximum throughput also without delay revives path with current track of information.

Collaborative feedback learning [16] used to give optimization solutions by analyzing information from multiple agents. In CRL an isolated agents monitors system states and continuously updates gathered information to optimal policy table maintained by agents and based on this feedback learning decisions would be taken and Markov processes used to model feedback (reinforce) learning problems and SAMPLE algorithm tunes with changing scenarios dynamically to maximize throughput. Minimum-delay-routing algorithm [17] uses two-ways of vehicles in cluster to forward message from source to destination. MDRA technique applied to identify end to end path with minimum delay and epidemic routing is used to avoid duplicate packets such that cluster contains single-copy of message. To find distance between vehicles author used probability distribution function for message forwarding process, Markov-renewal technique and dijkstra's algorithm is used to find reliable and optimal path with less delay. In [18] VOEG -VANET oriented Evolving graph paradigm used prediction algorithm to find vehicles at particular instant and EG-dijkstra's (Evolving- Graph) technique is used to find reliable path and reliable graph[RG] array stores overall vehicle information so that whenever path is required then RG generates most optimal and reliable routes. If the link is not there in between two nodes i.e. reliability equals to zero then VOEG verifies current traffic conditions and adjusted to new node to attain journey reliability using graph information which avoids route requesting process but graph based approach well suited for static or slow speed networks. In MOZO [19] for decision making a captain node is elected and cluster members for each cluster also named as zones to forward packets form source to destination. Dijkstra's procedure to compute the shortest path and for zone formation moving object modeling and indexing techniques were used. CLV-Tree algorithm calculates and maintains similar vehicles information (velocity, direction, position).

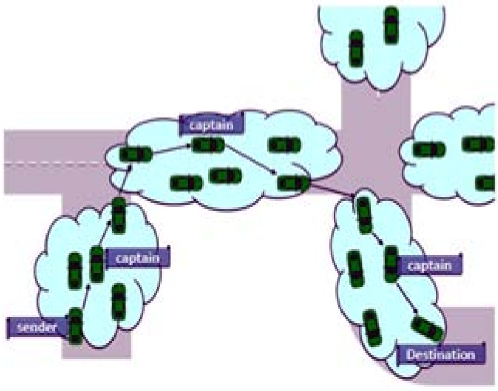


Fig. 2: Moving zone based protocol model

VADD [20] supports multi hop data forwarding using carry and forward technique particularly for sparse area networks whenever node carrying packets notable find path then node simply carries packets until next node comes to availability. VADD uses Directed Graph to represent vehicular network and Dijkstra's method to compute shortest path basic idea is to reduce forwarding distance without loops for that purpose author designed H-VADD. In [21] Node rotation concept is used here for increase network lifetime so the power consumption of all the nodes would be equally utilized. Repeated-optimal-matching used to make multiple rounds to identify nodes that are optimally matched and gathers local information from other nodes like energy, position and load. Consumption-swap-rate-algorithm swaps only the nodes at high rate consumption positions. Energy level swap used for nodes which come down below threshold energy point.

In [5] SAMQ initially gets complete insight of vehicular network like locations, velocities, traffic information, behavior of drivers and environmental conditions etc. Current situation of network could be analyzed by using gathered information. With precise information routing algorithms estimates link life time between nodes i.e. reliability of link and last appropriate actions will be taken to discover path between two nodes in case of current link failure. SAMQ uses Ant-Colony-System algorithm to build optimization solutions with three common rules Pheromone deposit, State Transition and Pheromone evaporation.

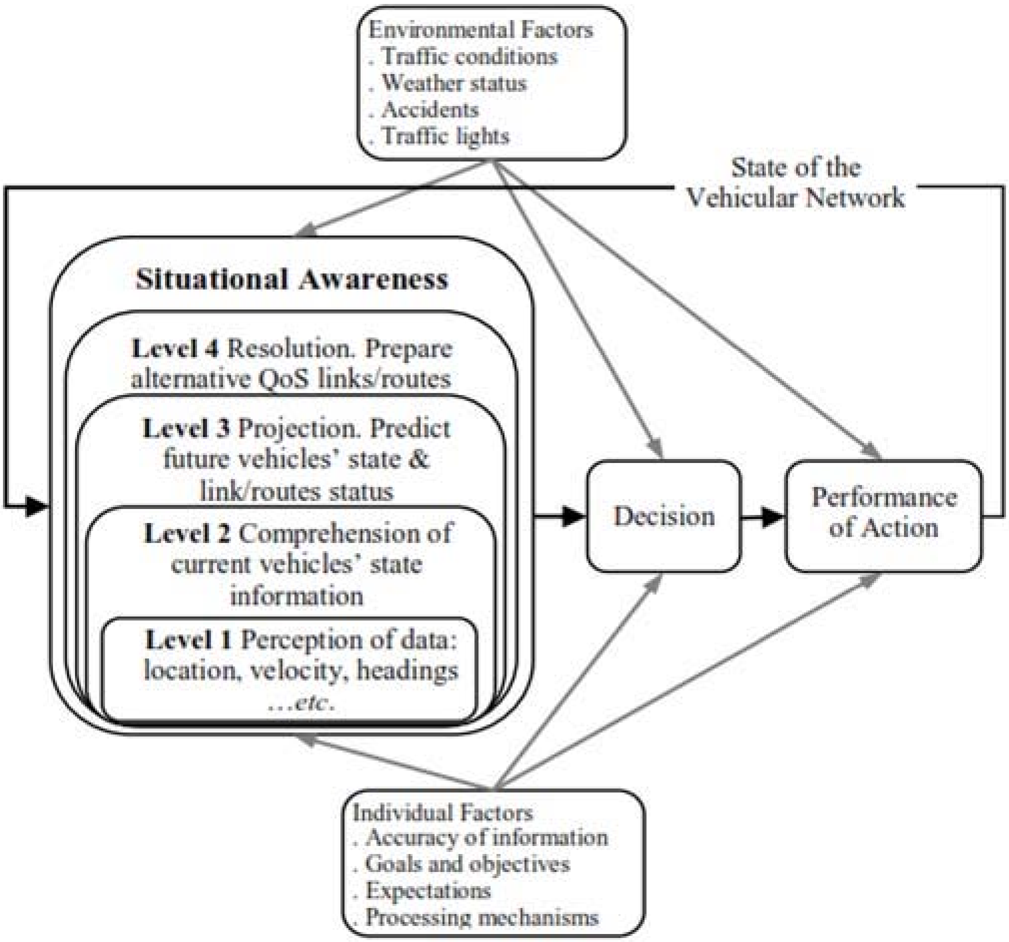

Environmental Factors
. Traffic conditions
. Weather status
. Accidents
. Traffic lights
State of the Vehicular Network
Situational Awareness
Level 4 Resolution. Prepare alternative QoS links/routes
Level 3 Projection. Predict future vehicles' state & link/routes status
Level 2 Comprehension of current vehicles' state information
Level 1 Perception of data: location, velocity, headings ...etc.
Decision
Performance of Action
Individual Factors
. Accuracy of information
. Goals and objectives
. Expectations
. Processing mechanisms

Fig.3: SMAQ Model

It aims to select reliable path among alternatives proactively rules pheromone deposit, State Transition and pheromone evaporation. Motivation for our proposed drawn from SAMQ technique.

III. Glimpse of Proposed System

a) Instant Look up –Immediate Action (ILU-IA)

1. Intelligent RSU's (IRSU) Collects clusters state information i.e. number of vehicles, positions, directions and link failures points at various traffic situations and reliable path links and stores in repository server.
2. Later Case Based Learning and Q- learning algorithms applied on stored data for Learning.
3. All cluster head maps their current traffic patterns to IRSU's, instantly IRSU picks information from server and sends corresponding data like expected failure points and reliable links etc. to cluster heads.
4. Using past information cluster head can anticipate where exactly link failures could occur in particular traffic pattern then immediately locates a position nearer to failure point and temporarily allocates a node called free hit node (FHN) to handover packets for smooth communication.

IV. System Model

Cluster Maintenance

In general Cluster comprises of Cluster Head (CH) also Cognitive node which is responsible for cluster maintenance and Cluster Members (CMs) used to carry and forward packets and one gateway node for inter cluster communication along with above nodes proposed solution maintains two significant nodes called:

1. Free Hit Node (FHN).
2. Recently Link Failure Node (RFN).

Intelligent Road side Units: We assume that all clusters are connected to set of road side units (RSU's) in turn RSU's are connected to main server. Initially RSU, s collects live traffic information from clusters and updates same in main server also shares information between clusters.

Repository Server: Graph structures are used to store traffic patterns in repository later machine learning algorithms are applied to train server, once current traffic pattern matches with stored pattern then essential feedback will send cluster head to manage situations such as link failure points and reliable paths patterns.

Handling Link breaks: Cluster Head knows concise traffic information bit early with the use of it CH identifies and temporarily reserves a special node which is labeled as FREE HIT NODE (FHN) nearer to position where link break might occur and FHN cannot be used by another task except waits to get connect with node at link failure point and CH adds necessary information like FHN address to data packets and also stores path details in FHN from point of failure .

Node Rotation: Proposed uses node rotation [21] concept for efficient utilization of failure nodes because whenever link break arises CH diverts packets to Free-Hit-Node from point of failure for sending packets towards destination but here recently link failed node (RFN) becomes free from usage at particular situation so in order to rehash RFN we used node rotation so that later RFN could be used as FHN or co–operative node. Vanets - Graph Based Mobility Model:

To epitomize VANETs, proposed system uses graphs where vehicles and links can be showed as vertices and edges and below fig shows grid graph modeling used to represent cluster type of networks.

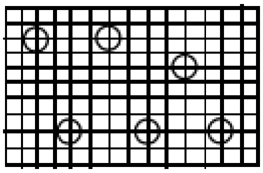


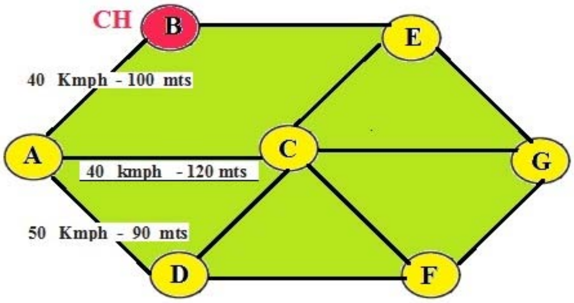
Fig.4: Grid graph

Gross area (GA) = > gross length and gross width of the graph and assuming all nodes are communication under same radio frequencies R.

C Max Graph □ Maximum graph walk coverage with set of edges E and l(e) is length of edge e. Cmaxg approximately equals to sum of all edges multiplied with radio frequency range diameter [22].this equation suitable for short ranges like cluster based networks.

$$\boldsymbol{CMAX = \sum l(e) * 2R}$$

$$\textbf{\textit{e belongs to E}}$$

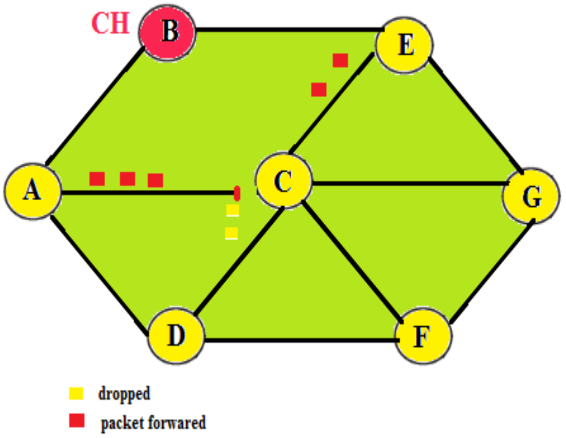


Node	NeighbourNode - Speed - Distance
A	B - 40 Kmph - 100 mts D - 50 Kmph - 90 mts C - 40 kmph - 120 mts
D	C - 40kmph - 90 mts F - 45kmph - 100mts

Fig. 5: shows graph representation

Intelligent RSU (IRSU) collects live traffic information from cluster head and forwards to server, initially all the patterns allowed to store into repository later server discards if similar pattern arises.

IRSU explores state of link failures and reliable paths i.e. in certain traffic pattern- speed of vehicle, position, direction, and link status and active information (link failure patters & reliable paths) etc. later information pushed into repository server.



Node	NeighbourNode - Speed - Distance
A	B - 40 Kmph - 100 mts D - 50 Kmph - 90 mts C - 40 kmph - 120 mts
D	C - 40kmph - 90 mts F - 45kmph - 100mts

A --> C Link Failure

Fig. 6: Link failure situation

V. ALGORITHMS

Case-Based Learning for Attribute Graphs

CBL algorithms [23],[24] basic feature is to extract re-usable cases which have relevant structures to the new patterns and uses hierarchical decision trees tot stores graph attributes so that information retrieval becomes simple and fast. Initially CBL stores all traffic patterns knowledge and rehash the information obtained to new similar patterns from previous quality solutions, generally instance based learning models applied to solve tasks like real valued functions, in proposed case-based-reasoning (CBR) algorithm used to match complex traffic pattern instances also for efficient indexing to extract matched patters and this model usually collect and store traffic patterns in database and compares new traffic patterns with stored ones to find best fit match and immediately pushes pattern state to Q-learning module for necessary actions to avoid link failures fig.6 Case based learning and Q-learning framework.

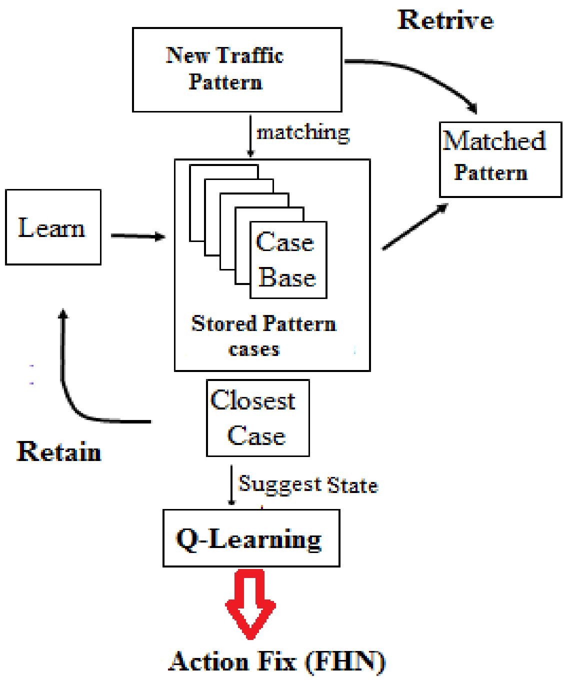


Fig. 7: Case Based Learning & Q-Learning Frame work

Q-learning Algorithm to locate Free Hit Node

Q-Learning [25] is kind of reinforcement process used to estimate the values of state and action pairs i.e.

For each step "s "selects action "a" which maximizes fun Q(s, a)

Where Q→ estimated function
s → State
a → Action.

In proposed Q (traffic patterns states, actions)→ action specifies where to place "FHN" for corresponding traffic pattern.

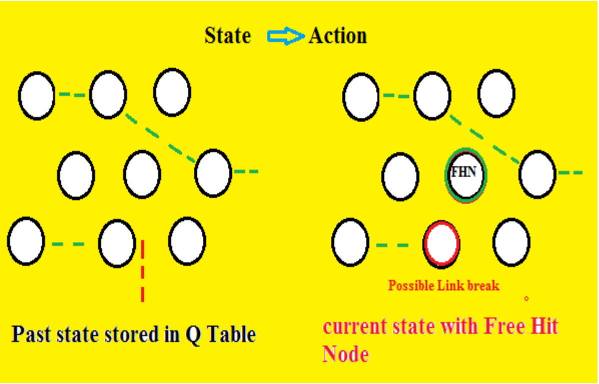

State
Action
FHN
Possible Link break
Past state stored in Q Table
current state with Free Hit Node

Fig. 8: Free hit node

```
Q-Learning Process
  Initialize Q (tps, a) randomly
While (For Each Traffic Pattern State stored in
                Q- table derived from CBL)
{
 IF (Current state matched)
   THEN
      If there is no failure points then
        Q (TPS, a)→c + Q (TPS, Null);
          // action = Null; Else
      Q (Pattern, a)→ Q (TPS, action →Link
                     Break point, FHN (nn)
//adds link break points and predicts optimal
        neighbour node
     End if;
END IF;
}
```

VI. EXPERIMENTAL SETTING AND PERFORMANCE ANALYSIS

This section demonstrates our ILU–IA features improved in terms of reducing end to end delay, minimizes packet drop ratio and reduces time taken to find neighbour node when compared with existing approaches. The vehicular traffic is generated using network simulator with some initial values like 40m/sec speed; each cluster comprises maximum 10 vehicles, acceleration values -7 to 7m/s2 and rate of data packets 15packets/sec. Performance evaluation factors:-

Routing overhead: In proposed system total number of control messages for finding new node almost negligible because our history based prediction approach straight way expects and places free hit node (FHN) nearer to failure.

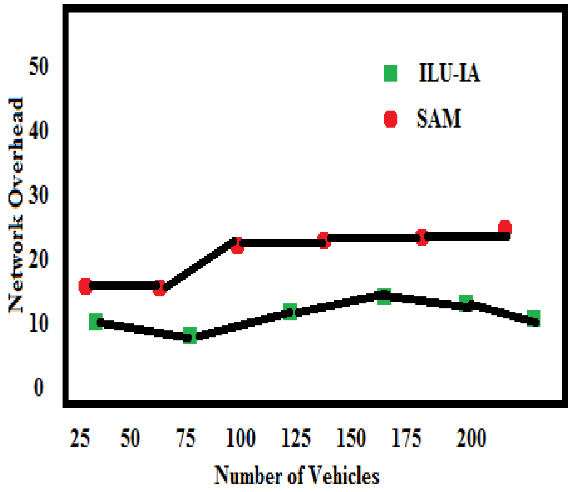


Fig. 7: Network over head

Packet drop ratio: Due to dynamic decision making nature of ILU-IA approach, link failures can efficiently handle by cluster head therefore reduces packet drop ratio between vehicles.

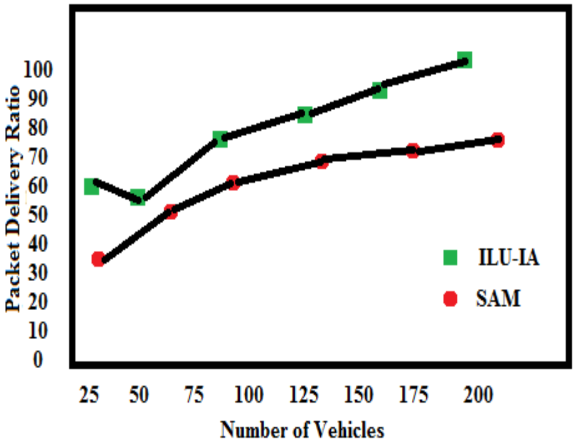


Fig. 8: Packet delivery ratio

Transmission delay: aforementioned parameters are directly reflects delay, in our proposed approach both routing overhead and packet drop ratios minimized. Hence end to end delay also reduced.

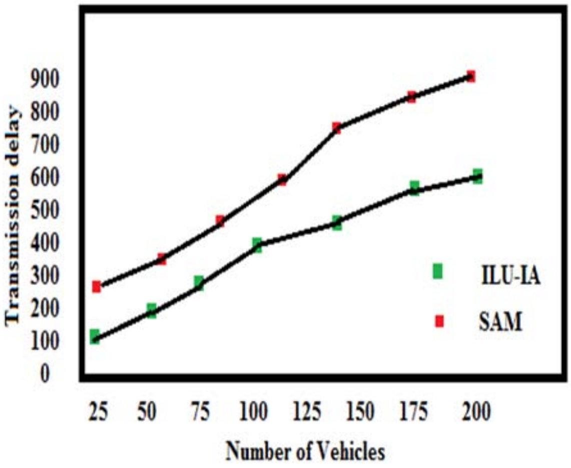


Fig. 9: Transmission delay

VII. Conclusion

In this research we introduced innovative solution to construct fast path restoration in cluster based vehicular networks. The main objective behind ILU-IA protocol is that instead of looking for new neighbour node after link break, which in turn produces more delay and packet drops. Our proposed system uses past experiences or history to handle any kind of situation efficiently here cluster head could able to foresee entire behavior of current network with information obtained from IRSU like expected failure points, packet drop points etc. so proactively cluster head selects alternative nodes nearer to failure points. Simulation analysis shows ILU-IA outstanding performance in terms accomplishing high throughput and increase in overall network performance.

References Références Referencias

1. Hartenstein and Labrteaux, "A tutorial survey on vehicular Ad hoc Networks", IEEE communications, June 2008.
2. Abhilash and Rama Mohan reddy," A survey on vehicular ad hoc networks routing protocols", I-managers JMT, Vol 3 No 2 July 2016.
3. Hamza and Benayad," A hybrid routing protocol for vanet using ontology ", science direct, pp. 94-101, 2015.
4. Abhilash and Rama Mohan Reddy," Position based channel allocation for vehicular ad hoc networks", IJANA, Vol 8, issue 4 , Feb 2017.
5. Hashem, owens, qiang and shi," Situation aware qos routing algorithm for vehicular ad hoc networks", IEEE Transactions,2015.
6. Wahab, otrok and mourad," Qos based clustering protocol for vehicular ad hoc networks", Elsever, computer communications, 2013.

7. Hum Kim and Lee, "Reliable routing protocol for vehicular ad hoc networks ", Elsevier, Journal of Elec and communications Feb 2010.
8. Amitkothari and Ashok,"on demand temporary parallel route for frequent link failure in ad hoc networks", IJCA, Vol 11, pp. 11-17.
9. Perkins and Royer ,"Ad hoc on demand distance vector routing", IEEE WMCSA ,pp. 90-1000 , 1999.
10. Celimuge, yusheng and Fuqiang," Toward practical and intelligent routing in vanets", IEEE Transactions ,Vol 64 ,No 12 ,Dec 2015.
11. Toutouh and Garcia," Intelligent olsr routing protocol optimization for vanets", IEEE Trans, Vol 61, No 4, May 2012.
12. Taleb, Sakhaee, Jamalipour and Hashimtoto," A stable routing protocol to support ITS In Vanets", IEEE trans, Vol 56, No 6 Nov 2007.
13. Mohamed and Bahget," A performance evalution for rate adaptation algorithms in wireless networks", IJCA,Vol 99, No 4 Aug 2014.
14. Czibula and Bocico," A distributed reinforcement learning approach for solving optimization problems", researches IT Aprl 2015.
15. Celimuge, Kumekawa and kato "Distributed Reinforcement learning approach vanets", IEICE Trans, Vol 93 No 6,June 2010.
16. Dowling, curran and Cunningham," using feedback in collaborative reinforcement learning to optimize manet routing ",IEEE , May2005.
17. jianping He , Lin and Pan," Delay analysis and routing for two dimensional vanets using carry and forward mechanism ",IEEE July 2017..
18. Hashem and qiang," An evolving graph based reliable routing scheme for vanets ", IEEE transactions, Vol 62, No 4, May 2013.
19. Lin, Kang, Squiiciarini and gurang," A moving zone based routing protocol using pure v2v comm in vanets", IEEE Trans , May 2017.
20. Zhao and Guohong ," Vehicle assisted data delivery vehicular ad hoc networks", IEEE Transactions ,Vol 57,No 3, May 2008.
21. Moukaddem, Torng and Guoliang," Maximizing network topology lifetime using mobile node rotation", IEEE transactions 2013.
22. Tian, Hahner, Beckerand stepanov," Graph based mobility model for mobile ad hoc network" European ,CAR Talk project ,2000.
23. Burke, Mac carthy and petrovic," structured cases in case based reasoning", Elsevier Knowledge base systems, pp.159-165,2000.
24. Aha David ," case based learning algorithms", workshop 1991
25. Watkins, " Learning from delayed rewards", Thesis , Cambridge 1989.

Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 17 Issue 4 Version 1.0 Year 2017
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Capacity-Aware Control Topology in MANET

By Madhusudan G & Kumar TNR

Abstract- The wireless mobile adhoc networks are dynamically Varying, the network performance may change by different unknown parameters such as the total number of nodes in the network, the transmission power range of the network and area of deployment of the network. The main aim is to increase the efficiency of the system through dynamically changing the trasmission range on every node of the network. contention index is the network performance factor is considered. we presented a study of the effects of contention index on the network performance, considering capacity of the network and efficiency of the power. The result is that the capacity is a concave function of the contention index. if the contention index is large the impact of node mobility is minimal on the network performance. we presented GridMobile, a distributed Network topology algorithm that attempts to shows the best possiblity, by maintaining optimal contention index by dynamically adjusting the transmission range on every nodes in the network

Keywords: MANET, MAC, GRIDMOBILE.

GJCST-E Classification: B.4.3, C.2.1

Capacity-Aware Control Topology in MANET

Madhusudan G [α] & Kumar TNR [σ]

Abstract- The wireless mobile adhoc networks are dynamically Varying, the network performance may change by different unknown parameters such as the total number of nodes in the network, the transmission power range of the network and area of deployment of the network. The main aim is to increase the efficiency of the system through dynamically changing the trasmission range on every node of the network. contention index is the network performance factor is considered. we presented a study of the effects of contention index on the network performance, considering capacity of the network and efficiency of the power. The result is that the capacity is a concave function of the contention index. if the contention index is large the impact of node mobility is minimal on the network performance. we presented GridMobile, a distributed Network topology algorithm that attempts to shows the best possiblity, by maintaining optimal contention index by dynamically adjusting the transmission range on every nodes in the network.

Keywords: MANET, MAC, GRIDMOBILE.

I. Introduction

Manet is infrastructure less collection of mobile nodes with multi hop network gives fast network establishment, that communicate over relatively bandwidth constrained wireless links [13] [14]. Mobile Ad-Hoc Networks (MANETs) represent an interesting substrate for many types of applications that do not require a fixed network infrastructure (Access Points) [11].The combination of wireless communications such as new technology is in diversity wireless bandwidth and increase in reliability. The adjustment of transmission power through the dynamic transmission power control protocol is an effective technique to reduce the power consumption of a network [15] [16]. The conventional broadcasting information to direct source-destination signal, while cooperative communication [1][2] to take advantage of user diversity combined signal decoding the source destination signs direct and relayed signals of interest. It is challenging to develop robust routing protocol for dynamic Mobile Ad Hoc Networks (MANET). Geographic routing protocols [7] [8] are generally more scalable and reliable than conventional topology-based routing protocols [9] [10] with their forwarding decisions based on the local topology. The Selection of proper relay transmission rate can maximize reliability [10]. The mathematical model will derives the relationship between energy consumption and node transmission power ranges, if the adhoc network is stationary without mobility of the nodes of the network. This model may be used to optimize the topology to conserve less power. But the transmission power range is not a independent component that affects power efficiency and network capacity. The changing number of nodes in the network and the physical area of deployment plays a major role in adhoc networks. In order to identify one single parameter in controlling the network performance, The term contention index, plays a major role in adhoc network. The contention index means the number of contending nodes within the interference range. In this work, the term contention index, rather than the transmission power range on each node, is the important and independent driving force that influences the network performance. The results of the simulation shows that the network capacity is a concave function of contention index. The optimal values of contention index will achieve the best possible performance. Base on the performance evaluation of simulation results, we propose *GridMobile*, Capacity-aware control topology algorithm is used to ensure that the every node in a mobile adhoc network adjusts the transmission power ranges to maintain optimal contention index which may lead to a topology that yields optimal performance in terms of network capacity and power efficiency. The network is stationary, with uniform node density and fixed transmission power ranges. Previous studies on capacity of wireless networks have been reported in [5], [6]. It has been shown that the per-node capacity may be estimated in the order of $O(1/\sqrt{n})$, n being the number of nodes in the network. However, the compensating effects of local per-node transmission range an adjustment on the network performance has yet to be studied [3].

We formally define the contention index as the within the transmission power range, The total number of network nodes avialable, B*ut* the interference range is differnt. The parameter is referred to as the contention index, since it represents the potential congestion level in the local neighborhood of the network. For the Open System Interconnection medium Access Control protocol, we assumed that the transmission ranges of all nodes are identical. The contention index is related to three parameters in the simulation setup: (i) the total number of nodes n; (ii) the physical area of deployment of the network L^2 (iii) the node transmission power range[3] Naturally, when there are more nodes in the network, the contention in the network increases. Each node adopts a larger transmission range, or decreeasing size of the network area. With the node density D calculated as n/L^2, the contention index, CI, is

Author α: Asst. Professor, Department of CS & E, SJCE, Mysore.
e-mail: madhusudan@sjce.ac.in
Author σ: Asst. Professor, Department of CS & E, MSRIT, Bangaluru.
e-mail: tnrkumar@msrit.edu

the product of node density and area of the network size of local transmission range:

$$CI = D\pi R^2 = n\pi R^2 / L^2 \qquad (1)$$

We vary the contention index in the performance evaluations as a primary driving force, in order to measure its impact on the performance of the network in terms of network capacity and power efficiency[3].

In dense network when two nodes are close to each other, a low transmission power is sufficient for communication [17].

MANET applications include supporting battlefield communications, emergency relief scenarios, law enforcement, public meeting, virtual class room, and other security-sensitive computing environments. The ad-hoc networking technology has stimulated substantial research activities in the past years [12].

II. MobileGrid

MobileGrid is the nodes in mobile ad hoc networks to make fully localized decisions on the optimal transmission range to maintain an optimal contention index, so that the network capacity is optimized. The node can estimate the contention index by knowing how many neighbors a node has. Based on this observation, The distributed topology control algorithm, called GridMobile, is implemented as a three-phase protocol, executed at each node periodically (by the end of each time window) to accommodate node mobility.

The different phases to be followed in the implementation are as follows:

Phase 1: Estimating Contention Index: with its current transmission power (or maximum power at 0^n time window) a node starts to discover its neighbors at the MAC layer by hearing both control (e.g. RTS/CTS/ACK) and data messages. Since the header of each message contains the source node ID, the node may compute the number of unique node IDs that it may overhear over the time window. Such a set of unique node identifiers forms the set of neighbors that the node may find. Such a passive approach does not introduce additional overhead to the existing network traffic. Tthe nodes may not be able to detect "silent" nodes in the neighborhood that did not transmit any control or data messages. We argue that, since such silent nodes did not inject network traffic in the current time window, the possibility that they start to transmit in the next time window is low. In this case, the calculation of contention index may safely ignore such nodes. If the discovered number of neighboring nodes is N, the estimated contention index CI is N + 1.

Phase 2: Looking up Optimal Values of the Contention Index if the system operating around an optimal value of contention index, Each node looks up in a particular optimization table to determine the table stores optimal values of contention index to maximize the network capacity, which it may obtain from off-line experiments using identical physical, Medium Access Control routing layer characteristics and parameters. Since the optimal contention index is an inherent property that does not vary much when changing node mobility, we may safely assume that such an optimization table may not need to be updated frequently. With respect to an interested QoS parameter such as network capacity, if the contention index it has estimated from the first phase does not fall into the specific optimal range in the table, the node proceeds to the next phase to adjust its transmission range. Otherwise, the current transmission range is adopted for the next time window.

Phase 3: Transmission Range Adjustments: In the second phase, each node decides that its current transmission range is not optimal by a table look-up, uses the following scheme to eventually keep it checked within the range of optimal contention index values. If the contention index *CI* calculated in the first phase is out of the optimal range in the optimization table (either smaller than the lower bound or higher than the upper bound), the node tunes the transmission power *R* as illustrated in Equation: Rnew = min(√CI optimal/CI current Rcurrent,Rmax)where *R*max is the maximum transmission range decided by the physical layer and radio characteristics, and CI optimal is chosen as the median point of the optimal range in the table.

This scheme guarantees convergence towards either the maximum range *R*max, or the optimal range of contention indices, whichever appears earlier.

III. Experiments on The Mobile Grid Algorithm

In order to evaluate if Grid *Mobile* works as effective as the centralized solution in previous performance evaluations, we use a snapshot of a wireless adhoc network in an area of 350 meters by 350 meters where each node's maximum transmission range is 200 meters. The number of nodes in such a network varies from 20 to 200. Network capacity is chosen to be optimized and the optimal contention index *CI* is set to be 6. Both the average transmission power and standard deviation of transmission powers are measured in the experiments, where average transmission power is calculated as the sum of transmission powers at each node divided by number of nodes in the network. The standard deviation of transmission powers is calculated to demonstrate how diverse the transmission ranges among all network nodes are. Figure below 3.1 (a) demonstrates the respective average transmission range in the resulted topology based on the centralized solution and MobileGrid algorithm. We result is that the two curves are very close to each other, which means that GridMobile performs nearly better as compared to the centralized solution. Furthermore, this results does not change with the total number of nodes in the network. In the centralized solution, all nodes are supposed to adopt a uniform transmission. Hence, in Figure below 3.2.(b) the curve for the centralized solution is flat with values of 0. However, in GridMobile, the standard deviation of transmission powers is always positive because the network is not evenly distributed, different nodes adopts different powers to cover the same number of neighboring nodes. As we may observe, the standard deviation of transmission powers tends to decline with the large number of nodes in the network. The results are considered comparing the centralized solution and GridMobile, Considering the parameters Average Transmission range and Standard Deviation of Transmission ranges. The Graph shows that the GridMobile Technique provides better solution compared to Centralized solution [3].

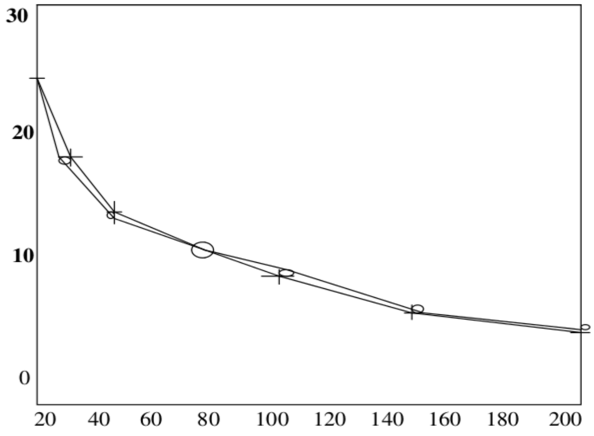


Fig 3.1: (a) Centralized Solution vs. GridMobile

(Average Transmission Power)

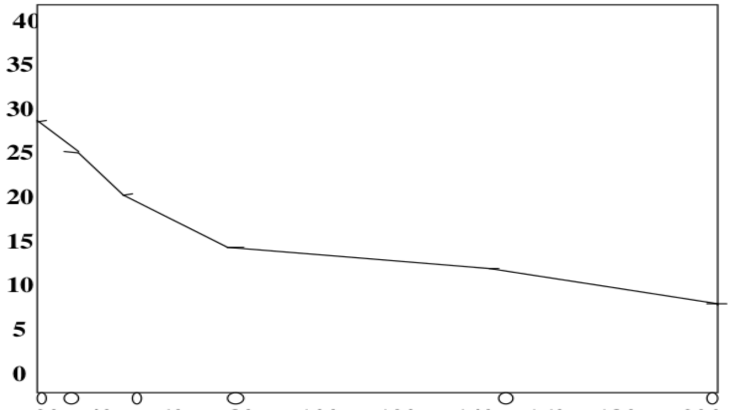


Fig 3.2: (b) Centralized Solution vs. GridMobile

(Standard Deviation of Transmission Power)

IV. Conclusion and Future Work

We introduced an interesting important parameter, contention index, in mobile ad hoc networks. With extensive performance evaluations, it is found that the contention index is the primary factor force that influences the network performance with respect to network capacity and power efficiency of the network. Furthermore, Maximum values of the contention index do exist to optimize the network performance. GridMobile, a distributed topology control algorithm, is introduced to ensure optimality regarding the contention index. It is proved to be effective by the simulation results.

Futute works comprises considering different parameters of the network constriants, the system is campared with the same parameter contention index.

References Références Referencias

1. A Nosratinia T. Hunter, and A. Hedayat, “Cooperative communication in wireless networks,” IEEE Commun.Mag., vol. 42, no. 10, pp. 74-80, 2004.
2. L. Cottatellucci X. Master, E. G. Larsson, and A. Ribera, “Cooperative communications in wireless networks,” EURASIP J. Wireless Commun. Newt. Vol. 2009, 2009.
3. MobileGrid: Capacity-aware Topology Control in Mobile Ad Hoc Networks Jilei Liu, Baochun Li Department of Electrical and Computer Engineering University of Toronto{jennie, bli}@eecg.toronto.edu.
4. K. Woradit, T. Quek, W. Suwansantisuk, M. Win, L. Wuttisittikulkij, and H. Wymeersch, “Outage behavior of selective relaying schemes,” IEEE Trans. Wireless
5. Commun., vol. 8, no. 8, pp. 3890-3895, 2009. P. Gupta and P. R. Kumar, “The Capacity of Wireless Networks,” vol. 46, no. 2, pp. 388–404, March 2000.
6. J. Li, C. Blake, D. S. J. De Couto, H.I.Lee, and R. Morris, “Capacity of Ad Hoc Wireless Networks,” in Proceedings of the 7th ACM International Conference on Mobile Computing and Networking, Rome, Italy, July 2001, pp. 61–69.
7. Karp and H. T. Kung, “Greedy perimeter stateless routing for wireless networks,” in ACM/IEEE MOBICOM, August 2000, pp. 243–254.
8. Y. Ko and N. Vaidya, “Location-aided routing in mobile ad hoc networks,” in ACM/IEEE MOBICOM, August 1998.
9. E. Perkins and E. M. Royer, “Ad-hoc on-demand distance vectorrouting,” in Proc. 2nd IEEE Workshop on Mobile Comp. Sys. and Apps., February 1999, pp. 99–100.
10. D. B. Johnson and D. A. Maltz, “Dynamic source routing in ad-hoc wireless networks,” Mobile Computing, T. Imielinski and H. Korth, Eds., Kluwer, pp. 153–81, 1996.
11. Pedro Garcia Lopez,Raul Gracia Tinedo,”Topology-Aware Group Communication Middleware for MANETs”http://ast-deim.urv.cat/mchannel_documentati on/comsware_2009.pdf
12. Jagrati Nagdiya, Shweta Yadav, Study of Various IP Auto-configuration Techniques, International Journal of Scientific & Engineering Research, Volume 4, Issue 8, August-2013
13. Shih-Lin Wu and Yu Chee Tseng. Wireless Ad Hoc Networking. Auerbach Publications, 2007.
14. M. Ilyas and I. Mahgoub. Mobilecomputing handbook. CRC, 2004.
15. S. Misra, I. Woungang, and S.C. Misra. Guide to Wireless Ad Hoc Networks. Springer, 2009
16. E.M. Royer and C.K. Toh. A review of current routing protocols for ad hoc mobile wireless networks. Personal Communications, IEEE, 6(2):46-55, 1999.
17. S. Singh, M. Woo, and C.S. Raghavendra. Power-aware routing in mobile ad hoc networks. Proceedings of the 4th annual ACM/IEEE international conference on Mobile computing and networking, pages 181-190, 1998I.

Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 17 Issue 4 Version 1.0 Year 2017
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Data Leakage Detection

By Rajesh Kumar

Manav Rachna International University

Abstract- Perturbation is a very useful technique where the data is modified and made 'less sensitive´ before being handed to agents. For example, one can add random noise to certain attributes, or one can replace exact values by ranges. However, in some cases it is important not to alter the original distributor's data. For example, if an outsourcer is doing our payroll, he must have the exact salary and customer bank account numbers. If medical researchers will be treating patients (as opposed to simply computing statistics), they may need accurate data for the patients. Traditionally, leakage detection is handled by watermarking, e.g., a unique code is embedded in each distributed copy. If that copy is later discovered in the hands of an unauthorized party, the leaker can be identified. Watermarks can be very useful in some cases, but again, involve some modification of the original data. Furthermore, watermarks can sometimes be destroyed if the data recipient is malicious. In this paper we study unobtrusive techniques for detecting leakage of a set of objects or records. Specifically we study the following scenario: After giving a set of objects to agents, the distributor discovers some of those same objects in an unauthorized place.

GJCST-E Classification: *K.8.1, B.4.2*

Data Leakage Detection

Rajesh Kumar

Abstract- Perturbation is a very useful technique where the data is modified and made 'less sensitive´ before being handed to agents. For example, one can add random noise to certain attributes, or one can replace exact values by ranges. However, in some cases it is important not to alter the original distributor's data. For example, if an outsourcer is doing our payroll, he must have the exact salary and customer bank account numbers. If medical researchers will be treating patients (as opposed to simply computing statistics), they may need accurate data for the patients. Traditionally, leakage detection is handled by watermarking, e.g., a unique code is embedded in each distributed copy. If that copy is later discovered in the hands of an unauthorized party, the leaker can be identified. Watermarks can be very useful in some cases, but again, involve some modification of the original data. Furthermore, watermarks can sometimes be destroyed if the data recipient is malicious. In this paper we study unobtrusive techniques for detecting leakage of a set of objects or records. Specifically we study the following scenario: After giving a set of objects to agents, the distributor discovers some of those same objects in an unauthorized place.

I. Introduction

In the course of doing business, sometimes sensitive data must be handed over to supposedly trusted third parties. For example, a hospital may give patient records to researchers who will devise new treatments. Similarly, a company may have partnerships with other companies that require sharing customer data. Another enterprise may outsource its data processing, so data must be given to various other companies. We call the owner of the data the distributor and the supposedly trusted third parties the agents. Our goal is to detect when the distributor's sensitive data has been leaked by agents, and if possible to identify the agent that leaked the data.

The distributor can assess the likelihood that the leaked data came from one or more agents, as opposed to having been independently gathered by other means. Using an analogy with cookies stolen from a cookie jar, if we catch Freddie with a single cookie, he can argue that a friend gave him the cookie. But if we catch Freddie with 5 cookies, it will be much harder for him to argue that his hands were not in the cookie jar. If the distributor sees 'enough evidence´ that an agent leaked data, he may stop doing business with him, or may initiate legal proceedings. In this paper we develop a model for assessing the 'guilt´ of agents. We also present algorithms for distributing objects to agents, in a way that improves our chances of identifying a leaker. Finally, we also consider the option of adding 'fake´ objects to the distributed set. Such objects do not correspond to real entities but appear realistic to the agents. In a sense, the fake objects acts as a type of watermark for the entire set, without modifying any individual members. If it turns out an agent was given one or more fake objects that were leaked, then the distributor can be more confident that agent was guilty[1].

The distributor may be able to add fake objects to the distributed data in order to improve his effectiveness in detecting guilty agents. However, fake objects may impact the correctness of what agents do, so they may not always be allowable[1]. The idea of perturbing data to detect leakage is not new, e.g.,. However, in most cases, individual objects are perturbed, e.g., by adding random noise to sensitive salaries, or adding a watermark to an image. In our case, we are perturbing the set of distributor objects by adding fake elements. In some applications, fake objects may cause fewer problems that perturbing real objects. For example, say the distributed data objects are medical records and the agents are hospitals. In this case, even small modifications to the records of actual patients may be undesirable. However, the addition of some fake medical records may be acceptable, since no patient matches these records, and hence no one will ever be treated based on fake records. Our use of fake objects is inspired by the use of 'trace´ records in mailing lists.

In this case, company A sells to company B a mailing list to be used once (e.g., to send advertisements). Company A adds trace records that contain addresses owned by company A. Thus, each time company Buses the purchased mailing list, A receives copies of the mailing. These records area type of fake objects that help identify improper use of data. The distributor creates and adds fake objects to the data that he distributes to agents. We let Fi _ Ri be the subset of fake objects that agent Ui receives.

As discussed below, fake objects must be created carefully so that agents cannot distinguish them from real objects. In many cases, the distributor may be limited in how many fake objects he can create. For example, objects may contain email addresses, and each fake email address may require the creation of an actual inbox (otherwise the agent may discover the object is fake). The inboxes can actually be monitored by the distributor: if email is received from someone other than the agent who was given the address, it is

Author: *Manav Rachna International University.*
e-mail: rajesh.sharmag96@gmail.com

evidence that the address was leaked. Since creating and monitoring email accounts consumes resources, the distributor may have a limit of fake objects. If there is a limit, we denote it by B fake objects. Similarly, the distributor may want to limit the number of fake objects received by each agent, so as to not arouse suspicions and to not adversely impact the agent's activities. Thus, we say that the distributor can send up to bi fake objects to agent Ui Creation.

The creation of fake but real-looking objects is a non-trivial problem whose thorough investigation is beyond the scope of this paper. Here, we model the creation of a fake object for agent Ui as a black-box function CREATE FAKE OBJECT(Ri; Fi; Condi) that takes as input the set of all objects Ri, the subset of fake objects.Fi that Ui has received so far and Condi, and returns anew fake object. This function needs Condi to produce a valid object that satisfies Ui's condition. Set Ri is needed as input so that the created fake object is not only valid but also indistinguishable from other real objects. For example, the creation function of a fake payroll record that includes an employee rank and a salary attribute may take into account the distribution of employee ranks, the distribution of salaries as well as the correlation between the two attributes. Ensuring that key statistics do not change by the introduction of fake objects is important if the agents will be using such statistics in their work.

II. Literature Survey

a) *Agent Guilt Model*

Suppose an agent Ui is guilty if it contributes one or more objects to the target. The event that agent Ui is guilty for a given leaked set S diesnoted by G i| S. The next step is to estimate Pr {Gi| S }, i.e., the probability that agentGi is guilty given evidence S.

To compute the Pr {Gi| S}, estimate the probability that values in Sbcean "guessed" by the target. For instance, say some of the objects in t are emails of individuals. Conduct an experiment and ask a person to find the email of say 100 individuals, the person may only discover say 20, leading to an estimate of 0.2. Call this estimate as pt, the probability that object t can be guessed by the target.

The two assumptions regarding the relationship among the various leakage events.

Assumption 1: For all t, t ∈ S such that ∉ T the provenance of t is independent of the provenance of T.

The term provenance in this assumption statement refers to the source of a value t that appears in the leaked set. The source can be any of the agents who have t in their sets or the target itself.

Assumption 2: An object t ∈ S can only be obtained by the target in one of two ways.

- A single agent Ui leaked t from its own Ri set, or
- The target guessed (or obtained through other means) t without the help of any of the n agents.

To find the probability that an agent Ui is guilty given a set S, consider the target guessed t1 with probability p and that agent leaks t1 to Sthweith probability 1-p. First compute the probability that he leaks a single object t to S. To compute this, define the set of agents V_t= {U_i | t<-R_t} that have t in their data sets. Then using Assumption 2 and known probability p,

We have,

$$\Pr\{\text{some agent leaked t to S}\} = 1\text{- p} \qquad (1.1)$$

Assuming that all agents that belong to Vt can leak t to S with equal probability and using Assumption 2 obtain,

$$\Pr\{\text{Ui leaked t to S}\} = \qquad (1.2)$$

Given that agent Ui is guilty if he leaks at least one value to S, with Assumption 1 and Equation 1.2 compute the probability Pr { Gr| S}, agentUi is guilty,

$$\Pr\{\text{Gi}|\text{ S}\} \qquad (1.3)$$

b) *Data Allocation Problem*

The distributor "intelligently" gives data to agents in order to improve the chances of detecting a guilty agent. There are four instances of this problem, depending on the type of data requests made by agents and whether "fake objects" [4] are allowed. Agent makes two types of requests, called sample and explicit. Based on the requests the fakes objects are added to data list.

Fake objects are objects generated by the distributor that are not in set T. The objects are designed to look like real objects, and are distributed to agents together with the T objects, in order to increase the chances of detecting agents that leak data.

c) *Optimization Problem*

The distributor's data allocation to agents has one constraint and one objective. The distributor's constraint is to satisfy agents' requests, by providing them with the number of objects they request or with all available objects that satisfy their conditions. His objective is to be able to detect an agent who leaks any portion of his data.

We consider the constraint as strict. The distributor may not deny serving an agent request and may not provide agents with different perturbed versions of the same objects. The fake object distribution as the only possible constraint relaxation. The objective is to maximize the chances of detecting a guilty agent that leaks all his data objects.

The Pr {G_i |S =R_i } or simply Pr {G_i |R_i } is the probability that agent U_i is guilty if the distributor discovers a leaked table S that contains all R_i objects. The difference functions Δ (i, j) is defined as:

$$\Delta\ (i,\ j) = \Pr\ \{G_i\ |R_i\ \} - \Pr\ \{G\ |R_i\ \} \qquad (1.4)$$

i. *Problem Definition*

Let the distributor have data requests from n agents. The distributor wants to give tables

R1, .Rn. to agents, U1 . . . , Un

respectively, so that

- Distribution satisfies agents' requests; and
- Maximizes the guilt probability differences Δ (i, j) for all i, j = 1. . . n and i= j.

Assuming that the sets satisfy the agents' requests, we can express the problem as a multi-criterion

ii. *Optimization Problem*

Maximize (. . . , Δ (i, j), . . .) i! = j (1.5)

(Over R1,….., Rn,)

The approximation [3] of objective of the above equation does not depend on agent's probabilities and therefore minimize the relative overlap among the agents as

Minimize (. . . ,(|Ri∩Rj|) / Ri , . . .) i != j (1.6)

(over R1 , . . . ,Rn)

This approximation is valid if minimizing the relative overlap, (|Ri∩Rj|) / Ri maximizes Δ (i, j).

III. Allocation Strategies Algorithm

There are two types of strategies algorithms

a) Explicit data Request

In case of explicit data request with fake not allowed, the distributor is not allowed to add fake objects to the distributed data. So Data allocation is fully defined by the agent's data request. In case of explicit data request with fake allowed, the distributor cannot remove or alter the requests R from the agent. However distributor can add the fake object.

In algorithm for data allocation for explicit request, the input to this is a set of requestR1, R2,……, Rn from n agents and different conditions for requests. The e-optimal algorithm finds the agents that are eligible to receiving fake objects. Then create one fake object in iteration and allocate it to the agent selected. The e-optimal algorithm minimizes every term of the objective summation by adding maximum number bi of fake objects to every set Ri yielding optimal solution.

Algorithm 1 : Allocation for Explicit Data Requests (EF)

```
Input: R1, . . . , Rn, cond1, . . . , condn, b1, . . . ,bn, B
Output: R1, . . . , Rn, F1,. . . ,Fn
Step 1: R $\leftarrow$ Ø , Agents that can receive fake objects
Step 2: for i = 1,……., n do
Step 3: if bi > 0 then
Step 4: R $\leftarrow$ R U {i}
Step 5: Fi $\leftarrow$ Ø; Step 6: while B > 0 do
Step 7: i $\leftarrow$ ELECTAGENT(R,R1,……..,Rn)
Step 8: f $\leftarrow$ REATEFAKEOBJECT (Ri, Fi, condi)
Step 9: Ri $\leftarrow$ Ri U {i}
Step 10: Fi $\leftarrow$ Fi U {i}
Step 11: bi $\leftarrow$ bi - 1
Step 12: if bi = 0 then
Step 13: R $\leftarrow$ R \{Ri}
Step 14: B $\leftarrow$ B – 1.
```

Algorithm 2 : Agent Selection for e-random

```
Step 1: function SELECTAGENT(R,R1,……,Rn)
Step 2: i $\leftarrow$ select at random an agent from R
Step 3: return I
```

Algorithm 3: Agent selection for e-optimal

```
Step 1: function SELECTAGENT(R;R1; : : : ;Rn)
Step 2: i $\leftarrow$ argmax $\left(\frac{1}{R_{i'}} - \frac{1}{R_{i'}+1}\right) \sum_j |R_{i'} \cap Rj|$
Step 3: return i $i'$:R $\in$ R
```

b) Sample Data Request

With sample data requests, each agent Ui may receive any T from a subset out of $\binom{|T|}{m}$ different ones. Hence,there are $\prod_{i=1}^{n}\binom{|T|}{m}$ different allocations.In every allocation, the distributor can permute T objects and keep the same chances of guilty agent detection. The reason is that the guilt probability depends only on which agents have received the leaked objects and not on the identity of the leaked objects. Therefore, from the distributor's perspective there are $\prod_{i=1}^{n}\binom{|T|}{m} / |T|$ different allocations. An object allocation that satisfies requests and ignores the distributor's objective is to give each agent a unique subset of T of size m. The s-max algorithm allocates to an agent the data record that yields the minimum increase of the maximum relative overlap among any pair of agents. The s-max algorithm is as follows.

Algorithm 4: Allocation for Sample Data Requests (SF)

```
Input: m1, . . . , mn, |T| .  Assuming mi <=|T|
Output: R1,……..,Rn
Step 1: a $\leftarrow$ 0|T|   . a[k]:number of agents who have received object tk
Step 2: R1,……….,Rn  ;
Step 3: remaining $\leftarrow$ $\sum_{i=1}^{n} mi$
Step 4: while remaining > 0 do
Step 5: for all i = 1,….., n : |Ri| < mi do
Step 6: k ← SELECTOBJECT (i, Ri). May also use additional parameters
Step 7: Ri ← Ri U {tk}
Step 8: a[k] ← a[k] + 1
Step 9: remaining ← remaining−1.
```

Algorithm 5 : Object Selection for s-random

```
Step 1: function SELECTOBJECT(i , Ri)
Step 2: k ← select at random an element from
            set{ k' ≠ tk'      Ri }
Step 3: return k.
```

Algorithm 6 : Object Selection for s-overlap

```
Step 1: function SELECTOBJECT(i;Ri; a)
Step 2: K ←  {k | k = argmin a[k']}
Step 3: k ←  select at random an element from
             set {k' |  k' ∈ K ^ tk' ≠ Ri}
Step 4: return k.
```

Algorithm 7 : Object Selection for s-max

```
Step1: function SELECTOBJECT(i,
R1,…….,Rn ,m1,……..,mn)
Step 2: min_ overlap ← 1 . The minimum out of the maximum relative overlaps that the allocations of different objects to Ui yield
Step 3: for k  {k' | tk'  Ri } do
Step 4: max_ rel_ ov ← 0. The maximum relative overlap between Ri and any set Rj that the allocation of tk to Ui yields
Step 5: for all j = 1,…………, n : j  i and tk  Rj
do
Step 6: abs_ ov ← | Ri ∩ Rj | + 1
Step 7: rel_ ov ← abs_ ov /min (mi , mj )
Step 8: max_ rel_ ov ←  MAX(max_rel_ov ,
        rel_ov)
Step 9: if max_ rel_ ov <= min_ overlap then
Step 10: min_overlap ← max_ rel_ ov
Step 11: ret_ k ← k
Step 12: return ret_ k.
```

IV. Existing System

There are conventional techniques being used and include technical and fundamental analysis. The main issue with these techniques is that they are manual and need laborious work along with experience.

Traditionally, leakage detection is handled by watermarking, e.g., a unique code is embedded in each distributed copy. If that copy is later discovered in the hands of an unauthorized party, the leaker can be identified. Watermarks can be very useful in some cases, but again, involve some modification of the original data. Furthermore, watermarks can sometimes be destroyed if the data recipient is malicious. E.g. . A hospital may give patient records to researchers who will devise new treatments. Similarly, a company may have partnerships with other companies that require sharing customer data. Another enterprise may outsource its data processing, so data must be given to various other companies[4].

We call the owner of the data the distributor and the supposedly trusted third parties the agents. The distributor gives the data to the agents. These data will be watermarked. Watermarking is the process of embedding the name or information regarding the company. The examples include the pictures we have seen in the internet. The authors of the pictures are watermarked within it. If anyone tries to copy the picture or data the watermark will be present. And thus the data may be unusable by the leakers.

a) Disadvantage

This data is vulnerable to attacks. There are several techniques by which the watermark can be removed. Thus the data will be vulnerable to attacks.

V. Proposed System

We propose data allocation strategies (across the agents) that improve the probability of identifying leakages. These methods do not rely on alterations of the released data (e.g., watermarks). In some cases we can also inject "realistic but fake" data records to further improve our chances of detecting leakage and identifying the guilty party. We also present algorithm for distributing object to agent.

Our goal is to detect when the distributor's sensitive data has been leaked by agents, and if possible to identify the agent that leaked the data. Perturbation is a very useful technique where the data is modified and made 'less sensitive´ before being handed to agents. We develop unobtrusive techniques for detecting leakage of a set of objects or records. In this section we develop a model for assessing the 'guilt´ of agents. We also present algorithms for distributing objects to agents, in a way that improves our chances of identifying a leaker.

Finally, we also consider the option of adding 'fake´ objects to the distributed set. Such objects do not correspond to real entities but appear realistic to the agents. In a sense, the fake objects acts as a type of watermark for the entire set, without modifying any individual members. If it turns out an agent was given one or more fake objects that were leaked, then the distributor can be more confident that agent was guilty. Today the advancement in technology made the watermarking system a simple technique of data authorization. There are various software which can remove the watermark from the data and makes the data as original[5].

a) *Advantage*

This system includes the data hiding along with the provisional software with which only the data can be accessed. This system gives privileged access to the administrator (data distributor) as well as the agents registered by the distributors. Only registered agents can access the system. The user accounts can be activated as well as cancelled. The exported file will be accessed only by the system. The agent has given only the permission to access the software and view the data. The data can be copied by our software. If the data is copied to the agent' system the path and agent information will be sent to the distributors email id thereby the identity of the leaked user can be traced[2].

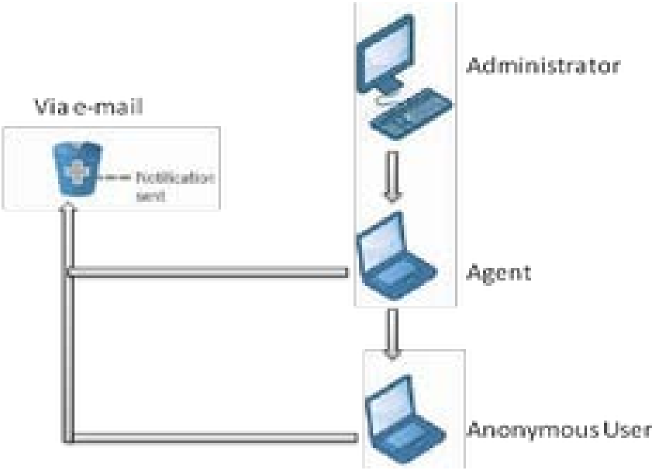


Figure 1: Illustration Diagram

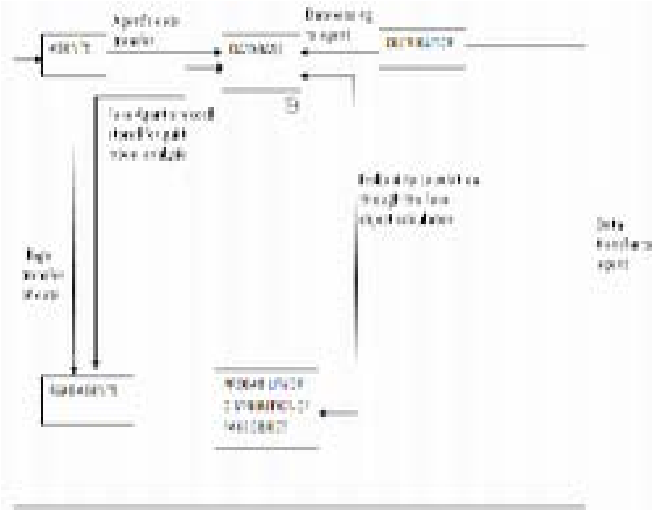


Figure 2: System Architecture Design

b) *System Implementation*

The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

i. *Modules*

(1) Data Allocation Module,
(2) Data Distribution Module,
(3) Data Leakage & Detection Module.

ii. *Module Description*

1. *Data Allocation Module*

In this module, administrator has to login with his id and password. Administrator has all the agent information, user data inside his database. Administrator is now able to view the database consisting of the original data as well as the fake data.

Administrator can also list the agents here. He will be able to add additional information to the database. Agent's information can be added here.

2. *Data Distribution Module*

Once the agent has been added by the administrator, he can create one username and password for that particular agent, in fact registering. After the agent has been successfully registered we now want to send the data to agent according to their request. Administrator will now select a requested amount of data and then export these data into an excel file in byte format. After the file is created, the administrator will send the data to agent. Sending the data includes transferring the data through the network (LAN).At the same time the administrator will keep the record of the agent with his id.

3. *Data Leakage and Detection Module*

Agent can login with their given username and password. Now they can view the data that is being sent by the administrator, but they cannot edit nor do any changes with it. He can now copy the data anywhere he wants to. The path and the agent which is copying the file will be recorded and the notification is sent through e-mail. Whenever a guilty agent tries to send the data to any other anonymous user i.e. leaking the data, a notification will be sent through email. The administrator has an email id with all the notifications, including the path to which the data is saved along with agent id[6].

Figure3: Login for Distributor & Agent

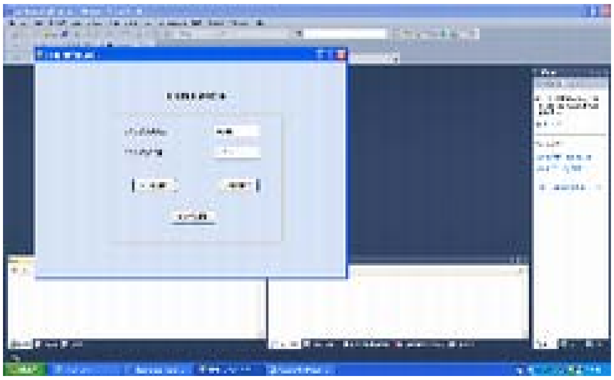


Figure 4: Distributor Login

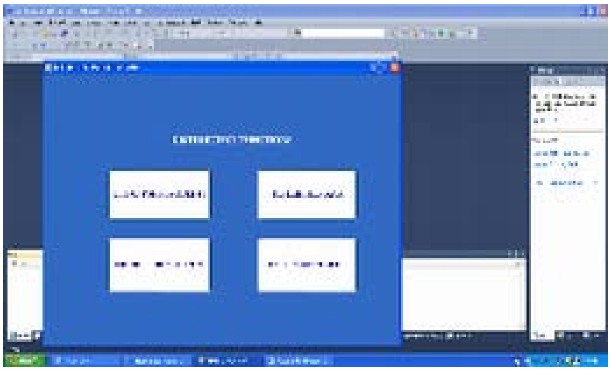


Figure 5: Distributor Function

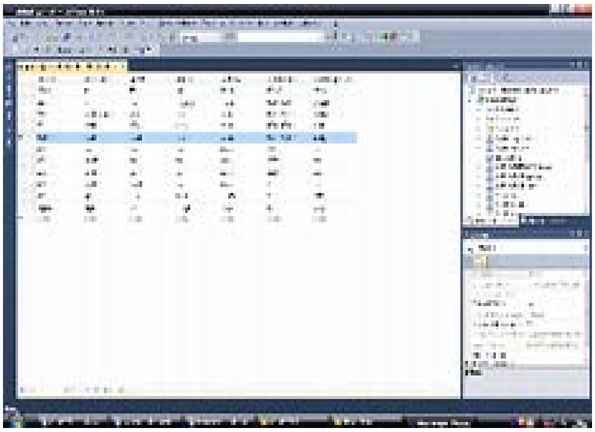


Figure 6: The Agent Detai in Database Table

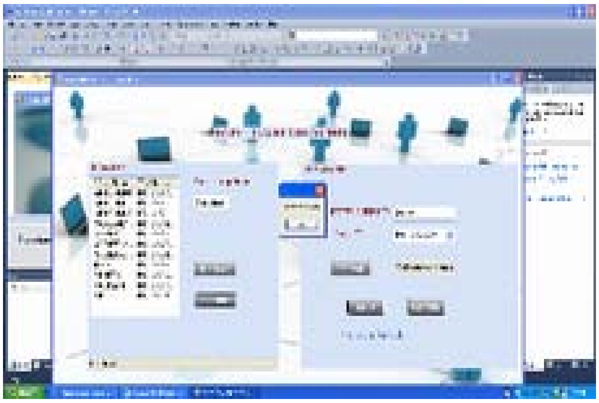


Figure 7: Distributor Sending Data to Agent

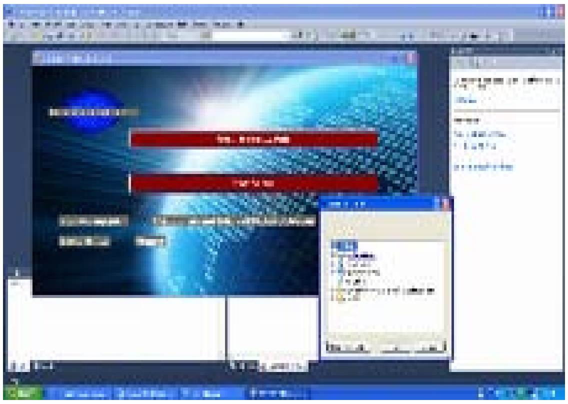


Figure 8: Selection of Agent Side Path

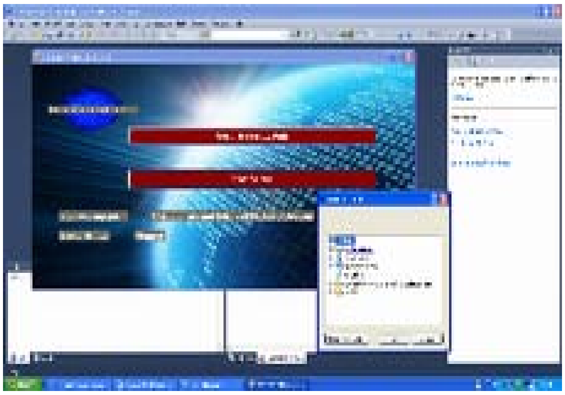


Figure 9: Conformation of Data Reception

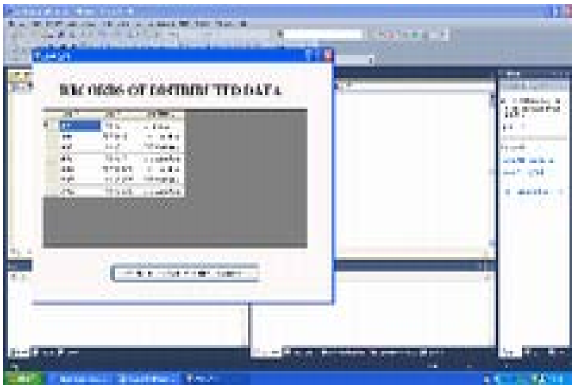


Figure 10: Transfer Data to the Agent is Saved in Record of Distributor Data

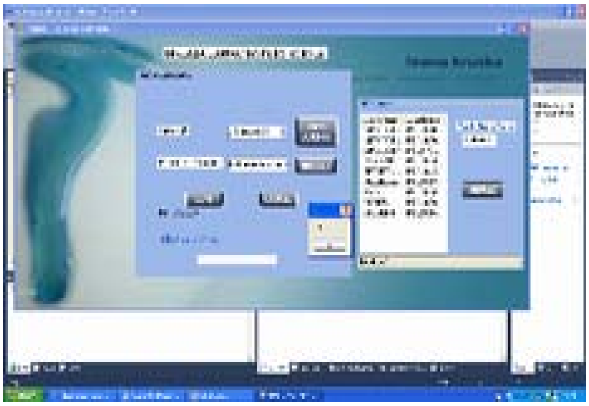


Figure 11: Agent to Agent Data Transfer

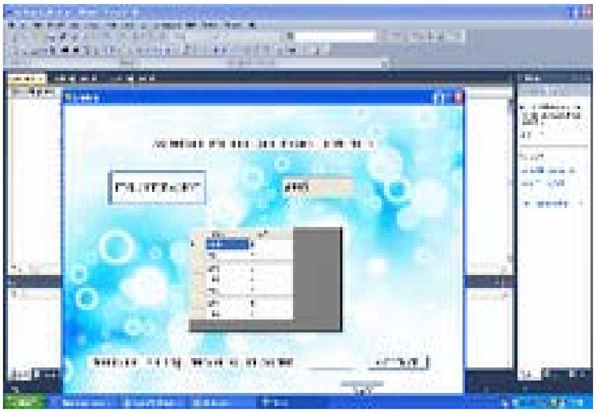


Figure12: Data Leakage can seen in Agent Guilt Model

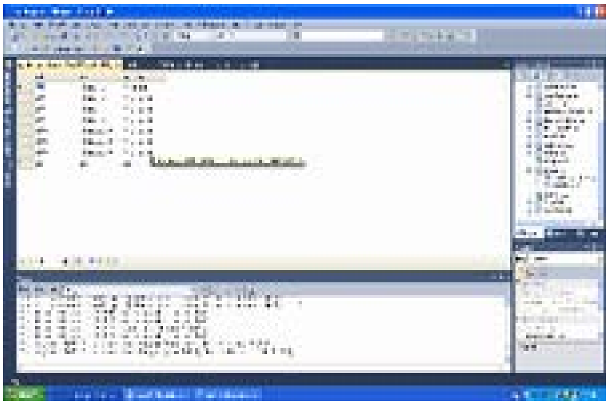


Figure 13: Agent Record

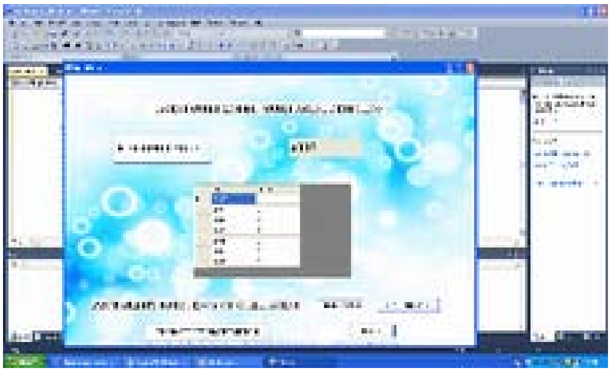


Figure 14: Find Probability of Agent Guilt Model

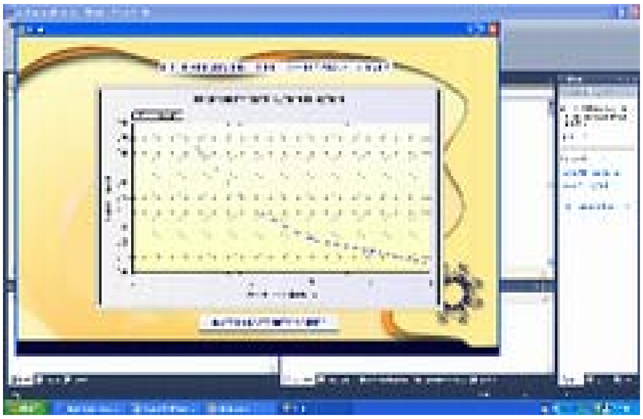


Figure 15: Draw Graph of Guilty Model

VI. Future Work

The notion of a trusted environment is somewhat fluid. The departure of a trusted staff member with access to sensitive information can become a data breach if the staff member retains access to the data subsequent to termination of the trust relationship. In distributed systems, this can also occur with a break down in a web of trust. Most such incidents publicized in the media involve private information on individuals, i.e. social security numbers, etc Loss of corporate information such as trade secrets, sensitive corporate information, details of contracts, etc or of government information is frequently unreported, as there is no compelling reason to do so in the absence of potential damage to private citizens, and the publicity around such an event may be more damaging than the loss of the data itself.

Although such incidents pose the risk of identity theft or other serious consequences, in most cases there is no lasting damage; either the breach in security is remedied before the information is accessed by unscrupulous people, or the thief is only interested in the hardware stolen, not the data it contains. Never the less, when such incidents become publicly known, it is customary for the offending party to attempt to mitigate damages by providing to the victims subscription to a credit reporting agency, for instance.

VII. Conclusion

In a perfect world there would be no need to hand over sensitive data to agents that may unknowingly or maliciously leak it. And even if we had to handover sensitive data, in a perfect world we could watermark each object so that we could trace its origins with absolute certainty. However, in many cases we must indeed work with agents that may not be 100% trusted.

In spite of these difficulties, we have shown it is possible to assess the likelihood that an agent is responsible for a leak, based on the overlap of his data with the leaked data and the data of other agents, and based on the probability that objects can be 'guessed´ by other means. Our model is relatively simple, but we believe it captures the essential trade-offs. The algorithms we have presented implement a variety of data distribution strategies that can improve the distributor's chances of identifying a leaker. We have shown that distributing objects judiciously can make a significant difference in identifying guilty agents, especially in cases where there is large overlap in the data that agents must receive. It includes the investigation of agent guilt models that capture leakage scenarios that are not studied in this paper.

References Références Referencias

1. Data Leakage Detection, an IEEE paper by Panagiotis Papadimitriou, Member, IEEE, Hector Garcia-Molina, Member, IEEE NOV-2010.
2. Watermarking relational databases. In VLDB '02: Proceedings of the 28th international conference on Very Large Data Bases, By R. Agrawal and J. Kiernan, pages 155–166. VLDB Endowment, 2002.
3. An algebra for composing access control policies, By P. Bonatti, S. D. C. di Vimercati and P. Samarati, ACM Trans. Inf. Syst. Secur., 5(1):1–35, 2002.
4. P. Buneman, S. Khanna, and W. C. Tan. Why and where: A characterization of data provenance. In J. V. den Bussche and V. Vianu, editors, Database Theory - ICDT 2001, 8th International Conference, London, UK, January 4-6, 2001, Proceedings, volume 1973 of Lecture Notes in Computer Science, pages 316–330. Springer, 2001.
5. P. Buneman and W.-C. Tan. Provenance in databases. In SIGMOD '07: Proceedings of the 2007 ACM SIGMOD international conference on Management of data, pages 1171–1173, New York, NY, USA, 2007. ACM.
6. Lineage tracing for general data warehouse transformations, By Y. Cui and J. Widom, In The VLDB Journal, pages 471–480, 2001.
7. Digital music distribution and audio watermarking, by S. Czerwinski, R. Fromm, and T. Hodes.

Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 17 Issue 4 Version 1.0 Year 2017
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

An Efficiency Study on Fault Tolerent Fir Filters

By Augusta Angel M & Julie Antony Roselin J

VV College of Engineering

Abstract- In this Digital World, Digital filters are the boom for modern digital communications in which Fir filters play a vital role. But the reliability of these filters is still a paradox. Nowadays electronic devices with multiple numbers of filters are used in various fields. Hence the performance and reliability of the filters must be improved. A number of techniques have been introduced to detect and correct errors that occur in those filter circuits. In this paper, the use of hamming code error correction technique on 4 tap fir filters are studied in order to obtain optimized and efficient reliability.

GJCST-E Classification: I.4.3

An Efficiency Study on Fault Tolerent Fir Filters

Augusta Angel M [α] & Julie Antony Roselin J [σ]

Abstract- In this Digital World, Digital filters are the boom for modern digital communications in which Fir filters play a vital role. But the reliability of these filters is still a paradox. Nowadays electronic devices with multiple numbers of filters are used in various fields. Hence the performance and reliability of the filters must be improved. A number of techniques have been introduced to detect and correct errors that occur in those filter circuits. In this paper, the use of hamming code error correction technique on 4 tap fir filters are studied in order to obtain optimized and efficient reliability.

I. Introduction

In analog and digital communication fields, the Digital Filters play a vital role. The main purpose of using the filters is to remove the unwanted signal components in order to produce the better quality signal at the output. Figure 1 shows the functional block of digital filter. The digital filter is a discrete system, and it can do a series of mathematic processing to the input signal, and therefore obtain the desired information from the input signal.

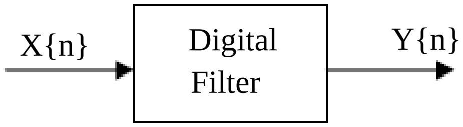


Figure 1: Digital filter functional block

while compared with the analog filters, the digital filters have unique characteristics of generating the stabilized signal at the output. So that the digital filters are preferred than the analogue one in electronic circuits. The two major classification of digital filters are FIR (Finite Impulse Response) and IIR (Infinite Impulse Response) filter. The FIR filters are employed in filtering problems than IIR filters because of efficient hardware implementation with fewer precision errors and also the stabilized response with the linear phase. Due to its linear phase characteristics, Finite impulse response (FIR) filter plays an vital role in the processing of digital signal.

a) FIR Filter Design

Finite-Impulse Response (FIR) filters have considered as important building blocks in many digital signal processing (DSP) systems. The FIR filter is preferred over the IIR filter because of efficient implementation with fewer finite precision error and having better stability with linear phase. In any Fir filter, the output signal is obtained by convoluting the input signal with the filter co-efficient i.e.,

$$y[n] = x[n] ** h[n] = \sum_{k=0}^{N-1} x[k]h[n-k]$$

Figure 2: Depicts the 4 tap fir structure. Where, x(n) is the given input sequence, the output of the filter is given by y(n) and the h(n) denotes the filter co-efficient.

Author α σ: Dept. of ECE, W College of Engineering, Tisaiyanvilai, TamilNadu. e-mail: augusangel@gmail.com

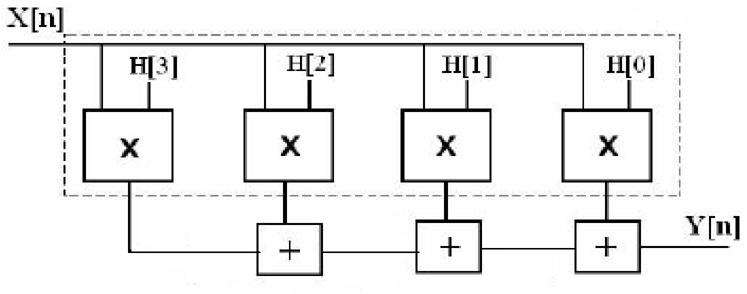


Figure 2: Fir filter structure

b) Error Detection and Correction Hamming Code

Data that is either transmitted over communication channel is not completely error free. This change in the data is caused due to external interference, signal distortion, attenuation or from noise. There are two types of errors. Firstly single error in which only one bit is changed. And secondly the burst error in which more than one bits are changed. There are various error detection and correction techniques such as Cyclic Redundancy Checks (CRC), Parity check, LRC, VRC and Hamming Code. This work focuses on Hamming code. A commonly known linear Block Code is the Hamming code. In a block of data, Hamming codes can detect and correct a single bit-error. In these codes, every bit is included in a unique set of parity bits [2]. By analyzing parities of combinations of received bits, the presence and location of a single parity bit-error can be determined. The parities of combinations of received bits are used to produce a table of parities which corresponds to a particular bit-error combination.

This table of errors is called as the error syndrome. If all parities are correct according to this pattern, it can be concluded that there is no single bit-error in the message (there may be multiple bit-errors). Due to single bit-error , if there is any error in the parities , the erroneous data bit can be found by adding up the positions of the erroneous parities. Hamming codes are easy to implement. They are generally used in computing, telecommunication, and other applications including data compression, and turbo codes [3]. They are also used for low cost and low power applications.

II. Fault Tolerant FIR Filters

To protect a circuit from errors, so many techniques can be used. In the manufacturing process of the circuits, modifications can be done to minimize the number of errors by adding redundancy at the logic to ensure that errors do not affect the system functionality. In signal processing and communication systems, digital filters are most commonly used. More number of techniques has been proposed to protect the circuits. By using number of methods, we can identify the faults and also correct the errors within circuit itself. There are different fault tolerance approaches to conventional circuits and the digital signal processing circuits. Fault tolerant filter implementations are needed, whenever the system reliability is critical. So, using error correction codes, the filters can be protected. Here, we use hamming code for error correction.

The fault tolerant of fir filters are achieved by including the ecc in the fir architecture. Hence if the filter produces a error at the output, it can be detected and corrected by using the error correction unit. Figure 3 depicts that the output of fir filter is given to the error correction unit in which the errorous bit is identified and it is corrected. The error correction unit includes the hamming encoder and decoder.

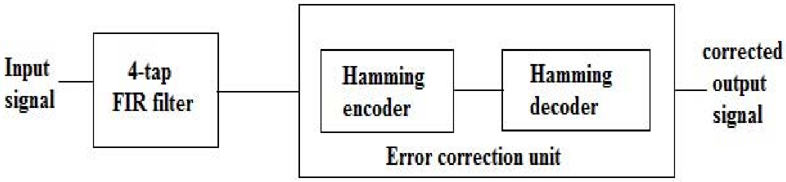
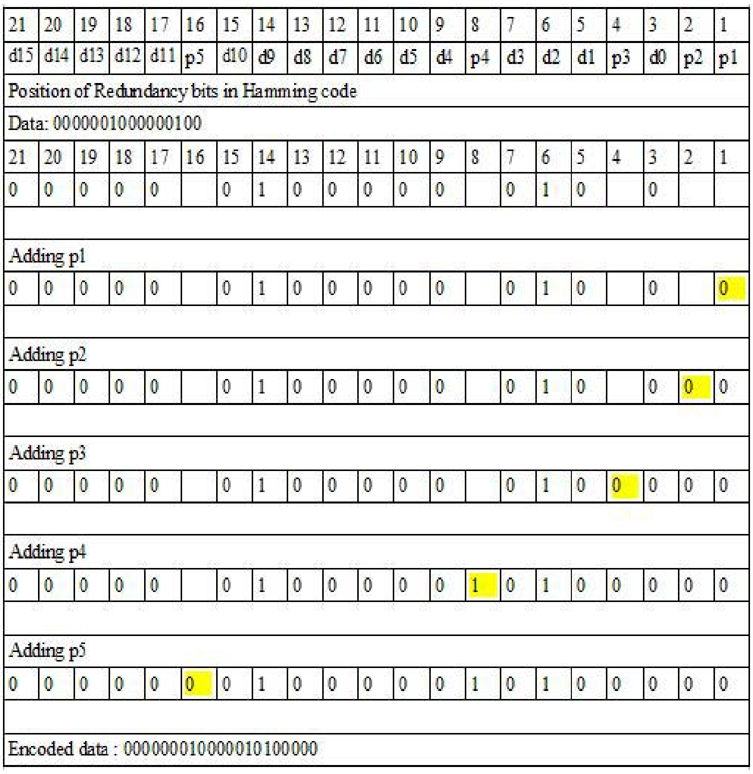


Figure 3: Fault tolerant fir filter module

a) Hamming code algorithm for filter protection

An (ECC) Error Correction Codes block takes a block of d bits and produces a block of n bits by adding (n-d) parity check bits . The Parity check bits are xor combinations of input d data bits. Considering Hamming Code with input k =16 data bits and output n=21 bits, five parity check bits p1, p2, p3 ,p4,p5 are needed which are computed as follows: The redundancy bits are placed in positions 1, 2, 4, 8 and 16 (the positions in an 21-bit sequence that are powers of 2). The parity bit pl is calculated using all bits positions whose binary representation includes a 1 in the least significant position. p2 bit is calculated using all the bit positions with a 1 in the second position and so on. Thus, the parity bits are generated for different combination of bits. The various combinations are:

p: bits 1,3,5, 7, 9, 11, 13,15, 17, 19, 21
p2: bits 2, 3, 6, 7, 10, 11, 14, 15, 18, 19
p3: bits 4, 5, 6, 7 ,12, 13, 14, 15, 20, 21
p4: bits 8, 9, 10, 11, 12, 13, 14, 15
p5: bits 16, 17, 18, 19, 20, 21

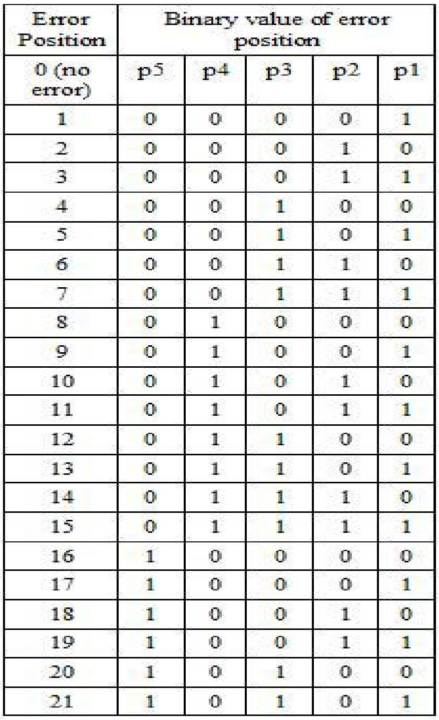


21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
d15	d14	d13	d12	d11	p5	d10	d9	d8	d7	d6	d5	d4	p4	d3	d2	d1	p3	d0	p2	p1
Position of Redundancy bits in Hamming code																				
Data: 0000001000000100																				
21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
0	0	0	0	0		0	1	0	0	0	0	0		0	1	0		0		
Adding p1																				
0	0	0	0	0		0	1	0	0	0	0	0		0	1	0		0		0
Adding p2																				
0	0	0	0	0		0	1	0	0	0	0	0		0	1	0		0	0	0
Adding p3																				
0	0	0	0	0		0	1	0	0	0	0	0		0	1	0	0	0	0	0
Adding p4																				
0	0	0	0	0		0	1	0	0	0	0	0	1	0	1	0	0	0	0	0
Adding p5																				
0	0	0	0	0	0	0	1	0	0	0	0	0	1	0	1	0	0	0	0	0
Encoded data : 000000010000010100000																				

Figure 4: Hamming encoding

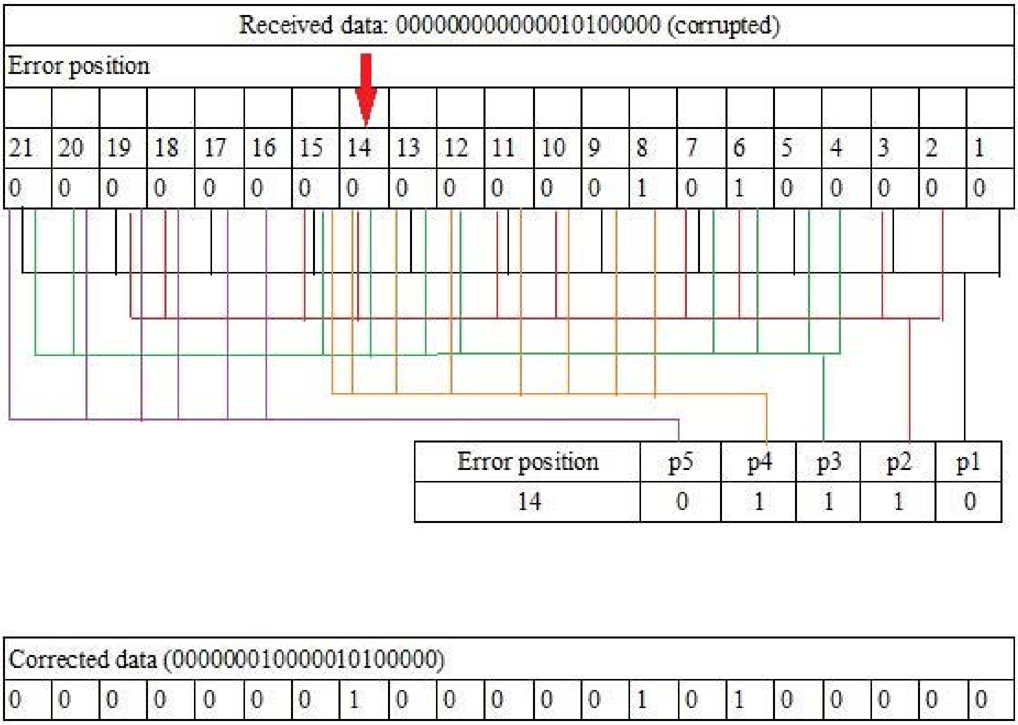
Figure 4 shows the hamming encoding technique, it shows how the parity bits are included in the data bits. If there is any error on input data bits it can be detected and corrected by using these parity check bits. Table I shows the position of error bits based on the parity check bits. For example, an error on d1 will cause errors on the three parity check bits p1, p3; an error on d2 will affect only p2 and p3; an error on d3 will affect only on p1,p2 and p3 and so on. Hence, once the erroneous bit is identified, it is corrected by simply inverting that bit.

Table I: Position of error bit



Error Position	Binary value of error position				
0 (no error)	p5	p4	p3	p2	p1
1	0	0	0	0	1
2	0	0	0	1	0
3	0	0	0	1	1
4	0	0	1	0	0
5	0	0	1	0	1
6	0	0	1	1	0
7	0	0	1	1	1
8	0	1	0	0	0
9	0	1	0	0	1
10	0	1	0	1	0
11	0	1	0	1	1
12	0	1	1	0	0
13	0	1	1	0	1
14	0	1	1	1	0
15	0	1	1	1	1
16	1	0	0	0	0
17	1	0	0	0	1
18	1	0	0	1	0
19	1	0	0	1	1
20	1	0	1	0	0
21	1	0	1	0	1

Suppose a binary data 0000001000000100 is to be transmitted, it is encoded by adding redundancy bits in their corresponding position. Now, the encoded data 0000001000000100 will be transmitted to the receiver. The error detection and correction are shown in figure 5. If bit position 14 has been changed from 1 to 0 (i.e, 000000000000010100000)in transmitted data, Then the data will be erroneous.



Received data: 000000000000010100000 (corrupted)																				
Error position																				
21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0

Error position	p5	p4	p3	p2	p1
14	0	1	1	1	0

Corrected data (000000010000010100000)																				
0	0	0	0	0	0	0	1	0	0	0	0	0	1	0	1	0	0	0	0	0

Figure 5: Hamming Decoding

At the receiver side, the hamming decoder recalculates the same set of bits used by sender plus the relevant parity (p) bit for each set. The recalculated value of p5 p4 p3 p2 p1 is 01110, which corresponds to decimal 14. Therefore bit position 14 contains an error. To correct this error, bit position 14 is reversed from 0 to 1.

III. Results and Discussion

The described structure has been implemented by using verilog HDL. The error dectection and correction are verified using the Xilinx 13.4 software tool. Figure 6 shows the RTL schematic of fault tolerant fir filter.

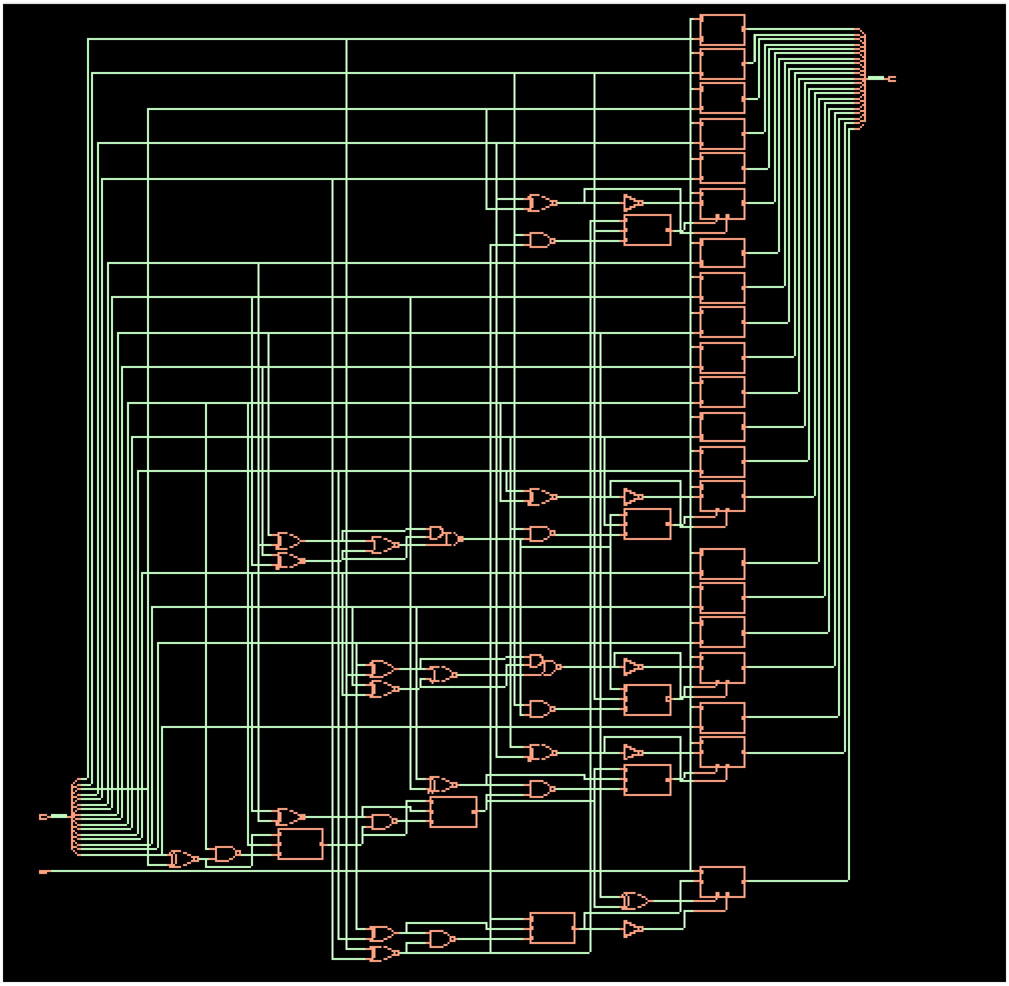
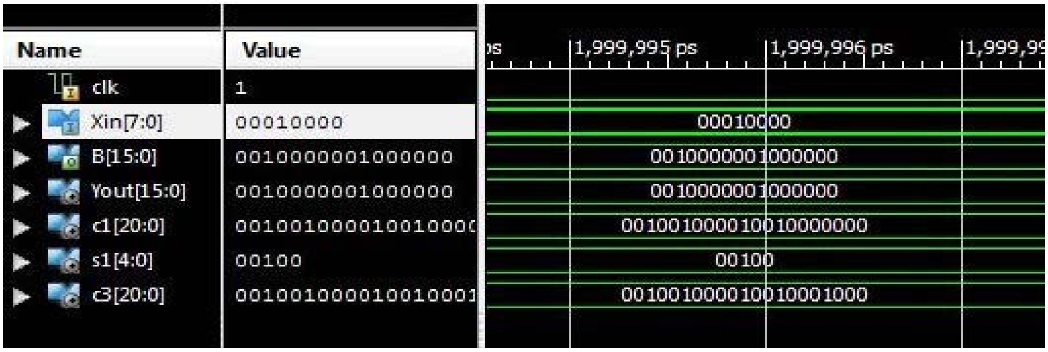


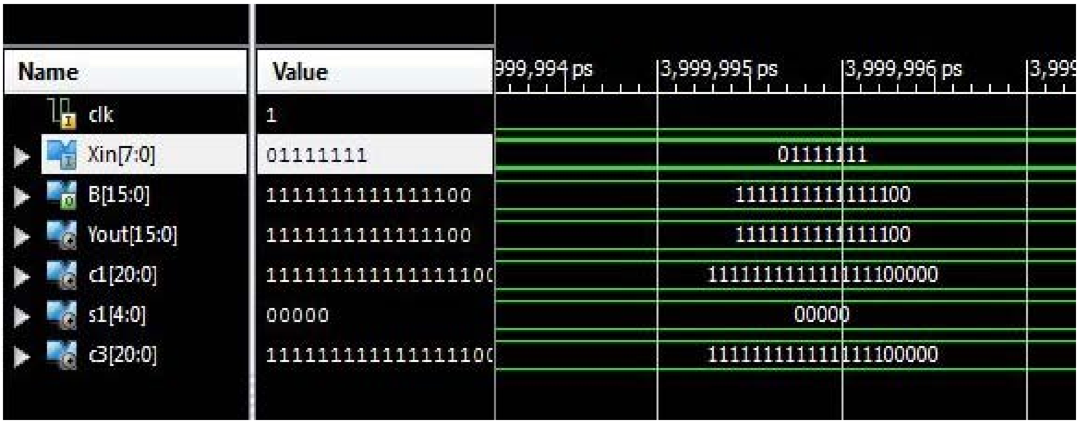
Figure 6: RTL schematic of Fault tolerant Fir filter

For example figure 7 shows a output in which a error at the 4th bit of the transmitted signal is detected by the syndrome (s1) and it is corrected by the error correction unit at the output. Now the error free signal is obtained as a output. By this way the reliability of the system is improved. Figure 8 shows the signal with no error. Since the Syndrome (s1) is 0000, no error is detected. Hence it is transmitted without any correction.



Name	Value	ps |1,999,995 ps |1,999,996 ps |1,999,99
clk	1	
Xin[7:0]	00010000	00010000
B[15:0]	0010000001000000	0010000001000000
Yout[15:0]	0010000001000000	0010000001000000
c1[20:0]	001001000010010000	001001000010010000000
s1[4:0]	00100	00100
c3[20:0]	001001000010010001	001001000010010001000

Figure 7: Error detected and corrected output signal



```
Name          Value                  999,994 ps   |3,999,995 ps   |3,999,996 ps   |3,999
clk           1
Xin[7:0]      01111111                            01111111
B[15:0]       1111111111111100                    1111111111111100
Yout[15:0]    1111111111111100                    1111111111111100
c1[20:0]      111111111111111110(                 111111111111111100000
s1[4:0]       00000                               00000
c3[20:0]      111111111111111110(                 111111111111111100000
```

Figure 8: Transmitted signal with no error

Table II: Performance chart

Power Consumption	Area	Time
Leakage power : 0.017mw	Cells : 317	Minimum Period : 7.312 ns
Dynamic Power : 0.7mw	Cell Area : 3205	Minimum input arrival time before clock : 7.389 ns
Total power : 0.9 mw		Minimum output required time after clock : 4.118 ns

The total power, area and time taken used by the fault tolerant fir module are shown in table. It provides good performances, since it uses less area as well as power. It uses very less time to detect and correct errors which make it efficient in case of usage in high speed communication networks where multiple number no of filters are used.

IV. Conclusion

Filters are widely used in various digital signal processing applications. Protecting filters from errors is an important task which is addressed by various techniques. In this paper, a study was done on protecting errors by using error correction codes. The hamming code technique is employed along with fir filters, the error which arise due to any fault in the circuits are detected and corrected by this hamming encoder and decoder. The study shows that the reliability of the filters are improved by using this fault tolerant module and it also improves the performance by reducing the area complexity, delay and power.

References Références Referencias

1. Sneha P and Jamuna S," FPGA Implementation of Reduced Precision Redundancy Protected Parallel Fir Filters", IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)Volume 10, Issue 3, Ver. II (May - Jun.2015), PP 57-64.
2. Daitx F., Vagner S. R., Eduardo Costa, Paulo Flores, Bampi S., "VHDL Generation of Optimized FIR Filters", IEEE International Conference on Signals, Circuits and Systems, 2008.
3. Zhen Gao, Pedro Reviriego, Wen Pan, Zhan Xu, Ming Zhao, Jing Wang, and Juan Antonio Maestro, ―Fault Tolerant Parallel Filters Based on Error Correction Codes, 1063-8210 © 2014 IEEE.
4. A. V. Oppenheim and R. W. Schafer, Discrete Time Signal Processing. Upper Saddle River, NJ, USA: Prentice-Hall 1999.
5. S. Lin and D. J. Costello, Error Control Coding, 2nd ed. Englewood Cliffs, NJ, USA: Prentice-Hall. 2004.
6. R. W. Hamming, "Error correcting and error detecting codes," Bell Syst. Tech. J., vol. 29, pp. 147–160, Apr. 1950.
7. P. Reviriego, S. Pontarelli, C. Bleakley, and J. A. Maestro, "Area efficient concurrent error detection and correction for parallel filters," IET Electron. Lett., vol. 48, no. 20, pp. 1258–1260, Sep. 2012.
8. "Single Error Correction and Double Error Detection (SECDED) with CoolRunner-II™ CPLDs", Xilinx, XAPP383 (v1.1) August 1, 2003

This page is intentionally left blank

Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 17 Issue 4 Version 1.0 Year 2017
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

MANET & its Qos

By Mahak Singla

Abstract- MANET is used to provide communication among the nodes. There is no central authority which control communication session between nodes i.e. there is no any defined infrastructure. Nodes moves frequently in the network which generate some issues like routing, coverage, congestion and security issues. Quality of service (QoS) in MANET is universally a growing area. Here, different mobile devices collaborate to form a communication network without any pre-existing infrastructure. Due to vast expansion of multimedia technology, mobile technology and real time applications has need to strictly support quality of service such as throughput, delay, energy consumption, jitter etc. This paper presents the description about the message sending in MANET and its QoS.

Keywords: MANET, QoS, ad-hoc networks.

GJCST-E Classification: C.2.1

MANET & its Qos

Mahak Singla

Abstract- MANET is used to provide communication among the nodes. There is no central authority which control communication session between nodes i.e. there is no any defined infrastructure. Nodes moves frequently in the network which generate some issues like routing, coverage, congestion and security issues. Quality of service (QoS) in MANET is universally a growing area. Here, different mobile devices collaborate to form a communication network without any pre-existing infrastructure. Due to vast expansion of multimedia technology, mobile technology and real time applications has need to strictly support quality of service such as throughput, delay, energy consumption, jitter etc. This paper presents the description about the message sending in MANET and its QoS.

Keywords: MANET, QoS, ad-hoc networks.

I. Introduction

The Ad hoc On-Demand Distance Vector (AODV) algorithm provides dynamic multihop routing among various participating mobile nodes that wish to establish and maintain an ad hoc network. AODV allows mobile nodes to obtain routes quickly for new destinations, and does it not require nodes to maintain routes to destinations that are not active at time of communication.

Some issues in MANET are:
(i) unpredictable link properties that may lead to packet collision and signal propagation, (ii) the dynamic topology created by mobility of nodes, (iii) limited life of mobile device batteries, (iv) hidden and revealing terminal problems that occur when signals of two nodes are colliding with each other. (v) maintenance of route is very difficult because of changing behavior of the communication medium, and (vi) inadequate security measures in MANET leads to various attacks like passive attack, eavesdropping, leakage of secret information, data tampering, message replay, message contamination, and denial-of-service (DoS)[1].

II. Message Processing in AD-HOC Networks

AODV use 3 messaging types namely, Route Requests (RREQs), Route Replies (RREPs), and Route Errors (RERRs). These message types are received using UDP, and then normal IP header processing is applied. The requesting node use its IP address as the Originator IP address for the messages. For broadcasting messages, the IP limited broadcast address (255.255.255.255) is used i.e. messages are not forwarded blindly. However, operation of AODV do need some messages (e.g., RREQ) to be disseminated widely over the entire ad hoc network. The range of dissemination of such RREQs is indicated by the TTL in the IP header and no need of fragmentation is there[14].

The status of links present at next hops in the active routes is monitored by the nodes. Whenever a link break is detected in an active route, message is used to inform other nodes that the link loss has occurred at that node is RERR[14]. It indicates only those nodes that are reachable through the broken link, eg. If there is a link break at B, then RERR message will indicate that node D is no longer reachable destinations which are no longer through node B.

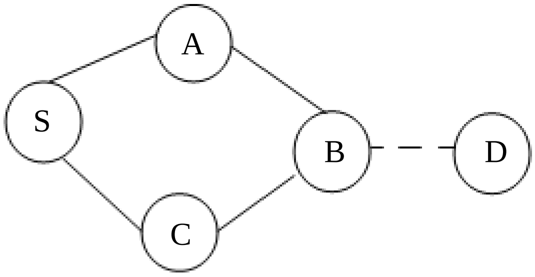


Fig 1: RERR Message Indication

To enable this mechanism, each node have a "precursor list" that contains the info regarding IP address for each of its neighbors that may use it as a next hop to reach destination. The information present in precursor list is easily obtained during the processing for generation of a RREP message, which has to be sent to node of precursor list .If the RREP has nonzero prefix length, then the originator of the RREQ which solicited the RREP information is included among the precursors for the subnet route (not specifically for the particular destination).

AODV routing protocol deals with route table management by keeping information ven for short-lived routes, that are created for temporarily store reverse paths towards nodes originating RREQs. AODV uses the following fields with each route table entry:

- IP Address of destination node
- Sequence Number of destination node
- Valid Destination Sequence Number flag
- Other state and routing flags (e.g., valid, invalid, repairable, being repaired)
- Network Interface

Author: Giani Zail Singh, MRSSTU, Bathinda.
e-mail: mshappy92@gmail.com

- Hop Count (i.e. total number of hops needed to reach destination)
- Next Hop
- List of Precursors
- Lifetime (expiry time or deletion time of the route) [14]

III. Layered Architecture of QoS

QoS have a layered view which contains 3 parts :

- User
- Application
- Network

a) *Application layer QoS:* This layer explain how well user expectations like clear voice, jitter –free video, etc are satisfied. This layer also describes arrival pattern and sensitivity to delivery delays. End-to-end protocols (RTP/RTCP), application-specific representations and encoding (FEC, interleaving) are implemented at this layer[13].

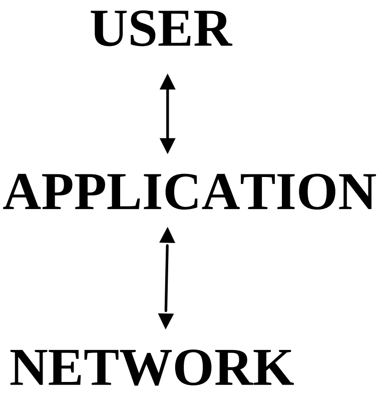


Fig 2: Layeres Structure of MANET [13]

b) *Network layer QoS:* This layer has four quality factors:

i. *Bandwidth* - The rate at which an traffic of application must be carried by the network.

ii. *Latency* - The delay that one application can tolerate while delivering a single packet of data.

iii. *Jitter* - The variation in latency.

iv. *Loss* - The percentage of data lost [13].

IV. Challenges in Manet

The following challenges make QoS hard in MANET:

- *Autonomous*- There is no centralized administration available to manage the operation of different mobile nodes.
- *Dynamic topology*- Nodes are mobile and they can be connected dynamically in any arbitrary manner.
- *Device discovery*- Identifying relevant new nodes that have joined the network and informing about their existence need dynamic updates to automatically select the optimal route.
- *Poor Transmission Quality*- This is a major problem of wireless communication that is caused by several erroneous sources that result in degradation of the received signal.
- *Network configuration*- The entire infrastructure of MANET is dynamic and thus it results in dynamic connection and disconnection of the variable links.
- *Topology maintenance*- Updation of dynamic link data among nodes in MANETs is a major challenge [2].

V. Conclusion

This paper deals with the message processing in Ad-hoc Networks and QoS in MANETs. Mobile ad-hoc networks must be able to provide the required quality of service for the delivery of real-time communications such as audio and video that poses a number of different technical challenges and new definitions. The development of mobile ad-hoc networks helps in various areas including academic, defence, disaster recovery, industrial environments, and healthcare. Nevertheless, there are many challenges that require to be addressed as well. These challenges needs to develop efficient routing procedures, mechanisms for reducing power consumption and extending the battery life, mechanisms for efficient use of limited bandwidth and communication capacity, new algorithms for information security, and making smaller but more powerful mobile devices. In short have to improve QoS in MANETs. This paper provides basic concepts related to QoS in networking, especially in MANET. In the upcoming paper tries to represent the improve QoS in MANET by applying genetic algorithm to routing protocol.

References Références Referencias

1. P.PERIYASAMY and E.KARTHIKEYAN, " a Novel Approach To Enhance the Quality of Aomdv Routing Protocol for Mobile Ad Hoc Networks, "vol. 69, no.2, pp. 394–404, 2014.
2. N. Tiwari and S. Shibu, "Load Balancing Congestion Control Techniques in Mobile Ad hoc Network : A Survey," vol. 3, no. 2, pp. 2652–2659, 2014.
3. Dr MadhumitaDash and Mrs Ricky Mohanty, "Quality- Of- Survey Routing Solutions forMobile Ad HocNetworks: A Review," *IOSR J. Electron. Commun. Eng.*, vol. 9, no. 2, pp. 29–36, 2014.
4. K. Fall and K. Varadhan, "The ns Manual (formerly ns Notes and Documentation)," *VINT Proj.*, no. 3, p. 434, 2011.
5. R. Kumar, M. Misra, and A. K. Sarje, "A Proactive Load-Aware Gateway Discovery in Ad Hoc Networks for Internet Connectivity," *Int. J. Comput. Networks Commun.*, vol. 2, no. 5, pp. 120–139, 2010.
6. K. S. Madhusudhananagakumar, Aghila, and G., "A Survey on Black Hole Attack Detection in MANET

Using AODV Protocol," *Int. J. Comput. Appl.*, vol. 34, no. 7, pp. 23–30, 2011.

7. A Modi and D. Rathod, "Improve Performance of AOMDV Protocol in," vol. 1, no. 11, 2015.
8. F. De Rango, P. Fazio, S. Member, and F. Conte, "A New Distributed Application and Network Layer Protocol for VoIP in Hostile Environments."
9. T. B. Reddy, I. Karthigeyan, B. S. Manoj, and C. S. R. Murthy, "Quality of service provisioning in ad hoc wireless networks: A survey of issues and solutions," *Ad Hoc Networks*, vol. 4, no. 1, pp. 83–124, 2006.
10. N. Simulator, "This Installation of Network Simulator 2 on the Ubuntu 16 . 04 Live CD UDisk," 2011.
11. K. N. Sridhar and M. C. Chan, "Channel-aware packet scheduling for MANETs," *2008 IEEE Int. Symp. A World Wireless, Mob. Multimed. Networks, WoWMoM2008*, 2008.
12. P. P. White, "RSVP and integrated services in the internet: A tutorial," *IEEE Commun. Mag.*, vol. 35, no. 5, pp. 100–106, 1997.
13. Seema, Y. Singh, and V. Siwach, "Quality of Service in MANET," *Int. J. Innov. Eng. Technol.*, vol. 1, no. 3, pp. 28–31, 2012.
14. R. Braden, D. Clark, and S. . Shenker, "RFC1633: Integrated Services in the Internet Architecture: an Overview," *IETF RFC 1633, July*, pp. 1–28, 1994.

This page is intentionally left blank

Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 17 Issue 4 Version 1.0 Year 2017
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

A Survey on Bandwidth Management Techniques Via the OSI Model Network and Application Layers

By Umeh Innocent Ikechukwu
Nnamdi Azikiwe University

Abstract- Nowadays, virtually all the basic aspects of human endeavor is computer and network dependent. Therefore bandwidth being one of the most valued resource and component of any network must be properly managed to yield a reliable performance. Over the years, different algorithms, models, techniques and applications have been developed for network and bandwidth management yet bandwidth problems has persistently remained on the increase. This work is an indepth survey on the causes of bandwidth problems, the basic models and techniques for bandwidth management and is followed by an analysis which is aimed at yielding meaningful suggestions on how a better technique or method for securing an efficient and improved bandwidth management solution using the application layer of the OSI network model can be achieved.

Keywords: network, OSI models, techniques, bandwidth, bandwidth management, layer(s), internet, administrator.

GJCST-E Classification: C.2.1, C.2.3

A Survey on Bandwidth Management Techniques Via the OSI Model Network and Application Layers

Umeh Innocent Ikechukwu

Abstract- Nowadays, virtually all the basic aspects of human endeavor is computer and network dependent. Therefore bandwidth being one of the most valued resource and component of any network must be properly managed to yield a reliable performance. Over the years, different algorithms, models, techniques and applications have been developed for network and bandwidth management yet bandwidth problems has persistently remained on the increase. This work is an in-depth survey on the causes of bandwidth problems, the basic models and techniques for bandwidth management and is followed by an analysis which is aimed at yielding meaningful suggestions on how a better technique or method for securing an efficient and improved bandwidth management solution using the application layer of the OSI network model can be achieved.

Keywords: network, OSI models, techniques, bandwidth, bandwidth management, layer(s), internet, administrator.

I. Introduction

Nowadays, almost every endeavor of human daily lives depend primarily on computers and related devices which in turn are based on networks. Domestic, official, social, financial, economic, religious and many other human activities have all become computer and network based. Also, these activities when carried out with the computer have been proved to be more successful and cheaper when computer networks get involved. Computer networks on its side, requires data bandwidth for its operation and functionality. Bandwidth is a very essential but expensive network resource which must be properly managed to provide the maximum required throughput expected by the network owners and the network users. The lack of or improper management of a network to conserve bandwidth results to network crisis or failure.

a) *Requirements for a Good Network*

Like every other project, a network projects must have a proper design for the network to survive expansion after deployment. According to ANAND (2005), good networks do not happen by accident rather good networks are the result of hard work by network designers and technicians, who identify network requirements and select the best solutions to meet the needs of a business. Network users generally do not think in terms of the complexity of the underlying network. They think of the network as a way to access the applications they need, when they need them. A few of the requirements to achieve a good network have been identified to include the following;

i. A network should stay up all the time, even in the event of failed links, equipment failure, and overloaded conditions.
ii. Every network should reliably deliver applications and provide reasonable response times from any host to any host.
iii. A network should be secure. It should protect the data that is transmitted over it and data stored on the devices that connect to it.
iv. A network should be easy to modify to adapt to network growth and general business changes.
v. Because failures occasionally occur, troubleshooting should be easy. Finding and fixing a problem should not be too time-consuming.

The statements above fall in line with Sunjay Sharma (2011) recommendations for a manageable network to be achieved.

b) *Network Management*

Network management is the process of manipulating resources of a network such as bandwidth, storage, etc. in other to improve the performance of the network.

Over the years, various techniques andmodels of layered architecture has been employed to either, administer, manage and or secure computer networks. John S. et al. (2011),in a study on the causes of failure in internet access delivery in Nigerian university libraries, observed that planning and eventual management of the bandwidth of a computer network is always a challenging task yet, networks must be properly managed to provide efficiency, throughput and good quality of service (QoS). Layering which implies the division of one whole network process into smaller tasks where each of the small task is then assigned to a particular layer which works dedicatedly to process only that task. Layering idea has been greatly employed in managing network and its complex and important resources like bandwidth.

Author: Computer Science Department, Nnamdi Azikiwe University, Awka Anambra State, Nigeria. e-mail: Ik.umeh@unizik.edu.ng

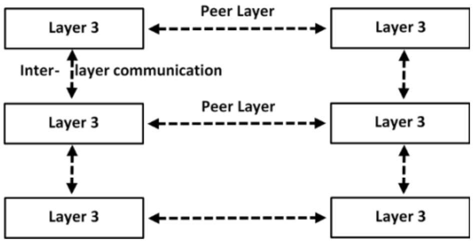


Fig.1: The structure of a layered task

In layered communication system, one layer of a host deals with the task done by the layer or to be done by its peer layer at the same level on the remote host as shown in Fig. 1.

The two most popular layer models used in network communication are the OSI (Open System Interconnection) and Internet or DOD (Department of Defence) models.

c) OSI Network Model

Open System Interconnect (OSI) is an open standard for all communication systems. OSI model is established by International Standard Organization. The model provides a seven layered structure which proffer great benefits in troubleshooting because each layer of the model serves a specific function. For example, the network layer, Layer 3, is charged with logical routing functions. The transport layer, Layer 4, is above Layer 3 and provides additional services. In the TCP/IP world, Layer 3 is served by IP, and Layer 4 is served by TCP (Transmission Control Protocol) or UDP (User Datagram Protocol) as illustrated in the Fig. 2.

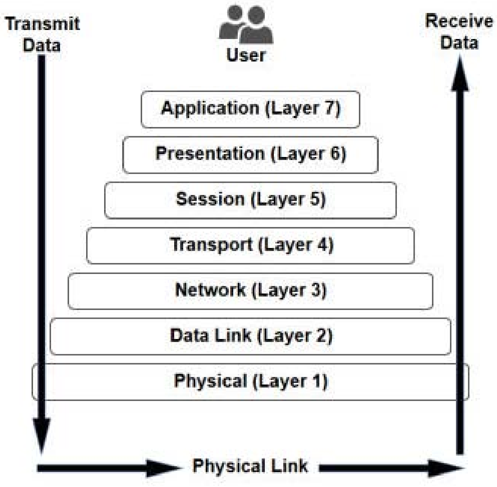


Fig. 1.2: The OSI model layers (image from Webopedia)

d) Network Bandwidth

Bandwidth is a very important network resource and plays a very key factor in networking. Bandwidth can be defined in variety of ways depending on the context. In computing, bandwidth can be defined as; the bit-rate of available or consumed information capacity in a network and expressed typically in metric multiples of bits per second (bps). Bandwidth may be characterized as network bandwidth, data bandwidth or digital bandwidth. Behrouz (2013) defined bandwidth as a range within a band of frequencies or wavelengths while Devajitet al. (2013)defined bandwidth in computer networking as, a reference to the data rate supported by a network connection or interface.

e) Bandwidth Management Challenges

Bandwidth is one of the most required and most expensive components of the internet today. It is a general knowledge that the higher the available bandwidth, the better the performance of their networks but this is not always true rather actually dependent on certain factors viz;

i. The cost of bandwidth is a major cost of network and most organization obtain as much as they can only afford rather than as they need. But most times, the users' demand on bandwidth exceeds the capacity of their link causing saturation and leading to network poor performance.
ii. Most network face the challenge of bandwidth misuse and abuse causing such networks to surfer from bandwidth insufficiency or vulnerability of their networks.
iii. Some networks are not managed at all. Reference Sara gywnn (2013) stated categorically that most research centers and educational institutions in Africa and the developing world are not managed at all thereby causing network failures and sometimes the extinction of such networks.
iv. Avister (2009) alsoproved that although most people assume that internet congestions is only on the link to the internet, but congestion is mainly in the incoming direction.

Therefore, the significance of bandwidth in a network cannot be overemphasized and suggest that there is the need for efficient bandwidth management systems and models in every network.

f) Significance of Bandwidth Management

In order to meet the objectives of organizations and internet users, internet usage must be managed to achieve the following;

1. To control the expensive cost of bandwidth
2. To proffer good network performance and efficiency for critical and useful applications
3. To enable the use of non-critical applications when resources are available

4. To deter the use of insecure and illegal applications within their networks

II. Bandwidth Management Techniques

Different traffic requirements exist for different users and different applications in a network. While some users or applications are termed critical because of their importance or bandwidth requirements, others are not. Bandwidth management techniques are employed in networks to basically provide proper utilization of bandwidth. Bandwidth management begins with network planning and design at the inception of a network but eventually through various other techniques by using the different layers of the OSI model. Bandwidth management techniques are aimed at;

1. Limiting the non-critical traffic in such a way that it does not affect the necessary critical traffic
2. Bandwidth traffic attempts to separate the critical traffic from the non-critical in other to achieve 1 above.
3. It also aims at providing sufficient resources traffic for areas deemed critical by the network owner
4. To carry non-critical traffic on the basis of resource availability.
5. To limit the usage of unauthorized applications within the network.
6. To limit the size of bandwidth usage and avoid waste.

In order to achieve these outlined objectives of bandwidth management, the various techniques employed by different network owners, administrators and users to manage bandwidth apart from the measures considered during the planning and design of a network can be categorized into four main follows;

a) *Restriction of Internet Usage Technique*

This technique implies placing a restriction on those users, group of persons or applications from accessing the available bandwidth by means of software embedded in a routers and seems to be more effective in providing security. Most internet users in organizations only require to access their corporate intranet and email. Such users should be restricted from accessing the internet rather may be provided with web machine for their occasional internet need since not providing internet access to those who do not need it for corporate functions improves the network security. Also, access restriction include the prevention of unauthorized users and non-critical applications from accessing the bandwidth. This is a sure way of improving network bandwidth and security. Sometimes, users are equipped with applications that are not necessary for their corporate function and they end up wasting bandwidth and causing network traffic hugs. For example running streaming media, social media and torrent download in a corporate environment. Such should be restricted to improve network performance by reducing unnecessary traffic in the network. Access restrictions are implemented by assigning private IP addresses (e.g. 192.168.xx.xx) to users, none use of se network address translation (NAT) and through channeling web access via a proxy server. Access restriction can be summarized as taking administrative measure to prevent unauthorized bandwidth usage.

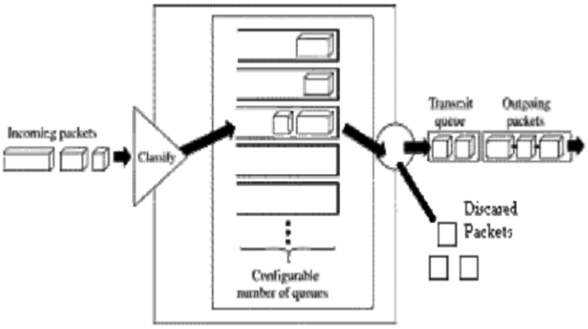


Fig. 2: Restriction of internet usage technique

b) *Time Shift Internet Usage*

This bandwidth management technique uses ftp (file transfer protocol) and web mirror servers to upload files on to the server at night which can be accessed by day. It applies off-line downloading where large files downloads are queued for off-peak hours. User are requested on appeal to shift their internet usage time and this technique often yields low success.

c) *Managing multiple connections*

This is another technique used for managing bandwidth. Obviously, managing a single network is a lot easier than managing multiple sites but many sites use multiple connections as a result of cost and reliability problems. It is ideal to share network load proportionally among multiple connections but it is easier to control outing traffic as against in coming traffic because of the difficulty of managing the dynamic assignment of IP addresses from different connections to different group of users. Border Gateway Protocol (BGP) is a standardized exterior gateway protocol designed to exchange routing and reachability of information among autonomous systems. BGP is difficult to configure for managing multiple connections and requires the co-operation of the ISPs involved as well as the services of an expert to configure it. Furthermore, multiple connections bandwidth management technique is done using NAT and use of proxies with multiple IPs apportioned to the IP.

d) *Network Layer Bandwidth Management*

The network layer of the OSI network model is responsible for address assignment and the unique addressing of hosts in a network using the IP network protocol to route messages using the best path available. Bandwidth management at the network layer operates as a real time management technique by processing data packets as they arrive. Managing bandwidth at the network layer involve network traffic also called data traffic which refers to the amount of data moving across a network at a given point of time as stated by Jianguo (2013). Network data is mostly encapsulated in network packets which provide the load in the network. Network traffic is the main component for network traffic measurement, network traffic control and simulation. The proper organization of network traffic helps in ensuring the quality of service (QoS) in a given network. The QoS techniques of Integrated Services (Intserve) and differentiated services (Diffserve) can be used to manage bandwidth since it has to do with data traffic. QoS is used to provide service to applications at the required quality by checkmating data loss, delay and jitter to manage and make efficient use of bandwidth to meet organization’s needs. QoS and bandwidth management have similar objectives except that QoS is real-time and only applicable at the network layer while bandwidth management can be done using different techniques at different layers of the OSI model to achieve the required objectives. QoS uses packet classification, queuing disciplines, packet discard policies, policing and shaping as to perform bandwidth management functions. Conclusively, one can include QoS in a bandwidth management system by configuring QoS in a router to control outgoing traffic as far as the internet link is not congested. Incoming traffic is though difficult to control using this technique. Bandwidth management at the network layer is traffic control based using a router as illustrated in Fig.2.1.

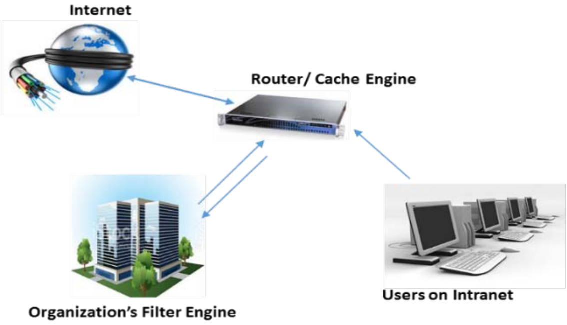


Fig.2.1: Traffic control router based bandwidth management

Network layer bandwidth management divide traffic into classes viz. IP address based, using subnetwork, based on application versus port assignment or the combination of both classes and thereafter applying QoS techniques for each class on input of Internet connection and on the output (e.g. Ethernet port) of the network border router and applying static or dynamic bandwidth allocations to manage bandwidth.

i. *Bandwidth allotment model (BAM)*

Bandwidth allotment model was the first bandwidth modelling management model developed and was used in a triggered dynamic bandwidth management mechanism [15].

ii. *Bandwidth Constraint Models*

One of the goals of DiffServ or MPLS traffic engineering is to guarantee bandwidth reservations for different service classes. For these goals two functions are defined

(i) Class - type (CT) is a group of traffic flows, based on QoS settings, sharing the same bandwidth reservation; Bandwidth constraint (BC) is a part of the output bandwidth that a CT can use.

iii. *Static Bandwidth Allocation*

This management technique allocates maximum bandwidth level to each class and uses traffic-shape or rate-limit command to control the data traffic. If a class uses less than the allocated bandwidth, it is not restricted but if the class attempts to use more than the allocated bandwidth, it is limited. If total allocations is less than or equal to the available BW then all allocations can be satisfied. Otherwise, Total allocation ids greater that the available bandwidth.

iv. *Dynamic Bandwidth Allocation*

In dynamic bandwidth allocation policy-map and bandwidth or priority commands are used to provide limited bandwidth only when link is congested. The classes are not subjected to limitation only when the link is not congested.

v. *Bandwidth Reservation*

Bandwidth reservation is another allocation method which is based on priority of a class. The remaining bandwidth can then be allocated to none priority classes. It is best used when a fixed bandwidth is required for priority or critical traffic.

e) Limiting Non-priority Traffic

This is done allocating Small bandwidth nonpriority traffic classes while the remaining available bandwidth is left for the priority traffic. The method is suitable when traffic is variable and the priority traffic does not require unnecessarily limitation.

i. *Priority Queuing*

This method gives priority to the priority class and sends traffic to others only if the link is free. They remain in que until there is no traffic requirement from the priority class.

ii. *Proxy and Caching*

These are two other network layer bandwidth management methods. Maximum Connections and Bandwidth are two parameters that can be used to control browsing speed of clients in a network using a proxy server [9]. Reference [9] further stated that in computer networks, a proxy server may be a computer system or an application which serves as an intermediary between servers sought after by clients. Proxy servers are hosts systems which relays web access requests from clients. They are used when clients do not have direct access to the web to improve security, logging, accounting and performance in networks.

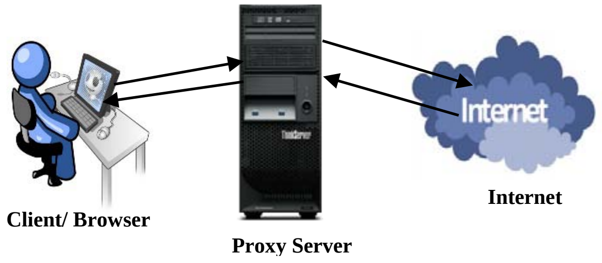


Fig.2.2: Proxy Server used for bandwidth and other management

Caching and storing copies of recently accessed web pages for faster data access is another method of managing bandwidth. It enable pages to be delivered from the cache when requested for again. The pages are stored in browser caches and or proxy caches and manage bandwidth by;

- providing shorter response time to data
- reduced bandwidth requirement from users or client
- reduced load on servers thus increasing their efficiency
- providing network access control and logging
- Some examples of proxycache include; Apache proxy, MS proxy server and Squid.

III. Application Layer Bandwidth Management

Network application layer techniques for bandwidth management is another bandwidth management techniques which has been proved by recent research to be one of the most critical areas that can be used to improve bandwidth management and provide efficient network performance yet it has been observed to be the least area that has been researched in solving bandwidth or network management problems. According to Avister (2009),Youngzsoft (2015) and Ronget al. (2010),different application have been developed and distributed for managing network at the application layer while more are still undergoing development for use as network based bandwidth management applications. New network technologies are emerging and network usage is also growing very rapidly such that today, almost all organizations and individuals cannot work without the internet which is the largest network as stated by Kassimet al. (2012). Networks provide better communications, transfers of data and information, businesses through cloud computing and many more. These needs have resulted in the development of more applications to meet up with the need of these services. The application tools need to be monitored for business purposes and must prioritize the network bandwidth as it should be used since internet bandwidth usage ranks top among other network application needs.

Application layer bandwidth management (BWM) allows for the creation of policies which regulate bandwidth consumption by specific file types within a protocol, while allowing other file types to use unlimited bandwidth. This enables a network administrator to distinguish between desirable and undesirable traffic within the same protocol. Application layer bandwidth management is supported for all Application matches, as well as custom App Rules policies using HTTP client, HTTP Server, Custom, and FTP file transfer types.

a) Firewalls

Firewalls are usually configured to manage bandwidth at global or WAN levels. Bandwidth management modelling using the network applications layer which was based on a comparative study on five recent research on this subject, it was and discovered that each of them used a different mathematical equation to model the bandwidth management method in a network [12]. Reference [12] survey showed that apart from the use of firewall and "Big pipe" approaches to manage network and bandwidth, different recent researches adopted different model, algorithms or techniques in solving either network or bandwidth management problems at the application layer of the OSI model which have also been agreed as the best layer for bandwidth management even though bandwidth management problems still exists.

b) Application Bandwidth Management

Application bandwidth management (ABM) is the collection of a set of Quality of Service (QoS) tools used to manipulate and prioritize data traffic by application type thereby preventing bandwidth-intensive applications, such as peer-to-peer applications like BitTorrent from crowding or taken over legitimate business traffic in a network.

Dan Dinicolo (2013) mentioned that, advanced bandwidth management solutions are employed to maximize an organization's available bandwidth through carrying out inspections and classifying the generated traffic by common business applications based on granular policies, and ensuring that the most critical network traffic receives the highest priority across WAN links.

Solutions provide automatic application protocol classification and comprehensive policies and traffic controls such as rate shaping, rate limiting, selective dropping and priority marking.

c) Application Protocol Classification

Application protocol Classification involves Deep Packet Inspection (DPI) techniques which will enable bandwidth management devices to identify application protocols not withstanding whether those applications use deceptive port-hopping, port-tunnelling, and encryption techniques to avoid detection or not.

d) Innovative User-Based QoS Policies

This technique allocate bandwidth and network application access transparently to network users solely on the bases user IDs or using traditional QoS policies with respect to Layer 3-7 traffic classifications.

e) Bandwidth Utilization Reports

Bandwidth utilization reports are used to quickly identify top protocols, and find users that are consuming too much bandwidth with a view of managing and effectively utilizing the available bandwidth on a network.

f) Internet Access Bandwidth Management Techniques

Internet Access Management is one of the resource management techniques and is often based on using the network applications layer to conserve bandwidth in a network. The implementation of user's bandwidth control at this level raise critical concern most especially in a broad organization's network. Devajitet al., Ronget al. and Cao et al.'sresearch on bandwidth management proffered efficient solutions for bandwidth management using different internet monitoring scheme. Their results followed that capturing data by monitoring and filtering access to the internet is one of the scheduling schemes for conservation and management of bandwidth on the applications layer. Internet access management systems enable network owners to monitor, create reports and manage traffic travelling for inbound or outbound traffic in the network. Internet access management provides better network bandwidth management resulting in increased employees productivity and reduced legal liability associated with undesirable Internet content as specified by Devajitet al..Many tools can be implemented to run internet filtering management in data collections which is based on routing layer protocol or application layer protocol Avister(2013).

IV. Analysis of the Existing Bandwidth Management Applications

All the existing different BWM models and techniques used for network bandwidth management which were x-rayed in section IIIproved to be efficient but each of the model, techniques of algorithm lacked in certain aspects therefore failed to provide total bandwidth management due to one or two deficiencies as follows.

a) Lack of Security in Some Models

One of the major challenges facing modern networks management is security. Security begin with the users in a network to other threats from outside the network especially through the internet. An unsecured or an insecure network is prone to bandwidth wastage, misuse and other network problems which can affect bandwidth most especially when the network user causing the problem remains unidentifiable.

b) Non-Consideration of Human Factors on Management

All the existing bandwidth management methods reviewed did not consider the human intervention / user involvement in both using and managing bandwidth as necessary parameters to be considered in order to secure an efficient bandwidth management in a network. It can be seen that biometric parameters can have serious effect on bandwidth but are not considered by the various techniques for bandwidth management reviewed.

c) Specialization of Management

The network layer techniques considered data traffic as the major parameter for bandwidth management while the application layer management techniques considered filter and bandwidth allotment based on classes or policies as the possible methods for bandwidth management. These alone cannot yield complete bandwidth management.

d) Lack of Biometric Impact

In almost every network management practice, the facial identity, department, position, job title are not deemed necessary for user account creation. Most often, only a User name, user ID and password are the only identification and authorizations considered when creating user accounts in most network. The implication is that the network admins most often do not have access or opportunity of seeing or physically identifying who is using or doing what in their networks. Therefore such practices like impersonation, stealing a user ID or masquerading a user can easily grant network access to an unauthorized user who may misuse bandwidth and malicious activities which can eventually cause harm to the network. Also, an authorized user in a large network may tend to waste or misuse bandwidth when he or she cannot be physically identified.

e) Recommendations for Good Bandwidth Management Model

Based on the analysis of this survey, the following recommendations are suggested to be included in any bandwidth management application to proffer bandwidth or network management efficiency.

a) Inclusion of biometrics parameters for identity of users' account in every bandwidth management application.
b) The development of a hybrid model or system that will encompass the features of the various application layer models applied for bandwidth management.
c) The inclusion of an automatic and immediate feedback system to any bandwidth management system with the capability of using the mac address of every user who attempts to gain entrance to a network but fails after two attempts. The user will only be able to login after a biometric or physical identification is made by the admin.

In conclusion, of an audit trail system that is capable of always monitoring the activities of high end bandwidth users.

V. Conclusion

Despite improvements in equipment performance and media capabilities, network design is becoming more and more difficult as networks are expanding on daily basis due to the digital age. The trend is toward increasingly complex environments involving multiple media, multiple protocols, and interconnection to networks outside any single organization's dominion of control. Carefully choosing the most appropriate model in designing networks can reduce the hardships associated with growth as a networking environment evolves. Choosing the appropriate network model must not be overlooked because, it is a prerequisite for a network design and the eventual management of a network and its resources. Different bandwidth management technique and models were surveyed with respect to the layers of the OSI network model. The survey showed that the application layer bandwidth management techniques was recommended by most researchers as the most effective for bandwidth management not withstanding some minor problems which this survey observed to have resulted basically from the non-inclusion of human parameters in the various application layer models surveyed. In conclusion, to curb network and bandwidth management problems, with human being traffic generators and bandwidth users, human factors and influence on bandwidth must be considered by any model before a very efficient bandwidth management solution can be achieved. The survey recommend the development of a model or algorithm which will use the application layer to manage bandwidth while considering bandwidth allocation, sharing methods and using organizational policies based on human biometric and influence to manage networks.

References Références Referencias

1. ANAND,(2005). Wireless Hotspots: Current challenges and future directions, mobile networks and applications,10, pp 265–274
2. Sunjay Sharma. (2011). A course in computer networks (Principles,Technologies and Protocols). OSI reference model and network architecture.First Edition, pp 1 – 44,
3. John S., Okonigene R.E., Matthews V.O., Akinade B., Chukwu I.S,(2011). Managing and Improving Upon Bandwidth Challenges in Computer Network, Journal of Emerging Trends in Engineering and Applied Sciences (JETEAS)2 (3) pp 482 -486
4. BehrouzA.Forouzan, (2013). Data communications and networking 5E, Introduction Global Edition, Chapter 1,13 – 26.
5. Devajit M.., Majidul A., Utpal J., Bora, (2013). A study of bandwidth management in computer networks. International Journal of Innovative Technology and Exploring Engineering, (IJITEE) ISSN:2278-3075Vol-2 issue 2, 69 -73
6. Sara Gywnn, (January 2013). IAP Workshop: "Promoting access and capacitybuilding for scientific information resources. Darker, Senegal, pp 30-32
7. Avistar Communications Corp.(2009).Product approach document bandwidth management, pp 2-10
8. Jianguo Ding, (2013). Advances in network management, CRC Press, Tylor&Francis Group, Boca Raton London New York, International Standard BookNumber 13:978-1-4200-6455-1 (EBook-PDF), pp 90 - 113
9. Youngzsoft,(July 2015).Retrieved from, http://youngzsoft.net/ ccproxy/manage ebandwidth.htm,.
10. Rong, I., Aragao M., C.C. Uchoa, E & Werneck, R.F.,(2010). NewBenchmark Instances for the Steiner problems in Graphs. In M.G.C. Resende J.P. Sousa & A. Viana (Eds) Metaheuristics: Computer decision Making Applied Optimization Series, Norwell, MA, USA: Kluwer Academic Publishers, 2010, Vol. 68, 601 -614
11. Kassim M., Ismail M., Jumari K., and Yusof J., (2012). International scholarly and scientific research & innovation, 6(2) World Academy of Science, Engineering and Technology, Vol:6 2012-02-22, 332 -339
12. Dan DiNicolo,(2013)www.2000Trainers.com. Retrieved on August 23rd 2016. https://en.wikipedia.org/wiki/Layered_ServiceProvider, page was last modified on, at 01:31
13. Cao H., Yeng G., (2010) Bandwidth Management in Computer Networks2010, Retrieved from http//netmag.edu/~poi/clepis233/ebook/index.htm
14. Rafael F. Reale1, Romildo M. da S. Bezerra2 and Joberto S. B. Martins, (November 2013). A

Bandwidth Allocation Model Provisioning Framework With Autonomic Characteristics. International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.6,DOI : 10.5121/ijcnc,, 5606, pp 103 -119

Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 17 Issue 4 Version 1.0 Year 2017
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Survey: Trust-based Approaches to Solve Routing Issues in MANET

By Pawan Makhija & Neha Sharma
Shri G.S. Institute of Technology and Science

Abstract- A mobile ad hoc network is a wireless network. The ability to work without any central controlling authority without any requirement of established infrastructure makes it need of the present scenario. This dynamicity comes with a downside of security. Since the nodes may act maliciously and pose threat to the working condition of the MANET. Trust approaches are well suited in these situations. Here we discuss TRUST; the meaning, characteristics and different schemes.

Keywords: MANET, trust, mobile node, black hole attack.

GJCST-E Classification: E.3

Survey: Trust-based Approaches to Solve Routing Issues in MANET

Pawan Makhija α & Neha Sharma σ

Abstract- A mobile ad hoc network is a wireless network. The ability to work without any central controlling authority without any requirement of established infrastructure makes it need of the present scenario. This dynamicity comes with a downside of security. Since the nodes may act maliciously and pose threat to the working condition of the MANET. Trust approaches are well suited in these situations. Here we discuss TRUST; the meaning, characteristics and different schemes.

Keywords: MANET, trust, mobile node, black hole attack.

I. Introduction

Since the invention of computer networks there has been a constant demand for three things: increased connectivity, increased communication speed, and increased storage capacity. It is clear that if a user cannot connect to the infrastructure the speed and the storage demands become irrelevant. Recently, wireless devices (hereafter referred as nodes) have become the preferred mean to access the networked infrastructure. In this paper, we focus on trust based approaches designed for ad-hoc networks, which, by definition are networks that do not have a previously deployed infrastructure. Here nodes collaborate to forward packets from a source to a destination [2]. However, since nodes are resource constrained they may behave selfishly. If the number of selfish nodes grows considerably the performance of the network may degrade to the point where nodes can only communicate with nodes located within its transmission range. A large numbers of trust-based approaches have been proposed to deal with nodes' malicious behaviours [5, 6, 7, 8, 9, 10, 11, 12, 13].

II. Trust Characteristics

Trust is useful in environments where the participants need to depend on each other to achieve a goal. In ad-hoc networks nodes need to rely on routers to forward the packets from the transmitting to the receiving nodes. However with current technology restrictions (memory, power, etc.) one or more routing devices may choose to behave selfishly. To achieve a reliable cooperation trust must be established.

Trust is context sensitive: Trust should not be calculated over a node as an entity, but rather as a set of actions that a node can perform. e.g. Instead of expressing trust of a node say 'A' as "node A is trusted", in an ad-hoc networks use "node A trusts node B to forward a packet to the required destination, but Node B may or may not be making copies of a received packet".

Trust is subjective: Trust, as defined in psychology, is not only evaluated based on the behavior of the entity, but also on how the evaluator perceives the behavior. The variations in point of view depend on the intrinsic characteristics of the evaluator such as how easily the evaluator trusts others, and the expectation of trust. In trust-based approaches for ad-hoc networks all the intrinsic believes and requirements of ad-hoc nodes are reflected in a threshold value.

Trust is not reciprocal: When a node trusts another node, the trusted node is not required to trust the trusting node in return. For example: node A may trust node B to forward its packets, but this does not necessarily y mean that node B trusts node A to forward its packets. This is because the expectations of trust may be different in every node.

Trust may not be transitive: Transitivity is a logical relationship in which if it holds, for an operator (op), that A op B, and B op C hold then A op C must be true. Most authors argue that this property does not apply to trust-based approaches. Therefore the fact that node A trusts node B, and node B trusts node C does not necessarily imply that node A trusts node C.

Trust is dynamic: Due to the quick and unpredictable change in a node's behavior and to the unpredictability of a node becoming compromised trust should be updated frequently.

Trust is a measure of uncertainty: Trust is most frequently represented as the probability that an agent will perform an action. When the probability is different from 1 or 0 then the subject has no way of knowing for sure whether the agent will perform the action.

III. Trust Methodology

We here present a variety of approaches based on Trust methodology. These approaches are applied on MANETs. As MANET provides open for all environments to all the aspiring nodes, the need of secure route is even more required. This survey paper is

Author α: Assistant Professor, Department of Information technology, Shri G.S. Institute of technology and science, Indore(M.P).
e-mail: pawanmakhijaacro@gmail.com
Author σ: Assistant Professor, Department of Information technology, Shri G.S. Institute of technology and science, Indore(M.P).
e-mail: ne3haa@gmail.com

aimed to provide different ideologies of Trust in MANET.

a) Trusted AODV [5]

In this scheme, AODV protocol is modified implementing node trust and route trust. Two new control packets are added to AODV protocol i.e. trust request packet(TREQ) and trust reply packet(TREP) and routing table is modified by adding one new field: route trust. The RREP packet of AODV is also modified by extending two new fields: neighbour list and route trust.

i. *Calculation of Node Trust*

All the nodes maintain neighbour table to keep information of frequently changing node and node trust value. Node trust value is evaluated using neighbour's collective opinion. The node trust value (NTV) of a node i is calculated by the following formulae:

$$NTV=[NNT(1)+NNT(2)+NNT(3)+\ldots\ldots+NNT(n)]/n$$

where NNT is the neighbour node trust value about the i node and n is the no of neighbour in the neighbour list.

ii. *Calculation of Route Trust*

Every node calculates route trust for each route in the routing table at some regular interval. Destination node in each entry in the routing table generates R_ACK packet and send back in reverse path. The nodes that receive R_ACK calculate the route trust value using the value in the no_of_packets_received field of R_ACK packet and the value of no_of_packets_sent field in the routing table. Route trust value is calculated by the following formulae: Route trust= (no of packets send by source - no of packets received by destination). The route with route trust value 0 is the perfect one. If the route trust value is equal to the no of packets sent the route is rejected.

iii. *Route Discovery*

In route discovery phase when a node has packets to send it broadcasts RREQ packets. When all RREQ reaches to the destination, it sends RREP packets. After receiving the RREP packets, source node selects three RREP packets that have high route trust value. Then the source node generates the TREQ packets and sends it to all neighbours in the neighbour list of that RREP packet. After receiving the TREQ packet, all neighbours replies with TREP packet to the source node. Then the source node calculates the node trust of the nodes. Next, the source node arrange the RREP packets in the ascending order based on node trust value and selects the first RREP packet and hence that path is selected for communication.

b) Cooperation of Nodes: Fairness in Dynamic Ad-hoc Networks [6]

The main idea of CONFIDANT protocol is to identify non-cooperative nodes. A node selects a route based on trust relationships which is built up from experienced routing and packet forwarding behavior of other nodes. Each node monitors the behavior of all neighbor nodes. When any misbehaving node is found, alarm messages are sent to all other nodes in the network. As a result, all nodes in the network will be able to avoid that misbehaving node while selecting a route. The components of CONFIDANT protocol works as follows:-

i. *The Monitor*

This component watches the behavior of nodes during the routing procedure. If any node misbehaves, then the monitor module detects that misbehaving node and immediately calls reputation system.

ii. *The Trust Manager*

The trust manager handles ALARM messages. When any misbehaving node is found ALARM messages are sent to all other nodes to inform about that node. The trust manager maintain alarm table and trust table for checking the trustworthiness of alarm. The rating function assigns greater weights for own experience and smaller for other nodes opinion about that detected node. The rating of a node is updated when sufficient proof of the nodes maliciousness is found. If the rating falls below threshold value path manager module is called.

iii. *The Reputation System*

The reputation system maintains the rating of nodes in a table which has 2 fields node id and their ratings. The ratings are done according to the type of nodes behavior detected. The rating of a node is updated when sufficient proof of the nodes maliciousness is found. If the rating falls below threshold value path manager module is called.

iv. *The Path Manager*

The path manager manages the routing path according to ratings of the nodes. The path containing malicious nodes are deleted by this module. If any route request comes from malicious node path manager takes appropriate action like ignore request or don't reply etc.

c) Friendship Based AODV (FrAODV) [7]

In Friendship based AODV is based on AODV, there are two evaluation algorithms to evaluate forward and reverse path between source and destination. In this scheme, it is assumed that each node has identity can't be forged by any other malicious node and no of malicious node is less than the no of good nodes. In this proposed scheme every node has a list of friends with friendship values. The range of friendship values is 0 to 100. More the friendship values means more trustable. The two algorithms for establishing path are described as follows:

i. *RvEvaluate Algorithm*

This algorithm sets up reverse path from destination to source. After broadcasting RREQ packet the two things can happen: -

Case-1: The receiving node can be destination node itself. If so it checks the friendship value of the node from which it receives the RREQ packet, as every node maintains a friendship list along with friendship value of the neighbor nodes. If the node is not a friend the node rejects the RREQ packet. Otherwise it calculates the friendship value of the route to originator from destination and then compares the current routes friendship value with the existing route's friendship values. The reverse route's friendship value (RvFrRte) is the sum of friendship values of all nodes in that path and it is calculated as follows:

$$RvFrRTe = \sum_{i=1}^{n} \frac{PrFrHpi}{h}$$

where PrFrHpi is friendship value of that node from which the current node receives RREQ packet and h is the no. of hops between source and destination. If the friendship value of the new route is less than the existing route the new route is rejected otherwise it is registered as a friendly route.

Case-2: If the receiving node is intermediate one, it first checks the friendship value of the node from which it receives the RREQ packet and next neighbor node. If one of these two nodes is not in friend list, the intermediate node rejects the RREQ packet. Otherwise it calculates the friendship value of the route to originator from destination using the previously mentioned formulae and compares it with the existing route's friendship value. If the friendship value of the new route is less than the existing route the new route is rejected otherwise the reverse path is established from current node to the previous node.

ii. *FwEvaluate Algorithm*

This algorithm sets up the forward path i.e. from source to destination during RREP forwarding. There are following two cases when any node receives that packet:

Case-1: If the node receiving the RREP packet is sender node itself, it checks the friendship list and the friendship value of the node from which it receives the RREP packet i.e. the next node. If the next node is not a friend, rejects the RREQ packet. Otherwise it calculates the friendship value of forward route to destination and then compares it with the existing route's friendship value. If the friendship value of the new route is less than the existing route the new route is rejected otherwise it is registered as a friendly forward route. If there is not any existing route the new route is included as a friendly route. The forward path's friendship value is formulated as:

$$FwFrRte = \sum_{i=1}^{n} \frac{FwFrHpi}{h}$$

Where FwFrHpi is friendship value of that node from which the current node receives RREP packet and h is the no. hops between source and destination.

Case-2: If the node is an intermediate node then it checks the friendship value of the node from which it receives the RREP packet and previous node. If one of these nodes is not friend, rejects the RREP packet. Otherwise it calculates the friendship value of the route to destination in the same way and compares it with the existing forward route's friendship value. If the friendship value of the new route is less than the existing route the new route is rejected otherwise the forward path is established from current node to the next node. In this way after establishing friendly path from source to destination the sender sends data packet along that path.

d) *Secure Routing using Trust (SRT) [8]*

In this paper, a secure routing using trust level is proposed. This scheme is based on node transition probability (NTP) and AODV. This scheme develops a new algorithm to secure NTP protocol. A trust rate (T rate) is calculated as a parameter. When a node has data packet to send, it first floods control frame (beacon) in search of secure and reliable route. After broadcasting the first beacon trust rate is evaluated as:

$$Trate = \frac{(r - t)}{r}$$

Where r = no of beacons received by a node, t =no of beacons send by a node. This T rate value divides the nodes of the network into 3 categories: Ally list (level2), Associate list(level1), Acquaintance list (level0).

Ally list: The nodes of the ally list send highly secured information.

Associate list: The nodes of this list send medium secured information.

Acquaintance list: The nodes of this list send the information that does not require any security.

An additional field "level" is there in neighbor table. When a node has data to send it just checks its neighbor table, if the destination is available it just sends data packets. If not, it searches for a node which has route to destination in its same level. If no suitable node is not found it goes to next lower level and so on. If any node in the same level is not found trust is compromised by choosing a neighbor in the next lower level using the following formulae:

Trust compromise= n (associate) + 2*n (acquaintance)

Where n (associate) is the no of nodes in associate list and n (acquaintance) is the no of nodes in acquaintance list. When all the nodes including destination node are in the same level with the source node trust compromise will be very low because trust rate is very high as it is better to forward control packets in the same level than to forward the packets to the another level. In this way after finding secure route the data packets are sent to the destination.

e) *Trusted AOMDV [9]*

AOMDV is a multipath routing protocol. In the paper, a trust mechanism is employed with soft encryption methodology in AOMDV protocol. This Trusted AOMDV protocol has the following steps:

i. *Degree of Secrecy for Path /Message*

Degree of secrecy of a path implies how much degree of security level required for a path to transfer packets. The path trust value (Tp) is the minimum trust value among all nodes along the path p depending upon the path trust value there are three classifications: - If Tp ≥8 implies class A paths. All the class A paths have degree of secrecy≥8. Tp ≥5 implies class B paths. All the class B paths have degree of secrecy ≥5. Tp ≥3 implies class C paths. All the class C paths have degree of secrecy ≥3. This classification is also applied for data packets. Class A data only is transferred to class A category path. It is same for other categories.

ii. *Message Encryption*

The message is divided into three parts and then encrypted using soft-encryption methodology to secure the message. It is encrypted in the following way:

$$a' = a\text{XOR}c;\ b' = b\text{XOR}c;\ c' = a\text{XOR}b\text{XOR}c$$

iii. *Message Routing*

Before routing the encrypted messages a secure trusted path is established using the following trust mechanisms:-

The trust mechanism of this scheme depends on the monitoring of packets and node's behavior. It is assumed here that when a node sends packets it will monitor its neighbor node to which it sends its packet and determines node's trust value depending on its behavior. If the neighbor node sends the packets correctly node's trust will increase, otherwise it is decreased. The trust value of a node (Tn) is calculated as:

$$Tn = Wd * Td + Wr * Tr$$

where Wd is the weight assigned to direct trust Td, Wr is the weight assigned to recommendation trust Tr. Again Direct trust is calculated as:

Td= Td+c.Ts, if no. of successful packet transmission time is high and

Td= Td- c.Tf, if the no. of packet transmission failed time is high.

where Ts is the aggregate successful transfer time, Tf is the aggregate failure transfer time and c is the predefined constant value. Ts is incremented by 1 for every successful transfer of packet, otherwise Tf is incremented by 1. The trust table values determined through hello message transmission. When a node receives hello message it first check trust table contained in hello packet and find some common nodes it has. If any node common node is found that wants to participate in forwarding packets the trust recommendation (Tr) is calculated by the formulae:-

$$Tt = \sum_{x=0}^{n} 0.1 * Td(A \rightarrow X) * td(X \rightarrow D)/n$$

where Td(A → X) implies source A's trust on intermediate node X and Td(X → D) implies X's trust on destination D and n is the no. of hop.

In the routing process, source broadcasts RREQ packet. When an intermediate node receives the first RREQ packet it checks the path list and hop count and updates its reverse route table and sets up reverse path. When duplicate request packet arrives at node it checks the hop count of that packet, if it has lesser hop count than the previous one, record of the previously received packet is replaced by the new one in the reverse route table. After receiving request packet destination node generates reply packet (RREP) and sends back to the sender. When an intermediate node receives RREP packet, it compares the trust value in RREP packet with the node's trust value from which it receives the RREP packet. If the node's trust value is less than the one in RREP packet, the trust value in RREP packet is replaced by that node's trust value. In this way, finally when RREP packet reaches to the source node, it gets the trust value from the RREP packet and set it as a trust value of that path. After receiving all the RREP packets and the path trust values, it sorts the paths based on the trust values. Then it breaks Computer Science & Information Technology the message in three parts and encrypts it in the previously mentioned way and starts sending it to the appropriate path according to the data degree of secrecy. After route discovery, if the appropriate path is not found, routing process will be restarted.

f) *Friend Based Ad Hoc Routing using Challenges to Establish Security [10]*

This algorithm achieves security in ad hoc network by sending challenges and sharing friend lists. In this scheme, there are different list of nodes: **Question mark List, Unauthenticated List, Friend List.** The rating of friends ranges from 0 to 10. This algorithm has four steps: challenging neighbor, friends rating, sharing friends and route through friends. FACES is a hybrid protocol as the routing of data is on demand where as challenging and sharing occurs periodically. When the network is initialized, the nodes are not familiar with each other. So after initializing the network the nodes challenge each other to find the friend nodes. The challenging mechanism works as – suppose node A challenges its neighbor B. A first performs share Friend list with B by sending FREQ packet to B. After receiving FREQ packet from A, B replies by sending its all three list to A. After getting replies A picks one node (let C) from B's list to which it can reach by own. Then send a challenge packet to C directly and through node B. When C receives challenge packet it replies node A and node B in turns replies to node A. then node A compares these two results if it matches node A add B in its friend list otherwise in question mark list.

Friends are rated in this scheme using three parameters: Data rating (DR), friend rating (FR), net rating (NR). Initially the nodes only have friend List, nodes of which perform a successful challenge. The sharing of friend list takes place periodically. Let node B sends its friend list to node A during the friend sharing stage, then node A picks those nodes that are not in its own list from friend list of B and includes those nodes in its own list and the rating of those nodes, which is obtained from B set as FR of those nodes. The data rating (DR) of those nodes is set to zero. Then the net rating (NR) of node is calculated as:

$$NR = \frac{W1 * DR + w2 * FR}{w1 + w2}$$

where w1 and w2 are the weight that is network dependent.

If the friend of B is already in the list of A i.e. if the nodes A and B have common nodes (let C) then A obtains rating of C from B and calculate obtain rating as:

OR= (net rating of B in list of A * net rating of C in list of B)/ 10

FR of node C is obtained by adding all OR from various neighbor nodes and divides the value by the sum of ratings of those various nodes. The data rating is calculated on the basis of data transfer by a node. DR is calculated as: DR=10*(1-e-λx), where x is no of forwarded data packets and λ is a factor by which data packets are related to rating. The routing of data takes place when any node has data to end. It broadcasts route request message including no of data it wants to send. After receiving route reply messages, it finds the best route depending on the net rating value of nodes, to the destination from its friend list.

g) Trust Based Security Protocol Routing [11]

In this protocol a trust mechanism is employed in DSR protocol. An extra data structure is maintained by every node that is Neighbor's Trust Counter Table (NTT) which is used to keep track of no. of sent packets by a node using a forward counter (FC) and also stores the trust counter(TC) corresponding to node. Initially a node can completely trust its neighbor or fully distrust its neighbor as the nodes don't have any information about its neighbor nodes reliability. When any node needs to send data it broadcasts RREQ packets. Each time a node (let nk) receives packet from another node (let ni), node nk increments the FC of ni as:

FCni=FCni+1; i=1, 2….

then, this new FCni value is stored in NTT of node nk. After receiving all RREQ packets, destination node makes a MAC on the no of packets it received (Prec) using the shared key between the sender and destination. Then the destination node attaches that MAC and also the accumulated path from the RREQ after digitally signed it, in the RREP packet and sends back in the reverse path to the destination. The intermediate nodes of that path determines Success ratio as: - **SCni=FCni/Prec,** where Prec is the no. of packets received at destination. This SCni is appended in RREP packet. The intermediate nodes in reverse path check the validity of the RREP packet by verifying digital signature of destination. If it is valid, the intermediate node signs the packet and forwards it to the next, otherwise the packet is dropped. When source node finally gets the reply it first verifies the first node id in RREP packet. If it is its neighbor, then all other intermediate nodes' digital signature is verified. If the verifications of all the nodes are successful then the trust counter is incremented for all the nodes as: **Tci = Tci + δ1**, if the verification is failed the trust counter value is decremented by 1: **Tci = Tci - δ1**.where δ1 is the small fractional value. The source node also checks the success ratio of all other nodes and compares it with the minimum threshold value (SRmin), if the SRni of a node is less than the SRmin the trust counter is decremented by another step value δ2 again, otherwise it is incremented.Another comparison is made by comparing trust counter with a minimum threshold. If trust counter is less than the trust threshold value the node is marked as malicious. This mechanism is applied to all the other routes and a route with no or least malicious node is selected. In this way, a trusted and authenticated route is found for secure routing.

h) Trust Based DSR [12]

This protocol is proposed to improve the security of the existing DSR protocol. The trust based secure route is established in this scheme. In DSR the shortest route is selected which may not be secure. There are some malicious nodes in the network that replies to the route request packet with shorter hop count (black hole) so that the source will select that path, and routing process is disrupted. The following components are used in this newly proposed protocol: Initialiser, Upgrader, Administrator, Monitor, and Router. In this scheme, there is a separate administrator to maintain the trust values of all other nodes. An acknowledgement module is there which is used to keep track of all received acknowledgements and trust values of nodes are adjusted. Every node has trust value which depends on its interaction with its neighbor. Trust unit of this scheme comprises of three modules: - Initialiser module assigns low trust values to the unknown nodes in initial stage. If the route contains some known and unknown nodes, then it assigns trust of those known nodes as the initial trust value of the unknown nodes. Upgrader module upgrades the trust value of a node based on experiences of that node in a particular situation. When a node receives any reply from its neighbor the trust value of neighbor node is updated. If any reply is not received by a node the trust value of the neighbor node is decreased. Trust value is evaluated as: $T= \tanh[(\Delta+W) *Te]$ where T is the updated trust, Te is existing trust, W is a weight i.e. 1 for acknowledgements and 0.5 for data packets forwarded and received,Δ is +1 for positive and 0 for negative experiences. Positive experience means acknowledgement is received within the time frame and otherwise it is considered as the negative experience. Administrator module keeps the trust information of all the known nodes and also has some methods to query this trust information. The monitor module monitors the received acknowledgments to adjust trust values of nodes. The router module selects the route to forward packets based on nodes trust values. Monitor module uses two routing strategy: In the first routing strategy, the route is rated based on the average value of all nodes along that path. The route which gets highest rating is selected for routing. In the second routing strategy, the average of all nodes trust value is divided by no of nodes to get shorter path. The route which gets high value is selected.

i) GAODV : Against single Black Hole and Collaborative Black Hole [13]

The AODV protocol has a provision of sending a gratuitous RREP packet to the destination node. Whenever an intermediate node has a route towards destination, in addition to sending the RREP to the source, it also unicasts a gratuitous RREP to the destination node. In our protocol the gratuitous RREP is conceptualized and simulated as the CONFIRM packet. Thus, a CONFIRM packet is unicasted/routed by the RREPN to the destination. Note that it can be sent only if the RREPN has a route towards destination. It is only after the receipt of CONFIRM will the destination await for packets from the source. In order to facilitate cross checking by the source (of the route claimed by the RREPN), the source unicasts a CHCKCNFRM to the destination. Upon CHCKCNFRMs receipt the destination replies by broadcasting a REPLYCONFIRM to the source, only if it received a CONFIRM and a CHCKCNFRM. Since a black hole does not possess a route towards the destination, it fails to send the CONFIRM, thus reply to the CHCKCNFRM is never generated by the destination. This leads the source to conclude that the RREP sending node was the black hole one.

IV. Conclusion

MANETs are vulnerable to different types of attacks due to its infra-structure less network. Different trust based approaches are proposed to prevent such types of attacks and to improve Quality of Services (QoS). These trust based approaches try to give a secure node in routing path by implementing trust mechanism in the existing routing protocols. In this paper, firstly we have given a brief idea on several types of characteristics that Trust posses in itself and then different Trust schemes.

We have seen that there are different methods in which Trust can be applied. But there is a possibility to develop an approach that can be standardised to attain QoS as well as minimizing the several attacks. Trust mechanism can be applied in various environments like in hybrid environments. We can also develop some rules in the protocol on the basis of which the actions are taken to detect the nodes that are authenticated but perform malicious behaviour without dropping packets and also authenticate the nodes to prevent attacks. So we can work on these approaches to develop a new trust based protocol for standardisation.

References Références Referencias

1. G. Aggelou (2004) Mobile Ad Hoc Networks, Mcgraw-Hill.
2. MANET Working Group : http://datatracker.ietf.org/wg/ace/documents/
3. S. Corson, J.Macker. Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations. IETFRFC2501, 1999.
4. Jin-Hee Cho, Ananthram Swami, and Ing- Ray Chen " A Survey on Trust Management for Mobile Ad Hoc Networks" IEEE Communications Surveys & Tutorials, VOL. 13, NO. 4, FOURTH QUARTER 2011.
5. M. Pushpa, (2009) "Trust Based Secure Routing In Aodv Routing Protocol", International Conference On Internet Multimedia Services Architecture And Applications (Imsaa), Usa: Ieee Press, 1-6.
6. S. Buchegger, J. L. Boudec, (2002) "Performance Analysis Of Confidant Protocol", Mobihoc'02, Epfl Lausanne, Switzerland, Pp226-236.
7. Essia, T., Razak, A., Khokhar, R.S.,Samian, N.: Trust-Based Routing Mechanism In Manet: Design And Implementation. Springer, 18 June 2011.

8. Edua Elizabeth, N., Radha, S.,Priyadarshini, S., Jayasree, S., Naga Swathi, K.:Srt-Secure Routing using Trust Levels in Manets. European Journal of Scientific Research, Issn 1450-216x Vol. 75, No. 3 (2012), Pp. 409-422.
9. Huang, J., Woungang, I., Chao, H.,Obidant, M.,Chi, T., Dhurandher, S.K.: Multi-Path Trust–Based Secure Aomdv Routing In Ad Hoc Networks.Ieee 2011.
10. Dhurandher, S.K., Obidant, M.S., Verma, K., Gupta, P., Dhuradar, P.: Faces: Friendhip-Based Hoc Routing using Challenges to Establish Security InManets Systems. Ieee System Journal, Vol.5, No. 2, June 2011.
11. Sharma, S., Mishra, R., Kaur, I.: New Trust Based Security Approach For Ad-Hoc Networks. Ieee (2010).
12. Bhalaji, N., Mukherjee, D., Banerjee,N., Shanmugam, A.: Direct Trust Estimated on Demand Protocol For Secured Routing In MobileAd-Hoc Networks. International Journal of Computer Science & Security, Vol. 1, Issue (5).
13. GAODV: A Modified AODV against single and collaborative Black Hole attacks in MANETs: Dhurandher S.K.; Woungang I.; Mathur R.; Khurana P. Advanced Information Networking and Applications Workshops (WAINA), 2013.

This page is intentionally left blank

Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 17 Issue 4 Version 1.0 Year 2017
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Web usage Mining: Web user Session Construction using Map-Reduce

By Neha Sharma & Pawan Makhija
Department of Computer Science

Abstract- Web Usage Mining deals with the understanding of user behavior while interacting with the website by using various log files. The whole process of Web Usage Mining gets completed in three phases namely Data Preprocessing, Pattern Discovery and Pattern Analysis. Data Preprocessing is important because it takes 80% of the time of the whole process of Web Usage Mining. Data Preprocessing involves Data Cleaning, User Identification, and Session Identification. In Session Identification we find out the set of pages visited by a user within the duration of one particular visit to a website, also called as Sessionization.

In paper[1], we proposed a new method for session construction. As the size of log files are very large so there is a requirement of an approach for Session Identification by which processing time of our proposed method will be reduced to a great extent.

In this paper, we used Map-reduce method to calculate sessions in which we combine both time and user navigation method. This approach is faster than the existing approach because we have performed the whole process in distributed environment.

Keywords: web mining, web server logs, web usage mining (WUM), map reduce, session identification.

GJCST-E Classification: E.3

Web usage Mining: Web user Session Construction using Map-Reduce

Neha Sharma [α] & Pawan Makhija [σ]

Abstract- Web Usage Mining deals with the understanding of user behavior while interacting with the website by using various log files. The whole process of Web Usage Mining gets completed in three phases namely Data Preprocessing, Pattern Discovery and Pattern Analysis. Data Preprocessing is important because it takes 80% of the time of the whole process of Web Usage Mining. Data Preprocessing involves Data Cleaning, User Identification, and Session Identification. In Session Identification we find out the set of pages visited by a user within the duration of one particular visit to a website, also called as Sessionization.

In paper[1], we proposed a new method for session construction. As the size of log files are very large so there is a requirement of an approach for Session Identification by which processing time of our proposed method will be reduced to a great extent.

In this paper, we used Map-reduce method to calculate sessions in which we combine both time and user navigation method. This approach is faster than the existing approach because we have performed the whole process in distributed environment.

Keywords: web mining, web server logs, web usage mining (WUM), map reduce, session identification.

I. Introduction

Web Usage Mining deals with observing user behavior, while interacting with web site, by accessing various log files to extract knowledge from them. This knowledge can be applied for reorganizing the website contents by giving a personalization and recommendation that is more efficient as compared to previous one by improving the links and navigation which in turns increase the rate of advertisement. This will results the users to access the website in a comfortable manner which obviously generate more revenue to them.[2] This scheme comprises of three steps as data preprocessing, data mining and pattern analyzing. Data preprocessing contains three steps as data cleaning, user identification, session identification. Session identification is an crucial step in data processing of web log mining. A session is defined as multiple requests made by a user for a single navigation. A user may have a single or multiple sessions during a particular period. Basically sessions are identified either by Time based method or by Navigation based method. Here, we proposed a unique approach for user session identification by blending Time based method with Navigation based method to get better results.

To increase the pace of Sessionization, the process is performed on distributed systems using Map-reduce. Map- reduce [3] is a programming model and an associated implementation for processing and generating large data sets that supports fault tolerance, automatic parallelization, scalability, and data locality-based optimizations. Users define a Map function that will use this key/value pair for processing the data to generate a set of intermediate key/value pairs and a Reduce function will be called that concatenates all intermediate values related with the same intermediate key.

II. Motivation

Map Reduce is a programming model and an associated implementation for processing and generating large data sets. This process takes a set of input key and value pairs and generates an list of key and value pairs. The user of the Map-Reduce library classifies this calculation as two function as map and reduce functions.

The Map function takes a pair of input and generates a list of intermediate key and value pairs. The values grouped with the help of the Map-Reduce library is fed to the Reduce function.

The Reduce function accepts the output that was generated by the library as value and key pair, merge them to produce a small set of values e.g. zero or one value. The intermediate values that were produced during invocation are feded into the Reduce function with the help of an iterator. This will enable the user to handle large set of values so that it will be stored easily in the memory.

III. Proposed Approach

In order to enhance the performance of the proposed method in [1], we have used Map-Reduce method to lower the session generation time.

We have applied Map-Reduce on the time-based method, maximal forward sequence method and our proposed method[1]. The results that were generated during this approach has tremendously reduces the session generation time as it was fasten up by the Map and Reduce function.

Author α: Department of Computer Science, SGSITS Indore (M.P.), India. e-mail: ne3haa@gmail.com
Author σ: Department of Information Technology, SGSITS Indore (M.P.), India. e-mail: pawanmakhijaacro@gmail.com

The experiment is performed on the log data of www.smartsync.com on 8 Dec 2013.

IV. Testing and Results

The input data that was supplied during our proposed method are the access log files of the www.smartsync. com web server. Because data of log files are large, we have taken the log dataset of only one day (dated 8 Dec 2013) of size 1 GB, 2 GB, and 4 GB. Table-1 shows the time required for completing the process on a single system and multiple systems (ET=Execution Time):

Table-1: Comparison of Time Requirement by an Existing Methods and the Proposed Method on Single System and Multiple System

	Methods	Time in (Seconds)		
		1 GB dataset	2 GB dataset	4 GB dataset
1.	ET on Single System by Time based Method	4932	10221	19312
2.	ET on Single System by Maximal Forward Sequence Method	5014	9142	19514
3.	ET by Proposed Approach (Single System)	4821	8912	19455
4.	ET on Multiple Systems by Time based Method	2187	5346	10132
5.	ET on Multiple Systems by Maximal Forward Sequence Method	2034	5674	10314
6.	ET by Proposed Approach (Multiple Systems)	2512	5112	10248

Figure-1 shows the graphical representation of Table-1 for comprising the time requirement in completing the process by an existing method and the proposed method.

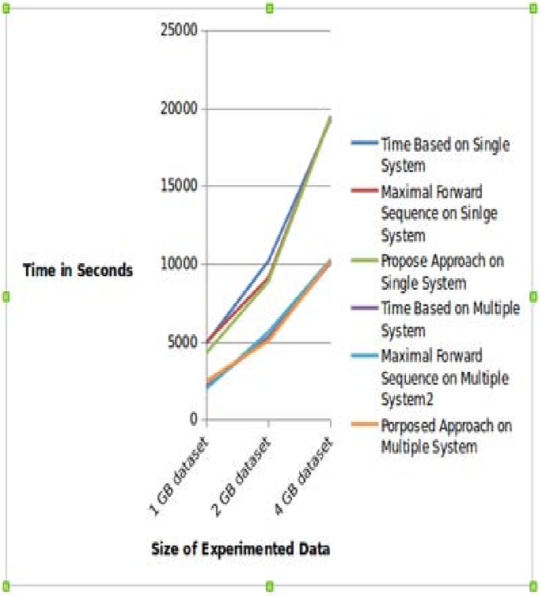


Figure-1: Graph for comparison of various time requirements

V. Conclusion

The information available on the web is increasing day by day in a fast manner. This lets the user to have a lot of data to access freely on the web. Our method have generated sessions that took less time comparable to the existing method. The experiment on 1GB, 2GB, and 4GB data shows that the new method proposed in [1] generates more sessions (3102) than the traditional Time Based Method (2875) and Maximal Forward Sequence Method (2742). As per the result shown in Table-1 with the proposed approach, this process takes less time in completion because of Map Reduce method.

References Références Referencias

1. Neha Sharma, Pawan Makhija, "Web Usage Mining:A novel approach for web user session construction" GJCST vol. 15 issue 3 version 1.0, 2015.
2. Jeffrey Dean and Sanjay Ghemawat, "MapReduce: Simplifed Data Processing on Large Clusters" OSDI 2004.
3. Nirali N. Madhak, Trupti M. Kodinariya, Jayesh N. Rathod, "Web Usage Mining: A Review on Process", IEEE 2013.

4. Robert.Cooley,Bamshed Mobasher, and Jaideep Srinivastava, " Web mining:Information and Pattern Discovery on the World Wide Web", *In International conference on Tools with Artificial Intelligence*, pages 558-567, Newport Beach, IEEE,1997.
5. He Xinhua, Wang Qiong, "Dynamic Timeout-Based A Session Identification Algorithm", IEEE 2011.
6. Fang Yuankang and Huang Zhiqui, "A session identification algorithm based on frame page and page threshold", *Computer Science and Information Technology (ICCSIT)*, 3rd IEEE International Conference, 2010 .
7. R. F. Dell et al.,"Web user session reconstruction using integer programming", International Conference on Web Intelligence and Intelligent Agent Technology, IEEE/ACM/WIC, 2008.
8. Jozef Kapusta, Michal Munk, Martin Drlík, "Cut-off Time Calculation for User Session Identification by Reference Length" IEEE 2012.
9. Zhixiang Chen, Richard H. Fowler and Ada Wai-Chee Fu," Linear Time Algorithms for Finding Maximal Forward References", *Intl Conf On Info Tech: Coding and Computing (ITCC03)*, Proc. of the 2003 IEEE.
10. G. Arumugam, S. Sugana, "Optimum algorithm for generation of user session sequences using server side web user logs", IEEE, 2009.
11. Dr. Antony Selvadoss Thanamani, V.Chitraa, "A Novel Technique for Sessions Identification in Web Usage Mining Preprocessing", *International Journal of Computer Applications*, Volume 34– No.9, November 2011.

Global Journals Inc. (US) Guidelines Handbook 2017

www.GlobalJournals.org

Fellows

FELLOW OF ASSOCIATION OF RESEARCH SOCIETY IN COMPUTING (FARSC)

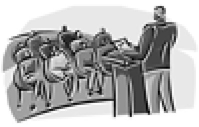
Global Journals Incorporate (USA) is accredited by Open Association of Research Society (OARS), U.S.A and in turn, awards “FARSC” title to individuals. The 'FARSC' title is accorded to a selected professional after the approval of the Editor-in-Chief/Editorial Board Members/Dean.

- 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%.



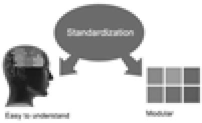
Once FARSC title is accorded, the Fellow is authorized to organize a symposium/seminar/conference on behalf of Global Journal Incorporation (USA).The Fellow can also participate in conference/seminar/symposium organized by another institution as representative of Global Journal. In both the cases, it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

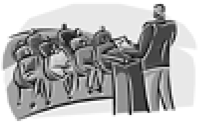
Global Journals Incorporation (USA) is accredited by Open Association of Research Society, U.S.A (OARS) and in turn, affiliates research institutions as "Institutional Fellow of Open Association of Research Society" (IFOARS).

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%.



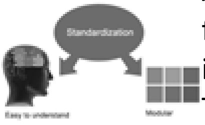
The Global Journals Incorporation (USA) at its discretion can also refer double blind peer reviewed paper at their end to the board for the verification and to get recommendation for final stage of acceptance of publication.

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.

THE ADMINISTRATION RULES

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