Proceeding
of
International Conference on Civil and Chemical Engineering - ICCCE 2014
&
International Conference on Advances in Computer and Electronics Technology - ACET 2014

Date: 16th November, 2014
Bangalore

Editor-in-Chief

Dr. D.J. Ravi
Professor & HOD, Department of ECE
Vidyavardhaka College of Engineering, Mysore

Organized by:

TECHNICAL RESEARCH ORGANISATION INDIA
Website: www.troindia.in
ISBN: 978-81-930280-1-8

About Conference

Technical Research Organisation India (TROINDIA) is pleased to organize the International Conference on Civil and Chemical Engineering - ICCCE 2014 & International Conference on Advances in Computer and Electronics Technology - ACET 2014

ACET is a comprehensive conference covering all the various topics of Engineering & Technology. The aim of the ACET 2014 is to gather scholars from all over the world to present advances in the aforementioned fields and to foster an environment conducive to exchanging ideas and information. This conference will also provide a golden opportunity to develop new collaborations and meet experts on the fundamentals, applications, and products of Computer science and Electronics. We believe inclusive and wide-ranging conferences such as ACET can have significant impacts by bringing together experts from the different and often separated fields of Electronics and Computer. creating unique opportunities for collaborations and shaping new ideas for experts and researchers. This conference provide an opportunity for delegates to exchange new ideas and application experiences, we also publish their research achievements.

ICCCE shall provide a plat form to present the strong methodological approach and application focus on civil engineering that will concentrate on various techniques and applications. The conference cover all new theoretical and experimental findings in the fields of Civil engineering or any closely related fields

Topics of interest for submission include, but are not limited to:

Computer Science & Engineering
Electronics Engineering
Telecommunication Engineering
Chemical Engineering
Engineering Science
Software Engineering
Architectural engineering
Transportation engineering
Civil Engineering Materials and Construction Practice
Geotechnical and Foundation Engineering
Water Resources Systems
Analysis and Design of Structures
Structural Engineering
Environmental Engineering
Infrastructure of Urban Development
Transportation Engineering
Analysis and Design of the Traffic Control System
Engineering Geology
Fundamental Specifications for Steel Construction
House Construction
Soil Mechanics
Transportation Geography and Network Science
Urban Traffic Operations
Vibrations of Structures
Water Resources Directory
Weatherization And many more....

Organizing Committee

Programme Chair

Dr. D.J. Ravi
Professor & HOD, Department of ECE
Vidyavardhaka College of Engineering, Mysore

Prof. Roshan Lal
PEC University of Technology/Civil Engineering Department,
Chandigarh, India
rlal_pec@yahoo.co.in

Programme Committee Members:

DR. BHASKER GUPTA
Assistant Professor. Jaypee University of Information Technology, Himachal Pradesh

Dr. A. Lakshmi Devi,
Professor, department of electrical engineering,
SVU college of Engineering, Sri Venkateswara university, Tirupati
Prof. SHRAVANI BADIGANCHALA

Assistant professor, Shiridi sai institute of science and engineering

Prof. Surjan Balwinder Singh
Associate Professor in the Electrical Engineering Department,
PEC University of Technology, Chandigarh.

Dr. Shilpa Jindal did her Ph.D and M.E. in Electronics and Communication Engineering from PEC University of Technology (Deemed University), Chandigarh
ji_shilpa@yahoo.co.in

IIT KHARAGPUR
Prof. Rajakumar R. V.
DEAN Acadedemic, rkumar @ ece.iitkgp.ernet.in
Prof. Datta D., ddatta @ ece.iitkgp.ernet.in
Prof. Pathak S S,r,ssp @ ece.iitkgp.ernet.in

XIMB,BHUBANESWAR
Prof Dr. Subhajyoti Ray.M-Stat, (ISI); Fellow, IIM(A),
Dean academic,XIMB-subhajyoti@ximb.ac.in ,
Prof.Andrew Dutta

Prof. Saveeta Mohanty

Dr. S. Peppin

Prof. Dipak Misra

Dr. W.S. William

Prof. Sunil agrawal

Prof(Dr.) P.Padhi:Principal KIST,Bhubaneswar

Prof(Dr.)B.D.Sahu,KIST,Bhubaneswar.

Prof(Dr.)B.Sarangi:Principal REC,Bhubaneswar

Prof(Dr.) S. Hota: Principal ,SIET,Dhenkanal

Prof(Dr.) A.Sarangi: Director, SIET,Dhenkanal

Prof(Dr.) Amiya Kumar Rath:Principal DRIEMS,Bhubaneswar

Prof(Dr.) N.C.Kundu,ITER

Prof(Dr.)P.R.Das,ITER

Prof(Dr.) K.C.Panda,ITER

Prof(Dr.)D.Pattanaik,Vice Principal GITA,Bhubaneswar.

Prof(Dr.) Kabi Sathpathy,CET,Bhubaneswar.

TABLE OF CONTENTS

SL NO **TOPIC** **PAGE NO**

Editor-in-Chief

Dr. D.J. Ravi

Editorial

The conference is designed to stimulate the young minds including Research Scholars, Academicians, and Practitioners to contribute their ideas, thoughts and nobility in these two integrated disciplines. Even a fraction of active participation deeply influences the magnanimity of this international event. I must acknowledge your response to this conference. I ought to convey that this conference is only a little step towards knowledge, network and relationship.

The conference is first of its kind and gets granted with lot of blessings. I wish all success to the paper presenters.

I congratulate the participants for getting selected at this conference. I extend heart full thanks to members of faculty from different institutions, research scholars, delegates, TROI Family members, members of the technical and organizing committee. Above all I note the salutation towards the almighty.

Editor-in-Chief

Dr. D.J. Ravi
Professor & HOD, Department of ECE
Vidyavardhaka College of Engineering, Mysore

EXPERIMENTAL STUDIES ON CONCRETE REPLACING FINE AGGREGATE WITH QUARRY DUST WASTES

[1]T.Sravani, [2]A.Anitha, [3]D.Shanthi Kumar
Assistant Professor, Department of Civil Engineering,
Annamacharya Institute of Technology and Sciences, Tiruapti, Andhra Pradesh, India
[1]sravani_tum@yahoo.com

Abstract
Concrete is the most undisputable and indispensable material being used in infrastructure development throughout the world. Many investigations were done to produce various varieties of concrete by reusing waste materials. Fine Aggregate (FA) plays a major role in making of concrete and the availability of fine aggregate is dwindling due to it's over explosion throughout the world. In this context an experimental studies was done based on Quarry Dust Wastes (QDW) for replacement of fine aggregate in concrete. Compressive strength tests were carried out with different proportions of replacements of FA with QDW. It was observed that on 75% substitution of FA with QDW the compressive strength of concrete was within permissible limit for use in construction industry.

Key words: - Pozzolana Portland Cement, Quarry Dust Waste, Concrete, Compressive strength.

I. Introduction

Explosion in population coupled with rapid industrialization and subsequent demand for infrastructure facilities has ushered a need to provide the necessary civil engineering structures. As the resources available for construction are limited, there is a need to go for some alternatives and use of industrial wastes appears to be an attractive option. Several waste materials such as spent fire bricks and recycled aggregate were used as replacements to concrete with varying compressive strength values

S. Keerthinarayana et.al.,[2] had studied the strength and durability properties by partial replacement of fine aggregate with crushed spent fire bricks and have reported an increase in the compressive strength with the partial replacement of CFBS. Malek Batayneh et.al.,[3] have successfully demonstrated the application of demolished concrete, glass and plastics as partial substitutes to concrete. J. Selwyn Babu et.al.,[9] had studied the physical and mechanical properties of concrete, replacing fine aggregate with GGBFS and BFS.

Quarry Dust Waste (QDW) has the same phycial characteristics of fine aggregate, as its size and properties are very to sand. In this investigation it is proposed to utilize Quarry Dust Waste (QDW) as replacement in the fine aggregate in different proportions.

II. Materials and Methods

A. Cement

In this present investigation Pozzolana Portland Cement (PPC) was used.

B. Fine Aggregate (FA)

The sand used for the experimental procedure was locally procured from a river and confirmed to Indian Standard Specifications [4]. It was passed through a 4.75 mm sieve, washed to remove any dust and then used as it was for further investigations.

C. Coarse Aggregate (CA)

Broken granite stones are generally used as a Coarse Aggregates (CA). The nature of work decides the maximum size of the CA. Locally available CA having the maximum size of 20 mm was used in our work. The aggregates were washed to remove any dust and were dried. The aggregates were tested as per Indian Standard Specifications [4].

D. Water

Water is an important ingredient of concrete s it actually participates in the chemical reaction with cement. Since it helps to form the strength giving cement gel, the quantity and quality of water required is to be looked into very carefully. In practice, very often great control on properties of cement and aggregate is exercised but the control on the quality of water is often neglected. So quality of water is checked to its purity.

E. Quarry Dust Wastes (QDW)

The QDW is the by product which is formed in the processing of the granite stones. QDW has the same physical characteristics to sand. It was made to pass through a 4.75 mm sieve [4], washed and used for further studies.

F. Methodology

Cement used for the study was tested for the parameters, Fineness, Consistency, Initial & Final Setting times and Specific Gravity [6]. Aggregates were tested for Fineness Modulus, Specific gravity, Water Absorption [5], Bulk density and Moisture content as per IS codes. Concrete was tested for Compressive strength under five cases as per M 25 mix design. In case-A, conventionally used Cement, Fine Aggregate, Coarse Aggregate and Water were mixed and analyzed for strength parameters. In case-B, fine aggregates was completely replaced by QDW and the other ingredients were the same as in case-A. In case-C, 50% fine aggregates and 50% QDW were used and the other ingredients were the same as in Case-A. In case-D, 75% fine aggregates and 25% QDW were used and the other ingredients were the same as in case-A. In case-E, 25% fine aggregates and 75% QDW were used and the other ingredients were the same as in case-A.

III. Mix design

As per the code IS: 10262 –1979 [8], the mix design is found and the amount of materials is calculated. According to the mix ratio, the amount of materials is given below, in Table I.

TABLE I. MIX PROPORTION

Water	Cement	Fine Aggregate	Coarse Aggregate
150	300	200	265
0.5	1	1.77	2.88

IV. Results and Discussion

The various results of tests done for cement are presented in Table II. All the parameters were observed to be within the permissible limits, though the initial setting time was found to be at a slightly upper level.

TABLE II. RESULTS OF TESTS DONE ON CEMENT

Type of tests	Results
Fineness	0.9%
Consistency	30.5%
Initial Setting Time	30 min
Final Setting Time	350 min
Specific Gravity	2.64

The results of tests done on aggregates are presented in Table III, and all the parameters were within the permissible limits.

TABLE III. RESULTS OF TESTS DONE ON AGGREGATES

Type of Tests	CA	FA	QDW

Specific Gravity (%)	2.72	2.65	2.56
Water Absorption (%)	0.5	1.0	.5
Bulk Density (kg/m^3)	1469.8	1460	1765
Fineness Modulus (%)	4.51	3.54	3.81
Moisture content (%)	1.90	1.50	Nil

The results of Compressive strength test on four cases are presented in Table IV**.** It was observed that concrete of all the five cases exhibited good compressive strength.

TABLE IV. RESULTS OF COMPRESSIVE STRENGTH ON CONCRETE

Type of Concrete	**Compressive strength of cubes, MPa**	
	7 days	**28 days**
Case-A	28.50	36.05
Case-B	27.32	37.98
Case-C	24.16	33.80
Case-D	26.81	26.04
Case-E	22.52	34.10

A graphical comparison of 7 day compressive strengths of all the five cases of mix designs is presented in figure 1. It can be observed that case-B exhibited a compressive strength of 27.32 MPa, which is close to the conventionally used case-A mix design. This is far better than the replacement of fine aggregate with 15% Ground Granulated Blast Furnace Slag which gave a 7 day compressive strength of 22.82 MPa [9]. Case-E obtained a compressive strength of 22.52 MPa which is similar to 10% replacement of Quarry dust [10] for 7days.

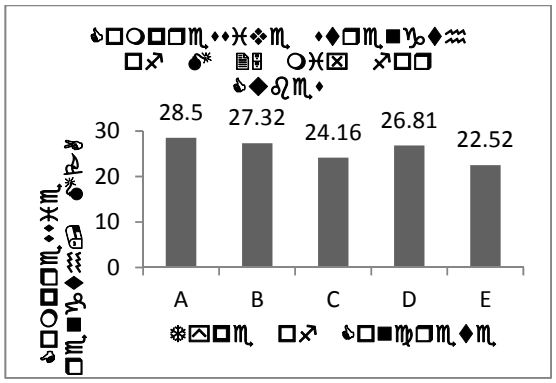

Figure 1. Compressive strength of 7 days for cube

Figure 2. depicts the 28 day compressive strengths of five cases of mix designs. In case-B which was replaced by QDW the 28 day compressive strength was observed to be 37.98 MPa which is quite a satisfactory value. This is very close to the replacement of fine aggregate with 20% Blast Furnace Slag which gave a 28 day compressive strength of 36.47 MPa [9]. Case-E obtained a compressive strength of 34.10 MPa for 28 days which is similar to 10% replacement of Quarry dust [10] for 27 days.

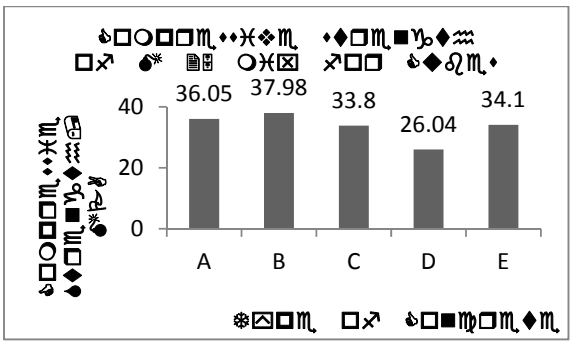

Figure 2. Compressive strength of 28 days for cube

V. Conclusion

The following conclusions were drawn from the experimental investigation.

1. A maximum compressive strength of 37.98 MPa was obtained with 100% replacement of QDW for 28 days.

2. It was observed that 100% replacement of QDW gave a satisfactory result when compared with conventional concrete for 7 days.

3. From this test, replacement of fine aggregate with QDW gave a compressive strength of 50% and 75% replacement respectively.

4. Partial replacement of FA with QDW showed encouraging results in terms of compressive strength.

5. Environmental wastes which pose a difficult problem in its disposal can be efficiently addressed through the results of this research.

VI. Reference

[1]D Brindha and S Nagan, "Durability studies Copper Slag admixed Concrete", *Asian Journal of Civil Engineering (Building and Housing)*, Vol. 12 (5), pp. 563 – 578, 2011.

[2] S. Keerthinarayana and R. Srinivasan, "Study on strength and durability of concrete by Partial replacement of fine aggregate using Crushed spent fire bricks", , pp. 52-63

[3] Malek Batayneh, Iqbal Marie, Ibrahim Asi, "Use of selected waste materials in concrete mixes", *Waste Management*, Volume 27, Issue 12, 2007, pp. 1870–1876

[4] "Specification for coarse and fine aggregates from natural sources for concrete", *Bureau of Indian Standards*, New Delhi, IS: 383-1970.

[5]"Methods of test for Aggregates for concrete, Part-III specific gravity, density, voids, absorption and bulking", *Bureau of Indian Standards*, New Delhi, IS: 2386(P-III)-1963.

[6]"Ordinary Portland Cement, 53 grade-specification", *Bureau of Indian Standards*, New Delhi, IS: 12269-1987.

[7]"Code of Practice for Plain and Reinforced Concrete", *Bureau of Indian Standards*, New Delhi, IS 456-2000.

[8]"IS Method of mix design", *Bureau of Indian Standards*, New Delhi, IS: 10262-1981.

[9] J.Selwyn Babu, Dr. N. Mahendran, "Experimental Studies on Concrete Replacing Fine Aggregate with Blast Furnace Slags", *International Journal of Engineering Trends and Technology (IJETT*, Volume 10, Number 8 - Apr 2014.

[10] Chandana Sukesh, Katakam Bala Krishna, P.Sri Lakshmi Sai Teja, S.Knakambara Rao, "Partial replacement of sand with Quarry dust in concrete", *International journal of Innovative Technology and Exploring Engineering*, Volume 2, Issue 6, May 2013, pp. 254-258.

IMPORTANCE OF ROADSIDE VEGETATION

[1]Dr. R.R. Singh, [2]Er. Nitin Goyal, [3]Er. Navpreet Kaur

[1]Associate professor (CED),PEC University of Technology,Chandigarh, INDIA
[2,3]Research scholar (CED),PEC University of Technology,Chandigarh, INDIA.
Email: [1]nitingoyal121@gmail.com, [2]navpreetkaurpec@gmail.com,

ABSTRACT

Roads are the integral part of transportation system. It plays a significant role in achieving national development and with the help of road side vegetation and by selecting right species of plant at right area we can reduce the maintenance needs and cost of road, provides safety for vehicles, improves the overall driving experience of roads, reduce soil erosion.

Enhance the drainage aspect of roads as vegetation increase the water infiltration capacity of soil, improves the shear strength of embankments by controlling the moisture content and increase the life of shoulder. Beside all these factors vegetation also cover the environmental aspect such as control noise pollution, air pollution and maintains the ecological balance and aesthetic view.

1. INTRODUCTION

As with growing time government of every country wants the best & economic technique should be adopted in each part of the country & an attempt is made by the engineers to find the alternatives of each technique. The Roadside vegetation or bio engineering is a technique through which the life of road can be increased by controlling the moisture content of soil, by improving shear strength of soil, by improving infiltration capacity of soil & by controlling soil erosion. Through this technique we can also reduce the cost of construction, maintenance cost of roads.

The road side vegetation technique or bio engineering technique requires assessment of existing road condition determination of type of roadside environment desired according to increased public demand and customer expectations. There are various factors on which vegetation techniques depend:

Soil conditions; Traffic Composition; Location of road; Topography; Adjacent Land Use; The Priority of Road; Aesthetic appearance

It is a rapidly growing field subject to innovations & changing design specifications. Due to increased environmental awareness this technique is beneficial than traditional approaches.

2. BENEFITS OF VEGETATION

2.1 ECONOMIC ASPECTS

- Improved Road side conditions enhance the visitor visit.
- Reduce cost of construction activities due to less requirement of improved technology.
- Also improves life of pavement. (This technique can be used in soil stabilization situations)
- It also reduces maintenance cost and needs.
- It improves water infiltration capacity of soil & reduces run off.
- The roots, stems & associated woods that we obtained from cutting are used to build the structures.
- Traditional method of controlling stream flow & wave induced erosion on embankment have relied on structural practice like retaining wall & sheet piles which are expensive, ineffective whereas Bio engineering technique as one of best economic alternative approach.

2.2 ENVIRONMENTAL ASPECTS

- It improves air quality by absorbing carbon monoxide, and carbon dioxide.
- It also stabilizes the ground surface to prevent soil erosion as with time the strength of root system increases which increase the soil stability and the soil is less prone to soil erosion.
- Provides habitats for wildlife.
- Control weeds on roadside conditions.
- Increased biodiversity (variation of species)

2.3 SAFETY ASPECTS

- Vegetation proves an effective tool for slope protection in road projects.
- It minimizes effect of rain, snow and ice formation.
- It also minimizes hazardous conditions for maintenance staff.
- It reduces the slippery on the roads and provides safety for vehicles.

3. BENEFITS OF VEGETATION ON EMBANKMENTS

In Embankment design slope stability is the major consideration or element on which design of embankments depends and there is complex relationship between vegetation and slope stability. Vegetation enhance slope stability in following ways:-

By Removing water from soil

(i) Due to shading of trees, the soil becomes dry which increases the infiltration capacity of the soil and allows deep penetration of the rain water.

(ii)Due to capillary action of plants the r is drawn up from the roots or soil to the leaves which is then removed through process of transpiration it also by controlling moisture content of soil.

Mechanical Reinforcement

i. Roots increase the shear strength of the soil by binding the particles along the potential failure plant.

ii. Due to root elongation across slip plane there is development of root tensile force which is transferred to soil.

4. EFFECT OF VEGETATION ON SHOULDER

A shoulder is a portion of roadway that is continuous with the travelled way and is provided for lateral support of base and surface course. Due to lack of funds most common types of shoulder prevail in India are earthen shoulders that are compacted in different layers. Due to earthen shoulders maintenance requirement is an essential component and vegetation plays a vital role in maintaining shoulders during rainy season as it prevent the rain cuts, reduce slipperiness of the shoulder. Improves the water Infiltration capacity of the shoulder and also avoid soil erosion during rainy season by firmly biding the soil particles. Vegetation is also the one of way of keeping the earthen shoulder in proper shape of profile. With the help of vegetation dust nuisance is also minimized and load carrying capacity of shoulder is also increased.

5. IMPORTANCE OF VEGETATION ON HILL ROADS

As hill ranges are very young due to which a minor disturbances can cause slips, subsidence and Land-slides. Landslides are basic problem on all hill roads. There are many factors which contribute the land slide whereas deforestation, grazing of animals is also a major contributing factor. As trees or vegetation on roadside not only increase shear strength along the failure plane but also improves the load carrying capacity of soil along the failure plane, provides lateral support by preventing soil erosion. As a preventive measure to avoid landslides afforestation & fencing should be done so that grazing of animals should be stopped.

6. AESTHETIC ASPECT OF VEGETATION

- Roadside vegetation protects from unsightly views such as slums, Junk Yards, Storage depots etc.
- Trees provide shade, colour if they are of flowering variety and also yields fruits.

7. ENVIRONMENTAL ASPECT OF VEGETATION

Noise Pollution: Noise is an unwanted sound on the road &it is mainly caused by breaks, horn, and engine of vehicles. So for highway engineering it is also a better opportunity to control noise pollution by just planting the trees and shrubs on the roadside.

Air Pollution: As lot of poisonous fumes and smell are caused by the engines of vehicles which are hazardous to environment and driver. All types of pollutant like lead particles, oxides of nitrogen, Carbon monoxide, Oxides of nitrogen can be easily controlled by the roadside vegetation.

8. LIMITATIONS OF VEGETATION

- Vegetation doesn't stabilize instable slopes as due to higher planting difficulties and a higher erosion hazard produce by greater runoff velocity.

- Improper drainage and poor consolidation of roads are less stabilized by vegetation.
- The availability of easily adapted plants may be limited.
- Labour needs are intensive & skilled experience labour may not be available. So pre-requisite training is required.
- The planting season of plant or vegetation may be limited.
- If trees are planted at top of slope extra 10% factor of safety should be required as tree of 30-50m height generally applies loading of 150km/m^2.

9. SPECIES SELECTION

It should be beneficial to select native species instead of non-native species as these can easily compete with the prevailing climatic conditions and one should try to select those species of vegetation that can roughly match with the environmental conditions of road and special attention should be given in following cases:-

- Select those species with that are comfortable with soil movement at project sites.
- The deep and widespread root system should be adopted where deep earth movements are there. E.g.: Popular, Eucalypts Acacia.
- Special attention should be given in shady regions as most of plants material will grow poorly and their life is also short.

10. CONCLUSION

Although roadside vegetation has certain limitations like limited plantation season of trees but keeping in view all the above benefits of roadside vegetation, considering its economic, environmental, safety aspect etc. ; it should be given due importance.

Since, roadside vegetation has varied benefits on hilly roads, embankments, to improve soil strength, improving infiltration capacity of soil, reduction in soil erosion. So considering the benefits of roadside vegetation, this paper has been attempted to promote roadside vegetation as an important aspect in Highway Engineering.

REFERENCES:

1. Pandey DK & Rao Nilanjana, "Bio-Engineering Techniques for slope protection in road projects", Journal of Indian Highways, April 2004.
2. Kadyali LR & Lal N.B., "Principle and practice of highway engineering, sixth edition, 2013".
3. **http://en.wikipedia.org/wiki/Vegetation_and_slope_stability**
4. **http://www.lrrb.org/media/reports/200820.pdf**

AN INVESTIGATION OF STRENGTH CHARACTERISTICS OF CONCRETE CONTAINING RECYCLED AGGREGATES OF MARBLE AND GRANITE WASTE.

Prof. Roshan Lal[1],Er. Kuldeep Kumar[2]
[1] PEC University of Technology/Civil Engineering Department, Chandigarh, India
[2] CCET Chandigarh/Civil Engineering Department, Chandigarh, India
Email: rlal_pec@yahoo.co.in[1],kkdipcivil2007@gmail.com[2]

***Abstract*— The results obtained from the present investigation on strength characteristics of concrete containing natural aggregates and natural aggregates with partial replacement by marble and granite waste aggregates in different percentages have been presented. In the series of test conducted when natural aggregates were replaced by marble waste and granite waste aggregates used in equal proportions with replacement of natural aggregates by 20% (10% marble +10% granite) , 30% (15% marble +15% granite),40% (20% marble +20% granite) were cast. The compressive strength of specimens were tested for mixes containing marble and granite waste as recycled aggregates increased for replacement 20% and 30%. However for the 40% replacement of marble and granite waste aggregate with natural aggregate a marginal decrease in compressive strength is recorded. Therefore it can be concluded that the production of concrete of normal strength is feasible and viable by replacing the natural aggregates by the waste marble and granite aggregates without compromising the strength characteristics.**

***Index Terms*—Specific Gravity, water Absorption , Fineness Modulus and Compressive Strength.**

I. INTRODUCTION

Recycling is the act of processing the used material for use in creating new product. Stone waste i.e. Marble and Granite waste has been commonly used as building materials. Today industry's disposal of stone waste is one of the environmental problems around the world .Stones are cut into smaller blocks in order to give them the desired shape and size. During the process of cutting, the original stone mass is lost by 30%. The waste is dumped in nearby pits and vacant spaces. This leads to serious environmental pollution an occupation of vast area of land. So it poses a severe threat on the environment, eco-system and the health of the people. The Quarrying and Trimming waste also poses a serious environmental damages.

So it is necessary to use this stone waste in construction industry. Recycled aggregate of Marble and Granite waste are comprised of crushed, graded inorganic particles processed from the materials that have been considered as a waste material. In the present study an effort has been made to explore the possibility of using these materials as part replacement of natural aggregates for making concrete.

Terzi and Karasahin (2003) investigated the use of marble dust in asphalt mixtures as a filler material for optimum filler/bitumen and filler ratio. They have concluded that marble wastes in the dust form could be used in such cases.

Abkulut and Cahit (2007) studied the use of marble quarry waste in asphalt pavements with bitumen. They reported that waste materials can potentially be used as aggregates in light to medium trafficked asphalt pavement binder

layers.

Binici etal. (2008) studied durability of concrete containing granite and marble as coarse aggregates. The result indicated that marble, granite and ground blast furnace slag replacement provide a good durable concrete.

Wattanasiriwech et al. (2009) investigated the use of waste mud from ceramic tile production in paving blocks and determined compressive strengths of these blocks. They observed that the blocks containing cement 20 weight% gave satisfactory strength values.

Pereira et al. (2009) performed an experimental study using a number of coarse aggregates from different geological sources including granite, basalt, limestone and marble. They produced concretes in specific mix proportions and laboratory controlled conditions. They explored that concrete durability properties were not affected by aggregates mineralogy, but in turn were significantly affected by the aggregate size and its water content.

Padmini et al. (2009) investigated the properties of recycled aggregates from parent concrete (PC) of three strengths, each of them made with three maximum sizes of aggregates. They produced recycled aggregate concrete (RAC) using these recycled aggregates. They found that RAC required relatively lower water-cement ratio as compared to PC to achieve a particular compressive strength. They also determined that the difference in strength between PC and RAC increased with strength of concrete.

Martínez-Barrera and Brostow (2010) studied effects of gamma irradiation and the marble particle size on compressive properties and the dynamic elastic modulus of polymer concretes. One of the conclusions was that both compressive properties and the dynamic elastic modulus values depend on the combination of the marble particle sizes and the applied radiation dose. Higher numbers of dispersed particles per unit volume provide more resistance to crack propagation. Medium size marble particles provide better compression modulus.

II EXPERIMENTAL PROGRAMME

The test programme consisted of the testing of the constituent materials i.e. cement, fine aggregate, coarse aggregate as per relevant Indian Standard Codes of Practice and testing of specimens containing Natural aggregates and with recycled aggregates of marble for compression and split tensile strength. The physical properties of cement used in the present study are given in Table 1.The physical properties of fine and coarse natural and granite aggregates used in investigation are presented in Tables 2, 3, 4 and 5.

Table 1: Physical Properties of Cement

Sr. No.	Property	Experimental value
1	Consistency of Cement	30%
2	Specific Gravity	3.14
3	Initial Setting Time	92 minutes
4	Final Setting Time	298 minutes
5	Comp. Strength i) (N/mm^2) ii) 3 days iii) 7days 28 days	 24.67 35.04 47.28
6	Fineness (Dry Sieving)	2.5 %

Table 2: Physical Properties of Fine Aggregates

Characteristics	Results Obtained
Grading	Grading Zone II (IS: 383-1970)
Fineness Modulus	2.55
Specific Gravity	2.62
Water Absorption (%)	0.48%
Free Moisture Content (%)	Nil

Table 3: Physical Properties of Coarse Natural Aggregates

Characteristics	Results Obtained
Fineness Modulus	6.6
Specific Gravity	2.66
Water Absorption (%)	0.50%
Moisture Content (%)	Nil

Table 4: Physical Properties of Coarse Marble Aggregates

Characteristics	Results Obtained
Fineness Modulus	6.51
Specific Gravity	2.68
Water Absorption (%)	0.32
Moisture Content (%)	Nil

Table 5: Physical Properties of Coarse Granite Aggregates

Characteristics	Results Obtained
Fineness Modulus	6.51
Specific Gravity	2.70
Water Absorption (%)	0.49
Moisture Content (%)	Nil

Sieve analysis of fine aggregates, coarse natural, marble and granite waste aggregates is carried out and the results are presented in Tables 6, 7, 8 and 9. The details of mixes with and without marble and granite waste aggregates are given in Table 10.

Table 6: Sieve Analysis of Fine Aggregates

IS Sieve Designation	Wt. Retained on Sieve (gm)	Cumulative Weight Retained (gm)	Cumulative Percentage Weight Retained (gm)	%age Passing
10mm	0.00	0.00	0.00	100.00
4.75 mm	15.10	15.1	1.51	98.49
2.36 mm	25.20	40.30	4.03	95.97
1.18 mm	250.10	290.40	29.04	70.96
600 µ	160.00	450.40	45.04	54.96
300 µ	320.10	770.50	77.05	22.95
150 µ	217.10	987.60	98.76	1.24
Pan	12.40	1000	-	-

Table 7: Fineness Modulus of Proportioned Coarse Aggregates

I S Sieve Designation	Wt. Retained on Sieve (10 mm Agg) (gm)	Wt. Retained on Sieve (20mm Agg) (gm)	Average Weight Retained (gm)	Cumulative Wt. Retained (gm)	Cumulative %age Wt Retained (gm)	%age Passing
80mm	0.00	0.00	0.00	0.00	0.00	100.00
40 mm	0.00	0.00	0.00	0.00	0.00	100.00
20 mm	0.00	335	167.5	167.5	3.35	96.65

10 mm	1225	4565	2895	3062.5	61.25	38.75
4.75 mm	3625	90	1857.5	4920	98.40	1.6
Pan	-	-	-	-	-	-

Table 8: Fineness Modulus of Proportioned Coarse Marble Aggregates

I S Sieve Designation	Wt. Retained on Sieve (10mm Agg) (gm)	Wt. Retained on Sieve (20mm Agg) (gm)	Average Weight Retained (gm)	Cumulative Wt. Retained (gm)	Cumulative %age Wt Retained (gm)	%age Passing
80mm	0.00	0.00	0.00	0.00	0.00	100.00
40 mm	0.00	0.00	0.00	0.00	0.00	100.00
20 mm	0.00	275	137.5	137.5	2.75	97.25
10 mm	170	4570	2370	2507.5	50.15	49.85
4.75 mm	4715	145	2430	4937.5	98.75	1.25
Pan	-	-	-	-	-	-

Table 9: Fineness Modulus of Proportioned Coarse Granite Aggregates

I S Sieve Designation	Wt. Retained on Sieve (10mm Agg) (gm)	Wt. Retained on Sieve (20mm Agg) (gm)	Average Weight Retained (gm)	Cumulative Wt. Retained (gm)	Cumulative %age Wt Retained (gm)	%age Passing
80 mm	0.00	0.00	0.00	0.00	0.00	100.00
40 mm	0.00	0.00	0.00	0.00	0.00	100.00
20 mm	0.00	225	112.5	112.5	2.25	97.75
10 mm	2432.5	4190	3311.25	3423.75	68.47	31.53
4.75 mm	1916.75	505	1210.87	4634.62	92.69	7.31
Pan	-	-	-	-	-	-

Cumulative percentage wt. retained = 163.41 + 500

= 663.41

Fineness Modulus (F.M.) = 663.41/100=6.63

Table 10: Detailed Mix Proportions for Natural and Recycled Aggregates of Marble and Granite

Mix Design-gnation	Cement (kg/m3)	Fine aggregates (kg/m3)	Natural Coarse Aggregates (kg/m3)	Marble Coarse Aggregates (kg/m3)	Granite Coarse Aggregates (kg/m3)	Water (kg/m3)	w/c ratio
M	3	64	115	---		19	0.48
M2	399	643	926.0	115.76	115.76	191.5	0.48

M 3	3 9 9	64 3	810. 3	173. 64	173. 64	19 1. 5	0.48
M 4	3 9 9	64 3	694. 5	231. 52	231. 52	19 1. 5	0.48

From the tables the fineness modulus of fine aggregates, coarse natural aggregates, marble and granite waste aggregates are 2.55, 6.6, 6.51 and 6.63.

III RESULTS AND DISCUSSION

COMPRESSIVE STRENGTH

To study the effect of replacement of natural aggregates by marble waste and granite waste aggregates used in equal proportions, cubical specimens with replacement of natural aggregates by 20% (10% marble +10% granite) , 30% (15% marble +15% granite),40% (20% marble +20% granite) were cast and tested. The results obtained for the specimen tested for compressive strength at 7 days and 28 days are reported in Table 11 and 12 respectively. The comparison of compressive strength at 7 days and 28 days for specimens with natural aggregates and the specimens containing marble and granite waste aggregates in different percentages is shown in Figure 1 and 2.

Table 11: Test Results of Compressive Strength of Specimens at 7 Days

Mix Design ation	%age Replac ement	Loa d (kN)	Compr essive Strengt	Averag e Compr
M1	0	473. 70	21.05 26.19	22.87
M2	20	589. 27	26.19 25.90	25.95
M3	30	558. 00	24.80 24.33	25.22
M4	40	515. 70	22.92 24.65	24.39

Table 12: Test Results of Compressive Strength of Specimens at 28 Days

Mix Design ation	%ag e Repl	Load (kN)	Compr essive Strengt	Averag e Compr
M1	0	670.5 0	29.78 28.47	29.53
M2	20	771.7 5	34.30 27.56	32.12
M3	30	745.6 5	33.14 31.52	31.15
M4	40	657.6 7	29.23 29.38	29.20

It can be seen from Tables 11, 12 and Figures 1, 2 that the compressive strength of mix M2 at 7 days and 28 days increased with replacement of natural aggregates by marble and granite waste aggregates by 20% when compared to the control mix M1. For M3 30% replacement of natural aggregates by marble and granite waste aggregates further increase in compressive strength was recorded as compared to control mix M1. For the mix M4 containing 40% replacement of natural aggregates by marble waste aggregates the decrease in compressive strength is recorded. The increase in compressive strength of concrete with replacement of natural aggregate by marble and granite waste aggregates can be attributed to improved microstructure of concrete containing marble and granite waste aggregates which may be due to higher specific surface area of marble and granite aggregates and thus improving bond in between mortar and aggregates. The decrease in percentage improvement in compressive strength at higher replacement levels may be attributed to the grading effect. Figure 3 represents the typical mode of failure of cubical specimens.

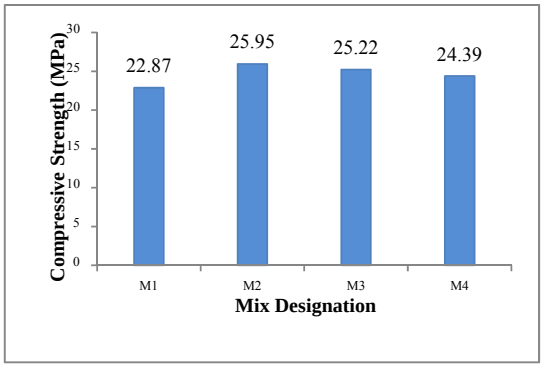

Fig. 1: Comparison of Compressive Strength of Specimens at 7 Days

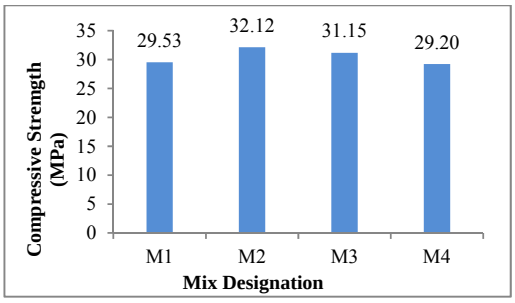

Fig. 2: Comparison of Compressive Strength of Specimens at 28 Days

Fig.3:Typical Mode of Failure for Cubical Specimens.

SPLIT TENSILE STRENGTH

To study the effect of replacement of natural aggregates by marble waste and granite waste aggregates used in equal proportions, cylindrical specimens (Series-2) with replacement of natural aggregates by 20% (10% marble+10%granite),30%(15%marble +15% granite),40% (20% marble +20% granite) were caste and tested. The results obtained for the specimen at 7 days and at 28 days are reported in Table 13 and 14.

Table 13: Test Results of Split Tensile Strength of Specimens at 7 Days

Mix Designation	%age Replacement	Split Tensile Strength (Tonnes)	Split Tensile Strength (N/mm^2)	Average strength (N/mm^2)
M1	0	14 14	1.98 1.98	2.07
M2	20	16 16	2.26 2.26	2.21
M3	30	16 14 16	2.26 1.98 2.26	2.17
M4	40	14 14	1.98 1.98	1.98

Table 14: Test Results of Split Tensile Strength of Specimens at 28 Days

Mix Designation	Split Tensile Strength (Tonnes)	Split Tensile Strength (N/mm^2)	Average strength (N/mm^2)
M1	20 22	2.83 3.11	2.92
M2	24 24	3.39 3.39	3.29
M3	24 20	3.39 2.83	3.10
M4	20 20	2.83 2.83	2.73

The comparison of compressive strength at 7 days and 28 days for specimens with natural aggregates and the specimens containing marble and granite waste aggregates in different percentages is shown in Figures 4 and 5.

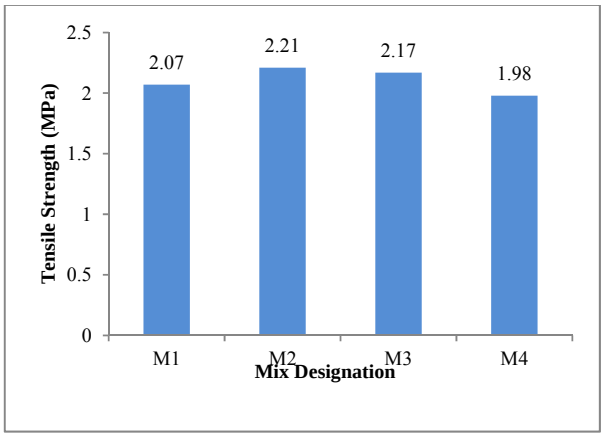

Fig. 4: Comparison of Split -Tensile Strength of Specimens at 7 Day

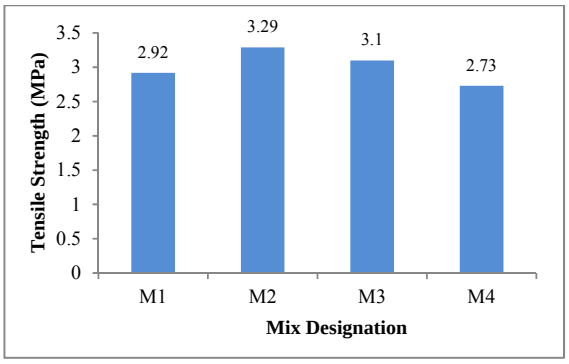

Fig. 5: Comparison of Split -Tensile Strength of Specimens at 28 Days

It can be seen from above Tables 13 and 14 and Figures 4 and 5 that in line with the results obtained for compressive strength for both the series, the similar trends were obtained for split tensile strength also which correlate the beneficiary effect of replacing natural aggregates by marble waste and granite waste aggregates mixed in equal proportions.

FLEXURAL STRENGTH

To study the effect of replacement of natural aggregates by marble waste and granite waste aggregates used in equal proportions, beam specimens with replacement of natural aggregates by 20% (10% marble +10% granite), 30% (15% marble +15% granite),40% (20% marble +20% granite) were cast and tested. The results obtained for the specimen are reported in Tables 15 and 16.

Table 15: Test Result of Flexural Strength of Specimens at 7 days

Mix Designation	%age Replacement	Flexural Strength (Tonnes)	Flexural Strength (N/mm^2)	Average strength (N/mm^2)
M1	-	1.0 1.2	2.02 2.43	2.29
M2	2	1.4 1.3	2.83 2.63	2.76
M3	3	1.4 1.4	2.83 2.63	2.69
M4	4	1.2 1.2	2.43 2.43	2.49

Table 16: Test Result of Flexural Strength of Specimens at 28 days

Mix Designation	%age Replacement	Flexural Strength (Tonnes)	Flexural Strength (N/mm^2)	Average strength (N/mm^2)
M1	-	1.8 1.9	3.64 3.84	3.70
M2	2	2.1 2.1	4.25 4.25	4.18
M3	3	1.8 2.0	3.64 4.05	3.98
M4	4	1.8 1.8	3.64 3.64	3.64

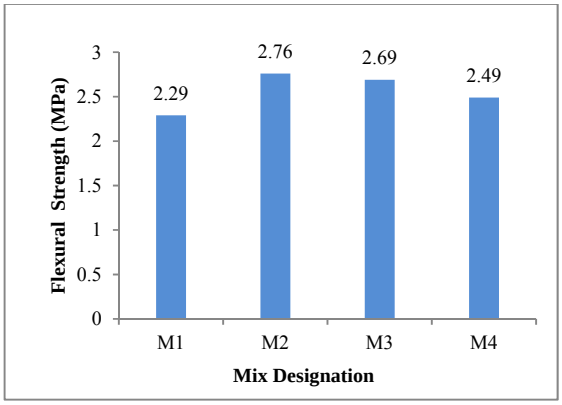

Fig. 6: Comparison of Flexural Strength of Specimens at 7 Days

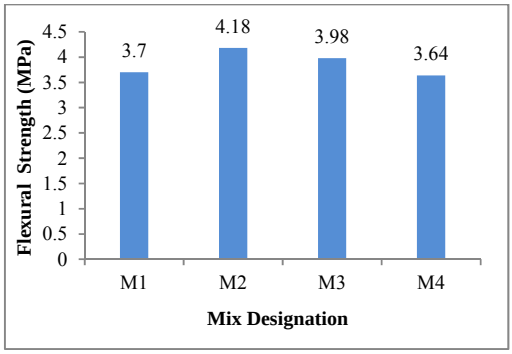

Fig. 7: Comparison of Flexural Strength of Specimens at 28 Days

It can be seen from above Tables 17 and 18 and Figures 6 and 7 that in line with the results obtained for compressive strength for both the series, the similar trends were obtained for flexural strength also which correlate the

beneficiary effect of replacing natural aggregates by marble waste and granite waste aggregates mixed in equal proportions.

CONCLUSIONS

1. The compressive strength, split-tensile strength and flexural strength of specimens tested in mixes containing marble and granite waste as recycled aggregates increased for replacement of 20% and 30%. However for the 40% replacement of marble and granite waste aggregates with natural aggregates marginal decrease in compressive strength is recorded. For mix containing 20% and 30% waste marble aggregates the compressive strength at 28 days was increased by 8.7 % and 5.5% when compared to the control mix.
2. The split tensile strength of specimens tested for mixes containing marble and granite waste as recycled aggregates increased for replacement of 20% and 30%. However for the 40% replacement of marble and granite waste aggregate with natural aggregate a marginal decrease in compressive strength is recorded. For mix containing 20% and 30% waste marble aggregates the split tensile strength is increased by 12.0% and 6% when compared to the control mix.
3. The flexural strength of specimens tested for mixes containing marble and granite waste as recycled aggregates increased for replacement of 20% and 30%. However for the 40% replacement of marble and granite waste aggregate with natural aggregate a marginal decrease in compressive strength is recorded. For mix containing 20% and 30% waste marble aggregates the flexural strength is increased by 12.9% and 7.5% when compared to the control mix.

REFERENCES

[1] Akbulut, H., Cahit, G,(2007) "Use of aggregates produced from marble quarry waste in asphalt pavements. Building and Environment",42, 1921-1930.

[2] Binici, H. etal. (2008), "Durability of concrete made with granite and marble as recycle aggregates" ,Journal of Materials Processing Technology 208, 299-308.

[3] IS 10262:2009 Recommended Guidelines for concrete mix design, Bureau of Indian Standards, New Delhi.

[1] IS 456:2000 "Indian Standards Code of Practice for plain and reinforced concrete" (4th revision), Bureau of Indian Standards, New Delhi.

[2] IS 8112-1989. "Specifications for coarse and fine aggregates from natural sources" Bureau of Indian Standards, New Delhi,1997.

[3] IS 8112-1989. "Specifications for Ordinary Portland Cement 43 grade" Bureau of Indian Standards, New Delhi,1989.

[4] Martínez-Barrera, G., Brostow, W.(2011), " Effect of marble particle size and gamma irradiation on mechanical properties of polymer concrete"(2011), E-Polymers 61, 1-14.

[5] Pereira etal. (2009)," Influence of natural coarse aggregate size, mineralogy and water content on the permeability of structural concrete. Constr. Build. Mater"(2009). 23: 602-608.

[6] Padmini,AK,etal.(2009),"Influence of parent concrete on the properties of recycled aggregate concrete. Constr. Build. Mater", 23: 829-836.

[7] Terzi, S.(2009), " Use of marble dust in the hot mix asphalt as a filler material." Technical Journal of Turkish Chamber of Civil Engineers 14 (2),2903-2922. in Turkish.

[8] Wattanasiriwech,D.etal.(2009),"Paving blocks from ceramic tileproductionwaste".JournalofCleanerProduction17,1663-1668.

DESIGN, FABRICATION, DEVELOPMENT AND CONSTRUCTION OF LOW COST LAVATORY

[1]Mr. R. Haresh, [2]Mr. N. Shiva Chary, [3]Dr. G. V. Praveen
[1,2]B.Tech. (Civil) Final Year Student, Department of Civil Engineering
S. R. Engineering College, Warangal..
[3]Professor and Head,Department of Civil Engineering
S. R. Engineering College, Warangal.

***Abstract*— It is evident that, in India, approximately 30% rural people live below the poverty line. In this context, assuring basic hygiene for one and all is a major task. Further, poor sanitation affects the health of the people and also the development of the nation. Also, it is observed that, in India, rural community lives housing without toilets due to their poverty. In this paper, an attempt is made to show the solution for sanitation of rural people by providing them with a low–cost lavatory, developed in such a way that, it can be affordable by a common man. The main aim of this work is to promote better human health and improve quality of life among people living in rural areas through improved sanitation measures.**

***Keywords*-Rural India; Sanitation; Low–Cost Lavatory.**

I. Introduction

In India, 80% of the population resides in 6, 00, 000 villages spread across the country. In rural areas, people live in adverse conditions of sanitation without having adequate facilities for defecation, due to their poverty and ignorance. People require safe and hygienic facilities for excretion . In this connection, it is important to consider several technological aspects such as affordability, space, cultural habits, availability of water and labour for construction etc., to maintain sanitation for rural people. The present paper deals with design, fabrication development and construction of Low-Cost Lavatory for Rural India.

II. Need of the Study

In India, many villagers go barefoot for open air defecation due to which ailments such as dysentery, diarrhea and cholera spread over.

Despite several programs have been taken up by government on sanitation, adverse effects of insanitation and its impact on human health, rural people are still neglecting safe mode of defecation system. Generally, rural people prefer low–cost, location specific and acceptable design and technologies depending on their socio–economic status. Hence, there is a dire necessity to have a lavatory system which is cost effective.

III. Fabrication and construction of Low Cost Lavatory

For the construction of a model design of Low–Cost lavatory, the site nearby workshop area of S. R. Engineering College, Warangal was chosen. The site is cleared from debris and leveled. A soak pit (5’ depth and 3.5’ diameter) was excavated and cement rings were dropped slowly into the pit with the help of rope to stop collapse sides of pit (Fig. 2).

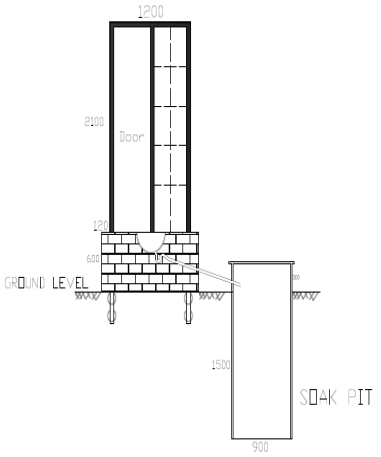

Fig. 1. Front view of Low–Cost Lavatory.

For the construction of lavatory, the prefabricated steel cage was used. The legs of the cage were driven into the pits (2' depth and 4' apart) and concrete was poured into pits for firm gripping of the legs. A basement with cement bricks is constructed and the set up for Indian water closet was arranged. This arrangement is connected to soak pit to facilitate the passage of digested waste (Fig. 1 and 2).

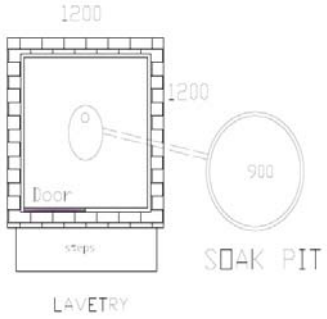

Fig. 2. Top view of Low–Cost Lavatory.

Plate 1. Students at work

The cage was enclosed with the Fiber Reinforced Plastic (FRP) sheets for privacy. This sheet is fixed to steel anglers with nut and bolt system to get the final shape of the lavatory (Plate 1). The surrounding ground is leveled for accessibility.

IV. Salient features of Low-cost Lavatory

- Less time of construction.
- Superstructure is made from steel giving rise to high strength.
- Low cost of the construction **(less than INR 10,000)** (Table 1).
- Suitable for local festival places/people gathering.
- Trouble-free to empty the pit when it fills.
- Apt for construction where limited space is available.

v. Advantages of Low–Cost Lavatory

- Prevents spreading of infections and diseases (diarrhea, dysentery, dehydration and cholera) due to open air defecation.
- Reduces the rate of dropping out school going girl children.
- Hygiene of surroundings can be maintained.
- Contamination of soil is also avoided.
- Decomposed material in soak pit can be utilized as manure (natural fertilizer) for growth of crops.

vI. Cost Estimate

Table 1. Estimation of the cost incurred in the construction of Low–Cost Lavatory

S.No.	Description of Item/Work	Quantity	Unit Cost (INR)	Total Cost (INR)
1.	Earth work Excavation for pit (5' depth, 3' diameter)	L.S.	---	650
2.	Cement Concrete Rings (3' diameter	6	180	1080

	and 1' height)			
3.	Cover Slab for Pit	1	410	410
4.	Cement	3	325	975
5.	Mason Charges	L.S.	---	1000
6.	L-Angulars, Steel Strips	60 kg	45	2700
7.	Welding Charges	L.S.	--	300
8.	Indian Water Closet	1	400	300
9.	Plumbing Items (PVC pipe, P-Trap)	L.S.	---	250
10.	FRP Sheet	112 sft	10/sft	1120
11.	Cement Bricks, Sand and Aggregate	L. S.	---	550
			Total Cost	**9335**
(Rupees Nine Thousand Three Hundred and Thirty Five only)				

vII. Conclusions

Low–Cost Lavatories promote better human health and also improve the quality of life of rural people through improved sanitation measures. As these lavatories can be constructed to serve for various purposes such as house hold, public places, institutions, at the places of religious festivals etc., the hygiene could be maintained. *Further, they serve the society and support in order to have a* ***cleaner India*** *to achieve* ***Swach Bharath*** *to fulfill the dream of our* ***Honorable Prime Minister, Mr. Narendra Modi.***

Acknowledgment

The authors are thankful to Mr. A. Madhukar Reddy, Secretary of S. R. Engineering College, Warangal for his motivation and encouragement to carry out 'Socially Relevant Projects' by applying engineering knowledge. Further, the authors are grateful to him for providing financial assistance to accomplish the project work. Also, authors are indeed thankful to all the staff members of the institution who are directly or indirectly helped to complete this task.

References

1. "CSR Guideline for Sanitation Programme", Govt. of India, Ministry of Drinking Water and Sanitation.
2. "Rural Sanitation" Sulabh International Social Service Organization, New Delhi.

DRAINAGE ON ROADS

[1]Dr. R. R.Singh, [2]Er.Navpreet Kaur, [3]Er.Nitin Goyal

[1]Associate professor (CED), PEC University of Technology,Chandigarh,INDIA

[2,3]Research scholar (CED), PEC University of Technology,Chandigarh,INDIA.

Email: [1]navpreetkaurpec@gmail.com, [2]nitingoyal121@gmail.com

ABSTRACT:

It has been seen many times that water in pavements is one of the major causes of premature pavement failure. Water may enter the pavement due to various reasons which may be stagnation of water on the surface or faulty construction of the roads leading to seepage of water into the pavement and thus causing damage to the same. Water in the pavement system can lead to moisture damage, modulus reduction and loss of strength. In order to prevent such damages to the pavement, it is essential to provide proper drainage to the roads. The presence of water in a highway layer reduces the bearing capacity of the road, and in doing so it also reduces the structure's lifetime. Highway drainage is used to clear surface water from the highway. . Roads need to be well drained to stop flooding, even surface water can cause problems with ice in the winter. Water left standing on roads can also cause maintenance problems, as it can soften the ground under a road making the road surface break up.

1. INTRODUCTION:

Highway drainage is the process of removing and controlling excess surface and sub-surface water within the right way. This includes interception and diversion of water from the road surface and sub-grade. The installation of suitable surface and sub-surface drainage system is an essential part of highway design and construction.

During rain, part of the rain water flows on surface and part of it percolates through the soil mass as gravitational water until it reaches the ground water below the water table. Removal and diversion of surface water from the roadway and adjoining land is termed as surface drainage, while the removal of excess soil-water from the sub-grade is termed as sub-surface water.

2. NECESSITY OF HIGHWAY DRAINAGE

Highway drainage is important from various view points:

- Excess moisture in soil sub-grade causes instability under the road surface. The pavement may fail due to sub-grade failure. In some clayey soil variation in moisture content causes considerable variation in volume of sub-grade. This sometimes contributes to pavement failure.
- The waves and corrugations formed in case of flexible pavements also play an important role in pavement failure.
- Sustained contact of water with bituminous pavements causes failure due stripping bitumen from the aggregates like loosening of some of the bituminous pavement layer and formation of pot holes.
- The prime cause of failures in rigid pavements by mud pumping is due to the presence of water in fine sub-grade soil.
- Excess water on shoulders and pavement edge causes considerable damage.
- Excess moisture causes increase in weight and thus increase in stress and simultaneous reduction in strength in soil mass. This is one of the main reasons of failure of earth slope and embankment foundations.
- In place where freezing temperatures are prevalent in winter, the presence of water in sub-grade and a continuous supply of water from the ground water can cause considerable damage to the pavement due to in frost action.
- Erosion of soil from top of un-surface roads and slopes of embankment, cut and hill side is also due to surface water.
- Failure due to hydraulic pressure and failure due to binder stripping can be avoided with the help of proper drainage on roads.

3. ROAD DRAINAGE

Well designed and well maintained road drainage is important in order to:

- Minimize the environmental impact of road runoff on the receiving water environment.
- Ensure the speedy removal of surface water to enhance safety and minimize disruption to road users.
- Maximize the longevity of the road surface and associated infrastructures.

There are many different types of drainage systems with different design features and attributes that can be used to manage flows and treat water quality. Drainage which is needed on the Highways Agency network depends not just on any flood risks and pollution risks identified but the characteristics of the natural water catchment area in which the network is based. The size, shape, gradient and geology of a catchment area are all factors which can influence the type of drainage methods used.

4. SURFACE DRAINAGE

The surface water is to be collected and then disposed off. The water on the surface is first collected in longitudinal drains, generally in side drains and then the water is disposed off at the nearest stream, valley or water course. For the preparation of surface drainage, we should keep in mind various things like

COLLECTION OF SURFACE WATER

Seeing the amount of rainfall and slope a suitable camber is to be provided for collection of surface

water. The shoulders of rural roads are constructed with suitable cross slopes so that the water is drained across the shoulders to the side drains. These side drains of rural roads are generally Open (kutcha) drains of trapezoidal shape, cut to suitable cross-section and longitudinal slopes. These sides are provided parallel to the road alignment and hence these are also known as longitudinal drains. In embankments the longitudinal drains are provided on one or both sides beyond the toe; in cutting, drains are installed on either side of the formation.

In urban roads because of the limitation of land width and also due to the presence of

footpath, diving island and other road facilities, it is necessary to provide underground longitudinal drains. Water drained from the pavement surface can be carried forward in the longitudinal direction between the kerb and the pavement for short distances which may be collected in catch pits at suitable intervals and lead through underground pipes.

Drainage of surface water is all the more important in hill roads. In hill roads disposal of water is also very important. Certain maintenance problems may arise due to faulty hill road construction.

5. CROSS DRAINAGE

For streams crossing the runways, drainage needs to be provided. Also often the water from the side drain is taken across by these cross drains in order to divert the water away from the road, to a water course or valley in the form of culverts or bridges. When a small stream crosses a road with linear water way less than amount six meter, the cross drainage structure provided is called culvert; for higher value of linear waterway, the structure is called bridge.

6. SUB-SURFACE DRAIN

Change in moisture content of sub-grade are caused by fluctuations in ground water table seepage flow, percolation of rain water and movement of capillary water and even water vapour. Although sub-surface drainage helps in removal of gravitational water, it is designed to keep minimum moisture in sub-grade.

LOWERING OF WATER TABLE

The highest level of water table should be fairly below the level of sub grade, in order that the sub grade and pavements layers are not subjected to excessive moisture. From practical considerations it is suggested that the water table should be kept at least 1.0 to 1.2 meter below the sub grade. In place where water table is high (almost at ground level at times) the best remedy is to take the road formation on embankment of height not less than 1.0 to 1.2 meter. When the formation is to be at or below the general ground level, it would be necessary to lower the water table.

If the soil is relatively permeable, it may be possible to lower the high water table merely construction of longitudinal drainage trenches with drain pipe and filter sand. If the soil is relatively less permeable, the lowering of ground water level may not be adequate at the center of the pavement or in between the two longitudinal drainage trenches. Hence in addition, transverse drainage may have to provide in order to

effectively drain off the water and thus lower the water table up to the level of transverse drains.

7. PREVENTIVE MEASURES

- **CONTROL OF SEEPAGE FLOW**

When the general ground and impervious strata below are slopping, seepage flow is likely to exist. If the seepage zone is at depth less than 0.6 to 0.9 meter from the sub grade level, longitudinal pipe drain in trench filled with filler material and clay seal may be constructed to intercept the seepage flow.

- **CONTROL OF CAPILLARY RISE**

If the water reaches the sub grade due to capillary rise is likely to be detrimental, it is possible to solve the problem by arresting the capillary rise instead of lowering the water table. The capillary rise may be checked either by capillary cut-off of any one of the following two types:-

a) A layer of granular material of suitable thickness is provided during the construction of embankment, between the sub grade and the highest level of sub surface water table.

The thickness of the granular capillary cut-off layer should be sufficiently higher than the anticipated capillary rise with in the granular layer so that the capillary water cannot rise above the cutoff layer.

b) Another method of providing capillary cut-off is by inserting an impermeable or

Bituminous layer in the place of granular blanket.

8. CONCLUSION

Seeing the above properties of drainage and keeping in view the necessity of drainage at surface as well as sub-surface level, drainage plays an important role in highway engineering. As drainage helps in avoiding various types of failures as may be caused by stagnant water on the road surface or its seepage beneath the pavement, it is important to provide drainage facility while construction of roads. Thus to increase the life of the road and to reduce the maintenance cost drainage of roads must be properly provided. Considering the above factors, this paper has been attempted in lieu of highway engineering.

REFERENCES:

1. https://mailattachment.googleusercontent.com
2. https://mailattachment.googleusercontent.com
3. http://www.highwaysmaintenance.com/drainage.htm
4. *http://www.wq.uiuc.edu/dg/surface.htm*

A ROUTING ALGORITHM FOR LOCALIZATION OF LINK FAILURE IN MANET

Srinivas Aluvala[1],Deepika Vodnala[2],Nagendar Yamsani[3],Dr. S. Phani Kumar[4]
[1,3]Asst. Professor, SR Engineering College
[2] Research Scholor, GITAM University
[4]Professor and HOD, GITAM University
[1]srinu.aluvala@gmail.com, [2]deepuvodnala8@gmail.com, [3]nagendar.yamsani@gmail.com,
[4]phanikumar.s@gmail.com

***Abstract*—Routing is a critical task in Mobile Ad hoc Networks (MANET's) due to the adaption of dynamic topology. Plenty of routing protocols were proposed and in use. Routing and route maintenance is a challenging task in MANETs due to frequent link failures which causes more data loss and delay. To overcome such problems, many of link repair mechanisms were proposed, still all of these have some limitations. This paper proposes a routing algorithm for route maintenance based on localization of link failure called DSR-LLF. It takes decision based on location of failure link of source route. Our proposed algorithm may achieve better packet preserving, increases the number of delivered packets to destination and performance of DSR.**

***Keywords*—MANET,DSR-LLF, dynamictopology, routing, preserving.**

I. Introduction

MANET is a collection of wireless mobile nodes which comply with the other nodes in moving packets in multi-hops without any control. The nodes mobility is random, therefore MANET has dynamic topology. Due to the approach of dynamic topology, link failures in MANET's occur frequently. These failures cause many problems such as data loss, delay in transmission etc and many other factors, which results in the degradation of capability of the network. Routing in MANET is crucial because of its dynamic topology. Many routing protocols have been proposed and in use for MANET, and these protocols categorized as proactive and reactive routing protocols.

Reactive routing protocols are mostly used because of their low frequency of route discovery in comparison with pro-active routing protocols. DSR is mostly implemented in MANET. DSR protocol comes with, Route Discovery and Route Maintenance mechanisms, which work hand in hand to allow nodes in the network to discover and maintain routes to carry the data packets to the destination. However, the link failures in the network can significantly increases the overhead and decreases the performance of the network, because link failure may result in packet loss, delay and may also need global information of the nodes in the network to discover a new route, when no other route is available in route cache.

Route maintenance is one of the major challenges in MANET. To mitigate the link failure problems, many local link repair mechanisms were proposed. But those mechanisms do not work on the basis of location of link failure in source route and does not make use of relay node location in source route. Our proposed routing algorithm works on link failure location in source route.

II. Discovery And Maintenance Of Route

The key features of DSR routing protocols are laid on the implementation process of source routing. This protocol implements Route Discovery and Route Maintenance, works hand in hand to allow nodes in the network to discover and maintain routes to transmit the packets to the destination.

A. *Discovery of Route*

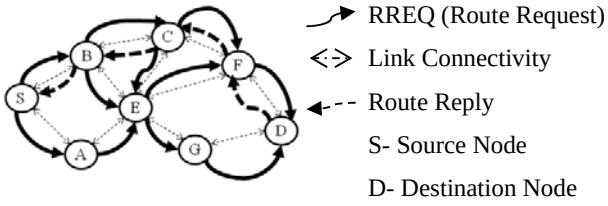

Figure 1. Discovered Route (**S, B, C, F, D**)

The above figure shows the route finding mechanism of DSR. When source node (S) wants to transmit data packets to the destination node (D) initially, it looks its routing cache for a path to the destination, if found then source node forward the packet accordingly to the route found in route cache. Else, source node (S) broadcasts Route Request Packet (RREQ) to all the neighbor nodes which are in the range of its transmission. Each RREQ contains sender address, receiver address, request ID, and route record. In this process if any node receives the packet of route request, it process the request, RREQ processing steps:

- If this (current) route request is found with that node, in the list of very recently seen requests, then the route request is not processed further.
- In case, if a node's address is already present in the route cache of the current node in the request, then the route request packet is discarded and do not process it further.
- Else, if the request matches with the destination node's own address, in this case the route record in the packet knows the route by which the request packet reached this destination node from the source. So a copy of this route is sent in a route reply packet to the source.

Else, add the current node address, in the route request, and again broadcasts the request. So the route request is propagated over the network till it reaches the intended destination node, which then results in replying to the source. In our above example, when a route request packet reaches at the destination (D), it returns a Route Reply Packet (RREP) along with the vise versa of a recorded path to the source (S), which is (S, B, C, F, D).

B. *Maintenance of Route*

When relay node sends the packet and if it is found that it's not reachable to the next node in the source route because of any reason then it propagates a route error message to the source. To preserve packet loss relay node initially checks its route cache for an alternate route to destination, in case if a route is found then it forwards the packet and informs the source about the available new route to destination. When source node receives route error packet, it discards all routes which contains the failure link.

III. Route Repair Mechanisms

DSR_DI in DSR adopts route repair mechanisms based on downstream node's Information. DSR_DI broadly classified into two algorithms such as Local relay node cache search algorithm and local area route discovery. To find the new routes to any downstream node, when a link failure occurs, DSR_DI implements a mechanism called local relay node cache search algorithm to search the alternate route to any downstream node in the network. In other case, it applies local area route discovery algorithm to search a route to any downstream node. The DSR-DI protocol will raise the performance of DSR protocol. In Proximity Approach to Connection Healing (PATCH) if the link between source and destination breaks off, assumed to be always exists from relay node, in most cases, an alternate route to the original next node via neighboring nodes. In these scenario, if a request packet is put to find an alternate node which is at a distance to the original route with limited time-to-live (e.g. 2 hops), at this instance the possibility to put right the existing route should be high and the overhead on the intermediate nodes should be much lower when compared to end-to-end global recovery. In Witness-Aided Routing (WAR) when a link breaks off, it carries out recovery mechanism by broadcasting the data

packets with predefined hop limits. WAR renders fast route recovery, but needs more control on the overhead since data packet is broadcasted as a recovery packet. Associability Based Routing (ABR), a routing technique to select the routes which are likely to be long-lived. In case, if a link breaks off, two scenarios come over. In scenario one if relay node is situated in less than the first half part of the source route, then a route error is sent to the source, so the source will handle route discovery to recover the route. In scenario two relay node will transmits over the network a route request with a hop count equal to the left number of hops that was in the current failured route. In this case destination only will able to response to the route request. If this succeeds, this route is found to be an alternate and no route error will be reported. Or else, a route error will be sent to the node next to the relay node, which in turn repeats the above two scenarios techniques again and again. This process is recursively carried out until the broken route is set right. Implementing of this approach needs more bandwidth and delay is more if in the process of route repair, if failing recursion keeps on going. Relative Distance Micro-discovery Ad Hoc Routing (RDMAR) also employs a similar mechanism of local repair of route as ABR. However, the location of the localized route repair is assumed from the node cache record.

A. Existing DSR Algorithms Limitations

- Forwarding of every packet on the network causes flooding and maximum consumption of bandwidth occurs.
- Number of error messages is more.
- Packet drops/losses are more.
- As network size increases the efficiency decreases.

B. Local Link Recovery Mechanisms

- Local information plays vital role in making decisions.
- Load on all in between nodes is more.
- All the in between nodes from source to destination adopt same processes of recovery irrespective of their location in the source route.

C. Based on Downstream Nodes Information

- If a failed link is distant to destination, their exists always a possibility of overhead on intermediate nodes.
- If the mobility of the nodes is highly then more links failure occurs and may decrease the entire network performance.

IV. Proposed Algorithm

To overcome the above discussed mechanisms limitations, this paper introduces a new algorithm DSR-LLF based on DSR which make up the decisions depending on the location of the Relay Node (i.e. where the link failure is found) in source route.

A. DSR-LLF brief Description

When a failure occurs in the routing, the DSR, DSR-DI and PATCH will not take decision based on the failed link location in source route. Our proposed algorithm DSR-LLF is mainly a route maintenance algorithm, which takes decision depending on the location of failure link in source route. DSR-LLF divide source route into three clusters, i.e. source cluster, destination cluster and intermediate cluster, if possible equal sized regions otherwise it divides the regions with the source and destination clusters equal in size and intermediate cluster larger in size compared to the source and destination. Conditionally the intermediate cluster needs to be equal in size with the source and destination clusters or else larger in size but not in small.

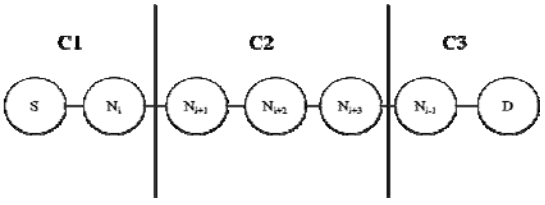

Figure 2. Clustering of Source Route

In the above figure cluster denoted with C: 1 is for the nodes near to the source node called Source cluster, C: 2 is for the intermediate cluster which is in between the source and destination, C: 3 is for the nodes near to the destination called destination cluster. When a relay node forwards packet to the next node in

source route and if it founds link failure then the proposed algorithm DSR-LLF work as follows:

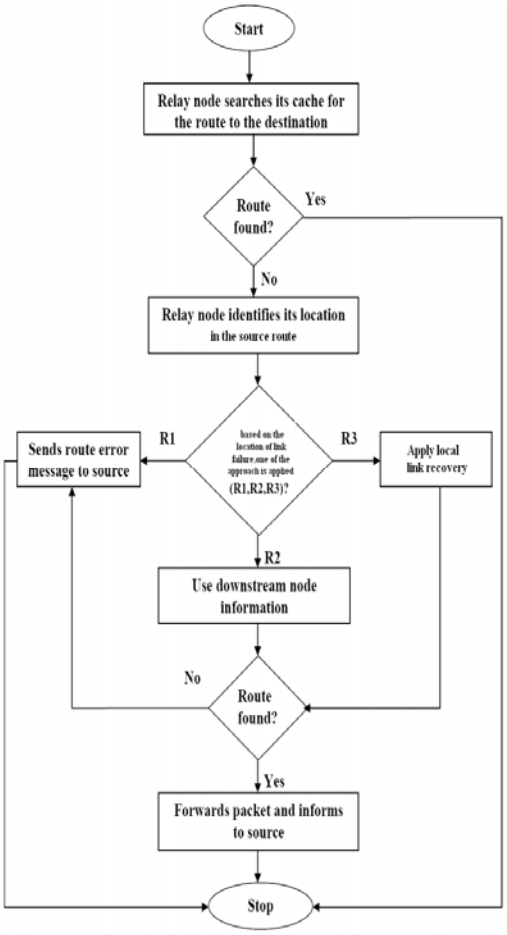

Figure 3. Working process of DSR_LLF

- Firstly, Relay Node looks into its route cache for another route to the destination.
- If it finds the route then forwards the packet to destination using new available route and inform it to the source about the new route.
- Otherwise, Relay Node identifies the location of failure, where the Relay node relates to any one of the cluster.
- If Relay Node belongs to Source Cluster, then Route Error message is send to source. So source make decisions to find the route to the destination.
- If Relay Node belongs to Destination Cluster, then Route Error message is send to destination. Then relay node will make use of downstream information to find new route to destination, if new path is found, relay node forwards the packet and informs to source.
- If Relay Node belongs to intermediate cluster, then recovery of the link can be done locally using one hope or two hope requests. So Local Link Recovery is applied at Relay Node. Relay Node forward the packet and informs to source when link recovery is successful.

V. Algorithm Outcomes

The proposed algorithm DSR-LLF may overcome the limitations of already existing algorithms. It improves the route maintenance mechanism of DSR. Because of divide and solve approach intermediate nodes load will vary and depends on their cluster. Expected results of DSR-LLF are:

- Packet salvaging and delivery ratio is increased.
- Number of error messages are reduced.
- Scalability of network as compared to DSR will improve.

VI. Conclusion

The DSR-LLF algorithm works when a link failure occurs in MANET. It takes decision depending on the location of link failure in the source route. Source route is divided into three clusters, and depending on the cluster of relay node DSR-LLF will apply a right mechanism for route maintenance. Because of unique approaches intermediate nodes load will vary and depends on their cluster. DSR-LLF will be helpful to improve the solutions in discovery of route, route maintenance and the overall performance of DSR.

References

[1] D.B. Johnson and D. A. Maltz, "Dynamic Source Routing Protocol for Mobile Ad Hoc Networks", Mobile Computing, T. Imielinski and H. Korth, Eds., Kluwer, 1996, pp. 153-81.

[2] Junjie Chen, Chang'en Zhou, Deli Chen, Bin Huang, Jiajun Hong, Chao Zhou1, Xiao Yang, "A Novel Routing Algorithm for Ad hoc Networks Based on the Downstream Nodes Information", International Conference on Multimedia Information Networking and Security, 2009. 978-0-7695-3843-3/09 IEEE 2009.

[3] Genping Liu, Kai Juan Wong, Bu Sung Lee, Boon Chong Seet, Chuan Heng Foh, Lijuan Zhu, "PATCH: a novel local recovery mechanism for mobile ad-hoc networks", Vehicular Technology Conference, 2003. VTC 2003-Fall. 58th. Page(s):2995 – 2999 Vol.5. IEEE, 2003.

[4] Aron and S. Gupta. “A Witness-Aided Routing Protocol for Mobile Ad-Hoc Networks with Unidirectional Links”, Proc. First lnt'l Conf. on Mobile Data Access (MDA '99), Hong-Kong, Dec. 1999, pp. 24-33.

[5] C-K. Toh, "A novel distributed routing protocol to support ad-hoc mobile computing," IEEE International Phoenix Conf. on Computers and Communications, IPCCC'96.

[6] C. K. Toh, "Long-lived ad hoc routing based on the concept of associativity", Internet draft, IETF, Mar. 1999.

[7] George Aggelou , Rahim Tafazolli, “RDMAR: a bandwidth-efficient routing protocol for mobile ad hoc networks”, Proceedings of the 2nd ACM international workshop on Wireless mobile multimedia, Seattle, Washington, United States, August 20-20, 1999, pp.26-33.

[8] C. Gomez, D. Mediavilla, P. Salvatella, X. Mantecon, J. Paradells, “A Study of Local Connectivity Maintenance Strategies of MANET Reactive Routing Protocol Implementations”, 1-4244-0398-7/06 IEEE 2006

A Survey Paper On Toward Privacy Preserving and Collusion Resistance in A Location Proof Updating System

[1]Mr. Kamlesh S. Samrit, [2]Mr. Prajyot A. Gawarkar, [3]Prof. Priyanka A. Jalan
[1,2,3]Department of Computer Engineering, Bapurao Deshmukh College of Engineering, Sewagram,
[1]kamleshsamrit@gmail.com, [2]qwertyprajyot@gmail.com, [3]priyanka9.jalan@gmail.com

***Abstract*— Today's location-sensitive service relies on user's mobile device to determine the current location. This allows malicious users to access a restricted resource or provide bogus alibis by cheating on their locations. To address this issue, we propose A Privacy-Preserving Location proof Updating System in which collocated Bluetooth enabled mobile devices mutually generate location proofs and send updates to a location proof server. Extensive experimental results show that A Privacy-Preserving Location proof Updating System can effectively provide location proofs, significantly preserve the source location privacy, and effectively detect colluding attacks. The Cloaked Area determination algorithm aims to minimize communication and computational cost. The effectiveness of proposed detection system is evaluated and influences of both non normalized data and normalized data on the performance of the proposed detection system are examined. The above proposed algorithms minimizes the communication and computational cost, size of the cloaked areas and also maximizes the accuracy of the aggregate locations reported to the server.**

***Index Terms*—anonymity, location proof, location privacy, localization techniques.**

I. INTRODUCTION

Mobile Networks are insecure due to its broadcasting nature. A mobile network doesn't have a clear line of protection. So mobile nodes can join the network and leave the network at any time and at any location. The location based services is based on the user location which can be provided by the mobile devices. Loopt and Google latitude are applications used to update the user's current location proof. Location-based services provide information about nearest entities (i.e. Nearby ATM, Restaurants, airports, etc.,) and offer location aware services. Geo-location data is gathered in a number of ways, including built-in Global Positioning System devices, IP address, or Wi-Fi network mapping. Location proof plays a vital role in location sensitive applications. Location sensitive applications such as [1][2] Location based access control, Location aware routing,

etc., are used in location proofs. They are also helpful in providing a history of location proofs and identifying a geographical location of users. Location proof is a piece of data that certifies a receiver to a geographical location [2].

In the location proof updating system, location information can be eavesdropped by adversaries. It may cause vulnerability towards location privacy of the user. Public key Cryptographic operation is used for encryption and decryption of communicating messages and prevents from eavesdropping. The Process of hiding the identity of nodes is an approach to obtain identity privacy; the identity of the node is hidden by using pseudonym.

To obtain the location privacy mobile nodes are expected to satisfy some or all of the basic properties given below: [3]

Location privacy: It is defined as an ability to prevent the unauthorized entities to access the location data of current and past locations.

Identity privacy: Mobile node is not able to find the identity of the user, based on the location information received during the location proof request .The real identity of the user should not be traced by the malicious node known as untraceability.

Unlinkability: No unauthorized entity should be able to relate different sessions of the mobile node. Depending on the scope, nature, and behavior of attacks, the attackers can be classified as follows: [4]

- Passive attackers participate in eavesdropping messages in communication.
- Active attackers will not forward the received packet to its destination by dropping or it may generate packet containing immoral information.
- Inside attacker are the authentic members of the network, sometimes it acts as the adversary.
- Outside attackers are the intruders.
- Malicious attackers are not getting any benefit personally by their attack. Their aim is to harm other members of the network or disrupt the functionality of a MANET.
- Local attacker attacks up to the limited radio range. An attack can be extended, where an attacker organized as a group across the network

II. LITERATURE SURVEY

Pranali Pise, et.al "A Review on Privacy Preserving in Location Proof System", They presented a survey about the various techniques that are well suited to preserve location privacy and location proofs[14].

Chi-Yin Chow, et.al "A Privacy-Preserving Location Monitoring System for Wireless Sensor Networks", they design two in-network location anonymization algorithms, namely, resource- and quality-aware algorithms, that aim to enable the system to provide high quality location monitoring services for system users, while preserving personal location privacy[15].

S. Suresh Kumar, et.al "Location Monitoring System in Wireless Sensor Networks Using Aggregate Query Processor", This paper proposes a privacy-preserving location monitoring system for wireless sensor networks to provide monitoring services. they propose two in-network aggregate location anonymization algorithms, namely, resource- and quality-aware algorithms[20].

Zhichao Zhu, et.al "Toward Privacy Preserving and Collusion Resistance in a

Location Proof Updating System", In this paper they propose A Privacy-Preserving Location proof Updating System (APPLAUS) in which co-located Bluetooth enabled mobile devices mutually generate location proofs and send updates to a location proof server. they also develop user-centric location privacy model in which individual users evaluate their location privacy levels and decide whether and when to accept the location proof requests[17].

H. Packiaraj, et.al "A Achieving Personalized Privacy and Compromised Conspiracy in Location Proof Updating System", In this paper they propose A Privacy-Preserving Location proof Updating System in which collocated Bluetooth enabled mobile devices mutually generate location proofs and send updates to a location proof server. Periodically changed pseudonyms

are used by the mobile devices to protect from the untrusted location proof server[16].

S. Saroiu,et.al "Enabling new mobile applications with location proofs", In this paper they presents location proofs – a simple mechanism that enables the emergence of mobile applications that require "proof" of a user's location. A location proof is a piece of data that certifies a receiver to a geographical location. Location proofs are handed out by the wireless infrastructure (e.g., a Wi-Fi access point or a cell tower) to mobile devices[1].

R. Poovendran, et.al "Caravan: Providing Location Privacy for VANET", In this paper, they study the problem of providing location privacy in VANET by allowing vehicles to prevent tracking of their broadcast communications. They first, identify the unique characteristics of VANET that must be considered when designing suitable location privacy solutions. Based on these observations, they propose a location privacy scheme called CARAVAN, and evaluate the privacy enhancement achieved under some existing standard constraints of VANET applications, and in the presence of a global adversary[12].

Mina Rahbari, et.al "Efficient Detection of Sybil Attack based on Cryptography VANET" The purpose of this paper present a method based on a fixed key infrastructure for detection impersonation attack, in other words, Sybil attack, in the vehicular ad hoc network. This attack, puts a great impact on performance of the network. The proposed method, using an cryptography mechanism to detection Sybil attack. Finally, using Mat lab simulator the results of this approach are reviewed, this method it has low delay for detection Sybil attack, because most operations are done in Certification Authority, so this proposed schema is a efficient method for detection Sybil attack[4].

III. CHALLENGES IN MOBILE NETWORKS

A. Insecure Boundaries

There is no clear secure boundary in the mobile ad hoc network, when compared with the defense available in the traditional wired network. This vulnerability originates because of its nature that gives the freedom to join, leave and move inside the network.

B. Restricted Power Supply

Due to the mobility of nodes in the ad hoc network, it is common that the nodes in the mobile ad hoc network will rely on battery as their power supply method. The restricted power supply may lead to denial-of-service attacks. Moreover, a node in the mobile ad hoc network may behave in a selfish manner when it finds that there is only limited power supply, and the selfishness can cause some problems when there is a need for this node to assist with other nodes to support some functions in the network.

C. Scalability

As the nodes are mobile, the scale of the Mobile ad hoc network keeps changing all the time. It makes it tough to predict how many

nodes will be in the network in the future. As a result, the protocols and services that are applied to the mobile network should be compatible to the continuously changing scale of the ad hoc network.

IV. PROPOSE METHODOLOGY

In this paper propose a Privacy-Preserving Location proof Updating System (APPLAUS) in which collocated Bluetooth enabled mobile devices mutually generate location proofs and send updates to a location proof server. It also develop user-centric location privacy model in which individual users evaluate their location privacy levels and decide whether and when to accept the location proof requests. In order to defend against colluding attacks, we also present betweenness ranking-based and correlation clustering-based approaches for outlier detection.

Fig.1. Location proof updating architecture and message flow.

APPLAUS can be implemented with existing network infrastructure, and can be easily

deployed in Bluetooth enabled mobile devices with little computation or power cost.

The Cloaked Area determination algorithm aims to minimize communication and computational cost. A quality enhanced histogram approach is used that estimates the distribution of the monitored persons based on the gathered aggregate location information. Then, the estimated distribution is used to provide location monitoring services through answering range queries. The effectiveness of proposed detection system is evaluated and influences of both non normalized data and normalized data on the performance of the proposed detection system are examined. The above proposed algorithms minimizes the communication and computational cost, size of the cloaked areas and also maximizes the accuracy of the aggregate locations reported to the server.

V. PRELIMINARY INVESTIGATION

In this paper, we focus on mobile networks where mobile devices such as cellular phones communicate with each other through Bluetooth. In our implementation, mobile devices periodically initiate location proof requests to all neighbouring devices through Bluetooth. After receiving a request, a mobile node decides whether to exchange location proof, based on its own location proof updating requirement and its own privacy consideration. Given its appropriate range (about 10 m) and low power consumption, Bluetooth is a natural choice for mutual encounters and location proof exchange.

A. Pseudonym

As commonly used in many networks, we consider an online Certification Authority (CA) run by independent trusted third party which can pre-establish credentials for the mobile devices. Similar to many pseudonym approaches, to protect location privacy, every mobile node i registers with the CA by preloading a set of M public/private key pairs KiPub, KiPrvMi=1 before entering the network. The public key KiPub is used to serve as the pseudonym of node i. The private key KiPrv enables node i to digitally sign messages so that

the receiver can validate the signature authenticity.

Due to the broadcast nature of wireless communication, probes are used for mobile nodes to discover their neighbours. When a node i receives a probe from another node, it checks the certificate of the public key of the sender and the physical identity, e.g., Bluetooth MAC address.

After that, i verifies the signature of the probe message. Subsequently, if confidentiality is required, a security association is established (e.g., with Diffie-Hellman).

B. Threat Model

We assume that an adversary aims to track the location of a mobile node. An adversary can have the same credential as a mobile node and is equipped to eavesdrop communications. We assume that the adversary is internal, passive, and global. By internal, we mean that the adversary is able to compromise or control individual mobile device and then communicate with others to explore private information, or individual devices may collude with each other to generate false proofs. We assume that the number of colluders is small compared with that of valid devices. In the worst case, the adversary could compromise the location proof server to get the stored location proof records.

However, it is not able to take control of the server to work as a colluder, since once compromised, the attack will be detected promptly and the location proof server will be replaced by a back-up server. The same assumption applies to the CA. By passive, we assume the adversary cannot perform active channel jamming, mobile worm attacks [12] or other denial-of service attacks, since these attacks are not related to location privacy. By global, we assume the adversary can monitor, eavesdrop, and analyse all the traffic in its neighboring area, or even monitor all the traffic around the server.

In practice, the adversary can thus be a rogue individual, a set of malicious mobile nodes, or eavesdropping devices in the network. In the worst case, it is possible that the untrusted location proof server may be compromised by the adversary and the location information can then be easily inferred by examining the records of location proofs, e.g., the adversary could apply statistical testing such as K-S test to identify a user although no real identity is included. Therefore, we need to appropriately design and arrange the location proof records in the untrusted server so that no private information related to individual users will be revealed even after it is compromised. Hence, the problem we address in this paper consists of collecting a set of location proofs for each peer node and protecting the location privacy of peer nodes from each other, from the adversary, or even from the untrusted location proof server to prevent other parties from learning a node's past and current location information.

C. Location Privacy Level

In this paper, we use multiple pseudonyms to preserve location privacy; i.e., mobile nodes periodically change the pseudonym used to sign messages, thus reducing their long term linkability. To avoid spatial correlation of their location, mobile nodes in proximity coordinate pseudonym changes by using silent mix zones [14], [15], or regions where the adversary has no coverage [13]. Without loss of generality, we assume each node changes its pseudonyms from time to time according to its privacy requirement. If this node changes its pseudonym at least once during a

time period (mix zone), a mix of its identity and location occurs, and the mix zone becomes a confusion point for the adversary

VI. CONCLUSION

In this paper, we investigate a privacy-preserving location proof updating system called APPLAUS, where collocated Bluetooth enabled mobile devices mutually generate location proofs and upload to the location proof server. We use statistically changed pseudonyms for each device to protect source location privacy from each other, and from the untrusted location proof server. We also investigate a user centric location privacy model in which individual users evaluate their location privacy levels in real time and decide whether and when to accept a location proof exchange request based on their location privacy levels. To the best of our to deal with colluding attacks, we investigate betweenness ranking based and correlation clustering-based approaches for outlier detection. Extensive experimental and simulation results show that APPLAUS can provide real-time location proofs effectively. Moreover, it preserves source location privacy and it is collusion resistant.

REFERENCES

[1] S. Saroiu and A. Wolman, et.al "Enabling new mobile applications with location proofs" ACM HotMobile, 2009.

[2] W. Luo and U. Hengartner,et.al "Proving your location without giving up your privacy" ACM HotMobile, 2010.

[3] Emmanouil Magkos,et.al "Cryptographic Approaches for Privacy P reservation in Location-Based Services A survey"

[4] Mina Rahbari, et.al "Efficient Detection of Sybil Attack based on Cryptography VANET", International Journal of Network Security & Its Applicarions Vol.3, No.6, Nov 2011, pp185-195.

[5] A.R. Beresford and F. Stajano. et.al "Location privacy in pervasive computing", IEEE Security and Privacy, 2003,pp46-55.

[6] M. Li, R. Poovendran, K. Sampigethaya, and L. Huang. Caravan et.al "Providing location privacy for vanet". In Proceedings of the Embedded Security in Cars (ESCAR) Workshop

[7] B. Gedik and L. Liu. et.al "A customizable k-anonymity model for p rotecting location privacy", In IEEE ICDCS, 2005.

[8] Y. Yang, M. Shao, S. Zhu, B. Urgaonkar, and G. Cao. Et.al "Towards event source unobservability with minimum network traffic in sensor networks", In ACM WiSec, 2008.

[9] Z. Zhu and G. Cao. et.al "APPLAUS: A privacy-preserving and collusion resistance in location proof updating system" IEEE INFOCOM 2011.

[10] Z. Zhu, G. Cao, S. Zhu, S. Ranjan, and A. Nucci, et.al "A Social Network Based Patching Scheme for Worm Containment in Cellular Networks," Proc. IEEE INFOCOM, 2009.

[11] L. Buttya´n, T. Holczer, and I. Vajda, et.al "On the Effectiveness of Changing Pseudonyms to Provide Location Privacy in VANETs," Proc. Fourth European Conf. Security and Privacy in Ad-Hoc and Sensor Networks, 2007.

[12] M. Li, R. Poovendran, K. Sampigethaya, and L. Huang, et.al "Caravan: Providing Location Privacy for VANET," Proc. Embedded Security in Cars (ESCAR) Workshop, 2005.

[13] M. Li, K. Sampigethaya, L. Huang, and R. Poovendran, et.al "Swing & Swap: User-Centric Approaches Towards Maximizing Location Privacy," Proc. Fifth ACM Workshop Privacy in Electronic Soc., 2006.

[14] Prof. Ratnaraj Kumar, et.al "A Review on Privacy Preserving in Location Proof System", International Journal of Advanced Research in Computer Science

and Software Engineering Volume 4, Issue 1, January 2014, pp 287-294.

[15] Chi-Yin Chow, et.al "A Privacy-Preserving Location Monitoring System for Wireless Sensor Networks", IEEE, pp 1-14.

[16] H.Packiaraj, et.al "A Achieving Personalized Privacy and Compromised Conspiracy in Location Proof Updating System", International Journal of Research in Advent Technology, Vol.2, No.2, February 2014, pp 195-200.

[17] Zhichao Zhu, et.al "Toward Privacy Preserving and Collusion Resistance in a Location Proof Updating System", IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 12, NO. 1, JANUARY 2013, pp 51-64.

[18] Dattatray P. Gade, et.al "Implementing Privacy Preserving Location Monitoring System in WSN", International Journal of Emerging Technology and Advanced Engineering Volume 3, Issue 3, March 2013, pp 610-615.

[19] Blessed Prince P, et.al "A Survey on Preserving Privacy towards Location Proof", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 2, February 2013, pp 773-776.

[20] S. Suresh Kumar, et.al "Location Monitoring System in Wireless Sensor Networks Using Aggregate Query Processor", International Journal of Advanced Research in Computer Science and Software Engineering(IJARCSSE) Volume 3, Issue 5, May 2013,pp-146-152.

FIR FILTER DESIGNING BY IMPLEMENTATIONS OF DIFFERENT OPTIMIZATION ALGORITHMS

AMRIK SINGH[1], NARWANT SINGH GREWAL[2]
[1] Student, E. C. E. department, G. N. D. E.C. Ludhiana, India,
[2]Assistant Professor, E. C. E. department, G. N. D. E.C. Ludhiana, India,
[1]amrikkhosa@gmail.com, [2]narwant@gndec.ac.in

Abstract- FIR filter is multimodal design problem. Due to multimodal and non-linear nature of error surface conventional gradient based technique are not efficient for filter designing. So numerous authors have been solved the filter design problem by implementation of different global optimization algorithms and achieve promising results. In this paper performance of various implementation techniques such as genetic algorithm, differential evolution algorithm, particle swarm optimization, adaptive differential evolution particle swarm optimization and cat swarm optimization are discussed and compared.

Key words: Optimization, FIR filter, genetic algorithm, differential evolution algorithm, particle swarm optimization, adaptive differential evolution particle swarm optimization, cat swarm optimization, pass band ripple, stop band attenuation.

INTRODUCTION

Today digital signal processing (DSP) has a wide range of applications in the fields of communication, pattern recognition, image processing, etc. Because of having numerous advantages such as more flexibility, good performance, better time response, environment stability and lower equipment production costs than traditional analog techniques it become one of popular application area in electronic engineering and need more advancements in present era. These all new DSP advancements caused from the advances in digital filtering. Digital filter is main component in DSP and it is define as a system that performs mathematical operations on a sampled discrete time signal to shrink or boost certain aspects of that signal. It is the digital filter which performs all basic function in DSP such as filtering, addition of signal or to separation of signal etc. Nowadays due to advancement in technology filters with high speed and less error are needed to design. Due to these requirements filter design become a popular search area. There are two basic types of digital filters, Finite Impulse Response (FIR) and Infinite Impulse Response (IIR) filters. FIR digital filter have many benefits like guaranteed stability, free from phase distortion and low coefficient sensitivity and simplicity make it preferred in most cases.

There are various traditional methods exist for digital FIR filter design. Out of those one is design of filter by making use of optimization algorithms. This method has an amazing ability that is it gives options of using of different optimization algorithms and improperness in design directly depend upon performance of algorithms. Initially this method has given by Parks and McClellan by using a simple iterative commuter program and is termed as PM method for filter designing [1],[2]. Later this method is further modified by replacing use of simple program with optimization algorithms. In initial genetic algorithm was used for all types of filter design [3-4]. This is followed by use other algorithms like stimulated annealing, artificial bee colony, and differential evolution

by different authors [5-7]. Then practical swarm optimization algorithm which is most popular algorithm proposed by Kennedy and Eberhart [8] has implemented for the filter design [9]. After this hybrid algorithms and modified algorithms has been developed from basic type of algorithm for further improvements in filter designs. Uses of improved particle swarm optimization, adaptive evolution particle swarm optimizations for the filter designing are witness of these trends [10-12]. Recently a novel algorithm named Cat swarm optimization has been implemented for design of filter for achieving more effective results [13].

DIGITAL FILTER:

In simple words digital filter is a system which performs a mathematical operation on input signals and covert into another form. So digital filters can be represented mathematically by its characteristic equation given as

$$H(z)=\sum_{n=0}^{M} h(n)z^{-n} \quad , n=0,1\ldots M \qquad (1)$$

where M is the order of the filter which has (M+1) number of coefficients and h(n) is the filter's impulse response. [14] H(z) is termed as transfer function it is the what which is multiplied by filter to input signal to convert into output. It is calculated by applying an impulse signal at the input. The values of h(n) will determine the type of the filter e.g. low pass, high pass, band pass etc. For linear phase FIR filter h(n) is symmetrical so only half of coefficient are need to calculate. For design of filter using optimization algorithm the filter design problem is converted into an optimization problem. That is one fitness function is calculated which is related to error of designed filter from ideal filter. Then this fitness function is optimized to find best fit individuals. The error function is a difference between the ideal filter response and practical response and can be calculated as

$$E(w) = G(w)(H_d(e^{jw}) - H_i(e^{jw})) \qquad (2)$$

Where H_i (w) correspond to ideal filter response, G (w) is weighting function, H_d (w) correspond to actual filter response calculated using given variables [9].

H_i (w) can be any type of ideal filter that is it can be low pass, high pass, band pass or band reject filter .By using different type of H_i (w) corresponds type of filter can be designed.

Fitness function which is to minimized using optimization algorithm is normally maximum values of this error function and can be represent as in equation (3) simplest form as

$$FIT = \min(\max|E(w)|) \qquad (3)$$

In this way by using FIT as fitness function filter design problem can be converted into optimization problem which can be solve by any of meta- heuristic algorithms. Accuracy of designed filter directly depends upon performance of algorithm that is "better is algorithm more accurate filter design can be achieved". However this basic form of fitness function shown in equation (3) has some disadvantage so it is improved by number of authors and gives rise to several versions of fitness functions for optimal design of filter. In this way there are two modifications available for better filter design one is use of better fitness function which gives more control on filter parameters and second is use of better optimization algorithm which has better performance. Both approaches are used by numerous authors and give rise to number of research work available in literature. Out of which some work of using different optimization algorithm is discussed in this paper.

OPTIMIZATION TECHNIQUE EMPLOYED

A. Genetic algorithm

Genetic algorithm (also known as real code genetic algorithm) is based on the concept of "survival of the fittest" [4]. This process equivalent to genetic recombination and mutation are employed in order to promote the evolution of a population that best satisfies a desired goal. The individual which are to be optimized are considered as chromosomes. The algorithm starts with an initial population representing random chromosomes solutions. Each individual in the population is awarded a score based on its performance. The individuals with the best scores are most likely to be selected to yield a new generation. The

selected individuals are used to yield a new population based on two main genetic operators, crossover and mutation. In crossover, two individuals are used to yield two new individuals by genes exchange between the two selected individuals. Random mutation is also applied to add some diversity to the population. The produced children are also scored, with the best performers are likely to be parents in the next generation. The process is repeated until achieving a termination criterion. Same approach is used in filter designing which best fit filter coefficient are find using given fitness function

B. DE algorithm

The differential evolution algorithm (DE algorithm) is a method based on the principles of GAs, but with crossover and mutation operations that work directly on continuous-valued vectors [6]. The main difference in constructing better solutions is that GAs relies on crossover, whereas the DE algorithm relies on the mutation operation. Crossover base on selection of best among two and mutation is related to adopt best quality of both and produced a new child. This main operation is based on the differences of randomly sampled pairs of solutions in the population due to this the name differential evolution is uses. Main aim of this algorithm is also to find individuals which are most suitable for given fitness function but have advantages like it finds the true global minimum of a multimodal search space regardless of the initial parameter values and it has fast convergence, As it has batter performance then standard GA so batter filters are obtained by implementation of this on same fitness function.

C. Particle swarm optimization

Particle swarm optimization (PSO) is a flexible, robust population-based stochastic optimization technique with implied parallelism, which can easily handle with non-differential objective functions [8]. PSO is developed through simulation of bird flocking in multidimensional space. Bird flocking optimizes a certain objective function. Each particle (bird) knows its best value so far (pbest). This information corresponds to personal experiences of each particle. Moreover, each particle knows the best value so far in the group (gbest) among pbests. Namely, each particle tries to modify its position using the two type of information one is the distance between the current position and the pbest and second is the distance between the current position and the gbest. Using this information each bird modifies its velocity toward these values. So a swarm of bird tried to reach at best suitable value hence optimized the function. This algorithm has a number of advantages over the other exiting algorithms such as less chance of frailer, more accuracy and can also be used for filter design to remove weakness of design obtained by using of other algorithms.

D. Adaptive DEPSO (ADEPSO):

DEPSO is a hybrid version of DE evolution and PSO which utilizes the benefits incurred in both the algorithms individually. DEPSO approaches in terms of robustness and accuracy of the optimization algorithms. The DEPSO is further modified with the use of fitness based adaptive cross over rate used for the cross over purpose. The one having better fitness value should have more probability of being transferred to the trial vector rather than the one having lower fitness value. So using this concept cross over rate is calculated separately for each and every element of the population set and a new version is obtained named as adaptive DEPSO. ADEPSO have batter performance then basic algorithms. This is proposed by Vasundhra et al. [13] and filter designed by implementations of these give rise to improvements in filter design.

E. Cat swarm optimization

The algorithm imitates the natural behavior of cats. Cats have a strong curiosity towards moving objects and possess good hunting skill. Even though cats spend most of their time in resting, they always remain alert and move very slowly. When the presence of a prey is sensed, they chase it very quickly spending large amount of energy. These two characteristics of cat are resting with slow movement and chasing with high speed and

are represented by Seeking and Tracing modes, The CSO algorithm reaches its optimal solution using two groups of cats, i.e., one group containing cats in seeking mode and the other group containing cats in tracing mode. The two groups combine to solve the optimization problem and algorithm achieves batter performance. Implementations of cat swarm optimization give rise to improvements in filter design spatially reduction in stop band ripple factor.

EXPERIMENT RESULTS AND DISCUSSION

This section presents the simulations results performed in MATLAB R2013a for the design of FIR filters. Order (N) of filter is each case is taken as 20, which results in the number of coefficients as 21. As in linear phase FIR filer coefficient are symmetrical only half of coefficients has been calculated in this problem. The sampling frequency is equal to 1Hz and the number of frequency samples is taken equal to 128. Each algorithm is run for fixed number of iterations (200) to obtain results. Although any of basic type FIR filter (low pass, high pass, band pass etc.) can be obtained using given approaches by change H_i (w) in equation (2). But only FIR design of high pass filter is discussed and compared in this paper because performance algorithm for of all other type is almost similar. For the design of 20 order high pass obtained filter coefficients h(n) by implementation of different algorithms are presented in Table 1.

h(n)	*RGA*	*PSO*	*DE*	*ADPSO*	CSO
h(1)= h(21)	0.0217	0.0256	0.0290	0.0295	0.0275
h(2) =h(20)	-0.0481	-0.0474	-0.0459	-0.0456	-0.0444
h(3) =h(19)	0.0062	0.0514	0.0029	0.0020	0.0032
h(4) =h(18)	0.0419	0.0400	0.0413	0.0369	0.0429
h(5) =h(17)	0.0008	0.0014	-0.0003	-0.0041	0.0010
h(6) =h(16)	-0.0590	-0.0603	-0.0600	-0.0548	-0.0582
h(7) =h(15)	-0.0000	0.0008	-0.0039	-0.0042	0.0032
h(8) =h(14)	0.1042	0.1051	0.1061	0.1031	0.1024
h(9)= h(13)	0.0004	-0.0001	-0.0006	0.0039	-0.0022
h(10)=h(12)	-0.3166	-0.3155	-0.3201	-0.3142	-0.3179
h(11)	0.4995	0.4999	0.5000	0.4920	0.4998

Table 1.Calculated filter coefficients for high pass FIR filter by using various algorithms

The coefficients are calculated up to high precision value using MATLAB R2013. But coefficients up to only 4th decimal value are shown in Table 1. Frequency response of filter designed can be obtained from coefficients and magnitude across the normalized frequency can be checked to note the amplification and attenuation across the different frequency range that is to find pass band and stop band range and behavior of filter in these bands. Magnitude responses of high pass filters having coefficients as shown in Table 1 are shown in Figure 1.

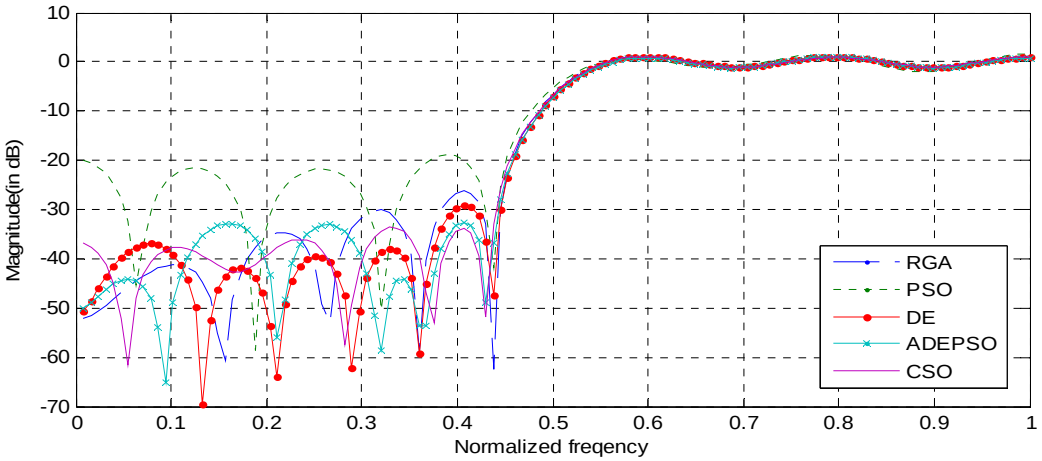

Figure 1 Frequency response of high pass filter using various algorithms

Figure 1 show comparative plot of high pass filter obtained by applying different optimization algorithms. This figure is obtained using filter coefficients shown in Table 1 and clearly shows the results obtained using different algorithms. For comparison in performance of designed filters maximum stop band attenuation is considered. Higher is the maximum stop band attenuation (lesser is ripple) better is the performance of filter. So hybrid version ADPSO and new type of algorithm CSO are said to better performing techniques. Pass band ripple value and maximum stop band attenuation obtained in all works is compared in Table 2.

Algorithm	Pass band ripple	Stop band ripple	Attenuation in stop band (in dB)
PM	0.066	0.0688	-23.55
RGA	0.117	0.0546	-25.25
PSO	0.122	0.0394	-28.01
DE	0.136	0.0348	-29.16
ADEPSO	0.132	0.0232	-32.68
CSO	0.132	0.0208	-33.62

Table 2 Comparative summary of parameters obtained for high pass filter using various algorithms

Table 2 shows the effective reduction in stop band attenuation using latest optimization algorithms.

That is signal will stopped more effectively in stop band and leakage noise become lesser in case of Filters obtained by hybrid and new algorithms. It is noted that pass band ripple is least in case of PM approach which is because equal weightage was given to both pass band ripple and stop band ripple in that approach. However after this researcher feels that there is more need to control on stop band attenuation so RGA and latter techniques design filter with better stop band attenuation on compromising the pass band ripple. Significant improvement using all later RGA techniques is mainly because of performance of algorithms. Similarly other types of filter (low pass, band pass, band reject) are also can be designed using all type of algorithm and almost similar improvements are noted using various optimization algorithm. Although large number of techniques and optimization algorithm are implemented for FIR filter

designed but only some popular are discussed in this paper to understand trends and future scope in digital filter designing.

CONCLUSION

Genetic algorithm, DE, algorithm are good approaches for FIR filter design but PSO is most effective than these algorithms. But if use the basic type algorithms is replaced by hybrid or advanced algorithms then more good results are obtained. This is because of advancement in optimization algorithms which lead to more accuracy in finding of suitable coefficients. So to achieve more improvement in FIR filter design use of more advanced algorithms is appreciated or there is need of devolvement of better performance algorithm by hybridization of exiting algorithm or introducing new type of concepts. However modification in fitness function should also possible. Mixer of both approaches gives more accurate results. Due to this reason FIR filter designs by latest approaches (ADPSO, CSO) achieve best results and these approaches can further extend in future for more improvements in filter designing.

References

[1] Parks, T.W. and McClellan, J.H. (1972), "*A Program For The Design Of Linear Phase Finite Impulse Response Filters*", IEEE Transaction on Audio Electroacoust, vol. 20, 3, pp. 195–199.

[2] McClellan, J.H. and Parks, T.W. (1973), "*A Unified Approach to The Design of Optimum FIR Linear Phase Digital Filters*", IEEE Transaction on Circuit Theory, vol. 20, pp. 697-701.

[3] Suckley, D. (1991), "*Genetic Algorithm in The Design of F IR Filters*", IET Journals and Magazines vol. 138, pp. 234 - 238.

[4] Lee, A., Ahmadi, M., Jullien, G. A., Miller, W. C. and Lashkari, R. S. (1998), "*Digital Filter Design Using Genetic Algorithm*", IEEE International Symposium on Circuits and Systems, Monterey, CA, pp. 34–38.

[5] Benvenuto, N., Marchesi, M. and Uncini, A. (1992), "*Applications of Simulated Annealing For The Design of Special Digital Filters*", IEEE Transaction on Signal Processing, vol. 40, 2, pp. 323–332.

[6] Karaboga, N. and Cetinkaya, B. (2006), "*Design of Digital FIR Filters Using Differential Evolution Algorithm*", Circuits Systems Signal Processing, vol. 25, pp. 649–660.

[7] Karaboga N. (2009), "*A New Design Method Based on Artificial Bee Colony Algorithm For Digital IIR Filters*", Journal of the Franklin Institute, vol. 346, 4, pp. 328–348.

[8] Kennedy, J. and Eberhart, R. (1995), "*Particle Swarm Optimization"*, IEEE International Conference on Neural Networks, Perth, Australia, pp. 1942–1945.

[9] Ababneh JI, Bataineh MH (2008) Linear phase FIR filter design using particle swarm optimization and genetic algorithms. Digit Signal Process 18(4):657–668

[10] Mandal, S., Ghoshal, S.P., Sengupta, D., Kar, R. and Mandal, D.(2012), "*Design of Optimal Linear Phase FIR High Pass Filter Using Improved Particle Swarm Optimization*", International. Journal on Signal & Image Processing, vol. 03, pp. 5-9.

[11] Mukherjee, S., Kar, R., Mdandal, D., Mondal, S. and Ghoshal, S. P. (2011), "*Linear Phase Low Pass FIR Filter Design Using Improved Particle Swarm Optimization*", IEEE Student Conference on Research and Development, Durgapur, India, pp. 358-363.

[12] Vasundhra , Mandal, D., Ghoshal, S.P. and Kar, R. (2013), "*Digital FIR Filter Design Using Fitness Based Hybrid Adaptive Evolution With Particle Swarm Optimization"*, Natural computations, vol. 2, pp. 650-659

[13] Saha, S.K., Mandal, D., Kar, R. and Ghoshal, S.P. (2013), "*Cat Swarm Optimization For Linear Phase FIR Filter Design"*, ISR Transactions,

[Online]. 52(2013), pp.781–794 Available http://dx.doi.org/10.1016/j.isatra.2013.07.009

[14] Ifeachor, E.C. and Jervis, B.W. (2001), "*Digital Signal Processing: A Practical Approach*", Prentice Hall Publishers, U.S.A.

[15] The MathWorks, [Online]. Available http://www.mathworks.com

[16] Nature inspired algorithms, [Online]. Available http://www.scholarpedia.com

A SURVEY PAPER ON SENSITIVE LABEL PRIVACY PROTECTION ON SOCIAL NETWORK

[1]Sandesha Patil,[2]Chiranjivi Kariya ,[3] Priyanka Vandile
Bapuroa Deshmukh Collage of Engineering,sevagram
University of RTMNU at Nagpur
[1]sandesha_2410@rediffmail.com
[2]chiranjivi.kariya@gmail.com

***Abstract* : Sensitive Label and data handling are important issues for social network users. Ideally, access control enforcement should not depend on the social networking provider but should be under the control of the user. We propose a privacy protection scheme that not only prevents the disclosure of identity of users but also the disclosure of selected features in users' profiles also, a graph model where each vertex in the graph is associated with a sensitive label. It makes all requests for private data from third party applications (TPAs) explicit and enables a user to exert fine-grained control over what profile data can be accessed by them. Users can share their access control configurations for TPAs with their friends who can reuse and rate such configurations. The social networks are modeled as graphs in which users are nodes and features are labels. Labels are denoted either as sensitive or as non-sensitive.**

Keyword - Sensitive Label, TPAs, Privacy Management, Cluster

1. INTRODUCTION

Sensitive information about users of the social networks should be protected. The challenge is to devise methods to publish social network data in a form that affords utility without compromising privacy. Previous research has proposed various privacy models with the corresponding protection mechanisms that prevent both inadvertent private information leakage and attacks by malicious adversaries. These early privacy models are mostly concerned with identity and link disclosure. The social networks are modeled as graphs in which users are nodes and social connections are edges. The threat Definition and protection mechanisms leverage structural properties of the graph. This paper is motivated by the recognition of the need for a fine grain and more personalized privacy. Users entrust social networks such as Facebook and LinkedIn with a wealth of personal information such as their age, address, current location or political orientation. We refer to these details and messages as features in the user's profile. We propose a privacy protection scheme that not only prevents the disclosure of identity of users but also the disclosure of selected features in users' profiles. An individual user can select which features of her profile. she wishes to conceal. The social networks are modeled as graphs in which users are nodes and features are labels1. Labels are denote either as sensitive or as non-sensitive. Figure 1 is a label graph representing a small subset of such a social network. Each node in

the graph represents a user, and the edge between two nodes represents the fact that the two persons are friends. Labels annotate to the nodes show the locations of users. Each letter represents a city name as a label for each node. Some individuals do not mind their residence being known by the others, but some do, for various reasons. In such case, the privacy of their labels should be protected at data release. Therefore the locations are either sensitive or non-sensitive. (Labels are in red italic in Figure 1). The privacy issue arises from the disclosure of sensitive labels. One might suggest that such labels should be simply deleted. Still,

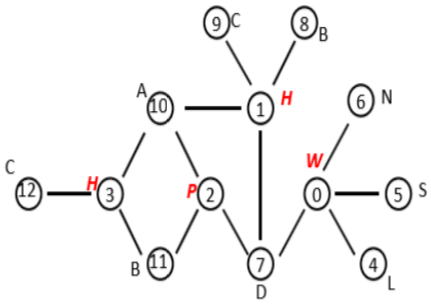

Figure 1. Example of the labeled graph representing a social network

One might suggest that such labels should be simply deleted. Still, such a solution would present an incomplete view of the network and may hide interesting statistical information that does not threaten privacy. A more sophisticated approach consists in releasing information about sensitive labels, while ensuring that the identities of users are protected from privacy threats. We consider such threats as neighborhood attack, in which an adversary Find out sensitive information based on prior knowledge of the number of neighbors of a target node and the labels of these neighbors. In the example, if an adversary knows that a user has three friends and that these friends are in A (Alexandria), B (Berlin) and C (Copenhagen), respectively, then she can infer that the user is in H (Helsinki). We present privacy protection algorithms that allow for graph data to be published in a form such that an adversary cannot safely infer the identity and an adversary cannot safely infer the identity and sensitive labels of users. We consider the case in which the adversary possesses structural knowledge and label +information. The algorithms that we propose transform the original graph into a graph in which any node with a sensitive label is indistinguishable from at least `−1 other nodes. The probability to infer that any node has a

Sensitive nodes) is no larger than 1/`. For this purpose we design `-diversity-like model, where we treat node labels as both part of an adversary's background knowledge and as sensitive information that has to be protected. The algorithms are designed to provide privacy protection while losing as little information and while preserving as much utility as possible. In view of the tradeoff between data privacy and utility [16], we evaluate empirically the extent to which the algorithms preserve the original graph's structure and properties such as density, degree distribution and clustering coefficient. We show that our solution is effective, efficient and scalable while offering stronger privacy guarantees than those in previous research, and that our algorithms scale well as data size grows

2. PROPOSED SYSTEM

In order to concern with social network privacy and data hiding is the major problem. According to existing system, currently available module are profiling and friend request. Profiling consist user (node) private/public data and friend request contain Third party which they want to interact.

In our proposed system, we explorer the two new module name as, privacy option and new graph positioning. In real world there were many privacy option as , only me ,friends of friends, private/public but, in order to used these option still there is problem to often tagged the information and this is obviously violate

privacy and also experienced more revelation. Here we are providing one more facility i.e. make a group within group and finely exchange of data can be possible. Whenever to giving privacy in group it will become more secure and also help to make sure to uploading text or may called information were use by know third party. It is easy to plot graph in group of the friend relationship.

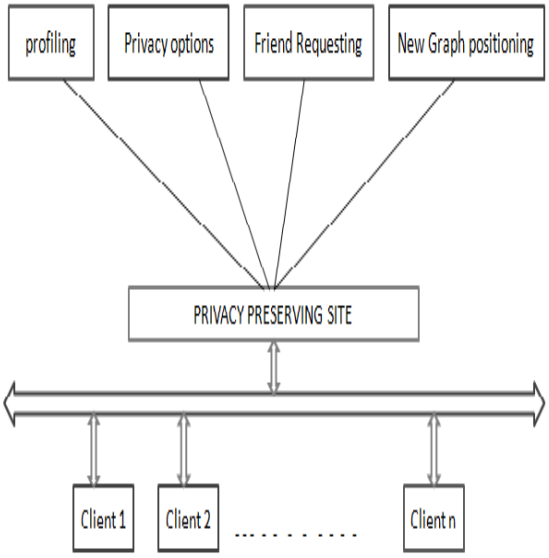

Figure 1 : Privacy preserving network

The social networks are modelled as graphs in which are nodes and features are labels1. Labels are denoted either as sensitive or as non-sensitive.

A. Problem Definition

We model a network as G(V;E;Ls; L**;** Γ**),** where V is a set of nodes, E is s set of edges, Ls is a set of sensitive labels, and L is a set of non-sensitive labels. Γ maps nodes to their labels,Γ : $V \rightarrow L^s \cup L$. Then we propose a privacy model, ℓ-sensitive-label-diversity; in this model, we treat node labels both as part of an adversary's background knowledge, and as sensitive information that has to be protected. These concepts are clarified by the following definitions:

- Definition 1. The neighbourhood information of node v comprises the degree of v and the labels of vs. neighbours.
- Definition 2. (*ℓ`-sensitive-label-diversity*) For each node v that associates with a sensitive label, there must be at least ℓ - 1 other nodes with the same neighbourhood information, but attached with different sensitive labels.

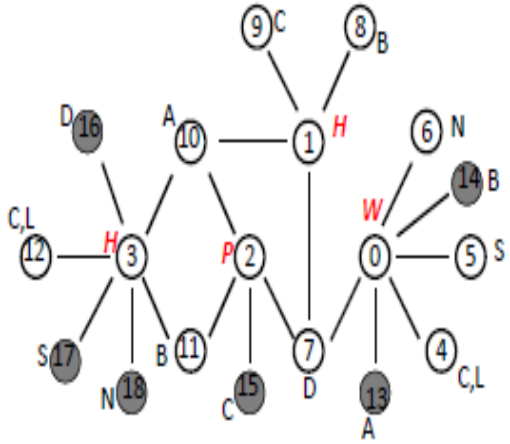

Figure 2 .Privacy-attaining network examples.

In Example 1, nodes 0, 1, 2, and 3 have sensitive labels. The neighbourhood information of node 0, includes its degree, which is 4, and the labels on nodes 4, 5, 6, and 7, which are L, S, N, and D, respectively. For node 2, the neighbourhood information includes degree 3 and the labels on nodes 7, 10, and 11, which are D, A, and B. The graph in Figure 2 satisfies sensitive label-diversity that is because, in this graph, nodes 0 and 3 are indistinguishable, having six
neighbours with label A, B,{ C,L}, D, S, N separately; likewise, nodes 1 and 2 are

indistinguishable, as they both have four neighbours with labels A, B, C, D separately.

B. Algorithm

We want to group nodes with as similar neighbourhood information as possible so that we can change as few labels as possible and add as few noisy nodes as possible. In the first run, two nodes with the maximum similarity of their neighbourhood labels are grouped together. Their neighbour labels are modified to be the same immediately so that nodes in one group always have the same neighbour labels. For two nodes, v1 with neighbourhood label set (LSv1), and v2 with neighbourhood label set (LSv2), we calculate neighbourhood label similarity (NLS) as follows :

$$NLS(v_1, v_2) = \frac{|LS_{v_1} \cap LS_{v_2}|}{|LS_{v_1} \cup LS_{v_2}|} \quad \text{……....(1)}$$

Larger value indicates larger similarity of the two neighbourhoods. Then nodes having the maximum similarity with any node in the group are clustered into the group till the group has ℓ nodes with different sensitive labels. Thereafter, the algorithm proceeds to create the next group. If fewer thanℓnodes are left after the last group's formation, these remainder nodes are clustered into

Existing groups according to the similarities between nodes and groups. After having formed these groups, we need to ensure that each group's members are indistinguishable in terms of neighbourhood information. Thus, neighbourhood labels are modified after every grouping operation, so that labels of

Nodes can be accordingly updated immediately for the next grouping operation. This modification process ensures that all nodes in a group have the same neighbourhood information.

The objective is achieved by a series of modification Operations. To modify graph with as low information loss as possible, we devise three modification operations: label union, edge insertion and noise node addition.

Label union and edge insertion among nearby nodes are preferred to node addition, as they incur less alteration to the overall graph structure. if there are nodes in a group still having different neighbourhood information, noise nodes with non-sensitive labels are added into the graph so as to render the nodes in group indistinguishable in terms of their neighbours' labels.

We consider the unification of two nodes' neighbourhood labels as an example. One node may need a noisy node to be added as its immediate neighbour since it does not have a neighbour with certain label that the other node has; such a label on the other node may not be modifiable, as its already connected to another sensitive node.

3. LITERATURE REVIEW

IEEE Transactions on Parallel and Distributed Systems Vol: pp no:99 Year 2013. Implemented the concept of SocialTube: P2P-assisted Video Sharing in Online Social Networks worked by Haiying Shen, Ze Li, Yuhua Lin. i,e, client/Server architecture deployed by Current video sharing system in Social network most a large amount of Resource for service provider and lack of scalability. Hence most of the video view are drive by Social relationship and rest of drive by Interest and viewer of the same video tend to reside in the same location. Based on their observation, they proposed SocialTube a system that was explores a Social relationship, SocialTube can provide a low video Start-up delay and low server Traffic. in this topic SN – Based Chunk Peftching Algorithm was implemented.

IEEE Transactions on Knowledge and Data Engineering VOL: 25 NO: 2 YEAR 2013 on Preventing Private Information Inference Attacks on Social Networks was proposed by Raymond Heatherly, Murat Kantarcioglu, Bhavani Thuraisingham. This was the first paper that discussed the problem of sanitizing a social network to prevent inference of social network data and then Examine the effectiveness of those approaches on a real-world dataset. In order to protect privacy, i,e, deleting some information from a user's profile and removing links between friends. they had presented a modification of the Naıve Bayes classification algorithm that wasl use details about a node, and link structure, to predict private details. The network consists of only nodes and edges. Trait details are not included. The goal of the attacker is to simply identify people.

International Conference On Distributed Computing Systems Year 2013 on Privacy Preserving Friending in Social Networks by Lan Zhang, Xiang-Yang Li. Their mechanisms establish a secure communication channel between the initiator and matching users at the time when the matching user is found.. This method was encryption based. The main idea of our mechanism is to use the request profile as a key to encrypt a message. Only a matching user, who shares the secret, can decrypt the message with his/her profile efficiently.

International Conference on Emerging Topics In Computing Vol: 1 no: 1 Year 2013 was implemented on Fairness-aware and Privacy-Preserving Friend Matching Protocol in Mobile Social Networks by Haojin Zhu, Suguo Du, Muyuan Li and Zhaoyu Gao. In this paper, they proposed their privacy-preserving and fairness-aware interest and profile matching protocol, which allows one party to match its interest with the profile of another, without revealing its real interest and profile and vice versa. The protocol proposed in this paper was based on Paillier's homomorphic encryption

IEEE Transactions on Social Networking Year 2013 on Outsourcing Privacy-Preserving Social Networks to a Cloud was implemented by Guojun Wang, Qin Liu, Feng Li, Shuhui Yang and Jie Wu The main design goal of their work was to reduce the probability of a social actor being re-identified while publishing social networks to a cloud In this paper, they were identify a novel type of privacy attack, termed 1*neighbourhood attack, where an attacker is assumed to know the degrees of the they consider a system that consists of a publisher, a cloud service provider.

IEEE confrerence paper 2013 on Game Theoretic Analysis of Multiparty Access Control in Online Social Networks presented by Hongxin Hu, Hongxin Hu, Ziming Zhao , they were explored that a multiparty Access Control (MPAC) model was recently proposed, including a systematic approach to identify and resolve privacy conflicts for collaborative data sharing in OSNs. In this paper, They take another step to further study the problem of analyzing the strategic behaviour of rational controllers in multiparty access control, where each controller aims to maximize her/his own benefit by adjusting her/his privacy setting in collaborative data sharing in OSNs.

IEEE International Confrence on Pervasive Computing and Communication Workshop 2010 on topic Relationship-based Access Control for Online Social Networks: Beyond User-To-User Relationships was presented by Yuan Cheng, Jaehong Park and Ravi Sandhu to ensure that U2U relationship. In this paper, they developed a relationship-based access control model for OSNs that incorporates not only U2U relationships but also user-to-resource (U2R) and resource-toresource (R2R) relationships. Furthermore, while most access control proposals for OSNs only focus on controlling users' normal usage activities, their model also

captures controls on users' administrative activities. Authorization policies are defined in terms of patterns of relationship paths on social graph and the hopcount limits of these path.

IEEE Transactions On Social Networking Year 2010 was design paper on Design of a Social Network Based Recommender System for Participatory Media Content by Aaditeshwar Seth, In this paper, they present an overview of our work in sociological theory and user modelling outlines the system design for a recommender system that makes use of this work, describe some open problems, and focus on one component of the System that is strongly grounded in social network theory.

IEEE Transactions In Computing Vol:1 no:1 Year 2008 on NOYB: Privacy in Online Social Networks was proposed by Saikat Guha, Kevin Tang, Paul Francis they proposed the system like NOYB short for none of your business was based on the observation that some online services notably social networking websites can operate on "fake "data. The solution was that user data was first encrypted and the cipher text encoded to look like legitimate data. The online services can operate on the ciphered data, however only authorized users can decode and decrypt the result. A simplistic approach would be to encrypt each atom and share the key with other users authorized to view that atom. While such a scheme does not reveal any users information to the online services.

IEEE Transactions on Knowledge and Data Engineering Vol: 26 no: 2 Year 2014 on Supporting Privacy Protection in Personalized Web Search by Lidan Shou, He Bai, Ke Chen, and Gan Chen and proposed system i,e, Personalized web search (PWS) has demonstrated its effectiveness in improving the quality of various search services on the Internet. They propose a PWS framework called UPS that can adaptively generalize profiles by queries while respecting user specified privacy requirements. They also provide an online prediction mechanism for deciding whether personalizing a query is beneficial.

Workshop on Privacy in the Electronic Society (WPES), 2005.
on paper Information Revelation and Privacy in Online Social Networks by Ralph Gross, H. John Heinz they was proposed paper based on the information they provide online, users expose themselves to various physical and cyber risks, and make it extremely easy for third parties to create digital dossiers of their behavior. These risks are not unique to the Facebook. However, the Facebook's public linkages between an individual profile and the real identity of its owner, and the Facebook's perceived connection to a physical and ostensibly bounded community (the campus), make Facebook users a particularly interesting population for our research.

International Journal of Computer Science and Mobile Applications, Vol.2 Issue. 1, January-2014 was presented paper on Securing Sensitive Information in Social Network Data Anonymization by Mr. A.Stalin Irudhaya Raj, Ms. N.Radhika. To secure sensitive Information in social network data anonymization using k-degree-l-diversity anonymity model. The disadvantages of the existing system were that it Simply removing the identifiers in social networks does not guarantee privacy. In this paper k-degree anonymity with l-diversity to prevent not only the reidentification of individual nodes but also the revelation of a sensitive attribute associated with each node.

4. CONCLUSION AND RESULT

From above survey paper, we conclude that, it is must to hide the sensitive data from thirty party application (TPAs). We propose a privacy protection scheme that not only prevents the disclosure of identity of users but also the disclosure of selected features in users' profiles

also our approach in maintaining critical graph properties while providing a comprehensible privacy guarantee. Our future work includes how to investigate more security and privacy issues in mobile social networks.

REFERENCE :

[1]http://www.symantec.com/connect/blogs/facebookapplications-accidentally-leaking-access-third-parties.

[2] Gionis A.; Tassa, T, IEEE Knowledge and data engineering 2009.*K anonymization with minimal loss of information.*

[3] Hogben Giles. Security issues and recommendations for online social networks. ENISA Position Paper N.1; 2007. IEEE. W2SP 2008. *Web 2.0 security and privacy*; 2008.

[4]R.Shokri, G. Theodorakopoulos, C. Troncoso, J.-P. Hubaux, and J.- Y. Le Boudec. Protecting location privacy: Optimal strategy against localization attacks. in Proc. of ACM CCS'12, pp.617- 627, 2012.

[5] R. Singh, M. Sumeeth, and J. Miller. A user-centric evaluatio of the readability of privacy policies in popular web sites. Information Systems Frontiers, pages 1{14, 2010
.

[6]P. Anthonysamy, A. Rashid, and P. Greenwood. Do the privacy policies reect the privacy controls on social networks? IEEE *International Conference on Privacy*, Security, Risk and Trust, 2011 IEEE International Conference on, 2011

[7]G. Wang, Q. Liu, and J. Wu, "*Hierarchical attribute-based encryption for fine-grained access control in cloud storage ervices,"* in Proceedings of ACM CCS, 2010.

[8]QI, Y., AND ATALLAH, M. Efficient privacy-preserving k-nearest neighbor search. In *IEEE ICDCS*, 2008, pp. 311–319.

[9]B. Li, M. Ma, Z. Jin, and D. Zhao. Investigation of a large-scale P2P VoD overlay network by measurements. *Peer-to-Peer* Networking and Applications, 5(4):398–411, 2012.

[10] CHASE, M. Multi-authority attribute based encryption. *Theory* of Cryptography, 2010, pp. 515–534.

[11] A. Seth and J. Zhang, "A Social Network Based Approach to Personalized Recommendation of Participatory Media Content" ICWSM, 2008.

[12] DE CRISTOFARO, E., AND TSUDIK, G. Practical private set intersection protocols with linear complexity. *Financial Cryptography and Data Security*, 2010, pp. 143–159.

[13] STAJANO, F., AND ANDERSON, R. The resurrecting duckling: Security issues for ad-hoc wireless networks. In Security Protocols, 2011, pp. 172–182

[14] DE CRISTOFARO, E., AND TSUDIK, G. Practical private set intersection protocols with linear complexity. *Financial Cryptography and Data Security*, 2010, pp. 143–159.

[15] YE, Q., WANG, H., AND PIEPRZYK, J. Distributed private matching and set operations. *Information Security Practice and Experience*, 2008, pp. 347–360.

[16] A. Seth and J. Zhang, "*A Social Network Based Approach to Personalized Recommendation of Participatory Media Content*," ICWSM, 2008.

SURVEY PAPER ON GIVING PRIVACY TO SENSITIVE LABELS

[1]Ashish Bundele, [2]Anuja Ghotkar, [3]Shimpli Dhale
Computer Engineering Department
Bapurao Deshmukh Collage of Engineering, Sevagram
University of RTMNU,Nagpur
[1]ashishbundile@gmail.com,[2]dhaleshimpli@gmail.com,[3]ghotkaranuja@gmail.com

***Abstract*: Sensitive Label and data handling are important issues for social network users. Ideally, access control enforcement should not depend on the social networking provider but should be under the control of the user. We propose a privacy protection scheme that not only prevents the disclosure of identity of users but also the disclosure of selected features in users' profiles also, a graph model where each vertex in the graph is associated with a sensitive label. It makes all requests for private data from third party applications (TPAs) explicit and enables a user to exert fine-grained control over what profiles data can be accessed by them. Users can share their access control configurations for TPAs with their friends who can reuse and rate such configurations. The social networks are modeled as graphs in which users are nodes and features are labels. Labels are denoted either as sensitive or as non-sensitive**.

***Keyword* - Sensitive Label, TPAs, Privacy Management, Cluster**

I. INTRODUCTION

We must protect the sensitive labels of users on social network site. Here, the challenge is that to devise methods to publish social network data in a form that affords utility without compromising privacy. Various privacy models with the corresponding protection mechanisms that prevent both inadvertent private information leakage and attacks by malicious adversaries have been previously proposed in research. These early privacy models are mostly concerned with identity and link disclosure. The social networks are modeled as graphs in which users are nodes and social connections are edges. The threat Definition and protection mechanisms leverage structural properties of the graph. This paper is motivated by the recognition of the need for a fine grain and more personalized privacy.

Users entrust social networks such as Facebook and LinkedIn with a wealth of personal information such as their age, address, current location or political orientation. We refer to these details and messages as features in the user's profiles. We propose a privacy protection scheme that not only prevents the disclosure of identity of users but also the disclosure of selected features in users' profiles. An individual user can select which features of her profiles she wishes to conceal. The social networks are modeled as graphs in which users are nodes and features are labels1. Labels are denoted either as sensitive or as non-sensitive. Figure 1 is a labeled graph representing a small subset of such a social network. Each node in the graph represents a user, and the edge between two nodes represents the fact that the two persons are friends. Labels annotated to the nodes show the locations of users. Each letter represents a city name as a label for each node. Some individuals do not mind their residence being known by the others, but some do, for various reasons. In such case, the privacy of their labels should be protected at data release. Therefore the locations are either sensitive or non-sensitive. (Labels are in red italic in Figure 1). The privacy issue arises from the

disclosure of sensitive labels. One might suggest that such labels should be simply deleted.

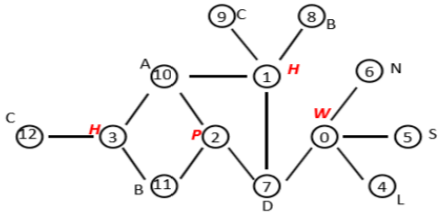

Figure 1. Example of the labeled graph representing a social network

One might suggest that such labels should be simply deleted. Still, such a solution would present an incomplete view of the network and

We present privacy protection algorithms that allow for graph data to be published in a form such that an adversary cannot safely infer the identity and an adversary cannot safely infer the identity and sensitive labels of users. We consider the case in which the adversary possesses structural knowledge and label information. The algorithms that we propose transform the original graph into a graph in which any node with a sensitive label is indistinguishable from at least `−1 other nodes. The probability to infer that any node has a certain sensitive label (we call such nodes Sensitive nodes) is no larger than 1/`. For this purpose we design `-diversity-like model, where we treat node labels as both part of an adversary's background knowledge and as sensitive information that has to be protected. The algorithms are designed to provide privacy protection while losing as little information and while preserving as much utility as possible. In view of the tradeoff between data privacy and utility [16], we evaluate empirically the extent to which the algorithms preserve the original graph's structure and properties such as density, degree distribution and clustering coefficient. We show that our solution is effective, efficient and scalable while offering stronger privacy guarantees than those in previous research, and that our algorithms scale well as data size grows. may hide interesting statistical information that does not threaten privacy. A more sophisticated approach consists in releasing information about sensitive labels, while ensuring that the identities of users are protected from privacy threats. We consider such threats as neighborhood attack, in which an adversary find out sensitive information based on prior knowledge of the number of neighbors of a target node and the labels of these neighbors. In the example, if an adversary knows that a user has three friends and that these friends are in A (Alexandria), B (Berlin) and C (Copenhagen), respectively, then she can infer that the user is in H (Helsinki).As shown in the above fig 1.

II. PROPOSED SYSTEM

In order to concern with social network privacy and data hiding is the major problem. According to existing system, module called profiling and friend request two model are already implemented. Profiling consist user (node) private/public data, friend request contain Third party application which they want to concern.

In our proposed system, we explorer the two new module name as, privacy option and new graph positioning. In real world there were many privacy option as , only me ,friends of friends, private/public but, in order to used these option still there is problem to often tagged the information and this is obviously violate privacy and also experienced were more revelation. Here we are providing one more facility i.e. make a group within group and finely exchange of data can be possible. Whenever to give privacy in group it will become more secure also help to make sure that uploading text or may called information were use by know third party. It is easy to plot graph in group of the friend relationship.

In the current system profiling and friend requesting these two options are already present and we should develop two new options that are privacy option and new graph positioning option.

Using privacy option user can select any disclosure of his profile which he wants to conceal. And using new graph positioning option we should create a cluster and mountain it on internally plotted graph so that our system work properly and there is no issue of privacy and security. In our proposed system we may add N-number of clients. The following figure shows the proposed system.

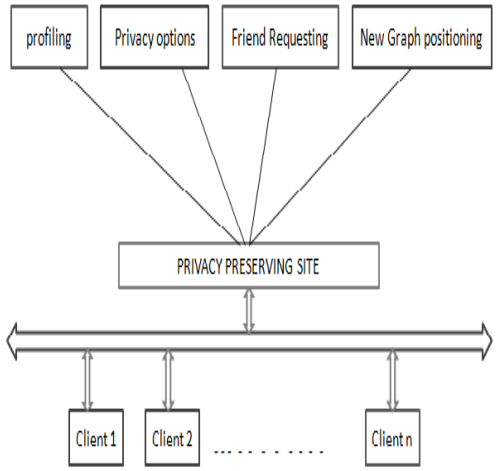

Figure 1: Privacy preserving network

The social networks are modelled as graphs in which are nodes and features are labels1. Labels are denoted either as sensitive or as non-sensitive.

III. ALGORITHIM

The main objective of the algorithms that we propose is to make suitable grouping of nodes, and appropriate modification of neighbours' labels of nodes of each group to satisfy the l-sensitive-label-diversity requirement. We want to group nodes with as similar neighbourhood information as possible so that we can change as few labels as possible and add as few noisy nodes as possible. We propose an algorithm, Global-similarity-based Indirect Noise Node (GINN) that does not attempt to heuristically prune the similarity computation as the other two algorithms, Direct Noisy Node Algorithm (DNN) and Indirect Noisy Node Algorithm (INN) do. Algorithm DNN and INN, which we devise first, sort nodes by degree and compare neighbourhood information of nodes with similar degree. Details about algorithm DNN and INN please refer to [15]

Larger value indicates larger similarity of the two neighbourhoods. Then nodes having the maximum similarity with any node in the group are clustered into the group till the group has ℓ nodes with different sensitive labels. Thereafter, the algorithm proceeds to create the next group. If fewer than ℓ nodes are left after the last group's formation, these remainder nodes are clustered into Existing groups according to the similarities between nodes and groups. After having formed these groups, we need to ensure that each group's members are indistinguishable in terms of neighbourhood information. Thus, neighbourhood labels are modified after every grouping operation, so that labels of

Nodes can be accordingly updated immediately for the next grouping operation. This modification process ensures that all nodes in a group have the same neighbourhood information. The objective is achieved by a series of modification Operations. To modify graph with as low information loss as possible, we devise three modification operations: label union, edge insertion and noise node addition.

Label union and edge insertion among nearby nodes are preferred to node addition, as they incur less alteration to the overall graph structure. If there are nodes in a group still having different neighbourhood information, noise nodes with non-sensitive labels are added into the graph so as to render the nodes in group indistinguishable in terms of their neighbours' labels?

Global-Similarity-based Indirect Noise Node Algorithm

Input: graph G(V,E,L,Ls), parameter l;
Result: Modified Graph G'

```
1  while Vleft > 0 do
2      if |Vleft| ≥ l then
3          compute pairwise node similarities;
4          group G ← v1,v2 with Maxsimilarity;
5          Modify neighbors of G;
6          while |G| < l do
7              dissimilarity(Vleft,G);
8              group G ← v with Maxsimilarity;
9              Modify neighbors of G without actually
               adding noisy nodes ;
10     else if |Vleft| < l then
11         for each v ∈ Vleft do
12             similarity(v,Gs);
13             GMax similarity ← v;
14         Modify neighbors of GMax similarity without actually
           adding noisy nodes;
15 Add expected noisy nodes;
16 Return G'(V' ,E' ,L');
```

In this algorithm, noise node addition operation that is expected to make the nodes inside each group satisfies sensitive-label-diversity are recorded, but not performed right away. Only after all the preliminary grouping operations are performed, the algorithm proceeds to process the expected node addition operation at the final step. Then, if two nodes are expected to have the same labels of neighbours and are within two hops (having common neighbours), only one node is added. In other words, we merge some noisy nodes with the same label, thus resulting in fewer noisy nodes.

IV. LITERATURE REVIEW

2012 IEEE International Conference on Pervasive Computing and Communications Workshops[1] on Access Control in Decentralized Online Social Networks: Applying a Policy-Hiding Cryptographic Scheme and Evaluating Its Performance presented by Oleksandr Bodriagov, Gunnar Kreitz, and Sonja Buchegger suggested that Privacy concerns in online social networking services had prompted a number of proposals for decentralized online social networks (DOSN) that remove the central provider and aim at giving the users control over their data and who can access it. This was usually done by cryptographic means. Existing DOSNs used cryptographic primitives that hide the data but revealed the access policies. At the same time, there were privacy-preserving variants of those cryptographic primitives that did not reveal access policies. They were, however, not suitable for usage in the DOSN context because of performance or storage constraints.

33rd International Conference on Distributed Computing System Year 2012[2] on Message in a Sealed Bottle: Privacy Preserving Friending in Social Networks presented by Lan Zhang∗, Xiang-Yang Li proposed that in this paper, they designed novel mechanisms, when given a preference-profile submitted by a user, that searched a person with matching-profile in decentralized multi-hop mobile social networks. There mechanisms were privacy-preserving: no participants' profile and the submitted preference-profiles were exposed. There mechanisms established a secured communication channel between the initiator and matching users at the time when the matching user was found. There rigorous analysis shows that there mechanism was secured, privacy-preserving, veritable, and efficient both in communication and computation. Extensive evaluations using real social network data, and actual system implementation on smart phones show that there mechanisms were significantly more efficient then existing solutions.

2011 IEEE International Conference[3] on Collaborative Privacy Management for Third-Party Applications in Online Social Networks presented by Pauline Anthonysamy, Awais Rashid proposed that Privacy control mechanisms for online social networks (OSNs)

offered little by way of managing access to a user's personal information by third-party applications (TPAs). Most OSNs provide an "accept all or nothing" mechanism for managing permissions from TPAs to access a user's private data. In this paper, they proposed an approach that makes all requests for private data from TPAs explicit and enables a user to exert fine-grained access control over what profile data can be accessed by individual applications. Equally importantly, there approach also allows users to shared their access control configurations for TPAs with their friends who can reused and rate such configurations. This was particularly beneficial to novice users or those new to a particular TPA or an OSN. They presented an implementation of their approach for managing privacy for third-party Facebook applications.

2011 IEEE International Conference[4] on Measuring Privacy Risk in Online Social Networks presented by Justin Becker, Hao Chen suggested in that paper the PrivAware, a tool to detected and report unintended information loss in online social net- works. Their goal is to provide a rudimentary framework to identify privacy risk and provide solutions to reduce information loss. The first instance of the software is focused on information loss attributed to social circles. In subsequent released they intended to incorporate additional capabilities to captured ancillary threat models. From there initial results, they quantify the privacy risk attributed to friend relationships in Facebook. They show that for each user in our study a majority of their personal attributes can be derived from social contacts. Moreover, they present results denoting the number of friends contributing to a correctly inferred attribute.

2012 IEEE International Conference[5] on Enforcing Access Control in Social Network Sites presented by Filipe Beato, Markulf Kohlweiss, and Karel Wouters proposed that l, SNS platform-independent solution, for social network users to control their data. We develop concepts that are general enough to describe access control restrictions for deferent SNS platforms. Our architecture uses encryption to enforce ac- cess control for users' private information based on their privacy preferences. We have implemented our model as a Firefox extension.

2009 IEEE International Conference [6] on Preserving Privacy in Social Networks against Neighbourhood Attacks presented by Bin Zhou Jian Pei, they take an initiative towards preserving privacy in social network data. They identify an essential type of privacy attacks: neighbourhood attacks. If an adversary had some knowledge about the neighbours of a target victim and the relationship among the neighbours, the victim may be re-identified from a social network even if the victim's identity is preserved using the conventional anonymization techniques. They show that the problem is challenging, and present a practical solution to battle neighborhood attacks. The empirical study indicates that anonymized social networks generated by our method can still be used to answer aggregate network queries with high accuracy.

2009 IEEE International Conference [7] on Privacy-Preserving P2P Data Sharing with One Swarm presented by Tomas Isdal, Thomas Anderson suggested a new design point in trade off between privacy and performance. They describe the design and implementation of a new P2P data sharing protocol, called One Swarm, that provides users much better privacy than Bit Torrent and much better performance than Tor or Freenet. A key aspect of the One Swarm design is that users have explicit configurable control over the amount of trust they place in peers and in the sharing model for their data: the same data can be shared publicly, anonymously, or with access control, with both trusted and untrusted peers. One- Swarm's novel lookup and transferred techniques yield a median factor of 3.4 improvements in download times relative to Tor and a factor of 6.9 improvements relative to Freenet. One Swarm is publicly available and has been downloaded by hundreds of thousands of users since it's released.

2011 IEEE International Conference[8] on Multiparty Access Control for Online Social Networks: Model and Mechanisms presented by Hongxin Hu, Gail-Joon Ahn proposed in this paper, that we proposed an approach to enable the protection of shared data associated with multiple users in OSNs. They formulate an access control model to capture the essence of multiparty authorization requirements, along with a multiparty policy specification scheme and a policy enforcement mechanism. Besides, they present a logical representation of our access control model which allows them to leverage the features of existing logic solvers to perform various analysis tasks on our model. They also discuss a proof-of-concept prototype of our approach as part of an application in Facebook and provide usability study and system evaluation of our method.

IEEE Transaction on parallel and distributed system vol:24 No:12year 2011[9], on Sybil Defender: Defend Against Sybil Attacks in Large Social Networks presented by WeiWei∗, Fengyuan Xu∗, Chiu C. Tan†, Qun Li∗ suggest that they present SybilDefender, a scheme that leverages the network topologies to defend against sybil attacks in large social networks. There evaluation shows that SybilDefender can correctly identify the sybil nodes even when the number of sybil nodes introduced by each attack edge approaches the theoretically detectable lower bound, and it can effectively detect the sybil community surrounding a sybil node with different sizes and structures.

2008 IEEE International Conference[10] CoPE: Enabling Collaborative Privacy Management in Online Social Networks presented by Anna Squicciarini, Xiaolong (Luke) Zhang, suggested that This paper presents a prototype system and a preliminary study on the perceptions of the usefulness and usage of the system. In addition to extending the design space of image-related privacy management, this research also suggests a general approach for privacy protection in online social networks (OSNs).

V.CONCLUSION

In this paper we have investigated the protection of private label information in social network data publication. We consider graphs with rich label information, which are categorized to be either sensitive or non-sensitive. We assume that adversaries possess prior knowledge about a node's degree and the labels of its neighbors, and can use that to infer the sensitive labels of targets. We suggested a model for attaining privacy while publishing the data, in which node labels are both part of adversaries' background knowledge and sensitive information that has to be protected. We accompany our model with algorithms that transform a network graph before publication, so as to limit adversaries' confidence about sensitive label data. Our experiments on both real and synthetic data sets con- firm the effectiveness, efficiency and scalability of our approach in maintaining critical graph properties while providing a comprehensible privacy guarantee.

VI. References

[1] L. A. Adamic and N. Glance. The political blogosphere and the 2004 U.S. election: divided they blog. In LinkKDD, 2005.

[2] L. Backstrom, C. Dwork, and J. M. Kleinberg. Wherefore art thou R3579X?: anonymized social networks, hidden patterns, and structural steganography. Com-mun. ACM, 54(12), 2011.

[3] S. Bhagat, G. Cormode, B. Krishnamurthy, and D. S. and. Class-based graph anonymization for social network data. PVLDB, 2(1), 2009.

[4] A. Campan and T. M. Truta. A clustering approach for data and structural anonymity in social networks. In PinKDD, 2008.

[5] J. Cheng, A. W.-C. Fu, and J. Liu. K-isomorphism: privacy-preserving network publication against structural attacks. In SIGMOD, 2010.

[6] G. Cormode, D. Srivastava, T. Yu, and Q. Zhang. Anonymizing bipartite graph data using safe groupings. PVLDB, 19(1), 2010.

[7] S. Das, ¨O. Egecioglu, and A. E. Abbadi. Anonymizing weighted social network graphs. In ICDE, 2010.

[8] A. G. Francesco Bonchi and T. Tassa. Identity obfuscation in graphs through the information theoretic lens. In ICDE, 2011.

[9] M. Hay, G. Miklau, D. Jensen, D. Towsley, and P. Weis. Resisting structural re-identification in anonymized social networks. PVLDB, 1(1), 2008.

[10] Y. Li and H. Shen. Anonymizing graphs against weight-based attacks. In ICDM Workshops, 2010.

[11] K. Liu and E. Terzi. Towards identity anonymization on graphs. In SIGMOD, 2008.

[12] L. Liu, J. Wang, J. Liu, and J. Zhang. Privacy preserving in social networks against sensitive edge disclosure. In SIAM International Conference on Data Mining, 2009.