JOURNAL OF CRITICAL REVIEWS

ISSN- 2394-5125 VOL 7, ISSUE 15, 2020

A PRIVACY PRESERVATION ANALYSIS ON EDGE WEIGHTED GRAPHS OF SOCIAL NETWORKS USING LAPLACE NOISE IMPLEMENTATION

SHARATH KUMAR JAGANNATHAN[1], SATHYARAJASEKARAN K[2], J.V.THOMAS ABRAHAM[3]

[1,2,3]School of Computer Science and Engineering, Vellore Institute of Technology, Chennai, India.
E-mail: sharathkumar.j@vit.ac.in

Received: 28.04.2020 Revised: 29.05.2020 Accepted: 25.06.2020

Abstract— Interpersonal interaction locales like Flickr, Orkut, Fb locate their significant use on web. These person to person communication locales allow a viable way of information sharing and informing functionalities among the clients . The assessment on informal communication diagrams might be made from such well known destinations .A whole know-how of long range interpersonal communication charts are fundamental to consider the bleeding edge front line frameworks and likewise change of recently outlined person to person communication locales .On this paper we can talk roughly the predetermined take a gander at and assessment of the long range informal communication diagrams with their individual sites and around the security upkeep norms . We take a gander at actualities amassed from four popular on-line informal organizations: flickr, youtube, livejournal, and orkut. We slithered the openly reachable client hyperlinks on each site, acquiring a major bit of every social group's diagram. Our results confirm the power direction, little worldwide, and sans scale places of on line interpersonal organizations. we contemplate the privacy of every process that is being done in a social network by tracking the graphical pattern of the process and preserving each and every edge weight of the network by laplace noise mechanisms.

Keywords: Edge weights, Laplace distribution, Laplace noise, perturbation, privacy preservation , average estimation.

1 INTRODUCTION

The associations in many systems are not just paired substances, either present or not, but rather have related weights that record their qualities in respect to each other. Late investigations of systems have, overall, avoided such weighted systems, which are frequently seen as being harder to examine than their unweighted partners. Here we call attention to that weighted systems can as a rule be broke down utilizing a basic mapping from a weighted system to an unweighted multigraph, enabling us to apply standard methods for unweighted charts to weighted ones also. We give various cases of the strategy, including a calculation for identifying group structure in weighted systems and a straightforward verification of the most extreme flow– least cut hypothesis.

1.1 EXTREME FLOW– LEAST CUTHYPOTHESIS

The maximum stream/min-cut hypothesis is a hypothesis about weighted systems. It expresses that, in a system where the weights speak to the most extreme permitted stream of a liquid or other product along the edges, the accompanying is valid: The greatest stream that can go between any two vertices is equivalent to the heaviness of the base edge cut set that isolates a similar two vertices**.**

1.2 WEIGHTED AND UN WEIGHTED GRAPHS

We swing now to a very extraordinary inquiry concerning weighted systems, that of group structure. Many systems comprise not of an undifferentiated mass of connected vertices, but rather of unmistakable "groups"— gatherings of vertices inside which the associations are thick yet between which they are sparser. This kind of structure is seen particularly in informal communities, yet in addition in some organic and innovative systems also. An intriguing issue that has pulled in much consideration as of late is that of making a

PC calculation which, when encouraged the topology of a system, can extricate from it the groups in the system, if there are any. The issue is identified with the issue of diagram parceling, which is very much concentrated in software engineering, however calculations for chart apportioning, for example, the Kernighan-Lin calculation [1] or phantom cut [2,3] are not in a perfect world suited to general system investigation: commonly they just separation organizes in two, instead of into a general number of groups, they give no measure of how great the division being referred to is, and sometimes they likewise require the client to determine the sizes of the groups previously they begin. By and large they likewise work just on unweighted systems.

2 PRIVACY PRESERVATION

2.1 PRIVACY

Heaps of helpful information out there, containing significant data. Significant, and sensible, worry about touchy information. Access control alone isn't an answer; we need to comprehend touchy parts of a dataset and distribute our decisions. In this discussion "security" will be tied in with discharging limited yet valuable data about delicate information.

1. Early protection definitions: k-namelessness, l-decent variety, m-invariance
2. A later definition: Privacy preservation.
3. A few applications thereof.

2.2 PRIVACY PRESERVATION TECHNIQUES

The primary goal of protection of information mining is to create information mining techniques without expanding the danger of misusing [4] of the information used to produce those strategies. The vast majority of the methods utilize some type of modification on the first information so as to accomplish the security safeguarding. The modified dataset is realistic for mining and should meet protection prerequisites without losing the [4] advantage of mining.

2.2.1 Randomization

Randomization procedure is a reasonable and productive approach for protection saving information mining (PPDM). With a specific end goal to guarantee the execution [6] of information mining and to protect singular security, this randomization plans should be actualized. The randomization approach ensures the clients' information by letting them subjectively adjust their records previously sharing them, taking without end some evident data and presenting some clamor. A few techniques in randomization are numerical randomization and thing set randomization Noise can be presented either by adding or increasing irregular esteems to numerical records (Agrawal&Srikant, 2000) or by erasing genuine things and including "counterfeit" qualities to the arrangement of properties.

2.2.2Anonymization

To ensure people's personality while discharging touchy data, information holders frequently scramble or expel unequivocal identifiers, for example, names and one of a kind security numbers. Be that as it may, decoded information gives no certification to secrecy. Keeping in mind the end goal to safeguard protection, k-obscurity display has been proposed by Sweeney [10] which accomplishes k-namelessness utilizing speculation and concealment [4], In K-secrecy, it is troublesome for a sham to decide the character of the people in gathering of informational collection containing individual data. Each arrival of information contains each mix of estimations of semi identifiers and that is indistinguishably coordinated to at any rate k-1 respondents [8]. Speculation includes supplanting an incentive with a less particular (summed up) yet semantically dependable esteem. For instance, the age of the individual could be summed up to a range, for example, youth, middle age and grown-up without indicating properly, in order to diminish the danger of recognizable proof. [4] Suppression includes diminish the precision of uses and it doesnot free any data .By utilizing this strategy it lessens the danger of recognizing definite data.

2.2.3 Secure multi-party computation

An option approach in view of the multiparty calculation is that all aspects of private information is truly known to at least one gatherings. Uncovering private information to gatherings, for example, by whom the information is possessed or the person to whom the information alludes to isn't a state of disregarding protection. The issue emerges when the private data is uncovered to some other outsiders. To manage this issue, we utilize a particular type of protection safeguarding disseminated information mining. Gatherings that every know a portion of the private information take an interest in a convention that creates the information mining comes about, [5] that ensures no information things is uncovered to different gatherings. Along these lines the procedure of information mining doesn't cause, or even increment the open door for rupture of security.

2.2.4 Sequential pattern hiding

Successive example concealing strategy [9] is important to disguise touchy examples that can generally be removed from distributed information, without truly influencing the information and the non delicate intriguing examples. [7]Sequential design covering up is a testing issue, since arrangements have more composite semantics than item sets, and calls for proficient arrangements that offer high utility.

3. LAPLACE NOISE

In social networks, the edge weights may reflect the frequency of communication, the price of commercial trade, the intimacy of relationship, and so forth, which are associated with sensitive information. A typical example is an intelligence network, in which edge weights denote the contact frequencies of two institutions. Too-frequent communications may imply potential problems. Another example is a commercial trade network, in which edge weights indicate the transaction price between two companies. Most managers would be reluctant to reveal a commercial secret to their adversaries, due to the fierce competition. Our goal is to protect the edge weights in social networks without leakage while preserving as much utility as possible.

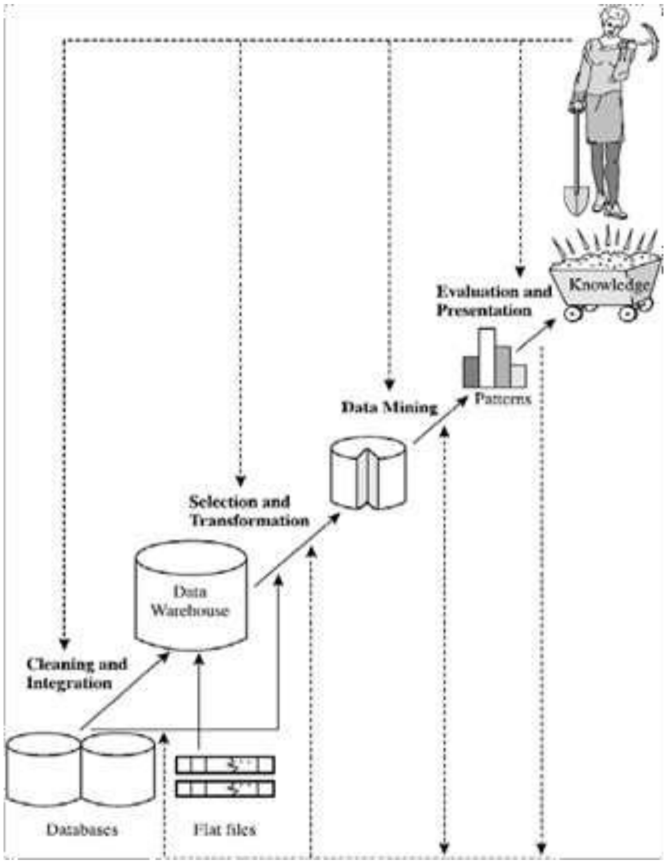
Das et al. [11] considered edge-weight anonymization in social graphs. They built a linear programming (LP) model to preserve the properties of the graph, for example, the shortest paths, -nearest neighbors, and minimum spanning tree, which are expressible as linear functions of the edge weights. Liu et al. [12] considered preserving the weights of some edges, while trying to preserve the shortest-path lengths and exactly the same shortest paths of some pairs of nodes. They developed two privacy-preserving strategies: Gaussian randomization multiplication and a greedy perturbation algorithm based on graph theory. Costea et al. [13] analyzed how privacy preservation can be used to protect the edge weights in graph structures. Our approach is to disturb the edge weights via laplacian noise for protection, which effectively improves the accuracy and utility of the released data.

Laplace noise ways of implementation:

1. Using ``sockpuppets" to hide one's true activities
2. Using a fake identity to create phony information
3. Using security tools to mask one's identity

In science, the Laplace change is an indispensable change named after its pioneer Pierre-Simon Laplace (/ləˈplɑːs/). It takes a component of a genuine variable t (frequently time) to an element of an unpredictable variable s (recurrence).

3.1 PROCESS OF PATTERN GENERATION TO IMPLEMENT LAPLACE NOISE:



3.2 ATTRIBUTES OF PRIVACY PRESERVATION

PPDP for the most part ponders anonymization approaches for distributing valuable information while preserving privacy. Each record comprises of the accompanying 4 sorts of properties:

Identifier (ID): Attributes that can straightforwardly and particularly distinguish an individual, for example, name, ID number and versatile no.

Semi identifier (QID): Attributes that can be connected with outer information to re-distinguish singular records, for example, sex, age and postal district.

Touchy Attribute (SA): Attributes that an individual needs to cover, for example, ailment and pay.

Non-touchy Attribute (NSA): Attributes other than ID,QID and SA

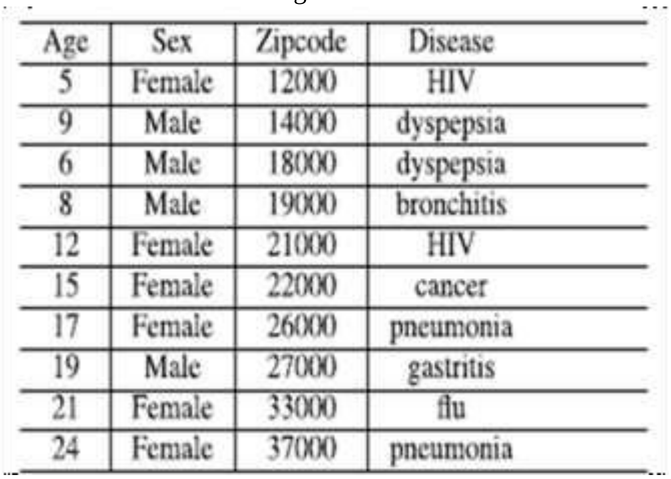
The 4 sort of customers in Data Mining process-

- Data Provider: The customer who asserts a couple of data that are needed by the data mining errand.

- Data Collector: The customer who assembles data from data providers and a short time later convey the data to the data excavator.
- Information Miner: The customer who performs data mining assignments on the data.
- Decision Maker: The customer who settles on decisions in light of the data mining achieves demand to fulfill certain targets

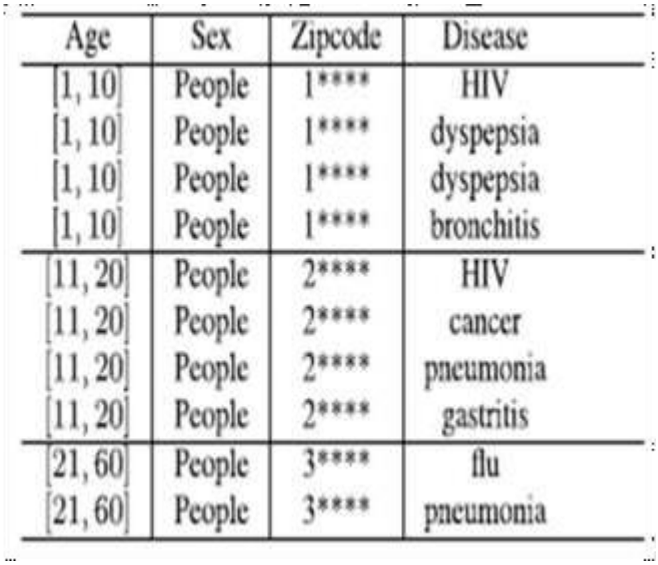
3.3 EXAMPLE FOR ORIGINAL TABLE VALUES VS LAPLACE IMPLEMENTED TABLE:

Original table:



Age	Sex	Zipcode	Disease
5	Female	12000	HIV
9	Male	14000	dyspepsia
6	Male	18000	dyspepsia
8	Male	19000	bronchitis
12	Female	21000	HIV
15	Female	22000	cancer
17	Female	26000	pneumonia
19	Male	27000	gastritis
21	Female	33000	flu
24	Female	37000	pneumonia

After laplace implementation:



Age	Sex	Zipcode	Disease
[1, 10]	People	1****	HIV
[1, 10]	People	1****	dyspepsia
[1, 10]	People	1****	dyspepsia
[1, 10]	People	1****	bronchitis
[11, 20]	People	2****	HIV
[11, 20]	People	2****	cancer
[11, 20]	People	2****	pneumonia
[11, 20]	People	2****	gastritis
[21, 60]	People	3****	flu
[21, 60]	People	3****	pneumonia

4. LAPLACE NOISE IMPLEMENTATION BY LAPLACE DISTRIBUTION METHOD

Laplace noise formula:

$x = \mu-\beta \text{signum}(\alpha) \ln(1-2|\alpha|)$

Terms and definitions:

μ - mean of edges
β - 1/N summation $(x_i - \mu)$
Sgn(α)= d/dx $|\alpha|$ where x!=0
α = weight of the choosen edge
W*= |Worg(1-X)|

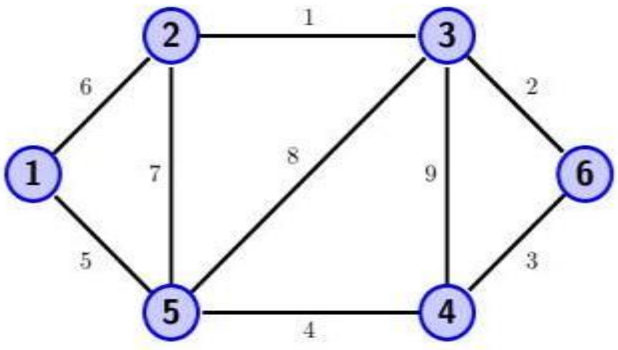


Fig 1: A sample edge weighted graph

The weight of the edges between two vertices is determined by the importance of the process that is being done in that interval (ie)

Consider the above edge weighted graph (fig1) to be a pattern of logging into a social network site like Facebook and performing some operations. In the above pattern the edge between the vertices 3 to 4 has the highest value which represents the user performance of some critical operations like changing password, editing the privacy settings, deleting some sensitive information etc. So to protect the same information of the process that is being done the edge weight between the vertices 3 to 4 will be altered or masked ,such that even if there is a breach of data the third party organization will not be able to trace the originality of the data which is masked. So lets consider the steps involved in masking the edge weight of between the vertices 3 and 4.

Step 1: Determine the value of μ where it mean value of all the edges of the pattern of generated graph.

$$\mu = \frac{\text{sum of all the edge weights}}{\text{total number of edges}}$$

$$\mu = \frac{(6+1+2+3+4+5+7+8+9)}{9}$$

$\mu = 45/9 = 5$

Step 2: Determine the value of the laplacian parameter β

Where $\beta = (1/N) * \sum(xi - \mu)$

N = number of edges

Xi= weight of all the edges

So calculate $\sum(xi - \mu)$,

$\sum(xi - \mu) =$

$(6-5)+(1-5)+(2-5)+(3-5)+(4-5)+(5-5)+(7-5)+ (8-5)+ (9-5)$

$\sum(xi-\mu) = 0$

Hence $\beta = 0$

Since the laplacian parameter is zero, the rest of the terms become zero . The laplacian noise in this case will be equal to the mean value of all the edges,

$X = \mu - \beta \text{ signum}(\alpha) \ln(1-2|\alpha|)$

$X = \mu - 0$

$X = \mu$

X=5(laplacian noise)

ISSN- 2394-5125 VOL 7, ISSUE 15, 2020

Step 3: Masking the edge weight using laplacian noise value

W* = | Worg (1-X)|

W* = |9(1-5)|

W* = |9 (-4)| = 36

Thus the new laplacian weight for the edge weight 9 is determined to be 36. Similarly all the other edge weights can also be masked using the same procedure. Now lets consider a another example (fig 2) where the laplacian parameter is not equal to zero and determine the new edge weight of a graph.

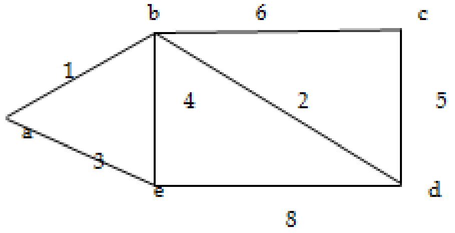


fig 2: Edge weighted graph before laplace noise implementation

Step 1: Calculation of µ

$$\mu = \frac{1+3+4+8+2+5+6}{7}$$

µ = 29/7

µ = 4.1

Step 2: Calculation of laplacian parameter β

∑(xi - µ) =
(1-4.1) + (3-4.1) + (4-4.1) + (8-4.1)+ (2-4.1) +(5-4.1) +(6-4.1)

= -3.1 -1.1 -0.1 +3.9 -2.1+0.9+1.9

= 0.3

To determine β the summation of these values must be divided by the total number of edges N.
So, $\beta = \frac{0.3}{7}$

Laplacian parameter β= 0.043

Step 3 : Determine the value of signum α

The signum is mathematical differential function which represents the d/dx of the given value in x variable form,

Such that, sgn (α) = d/dx (αx)

Where α represents the edge weight which is chosen to be masked. So from the above graph we choose the edge of maximum importance e and d whose value is 8.

Sgn (8) = d/dx (8x) where x must not be equal to 0.

Sgn(8) = 8.

Step 4: Determine the logarithmic function of ln(1-2|α|)

ln(1-2|8|) = -ln(15)

= -2.708

Step 5: Calculate the whole function βsgn(α)ln(1-2|α|)

βsgn(α)ln(1-2|α|) =0.043*8*(-2.708)

= -0.932

Step 6: Determine the laplacian noise value X

X = µ - βsgn(α)ln(1-2|α|)

X = µ -(- 0.932)

X = 4+ 0.932

X = 4.932 = 5(approx)

Step 6: To alter the edge weight

W* = | Worg (1 – X) |
W* = |8 (1- 5)|
W* = 32
So the new masked weight of the edge weight 8 between the vertices e and d is determined to be 32.

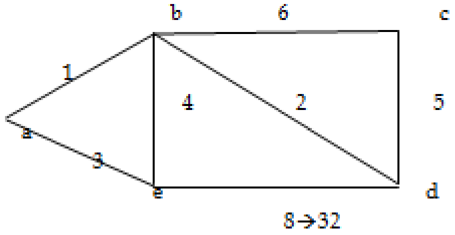


Fig3: Graph after laplace noise implementation

Consider two or more edges with the same edge weights so incase if the user wants to mask a particular edge weight ,the other edge weights which has the same value will also be masked. Based on the importance of process that is being done between two terminals the perturbation is decided whether to mask the edge weight or not. Also, masking the edge weight is based on user's decision.

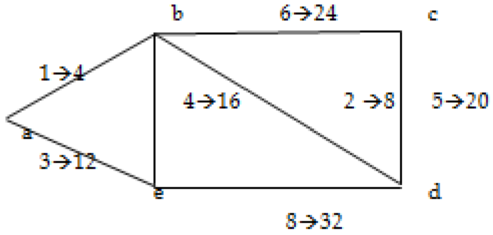


Fig4: Overall edge weight perturbation graph

The masked edge weight value will be the multiple of the chosen edge weight with the µ value approximately (fig 4). So the masked values for the edges can be determined theoretically just by ,multiplying the mean of edges with the edge weight that has to be masked.

4.1 PSEUDOCODE FOR LAPLACE IMPLEMENTATION

```
*identify the μ value from the graph which is the mean
 *μ = edge weights/ total number of edges
 *β  which is the laplacian parameter  is found  from the summation of all values of |xi - μ| divided by N which is the total edges
* find the signum of α which is the derivative of
  αx  value
* substitute in the formula for the laplace noise value
* The new edge weight is determined by
  W* = Worg(1-X)
```

4.2 ALTERNATE METHOD FOR LAPLACE NOISEBY AVERAGE ESTIMATION

There is also another method to determine the laplace noise with another laplace formula. Laplace is known for his transforming values from one state to another (ie) the general transformation is from frequency to time or vice versa. If we are going to consider a table of values ranging from one to n values, the laplace transformation can be performed from which the laplace noise can be determined. With a range of values, the average of the specific range will be determined first from the determined table values, then one value will be excluded from the given table and the average will be determined for the rest of the values. The two averages obtained must be subtracted and the maximum value of the average obtained is considered to be the noise value which will be added along with the original value to mask the value. Now lets consider a table of values for which we determine laplace noise.

TABLE1: ORIGINAL TABLE VALUES

Edges	Weights
a→b	1
b→c	6
c→d	5
d→e	8
e→a	3
b→d	2
b→e	4

Total number of values =7

Average of all the values (A) = (1+6+5+8+3+2+4) / 7

= 29 /7= 4.1

Now lets determine the average of the values excluding a particular value,

lets exclude 1

Average (A1) = 28/6 = 4.7

Avg(A) - Avg(A1) = 4.1- 4.7 = -0.6

Exclude 6,

Average (A1) = 23/6 = 3.8

Avg(A) - Avg(A1) = 4.1 – 3.8 = 0.3

Exclude 5,

Average (A1) = 24/6 = 4

Avg(A) - Avg(A1) = 4.1- 4 = 0.1

Exclude 8,

Average (A1) = 21/6 =3.5

Avg(A) - Avg(A1) = 4.1 – 3.5 = 0.6

Exclude 3,

Average (A1) = 26/6 = 4.3

Avg(A) - Avg(A1) = 4.1 – 4.3= -0.2

Exclude 2,

Average (A1) = 27/6 =4.5

Avg(A) - Avg(A1) = 4.1- 4.5 = -0.4

Exclude 4,

Average (A1) = 25/6 = 4.2

Avg(A) - Avg(A1) = 4.1 – 4.2= -0.1

Now the laplace noise value is determined by the maximum of these averages ,

$$\boxed{€ = \max [\ |Avg(A) - Avg(A1)|\ ]}$$

$$\boxed{€ = 0.6}$$

Sensitivity:

$\lambda = €/\mathbb{Z}$
$\mathbb{Z} \rightarrow$ privacy preservation constant

The value of privacy preservation constant is determined to be 0.5 [14]

$\lambda = 0.6 / 0.5$

$= 1.2$

Laplace noise formula:

$$\boxed{\text{Laplace}=[1/(2\lambda)][e-(x-\mu)/\lambda]}$$

where ,
μ is determined to be 0 [15].
In this case, the laplace noise must be determined for the individual values of X . where, X represents the average of the table values.
Noise for x= 4.1,

$= 1 /2(1.2) [e^{-(4.1)/1.2}]$

=0.0136

This value is determined to be the noise value which much be added to the other edge weights or table values.
So the laplace noise for the other values will be,

X1 = 4.7 + 0.0136 = 4.714

X2 =3.8 + 0.0136 = 3.814

X3= 4 + 0.0136= 4.014

X4 = 3.5+ 0.0136 =3.514

X5 = 4.3+ 0.0136 =4.314

X6 = 4.5+ 0.0136 =4.514

X7 = 4.2+ 0.0136 = 4.214

The range of x values from X1to Xn represents the new modified average values with which the noise values have been included. Since the noise value added is meager it does not affect the other properties of the network containing the values, when any algorithm is implemented the results are proven to be the same as the original network. Now to modify the values of the table directly, u can add the corresponding laplace average value to the edge values given in the table.

E1 = 1 + 4.714=5.714

E2 = 6 + 3.814 =9.814

E3= 5 + 4.014 =9.014

E4= 8+ 3.514 =11.514

E5= 3+ 4.314= 7.314

E6= 2+ 4.514 =6.514

E7 = 4+ 4.214 =8.214

Thus by adding the laplace noises to the original edge weight values ,the new edge weights have been obtained.

TABLE 2: TABLE WITH MODIFIED LAPLACE NOISE VALUES

egdes	Original edge weight	Modified edge weight
a→b	1	5.714
b→c	6	9.814
c→d	5	9.014
d→e	8	11.514
e→a	3	7.314
b→d	2	6.514

ISSN- 2394-5125 VOL 7, ISSUE 15, 2020

b→e	4	8.214

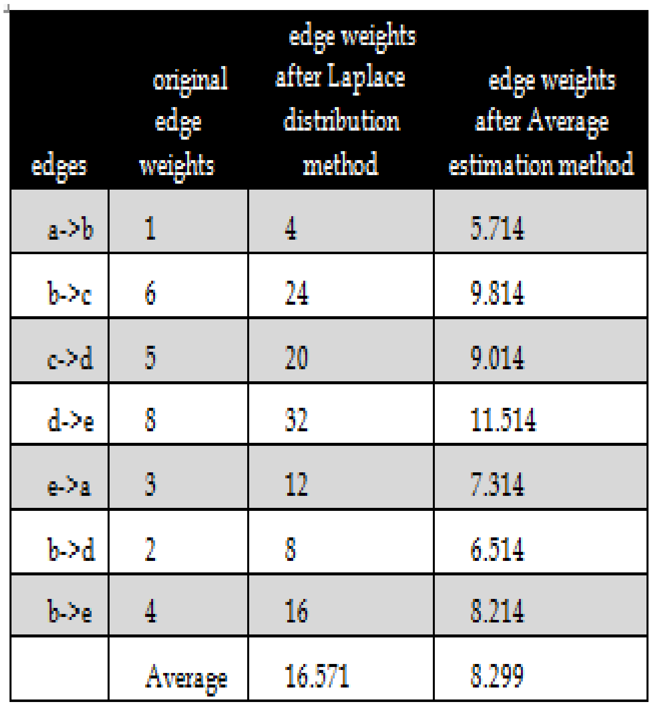
Hence in this method, the original edge weights have been preserved and while performing any operations with the values of this network,it turns to provide the desired results even in the masked form. On comparing method 1 and ,method 2, the first method seems to be more simpler and direct formula application and once the mean value is determined , the edge weights can be easily manipulated in method1. The second method involves more calculations but it provides the minimised noise value unlike the method1. Any of these methods can be used to preserve the privacy of the edge weights but it must not alter the properties of the original graph or network.

5 COMPARISON OF LAPLACE NOISE VALUES BETWEEN LAPLACE DISTRIBUTION NOISE METHOD AND AVERAGE ESTIMATION METHOD

Lets determine the differences between the method 1 which uses laplace distribution formula and method 2 which makes use of average estimation procedure. The average.

estimation method provides laplace noise much lesser in comparison with the laplace distribution formula method. Table 3 represents the edge pertubated values from method 1 and method 2

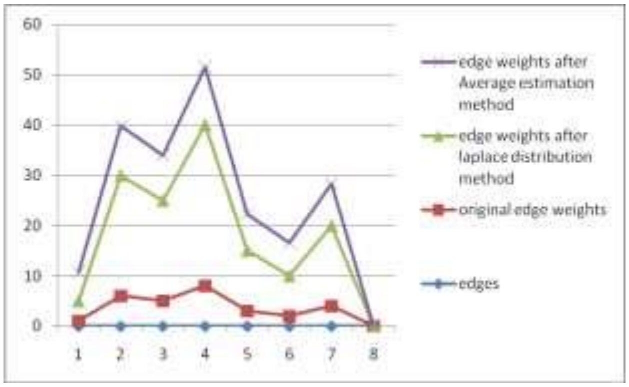
TABLE3: COMPARATIVE ANALYSIS BETWEEN METHOD1 AND 2



edges	original edge weights	edge weights after Laplace distribution method	edge weights after Average estimation method
a->b	1	4	5.714
b->c	6	24	9.814
c->d	5	20	9.014
d->e	8	32	11.514
e->a	3	12	7.314
b->d	2	8	6.514
b->e	4	16	8.214
	Average	16.571	8.299

From the table 3, its evident that the values of edge weights in laplace distribution method are higher in most cases in comparison with average estimation method values of edge weights. On considering the average between the two methods, the of difference between the methods is 2:1. The average of laplace distribution is twice as the value of average estimation method.

GRAPH 1: PLOT BETWEEN THE ORIGINAL,METHOD1 AND METHOD 2 EDGE VALUES



From the graph1, its clearly seen that the laplace implemented edge values from laplace distribution and average estimation methods, trace the same structure with similar peaks and falls as one another. The only difference observed is that the values of laplace distribution method is twice the values of average estimation method.

6 CONCLUSION

The laplace distribution method and average estimation method both can be used to determine the laplace noise of a particular edge of a social network graph. The laplace distribution method has an advantage in which the laplace noise values for all the edges can be determined by estimating the mean value (μ) ,whereas in case of average estimation method it involves many arithmetic computations which must be carried out in sequential order. Anyways on the implementation of any method to determine laplace noise, the other properties of the original graph will not be altered and it will provide the same results on performing any other algorithms in laplace noise implemented graph.

7 REFERENCES

[1] B. W. Kernighan and S. Lin, Bell Syst. Tech. J. 49, 291

[2] M. Fiedler, Czech. Math. J. 23, 298

[3] A. Pothen, H. Simon, and K.-P. Liou, SIAM J. Matrix Anal. Appl. 11, 430

[4] Pingshui WANG," Survey on Privacy Preserving Data Mining", International Journal of Digital Content Technology and its Applications, Volume 4, Number 9, December 2010.

[5] Jaideep Vaidya & Chris Clifton, "Privacy-Preserving Data Mining: Why, How, and When", the IEEE computer society, 2004.

[6] Yu Zhu& Lei Liu, "Optimal Randomization for Privacy Preserving Data Mining", ACM, August 2004.

[7] Aris Gkoulalas-Divanis, & Grigorios Loukides, "Revisiting Sequential Pattern Hiding to Enhance Utility", ACM, August

[7] Amruta Mhatre, Durga Toshniwal, "Hiding Co-occurring Sensitive Patterns in Progressive Databases", ACM, March 22, 2010.

[7] Shikha Sharma & Pooja Jain, "A Novel Data Mining Approach for Information Hiding", International Journal of Computers and Distributed Systems, Vol. No.1, Issue 3, October 2012.

[8] L.Sweeney, "Achieving k-Anonymity Privacy Protection Using Generalization and Suppression", International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, vol.10, no.5.

[9] C. C. Aggarwal, P. S. Yu, "Privacy Preserving Data Mining: Models and Algorithms". Springer, 2008.

[10] L. Sweeney, "K-anonymity: a model for protecting privacy. International Journal on Uncertainty, Fuzziness and Knowledge-based Systems", 10 (5), 2002.

[11] A. Blum, K. Ligett, and A. Roth. A learning theory approach to non-interactive database privacy. In STOC, pages 609–618, 2008.

[12] J. Cao, P. Karras, C. Raissi, and K.-L. Tan. ρ-uncertainty inference proof transaction anonymization. In VLDB, pages 1033–1044, 2010.

[13] I. Dinur and K. Nissim. Revealing information while preserving privacy. In PODS, pages 202–210, 2003.

[14] Úlfar Erlingsson, Vasyl Pihur, Aleksandra Korolova. "RAPPOR: Randomized Aggregatable Privacy-Preserving Ordinal Response". In Proceedings of the 21st ACM Conference on Computer and Communications Security (CCS), 2014.

[15] Kotz, Samuel; Kozubowski, Tomasz J.; Podgórski, Krzysztof (2001). The Laplace distribution and generalizations: a revisit with applications to Communications, Economics, Engineering and Finance. Birkhauser. pp. 23 (Proposition 2.2.2, Equation 2.2.8). ISBN 9780817641665.

[16] Dwork, C. and Yekhanin, S. (2008). New efficient attacks on statistical disclosure control mechanisms. In Proceedings of CRYPTO 2008, 468–480

[17]Composition attacks and auxiliary information in data privacy. In Proceedings of the 14th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD), 265–273. Also available at http://arxiv.org/abs/0803.0032. 153 [32] Gehrke, J., Kifer, D., Machanavajjhala, A., Abowd, J., and Vilhuber, L. (2008).

[18] Ravi Kumar, Prabhakar Raghavan, Sridhar Rajagopalan, and Andrew Tomkins. Corealgorithms inthecleversystem. ACMTrans.Inter. Tech., 6(2):131–152, 2006.

[19] . Mengzhi Wang, Tara Madhyastha, Ngai Hang Chang, Spiros Papadimitriou, and Christos Faloutsos. Data mining meets performance

evaluation:Fastalgorithms formodeling bursty traf¿c. ICDE,February 2002.

[20] Duncan J. Watts and Steven H. Strogatz. Collective dynamics of 'smallworld'networks