

# Permutation based K-Means Clustering Approach for Energy Conservation in MANETs

Ankita Chouhan

M.Tech Student of Computer  
Science and Engineering  
Lakshmi Narain College of  
Technology  
Bhopal, Madhya Pradesh, India

Sunil Phulre

Associate Professor in CS  
Department  
Lakshmi Narain College of  
Technology  
Bhopal, Madhya Pradesh, India

Vineet Richhariya

Associate Professor in CS  
Department  
Lakshmi Narain College of  
Technology  
Bhopal, Madhya Pradesh, India

## ABSTRACT

One of the important issue in MANETs is an energy saving and security. Each node in MANETs has limited energy resource, so that the lifetime of the network is one of the major critical issues. This paper studied SVM data aggregation method for classifying nodes according to their threshold values, this method eliminated the data redundancy and outliers but classification method is not much enough to reserve energy by power degradation on nodes in MANET. The sources of energy conservation are transmission cost, encryption/decryption, reducing data redundancy and transmission time in MANETs. Here P-coding can offered security based on symmetric key encryption, but symmetric key algorithms are not sufficient to provide security in MANETs. This paper introduce new scheme of energy saving called "Permutation based K-means Clustering" (PKMC) proposed for MANETs, which improves overheads, packet drops, transparency, security and energy efficiency. By the use of Permutation and K-means clustering, multiple clusters can be form with similar objects and each object provides security to data during data transmission. Thus, Permutation based K-means clustering contains minimum energy conservation as compares to previous data aggregation and encryption/decryption methods.

## Keywords

MANETs, Permutation Encryption, SVM, K-means Clustering, Energy saving.

## 1. INTRODUCTION

An ad-hoc wireless network is a distributed kind of wirelessly connected network. The ad-hoc nature demonstrates that, it does not depend on a pre-existing infrastructure, like routers in wired networks. In wired networks, there is an access point which is connected to all other devices in network for communication. Instead in wireless network, each node contributes in routing by forwarding data to other nodes. Energy saving is a major issue in ad-hoc wireless networks. In ad-hoc wireless network, energy consumption is based on number of data transmission. This means, more number of transmissions is equal to more energy consumption and less number of transmissions is equal to less energy consumption.

Cryptography is a mechanism of constructing and analyzing protocols that protect data from eavesdropper. It uses [1] Symmetric key cryptography that provides sharing of secret key between authenticated sender and receiver. These cryptographic algorithms makes hard to break data for eavesdropper, so that eavesdropper cannot break this unintelligible data. Data security contains some features like, data authentication, non-repudiation, confidentiality and data integrity. Data also contains redundant data and false data, which has to be eliminated or reduce for better performance of

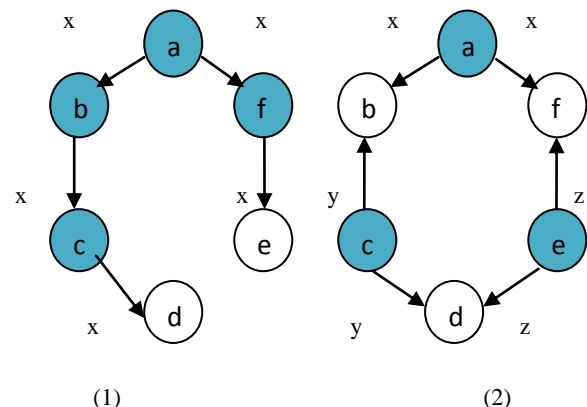
ad-hoc wireless network. This paper also studied that [2] Support Vector Machine (SVM) can detect and reduce these redundant data by using Locality Sensitive Hashing, it is based on the data similarity on each node and improved network performance with less energy consumption. For required level of security, MANETs also needs minimum amount of energy consumption in wireless communication environment. To provide security for MANETs, only symmetric key encryption algorithms are not efficient. Recently, there have been lots of works on developing energy efficient and low cost oriented security method in wireless networks.

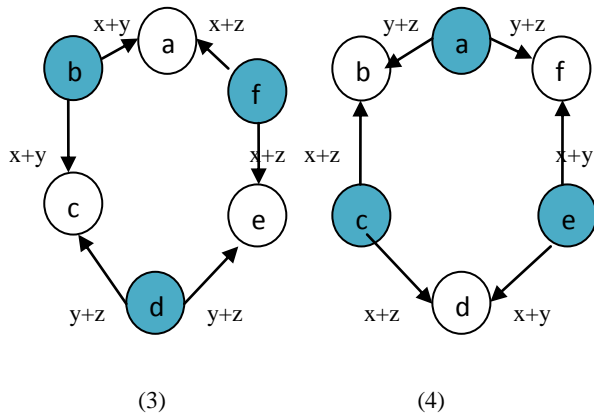
## 2. RELATED WORK

### 2.1 Literature Survey

There are various techniques are developed in order to find the appropriate energy saving technique in MANET. Link failure and security are common issue in multi-hop wireless Ad hoc networks because of their node mobility. This section includes the various research papers and articles that are providing us guideline to develop a new kind of energy consumption technique.

Recent studies [1] describes that network coding can help to obtain a low energy consumption in MANETs. This can reduce the energy used by each node in data transmission in network. The basic idea can be shows using the following example, suppose there are six nodes that forming a hexagon and they can communicate with only their left and right neighbours in transmission range. If node requires to broadcast one message to all other nodes without network coding; then each message require four broadcasts, as shown in Fig. 1(1). With network coding (Fig. 1(2)-(4)), three transmissions are required for each message. If it would not consider the energy consumed by encoding and decoding operations, then 1/4 energy can be saved.





**Fig. 1 Network coding for transmission, shaded nodes are involved in transmission**

In year 2013, author Peng Zhang Lin, Yixin Jiang, Yanfei Fan & Xuemin Shen, et al. [1], proposed a method for secure property for network coding. They describe a new technique i.e. P-coding, it is a lightweight encryption scheme to protect the data from external eavesdropper in network coded MANETs. The main idea is to divide data into generations and generate PEF key. There is a Key Distribution Center which can create PEF keys and distribute in each generation between sender and receiver. PEF key can disclose in any generation due to various numbers of generations but key is generated in each generation separately so that this method can protect security from single generation failure. In this, P-coding used permutation encryption by which data symbols can randomly mixes with its coding vector, it makes hard for eavesdropper to decode the data. So that, there paper proves that security can enhanced by permutation encryption technique.

In year 2013, author Prakashgoud Patil and Umakant Kulkarni, et al. [2], proposed a method called “Support Vector Machine based Data Redundancy Elimination for Data Aggregation in WSN (SDRE)”. This SDRE can reduce the redundant data and eliminate false data from wireless sensor network. In this paper, they built an aggregation tree of sensor network size and SVM method applied on data to remove redundancy. They used Local Sensitive Hashing for minimize redundant data and false data. LSH works based on data similarity and their threshold. This LSH code are send to aggregator supervisor node of tree, this sensor node will find same data node and select only one node for sending data. Aggregator supervisor can also reduce outliers and it does not receive data from another node. It proved improve performance of WSN based on such parameters as delay, energy, packet drops and overheads.

Kyung Tae Kim, Man Youn Kim, Ji Hyeon Choi, Hee Yong Youn, et. al, [11], proposed an energy efficient and optimal arbitrary clustering protocol that utilizing tree topology for self-organizing WSN. This scheme utilized a new probability function to determine the number of cluster-heads (CHs) in each round, function involves energy level, frequency for CH of each node and round information. The main aim of the proposed protocol is to minimize energy consumption at each node for maximizing the lifetime of network. After completion of levelling the member nodes with CH as the root, a tree is constructed in a cluster by broadcasting the topology by a hybrid medium access control approach. So that it significantly reduces energy consumption and increase the lifetime of the sensor network.

## 2.2 Problem Statement

To provide security, nodes will share a secret key only to the authenticated neighbor nodes, so that this can obtain various security goals like integrity, confidentiality, authentication, non-repudiation and availability.[6] To provide the required level of security, a MANET security solution also requires to consume minimum amount of energy in wireless communication environment. Recently, there have been lots of works on developing energy efficient and low cost oriented security method in wireless networks.

In previous paper, [1] provide security for MANETs using only symmetric key encryption algorithms but they are not efficient. Network coding can overcome energy consumption with transparency, scalability and performance in MANETs. They proposed Permutation encryption scheme [1] P-coding which is more efficient and assures confidentiality. The basic idea of this scheme is permutation encryption is applied on each packet before performing network coding operations. Without knowing the permutation, eavesdroppers cannot decode, and thus cannot obtain any meaningful information.

In paper [2], author describes a method for elimination of data redundancy for data aggregation using SVM method. This method uses aggregation tree and LSH (Locality Sensitive Hashing) function for defining low value and high value of threshold and they divide nodes according to their similarity. The procedure of LSH code generation described in previous paper [2]. In this, data aggregator supervisor node can detect and remove the data redundancy; aggregator selects only one node to send data from multiple nodes. The main advantage of this method is use of minimum energy by removing data redundancy. But in this method, there is still a chance to recover more energy that cannot be achieve in this approach.

## 3. PROPOSED DESIGNED AND METHODOLOGY

In our approach called “Permutation based K-means Clustering approach for energy conservation in MANETs” can reduce more energy consumption as compare to previous method.

### 3.1 Permutation Encryption

[1] The P-Coding scheme performs permutation encryption on the coded messages. Permutation encryption scheme, [2] P-coding which is more efficient and assures confidentiality. The basic idea of this scheme is permutation encryption is applied on each packet before performing network coding operations. Without knowing the permutation, eavesdroppers cannot decode, and thus cannot obtain any meaningful information.

Let  $m = [m_1, m_2, \dots, m_n]$  be a sequence of symbols and  $k$  be a permutation have length  $n$ , then PEF (Permutation Encryption Function) on  $m$  by key  $k$  is defined as:

$$Ek(m) = [mk(1), mk(2), \dots, mk(n)] \quad (1)$$

Similarly, Permutation Decryption Function on  $c$  by key  $k$  as  $Dk(c)$ ,

$$Dk(Ek(m)) = m \quad (2)$$

Here,  $k$  is the PEF key.

Permutation encryption is easy and simple to cryptographic analysis. The main idea of P-coding is to use permutation encryption on coded message. If in any generation PEF key will disclose to other user then secrecy will break but due to providing perturbing key in each generation, single generation failure will not occur.

### 3.2 Proposed Permutation based K-means Algorithm

#### Assumption

$N_{MANET}^i$  = Mobile adhoc network having  $i$  mobile node

List[node, id] = list contain node and their id maintain by each node of network

$M = \{X_i | X_i \text{ is } i^{\text{th}} \text{ mobile node} \in N_{MANET}^i\}$ , Set of Mobile node

$NN^{Xi} = \{Y_i | Y_i \text{ is } i^{\text{th}} \text{ neighbour node of } X_{i^{\text{th}}} \text{ mobile node} \in N_{MANET}^i\}$

#### Algorithm

- {
- Step 1. Source node ( $X_s$ ) call AODV and broadcast RRP to all there  $NN^{Xs}$  path towards their desired destination ( $X_d$ )
- Step 2. Every  $NN^{Xs}$  uni-cast Route reply packet (RRP) to  $X_s$  with their energy level. Where each node attached their node ID  
 $Ri_{Xs}^{Xd} = X_s, Y_1^{id}, Y_{1+1}^{id}, Y_{1+1+1}^{id}, \dots, X_d$
- Step 3. for every route  $Ri_{Xs}^{Xd}$   
 $Ri_{Xs}^{Xd} = X_s, Y_1^{id}, Y_{1+1}^{id}, Y_{1+1+1}^{id}, \dots, X_d$
- Step 4.  $X_s$  verify each node id and drop the route having lower resident energy node by using List [Node, id]
- Step 5. Lower resident energy node ( $N^{LE}$ ) search their neighbor node having energy above middle resident energy node as  $N^{ME}$  by using List [Node, id]
- Step 6. Lower resident energy node ( $N^{LE}$ ) swap their coordinate their neighbor node having energy above middle resident energy node as  $N^{ME}$  by using List [Node, id]
- Step 7.  $X_s$  select route and generate P code data packet.  
 $Di_{Xs}^{Xd} = "X_d"$

gerenrate p – code for that

$$P(Di_{Xs}^{Xd}) = * \#\#\#\%0^{\wedge}\$ "$$

- Step 8. Send P( $Di_{Xs}^{Xd}$ ) through selected route  
 $X_d$  apply inverse P( $Di_{Xs}^{Xd}$ )

Inverse P ( $Di_{Xs}^{Xd}$ ) = " $X_d$ "

}

### 4. SIMULATION AND RESULT

The performance of Permutation based K-means Clustering method is computed by NS2 simulator. Area size is created for MANET is up to 1000m X 800m and nodes can varies from 10 to 100 in the network. This table 1, shows the parameter values that used during simulation.

Table 1 Simulation Parameters

Parameters	Values
Number of Nodes	Vary from 10 to 100
Area Size	40
	50
	100
MAC	802.11
Routing Protocol and Techniques	AODV, K-Means and P-Coding
Simulation Time	300 Mili Seconds
Traffic Source	CBR
Packet Transmission Rate	1024 kbps
Transmit Power	1.0 w
Receiving Power	1.0 w

There are some performance metrics, on which this dissertation paper compares the performance of proposed method and the previous method.

#### 4.1. Performance Metrics

- Average Energy:

This is described as an amount of energy that required in successful data transmission. It is the average energy that conserve during data transmission.

- Overheads:

During data transmission, each data packet need an extra byte of information which is stored in packet header. It does not related with part of message, so it can reduce overall speed. To compare with overhead, energy will computed.

- End-to-End Delay:

End-to-end delay is the time between the packets is send by source and the time when packet reached at the receiver. It also consumes time by discovering route and queue in transmission. If delay is lower than assures better performance.

- Packet Drops:

Packet drops are the number of data packets which are dropped or lost in network during transmission.

Packet Lost = Total packet sent – no. of packet received

For better performance, packet drops should be low

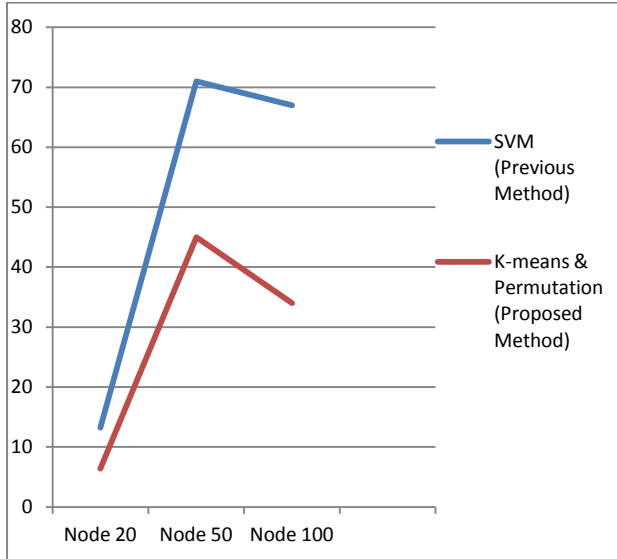
## 4.2. Result & Analysis

In this simulation, number of nodes are varies from 10 to 100 but for representation, report shows the graph between nodes 20, 50 and 100.

**Table 2 Comparison between Methods**

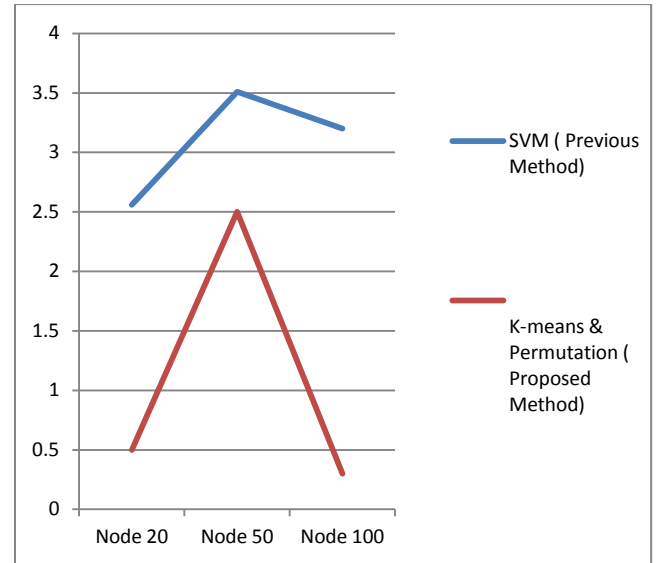
Nodes	SVM ( Previous Method)				K-means & Permutation ( Proposed Method)			
	Overheads (in bytes)	Energy (in Jules)	Packet drops (no. of Packets)	End-to-End Delay (in mili sec.)	Overheads (in bytes)	Energy (in Jules)	Packet drops (no. of Packets)	End-to-End Delay (in mili sec.)
20	13.2	2.56	1.67	0.05	6.4	0.5	2.4	1.62
50	71	3.51	109	-0.59	45	2.5	100	-1.59
100	67	4.5	4.7	-2.5	34	0.3	2.1	-5.1

In above Table 2, comparison shows between previous method i.e. SVM method and proposed method i.e. K-means & Permutation method. This comparison table between methods can easily describe the performance of both methods and help to find which one method is more better than another. Here, result of SVM (previous method) and K-means & Permutation (proposed method) are described by the graph according to the values of parameters such as, overheads, energy consumption, packet drops and end-to-end delay.



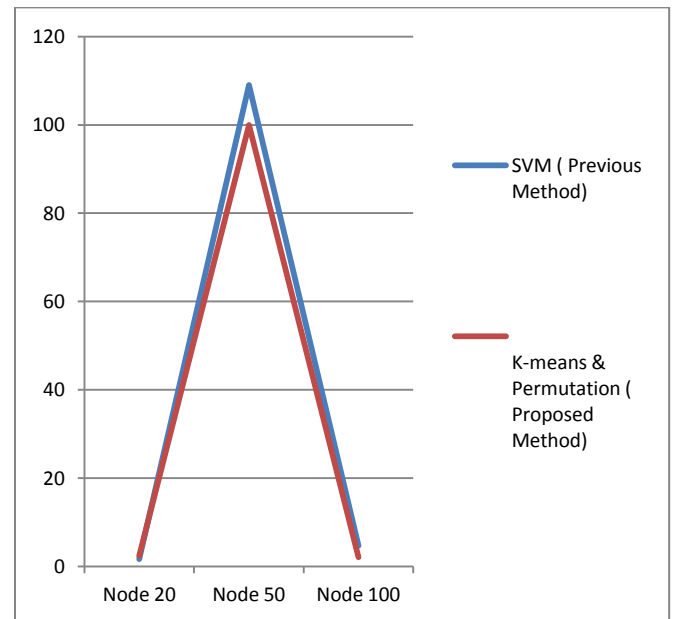
**Fig.2 No. of nodes Vs. Overheads**

In this graph, it shows the K-means and Permutation method are superior than SVM method.



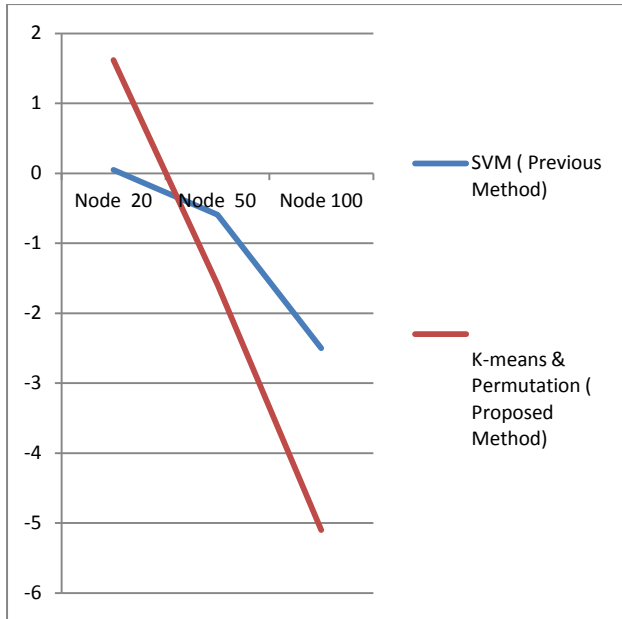
**Fig.3 No. of Nodes Vs. Energy consumption**

In above graph, it show the less energy consumed by new method as compare to SVM method.



**Fig.4 No. of node Vs. Packet Drops**

In this above graph, it shows the less packet drops in proposed method as compare to previous SVM method.



**Fig.5 No. of Nodes Vs. End-to-End Delay**

Here, some fluctuations are measured between nodes 20 to 50, but after that SVM method use more time delay as compare to K-means & permutation method.

After implementation of the proposed routing protocol, evaluation of the result performed and designed routing protocol under various performance parameters and research founds the results listed below.

**Table 3 Performance Summary**

Parameters	Results	Remarks
End-to-end delay	The comparison of end-to-end delay is performed with respect to AODV protocol is maximum.	Moderated
Overhead	Overhead of the system is much better than SVM based AODV	High performance results
Packet Drop Ratio	Low packet drop ratio	Adoptable
Energy	Gain high energy	High performance results

## 5. CONCLUSION

In the proposed study work described in above section provides the design and implementation of a K-Means and P-Coding based routing protocol. To identify the need of protocol paper study various techniques by which get the problem domain and the solution domain. To design the protocol, study the techniques of cryptography and clustering with AODV routing protocol and find the place where required to make change and implementation of this routing protocol performed using C++ scripts which is listed at end of

the document. The P-Coding, a lightweight encryption scheme on top of network coding, incurs less energy consumption. Further the key generation method is employed to improve the security of P-Coding with less overhead in computation. But it does not provide complete security, which can be provided by K-means Clustering method. It eliminated redundant data by making clusters. The performance of new proposed method is computed by parameters such as Overheads, Packet drops, Energy consumption and End-to-End delay. So that, proposed method PKMC achieves better in all parameter. But in future their performance can increase by using more suitable clustering algorithms or variation of K-means algorithms. So, in near future we stick with the same concept and this paper will further try to implement this concept with more adaptable clustering algorithm that can reduce more energy with different number of nodes.

## 6. REFERENCES

- [1] Peng Zhang, Chuang Lin, Yixin Jiang, Yanfei Fan, and Xuemin (Sherman) Shen "A Lightweight Encryption Scheme for Network-Coded Mobile Ad Hoc Networks," IEEE Trans. Parallel and Distributed Systems, Vol. 25, No. 9, September 2013.
- [2] Prakashgoud Patil, Umakant Kulkarni "SVM based Data Redundancy Elimination for Data Aggregation in Wireless Sensor Network", International Conference of Advance in Computing Communication and Informatics, IEEE, 2013
- [3] Ajay Kushwaha, Hariram Sharma, "Enhancing Selective Encryption Algorithm for Secured MANET", 2012 Fourth International Conference on Computational Intelligence, Modelling and Simulation
- [4] Emiliano De Cristofaro and Claudio Soriente, "Participatory Privacy:Enabling Privacy in Participatory Sensing", IEEE TRANSACTIONS ON NETWORKING VOL.27 NO.1 YEAR 2013
- [5] QUANSHENG GUAN, F. RICHARD YU, SHENGMING JIANG, VICTOR C. M. LEUNG, HAMID MEHRVAR, "TOPOLOGY CONTROL IN MOBILE AD HOC NETWORKS WITH COOPERATIVE COMMUNICATIONS", IEEE Wireless Communications April 2012
- [6] Adel ECHCHAACHOU, Ali CHOUKRI, Ahmed HABBANI and Mohamed ELKOUTBI, "Asymmetric and Dynamic Encryption for Routing Security in MANETs", IEEE 2014
- [7] Hongwei Li, "A Hierarchical Identity-Based Encryption for MANETs", IEEE 2011, ICCP2011
- [8] Adarsh Kumar, Krishna Gopal and Alok Aggarwal, "A Complete, Efficient and Lightweight Cryptography Solution for Resource Constrained Mobile Ad-Hoc Networks", 2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing
- [9] Chun Yuan, Hongyang Gao, Wenshuo Zhou, "Lightweight identity-based broadcast encryption over wireless ad hoc Networks", IEEE 2011
- [10] GU Hong , ZHAO Guangzhou , QIU Jun, "One-Class Support Vector Machine with Relative Comparisons", TSINGHUA SCIENCE AND TECHNOLOGY ISSN11007-02141108/161pp190-197 Volume 15, Number 2, April 2010

- [11] Kyung Tae Kim, Man Youn Kim, Ji Hyeon Choi, Hee Yong Youn, “An Energy Efficient and Optimal Randomized Clustering for Wireless Sensor Networks”, 2015 IEEE SNPD 2015, June 1-3 2015, Takamatsu, Japan
- [12] Obaida Mohammad Awad Al-Hazaimeh, “A NEW APPROACH FOR COMPLEX ENCRYPTING AND DECRYPTING DATA”, International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.2, March 2013
- [13] Data Mining - Cluster Analysis. Available online: [http://www.tutorialspoint.com/data\\_mining/dm\\_cluster\\_analysis.htm](http://www.tutorialspoint.com/data_mining/dm_cluster_analysis.htm)
- [14] k-means clustering. Available online: [https://en.wikipedia.org/wiki/K-means\\_clustering](https://en.wikipedia.org/wiki/K-means_clustering)
- [15] Book: Data Mining, Southeast Asia Edition: Concepts and Techniques By Jiawei Han, Micheline Kamber, Jian Pei
- [16] Book : Data Clustering: Theory, Algorithms, and Applications By Guojun Gan, Chaoqun Ma, Jianhong Wu