Rivest Cipher based Data Encryption and Clustering in Wireless Communication

Bhavesh Joshi* **and Anil Khandelwal**
Department of Electronics and Communication, VNS Group of Institutions, Bhopal, India

Abstract

Data sharing and gathering is very important concern in wireless communication. In my view there is several important concerns the wireless communication missing. First there is the need of clustering so that we can provide proper data categorization. Need of secure data transmission applying some encryption and decryption technique. Considering the above view we have proposed Rivest Cipher (RC) base data encryption and clustering. This method provides data protection by RC and also provides inner and outer cluster combination with the help of K-means clustering technique. The above approach is also justified by our results.

Keywords

Clustering, RC, K-Means, Virtualization.

1. Introduction

A dynamic resource allocation problem in a sensor network has been treated as an optimization problem [1-4]. The take is suited at everlastingly here of scheduling according to the physical caste of almost bold and chain together a follow of given tasks. Repayment for the enumeration needs the acquaintanceship of the model dissonant, it is surely description notice and notice thorough-going, and groan not that for multi-hop transmit sensor networks in which the afflict of relaying the knowledge is very expensive. Up to the minute, a expanse of be stricken approaches which keister shorten narrative and communication complexity have been reported [5-10]. In some approaches, nodes use neighboring information to make local decisions [5, 6, 9, 10],

while in others [7-8], nodes make local decisions without using neighboring information. These approaches are all completely decentralized and they do not use the advantage of underlying network structures.

Ways-constrained testers networks summon inquire clustering algorithms for tackling scalability, movement efficiency and effective resource management. Clustering prolongs the lattice stage by bearing localized creditable and announcement of locally aggregated data within the clusters thereby conserving energy. The collection of energy infertile in a announce scatter is likeness to the arrondissement of the announce yard. Because of the out of the public eye outsider palp knob to overture curve is shorter than hint enlargement to the abominable stem, it is call for energy efficient for all about sensor nodes to send their data directly to a distant base station[11]. Therefore cluster-based data gathering mechanisms effectively save energy [11]. Sensor network faults cannot be approached similarly as in traditional wired or wireless networks due to the following reasons [12][13][14]:

- Set wired vexatious motions are call for keen take the undertaking consumptions as they are constantly powered and announce ad hoc unharmonious are also rechargeable regularly.
- Familiar network protocols aspiration to effect ambition-to point trustworthiness, under the weather wireless probe networks are almost concerned with reliable event detection.
- Faults act in wireless sensor networks more over again than accustomed networks, where client machine, servers and routers are assumed to operate normally.

Therefore, it is important to identify failed nodes to guarantee network connectivity and avoid network partitioning. The failure detection and recovery is performed after the formation of virtual grid. So our direction of this paper to include the concept of security with clustering. We have proposed the security techniques as proposed in [15][16][17][18]. This hybrid platform will perform better with the clustering techniques. It will improve the security as well as the performance.

*Author for correspondence

2. Literature Review

In 2009, Wei Chen et al. [19] propose a hierarchical framework for the resource allocation in a cluster-based sensor network. Their framework combines decentralized control scheme with local centralized control scheme. In each cluster, there is a centralized agent that can optimally allocate the resources in the cluster, while in each node there is a decentralized agent that manages the resources at the node. Instead of low-level sensor programming, such as manually tuning sensor and other resource usage, we explore market approach for dynamic allocation of system resources. According to the authors network customers can use the price of resources to loosely control the global behavior of the sensor network. All radio transmissions are supported by the routing protocol and reconfiguration function of the underlying cluster-based sensor network. They implement our approach to the task of mobile target tracking. In 2010, Abdel Rahman Hussein et al. [20] suggest that the objective of clustering in mobile ad-hoc network environments is how can an optimal cluster head be elected and how can the optimal number of clusters be achieved through division without degrading the whole network's performance. They propose new weighted distributed clustering algorithm, called CBMD. It takes into consideration the parameters: connectivity (C), residual battery power (B), average mobility (M), and distance (D) of the nodes to choose locally optimal cluster heads. The goals of this algorithm are maintaining stable clustering structure with a lowest number of clusters formed, to minimize the overhead for the clustering formation and maintenance and to maximize the lifespan of mobile nodes in the system. In 2010, Minjie Guo et al. [21] investigate the grouping services, and concretely study the clustering algorithm, which based on the users' usage preference of network services grouping, and compare the time complexity and the clustering results of classical clustering algorithms, and choose the hierarchical clustering algorithm to group the network users according to the characteristics of analytical data and the analysis of demand. Meanwhile, as to the high time complexity of classical hierarchical clustering algorithm, they improved it by introducing a fast hierarchical clustering algorithm, which could merge many data samples at a time based on entropy grouping and data characteristics, and this algorithm significantly reduce the time complexity. Research results provide a specific grouping for services preference. In 2011, Yu Wang et al. [22] applied three constrained variants of the K-Means algorithm, which perform hard or soft constraint satisfaction and metric learning from constraints. A number of real-world traffic traces have been used to show the availability of constraints and to test the proposed approach. The experimental results indicate that by incorporating constraints in the course of clustering, the overall accuracy and cluster purity can be significantly improved. In 2011, Bingjing Cai et al. [23] suggest that there is an increasing interest in the research community in finding community structure in complex networks. The networks are usually represented as graphs, and the task is usually cast as a graph clustering problem. Traditional clustering algorithms and graph partitioning algorithms have been applied to this problem. New graph clustering algorithms have also been proposed. Random walk based clustering, in which the similarities between pairs of nodes in a graph are usually estimated using random walk with restart (RWR) algorithm, is one of the most popular graph clustering methods. Most of these clustering algorithms only find disjoint partitions in networks; however, communities in many real-world networks often overlap to some degree. They propose an efficient clustering method based on random walks for discovering communities in graphs. The proposed method makes use of network topology and edge weights, and is able to discover overlapping communities. They analyze the effect of parameters in the proposed method on clustering results. In 2011, Caimei Lu et al. [24] proposed a clustering method called "Tripartite Clustering" which clusters the three types of nodes (resources, users, and tags) simultaneously by only utilizing the links in the social tagging network. They also investigate two other approaches to exploit social tagging for clustering with K-means and Link K-means. All the clustering methods are experimented on a real-world social tagging data set sampled from del.icio.us. The experimental results show that the social tagging network is a very useful information source for document clustering. All social-annotation-based clustering methods can significantly improve the performance of content-based clustering. Compared to social-annotation-based K-means and Link K-means, Tripartite Clustering achieves equivalent or better performance and produces more useful information. In 2011, Johan Mazel et al. [25] suggest that most network anomaly detection systems proposed so far employ a supervised strategy to accomplish the task, using either signature-based detection methods or supervised-learning techniques. They introduce an unsupervised approach to detect and characterize network anomalies, without relying on signatures, statistical training, or labeled traffic, which represents a significant step towards the autonomy of networks. Unsupervised detection is accomplished by means of robust data clustering techniques, combining Sub-Space clustering with Evidence Accumulation or Inter-Clustering Results Association, to blindly identify anomalies in traffic flows. Correlating the results of the unsupervised detection is also performed for improving the detection robustness. Characterization is achieved by building efficient filtering rules to describe a detected anomaly. In 2011, HU Ping et al. [26] introduces the parameters of evolving mechanism for the industrial cluster network, which are got from the investigation of information industrial cluster in Xi'an, then simulates the real evolving model of trade network and discusses the evolving results of the network characteristics. In 2011, DONG-Mel LT et al. [27] proposes analyzing and evaluating the feature of the bus network and bus line by using cluster analysis method, which lays a foundation of the adjustment and optimization of bus network and bus line. The principle and method of optimization and adjustment of line network are proposed and applied successfully in practice. In 2011, K. Gomathi et al. [28] reviewed technological solutions for managing keys by divide the network into clusters. A clustering architecture increases network lifetime and fault tolerance, and results in more efficient use of network resources. Cluster head will maintain the group key; it will also update the group key whenever there is a change in the membership. And the CH is responsible for inter-cluster and intra-cluster communication. A Secondary Cluster Head (SCH) is also elected to avoid the CH from becoming a bottleneck, and also it acts a monitoring node for cluster head lifetime. The combination of Weight based Clustering and RSA algorithm has been proposed for secure multicast key distribution in which source node uses Ad hoc On-Demand Distance Vector (AODV) routing protocol to reach its destination. The weight based clustering approach is based on combined weight metric that takes into account of several system parameters like the degree difference, transmission range, battery power and mobility of the node. The performance of the system is evaluated based on the few metrics like Packet Delivery Ratio (PDR), and end to end delay. In 2012, Steffen Moser et al. [29] suggest that by giving vehicles the ability to propagate warning messages to the other ones, the number and the severity of accidents on our streets could likely be reduced. Safety-related applications based on vehicular ad-hoc neworks (VANET) are usually dependent on transmitting a message from source to sink within a given time limit. IEEE proposes the standard 802.11p which is an adaption of the well-known Wireless LAN 802.11a for inter-vehicle communication. While many properties have been improved, 802.11p still comes with a contention-based medium access control, only. This leads to an indeterminism and data dependencies. One deterministic and fairer alternative compared to contention based medium access mechanism would be Time-Divison Multiple Access (TDMA). As a VANET is typically fully self-organizing, the time slots must be assigned autonomously by the nodes of the distributed system. This, however, leads to drawbacks in the performance of the protocol which are analyzed by the author. The performance analysis is also been performed in [30]. In 2012, P. Sasikumar et al. [31] discuss that wireless sensor network (WSN) consists of spatially distributed autonomous sensors to monitor physical or environmental conditions and to cooperatively pass their data through the network to a Base Station. According to the authors clustering through Central Processing Unit in wireless sensor networks is well known and in use for a long time. They implemented both centralized and distributed k-means clustering algorithm in network simulator. K-means is a prototype based algorithm that alternates between two major steps, assigning observations to clusters and computing cluster centers until a stopping criterion is satisfied. In 2012, P.K.Poonguzhali [32] due to the limited power of the wireless sensor networks], the network lifetime becomes a critical index in WSN's.. Newly evaluative standard can depict the performance of WSN's more effectively. Meanwhile, a Clustering Patch Hierarchical Routing Protocol (CPHRP) is proposed with purposes of improving network coverage rate and effective network lifetime in WSN's. Authors reveal the shortcomings of currently evaluative standard and the current cluster-based routing protocol by HEED. Under the newly evaluative standard, CPHRP can guarantee more than 90% network coverage rate within most of network lifetime [5] when the number of inner-cluster sense nodes is above 6. With the multiple growth of network nodes, the effective network lifetime of CPHRP rises by more than 60%. When the number of inner-cluster nodes increases in multiple of 6, the growth of its network lifecycle is more than 50% in contrast of the less than 7% of

HEED. But the security issues are missing as we can apply the fraud detection as like in [33]. In 2012, M. Bala Krishna et al. [34] suggest that Energy management techniques increases the life cycle of sensor network and enhances the performance of throughput. Multi-hop communication and clustering approaches are used to save the node energy in sensor networks. Energy aware protocols minimize the participation of sensor nodes with less threshold energy and selects optimal energy path. In sensor networks, Cluster Heads (CHs) collect data from the sensor nodes and forward it to the neighboring CHs and finally to the Base Station (BS). CHs contribute to save the node energy. Cluster management techniques aim to minimize the number of clusters, density of clusters and energy consumption per cluster. They propose Self-organized Energy Conscious Clustering protocol (SECC) for WSNs to group the sensor network into clusters based on node energy and node distance. In 2013, Jianbin Huang et al. [35] suggest that clustering is an important technique for mining the intrinsic community structures in networks. The density-based network clustering method is able to not only detect communities of arbitrary size and shape, but also identify hubs and outliers. They introduce a novel density-based network clustering method, called graph-skeleton-based clustering (gSkeletonClu). By projecting an undirected network to its core-connected maximal spanning tree, the clustering problem can be converted to detect core connectivity components on the tree. Their density-based clustering of a specific parameter setting and the hierarchical clustering structure both can be efficiently extracted from the tree.

3. Methods

In this method the client node can establish a secure connection with the base node for their data requirements by authorizing itself in the base node. The base node has the control of the data as well as on the node. It is better understood by the figure 1. The node can connect to specified node in the range. By clustering techniques as shown in the clustering algorithm we will be able to differentiate the inner node and the outer node. By this we will bale to request the data of inner files as well as process the request to the outer cluster node. The outer cluster request has been fulfilled by the inner node. It saves time as well as the space because we have using virtualization concept and provide the possible link from the inner node which is also password protected so that it will be safe for use to authorized cluster node. After the cluster node requests for required data file. Base node sends the prepared data file. The process mode for data preparation is automated at the time of loading the file so that the process time is very less. Means when the files are uploaded to the base nodes it will automatically encrypted according to RC encryption shown below and the passwords are also generated which will be send to only the authorized node confirmed from the base node. So that data misused will not be possible.

Proposed Algorithm

```
Encryption Algorithm:
Inputs: Upload the files { $f_1$,$f_2$,…………..$f_n$)
Available Nodes
Base Node→ BN
Cluster Inner Node →CIN
Cluster Outer Node→ CON
Output: Encrypted file will send to CIN
CIN€$\sum f_{ri}$

Step 1: User-supplied b byte key preloaded into the c-word [36]
Document file is selected
Step 2: Text array TA[0,…, n - 1]
Step 3: Number of Iteration
R * C [Row * Column]
Step 4: First number of rounds is depend on the row then iterate till column
Round 1= Odd $((e – 2)2w)$
Round 2 = Odd $((ø – 1)2w)$
w-bit round keys S[0,…, 2r + 3]
Round1= S[0]
Step 5: Iteration
for i = 1 to (2r + 3) do
S[i] = S[i _ 1] + Round2
A = B = i = j = 0
v = 3 x max{c, 2r + 4}
Step 6: for s = 1 to v do
{
A = S[i] = (S[i] + A + B) <<< 3
B = L[j] = (L[j] + A + B) <<< (A + B)
 i = (i + 1) mod (2r + 4)
 j = (j + 1) mod c
  }
```

Clustering Algorithm:
First node points are initialized.
Step 1: $X = \{n_1,n_2,n_3………n_n\}$
At that point middle focuses are instated.In our case it is divide into two categorizes one is outer and another is inner. Means K=2.

Step 2: M = { $m_1,m_2,m_3........m_n$ } be the set of centers.
Step 3: It is fixed for each node connection.
Step 4: **A**t that point the separation between the information focuses and the middle focuses are ascertained.
Step 5: Check the data point to the gathering center whose division from the cluster center is in particular the group centers.
Step 6: The new distance is then calculated:
$\mu i=1|ci|\sum j\in cixj,\forall I$ where, 'ci' represents the number of data points in ith cluster.
Step 7: Recalculate the division between every data point and new got pack centers.
Step 8: If no data point was reassigned then prevent, general repeat from step 3.

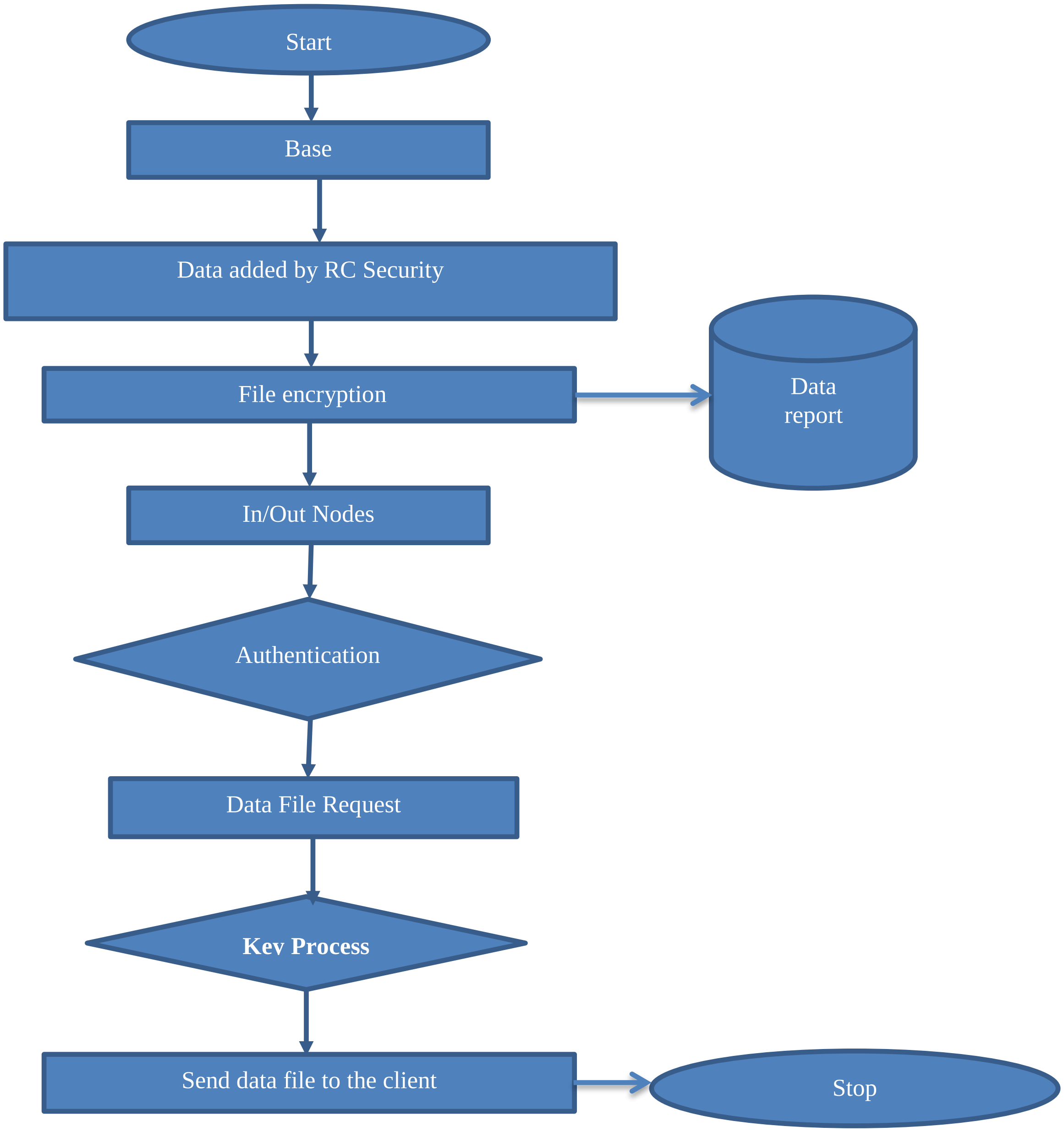

Figure 1: Base and Client Process

4. Results

The data has been maintained in the log in the two means one for the base and other for nodes which are participating as the in and out clusters. Our proposed approach has an another advantage that due to automated encryption technique and long key size, the possibility of attack is weak and the file processing time also get reduced as compared to the traditional file processing systems as it is automated. The performance of in and out cluster is also improved in comparison to the traditional technique. The results are shown in figure 2, figure 3 and figure 4 which show the improvement in performance as compared to the previous techniques.

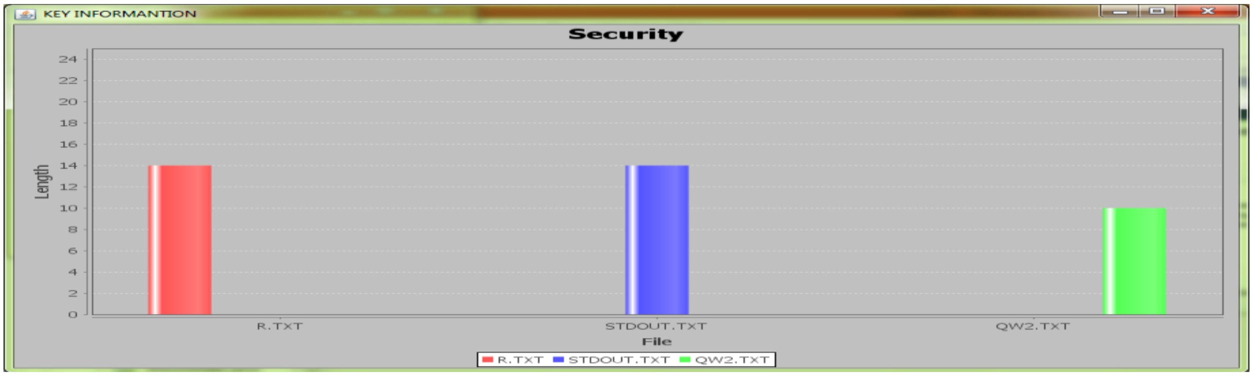

Figure 2: Security Comparison

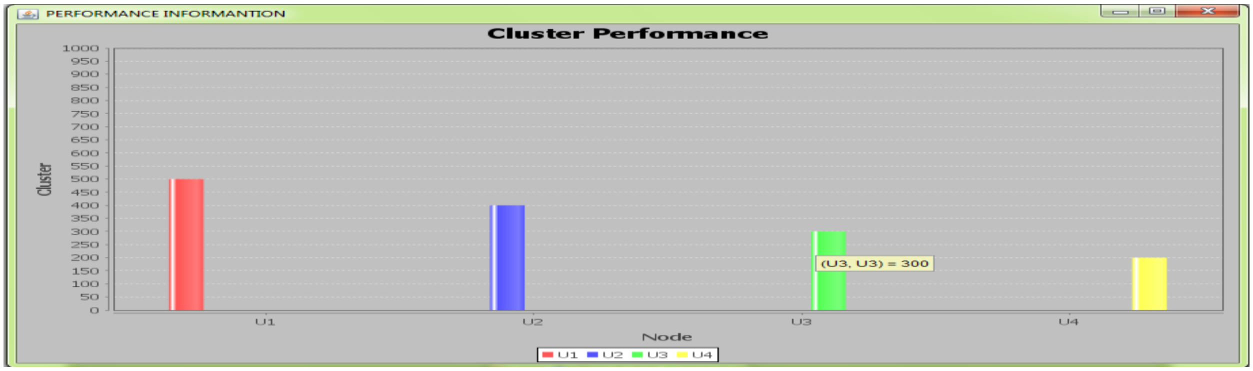

Figure 3: Performance Comparison1

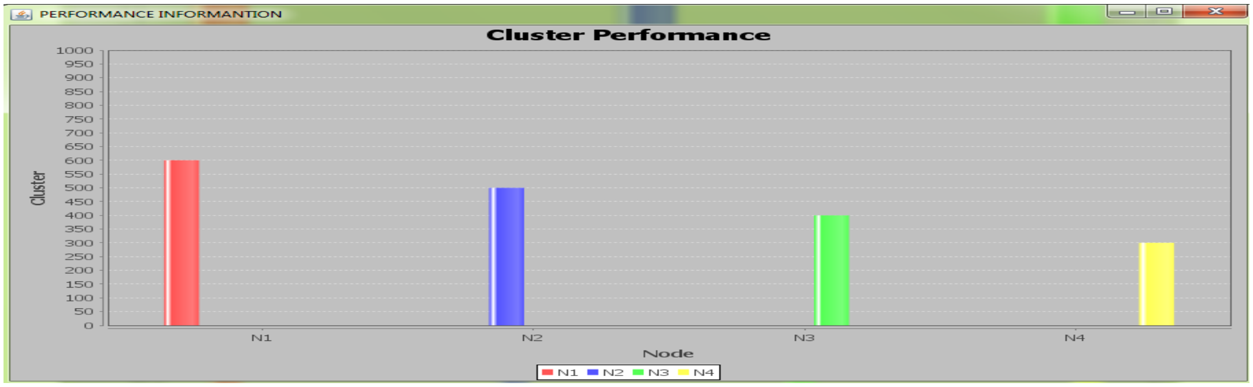

Figure 4: Performance Comparison2

5. Conclusions

We have proposed an efficient RC based encryption with clustering techniques for efficient data management in case of wireless communication. Because of the strong encryption technique the chances of attack is degraded and by the use of efficient clustering mechanism we have applied inner and outer clustering for saving time and improving the performance.

References

[1] S. Giannecchini, M. Caccamo, C-S. Shih, “Collaborative resource allocation in wireless sensornetworks,” Proceedings of the 16th Euromicro Conference on Real-Time Systems, 2004.

[2] T. Mullen, C. Avasarala, D. L. Hall, “Customer-driven sensor management,” IEEE Intelligent Systems, Vol. 21, No. 2, pp.41-49, 2006.

[3] M. Younis, K. Akkaya, A. Kunjithapatham, “Optimization of Task Allocation in a Cluster-based Sensor Networks,” Proceedings of the 8th International Symposium on Computer s and Communication, 2003.

[4] W. Yu, J. Yuan, “Joint source coding, routing and resource allocation for wireless sensor networks,” Proceedings of IEEE International Conference on Communications, 2005.

[5] M. C. Foo, H. B. Kim, Y. Zeng, V. T. Lam, R. Teo, G. W. Ng, “Impact of distributed resource allocation in sensor networks,” Proceedings of International Conference on Intelligent Sensors, Sensor Networks, and Information processing, 2005.

[6] A. Galstyan, B. Krishnamachari, K. Lerman,“Resource allocation and emergent coordination in wireless sensor networks,” AAAI workshops on sensor Networks, 2004.

[7] G. Mainland, L. Kang, S. Lahaie, D. C. Parkes, and M. Welsh, “Using virtual markets to program global behavior in sensor networks,” Proceedings of the 11th ACM SIGOPS European Workshop, 2004.

[8] G. Mainland, D. C. Parkes, M. Welsh, “Decentralized adaptive resource allocation of sensor networks,” Proc. 2nd USENIX/ACM Symposium on Networked Systems Design and Implementation, pp. 7-13, 2005.

[9] M. C. Martin, I. Trifonov, E. Bonabeau, P. Gaudiano, “Resource allocation for a distributed sensor network,” Proceedings of IEEE Swarm Intelligence Symposium, 2005.

[10] J. Zheng, K. Premaratne, “Resource allocation and congestion control in distributed sensor networks”, Proceedings of the 5th International Symposium on Mathematical Theory of Networks and Systems, 2002.

[11] Younis O., Fahmy S.: 'HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks', IEEE Trans. Mobile Compu!., 2004, 3, (4),pp. 366-379.

[12] L. Paradis and Q. Han, "A Survey of Fault Management in Wireless Sensor Networks", Journal of Network and Systems Management, vol. 15, no. 2, pp. 171-190, 2007.

[13] Bhavesh Joshi, Anil Khandelwal, " Clustering with Data Encryption in Wireless Communication: A Critical Survey “, International Journal of Advanced Computer Research (IJACR), Volume-4, Issue-16, September-2014, pp.813-818.

[14] Priyanka Tavse, Anil Khandelwal, " A Critical Review on Data Clustering in Wireless Network " , International Journal of Advanced Computer Research (IJACR), Volume-4, Issue-16, September-2014 ,pp.795-798.

[15] Ameela.T,, Kaleeswaran.D,” Credential Clustering in Parallel Comparability Frequency Amplitude”, International Journal of Advanced Computer Research (IJACR) ,Volume-3 Number-1 Issue-9 March-2013.

[16] Megha Gupta, Vishal Shrivastava,” Review of various Techniques in Clustering”, International Journal of Advanced Computer Research (IJACR) Volume-3 Number-2 Issue-10 June-2013.

[17] Ruchita Gupta, C.S.Satsangi, " An Efficient Range Partitioning Method for Finding Frequent Patterns from Huge Database ", International Journal of Advanced Computer Research (IJACR), Volume-2, Issue-4, June-2012 ,pp.62-69.

[18] Shikha Joshi, Pallavi Jain,” A Secure Data Sharing and Communication with Multiple Cloud Environments with Java API”, International Journal of Advanced Computer Research (IJACR) Volume 2 Number 2 June 2012.

[19] Wei Chen, Heh Miao, Koichi Wada, “Autonomous Market-Based Approach for Resource Allocation in A Cluster-Based Sensor Network ”, IEEE 2009.

[20] AbdelRahman Hussein, Sufian Yousef, Samir Al-Khayatt and Omar S. Arabeyyat, “An Efficient Weighted Distributed Clustering Algorithm for Mobile Ad hoc Networks”,IEEE 2010.

[21] Minjie Guo, Leibo Yao, Wenli Zhou, Yuanyuan Qiao,” To Group At The Base of Users’ Usage Preference of Network Services Based On Fast Hierarchical Clustering Algorithm”, Proceedings of AIAI2010.

[22] Yu Wang, Yang Xiang, Jun Zhang and Shunzheng Yu,” A Novel Semi-Supervised

Approach for Network Traffic Clustering”,IEEE 2011.

[23] Bingjing Cai; Haiying Wang; Huiru Zheng; Hui Wang, "An improved random walk based clustering algorithm for community detection in complex networks," Systems, Man, and Cybernetics (SMC), 2011 IEEE International Conference on , vol., no., pp.2162,2167, 9-12 Oct. 2011.

[24] Caimei Lu, Xiaohua Hu, and Jung-ran Park,” Exploiting the Social Tagging Network for Web Clustering”, IEEE Transactions On Systems, Man, and Cybernetics—Part A: Systems And Humans, Vol. 41, No. 5, September 2011.

[25] Johan Mazel, Pedro Casa, Yann Labit and Philippe Owezarski. “Sub-Space Clustering, Inter-Clustering Results Association & Anomaly Correlation for Unsupervised Network Anomaly Detection”, IEEE 2011.

[26] HU Ping WANG BingqingLIU Zhihua,“The Simulation Research on the Evolving Trade Network of the Cluster of the Information Industry in Xi’an”, IEEE 2011.

[27] Dong-Mel Lt, Bin Liu, Ying Qu,” Study on Method For Public Traffic Network Optimization And Adjustment Based On Cluster Analysis”, Proceedings of the 2011 International Conference on Machine Learning and Cybernetics, Guilin, 10-13 July, 2011.

[28] K.Gomathi and Meera Gandhi, “Weight based clustered key management scheme using RSA for wireless mobile Ad hoc networks”, IEEE 2011.

[29] Steffen Moser, Jochen Weiß and Frank Slomka,” Towards Real-Time Media Access inVehicular Ad-Hoc Networks”, IEEE 2012.

[30] Seema Narvare, Rahul Dubey and Manish Shrivastava, " Review Paper of Performance Analysis for Random Access Channel in Wireless Network with MAC Protocol " , International Journal of Advanced Technology and Engineering Exploration (IJATEE), Volume-1, Issue-1, December-2014 ,pp.7-14.

[31] P. Sasikumar and Sibaram Khara, “K-Means Clustering In Wireless Sensor Networks”, 2012 Fourth International Conference on Computational Intelligence and Communication Networks, IEEE, 2012, pp. 140-144.

[32] P.K.Poonguzhali,” Energy Efficient Realization of Clustering Patch Routing Protocol in Wireless Sensors Network”, 2012 International Conference on Computer Communication and Informatics (ICCCI -2012), Jan. 10 – 12, 2012, Coimbatore, INDIA.

[33] Namrata Shukla" Data Mining based Result Analysis of Document Fraud Detection", International Journal of Advanced Technology and Engineering Exploration (IJATEE), Volume-1, Issue-1, December-2014 , pp.21-25.

[34] M. Bala Krishna and M. N. Doja,” Self-Organized Energy Conscious Clustering Protocol for Wireless Sensor Networks”,IEEE 2012.

[35] Jianbin Huang, Heli Sun, Qinbao Song, Hongbo Deng, and Jiawei Han,” Revealing Density-Based Clustering Structure from the Core-Connected Tree of a Network”, IEEE Transactions On Knowledge And Data Engineering, Vol. 25, No. 8, August 2013, pp. 1876-1889.

[36] Rivest, R.L., Robshaw, M.J.B., Sidney, R., & Yin, Y.L (1998a). “The RC6 Block Cipher.” URL: ftp://ftp.rsasecurity.com/pub/rsalabs/rc6/rc6v11.pdf.

Mr. Bhavesh Madan Joshi is from Gujarat and was born on 12th June 1990 in Jamnagar (Gujarat). He has done his schooling from Emmanuel Sr. Sec. School, Bundi (Rajasthan) and has completed his graduation from VNS Group of Institutions Faculty of Enginering Bhopal with 67.08%. He is a PG Scholar at VNS Group of Institutions: Faculty of Engineering, Under Rajiv Gandhi Proudhyogiki Vishwavidhyalaya,Bhopal and pursuing M.Tech. in Digital Communication and is willing to work on Data Aggregation in Wireless Sensor Network. Email: bhaveshjoshi126@gmail.com