Multi Level Cryptographic Key Sharing for Secure Access and Authorization on Cloud Platforms

Kuldeep Singh[1], Amandeep Kaur[2]

Abstract: ***Cloud computing is attracting the large user bases and now-a-days hosting the large sized application with heavy and complex calculation load. The cloud computing platforms are because being popular and user at large scales, they are also being favorite targets of the hacking groups. Some cloud computing application carry secure and personal data, which may affect the social image, security or economics of a nation, personnel, organization or other similar entities. Hence, there is always a strong requirement of the secure authorization & request and data exchange model. The security is continuous process, and the models are kept changing from time to time. Effective & Secure key management and distribution scheme play an important role for the data security in Cloud Computing. The cryptographic keys are used on different communication levels of Cloud Computing communications i.e. neighbor nodes, cluster heads and base stations. We proposed a new model presents improved key management architecture, called multi-level complex key exchange and authorizing model (Multi-Level CK-EAM) for the Cloud Computing, to enable comprehensive, trustworthy, user-verifiable, and cost-effective key management. In this research, we will develop the proposed scheme named Multi-Level CK-EAM for corporate key management technique adaptable for the Cloud Computing platforms by making them integral and confidential. To add more security, there is a next step which includes Captcha, user has to fill the correct given Captcha which eliminates the possibility of robot, botnet etc. In addition, it also has to be created in way to work efficiently with Cloud nodes, which means it must use less computational power of the Cloud computing platforms.***

Keywords: Cloud Storage, Data Security, Cloud Computing, Data Encryption, Cryptographic Key, Security Attacks

1. Introduction

Cloud Computing is where applications and files are hosted on “cloud” consisting of thousands of computers and servers, linked together and can be accessed by using Internet. Research in cloud computing is receiving a lot of attention from both academic and industrial worlds. In cloud computing, users can outsource their computation and storage to servers (also called clouds) using Internet. This frees users from the hassles of maintaining resources on-site. Clouds can provide several types of services like applications (e.g., Google Apps, Microsoft online), infrastructures (e.g., Amazon’s EC2, Eucalyptus, Nimbus), and platforms to help developers write applications (e.g., Amazon’sS3, Windows Azure). Security and privacy are thus very important issues in cloud computing. In one hand, the user should authenticate itself before initiating any transaction, and on the other hand, it must be ensured that the cloud does not tamper with the data that is outsourced. User privacy is also required so that the cloud or other users do not know the identity of the user.

2. Literature Survey

(1) Zongwei Zhou et. al. proposed “a Key management algorithm named as Key it Simple and Secure (KISS). This paper presents a new key management architecture, called KISS, to enable comprehensive, trustworthy, user-verifiable, and cost-effective key management. KISS protects the entire life cycle of cryptographic keys. In particular, KISS allows only authorized applications and/or users to use the keys. Using simple devices, administrators can remotely issue authenticated commands to KISS and verify system output.

(2) N. Suganthi, V. Sumathy, “This algorithm supports the establishment of three types of keys for each sensor node, an individual key shared with the base station, a pair wise key shared with neighbor sensor node, and a group key that is shared by all the nodes in the network. The algorithm used for establishing and updating these keys are energy efficient and minimizes the involvement of the base station. Polynomial function is used in the study”

(3) Ivan Damgård et. al. proposed “A secure key management method for cloud environments. Authors have studied the levels of security on the basis what they can and what they cannot obtain in the security models. And after studying that all, authors have proposed a light-weight protocols achieving maximal security, and report on their practical performance. They have considered fully autonomous servers that switch between online and offline periods without communicating with anyone from outside the cloud, and semi-autonomous servers that need a limited kind of assistance from outside the cloud when doing the transition. “

(4)Ramaswamy Chandramouli et. al. have worked on “ **Cryptographic Key Management Issues & Challenges in Cloud Services.** An analysis of the common state of practice of the cryptographic operations that provide those security capabilities reveals that the management of cryptographic keys takes on an additional complexity in cloud environments compared to enterprise IT environments due to: (a) difference in ownership (between cloud Consumers and cloud Providers) and (b) control of infrastructures on which both the Key Management System (KMS) and protected resources are located. This document identifies the cryptographic key management challenges in the context of architectural solutions that are commonly deployed to perform those cryptographic operations.”

(5)Marco Tiloca et. Al. proposed, “Wireless Sensor Networks (WSNs) are currently used in many application scenarios, including industrial applications and factory automation. In such scenarios, Time Division Multiple Access (TDMA) is typically used for data communication among sensor nodes. However, TDMA-based WSNs are particularly prone to Selective Jamming attack, a specific form of Denial of Service attack aimed at severely thwarting network reliability. In this paper, we present SAD-SJ, a self-adaptive and decentralized MAC-layer solution against selective jamming in TDMA-based WSNs. SAD-SJ does not need a central entity, requires sensor nodes to rely only on local information, and allows them to join and leave the network without hindering other nodes activity. We show that SAD-SJ introduces a limited overhead, in terms of computation, communication and energy consumption."

3. Problem Formulation

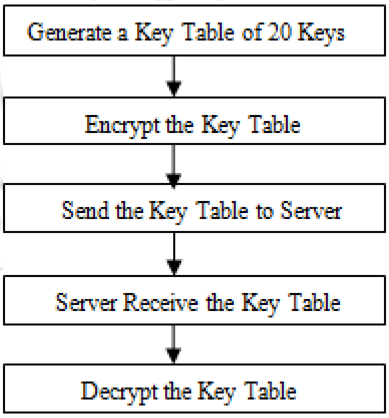
Cloud computing is attracting the large user bases and now-a-days hosting the large sized application with heavy and complex calculation load. The cloud platforms are economically competent, rather winners than the existing IT infrastructure and also comes pre-embedded with the high level features. The cloud computing platforms are because being popular and user at large scales, they are also being favorite targets of the hacking groups. Some cloud computing application carry secure and personal data, which may affect the social image, security or economics of a nation, personnel, organization or other similar entities. Hence, there is always a strong requirement of the secure authorization & request and data exchange model. The security is continuous process, and the models are kept changing from time to time. In the existing model, the key exchange model is applicable to ensure the security of the cloud platforms. The existing model uses a set of keys stored locally between the cloud servers in the cluster. A server needs to rebuild the encryption key after waking up from the sleeping period. The existing model utilizes the Diffie-Hellman key agreement scheme, which is not up to the mark and have become older scheme. Now-a-days this scheme is not considered secure against the Man in the Middle attack. Diffie-Hellman is also prone to various kinds of service denial and information stealing attacks. Because of all these reasons, the existing scheme must be improved in order to make it stronger against the attacks, which are possible on the existing scheme. In the proposed model, we are trying to solve the key-problem of data integrity and confidentiality using the effective random key exchange scheme with secure user authorization model.

4. Research Methodology

The research methodology in the dissertation focuses on multi-level cryptographic and authorization.We are proposing a improved key management architecture, called multi-level complex key exchange and authorizing model (Multi-Level CK-EAM) for the Cloud Computing, to enable comprehensive, trustworthy, user-verifiable, and cost-effective key management. Multi-Level CK-EAM protects the entire life cycle of cryptographic keys in the Cloud Computing platforms and applications. In particular, Multi-Level CK-EAM allows only authorized applications and/or users to use the keys. Using simple devices, administrators can remotely issue authenticated commands to Multi-Level CK-EAM and verify system output. In this research, we will develop the proposed scheme named Multi-Level CK-EAM for corporate key management technique adaptable for the Cloud Computing platforms by making them integral and confidential. To add more security, there is a next step which includes Captcha, user has to fill the correct given Captcha which eliminates the possibility of robot, botnet etc. In addition, it also has to be created in way to work efficiently with Cloud nodes, which means it must use less computational power of the Cloud Computing platforms.First step towards the research is the literature study of the existing algorithms for key sharing and authentication schemes for the cloud platforms. Literature study will lead towards the development of the new key exchange scheme to ensure the legitimate user session and data communication security. This is also very important to get the architecture of the existing key exchange and authentication schemes for clouds in order to know their merits and demerits.This project would be implemented in the **MATLAB** Simulator. A thorough performance and feature testing model would be formed and utilized to analyze the performance of the cloud security model based upon the key exchange scheme, to detect the flaws and to recover them.

5. Implementation

Key Generation


Generate a Key Table of 20 Keys
Encrypt the Key Table
Send the Key Table to Server
Server Receive the Key Table
Decrypt the Key Table

Basic control flow of Implemented application.-

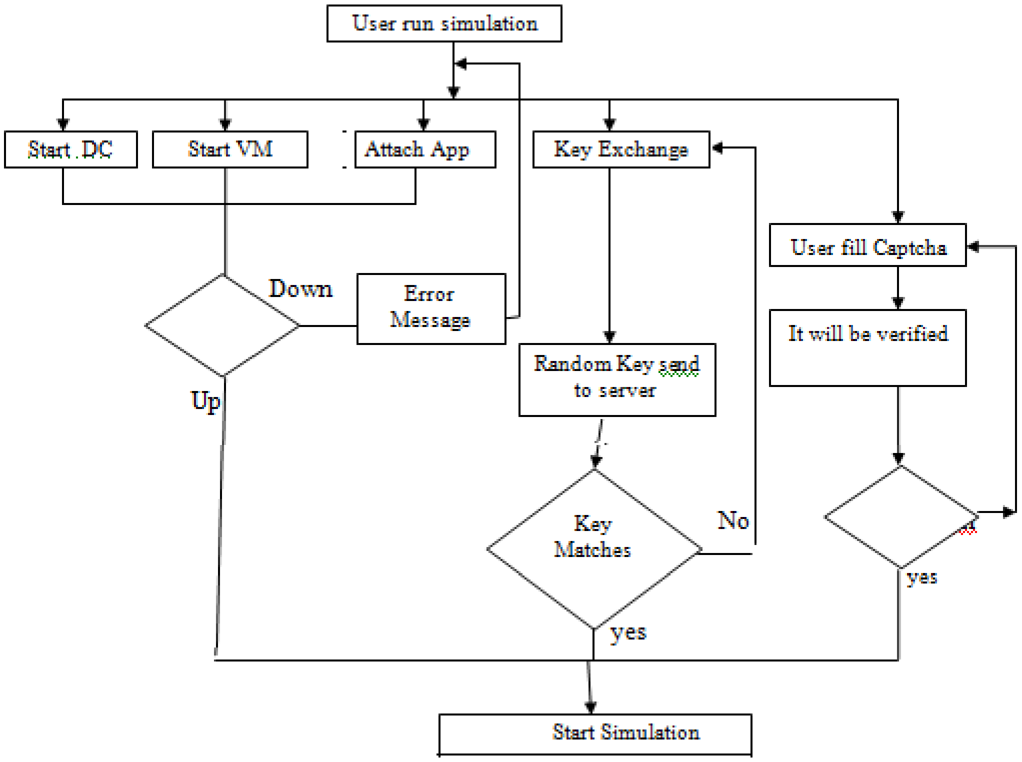


Figure 5.2: Basic control flow of Implemented application

In this research MATLAB is used to make an GUI which simulates the cloud model. This GUI makes it easier to run the application and get results. This interface has various buttons which are used to run the application for all three diffent conditions : normal simulation, attack simulation and then the implemented security simulation.

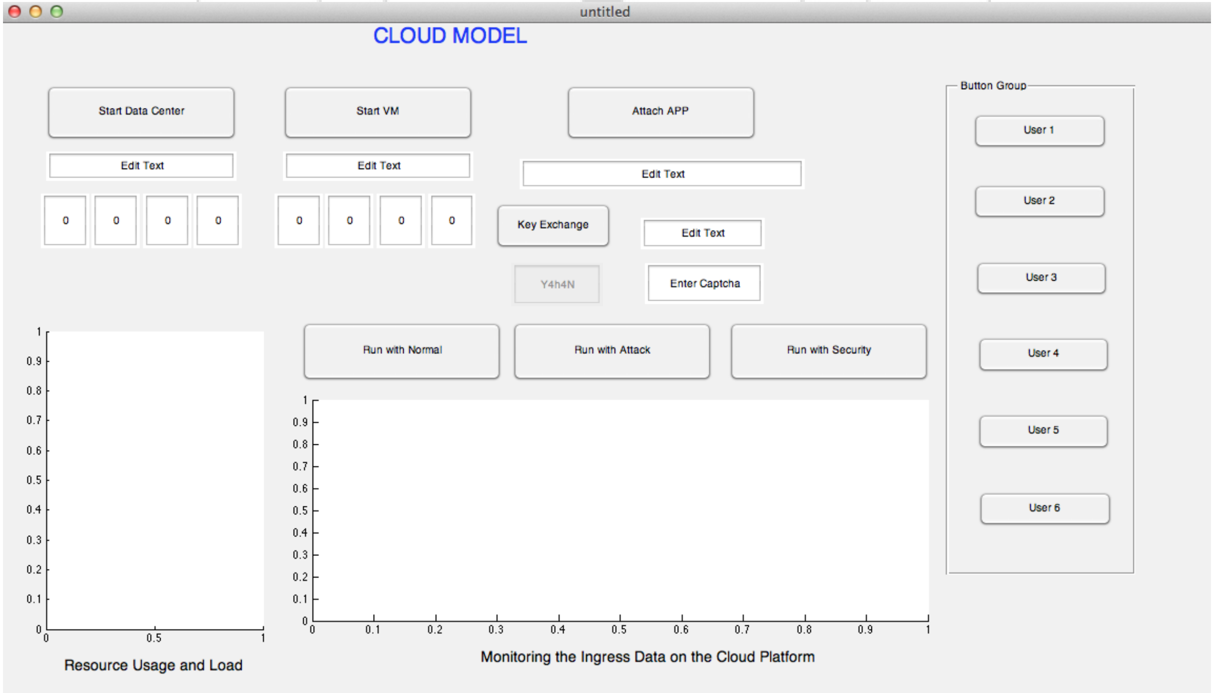
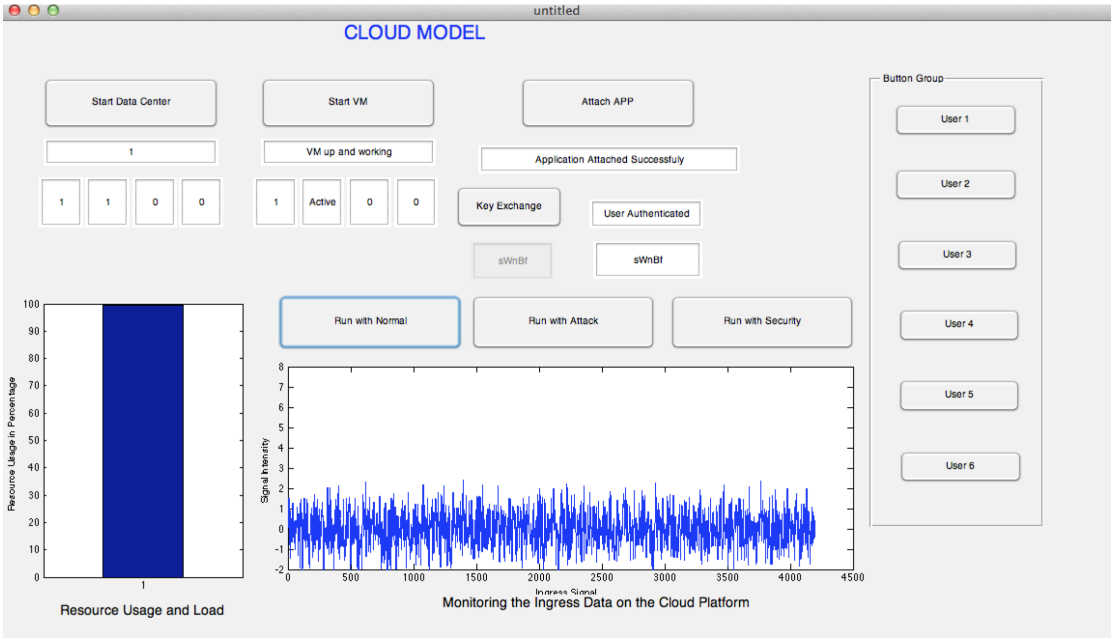


Figure 5.3: GUI for Cloud Model Simulation

Running in a normal mode

When we press the run with normal then the simulation starts which shows the normal simulation of cloud. In normal simulation mode there is no attacks and the selected no. of users are communicating with the server. This will become the basis for checking the performance of other modes. In normal execution the resource utilization is always below 100 percent mostly around 80 percent and the ingress data on the cloud platform is about 3600 bytes.

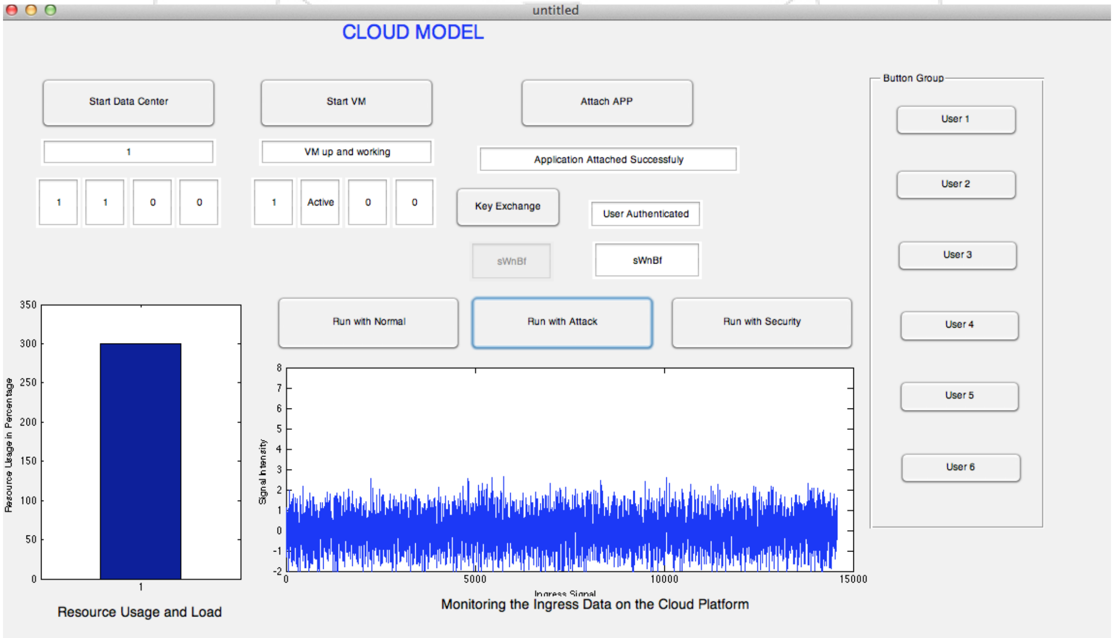


1
VM up and working
Application Attached Successfuly
1 1 0 0
1 Active 0 0
User Authenticated

Figure 6.1: Normal simulation of Cloud Model

Running in the Attack Situation

The attacks used in this model are the DDoS attacks which flood the data with large random data, so that the system hangs or takes up enormous amount of resources and ultimately breaks down. When the attack situation is simulated by using run with attack button then it can be observed that the performance is severely degraded and a large amount of data is forcefully transferred which ultimately used up all the resources. When the observation is done it is noted that the resource utilization is very high it is more than 300 percent and the ingress data on cloud is about 16000 bytes which indicate the large amount of data is transferring.



1
VM up and working
Application Attached Successfuly
1 1 0 0
1 Active 0 0
User Authenticated

Figure 6.2: Simulation of Attack in cloud model

- **Running with the implemented security scheme**

Previous section has shown the effects of DDoS attacks on the cloud model. Now the simulation is done using run with security button. In this situation the security using proposed key management scheme is implemented and same DDoS attacks are simulated on the cloud model. While running in this mode it is observed that performance is increased than the attack situation given in previous section. The resource utilization is now always below 100 percent, although a slightly higher than the normal simulation but overall there is tremendous increase in performance. The ingress data is about 16000 bytes as this also an attack situation so the huge amount of data is flooded. But the decreased resource utilization shows that the implemented security scheme successfully handles the attacks.

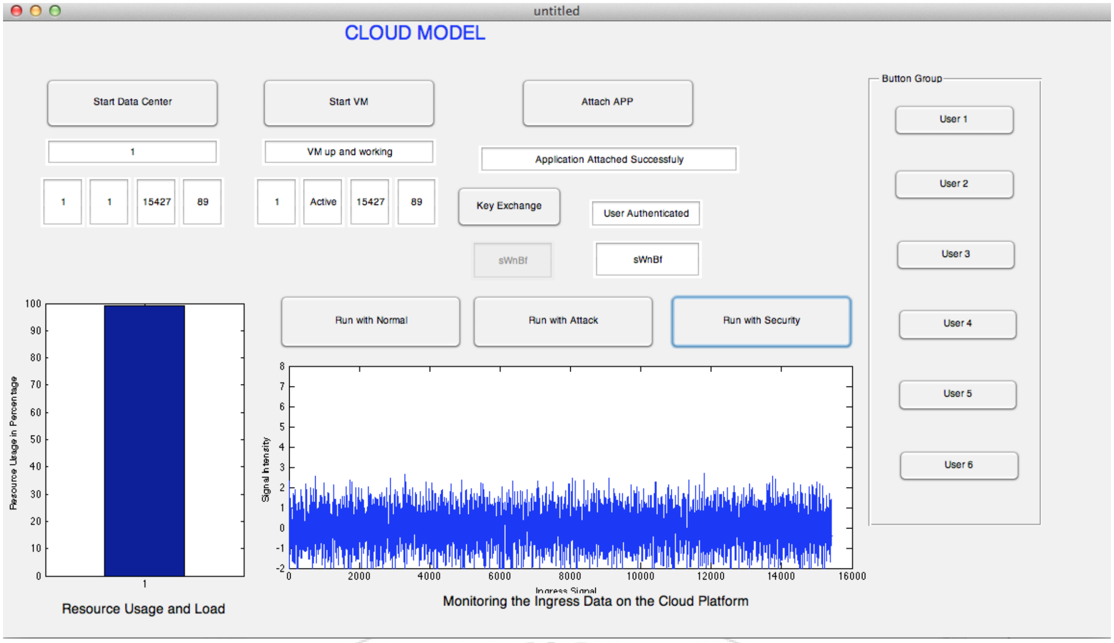


Figure 6.3: Simulation of attack with security on cloud model

6. Conclusion

The proposed model for Multi level cryptographic key for secure access has been implemented using the MATLAB simulator. The implementation of the MATLAB simulator will begin with the implementation of the Multi level cryptographic key for secure access. In future, this research presents improved key management architecture, called multi-level complex key exchange and authorizing model (Multi-Level CK-EAM) for the Cloud Computing, to enable comprehensive, trustworthy, user-verifiable, and cost-effective key management. Multi-Level CK-EAM protects the entire life cycle of cryptographic keys in the Cloud Computing platforms and applications. In particular, Multi-Level CK-EAM allows only authorized applications and/or users to use the keys. Using simple devices, administrators can remotely issue authenticated commands to Multi-Level CK-EAM and verify system output. In future, the proposed scheme named Multi-Level CK-EAM for corporate key management technique adaptable for the Cloud Computing platforms by making them integral and confidential. In addition, it also has to be created in way to work efficiently with Cloud nodes, which means it must use less computational power of the Cloud Computing platforms.

References

[1] Zongwei Zhou, Jun Han, Yue-Hsun Lin, Adrian Perrig, Virgil Gligor, "KISS: Key it Simple and Secure Corporate KeyManagement", Trust and Trustworthy Computing Lecture Notes in Computer Science, volume 7904, pp. 1-18, Springer, 2013.

[2] N. Suganthi, V. Sumathy, "Energy Efficient Key Management Scheme for Wireless Sensor Networks", vol 9, issue 1, pp. 71-78, INT J COMPUT COMMUN, 2014.

[3] Ivan Damgård, Thomas P. Jakobsen, JesperBuus Nielsen, and Jakob I. Pagter, "Secure Key Management in the Cloud", Cryptography and Coding Lecture Notes in Computer Science, volume 8306, pp. 270-289, Springer, 2013.

[4] RamaswamyChandramouli, Michaela Iorga, SantoshChokhani, " **Cryptographic Key Management Issues & Challenges in Cloud Services",** Computer Security Division Information Technology Laboratory, NIST, 2013.

[5] Marco Tiloca, Domenico De Guglielmo, GianlucaDini and Giuseppe Anastasi, "SAD-SJ: a Self-Adaptive Decentralized solution against Selective Jamming attack in Wireless Sensor Networks", ETFA, vol. 18, pp. 1-8, IEEE, 2013.

[6] Md. MonzurMorshed, Md. Rafiqul Islam, "CBSRP: Cluster Based Secure Routing Protocol", IACC, vol. 3, pp. 571-576, IEEE, 2013.

[7] Patrice Seuwou, Dilip Patel, Dave Protheroe, George Ubakanma "Effective Security as an ill-defined Problem in Vehicular Ad hoc Networks (VANETs)".

[8] SonamPaldenBarfungaPrativaRai, Hiren Kumar Deva Sarma, "Energy Efficient Cluster Based Routing Protocol for Wireless Sensor Networks", ICCCE IEEE 2012, 3-5 July 2012, Kuala Lumpur, Malaysia

[9] SajalSarkar, Raja Datta, "A Trust Based Protocol for Energy-Efficient Routing in Self-Organized MANETs", IEEE 2012.

[10] Said BEN ALL*, Abdellah EZZATI, Abderrahim BENI HSSANE, MoulayLahcen HASNAOUI, "Hierarchical Adaptive Balanced energy efficient Routing Protocol (HABRP) for heterogeneous wireless sensor networks", IEEE, 2010

[11] XU Jiu-qiang, WANG Hong-chuan,LANGFeng-gao,WANGPing,HOU Zhen-peng, "Study on WSN Topology Division and Lifetime", IEEE, 2011