International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 2 Issue: 7
ISSN: 2454-4248
01 – 06

A Novel Encryption Scheme for Providing Security and Energy Efficiency in Mobile Ad Hoc Networks

Ms. Shafiqua C. Pathan[1],Mr. Vikash Kumar[2]

[1]Student,Dept. Of Computer Science and Engineering ,ACE Nagthana,Wardha, Maharashtra,India.
[1]shafiquapathan@gmail.com

Abstract-A Mobile Ad Hoc Network is a decentralized kind of remote system. It doesn't have any altered foundation and the hubs can impart straightforwardly between one another. Because of its open nature issues like security and vitality utilization emerges. This paper presents an in number encryption calculation keeping in mind the end goal to expand dependability and security for MANETs. At the point when huge volume of information is to be sent, information pressure method is a straightforward procedure, with the advantage of diminishing the transmission rate that devours less transfer speed and low power. Lempel –Ziv – Welch (LZW) pressure calculation when connected on coded message assists in furnishing security with low battery utilization. Such a plan composed practically speaking will help in building secure MANET based application.

Keywords: *MANETs, Security, Energy Consumption, Encryption, Compression.*

*****

1. INTRODUCTION

An impromptu system is a decentralized kind of remote system. Portable Ad hoc Networks is a hearty base less remote system having versatile hubs. It doesn't have any altered base and the hubs can impart straightforwardly between one another. It is comprised of different hubs joined by connections. A MANET can be made either by portable hubs or by both static and element versatile hubs. A versatile hub has self-assertively connected with one another framing formally dressed topologies. They serve up as both switches and hosts. The capacity of portable switches to self-arrange makes this innovation suitable for provisioning correspondence to, for occasion, catastrophe strike territories where there is no correspondence framework, discussions, or in a fiasco pursuit and salvage operations where a system association is in a split second obliged [5].

1.1 LIMITATIONS OF MOBILE AD HOC NETWORKS (MANET)

A mobile ad-hoc network (MANET) is a self-configuring network where nodes connected by wireless links can move freely and thus the topology of the network changes constantly. Some issues of ad hoc networks are the limitations that affect the efficient operation, particularly when implementing security techniques and challenges that need to be taken into consideration to build an efficient network. However, designing new security protocols and mechanisms is constrained by the capabilities of the sensor nodes [1]. It is important to understand the constrained capabilities of sensor nodes to develop proper security that balances demanding security performance against sensor nodes' limitations.

1. Limited resources

The main obstacle for adopting complex security mechanisms is the limited resources that sensor nodes have. Although their limited size makes them attractive for use in a number of situations, at the same time their size affects resources such as the energy, computational power, and storage available.

2. Power restrictions

The power restrictions of sensor nodes are raised due to their small physical size and lack of wires. Since the absence of wires results in lack of a constant power supply, not many power options exist [2]. Sensor nodes are typically battery-driven. The power is used for various operations in each node, such as running the sensors, processing the information gathered and data communication. Keep in mind that communication between sensor nodes consumes most of the available power, much more than sensing and computation, power limitations greatly affect security. Encryption algorithms introduce a communication overhead between the nodes. More messages are exchanged, i.e. for key management purposes, and also messages become larger as authentication, initialization and encryption data are included.

3. Limited Computational power

In case of computational power, computations are linked with the available amount of power. Since there is limited amount of power, computations are constrained also. More power is used for communication than computations. Since the power for computations is even more constrained than the total quantity of power, complex security solutions are prohibited. The limitation of computational power limits the adoption of strong cryptographic algorithms such as the RSA public key algorithm, which is computationally expensive. Instead, symmetric encryption algorithms are used to secure sensor nodes' communication, since symmetric encryption does not have as demanding computational requirements as asymmetric encryption. Therefore, another challenge is to design appropriate algorithms to establish and verify trust among the nodes participating in a communication.

 ISSN: 2454-4248
01 – 06

1.2 BASICS OF CRYPTOGRAPHY

Cryptography is the practice and study of hiding information [3]. Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce.

Cryptography is referred exclusively to encryption, which is the process of converting ordinary information (called plain-text) into unintelligible form (called cipher-text). [4] Decryption is the reverse process, i.e. moving from the unintelligible cipher-text back to plain-text. A cipher is a pair of algorithms that create the encryption and the reversing decryption. The detailed operation of a cipher is controlled both by the algorithm and in each instance by a secret parameter -the key. Cryptanalysis is the term used for the study of methods of obtaining the meaning of encrypted information without access to the key. Cryptographic primitives are required by the security protocols and mechanisms in order to integrate the security properties into their operations. These cryptographic primitives are Symmetric Key Cryptography (SKC), Public Key Cryptography (PKC), and Hash Functions.

NEED FOR CRYPTOGRAPHY IN MOBILE AD HOC NETWORKS

Security requirements often vary with application, but in general, security for Mobile Ad hoc Networks should focus on the protection of the data itself and the network connection between the nodes. Confidentiality, integrity and authentication are the most important data security concerns [3]. When considering the network itself, we need to protect access to communication channels. We must defend against malicious resource consumption, denial of service, node capture and node injection. The encryption-decryption techniques devised for the traditional wired networks are not feasible to be applied directly for the wireless networks and in particular for Mobile Ad hoc Networks since MANET consist of tiny sensors which really suffer from the lack of resources like processing memory and battery power. Applying any encryption scheme requires transmission of extra bits, hence extra processing memory and battery power which are very important resources for the sensors‘ longevity. Applying the security mechanisms such as encryption could also increase delay, jitter and packet loss in wireless sensor networks. Moreover, some critical questions arise when applying encryption schemes to MANETs which include how the keys are generated or disseminated, how the keys are managed, revoked, assigned to a new sensor node being added to the network or how the keys are renewed for ensuring robust security for the network.

1.3 BASICS OF COMPRESSION

Another vital and basic method for diminishing force utilization is Data Compression, which expends less power by transmitting compacted information results expanding in battery life. The information pressure calculations are ordered into lossless pressure and lossy pressure.

A lossless system is that the restored information record is indistinguishable to the first. Because of pressure, the quantity of bits can be decreased to most extreme broaden so that the need of memory and data transfer capacity are less. Additionally, the compacted content looks like a scramble message and an assailant in center can't ready to get it. Along these lines, the information pressure not just diminishes the first's measure content, additionally gives information security. A decompression system gives back the data to its unique structure [5].

As vitality utilization and security are two primary issues if there should arise an occurrence of portable impromptu systems, the venture fundamentally concentrates on these two issues. In this task, we endeavor to utilize an in number encryption plot that can completely abuse the security issue in versatile specially appointed systems. What's more, this task likewise incorporates pressure strategy alongside most limited way calculation that will thusly spare the vitality amid the transmission of information in portable specially appointed systems.

2. RELATED WORK

In this paper, creator proposed another strategy to influence system coding to decrease the vitality devoured by information encryption in MANETs. To this end, creator proposed P-Coding, a lightweight encryption plan to give privacy to network-coded MANETs in a vitality effective way. The fundamental thought of P-Coding is to let the source haphazardly permute the images of every parcel, before performing system coding operations. Without knowing the stage, busybodies can't find coding vectors for right deciphering, and in this manner can't get any significant data and shows that because of its lightweight nature. P-Coding brings about negligible vitality utilization contrasted with other encryption plans. Yet, in this paper, for encoding information creator utilized Homomorphic Encryption Functions (HEFs) which is weak plan [1].

This paper presents various issues associated with the Mobile Ad-hoc Networks. It presents survey of different kind of solution to these problems in wired networks and in ad hoc networks. In this paper a new approach is proposed. Which presents an in number encryption calculation keeping in mind the end goal to expand dependability and security for MANETs. AndLempel –Ziv – Welch (LZW) compression algorithm is proposed which is when applied on coded message helps in providing security with low battery consumption [2].

In this paper, creator proposed P-Coding, a novel security plan against listening stealthily assaults in system coding. With the lightweight change encryption performed on every message and its coding vector, P-Coding can effectively foil worldwide busybodies in a straightforward manner. Besides, P-Coding is likewise included in adaptability and power, which empower it to be coordinated into handy system coded frameworks [3].

This paper tended to the configuration of secure direct system coding. What's more, particularly, explore the

 ISSN: 2454-4248
01 – 06

system coding outline that can both fulfill the pitifully secure prerequisites and amplify the transmission information rate of various unicast streams between the same source and destination pair. To this end, creator has created productive calculation that has the capacity locate the ideal unicast topology in a polynomial measure of time [4].

3. PROPOSED APPROACH

The proposed work is planned to be carried out in the following manner:

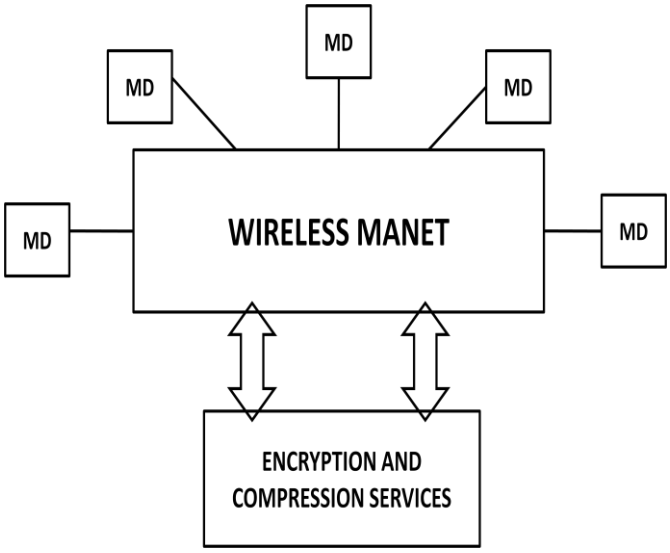

Fig -1: Basic System Architecture

An impromptu system is a decentralized kind ofremote system. Portable Ad hoc Networks is a hearty baseless remote system having versatile hubs. It doesn't have anyaltered base and the hubs can impart straightforwardlybetween one another. It is comprised of different hubsassociated by connections. A MANET can be made eitherby versatile hubs or by both static and element portablehubs. A versatile hub has self-assertively connected withone another framing formally dressed topologies. Theyserve up as both switches and has. As the information istransmitted among the different hubs with no foundation,security and vitality utilization issues emerges in Mobile AdHoc Networks. Proposed framework essentially managesthese two noteworthy issues of MANET.

Following figure shows the flowchart of design:

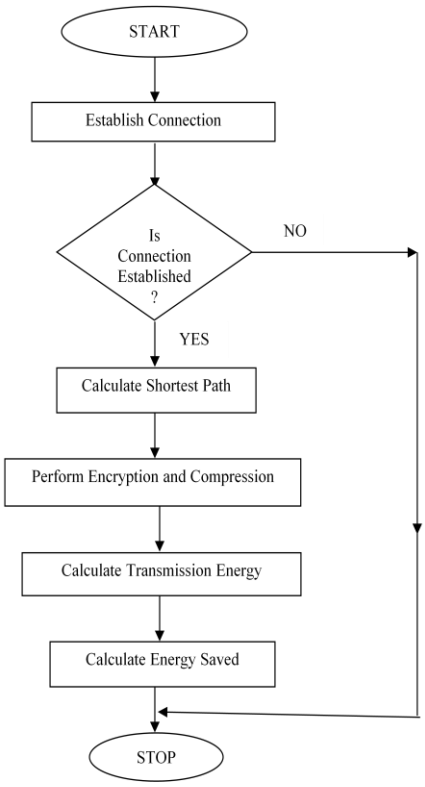

Fig-2: Flowchart of Design

Fig. 1 indicates fundamental framework design ofproposed framework. Firstly, the information which is to betransmitted is being scrambled utilizing a solid encryptionplan as a part of request to manage the security issues thatemerges amid transmission of information. At that point, the scrambled information is packed with a viable pressure planwhich thus diminishes the vitality utilization amidtransmission. In this manner, proposed frameworkespecially concentrates on explaining fundamental issues inMobile Ad Hoc Networks.

Advantages of Proposed System

1. As in proposed system we will be using heavy encryption scheme along with compression, it will give better throughput with better efficiency.

2. Use of strong encryption scheme with hashing algorithm will provide better security to the message during the transmission.

3. Use of effective compression scheme will help to reduce the energy consumption during the transmission of data as well as will provide security to the encrypted message.

4. METHODOLOGY

4.1 Simulating Nodes in MANET

Computer simulation is a simulation, run on a single computer, or a network of computers, to produce

 ISSN: 2454-4248
01 – 06

behavior of the system. PC reenactment is a reproduction, keep running on a solitary PC, or a system of PCs, to deliver conduct of theframework. The reproduction utilizes a unique model to mimic the framework. PC recreation utilizes scientific portrayal or model of a genuine framework as a PC program.

4.2 Encryption Scheme

Answer for giving security inside of MANETs proposes scrambling the message before sending it i.e. Cryptography empowers the client to transmit classified data over any unstable system with the goal that it can't be utilized by an interloper. Cryptography is the procedure that includes encryption and unscrambling of content utilizing different components or calculations. In this way, in proposed framework the information which is to be transmitted will be scrambled utilizing solid hashing calculation.

4.3 Compression Scheme

Another essential and straightforward strategy for lessening power utilization is Data Compression, which devours less power by transmitting compacted information results into expanded battery life. At the point when expansive volume of information is to be sent, information pressure method is a basic system, with the advantage of lessening the transmission rate that expends less transfer speed and low power. Lempel –Ziv – Welch (LZW) pressure calculation when connected on coded message assists in giving security low battery utilization.

4.4 Shortest Path Computation

At the point when the information is to be transmitted starting with one hub then onto the next in Mobile Ad Hoc Networks, the most brief way will be computed utilizing digkstra's calculation, so that the vitality amid the transmission can be decreased.

4.5 Energy Saving Using Low Size Transfer

As the information which is to be transmitted is in packed and scrambled structure, decreases vitality utilization amid the transmission of information in Mobile Ad Hoc Networks. And in addition before transmitting the information starting with one hub then onto the next, most limited way will be discovered utilizing Dijkstra calculation, which will thusly spare the vitality amid transmission.

5. DESIGN WORK

5.1 Source

Firstly, sender has to establish connection with the destination by entering its IP address. And once the connection get established sender selects the file which is to be transmitted. The file is transmitted along with the encryption and compression performed and the secret key is generated.

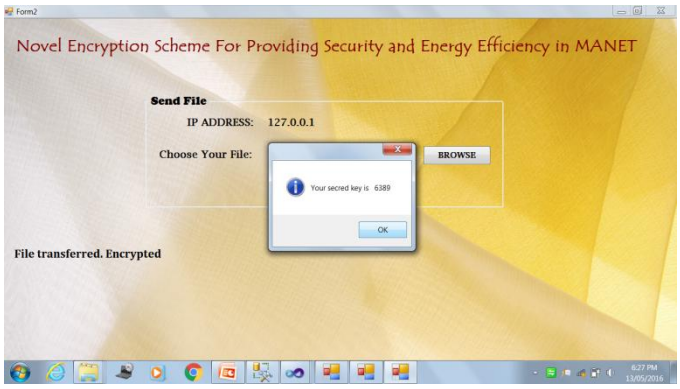

Fig -3: File Encryption

5.2 Router

This shows the system model which is considered as a typical MANET consisting of N nodes, each of which can be a source. The MANET can be modeled as an acyclic directed graph. It finds out the shortest path between source and destination using Dijkstra Algorithm.

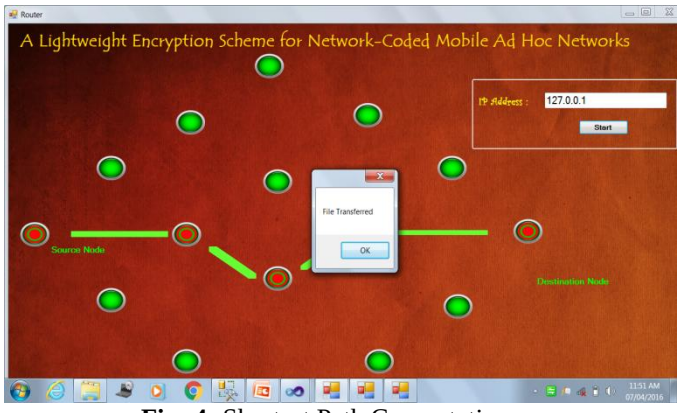

Fig -4: Shortest Path Computation

5.3 Destination

At the receiving end, user has to specify the location where the file is to be stored and enter the secret key generated. If the secret key matches the file get stored on the specified location. And Transmission Energy and Saved Energy get calculated. Otherwise, it will pop up an error message.

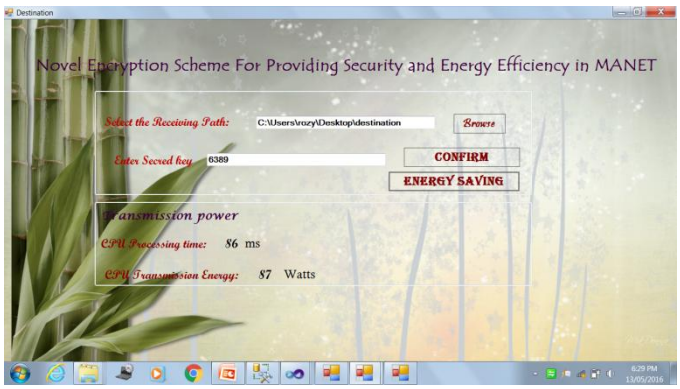

Fig -5: Transmission Time and Energy Calculation

 ISSN: 2454-4248
01 – 06

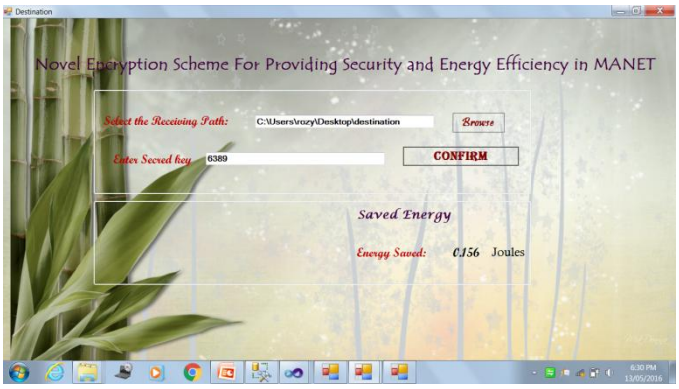

Fig -6: Saved Energy

6. RESULTS AND DISCUSSION

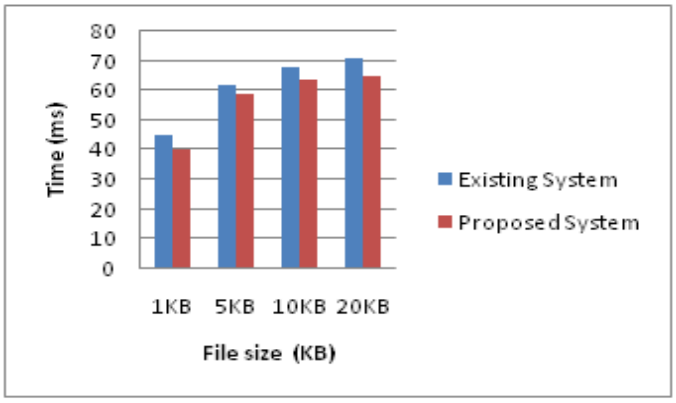

Fig-7: Transmission Time Vs File size

The above graph shows comparison between proposed system and existing system with respect to File Size (KB) and Transmission Time (ms).

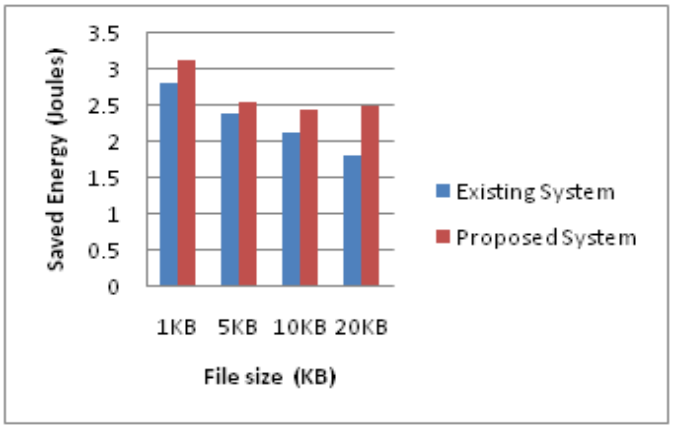

Fig-8: Saved Energy Vs File size

The above graph shows comparison between proposed system and existing system with respect to File Size (KB) and Saved Energy (Joules).

7. CONCLUSION AND FUTURE SCOPE

Mobile Ad hoc Network systems are vulnerable to security issues and can't employ heavy encryption scheme due to low life and heavy energy consumption. In the proposed work, we have proposed a way to employ heavy encryption scheme at the same time improve energy efficiency with the help of compression scheme.

From the results we can see that even after employing strong encryption scheme, the energy efficiency is not reduced and lifetime of MANET is maintained.

In Mobile Ad Hoc Networks security and energy consumption are two major issues. Thus, in future MANETs security can be improved by using multiple encryption algorithms at the same time. A faster compression algorithm can be developed in order to reduce transmission time. And the project can also be extended to transfer different kinds of files.

REFERENCES

[1]P. Zhang, C. Lin, Y. Jiang, Y. Fan, X. Shen, "A Lightweight Encryption Scheme For Network-Coded Mobile Ad Hoc Networks", IEEE Transactions On Parallel And Distributed Systems, Vol. 25, No. 9, September 2014.

[2]Shafiqua C. Pathan, Prof. D. S. Dabhade, Prof. Dhananjay M. Sable,"A novel encryption scheme for proving security and energy efficiency in mobile ad hoc networks", International Journal on Recent and Innovation Trends in Computing and Communication Volume: 4 Issue: 1, January 2016.

[3]P. Zhang, C. Lin, Y. Jiang, Y. Fan, X. Shen, "P-coding: Secure Network Coding against Eavesdropping Attacks" , IEEE Transactions on Parallel and Distributed Systems, March 2010.

[4]J. Wang, J. Wang, K. Lu, B. Xiao, and N. Gu, "Optimal Linear Network Coding Design for Secure Unicast With Multiple Streams" , IEEE Transactions on Parallel and Distributed Systems, March 2010.

[5]RehamAbdellatifAbouhogail, "Security Assessment for Key Management in Mobile Ad Hoc Networks",International Journal of Security and Its Applications Vol.8, No.1, 2014.

[6]Prachi Sharma, S.V. Pandit, *"Energy Efficient and Low Cost Oriented High Security Method For MANET: A Review"*, International Journal of Application or Innovation in Engineering & Management, Volume 3, Issue 3, March 2014.

[7]LeventErtaul and Vaidehi,"Implementation of Homomorphic Encryption Schemes for Secure Packet Forwarding in Mobile Ad Hoc Networks (MANETs)" , International Journal of Computer Science and Network S 132 ecurity, VOL.7 No.11, November 2007.

[8]Sonali Kulkarni, M. S. Chaudhari, "Energy Efficient Encryption Scheme for Secure Transmissions in Mobile Ad Hoc Networks",International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 9, September 2014.

[9]Y. Fan, Y. Jiang, H. Zhu, and X. Shen, "An Efficient Privacy- Preserving Scheme Against Traffic Analysis in Network Coding" , in Proc. IEEE INFOCOM, pp. 2213-2221, April 2009.

 ISSN: 2454-4248
01 – 06

[10]N.R. Potlapally, S. Ravi,A.Raghunathan, andN.K. Jha, "A Study of the Energy Consumption Characteristics of Cryptographic Algorithms and Security Protocols", IEEE Transactions on Mobile Computing, vol. 5, no. 2, pp. 128-143, Feb. 2006.
[11]Y. Wu, P. Chou, and S. Kung, "Minimum-Energy Multicast in Mobile Ad Hoc Networks using Network Coding" , IEEE Transactions Commun., vol. 53, no. 11, pp. 1906-1918, Nov. 2005.
[12]Sumati Ramakrishna Gowda,P.SHiremath,"Review of Security Approaches in Routing Protocol in Mobile Adhoc Network" , IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 1, No 2, January 2013.
[13]Reena Rani, ReenaThakral. "Review On Mobile Ad Hoc Network",Journal of Global Research in Computer Science, Volume 4, No. 4, April 2013.
[14]TanuPreet Singh, ShivaniDua, Vikrant Das, "Energy-Efficient Routing Protocols In Mobile Ad-Hoc Networks",International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 1, January 2012.
[15]May Cho Aye and Aye Moe Aung, "Energy Efficient Multipath Routing ForMobile Ad Hoc Networks" ,International Journal of Information Technology, Modeling and Computing (IJITMC) Vol. 2, No.3, August 2014.
[16]Saleh Ali K.Al-Omari, Putra Sumari, "An Overview Of Mobile Ad Hoc Networks For The Existing Protocols And Applications" , International journal on Applications of Graph Theory in Wireless Ad Hoc Networks and Sensor Networks, Volume 2, No. 1, March 2010.
[17]Ali Dorri ,Seyed Reza Kamel, Esmailkheyrkhah, "Security Challenges In Mobile Ad Hoc Networks: A Survey" , International Journal of Computer Science & Engineering Survey (IJCSES) Vol.6, No.1, February 2015.
[18] RenuDalal,Yudhvir Singh , Manju Khari, "A Review on Key Management Schemes in MANET" , International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.4, July 2012.
[19]Ms. Pallavi.S, Mr. SanthoshKumar.G, "Enhanced P-Coding: An Energy Saving Encryption Scheme For Mobile Ad Hoc Networks" ,International Journal of Advance Research In Science And Engineering IJARSE, Vol. No.3, Issue No.6, June 2014.
[20]J.P. Vilela, L. Lima, and J. Barros, "Lightweight Security for Network Coding" , in Proc. IEEE ICC, May 2008, pp. 1750-1754.