International Journal of Research
Available at https://edupediapublications.org/journals

p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 10
June 2016

Securing group based System and Providing key privacy in Multimedia Key Agreement System

Ms. Shafiqua C. Pathan[1] & Prof. Dhananjay M. Sable[2]

[1]Student, Dept. Of Computer Science and Engineering , ACE Nagthana, Wardha, Maharashtra,India.
[1]shafiquapathan@gmail.com
[2]Professor,Dept. Of Computer Science and Engineering , ACE Nagthana, Wardha, Maharashtra,India.
[2]dhananjay.sable165@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].

Answer for giving security inside MANETs recommends encoding the message before sending it i.e. Cryptography. Cryptography empowers the client to transmit private data over any unreliable system so that it can't be utilized by a gatecrasher. Cryptography is the procedure that includes encryption and decoding of content utilizing different components or calculations. There are two general classes of cryptographic calculations [1].

The first is named Symmetric Key Cryptography which characterizes a common key between every pair of hubs. On the off chance that every single shared key are the same, the technique will be called Shared Key Cryptography. Samples incorporate DES and AES. Yet, symmetric-key cryptography has a few constraints. One noteworthy impediment is the key dispersion issue. In this technique, trading off every hub results in annihilating security in the entire system.

The second cryptographic calculation is called Asymmetric Cryptography. In this sort of cryptography every hub has two keys, open key and private key. People in general key of every hub is open for any hub and the private key is known just by the key's proprietor. Here, if a hub needs to make an impression on another, it ought to scramble the message by the destination hub's open key. The scrambled message won't be unscrambled other than with the private key that is known just by the destination hub. In distinctive systems that utilization lopsided cryptography, there exists an outsider or a gathering of appropriated outsiders that creates a foundation. As talked about some time recently, MANETs don't have any base or server, so there is no outsider. Utilizing topsy-turvy cryptography as a part of MANETs without outsider or whatever other framework, prompts store people in general keys of all hubs in each one [4].

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. And Lempel –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 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].

This paper introduces most issues of securing key administration in specially appointed systems. It displays a review of diverse sorts of key administration conventions in wired systems and in specially appointed systems. It displays the most widely recognized sorts of assaults in impromptu systems. Another proficient methodology is proposed. It is in light of separating the individuals into bunches. This plan expects a most extreme permitted number of individuals in every group. This lessens the obliged number of encryption and decoding operations for every join operation in the group [5].

This paper presents new change encryption plan P-Coding in blend with system coding to build throughput, unwavering quality and security for MANETs. At the point when substantial volume of information is to be sent, information pressure method is a straightforward procedure, with the advantage of lessening the transmission rate that expends less data transfer capacity and low power. Subsequently, creator proposed a strategy which consolidates encryption with pressure keeping in mind the end goal to spare vitality utilization amid the transmission of information. For this reason, creator picked Lempel –Ziv – Welch (LZW) pressure calculation which is when connected on coded message assists in giving security low battery utilization [6].

3. PROPOSED APPROACH

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

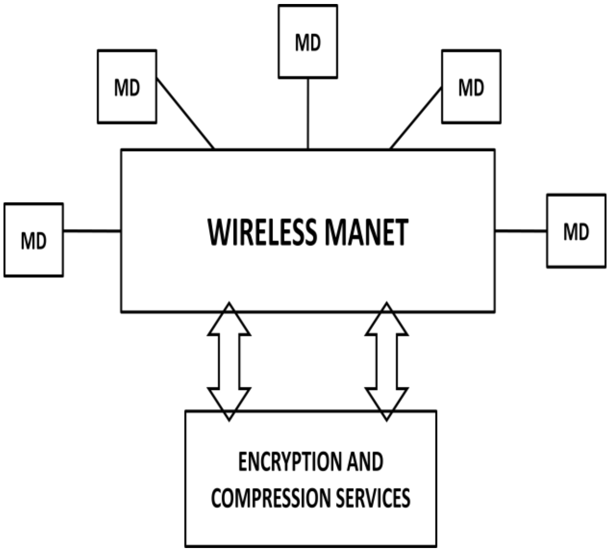


Fig -1: Basic System Architecture

An impromptu system is a decentralized kind 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 associated by connections. A MANET can be made either by versatile hubs or by both static and element portable hubs. A versatile hub has self-assertively connected with one another framing formally dressed topologies. They serve up as both switches and has. As the information is transmitted among the different hubs with no foundation, security and vitality utilization issues emerges in Mobile Ad Hoc Networks. Proposed framework essentially manages these two noteworthy issues of MANET.

Following figure shows the flowchart of design:

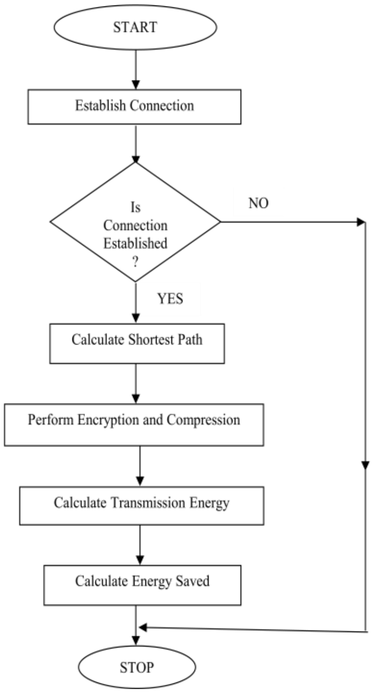

START
Establish Connection
Is Connection Established ?
NO
YES
Calculate Shortest Path
Perform Encryption and Compression
Calculate Transmission Energy
Calculate Energy Saved
STOP

Fig -2: Flowchart of Design

Fig. 1 indicates fundamental framework design of proposed framework. Firstly, the information which is to be transmitted is being scrambled utilizing a solid encryption plan as a part of request to manage the security issues that emerges amid transmission of information. At that point, the scrambled information is packed with a viable pressure plan which thus diminishes the vitality utilization amid transmission. In this manner, proposed framework especially concentrates on explaining fundamental issues in Mobile Ad Hoc Networks.

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 behavior of the system. PC reenactment is a reproduction, keep running on a solitary PC, or a system of PCs, to deliver conduct of the framework. 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

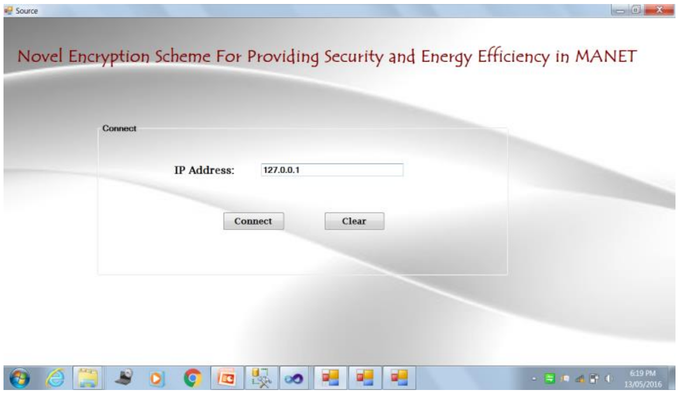
As the information which is to be transmitted is in packed and scrambled structure, decreases vitality utilization amid the transmission of information in Mobile Ad Hoc Networks. And in addition before transmitting the information starting with one hub then onto the next, most limited way will be discovered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

4.6

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.



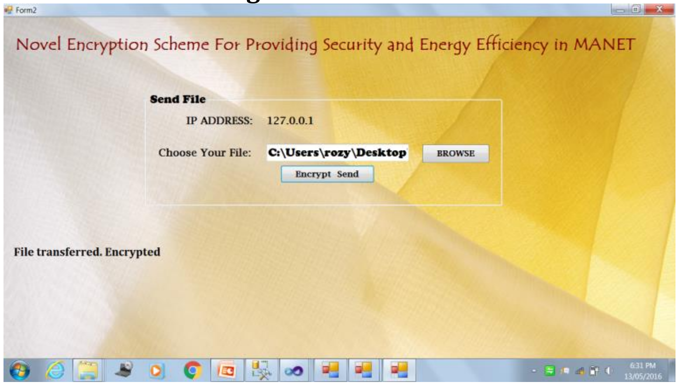
Source

Novel Encryption Scheme For Providing Security and Energy Efficiency in MANET

Connect

IP Address: 127.0.0.1

Fig -3: Establish Connection



Form2

Novel Encryption Scheme For Providing Security and Energy Efficiency in MANET

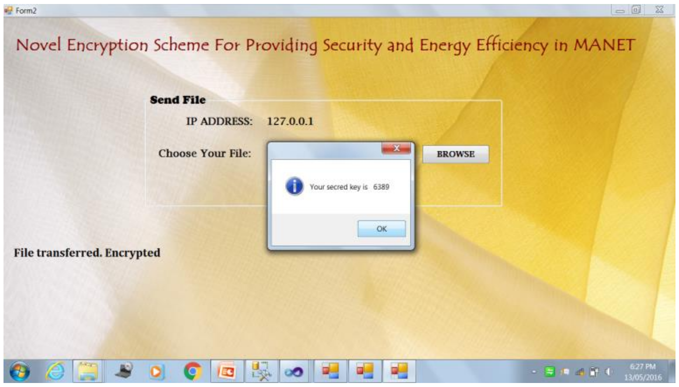
Send File

IP ADDRESS: 127.0.0.1

Choose Your File: C:\Users\rozy\Desktop

File transferred. Encrypted

Fig -4: Browse File



Form2

Novel Encryption Scheme For Providing Security and Energy Efficiency in MANET

Send File

IP ADDRESS: 127.0.0.1

Choose Your File:

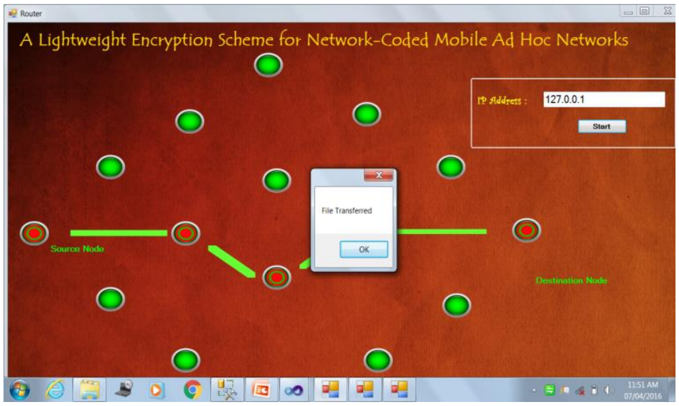
Your secred key is 6389

File transferred. Encrypted

Fig -5: 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.


Router
A Lightweight Encryption Scheme for Network-Coded Mobile Ad Hoc Networks
IP Address :
Start
Source Node
Destination Node
OK
11:51 AM
07/04/2016

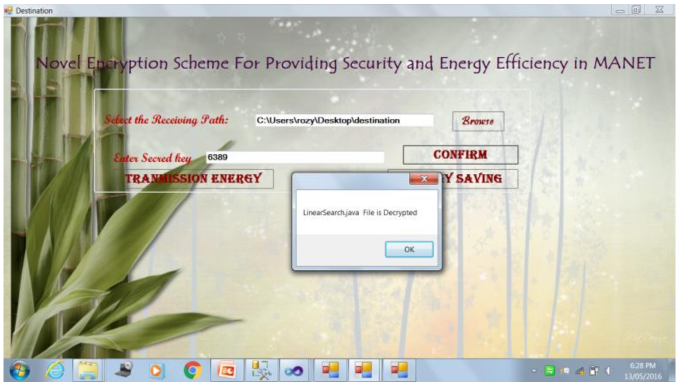
IP Address : 127.0.0.1

File Transferred

Fig -6: 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.

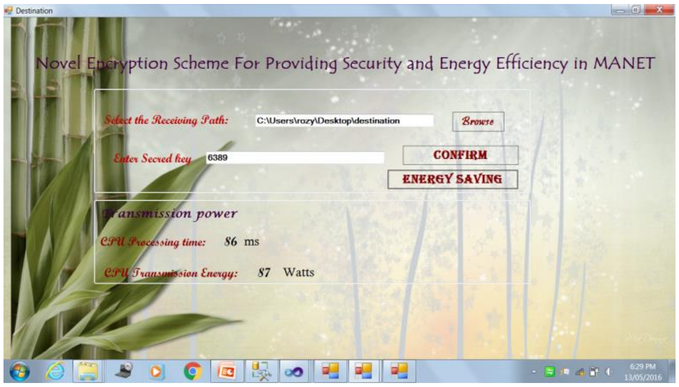

Destination
Novel Encryption Scheme For Providing Security and Energy Efficiency in MANET
Browse
CONFIRM
TRANMISSION ENERGY
Y SAVING
OK
6:28 PM
13/05/2016

Select the Receiving Path: C:\Users\rozy\Desktop\destination

Enter Secred key 6389

LinearSearch.java File is Decrypted

Fig -7: File Decryption


Destination
Novel Encryption Scheme For Providing Security and Energy Efficiency in MANET
Browse
CONFIRM
ENERGY SAVING
Transmission power
6:29 PM
13/05/2016

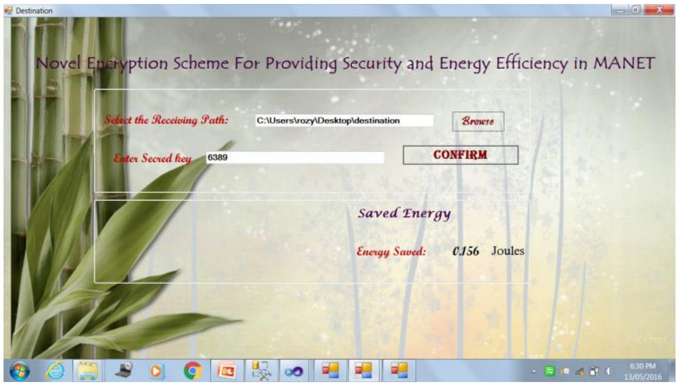
Select the Receiving Path: C:\Users\rozy\Desktop\destination

Enter Secred key 6389

CPU Processing time: 86 ms

CPU Transmission Energy: 87 Watts

Fig -8: Transmission Time and Energy Calculation


Destination
Novel Encryption Scheme For Providing Security and Energy Efficiency in MANET
Browse
CONFIRM
Saved Energy
6:30 PM
13/05/2016

Select the Receiving Path: C:\Users\rozy\Desktop\destination

Enter Secred key 6389

Energy Saved: 0.156 Joules

Fig -9: Saved Energy

6. CONCLUSION

MANET requires high energy usage for heavy encryption scheme so for normal usage user refer lightweight encryption schemes which makes system vulnerable to attacks. In proposed system we used heavy AES encryption algorithm with data compression so that the security and energy efficiency can be maintained at the same time.

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]Reham Abdellatif Abouhogail, "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]Levent Ertaul 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.

[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.S Hiremath, "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, Reena Thakral. "Review On Mobile Ad Hoc Network",Journal of Global Research in Computer Science, Volume 4, No. 4, April 2013.

[14]Tanu Preet Singh, Shivani Dua, 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, Esmail kheyrkhah, "Security Challenges In Mobile Ad Hoc Networks: A Survey" , International Journal of Computer Science & Engineering Survey (IJCSES) Vol.6, No.1, February 2015.

[18] Renu Dalal,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. Santhosh Kumar.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.