International Journal of Scientific Research & Engineering Trends
Volume 3, Issue 5, Sept.-2017, ISSN (Online): 2395-566X

Evolutionary Algorithm Based Optimized Encryption Scheme for Mobile Ad-Hoc Network

Neha Dwivedi, Dr. Rajesh Shukla
Department of Computer Science & Engineering, SIRT, Bhopal
Email: dwivedi.neha001@gmail.com

***Abstract* – In the proposed study work described in above section provides the design and implementation of ACO and P-Coding based routing protocol. To identify the need of protocol, various techniques by which we get the problem domain and the solution domain. This dissertation studied the problem of energy saving in MANETs based on the technique of network coding. Previous studies demonstrated that network coding can reduce energy consumption with less transmission in MANETs. Proposed optimized P-Coding, a lightweight scheme on top of network coding, to further reduce energy consumption in MANETs by cutting the security cost. For optimization proposed technique use ant colony optimization scheme. Optimized P-Coding exploits the intrinsic security property of network coding, and uses simple permutation encryptions to generate considerable confusion to eavesdropping adversaries. Optimized P-Coding is efficient in computation, and incurs less energy consumption for encryptions/decryptions.**

***Keywords* – MANET, P-Code, ACO, Evolutionary Algorithm, Encryption.**

I. INTRODUCTION

Ad-hoc wireless network is a distributed kind of wirelessly connected network. The ad-hoc nature demonstrates that, it does not depend on a pre-existing infrastructure, like routers in wired networks. In wired networks, there is an access point which is connected to all other devices in network for communication. Instead in wireless network, each node contributes in routing by forwarding data to other nodes. Energy saving is a major issue in ad-hoc wireless networks. In ad-hoc wireless network, energy consumption is based on number of data transmission. This means, more number of transmissions is equal to more energy consumption and less number of transmissions is equal to less energy consumption. We studied that network coding uses less transmission, so that network coding can used to reduce energy consumption in ad-hoc wireless network. With network coding energy can be reduce by help of encryption/decryption of data, due to encryption/decryption data transmission will be more secure from external users, this will create confusion to eavesdropper and eavesdropper cannot detect the actual data. Data also contains redundant data and false data that has to be eliminated or reduce for better performance of ad-hoc wireless network.

II. RELATED WORK

There have some recent works that promised to improve the Energy Consumption and Security for increasing the routing protocol's performance. Basically a common concepts are used that encryption/decryption technique and network coding, that proves the secure data transmission in less number of transmission in network. They defined that, each node in network have some attributes (like identity, threshold), based on these attributes data can transmit from one node to their neighbour node. It include the allowable overhearing of control messages from adjacent nodes and limiting the local repair for a small topological range of the link break therefore alternative routes to the sink node can be found quickly with optimum routing overheads. Cryptographic scheme[2] provides sharing of secret key between authenticated sender and receiver. It is the straight forward method to provide confidentiality for network coded MANETs is to encrypt the data packet using symmetric encryption algorithm, so that we can achieve confidentiality, integrity, non repudiation, authentication and availability. Due to node mobility, link failure is a common issue in multi-hop wireless ad hoc networks. With a reactive routing protocol like AODV, this condition can increase delay and routing overheads when route repair carried out. In year 2011, author Chun Yuan, Zhou and Hongyang Gao, et al. [19], introduce a method called "lightweight identity-based broadcast encryption", in which it used traitor tracing function, it has constant size cipher-text, private keys and public key. When any new user will add, then only adjustment done in symmetric key life cycle. In 2011, author Hongwei Li, et al. [11], proposed scheme in which a new encryption technique is used that Hierarchical Identity-Based Encryption for MANETs (HIBEM). It presents novel Hierarchical Identity Based Model for MANETs (HIBMM), it is based on integer lattices HIBEM achieves security under lattice hard problem. Here, Hierarchical Identity based Encryption (HIBE) used as a public key encryption method where elements are arranged in directed tree. In 2011, author Hiteishi and J.S. Shah, et al. [12], proposed a scheme for securing Biometric data by any cryptanalysis, brute force attack and all kinds of attack. Their scheme generate encryption key of 48 bit with fingerprint to enhance the security. The main idea is to produce all types of fingerprints and for creation of key, a set of fingerprint randomly selects but at the receivers side, it is mandatory to produce all feature sets of

fingerprints so that one key is find for encryption. In year 2012, author Guan, F. Richard, Jiang, Victor and Hamid Mehrvar, et al.[6], proposed a scheme, i.e. new topology control scheme called "Capacity-Optimized Cooperative (COCO)". It can improves the capacity of network in MANETs by considering both upper layer network capacity and physical layer cooperative communication. Cooperative communication is a system where user can share and coordinate with their resources to improve the information transmission quality. In year 2012, author Weng, Shin-Ming and Kwang-Cheng, et al.[4], defines a method to investigate the connectivity of cooperative secondary network from percolation-based perspective, in which each secondary user's have the secondary network user and those are acting as relay in transmission. This cooperative secondary network connectivity is defines in terms of percolation threshold. In year 2012, author Ajay Kushwaha & Hariram Sharma [7] introduced an enhanced approach of selective encryption algorithm for better security of data. This method ensures that the infrequent words or sensitive data can encrypted. In 2012, author Adarsh, Krishna and Alok Aggarwal, et al. [18], proposed a novel integration mechanisms to provide complete cryptography services for MANETs. They shows that DSDV performance better than AODV and DSR when discovery approach will change into reactive approach. In year 2012, author Ahmad Ali, Lin Cai and Fayez Gebali, et al, [3], proposed a new MAC protocol called "Dual-sensing directional MAC (DSDMAC)" protocol with directional antennas for wireless ad-hoc networks. This DSDMAC protocol provides dual-sensing scheme to identify hidden-terminal problem and to resolve it.DSDMAC protocol depends on dual sensing method that can identify the deafness, it can avoid unnecessary blocking and it can solve the hidden terminal problem. Integrity of DSDMAC can verified and validated using Spin. Spin is a verification and validation tool which verify the correctness of analysis. In year 2013, author Peng Zhang Lin, Yixin Jiang, Yanfei Fan &Xuemin Shen, et al.[2], proposed a method for secure property for network coding. They describe a new technique i.e. P-coding, it is a lightweight encryption scheme to protect the data from external eavesdropper in network coded MANETs. The main idea is to divide data into generations and generate PEF key. Then global encoding vector will chooses randomly and appended to the message. In 2013, author Yao, Lin, Deng, Miao and Yim & Guowei Wu, et al. [17], proposed anonymous mutual authentication based on biometrics in VANETs. According to this paper, during authentication phase, two vehicles negotiate their temporary session key and produce two temporary MAC address. Authentication procedure matched the user's biometric and stored templates in database by using field sampling. This will shows the user identity. In year 2013, author Prakashgoud Patil and Umakant Kulkarni, et al. [1], proposed a method called "Support Vector Machine based Data Redundancy Elimination for Data Aggregation in WSN (SDRE)". This SDRE can reduce the redundant data and eliminate false data from wireless sensor network. In this paper, they built an aggregation tree of sensor network size and SVM method applied on data to remove redundancy. They used Local Sensitive Hashing for minimize redundant data and false data. LSH works based on data similarity and their threshold. In year 2013, author Emiliano and Claudio Soriente, et al. [5], proposed a scheme in which, they focus on security in Participatory Sensing and provide a suitable secure infrastructure. They define Privacy-Enhanced

Participatory Sensing Infrastructure. This paper provides a set of rules of privacy need for both data sender and receiver.. Their solution is adaptable by recent Sensing Applications that provides security and increase user participation with low overhead.

III. PROPOSED METHODOLOGY

The data aggregation, security and energy consumption are most important issues in Wireless Ad-hoc Networks due to limitation of resources. The distribution of huge number of mobile node over sensing area increases the data correctness. Form [1]. The mobile nodes deployed on nearby area can sense the same data, which generate lots of data redundancy. When protocols send extra and un-necessary copies of data, then energy and bandwidth will be wasted. When many nodes sense the same area and send same data packet to their neighbor, in this situation there will be waste of resources in sensor node. This problem can be resolve by data aggregation technique, in which include combination of data by many nodes at intermediate nodes and then transmission will be done to the base station. In network, there is another issue that is data redundancy. Data redundancy is referred to duplicate data. Removing redundancy is a biggest challenge in mobile ad-hoc network. To provide security, the nodes must share a secret key only to the authenticated neighbor nodes, so that we can achieve the various security goals like confidentiality, integrity, non-repudiation, authentication, and availability. To provide the required level of security, a MANET security solution also needs to consume minimum amount of energy owing to the MANET operation in wireless communication environment. Recently, there have been lots of works on developing energy efficient and low cost oriented security method in wireless networks.[1]To provide security for MANETs, only symmetric key encryption algorithms are used but they are not efficient. Network coding can reduce energy consumption with scalability, transparency and performance in MANETs.

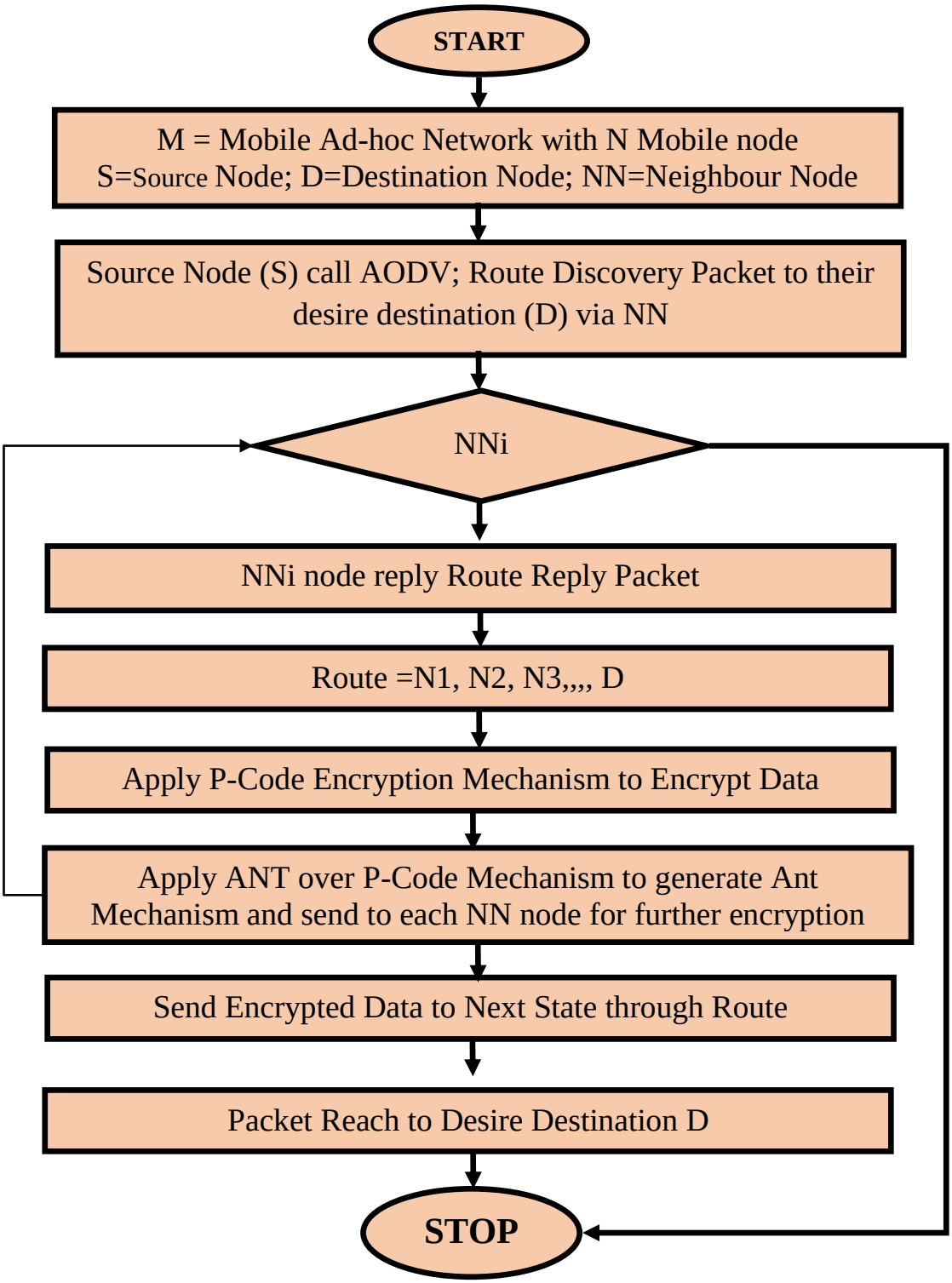

Fig.1. Proposed Flowchart

Applying P-Coding in these applications are not as high as in MANETs, since these applications are generally not energy-constrained and any symmetric cryptographic algorithms would function well. We extend our scheme to other scenarios where encryption efficiency is critical. The objective of this paper is to develop a new approach which can successfully maintain the confidentiality with lesser battery power in order to long survival of mobile ad-hoc network.

This paper studied the problem of energy saving in MANETs based on the technique of network coding. Previous studies demonstrated that network coding can reduce energy consumption with less transmission in MANETs. We proposed optimized P-Coding, a lightweight scheme on top of network coding, to further reduce energy consumption in MANETs by cutting the security cost. For optimization proposed technique use ant colony optimization scheme. Optimized P-Coding exploits the intrinsic security property of network coding, and uses simple permutation encryptions to generate considerable confusion to eavesdropping adversaries. We showed that optimized P-Coding is efficient in computation, and incurs less energy consumption for encryptions/decryptions. Mobility and energy consumption are complex issue in the ad hoc network, due to high and frequent mobility network partitioning like issues are arises. Therefore, that is router's responsibility to arrange the path and save energy in ad hoc network. So, here required to find a search technique, by which efficiently the new path discovered due to path break and/or link failure and consumes less energy. Thus here a clustering technique, i.e., k-means clustering and a cryptographic scheme, i.e., p-coding are used in proposed method, over the conventional routing techniques as shown in figure 1.

IV. Simulation Detail & Result Analysis

To implement this concept, the aodv.cc file was modified. When the simulation is started, the command is called. Each setting is related to the hole in this function. The functions for creating mobile nodes are added by reading the file node ID in this functionality. The script calls this function to create the cluster game in the simulation.

Table 1: Simulation Detail

Parameters	Values	
Number of Nodes	Vary from 40 to 100	
Area	40	600*300
	50	600*300
	100	1000*800
Traffic	CBR	
Simulation Duration	100 Mili Seconds	
Packet Transmission Rate	1024 kbps	
Carrier sense threshold Used In Normal Nodes	200 Meter	

The performance metrics which are used to analyze the performances of routing protocols in heterogeneous ad hoc networks are discussed in the following:

Encryption Time: Encryption Time means Time used by any node for successful Encryption of any packet for transmission. Need to minimum for ideal Encryption technique.

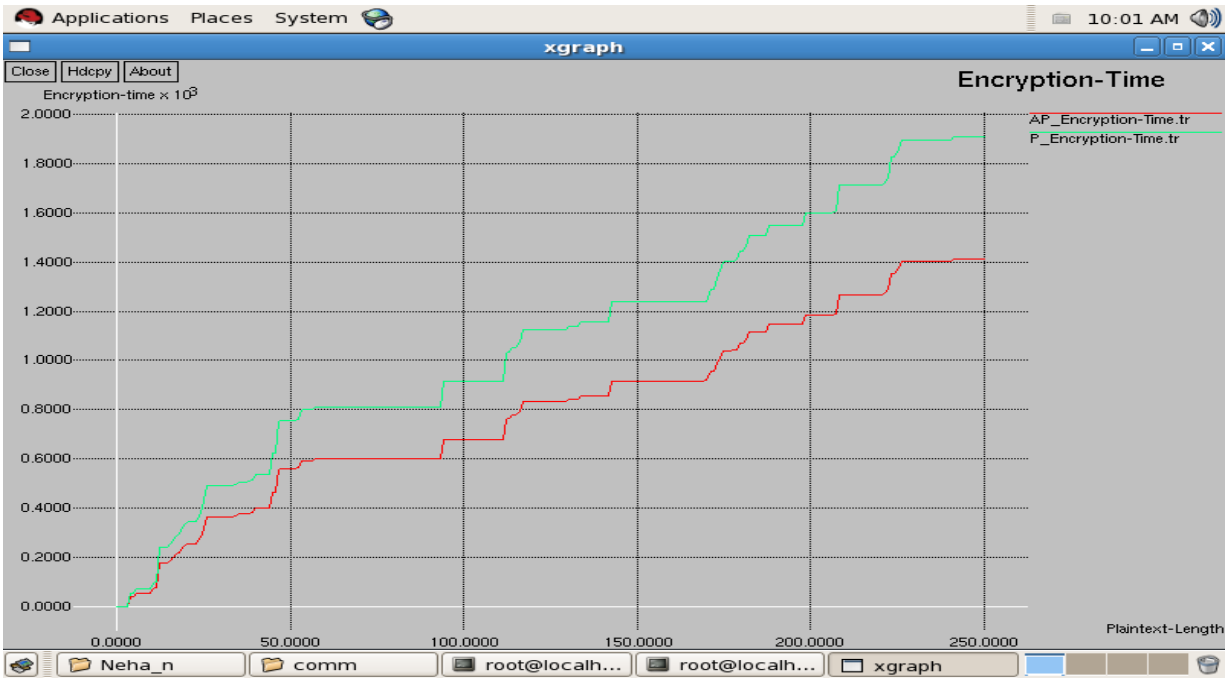

Fig.2. Encryption Time

Security Probability: Security Probability means probability that nothing bad will be happen to desire network. Need to maximize for ideal Encryption technique.

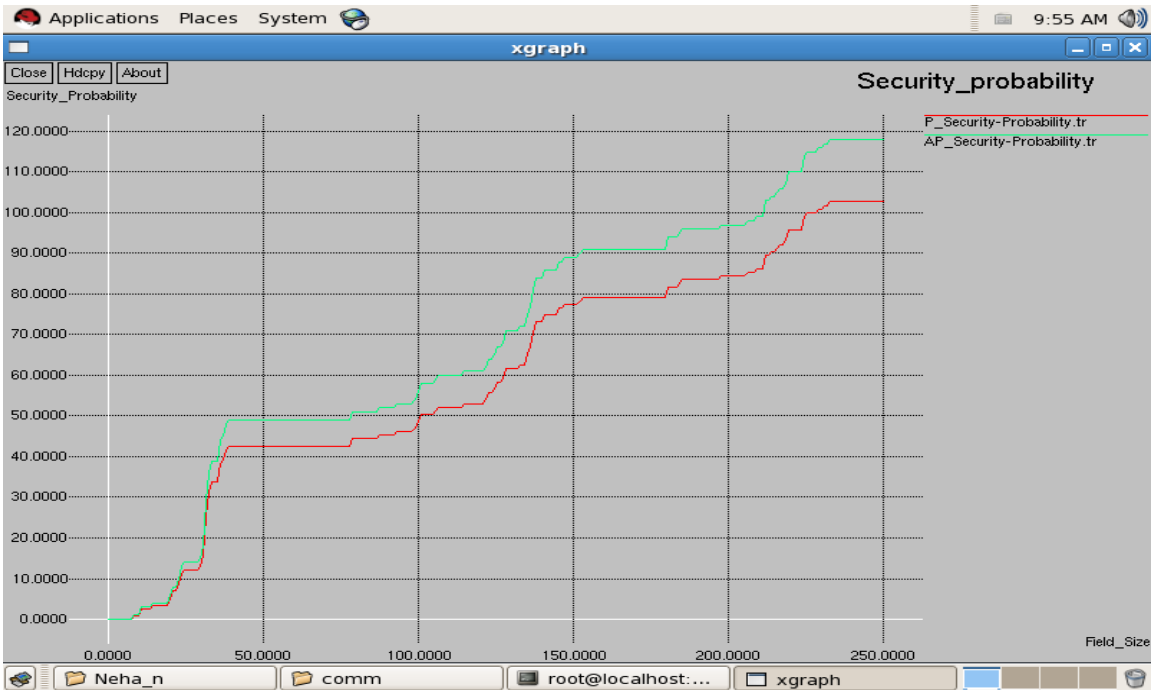

Fig.3. Security Probability

Success Ratio: Success Ratio, the ratio of the number of rounds in which the key is recovered, to the total number of rounds. Need to minimum for ideal Encryption technique.

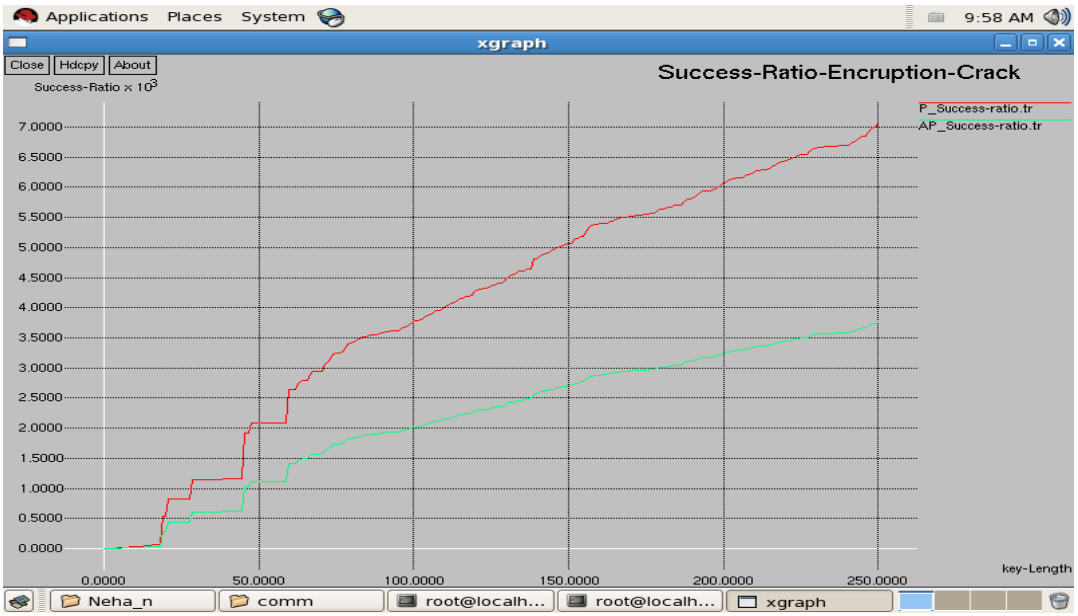

Fig.4. Success Ratio

Energy Consumption: Energy consumption means battery power used by any node for successful transmission. Higher energy consumption degrades the survival of network. And lower energy consumption maintains longer survival of network. For any ideal conduction network need longer survival.

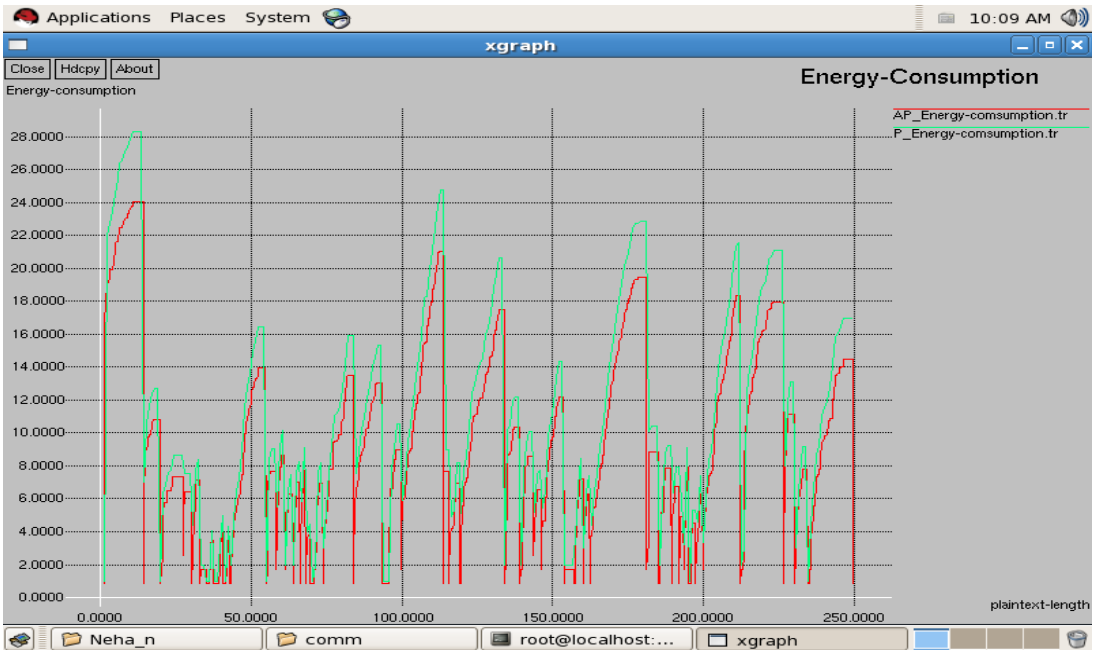

Fig.5. Energy Consumption

V. CONCLUSION

Network coding can help achieve lower energy consumption in MANETs. The energy saving comes from fact that less transmissions are required when in-network nodes are enabled to encode packets. We have to develop a new encryption scheme that can fully exploit the security property of network coding. Since both the coding vectors and message content are necessary for decoding, randomly reordering/mixing they will generate considerable confusion to the eavesdropping adversary. In the proposed study work described in above section provides the design and implementation of a ACO and P-Coding based routing protocol. To identify the need of protocol we study various techniques by which we get the problem domain and the solution domain. Our proposed work is based on the energy consumption and security. The study of the proposed work is completed yet and the performance evaluation is completed after that we found the proposed ACO and P-coding method based routing protocol provide high performance QoS parameters and adoptable for use. But in future their performance can increase by using more suitable clustering algorithms. So, in near future we stick with the same concept and we will try to implement this concept with more adaptable clustering algorithm that can reduce more energy.

REFERENCES

[1] Prakashgoud Patil, Umakant Kulkarni *"SVM based Data Redundancy Elimination for Data Aggregation in Wireless Sensor Network"*, International Conference of Advance in Computing Communication and Informatics, IEEE, 2013

[2] Peng Zhang, Chuang Lin, Yixin Jiang, Yanfei Fan, and Xuemin (Sherman) Shen *"A Lightweight Encryption Scheme for Network-Coded Mobile Ad Hoc Networks,"* IEEE Trans. Parallel and Distributed Systems, Vol. 25, No. 9, September 2013.

[3] Ahmad Ali Abdullah, Lin Cai and Fayez Gebali, *"DSDMAC: Dual Sensing Directional MAC Protocol for Ad Hoc Networks with Directional Antennas"*, IEEE Transactions On Vehicular Technology, Vol. 61, No. 3, March 2012

[4] Weng Chon Ao, Shin-Ming Cheng and Kwang-Cheng Chen, *" Connectivity of Multiple Cooperative Cognitive Radio Ad Hoc Networks"*, IEEE Journal On Selected Areas In Communications, Vol. 30, No. 2, February 2012

[5] Emiliano De Cristofaro and Claudio Soriente, *"Participatory Privacy:Enabling Privacy in Participatory Sensing"*, IEEE Transactions On Networking Vol.27 No.1 Year 2013

[6] Quansheng Guan, F. Richard Yu, Shengming Jiang, Victor C. M. Leung, Hamid Mehrvar, *"Topology Control In Mobile Ad Hoc Networks With Cooperative Communications"*,IEEE Wireless Communications April 2012

[7] Ajay Kushwaha,Hariram Sharma, *"Enhancing Selective Encryption Algorithm for Secured MANET"*,2012 Fourth International Conference on Computational Intelligence, Modelling and Simulation

[8] M.Umaparvathi1, Dr.Dharmishtan K Varughese, *"Evaluation of Symmetric Encryption Algorithms for MANETs"*, IEEE, 2010

[9] Mehta Manisha Pravinchandra, HiteishiMilindDiwanji&Jagdish and Hemali Kotak, *"Performace Analysis of Encryption and Decryption using Genetic Based Cancelable Non-Invertible Fingerprint based Key in MANET"*,IEEE,2012 International Conference on Communication Systems and Network Technologies

[10] Adel ECHCHAACHOUI, Ali CHOUKRI, Ahmed HABBANI and Mohamed ELKOUTBI,*"Asymmetric and Dynamic Encryption for Routing Security in MANETs",* IEEE 2014

[11] Hongwei Li, *"A Hierarchical Identity-Based Encryption for MANETs",* IEEE 2011, ICCP2011

[12] Hiteishi Diwanji and J.S. Shah, *"Enhancing Security in MANET through Unimodal Biometric Encryption Key",* Institute Of Technology, Nirma University, Ahmedabad – 382 481, 08-10 December, 2011

[13] Duan Hu, Furong Wang Chen Huang, Chunming Rong, *"A Novel Relay Encryption Scheme for Mobile Ad hoc Networks",* DOI 10.1109/UIC-ATC.2009.53, Symposia and Workshops on Ubiquitous, Autonomic and Trusted Computing, IEEE 2009

[14] Yomna M. Mohsen, Mohamad Hamdy and Mohamad Hashem, *"A Genetic IP based Scheme for Identity Hidding In MANETs",* 9th International Conference on INFOrmatics and Systems (INFOS2014)

[15] Paul Krier, Sai Seshabhattar, Jason Pereira, Daniel Engels, Suku Nair. *"Lightweight Key Agreement With Key Chaining"*IEEE 2010

[16] Wei Ren, Yi Ren and Hui Zhang, *"Fast Secure Routing for Highly Mobile Large-Scale Ad-hoc Vehicular Networks"*2009 Asia-Pacific Conference on Information Processing, 2009 IEEE DOI 10.1109/APCIP.2009.275

[17] Lin Yao, Chi Lin∗, Jing Deng, Fangyu Deng, Jingwei Miao , and KangbinYimGuowei Wu, *"Biometrics-based Data Link Layer Anonymous Authentication in VANETs"*2013 Seventh International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, IEEE 2013

[18] Adarsh Kumar, Krishna Gopal and Alok Aggarwal, *"A Complete, Efficient and Lightweight Cryptography Solution for Resource Contrainst Mobile Ad-Hoc Networks",*2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing

[19] Chun Yuan, Hongyang Gao, Wenshuo Zhou, *"Lightweight identity-based broadcast encryption over wireless ad hoc Networks",* IEEE 2011