Mobile Ad-hoc Network using P-Encryption Scheme

H.O. Archita Deore
Student of Information Technology
BVCOE & RI, Nashik

Shraddhha Satpute
Student of Information Technology,
BVCOE & RI, Nashik

Pradnya Nandwalkar
Student of Information Technology
BVCOE & RI, Nashik

K.S. Kumavat
D, Information Technology
BVCOE & RI, Nashik

ABSTRACT
In this paper, system describe in MANET Energy saving & security in data is an important issue in MANET. This can be solved by network coding which might reduce energy consumption also by using less transmission this system proposed data sharing using data encryption method. Encryption/decryption cost along with transmission time is factor of energy consumption in wireless network. In MANET unreliable wireless media, mobility, lack of infrastructure is a big challenge. Mobile ad hoc network refers to mobility of nodes rather than any fixed infrastructure, act as a mobile router. These mobile routers are responsible for the network mobility in MANET. A Mobile Ad-hoc Network (MANET) is a self configuring network composed of mobile nodes without any fixed wired network. A very important and necessary issue for mobile ad-hoc networks is to find the route between destination and source which is a major technical challenge due to the dynamic topology of the network. To an autonomous group of mobile users that communicate over relatively bandwidth constrained wireless links are refer by mobile ad hoc network. Various algorithms are used for data encryption successfully such as Data Encryption standard (DES), Transposition Substitution Folding Shifting Encryption Algorithm i.e. TSFS, Advance Encryption Standard. TSFS is used for avoiding errors occurring during the decryption process. DES & AES algorithm is used for query execution time & database size. P-coding scheme is used for the mobile ad-hoc network(MANET).

Keywords
MANET, P-coding, encryption, decryption, network coding, data sharing, energy saving.

1. INTRODUCTION
MOBILE Ad Hoc Networks (MANETs) are very important wireless communication. Mobile ad hoc networks (MANETs) is an infrastructure less, dynamic network consisting of collection of wireless mobile nodes that communicates with each other without the use of any centralized authority. Mobile ad hoc network is now becoming interesting research topic in the area of wireless communication. Vehicles in the particular range form a network to communicate with each other without any need of a base station. MANET provide comfort and safety applications such as lane changing, traffic sign violation, weather information, road condition, location of restaurants or fuel station, parking and interactive communication such as internet access [2]. As shown in figure 1 MANET provides multiple services, energy is required. Thus, energy saving is an important issue in Mobile ad hoc network. There are several energy efficient schemes used to overcome this problem [3], [4] and [5].

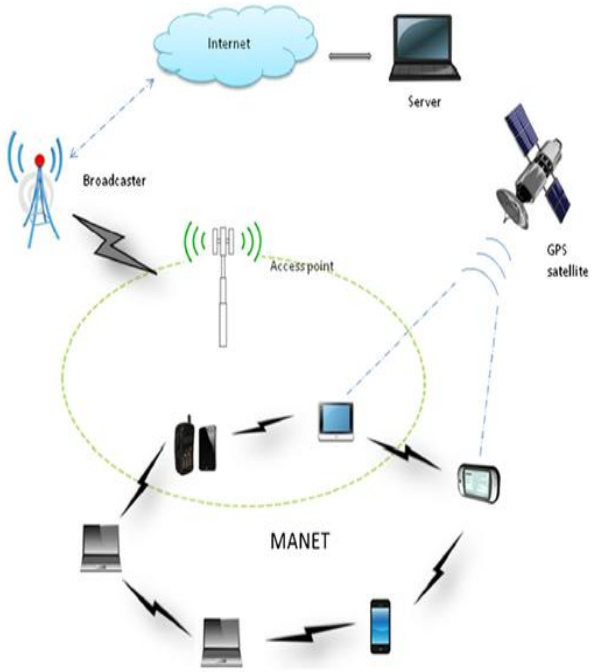

Fig 1: MANET Architecture

Many researchers show that network coding can reduce energy consumption in MANET with less transmission [6]. Network coding can be defined as coding performed at a node in a network, where coding means casual mapping from inputs to outputs. Idea behind it is to mix and forward data to output links [7]. A node in the network encodes the packet with the network coding and then forwards it to another node. Network coding requires less energy for this process of encoding. Figure 2 clarify the use of network coding in ad hoc network. Suppose there are six nodes forming hexagon and transmission range of each node reaches to its right and left neighbor. Each message would require four transmissions without network coding. When network coding is used is shown in (figure. 2(2), 2(4), 2(4),) for three messages the total number of nine transmissions are needed, i.e., three transmissions per message. It would save ¼ energy without considering energy required for the process of encryption and decryption.

Mobile ad hoc network is the network which provides seamless connectivity between devices when they move with their neighbor wireless nodes. For sending packets it does not have any access point and routers. In a MANET each device is free to move independently, and so it can frequently change its link at any time.

MANETs nodes can communicate directly between each other so that MANETs can emerged as a dominant mode of communication at any place. Some of the characteristics of MANETs includes infrastructure-less network, dynamic network topology and self-organization etc. In ad hoc networks all nodes are responsible for running the network services meaning that every nodes are also works as a router to forward the networks packets to their destination. Data communication in a MANET differs from that of wired networks in different aspects. The bandwidth availability and computing resources like hardware and battery power are restricted in mobile ad hoc networks. An ad hoc network is a decentralized type of wireless network. The ad hoc network is the network that links with each other for communication having fixed infrastructure. It is made up of multiple nodes connected by links. A MANET can be created either by mobile nodes or by both static and dynamic mobile nodes. Mobile ad hoc network is created by cluster of is a form a Mobile Ad Hoc Network (MANET) is formed.

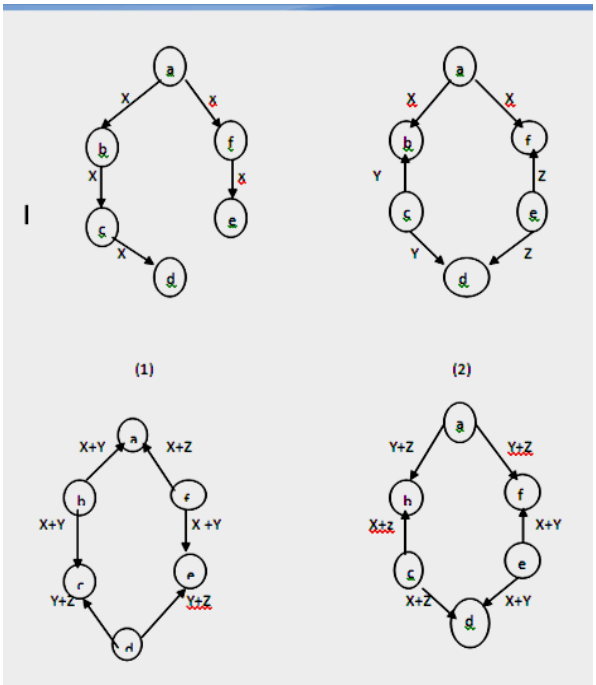

Fig 2: Network Coding in Ad- hoc Network

Mobile ad hoc network is the network which provides seamless connectivity between devices when they move with their neighbor wireless nodes. For sending packets it does not have any access point and routers. In a MANET each device is free to move independently, and so it can frequently change its link at any time.

MANETs nodes can communicate directly between each other so that MANETs can emerged as a dominant mode of communication at any place. Some of the characteristics of MANETs includes infrastructure-less network, dynamic network topology and self-organization etc. In ad hoc networks all nodes are responsible for running the network services meaning that every nodes are also works as a router to forward the networks packets to their destination. Data communication in a MANET differs from that of wired networks in different aspects. The bandwidth availability and computing resources like hardware and battery power are restricted in mobile ad hoc networks. An ad hoc network is a decentralized type of wireless network. The ad hoc network is the network that links with each other for communication having fixed infrastructure. It is made up of multiple nodes connected by links. A MANET can be created either by mobile nodes or by both static and dynamic mobile nodes. Mobile ad hoc network is created by cluster of is a form a Mobile Ad Hoc Network (MANET) is formed.

P- Coding:
In figure 3 method of P-coding used for encryption is performed on network coded message. In P-coding a Global Encoding Vector which is GEV is prefixed with the packet and then it is forwarded to the neighbouring node.

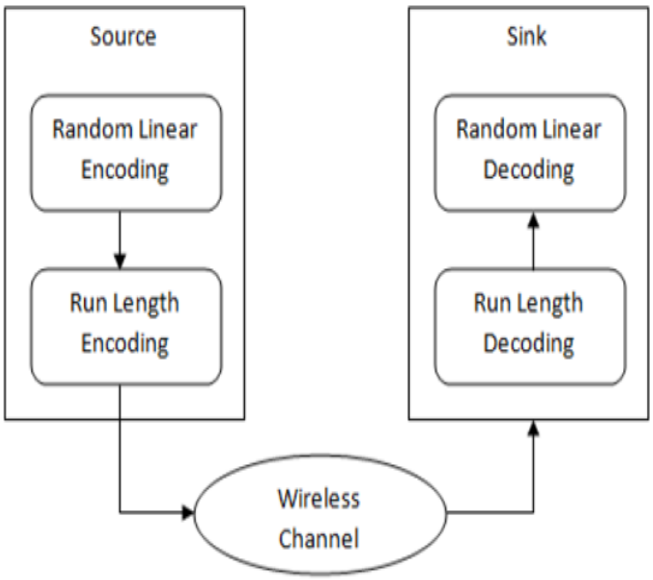

Fig 3: Enhanced P-Coding

Basically, P-Coding consists of three phases which is given below:
Source Encoding:
At first, consider that the source consists of n packets. Next the packets are prefixed with their corresponding Global Encoding Vector and then the encryption is performed on each packet. After that corresponding encrypted packet is generated.
Intermediate Recoding:
As the packets are transferred in order to their corresponding GEV"s, it is difficult to decrypt the packet for the intermediate nodes.
Sink Decoding:
By receiving encrypted packets, the destination node decrypts the packet by elimination method.

2. LITERATURE SURVEY

In MANET lower energy consumption is achieve by network coding. On encrypted coding vectors network coding can be perform directly[11].

Table1: literature survey

No.	Existing system	Merits
1	Network coding	1) Network coding in MANET can efficiently handle mobility and increase throughput.
2	SPOC	1) Use locked and unlocked coefficient. 2) Achieve confidentiality .
3	HEF	1) Privacy against flow tracing and traffic analysis.
4	VANET	1) Used in vehicular network
5	ARAN	1) Provide message integrity, repudiation and authentication.
6	RSA	1) Increased security and convenience. 2) Provide digital signature that can not be repudiated.

Network coding:

Network coding is a technique which is used to improved scalability , Resistance ,and Efficiency of network performance. Normally, network coding is performed using XOR operation on packet data.[12].

Secure Practical Network Coding (SPOC):

In this network coding unlocked and locked coefficients are encrypted which is used for encoding and decoding.

Homomorphism Encryption Function(HEF):

This function performs linear random combination on incoming packets and then gives resultant packets.

Vehicular ad hoc network(VANET):

In this vehicles in the particular range form a network to communicate with each other without the need for any base station.

Authenticated Routing for Ad Hoc Network(ARAN):

This protocol uses public key cryptography. It uses timestamp for the route freshness and this scheme requires all nodes must keep the routing table for all other node

Rivest Shamir Adleman Algorithm (RSA):

4. SYSTEM OVERVIEW DIAGRAM

The system diagram shows overall flow of the system which helps to recognize how the system work n what it is.

This is used for authentication, security and binding the public key. Location privacy is provided by RSA.

3. ALGORITHM

Algorithm shows p-coding strategy in the system as follow-

Input: a permutation k of length n, integers n, m, s, d

with$1 \le m \le n, s \in [0, n-m+1]$ and $d \in [0, m!-1]$

output: a permuted permutation $\tilde{Q}$ of length n

P_1 : // to generate the sequence $(a_1, \dots\dots, a_{m-1})$

For each $i \in [1, m-1]$ **do**

$$\begin{vmatrix} a(i) \leftarrow d\%(i+1); \\ d = \left\lfloor \frac{d}{i} + 1 \right\rfloor; \end{vmatrix}$$

End

P_2 : //to generate the sequence $(b_1, \dots\dots, b_{m-1})$

For each $i \in [1, m-1]$ **do**

$$| \; b(i) \leftarrow m - a(m-i);$$

End

P_3 : // Initialization of attributes

For each $i \in [1, n]$ **do**

$$|w(i) \leftarrow i;$$

End

P_4 : // to calculate the partial permutation

For each $i \in [1, m-1]$ **do**

$$\left|w(s-1+i) \leftrightarrow w\big(s-1+b(i)\big);\right.$$

End

P_5 :// to perturb the current key Q using w

For each $i \in [1, n]$ **do**

$$\left|\tilde{Q}(i) \leftarrow w\big(Q(i)\big);\right.$$

End

Return $\tilde{Q}$;

In the algorithm,

P_1, P_2, P_3, P_4, P_5 are the processes. Output of the process 1 is used as input for process 2, similarly output of the process 2 is input for the next process.

Q- it is used for permutation encryption function key.

n- Tagged packets length.

m- perturbing keys partiality.

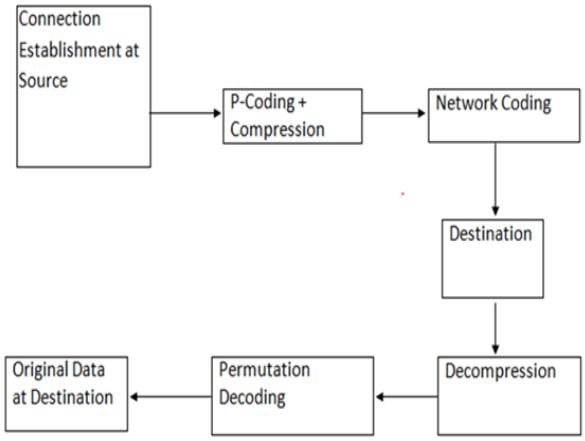

Fig 4: System Overview Diagram

System overview diagram is as shown in figure 4 which initially obtain topological information about the network. In P-Coding the permutation encryption is performed on the corresponding GEVs and symbols of messages. Compression is performed on coded message. After that the network coding is performed on this messages belonging to the same generation. Finally it is transmitted to the sink node. The sink node the decompression and permutation decryption is performed.

5. MATHEMATICALE MODULE

- Consider a MANET of N nodes,

G= (V, E), where, V= $\{v_1 , \ldots, v_n\}$ and E= $\{e_1, \ldots, e_n\}$

- Assume a node $h \in H$ where,

  (-h)= Links terminating at h.

  (+h)= Links originated from h.

- Here, a link has capacity of carrying one packet per unit i.e. y (e).
- When a source wants to send series of packet X= $[x_1, \ldots x_t]$ to a set of sink T where, $T \subseteq H$ then source computes y(e) as[1],

$$y(e) = \sum_{e \in (-h)} \beta(e) y(e)$$

  where, $\beta(e)$ is a Local Encoding Vector(LEV)

- Global Encoding Vector can be appended to message as[1],

$$y(e) = \sum_{i=1}^{t} g_i(e) x_i = g(e)x$$

  Y = GX

- Source encrypts packet with permutation encryption[1],

$$C[y(e)] = \sum_{e \in (-h)} \beta(e) C[y(e)]$$

- Intermediate node forward packet to sink node with simple recoding with no extra efforts.
- Sink node will decrypt the packet as[1],

$$D\{c[y(e)]\} = E^{-1}\{E[y(e)]\} = y(e)$$

- Thus source packets simply recover by applying Gaussian elimination,

  X = G-1(Y).

6. CONCLUSION

A light-weight encryption scheme is used for providing security in energy efficient way. This light-weight encryption scheme is based on network coding. P-coding is used with network coding for reducing the energy consumption and provides security in MANET. This scheme requires the processes of encryption/decryption. P-Coding is efficient in computation, and ensures less energy consumption for encryptions/decryptions. In MANETs network coding reduces energy consumption by less transmission, for that P-Coding is used to provide confidentiality to network coded MANETs.
A mobile ad hoc network is one of the most innovative and challenging areas of wireless networking and tends to become increasingly present in our daily life.hoc network is clearly a key step in the next-generation evolution of wireless data communication when we consider the different enabling networks and technologies. An ad hoc network inherits the traditional problems of wireless and mobile communications, including bandwidth optimization, power control, and transmission quality enhancement.The message is transmitted to the receiver by using network coding and P-coding schemes in order to conserve the energy consumption. Thus the proposed method ensures that the transmission can be done in a secured way by using Modified P-coding scheme which uses Advanced Encryption Standard algorithm for encryption and decryption process. Thus hackers cannot obtain the original message without generating the key and the global encoding vector. This ensures the confidentiality of the data transmission.

7. REFERENCES

[1] Peng Zhang, Chuang Lin, Yixin Jiang, Yanfei Fan, and Xuemin (Sherman) 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] A. Rahim, I. Ahmad, Z. S. Khan, M. Sher, M. Shoaib, A. Javed, R. Mahmood "A Comparative Study of Mobile And Vehicular Ad Hoc Networks," International Journal of Recent Trends in Engineering, Vol 2, No. 4, November 2009.

[3] S. Singh, C. Raghavendra, and J. Stepanek, ,,,,Power-Aware broadcasting in Mobile Ad Hoc Networks,"" in Proc. IEEE PIMRC, 1999, pp. 1-10.

[4] J. Wieselthier, G. Nguyen, and A. Ephremides, Algorithms for Energy-Efficient Multicasting in Static Ad Hoc Wireless Networks,"" Mobile Network. Appl., vol. 6, no. 3, pp. 251-263, June 2001.

[5] B. Chen, K. Jamieson, H. Balakrishnan, and R. Morris, Span: An Energy-Efficient Coordination Algorithm for Topology Maintenance in Ad Hoc Wireless Networks"" Wireless Network, vol. 8, no. 5, pp. 481.

[6] R. Ahlswede, N. Cai, S.-Y.R. Li, and R.W. Yeung, Network Information Flow,"" IEEE Trans. Inf. Theory, vol. 46, no. 4, pp. 1204-1216, July 2000.

[7] J.P. Vilela, L. Lima, and J. Barros, „„Lightweight Security for Network Coding,"" in Proc. IEEE ICC, May 2008, pp. 1750-1754.

[8] Ghassan Samara, Wafaa A.H. Al-Salihy, R. Sures, Penang "Security Issues and Challenges of Vehicular Ad Hoc Networks (VANET)".

[9] N.R. Potlapally, S. Ravi,A.Raghunathan, andN.K. Jha, A Study of the Energy Consumption Characteristics of Cryptographic Algorithms and Security Protocols,"" IEEE Trans. Mobile Computing, vol. 5, no. 2, pp. 128-143, Feb. 2006.

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

[11] Pooja Mundhe , Prof. V. S .Khandekar "energy efficient Encryption Scheme for Vehicular Ad-Hoc Network". Issue 25,March 2015

[12] P.Madhvan, Asst Professor, J.Nandhini, N. Nandhini , Dr P Malathi "Energy Optimization in MANET using Modified P-Coding Scheme" International Journal of Science ,Engineering and Technology Research(IJSETR),volume 3,Issue 4,April 2014

8. AUTHOR'S PROFILE

Archita B. Deore she is Engineering student of Information Technology at Brahma Valley College of Engineering And Research Institute, Nasik under University of Pune. She interest in the field of security.

Shraddha R. Satpute she is student of Engineering student of Information Technology at Brahma Valley College of Engineering And Research Institute, Nasik under University of Pune. Her interest in the field of security.

Pradnya R. Nandwalkar she is student of Engineering student of Information Technology at Brahma Valley College of Engineering And Research Institute, Nasik under University of pune. Her interest in the field of security.

K.S. Kumavat, ME, BE Computer Engg. Was educated at Pune University. Presently she is working as Head Information Technology Department of Brahma Valley College of Engineering and Research Institute, Nasik, Maharashtra, India. She has presented papers at National and International conferences and also published papers in National and International Journals on various aspects of Computer Engineering and Networks. Her areas of interest include Computer Networks Security and Advance Database.