Energy Optimization in MANET using Modified P-Coding scheme

P.Madhavan,Asst Professor,
Department of CSE,
Sri Krishna College of Technology,
Coimbatore-India.

J Nandhini, N. Nandhini ,
RMegalaPreethi (UG Scholar)
Department of CSE,
Sri Krishna College of Technology,
Coimbatore-India.

Dr.P.Malathi
Principal,
Bharathiyar Institute of Engineering for Women,
Salem, India.

Abstract-Energy saving is an important issue in Mobile Ad Hoc Networks (MANETs). Recent studies show that network coding can help reduce the energy consumption in MANETs by using less transmission. However, apart from transmission cost, there are other sources of energy consumption, e.g., data encryption/decryption. In this project, the network coding is done to reduce the energy consumed by data encryption in MANETs. It is interesting that network coding has a nice property of intrinsic security, based on which encryption can be done quite efficiently. Hence, P-Coding, a lightweight encryption scheme is proposed to provide confidentiality for network-coded MANETs in an energy-efficient way. The basic idea of P-Coding is to let the source randomly permutes the symbols of each packet (which is prefixed with its coding vector), before performing network coding operations. Without knowing the permutation, eavesdroppers cannot locate coding vectors for correct decoding, and thus cannot obtain any meaningful information. It is demonstrated that due to its lightweight nature, P-Coding incurs minimal energy consumption compared to other encryption schemes.

***Index Terms*- MANET, Network Coding, P-Coding, AES, Energy consumption.**

I. INTRODUCTION

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

MANET security goals:

MANETs (Mobile adhoc networks) provide security services such as

- Authentication
- Confidentiality
- Integrity
- Availability

Issues of Mobility in Ad hoc Networks:

Mobility affects

- Single Transmission
- Channel access
- Routing
- Multicasting

Network Coding

Network coding is a technique in which used to improve scalability, resilience and efficiency of the network performance. In Network coding two or more packets are combined and transmitted to the neighbor node, in order to reduce the energy consumption. It also reduces the transmission times.Normally, network coding is performed using xor operation on packet data. Network coding provides inbuilt error correction and adaptivity due to joins, link failures etc..

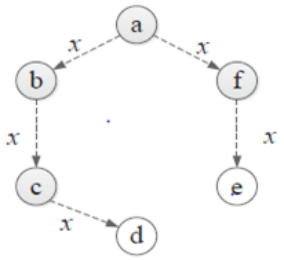

Fig 1: Packet transmission without network coding

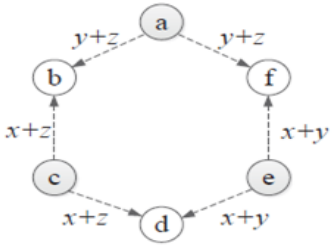

Fig2: Packet transmission with network coding

P-Coding

P-coding is a method in which encryption is performed on network coded message. In P-coding a Global Encoding Vector (GEV) is prefixed with the packet and then it is forwarded to the neighboring node. Normally, P-Coding consists of three phases: Source encoding, intermediate recoding and sink decoding.

Source Encoding

Firstly, consider that the source consists of 'h' packets. Next the packets are prefixed with their corresponding Global Encoding Vector(GEV) and then the encryption is performed on each packet. After which the corresponding encrypted packet is generated.

Intermediate Recoding

As the packets are transferred inthe order of their corresponding GEV's, it is difficult for the intermediate nodes to decrypt the packet.

Sink Decoding

After receiving encrypted packets, the destination node decrypts the packet by means of gauss elimination method.

II. RELATED WORKS

This paper proposes an under a layered model of wireless networks. The linear program can be used to find energy per bit for multicasting in Mobile Ad hoc Networks [1]. Due to the linearity of the pricing scheme it is possible to achieve minimum energy per bit for routing using single distribution tree. A Unified study of minimum energy multicasting with network coding and routing is presented. A wireless ad hoc network is modelled as a graph which is composed of structures in form of trees representing physical broadcast links. Each edge of the graph has a price, which is the energy-per-bit for the corresponding broadcast link. The minimum energy multicasting formulation amounts to minimizing the total cost of the consumed bit-rates on the edges, while providing a unit multicast rate.

Drawbacks

- It is difficult to find cost for every edge in the tree

Based on the battery power consumption at nodes five power aware metrics is used for determining routes in wireless ad hoc networks [2]. Power aware broadcasting algorithm reduces the cost of routing packets to all destinations by 5-50% using greedy strategy. The energy consumption can also be reduced to 40-70% using PAMAS. The broadcast route is established between the sender and receiver. Hence, cost of the routing packets is reduced.

Drawbacks

- It is difficult to select the appropriate broadcast trees to achieve this goal.
- One of the serious drawbacks of this metric is that nodes will tend to have widely differing energy consumption profiles which could result in early death for some nodes.

P-Coding scheme is proposed against eavesdropping attacks in network coding [3]. Random Linear Network Coding (RLNC) is used to linearly combine packets using linear coefficients. RLNC provides weak security. Weak security means that if meaning information about the source messages can be obtained from the intercepted packets by adversary, the system is said to be weakly secure and intrinsic secured. Lightweight permutation encryption is applied on each message and to its coding vector.

Drawbacks

- It is difficult to find codes to make network coding more secure.

To avoid the broadcast redundancy in MANET,neighbour topology based protocol is used[4].

It finds the minimum number of forward node set that form a connected dominant set.2-Hop Neighbour based protocol is used in MANET to reduce broad cast storm problem by selecting the minimum number of forwarding nodes from 1-Hop nodes to cover all 2-Hop nodes. To perform the above process DP(Dominant pruning) can also be used but it cannot eliminate all redundant transmissions. To overcome this problem TDP (Total Dominant Pruning) and PDP (Partial Dominant Pruning). But the above two proposed algorithm gets failed when used with the concept of wireless characteristics.

Drawbacks

- Network coding concept is focused only on the neighbour topologybased protocols like DP, PDP and TDP but not on existing reactive routing protocols like AODV and DSR for MANETs.

III. PROPOSED WORK

In MANET, during routing, packets will be transferred fromone node to the other node. Since packets are transferred one by oneto their neighbour node, the energy consumption will be more, and alsothe algorithm used for encryption to encrypt the data will consumesufficient energy. In order to overcome this problem, Network CodingTechnique is used along with light weight encryption scheme(Modified P-coding scheme) is applied to provide security andalso to reduce energy consumption.

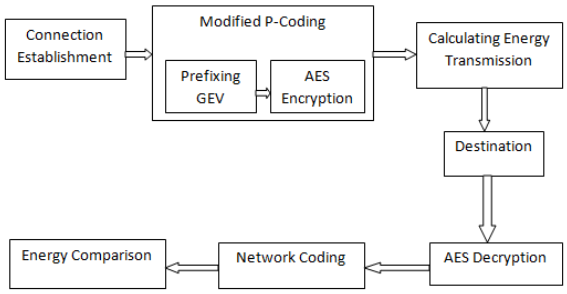

Fig 3 System Design

A. Establishing Connection and Performing Encryption

The connection is established between the nodes and the acknowledgement is received.After performing connection establishment, the file which is to be sent to the destination is chosen.Any type of file can be selected and sent to destination node.The corresponding file's contents are shown then it is encrypted using the Advanced Encryption Standard (AES) algorithm.The modified P-coding scheme is applied here. In the existing P-coding scheme, Permutation is used along with prefixing of GEV(Global Encryption Vector) but in Modified P-coding scheme, AES is used with GEV to improve security.

B. Energy transmission calculation

Normally for transmitting encrypted message from source to destination the amount of energy spent by the system to send the message to the destination is taken as energy transmission. So, here the energy transmission can be taken as CPU usage and memory. Reducing this energy is the main factor in this work. Here,the encrypted document is sent to the receiver and hencesome amount of power would be spent to forward that file to next node and some power would be spent on encryption process.The power that has been spent is measured by means of the amount of CPU utilization.This is taken as a reference and the power is reduced by network coding.

C. Decryption process

Decryption is the process of converting cipher text into the original text. Here the received data is decrypted using the Advanced Encryption Standard (AES) and the network coding is performed. In network coding the received file is split int three into n number of modules and the size of the file is reduced by allocating sizes to variables and symbols depending on their type. After the network coding the file is sent to the source and the minimized energy is obtainedAlong with the file, the GEV and the details about the power consumption is also sent and the results are shown

IV. RESULTS

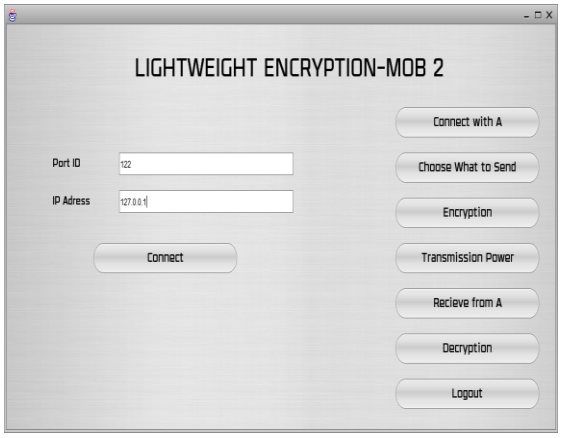

Fig 4 Connection Establishment

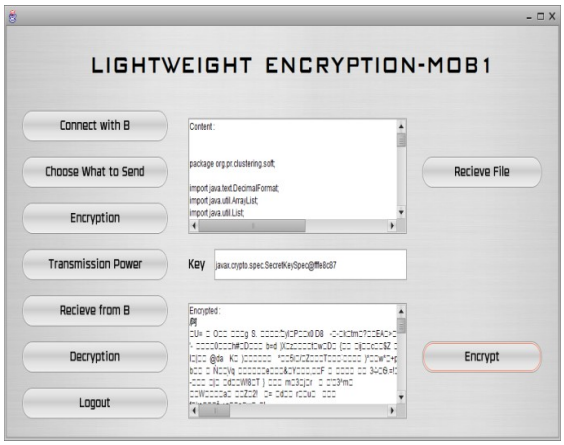

Fig5 explains the encrypted message and the key generation of the file to be sent.

Fig 6 Energy Transmission calculation

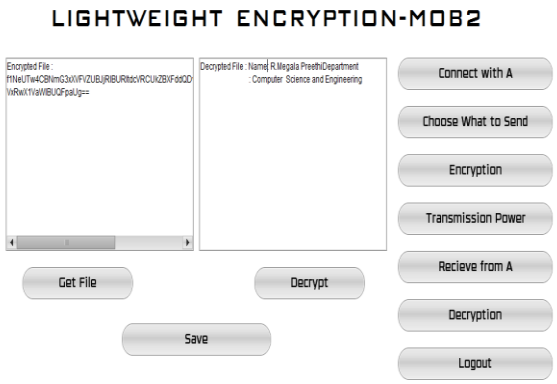

Fig 7 Decryption

V.PERFORMANCE EVALUATION

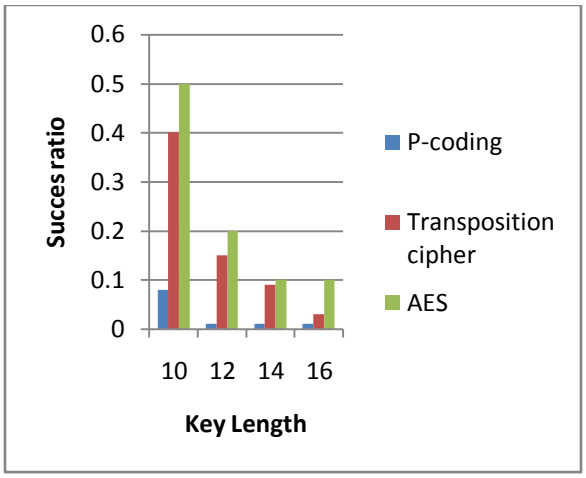

Fig 8. Calculation of Success ratio

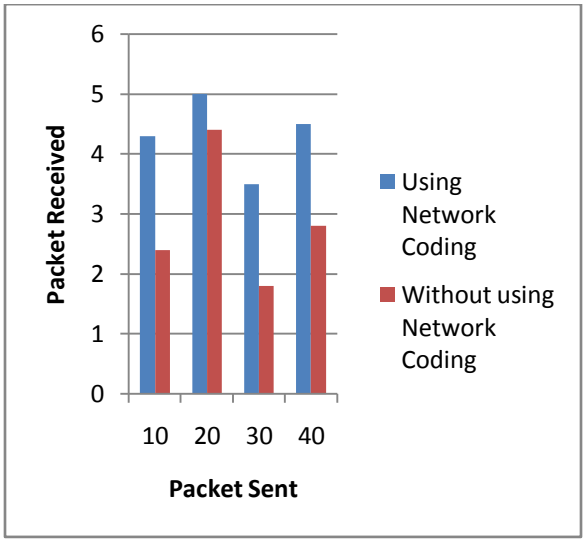

Fig 9 Calculation of Efficiency

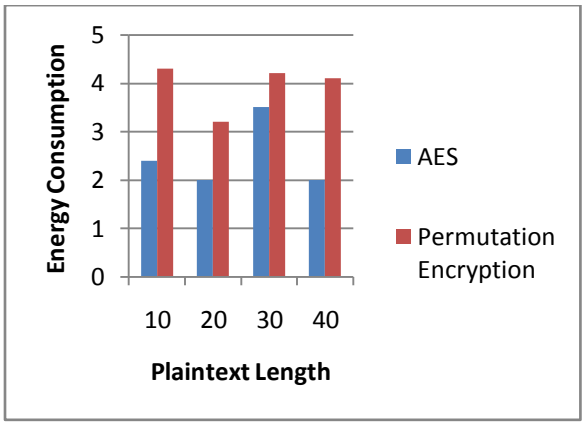

Fig 10Energy-per-byte Consumption

VI. CONCLUSION

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.

REFERENCES

[1]Y. Wu, P. Chou, and S. Kung, "Minimum-energy multicast in mobile ad hoc networks using network coding," *IEEE Transactionson Communications*, vol. 53, no. 11, pp. 1906–1918, 2005.

[2]S. Singh, C. Raghavendra, and J. Stepanek, "Power-aware broadcasting in mobile ad hoc networks," in *Proceedings of IEEE PIMRC*,1999.

[3]P. Zhang, Y. Jiang, C. Lin, Y. Fan, and X. Shen, "P-Coding: Secure network coding against eavesdropping attacks," in *Proceedings ofIEEE INFOCOM*, Mar. 2010.

[4]L. Li, R. Ramjee, M. Buddhikot, and S. Miller, "Network coding-Aware Neighbor based Topology Control in MANETs" in *Proceedings ofIEEE INFOCOM*, 2013.

[5] B. Chen, K. Jamieson, H. Balakrishnan, and R. Morris, "Span: Anenergy-efficient coordination algorithm for topology maintenancein ad hoc wireless networks," *Wireless Networks*, vol. 8, no. 5, pp.481–494, 2002.

[6] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, "Networkinformation flow," *IEEE Transactions on Information Theory*, vol. 46, no. 4, pp. 1204–1216, Jul. 2000.

[7] A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of appliedcryptography*. CRC Press, Oct. 1996.

[8] N. Cai and R. W. Yeung, "Secure network coding," in *Proceedingsof IEEE ISIT*, Jun 2002.

[9] A. Dimovski and D. Gligoroski, "Attacks on the transpositionciphers using optimization heuristics," in *Proceedings of InternationalScientific Conference on Information, Communication and Energy Systems and Technologies*, Oct. 2003.

[10] C. Gkantsidis and P. Rodriguez, "Network coding for large scalefile distribution," in *Proceedings of IEEE INFOCOM*, Mar. 2005.

[11] J. Daemen and V. Rijmen, *The design of Rijndael: AES–the advanced encryption standard*. Springer Verlag, 2002.

