Survey on Enhanced Compressed P-Coding for Energy Efficient Transmission in Mobile Ad Hoc Networks

Ankita Chouhan
M.Tech Student
CS Department
LNCT, Bhopal, Madhya Pradesh, India

Sunil Phulre
Associate Professor in CS Department
LNCT, Bhopal, Madhya Pradesh, India

Vineet Richhariya
Professor in CS Department
LNCT, Bhopal, Madhya Pradesh, India

ABSTRACT
One of the important issue in MANETs is energy saving. Recent studies show that Network coding can reduces energy consumption by less transmission in MANETs. Encryption/decryption, transmission cost and transmission time are worked as source of energy consumption in MANETs. Network coding provides intrinsic security based on which encryption can be done quite efficiently, but to provide security for MANETs symmetric key algorithms are not sufficient. This paper introduce new scheme of energy saving called Enhanced Lightweight P-Coding (ELP) proposed for MANETs, with network coding which improves throughput, transparency, security and energy efficiency. The basic idea is, let the source compress the coded message (which is prefixed with its coded vector) using Enhanced LZW algorithm and hence due to compression and without knowing the permutation, eavesdropper cannot decode the message. Data compression technique can reduce transmission time that consumes less bandwidth and low power. Thus Enhanced lightweight P-Coding consist minimal energy consumption as compare to other encryption/decryption methods.

Keywords
Mobile ad hoc network, Energy saving, Lightweight Encryption/Decryption, Compression.

1. INTRODUCTION
Mobile Ad Hoc Networks are important wireless communication system. MANETs have mobile and infrastructure-less behavior. MANETs nodes can communicate directly with each other so that MANETs emerged as a dominant mode of communication due to flexibility capability to install at any place.. It can easily collect emergency data in disastrous areas and perform communication in battle fields. Some of the characteristics of MANETs includes infrastructure-less network, dynamic network topology and self-organization etc. To minimize energy consumption and maintain longer lifetime of mobile nodes in MANETs, is critical and most important issue.

The energy saving comes from fact that less transmissions are required when in-network nodes are enabled to encode packets. Several papers describe methods to solve this energy efficiency issue. From recent studies [1] we have found that Network coding can help to reduce energy consumption. The energy saving in network coding is due to less transmission required when network nodes are enable to encode packet. Network coding is more suitable for broadcast transmission and it does not allow only intermediate nodes to store and forward packet but also allow to process incoming data to maximize multicast throughput. Apart from data transmission, energy can save by encryption/decryption operation at each node. Based on mixing property of network coding of data, it provides intrinsic security by designing more secure cryptographic scheme.

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. For required level of security, MANETs security solution also needs minimum amount of energy in wireless communication environment. To provide security for MANETs, symmetric key encryption algorithms are not efficient. Recently, there have been lots of works on developing energy efficient and low cost oriented security method in wireless networks.

There are many aspects to improve the battery life in which data compression technique is one [3]. This is achieved by transmitting the compressed data between the nodes (users) and retrieving the original data at the destination. For data compression we have many algorithms [4] in which Enhanced LZW (ELZW) compression algorithm is the best. ELZW algorithm is efficient because most of the data file to which we want to compress contains many spaces, by eliminate these spaces from the data file, results in high compression factor or less compression ratio.

Due to compression, the number of bits can be reduced to maximum extend so that the need of memory and bandwidth are very less. Also, the compressed text resembles a scramble message and an attacker in middle cannot able to understand. Therefore, the data compression not only reduces the size of the original text, but also gives data security..

2. RELATED WORK
2.1 Literature Survey
Recent studies [1] demonstrate that network coding can help achieve a 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. The basic idea can be illustrated using the following example. Suppose there are six nodes forming a hexagon, and the transmission range of each node can only reach its left and right neighbor. Each node needs to broadcast one message to all other nodes Without network coding, each message would require four broadcasts, as shown in Fig. 1(1). With network coding (Fig. 1(2)-(4)), a total number of nine transmissions are needed for three messages, i.e., three transmissions per message. If we would not consider the energy consumed by

encoding and decoding operations, this means 1/4 energy can be saved.

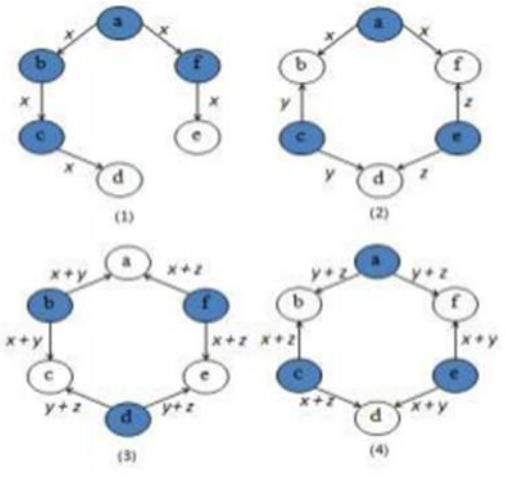


Fig 1: Network coding for transmission, Shaded nodes are those involved in transmission

The authors Vilela et al. propose such a scheme, in which the source performs random linear coding on the messages to be sent and locks/encrypts the coding vectors using the symmetric key shared between it and all sinks. Fan et al. propose to encrypt coding vectors using Homomorphic Encryption Functions (HEFs) in an end-to-end manner. Due to the homomorphic nature of HEFs, network coding can be performed directly on the encrypted coding vectors, without impacting the standard network coding operations.

2.1.1 P-Coding

The problem of energy efficiency studied by Zhang et al. [1] proposed such a scheme P-Coding, in which, a lightweight encryption method, randomly mixes symbol of each coded packet (which is prefixed with its coded vector) using permutation encryption, to make it hard for eavesdropper to locate coding vectors for decoding packet. Kulkarni et al. [3] proposed scheme Enhanced P-Coding, in which, coded message (which is prefixed with its coded vector) can compressed by LZW compression scheme and decoded by LZW decompression and Gaussian elimination scheme, so this generates confusion to eavesdropper

2.1.2 LZW Compression

Terry Welch has presented his LZW (Lempel–Ziv–Welch) algorithm in 1984[19], which is based on LZ78. It basically applies the LZSS principle of not explicitly transmitting the next non-matching symbol to LZ78 algorithm. The dictionary has to be initialized with all possible symbols from the input alphabet. It guarantees that a match will always be found. LZW would only send the index to the dictionary. The input to the encoder is accumulated in a pattern 'w' as long as 'w' is contained in the dictionary. If the addition of another letter 'K' results in a pattern 'w*K' that is not in the dictionary, then the index of 'w' is transmitted to the receiver, the pattern 'w*K' is added to the dictionary and another pattern is started with the letter 'K'. The algorithm then proceeds as follows:

w := NIL;

while (there is input) {

K := next symbol from input;

if (wK exists in the dictionary) {

w := wK;

} else {

output (index(w));

add wK to the dictionary;

w := k;

}

}

Table 1.

n	a=(3+n*2)	nth codeword	no. of code words	Range of integers
0	3	0xxx	2^3 =8	0-7
1	5	10xxxxx	2^5 =32	8-39
2	7	110xxxxxxx	2^7 =128	40-167
3	9	111xxxxxxxxx	2^9 =512	168-679
		Total	680	

In the original proposal of LZW, the pointer size is chosen to be 12 bits, allowing for up to 4096 dictionary entries. Once the limit is reached, the dictionary becomes static. Now in LZW algorithm if we make dictionary of 680 entries. Each entry occupy 9 bits up to 680 entries, And if we want to increase dictionary size up to 2044 entries then each entry occupy 10 bits. But in [4] scheme ELZW eliminate the spaces from the input data file. In this scheme if we make dictionary of 680 entries, Each entry occupy 10 bits, i.e. 1 bit higher than those in case of LZW encoding algorithm, 9bit data plus one parity bit used for checking the next character is space or not. If parity bit is set then next character is space otherwise not. But we save the 9 bits which is used for space. Now there are number of spaces in data file say n, Now we save n*9 bit space. But some extra parity bits are also sent, but many words in data file have small length. So spaces between these words occupy lot of space, so by eliminate these spaces we can achieve high compression.

2.1.3 Enhanced LZW Compression

Author Amit Setia and Priyanka Ahlawatet al. [4] performed comparison between various text compression methods, [4]-[6] in which ELZW performs better than other compression techniques. ELZW is enhanced LZW where LZW is a part of LZ78 (Lempel-Zip) family.

PRACTICAL COMPARISON OF LZW and ELZW ALGORITHMS

Table 2.

File size	Compression ratio with LZW compression	Compression ratio with enhanced LZW compression
5.7 kb	0.50	0.47
10 kb	0.61	0.53

For two files, one is of 5.7 kb and another is of 10 kb. When it compressed first file which is of 5.7 kb using LZW, the compression ratio of 0.50 achieved. But when it compressed same file using ELZW then it achieved compression ratio of

0.47. In second case when it compressed another file of 10 kb size using LZW algorithm then it achieved compression ratio of 0.61. But when it compressed same file using ELZW it achieved compression ratio of 0.50. But compression ratios in case of enhanced LZW vary data to data.

2.2 Problem Statement

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.

Permutation encryption scheme [2] P-coding which is more efficient and assures confidentially. The basic idea of this scheme is permutation encryption is applied on each packet before performing network coding operations. Without knowing the permutation, eavesdroppers cannot decode, and thus cannot obtain any meaningful information.

2.2.1 Network Coding

Network coding is a technique which allow intermediate node to mix incoming data flows in order to reduce energy consumption as well as transmission time. Network coding is implemented with performing X-OR operation on packet data Without network coding routers just store and forward the received messages to intended node. For example, Alice and Bob wants to exchange the data via router, so without network coding Alice sends data to router and then router send the data to Bob only then Bob send data to router and then router sends it to Alice. So this requires 4 transmission but with network coding, Alice and Bob simultaneously sends data to router and then router can forward data to intended receiver. It requires only 3 transmission.

2.2.2 P-Coding

[1]-[2] The P-Coding scheme performs permutation encryption on the coded messages. In the network each node prefixes the Global Encoding Vector (GEV) to the packet. Permutation encryption operation randomly mixes the symbols of the messages and corresponding GEVs. This operation creates considerable confusions to the eavesdroppers. Generally P-Coding scheme consists of three stages: source encoding, intermediate recoding, and sink decoding.

2.2.2.1 Source Encoding

Consider in general that a source s wants to transmit h messages. Each message is prefixed with the GEV and permutation encryption operation is performed. Finally the encrypted message is generated.

2.2.2.2 Intermediate Recoding

As the symbols of messages and corresponding GEVs are rearranged by permutation encryption operation it is difficult to construct the source messages. The intermediate nodes have no idea of the key being used and hence it is difficult to decrypt the message.

2.2.2.3 Sink Decoding

At the sink node the cipher-text is received and decrypted using the permutation decryption operation. Finally the original message is obtained by applying Gaussian elimination.

2.2.3 Enhanced P-Coding

[3] Network coding is applied in enhanced scheme in which, if the source may need to transmit large volume of data then source should divide this data into generations and network coding can performed on the message that belongs to same generation. If the same permutation encryption function (PEF) key is used throughout the transmission and if key disclosed in one generation will compromise the secrecy of the transmission. If this key is randomly chosen in each generation and shared only by source and sink, this scheme can effectively prevent single generation failure but it brings some space overhead as the key should be transmitted in each generation. This problem can be removed with compressing the coded message. This method consists of two phases: Source encoding and Sink decoding.

2.2.3.1 Source encoding

Consider source has h messages, to be sent. It first prefixes these h messages with their corresponding unit vectors. Then the source performs linear combinations on these messages with randomly chosen LEVs and get the coded messages ,finally, the source performs LZW encoding on each message to get its compressed form and the compressed form of the coded message is transmitted to the sink.

2.2.3.2 Sink Decoding

For each sink node, on receiving a compressed data it decompress the message by performing LZW decoding on it to obtain coded message., the sink derives the matrix Finally, the source messages can be recovered by applying Gaussian eliminations.

Data compression technique can reduce the power consumption because it consumes less power by transmitting compressed coded message results increasing in battery life. LZW is a general compression algorithm capable of working on almost any type of data. It is generally fast in both compressing and decompressing data and does not require the use of floating-point operations. LZW technique also has been applied for text file. This technique is very efficient to compress image file such tiff and gif. However, this technique not efficient for compress text file because it require many bits and data dictionary. Due to LZW compression scheme, it contains some space overhead. In LZW, the pointer size is chosen to be 12 bits, allowing for up to 4096 dictionary entries. Once the limit is reached, the dictionary becomes static.

Advantages of LZW Algorithm

1. LZW data compression algorithm is an adaptive and very effective means to save storage space and network bandwidth.
2. LZW algorithm is easy to implement.
3. It is a lossless compression algorithm, so no loss of information is there.

Disadvantages of LZW:

1. Files that do not contain any repetitive data at all, cannot be compressed much.

2. It is slow to adapt its input, since strings in the dictionary become only one character longer at a time.
3. Each and every time a new character is read in, the table has to be searched for a match. If match is not found then a new string has to be searched for a match. This causes problem, the string table can get very large very fast.
4. Some extra parity bits are also sent, but many words in data file have small length. So spaces between these words occupy lot of space.

3. PROPOSED DESIGNED AND METHODOLOGY

In [4] paper, we first discuss about enhanced LZW is an algorithm that removes space from data file. LZW [Welch 1984] is a popular variant of LZ78 [Ziv and Lempel 1978], developed by Terry Welch in 1984. It is a dictionary based adaptive algorithm. The first 256 entries are occupied in the dictionary before any data is input. Most of the data file to which we want to compress contains many spaces. By eliminate these spaces from the data file, results in high compression factor or less compression ratio described by Amit Setia and Priyanka.

3.1 Enhanced Lightweight P-Coding

The Enhanced Lightweight P-Coding scheme performs permutation encryption on the messages and then coded message will compressed by ELZW compression technique . In the network each node prefixes the Global Encoding Vector (GEV) to the packet. Permutation encryption operation randomly mixes the symbols of the messages and corresponding GEVs. Then perform ELZW compression on this coded message. This operation creates considerable confusions to the eavesdroppers.

Proposed scheme has some steps:

3.1.1 Encoding

Consider in general that a source s wants to transmit h messages. Each message is prefixed with the GEV and permutation encryption operation is performed. The source performs ELZW encoding on each message to get its compressed form and this compressed form of the coded message is transmitted to the sink.

3.1.2 Decoding

At the sink node the cipher-text is received, it first decompressed the cipher-text by ELZW decompression technique to obtain the coded message. Then sink obtain a matrix and by applying Gaussian elimination method on the coded matrix message, sink can recover the original message that is send by source.

Enhanced LZW Encoding Algorithm

Step 1. Initialize dictionary to contain all 0 to 255 single character string.

Step 2. Read first input character prefix string ω from the input data file.

Step 3. Read next input character says k from the input data file.

a. If no such k (input exhausted): output:=code(ω):Then EXIT

b. If k=space, then set M.S.B bit of ω equals to 1, Repeat step 3.

c. If ωk exists in dictionary: ω: = ωk; Repeat Step 3.

d. Else If ωk not in dictionary. Then output :=code (ω)

Dictionary: = ωk;

ω :=k;

Repeat step 3.

Step 4. End

Enhanced LZW Encoding Algorithm Description

In step no. 3 (b) we set the parity bit or M.S.B bit of suffix ω. that helps in decoding site.

Enhanced LZW Decoding Algorithm

Step 1. Read first input character ω, left shift the input character ω by 1. ie ω <<1. And result is stored in the carry bit. Then right shift the input character ω by 1. ie ω >>1. And CODE=OLD code=input code with CODE=code (k), output=k, Fin char=k.

Step 2. If carry bit = 1
Then next input character k = space.
Go to step 3.
Else Read next input character k from the input data file, left shift the input character k by 1. ie k <<1. And result is stored in the carry bit. Then right shift the input character k by 1. ie k >>1.
CODE = INCODE = next input code
If no new code: EXIT. Else:

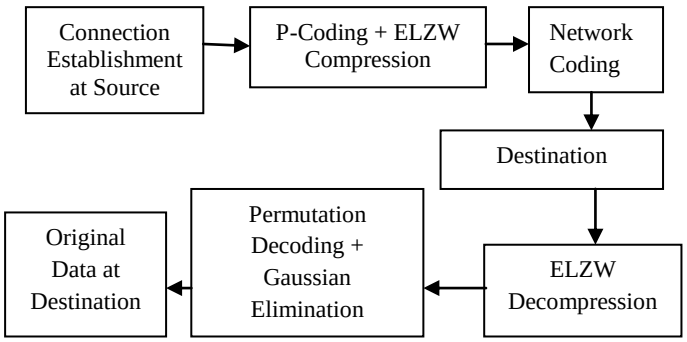
Step 3. If CODE=code (ωk): stack = k
CODE: =code (ω)
Repeat Step 3
Else if CODE = code (k): output=k, Fin char=k.
Do while stack not empty:
Output = Stack top, Pop stack.
Dictionary = OLD code, k.
OLD code = IN code;
Repeat step 2.

Step 4. End

Enhanced LZW Decoding Algorithm Description

In step 1 we first left shift the character ω by 1 and result stored in carry bit. And now for retrieving actual data we right shift the character by 1.

3.2 System Architecture Design



The system architecture design for the proposed scheme is as shown above. [9]Initially we obtain topological information about the network by using the AODV protocol. In P-Coding the permutation encryption is performed on the corresponding GEVs and symbols of messages.[14] Then ELZW compression is performed on coded message. Then the network coding is performed on this messages belonging to the same generation. Finally it is transmitted to the destination or sink node. At the sink node the ELZW decompression and

permutation decryption is performed and the Gaussian elimination is applied to obtain the original message.

4. CONCLUSION

Firstly, we study the problem of energy saving in MANETs is based on the network coding technique. Network coding reduces energy consumption in MANETs by less transmission, so the P-Coding is proposed to provide confidentiality to network coded MANETs. The P-Coding, a lightweight encryption scheme on top of network coding, incurs less energy consumption by cutting the security cost. Further the key perturbation method is employed to improve the security of P-Coding with less overhead in computation. But it does not provide complete security, which can be provided by Enhanced P-Coding by using LZW compression on ceded message but in this scheme LZW technique is not much efficient. So we proposed Enhanced Lightweight P-Coding with ELZW compression technique which will perform better than LZW compression technique. In this paper we accomplished a system which eliminate spaces from the data file so that we can achieve high compression. So any eavesdropper cannot decode this compressed coded message. Hence Enhanced method is efficient in computation and incurs less energy consumption for encryption/decryption.

5. 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 Trans. Parallel and Distributed Systems, Vol. 25, No. 9, September 2014.

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

[3] Ms. Sonali Kulkarni and Prof. M. S. Chaudhari, "An Energy Efficient Encryption Scheme for Secure Transmissions in Mobile Ad Hoc Networks", IJARCSSE, Volume 4, Issue 9, September 2014

[4] Amit Setia and Priyanka Ahlawat, "Enhanced LZW Algorithm with Less Compression Ratio", Proceedings of ICAdC, AISC 174, Springer India 2013.

[5] Senthil Shanmugasundaram and Robert Lourdusamy, "A Comparative Study Of Text Compression Algorithms", International Journal of Wisdom Based Computing,Vol. 1 (3), December 2011

[6] Kenneth Barr and Krste Asanovi´c., "Energy Aware Lossless Data Compression", May 2003..

[7] "The Data Compression Book", by Mark Nelson and Jean Loup Gailly

[8] Pooja Mundhe and Prof. V. S. Khandekar, "Survey of Energy Efficient Encryption Scheme for Vehicular Ad Hoc Network", IJIACS , ISSN 2347 – 8616, Volume 3, Issue 9 November 2014

[9] "Data Compression, the complete reference", by David Salomon

[10] Shruthi N and Manimozi "Dynamic Adaption of P-Coding Scheme for Network Coded Mobile AdHoc Networks" IJESC, ISSN-2321 -3361, Issue June 2014

[11] C. Fragouli, J. Widmer, and J. Boudec, "A network coding approach to energy efficient broadcasting: from theory to practice," in Proceedings of IEEE INFOCOM, 2006

[12] J. Wieselthier ,G. Nguyen, and A. Ephremides, "Algorithms for energy-efficient multicasting in static ad hoc wireless networks," Mobile Networks and Applications, vol. 6, no. 3, pp. 251–263, 2001

[13] Y. Fan, Y. Jiang, H. Zhu, and X. Shen, "An Efficient privacy preserving scheme against Traffic analysis in network coding," in Proceedings of IEEE INFOCOM, Apr. 2009.

[14] Bell T.C, Cleary J.G, and Witten I.H., "Text Compression", Prentice Hall, Upper Saddle River, NJ, 1990.

[15] Fiala E.R., and D.H. Greene, "Data Compression with finite windows", Communications of the ACM 32(4):490-505, 1989.

[16] G.Soma Sekhar and Dr.E.Sreenivasa Reddy, "An Enhanced Data Security with Compression for MANETs" in International Journal of Computer Networks and Communications Security, VOL. 2, NO. 12, DECEMBER 2014, 456–461

[17] Prachi Sharma and S.V. Pandit, "Energy Efficient and Low Cost Oriented High Security Method for MANET: A Review", IJAIEM, Volume 3, Issue 3, March 2014.