Volume 2, Issue VIII Aug 2014
ISSN 2320-6802

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

Providing Energy Efficient Security for Mobile Ad hoc Networks

Ms. Sonali Kulkarni[1], Prof. M.S.Chaudhari[2]

[1]Student (ME Computer Engg), Sinhgad Institute of Technology
[2]Guide (CSE Dept) Sinhgad Institute of Technology
Lonavala, Pune

***Abstract**: Network coding promises significant benefits in network performance. Transmission cost data; encryption /decryption are the sources of energy consumption in Mobile Ad Hoc Networks. Network coding helps to reduce energy consumption in MANETs, but is weak to provide confidentially and security for global evasdroppers.To provide security for MANETs symmetric key algorithms are not sufficient. This paper introduces new permutation encryption scheme in combination with network coding to increase throughput, reliability and security for MANETs. Such a scheme designed in practice will help in building secure MANET based application.*

***Keywords:** MANET, Security, Encryption, Decryption, Energy.*

1. INTRODUCTION

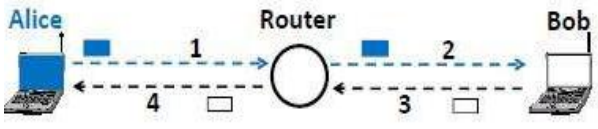
Due to flexibility capability to install at any place and would not require any infrastructure Mobile ad hoc networks have emerged as a dominant mode of communication. To minimize energy consumption is the critical problem in MANETs [2]. Network coding [5] can help to reduce lower energy consumption in MANETs with less transmissions [6],[9],[10]. Network coding not only allow intermediate nodes to store and forward packet but also allow to process and mix incoming data flows to maximize multicast throughput. Besides basic transmissions data encryption/decryption are also the sources of energy consumption in MANETs. Some MANETs like MANETs in military or banking require some level of security. Several energy-efficient schemes are proposed to resolve this issue [3-4].To provide security for MANETs symmetric key encryption algorithms are not efficient.

This paper proposes a new permutation encryption scheme which is more efficient and assures confidentially. The basic idea of the 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.

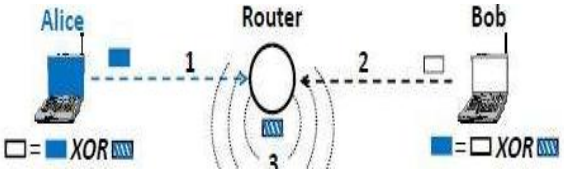
Our objective is to propose a new energy efficient encryption scheme which is more efficient and assures confidentially. We propose such a scheme to provide security, transparency, scalability robustness and energy efficiency for MANETs.

1.1 Network coding background:

Network coding is a technique which improves scalability, transparency, energy efficiency and performance in MANETs. Network coding 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.



(a)



(b)

Figure 1: Example how network coding reduces transmission time in MANETs.

Without network coding the router just store and forwards the received messages to intended node. When Alice and Bob want to exchange data 4 transmissions are required as shown in Figure 1(a). Whereas with network coding the in Figure 1(b) router combines the received messages into single message and forward to the intended nodes. This requires only 3 transmissions. If energy consumed by encryption/decryption is not considered ¼ energy can be saved.

2. RELATED WORK

Introduced symmetric key encryption [6] algorithms to encrypt packet to provide confidentiality for network coded MENETs. But this approach is not efficient. Another cryptographic approach, in which the source performs random linear coding on the messages to be sent and encrypts the coding vectors using the symmetric key shared between it and all sinks [7].

Fan et al. [8] 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. The above two approaches have large overhead with respect to either computation or space, and may not be suitable for MANETs.

This paper proposes a new encryption scheme to provide security, confidentiality transparency, scalability robustness and energy efficiency for MANETs.

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

3. The PROPOSED SCHEME

The proposed scheme based on permutation encryption.

Definition 1. Let $\boldsymbol{m} = [m1, m2, \ldots, mn]$ be a sequence of symbols, k be the permutation of length n. The permutation encryption function is

$E_k(m) = [m_{k(1)}, m_{k(2)}, \ldots\ldots\ldots\ldots m_{k(n)}]$.

The permutation decryption function is

$D_k(E_{k(m)}) = m$.

K is the PEF key.

The idea of proposed scheme is to mix symbols of the messages and corresponding GEVs and reorder together after performing permutation encryptions on coded messages. PEF key shared by symmetric key which is established by key distribution centre. The proposed scheme based on three stages Encoding by source, Recoding by intermediate node, and Decoding by sink

- **Encoding By Source:**

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 gets the coded messages finally, the source performs permutation encryption to get ciphertext.

Source Sink

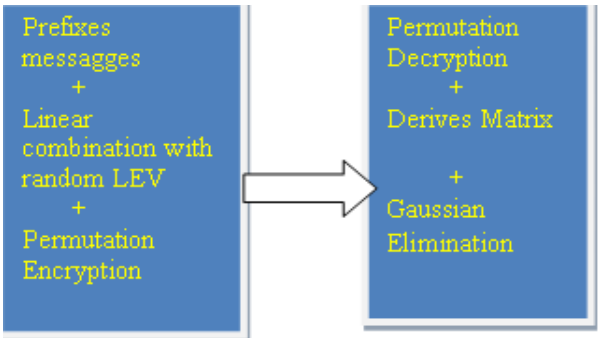


Figure 2: Permutation encryption

- **Recoding by intermediate node:**

Intermediate node have no knowledge of PEF key so cannot reconstruct source message. Performs recoding on encrypted message.

- **Decoding by sink:**

Each sink decodes message received from its neighbor by performing permutation decryption.

Sink derives the matrix and finally performs Gaussian elimination on matrix to recover source.

4. ENHANCED SCHEME

If the source may need to transmit a large volume of data *D*. The source should first divide *D* into generations and network coding can be performed on the messages that belong to same generations [1]. If the same PEF key is used throughout the transmission, if key disclosed in one generation will compromise the secrecy of the transmission. If the perturbing key is randomly chosen each generation and communicated securely between the source and sinks, this scheme can effectively prevent the single generation failure but definately bring some space overhead as the key should be transmitted in each generation.

The problem can be removed with compressing the coded message by Lempel-Ziv-Welch algorithm.

Another important and simple technique for reducing power consumption is Data Compression, which consumes less power by transmitting compressed data results increasing in battery life.

A lossless technique is that the restored data file is identical to the original.

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.

A decompression program returns the information to its original form.

4.1 Lempel-Ziv-Welch (LZW) compression

It is fast and simple to apply and works best for files containing lots of repetitive data. LZW compression algorithm has higher compression ratio than other coding techniques.

Table 1: Comparison of Compression Techniques

Types of file	Huffman Encoding	LZW compression	Run Length Encoding
Text file	34%	56%	25%
Speech file	35%	36%	27%
Image file	6%	12%	3%

LZW Encoding Algorithm

Initialize Dictionary with 256 single character strings and their corresponding ASCII codes;
Prefix←first input character;
CodeWord← 256;
while(not end of character stream){
Char← next input character;
if (Prefix + Char exist in the Dictionary)
Prefix ← Prefix + Char;
else{
Output: the code for Prefix;
insertInDictionary((CodeWord , Prefix + Char)) ;
CodeWord++;
Prefix← Char;
}
}
Output: the code for Prefix;

LZW Decoding Algorithm

output: string(first CodeWord);
while(there are more CodeWords){

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

if(CurrentCodeWord is in the Dictionary)
output: string(CurrentCodeWord);
else
output: Previous Output + Previous Output first character; insert in the Dictionary: PreviousOutput + CurrentOutput first character;
}

The basic idea of Enhanced scheme is to let source compress the coded messages (prefixed with coding vectors) using LZWencoding technique and hence the original message is said to be encrypted efficiently since it is very difficult for the eavesdropper to obtain any meaningful information from compressed data.

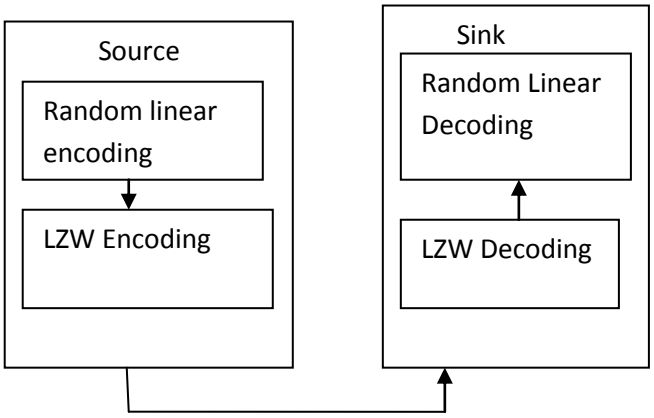


Figure 3: Enhanced Permutation Encryption

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 thesemessages 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.

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 .

5. CONCLUSION

The problem of energy saving in MANETs based on the technique of network coding is studied. Previous studies demonstrated that network coding can reduce energy consumption with less transmission in MANETs. Permutation Encryption an energy encryption scheme on top of network coding is proposed to further reduce energy consumption in MANETs by cutting the security cost and transmission cost. Enhanced scheme to transfer large volume of data is introduced with combination of LZW and permutation encryption .This will generate considerable confusion to eavesdropping adversaries. Hence Enhanced encryption scheme is efficient in computation, and incurs less energy consumption for encryptions/decryptions.

REFERENCES

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

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

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

[4] **B. Chen, K. Jamieson, H. Balakrishnan, and R.Morris, "Span: An energy-efficiencoordination algorithm for topology maintenance in ad hoc wireless networks", vol. 8, no. 5, pp.481– 494, 2001.**

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

[6] **N. R. Potlapally, S. Ravi, A. Raghunathan, and N. 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. 128–143,2006.**

[7] **J. P. Vilela, L. Lima, and J. Barros, "Lightweight security for network coding," In Proceedings of IEEE ICC, May 2008**

[8] **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.**

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

[10] **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.**