ENHANCED P-CODING: AN ENERGY SAVING ENCRYPTION SCHEME FOR MOBILE AD HOC NETWORKS

Ms. Pallavi.S¹, Mr. Santhosh Kumar.G ²

¹M. Tech. Student, ²Assistant Professor Department of CSE, Don Bosco Institute of Technology, Bangalore, (India)

ABSTRACT

Energy saving is an important issue in Mobile Ad Hoc Networks (MANETs). Network coding can help reduce the energy consumption in MANETs by using less transmissions. However, apart from transmission cost, there are other sources of energy consumption, e.g., data encryption/decryption. To address this issue, by exploiting networking coding technique, an energy saving encryption scheme called Enhanced P-Coding is proposed for MANETs. The basic idea of Enhanced P-Coding is to let source compress the coded messages (prefixed with coding vectors) using run length encoding 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. Random linear coding and run length coding are quite simple and vulnerable to cryptographic analysis. Enhanced P-Coding reduces the encryption time due to the light weight nature of random linear coding and run length coding. Lesser the encryption time also means fewer CPU cycles, and less energy consumptions. Thus Enhanced P-Coding incurs minimal energy consumption for encryptions/decryptions compared to other encryption schemes.

Keywords - Mobile Ad Hoc Networks, Energy Saving, Network Coding, Random Linear Coding, Run Length Coding.

1 INTRODUCTION

MOBILE Ad Hoc Networks (MANETs) are important wireless communication paradigms. Mobile ad hoc networks (MANETs) is an infrastructure-less, dynamic network consisting of a collection of wireless mobile nodes that communicates with each other without the use of any centralized authority. The mobile and infrastructure less nature of MANETs makes them suitable for collecting emergency data in disastrous areas and performing mission-critical communication in battle fields. A critical issue in MANETs is how to reduce energy consumption and maintain a longer life time for mobile nodes.

Recent studies demonstrate that network coding [5] can help achieve a lower energy consumption in MANETs [6]–[8]. 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 Alice and
Bob wants to exchange messages among them via router. Without network coding (Fig (a)), the router just store and forward the received messages to the intended node. Therefore 4 transmissions are required to exchange the messages. Whereas with network coding (Fig (b)), the router merges the received message into single message and forward to the intended nodes and thus require only 3 transmissions. If we would not consider the energy consumed by encoding and decoding operations, this means 1/4 energy can be saved.

Fig. 1.2: Example illustrating how network coding reduces transmission times in MANETs.

Besides basic transmissions, energy consumption can also come from encryption and decryption operations at each node, as most MANETs need some level of protection on their content. For example, in a battle field, the data communicated between soldiers with mobile devices can be very sensitive, and should be kept confidential during transmissions. The straightforward approach to provide confidentiality for network-coded MANETs is to encrypt the packet payload using symmetric-key encryption algorithms. While this method is not that efficient: reference [9] shows that on a Motorola’s “DragonBall” embedded microprocessor, it consumes around 13.9μJ to send a bit, while consumes another 7.9μJ per bit when symmetric-key algorithms are used. In fact, the information mixing feature of network coding provides an intrinsic security, based on which a more efficient cryptographic scheme can be designed. Vilela et al. [10] 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. [11] 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. However, the above two approaches have large overhead with respect to either computation or space, and may not be suitable for MANETs.

In this paper, we propose a new encryption scheme which is lightweight in computation by leveraging network coding which makes it very attractive in network-coded MANETs to further reduce energy consumption.

II THE PROPOSED SYSTEM

This section defines random linear coding and run length encoding, based on which Enhanced P-Coding is introduced.

2.1 Run-Length Encoding (RLE)
Run-length encoding is a very simple form of data compression in which runs of data (that is, sequences in which the same data value occurs in many consecutive data elements) are stored as a single data value and count, rather than as the original run. RLE is a lossless data compression. In lossless data compression, the integrity of the data is preserved. The original data and the data after compression and decompression are exactly the same because, in these methods, the compression and decompression algorithms are exact inverses of each other: no part of the data is lost in the process. Redundant data is removed in compression and added during decompression. Lossless compression methods are normally used when we cannot afford to lose any data.

2.2 Random Linear Coding

Consider the case that one node $s$ needs to deliver a series of packets $x_{i_1}, x_{i_2}, \ldots, x_{i_h}$ to a set of sinks $T \subset V$. Define the matrix of source packets as $X = [x_{i_1}, \ldots, x_{i_h}]^T$, i.e., $X$ consists of all source packets as its rows. For simplicity, let $\Gamma^+(s) \cap V \neq \emptyset$. $y(e)$ consists of $h$ imaginary links, $e_1, \ldots, e_{h_1}$, with $y(e_i) = x_{i_i}$. Then for any $e \in \Gamma^+(v) \cap V$, $y(e)$ is calculated by linearly combining the incoming packets of $v$ as:

$$ y(e) = \sum_{e' \in \Gamma^+(v)} \beta_{e'}(e) y'(e') = \beta(e) [y^T(e')]_{e' \in \Gamma^+(v)} $$

(1)

Where the coefficients $\beta_{e'}$ are chosen over $F_q$, and the row vector $\beta(e) = [\beta_{e'}]_{e' \in \Gamma^+(v)}$ is termed as the Local Encoding Vector (LEV) of link $e$. By induction, $y(e)$ can be represented as the linear combination of source packets:

$$ y(e) = \sum_{i=1}^{h} g_{i}(e)x_{i} = g(e)X $$

(2)

where $g(e) = [g_{e_1}(e), \ldots, g_{e_h}(e)]$ can be calculated recursively using Eq. (1), and is termed as the Global Encoding Vector (GEV) of link $e$. Assume that $h$ packets $y(e_1), \ldots, y(e_h)$ are received by a sink node $v$ from links $e_1, \ldots, e_h$. Then, by applying Eq. (2), we have:

$$ Y = \begin{bmatrix} y(e_1) \\ \vdots \\ y(e_h) \end{bmatrix} \begin{bmatrix} g(e_1) \\ \vdots \\ g(e_h) \end{bmatrix} X = GX $$

(3)

where $G$ is termed as the Global Encoding Matrix (GEM) of node $v$. Since $G$ is invertible with high probability when $q$ is sufficiently large [13], $v$ can reconstruct source messages $X$ by calculating $X = G^{-1}Y$.

In practice, the source prefixes each packet $x_i$ with the $i$th unit vector $u_i$:

$$ [u_i, x_i] = [0, \ldots, 0, 1, 0, \ldots, 0, x_{i_1}, \ldots, x_{i_h}] $$

(4)
Where each $u_i$ is termed as a tag. With the same coding operations performed on these tags, each packet will automatically contain its GEV.

### 2.3 Enhanced P-Coding Scheme

The basic idea of Enhanced P-Coding is to let source compress the coded messages (prefixed with coding vectors) using run length encoding 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.

![Diagram](image)

**Fig 2.3: Enhanced P-Coding**

The Enhanced P-Coding scheme primarily consists of two stages: source encoding and sink decoding.

#### Source Encoding

Consider the situation that a source $s$ has $h$ messages, denoted by column vectors $x_1, \ldots, x_h$, to be sent out. It first prefixes these $h$ messages with their corresponding unit vectors, according to Eq. (4). Then the source performs linear combinations on these messages with randomly chosen LEVs. For instance, with LEV $\beta(e_i)$ of output link $e_i$, we can get the coded message $y(e_i) = [\beta(e_i), \beta(e_i)X]$, where $X = [x_1^T, \ldots, x_h^T]^T$. Finally, the source performs run length encoding on each message $y(e_i)$ 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 run length decoding on it to obtain coded message. Once $h$ linearly independent messages $y(e_1), \ldots, y(e_h)$ are collected, the sink derives the following matrix representation similar to 3:

$$
Y = \begin{bmatrix}
    y(e_1) \\
    \vdots \\
    y(e_h)
\end{bmatrix}
= \begin{bmatrix}
    g(e_1), g(e_h)X \\
    \vdots \\
    g(e_h), g(e_h)X
\end{bmatrix}
= [G, GX]
$$

(5)
Finally, the source messages can be recovered by applying Gaussian eliminations on $Y$:

$$Y = [G, GX] \xrightarrow{Gaussian \ elimination} [I, X]$$  \hspace{1cm} (6)

**Advantages of Enhanced P-Coding**

- Compression of coded message using run length coding is done. Eavesdroppers cannot obtain the meaningful information from the compressed data. Hence compressed data can be called as encrypted data which is transmitted to the sink.
- Faster transmission time across the network and reduced transmission cost due to run length coding.
- Intermediate recoding is avoided. No extra effort or computation is needed at intermediate nodes and energy consumption at intermediate nodes is reduced. Random linear coding and run length coding are quite simple and vulnerable to cryptographic analysis.
- Enhanced P-Coding is quite lightweight in computation. In addition, Enhanced P-Coding does not cause any space overhead either.
- Enhanced P-Coding reduces the encryption time due to the light weight nature of random linear coding and run length coding. Lesser the encryption time also means fewer CPU cycles, and less energy consumptions. Thus Enhanced P-Coding incurs minimal energy consumption for encryptions/decryptions compared to other encryption schemes.

**III CONCLUSION AND FUTURE WORK**

3.1 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. Enhanced P-Coding, 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 P-Coding exploits the intrinsic security property of network coding and uses simple run length coding to generate considerable confusion to eavesdropping adversaries. Hence Enhanced P-Coding is efficient in computation, and incurs less energy consumption for encryptions/decryptions.

3.2 Future Work

The future work includes extending the application of Enhanced P-Coding to other communication networks, e.g., vehicular ad hoc networks.

**REFERENCES**


