A Lightweight Encryption Method with Enhanced Key Perturbing in Network Coded MANETs

Prathibha H K
PG Student Dept. of CS&E
CIT, Gubbi
Tumkur, India

Sharayu Pradeep
Assistant Professor Dept. of CS&E
CIT, Gubbi
Tumkur, India

***Abstract*-Saving energy is an important issue in Mobile Ad Hoc Networks (MANETs).By using less transmission network coding help to obtain low energy consumption in MANETs. Besides these basic transmissions, energy consumption can also come from encryption and decryption operations.In this paper we do network coding in order to minimize the energy consumed by packet encryption in MANETs. Intrinsic security is one of the property of network coding, based on which encryption can be down. To this end, we propose p-coding, a novel security scheme against eavesdropping attacks in network coding. With the lightweight permutation encryption performed on each message and its coding vector to provide confidentiality for network-coded MANETs in an energy-efficient way. The basic idea of p-coding is it randomly reorder the symbols of each coded packet (packet prefixed with its coding vector) using permutation encryption.This randomly reordering has become difficult for eavesdroppers to search coding vector for packet decoding.and thus no meaningful information has gained. Finally we can say that because of its lightweight nature, p-coding has obtained energy saving compared to other schemes.**

***Index Terms-Mobile ad hoc networks, energy saving, network coding, key perturbing lightweight encryption*.**

I. INTRODUCTION

Mobile ad hoc network is a self -configuring infrastructureless network of mobile devices connected by wireless. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. MANETs is a kind of wireless ad hoc networks. Figure 1 shows a simple ad hoc network with 3 nodes.Node 1 and node 3 are not within range of each other, however the node 2 can be used to forward packets between node 1 and node 2. The node 2 will act as a router and these three nodes together form an ad-hoc network.

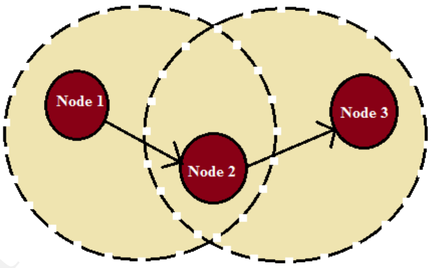


Fig 1: Example of MANET

MANETs characteristics:

- Distributed operation
- Multi-hop Routing
- Dynamic topology
- Light-Weight terminals
- Shared Physical Medium

Mobile ad hoc networks provides some of the security goals such as

- Confidentiality
- Resilience to attack
- Freshness
- Availability
- Integrity
- Authentication

Network Coding

Network coding allows to realize energy saving when broadcasting in wireless ad hoc networks. By broadcasting we refer to the problem where each node is a source that wants to transmit information to all other nodes.Here energy saving can be obtained by less transmission. Hence by doing network coding the transmission time can also be saved in MANETs.

Network coding was introduced in [1] to improve security, throughput, robustness, and complexity.

P-Coding

P-coding is a technique in which permutation encryption is performed on the coded message.Here each coded packet is prefixed with its Global Encoding Vector(GEV) and sent to the sink. For packet decoding we need to know both the coding vector and the message content.

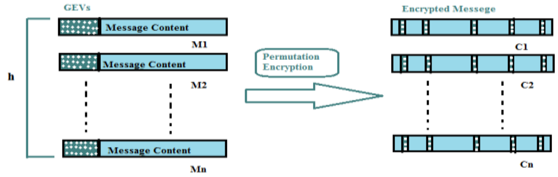


Fig 2: permutation encryption on coded message.

P-Coding scheme consist of three stages:

Sourceencoding, intermediate recoding, and sink decoding.

Source Encoding

Consider source s consist of 'h' messages. The messages are prefixed with its Global Encoding Vector(GEV) and then the permutation encryption is performed on each coded message. Finally the encrypted message is obtained as shown in figure 2.

Intermediate Recoding

As the symbols of messages are transmitted in the order of their corresponding GEV's, Since the intermediate nodes have no idea of which key being used its difficult for them to decrypt the message.

Sink decoding

On receiving the ciphertext, the sink node decrypts the message by performing the permutation decryption on it. Finally the original message can be obtained by applying Gaussian elimination method.

II. RELATED WORK

Unlike other packet-forwarding systems, network coding allows intermediate nodes to perform computation on incoming messages, making outgoing messages be the mixture of incoming messages.This approach has proved to maximize the multicast throughput . Participating nodes in Random Linear Network Coding(RLNC) linearly combine incoming messages using randomly chosen coefficients. This is verified to be both sufficient and efficient for network coding paradigms [2].

Fragouli et al. [3] studied the problem of energy-efficient broadcasting in MANETs using network coding, and propose some probabilistic algorithms. The same problem is treated in [4], in which the authors propose deterministic algorithms based on partial dominant pruning. This algorithm relies on the information of two-hop neighbours and opportunistic listening to encode packets.Bhattad et al. [5] innovatively introduced the concept of weak security, by which the system is said to be secure if the adversary cannot recover any meaningful information. They show that under this relaxed security requirement, the multicast capacity could be achieved by performing linear transformation at the source.

By doing the intrinsic security of network coding some cryptographic approaches have been proposed to secure network coding based application. One scheme is SPOC [6], proposed by vilela et al, in which the source decrypts/locks the GEV of each message after random linear coding, and attach another set of GEVs to enable standard network coding. Receivers can recover the source message by following a decode-decrypt-decode procedure. This scheme is one of the cryptographic approach and lightweight in computation. Fan et al. [8], proposed another scheme based on Homomorphic Encryption Function(HEF). This scheme has the coding coefficients encrypted using HEF. This scheme can achieve both confidentiality and privacy at the same time. However, both of these two schemes fail to fully exploit the mixing nature of network coding.

III. PROPOSED SCHEME

We propose enhanced scheme to improve the security of P-Coding. In MANETs, during practical network coding applications, such as distributed content distribution[7], the source may need to transmit a large volume of date D from one node to other node. In this case, the source should first divide D into generations:

$$D=[\underbrace{x1,\cdots,xh},\cdots,\underbrace{x_{(n-1)h+1,\cdots,x_{nh}}},\cdots] \qquad (1)$$

Then D is sent as a stream of generations, with network coding only performed among messages belonging to the same generation. In P-Coding, if the same key is used throughout the transmission, the problem of single generation failure may happen, in which an accidental key disclosure in one generation will compromise the secrecy of the following transmission.

We address this problem by randomly perturbing the key used in each generation. For the i^{th}generationG_i, let the key be used as k_i. Before the data transmission in each generation, the source conducts the following three steps:

(1) Source chooses a random permutation $\omega_i$of length n, which is termed as perturbing key.
(2) $k_i$is calculated by k_i= ωk_i, using this equation source can update k_i.
(3) The source encrypts $\omega_i$using another cryptographic approach such as AES, and sends the encrypted data of $\omega_i$to all sinks who can similarly update k_i.

If perturbing key is changedeach generation and only shared by the source and sinks, this approach could effectively prevent the single generation failure. This approach will also inevitably obtain some space overhead as the perturbing key should be transmitted in each generation. One of the possible implementation is to prefix each packet of the i^{th}generation with the ciphertext of ω_i. This will obtain 100% space overhead if no extra measure is taken, clearly not feasible. In the upcoming part, we will study how to make this approach more efficient.

Definition: Suppose π is a permutation with length n, if π(i) = i holds for each i $\notin$ [s,s+m-1]⊆[1,n], we say that π is m-partial.

For a partial permutation, some elements of it are in their original positions. It is easy to see that an m-partial permutation with length n can be represented by an integer s∈[0,n-m+1] and a permutation with length m. Thus, we could decrease the length of key to m, by using an m-partial permutation as the perturbing key.

Next we consider compressing the m-partial permutation to an integer d ∈ [0, m!-1] for efficient transmission. To achieve this goal, we must find a one-to-one correspondence between integers and permutations, so that given an integer it is efficient to calculate the corresponding permutation. In the following we will introduce proposition 1 and proposition 2, so that these two together can do the work.

Proposition 1: There is a one-to-one form correspondence between integers n∈[0,m!-1] and sequences A_{m-1}=[a_1,⋯,a_{m-1}], where a_i ∈[0,i]

Proof: First rewrite m!-1 in the following from:

m!-1= (m-1)(m-1)!+(m-1)!-1

=(m-1)(m-1)!+(m-2)(m- 2)!+⋯+2.2!+2!-1

=(m-1)(m-1)!+(m-2)(m-2)!+⋯+2.2!+1.1!

Then any n∈[0,m!-1] could be uniquely represented as:

n=a_{m-1}(m-1)!+a_{m-2}(m-2)!+⋯+a_2.2!+a_1.1!(a_i ∈[0,i])

Where a_i is calculated using three formulas: a_i=n_i%(i+1), n_{i+1}=n_i/(i+1), and n_1=n.■

Proposition 2: There is a one-to-one correspondence between sequences A_{m-1}=[a_1,⋯,a_{m-1}], where a_i ∈[0,i], and permutation with length m.

Proof: For each A_{m-1}=[a_1,⋯, a_{m-1}], we could construct a corresponding sequence B_{m-1}=[b_1,⋯,b_{m-1}] using b_i=m-a_{m-i}. As b_i ∈[i,m]follows froma_i ∈[0,i], we could obtain a unique permutation with length n, by replacing the random integer with b_i. Similarly, it is easy to verify that the reverse construction is also unique, thus a one-to-one correspondence is established.

Based on the above two propositions, we give Algorithm 1, which aims to perturb the key using five parameters, of which k is the current key to be perturbed; n and m are initially agreed upon by the source and sinks; s and d are already defined above, are chosen randomly from their respective domains to represent the perturbing key.

Algorithm 1: Key Perturbing

```
FunctionKey-Perturbing (k, n, m, s, d)
    for eachi∈[1,m-1]/* to generate the sequence[$a_1$,⋯,$a_{m-1}$] */
        a(i)←d%(i+1); d←d/(i+1);
    for each i∈[1,m-1] /* to generate the sequence [$b_1$,⋯,$b_{m-1}$] */
        b(i)←m-a(m-i);
    for each i∈[1,n] /* Initialization */
        $\pi$(i)←i;
    for each i∈[1,m-1] /* to calculate the m-partial permutation */
        $\pi$(s-1+i)↔ $\pi$(s-1+b(i));
    for each i∈[1,n] /* to perturb the current key k using $\pi$ */
        $\tilde{k}$(i)← $\pi$($k$(i));
    return $\tilde{k}$(i);
```

In this enhanced P-Coding scheme we can employ symmetric encryptions to secure the transmission of perturbing key (s, d) from the source to sink.

IV. SECURITY ANALYSIS AND PERFORMANCE EVALUATION

Security analysis: The Enhanced P-Coding Scheme

If the key does not leak out in any generation, which indicates the normal case, the security level of enhanced scheme is as high as that of the P-Coding scheme. When single generation failure occurs, the enhanced scheme can provide two extra properties.

Security: After the compromise of security in current generation, the security level in the following ones will be strong enough to avoid further attack. We show this by evaluating the computational complexity for the adversary to guess the next PEF key based on the current one. Firstly, it should locate the start point key perturbing operation, which has *O(n)* different choices. Then it should fix the correct sequence of the perturbed section of key, which has *O(m!)* different choices. It is fair to assume that these choices are equally possible, according to the randomness property of permutation encryption. Finally, it should decode the message by applying Gaussian elimination, which cost $O(h^3)$ multiplication operations. Thus, the computational complexity is $O(n,m!,h^3)$ in terms of multiplication operations, which can be made sufficiently large by choosing m property.

Recovery: As the PEF key is perturbed randomly and incrementally, it will become more and more irrelevant to its original form with iterations of generations. Consequently, even if the current key is disclosed, its randomness to the adversary will gradually recover after some generations. The following theorem will give the numerical result.

Theorem 1: After i generations, the expected number of all perturbed positions in the PEF key is approximately:

$$EX_i = \frac{i-1}{i+1}(\text{n-m})[1\text{-}(1-\frac{m}{n-m})^{i+1}]\text{+m} \qquad (2)$$

When n← ∞

Proof:Suppose there is a segment L with length n. In each round, a randomly chosen segment with length m<n in L is colored . Let X_i be the total length which has been colored after I rounds, then we are supposed to evaluate EX_i.

As n is sufficiently large, each start point of the i^{th} colored segments, defined by S_i satisfies an independent continuous uniform distribution over (0,λ), where λ=n-m. Defined a series of random variables δ_j as δ_0=$S_{(1)}$, δ_1=$S_{(2)}$-$S_{(1)}$,⋯,δ_{i-1}=$S_{(i)}$-$S_{(i-1)}$, where $S_{(j)}$ is the j^{th} order statistics of S_1,⋯,S_i. Then it follows that δ_0,δ_1,⋯,δ_{i-1} are identically distributed. Defined another series of random variables $\tilde{\delta}_j$,(1≤j≤i-1) as: $\tilde{\delta}_j$=δ_j if δ_j<m; $\tilde{\delta}_j$=m if δ_j ≥m. It is evident that $\tilde{\delta}_0$,$\tilde{\delta}_1$,⋯,$\tilde{\delta}_{i-1}$ are also identically distributed. Actually, $\tilde{\delta}_j$ is the length of segment being colored from start point $S_{(j)}$, without overlapping with that form $S_{(j+1)}$ (if there is). Thus we have $EX_i=\sum_{j=1}^{i-1} E\tilde{\delta}_j$+m=(i-1)E$\tilde{\delta}_o$+m. As the probability density function of δ_0 is f(x)=$\frac{i}{\lambda}(1-\frac{x}{\lambda})^{i-1}I_{(x\leq\lambda)}$, we also have:

$$E\tilde{\delta}_0=\int_0^m xdP(\tilde{\delta}_0 \leq x)=\int_0^m xf(x)dx + m\int_m^\lambda f(x)dx$$

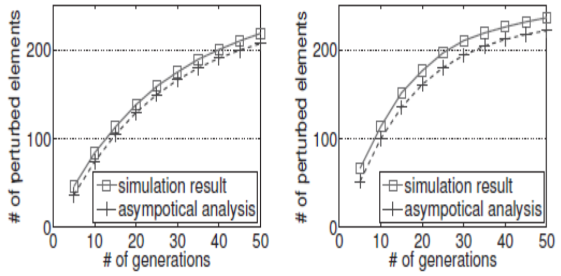
$$=\int_0^m (1-\frac{x}{\lambda})^i \text{dx}=\frac{\lambda}{i+1}[1\text{-}(1-\frac{m}{\lambda})^{i+1}]$$

Finally, the expectation of X_i can be calculated as:

$$EX_i=\frac{i-1}{i+1}.\lambda.[1\text{-}(1-\frac{m}{\lambda})^{i+1}]\text{+m}$$

Eq. (2) can be obtained by substituting λ with n-m.■

Figure 3 shows the number of perturbed symbols in PEF key increases with the number of generations, meaning that its randomness will gradually recover after accidental disclosure. we can obtain the approximated result from the theorem 1.



(a) n=255, m=10 (b) n=255, m=15

Fig 3: Number of perturbed positions vs. number of generations.

Performance Evaluation of Enhanced P-Coding scheme:

In the enhanced P-Coding scheme, the source should generate two integers s and d to represent the perturbing key generation. It is fair to assume that the generation of these two integers could be down with in constant time. So it is same with the encryption and decryption of them. As the computational complexity of key perturbing processes is *O(n)* according to Algorithm 1, the extra computational overhead incurred by the enhanced scheme is just *O(n).*

V. CONCLUSION

In this paper, we firstly studied the problem of energy saving in MANETs which is based on network coding technique. We proposed P-Coding (enhanced P-Coding), a lightweight permutation encryption scheme, to further achieve low energy consumption in MANETs by cutting the security cost. We showed that enhanced P-Coding employ symmetric encryptions to secure the transmission of perturbing key from the source to sink. And it is also efficient in computation and obtains less energy consumption for encryption/decryptions.

REFERENCES

1. R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, "Network information flow," *IEEE Trans.In Information Theory*, vol 46, no. 4, pp.1204-1216, Jul. 2000.
2. T. Ho, M. Medard, R. Koetter, D. R. Karger, M. Effros, J. Shi, and B. Leong, " A random linear network coding approach to multicast," *IEEE Transactions on Information Theory*, vol. 52, no. 10, pp. 4413-4430, Oct. 2006.
3. 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.
4. L. Li, R.Ramjee, M. Buddhikot, and S. Miller, "Network coding-based broadcast in mobile ad-hoc networks," *in Proceedings of IEEE INFOCOM*, 2007.

5. K. Bhattad and K. R. Narayanan, “Weakly secure network coding,” *in proceedings of NetCod*, Apr. 2005.
6. J. P. Vilela, L. Lima, and J. Barros, “Lightweight security for network coding,” *in proceedings of IEEE ICC,* May 2008.
7. C. Gkantsidis and P. Rodriguez, “Network coding for large scale file distribution,” *in Proceedings of IEEE INFOCOM,* Mar. 2005.
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. 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.
10. L. Lima, M. Medard, and J. Barros, “Random linear network coding: A free cipher?” *in proceedings of IEEE ISIT*, Jun. 2007.
11. 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.