

## Πρωτόκολλα και Αρχιτεκτονικές Διαδικτύου



Θέμα:

***Κωδικοποίηση Δικτύου στο Μελλοντικό Διαδίκτυο  
(Network Coding in Future Internet)***

## Περιεχόμενα:

<b>Εισαγωγή.....</b>	<b>1</b>
<b>1. Γραμμική κωδικοποίηση δικτύου (Linear network coding).....</b>	<b>2</b>
1.1 Διαδικασία κωδικοποίησης (Encoding)	
1.1.1 Επανακωδικοποίηση(Recoding)	
1.2 Διαδικασία αποκωδικοποίησης (Decoding)	
1.3 Παραδείγματα Κωδικοποίησης	
1.3.1 Ασύρματο Δίκτυο εξοικονόμησης	
1.3.2 Δίκτυο πεταλούδα (The butterfly network example)	
1.3.3 Multicasting (Πολυδιανομή)	
1.3.4 Ασφάλειες δεδομένων με κωδικοποίηση δικτύου	
<b>2. Η Τυχαία κωδικοποίηση δικτύου (Random Network Coding).....</b>	<b>9</b>
2.1 Πώς δουλεύει η Random Linear Network Coding (RLNC)	
2.2 Χρησιμοποιώντας Matlab για RNCL	
2.3 Σύγκριση: θεωρία – εφαρμογή	
<b>3.Τριγωνική κωδικοποίηση δικτύου (Triangular network coding).....</b>	<b>15</b>
<b>4.Το πλαίσιο των Δυνατοτήτων και των Ορίων της Τεχνικής Κωδικοποίησης.....</b>	<b>17</b>
4.1 Πλεονεκτήματα της τεχνικής Network Coding	
4.2 Μειονεκτήματα της τεχνικής Network Coding	
<b>5. Εφαρμογές Κωδικοποίησης Δικτύου.....</b>	<b>19</b>
5.1 Διανομή Ψηφιακού Περιεχομένου σε P2P	
5.1.1 Χρησιμοποιώντας Random Network Coding	
5.1.2 Περιορισμοί στην πρακτική εφαρμογή της Κωδικοποίησης Δικτύου	
5.1.3 Αξιοπιστία σε P2P	
5.1.4 Η Πρακτική Βελτίωση που προσφέρει η Κωδικοποίηση Δικτύου πάνω στην μελέτη μιας προσομοίωσης	
5.2 Εφαρμογή σε ασύρματη διάδοση και Multi- channel ασύρματη διάδοση	
5.2.1 Multi-channel multi-interface wireless mesh networks	
5.3 Η χρησιμότητα της κωδικοποίησης δικτύου σε δίκτυα Wimax	
5.4 Τεχνικές μετάδοσης VoIP με κωδικοποίηση δικτύου σε Ασύρματα Δίκτυα Πολλών Αλμάτων	
5.4.1 Τα βασικά χαρακτηριστικά της κωδικοποίησης δικτύου καθώς και το πως αυτή εφαρμόζεται στην πράξη στα ασύρματα δίκτυα	
5.4.2 Ενσωμάτωση της κωδικοποίησης δικτύου στη μετάδοση VoIP	
<b>Συμπεράσματα Κωδικοποίησης δικτύου στο Μέλλον.....</b>	<b>38</b>
<b>Βιβλιογραφική Αναφορά.....</b>	<b>39</b>

## Εισαγωγή

Η κωδικοποίηση δικτύου είναι νέα τεχνική που προτάθηκε το 2000 για τις δορυφορικές επικοινωνίες με στόχο τη βελτίωση της ρυθμαπόδοσης. Η καινοτομία της τεχνικής αυτής έγκειται στο ότι οι ενδιάμεσοι κόμβοι του δικτύου δεν προωθούν απλώς τα μηνύματα, αλλά έχουν τη δυνατότητα να τα επεξεργαστούν και να μεταδίδουν κατάλληλο συνδυασμό τους. Για παράδειγμα, στο στρώμα δικτύου οι ενδιάμεσοι κόμβοι μπορούν να εκτελούν δυαδική πρόσθεση των ανεξάρτητων ροών, ενώ στο φυσικό στρώμα ενός δικτύου οπτικών ινών μπορούν να υπερθέτουν τα εισερχόμενα οπτικά μηνύματα. Οι σχέσεις ανταλλαγής που προκύπτουν από την εισαγωγή της κωδικοποίησης δικτύου σε ένα σχήμα δρομολόγησης είναι μεταξύ πολυπλοκότητας, καθυστέρησης, πλεονασμού δεδομένων (overhead) και αριθμού απαιτούμενων μεταδόσεων για την παράδοση του μηνύματος.

### Ορισμός :

Κωδικοποίηση δικτύου είναι μια τεχνική δικτύωσης στην οποία διαβιβάζονται τα δεδομένα, κωδικοποιούνται και αποκωδικοποιούνται με σκοπό την αύξηση της ρυθμαπόδοσης (throughput), για την μείωση καθυστερήσεων και για την ισχυρή αποκατάσταση του δικτύου. Στην κωδικοποίηση δικτύου, εφαρμόζονται οι αλγεβρικοί αλγόριθμοι στα δεδομένα ώστε να συσσωρεύονται οι μεταδόσεις τους. Οι λαμβανόμενες μεταδόσεις αποκωδικοποιούνται στον προορισμό τους. Αυτό σημαίνει ότι απαιτούνται λιγότερες μεταδόσεις για να διαβιβαστούν όλα τα δεδομένα, αλλά αυτό απαιτεί περισσότερη επεξεργασία σε ενδιάμεσους και τερματικούς κόμβους.

Η κωδικοποίηση δικτύου «οφείλει» να μειώσει σημαντικά τον μεταδιδόμενο όγκο φορτίου χωρίς αντίστοιχη μείωση της μεταδιδόμενης πληροφορίας σε ένα δίκτυο. Ένα παράδειγμα αποτελεί όταν ένας κόμβος στέλνει ένα πακέτο πληροφορίας σε πολλούς κόμβους ταυτόχρονα.

### Ορολογίες:

#### ➤ Δρομολόγηση

Οι ροές αποστέλλονται χωρίς κωδικοποίηση από τις πηγές στους παραλήπτες και οι ενδιάμεσοι κόμβοι απλά προωθούν τις εισερχόμενες ροές πληροφορίας.

#### ➤ Κωδικοποίηση

Επιτρέπεται στους ενδιάμεσους κόμβους του δικτύου να εκτελούν πράξεις κωδικοποίησης αντί απλώς να προωθούν τα μηνύματα.

Μέρος της εργασίας μας είναι να μελετήσουμε διαφορετικές και αποδοτικές τεχνικές πάνω σε Network Coding, ώστε να εφαρμοστούν σε μελλοντικά δίκτυα (εάν μπορούν να εφαρμοστούν) στα οποία αναμένεται αύξηση του αριθμού των χρηστών και των απαιτήσεων τους σε ποιότητα εξυπηρέτησης και μεταφοράς δεδομένων.

Με την εφαρμογή της κωδικοποίησης δικτύου επιτρέπεται στους ενδιάμεσους κόμβους του δικτύου να εκτελούν πράξεις κωδικοποίησης αντί να προωθούν τα αρχικά μηνύματα (packets). Οι κυρίως μέθοδοι κωδικοποίησης δικτύου είναι :

- Γραμμική Κωδικοποίηση, όπου οι ενδιάμεσοι κόμβοι απαιτούνται να εκτελέσουν γραμμικές πράξεις μεταξύ των μηνυμάτων ή πακετών.
- Μη - Γραμμική Κωδικοποίηση , όπου οι ενδιάμεσοι κόμβοι επιτρέπεται να συνδυάσουν τα μηνύματα χρησιμοποιώντας οποιαδήποτε πράξη.

Σε αυτήν την ενότητα, ασχολούμαστε με την γραμμική κωδικοποίηση.

## 1. Γραμμική κωδικοποίηση δικτύου (Linear network coding)

Linear network coding, είναι μια τεχνική που μπορεί να χρησιμοποιηθεί για τη βελτίωση της απόδοσης ενός δικτύου, την ρυθμαπόδοση (throughput), την επεκτασιμότητα, καθώς και την ανθεκτικότητα στις επιθέσεις και τις υποκλοπές. Η απλή μετάδοση των πακέτων πληροφοριών που λαμβάνονται από τους κόμβους, αντικαθίσταται με τον συνδυασμό αυτών των πακέτων ως ένα ενιαίο πακέτο για αποστολή. Αυτό μπορεί να χρησιμοποιηθεί για να επιτευχθεί η μέγιστη δυνατή ροή πληροφοριών σε ένα δίκτυο.

### 1.1. Διαδικασία κωδικοποίησης (Encoding)

Θεωρούμε έναν αριθμό αρχικών πακέτων  $M_1, \dots, M_n$  τα οποία παράγονται από έναν ή περισσότερους κόμβους. Καθένα από τα πακέτα σχετίζονται με μία ακολουθία συντελεστών  $g_1, \dots, g_n$  το οποίο συμβολίζουμε με  $g$  και το οποίο ονομάζεται encoding vector. Ο συνδυασμός των  $g_i$  με τα πακέτα  $M_i$  μας δίνει το διάνυσμα  $X$  που αποτελεί τα κωδικοποιημένα δεδομένα (information vector). Το διάνυσμα  $X$  προκύπτει από την σχέση:

$$X = \sum_{i=1}^n g_i \cdot M^i$$

Το διάνυσμα  $g$  χρησιμοποιείται από τους κόμβους για τη διαδικασία της αποκωδικοποίησης (decoding). Τα πακέτα που συνδυάζονται με τον παραπάνω τρόπο πρέπει να έχουν το ίδιο μήκος. Πακέτα με μικρότερο μήκος συμπληρώνονται με μηδενικά (padding 0s). Από τον παραπάνω τύπο προκύπτει ότι όταν συνδυάσουμε πακέτα μήκους  $L$  bits το καθένα θα προκύψουν πακέτα μήκους  $L$  και πάλι. Δηλαδή με το encoding δεν κάνουμε απλά συνένωση των πακέτων. Έτσι, κάθε πακέτο που προκύπτει περιέχει ουσιαστικά ένα τμήμα της πληροφορίας που περιέχουν τα αρχικά πακέτα. Το  $k$ -οστό στοιχείο του διανύσματος  $X$  δίνεται από τον τύπο:

$$X_k = \sum_{i=1}^n g_i M_i^k$$

(π.χ. αν τα πακέτα των 8bit  $M_1=10101110$  και  $M_2 = 11010101$ , και  $g_1=g_2=1$ , τότε  $X=M_1 \oplus M_2 = 01111011$  (8bit). )

Δηλ. το  $X_k$  είναι το διαμορφωμένο πακέτο που σχηματίστηκε από τα αρχικά  $M$  πακέτα, πολλαπλασιαζόμενα από συντελεστές  $g_i$  οι οποίοι επιλέγονται από ένα πεπερασμένο σύνολο (finite field) Galois field  $GF(2^S)$ .

Galois:

Στην άλγεβρα, ένα πεπερασμένο πεδίο ή πεδίο Galois (που ονομάστηκε έτσι προς τιμήν του Εβαρίστ Galois) είναι ένα πεδίο που περιέχει έναν πεπερασμένο αριθμό στοιχείων. (Παράδειγμα όταν ορίζουμε, το  $GF(2)$  (που αλλιώς καλείται  $F_2$ ,  $Z/2Z$  ή  $Z_2$ ) είναι το πεδίο Galois με δύο στοιχεία, δηλ αποτελεί υποσύνολο του χώρου (πεδίο) Galois

#### 1.1.1 Επανακωδικοποίηση(Recoding)

Η Επανακωδικοποίηση εκτελείται σε κόμβους αναμετάδοσης του δικτύου και είναι παρόμοια με την διαδικασία της κωδικοποίησης. Ωστόσο, είναι πιο πολύπλοκη σε σύγκριση με την κωδικοποίηση, επειδή τα πακέτα είναι ήδη κωδικοποιημένα και οι νέοι συντελεστές πρέπει να αποτελούν γραμμικό συνδυασμό με τους παλιούς συντελεστές.

## 1.2. Διαδικασία αποκωδικοποίησης (Decoding)

Έστω ότι ένας κόμβος λαμβάνει ένα σύνολο πακέτων της μορφής  $(g_1X_1), \dots, (g_mX_m)$ . Για να ανακτήσει τα αρχικά πακέτα θα πρέπει να επιλύσει το γραμμικό σύστημα:

$$X^j = \sum_{i=1}^n g_i^j M^i$$

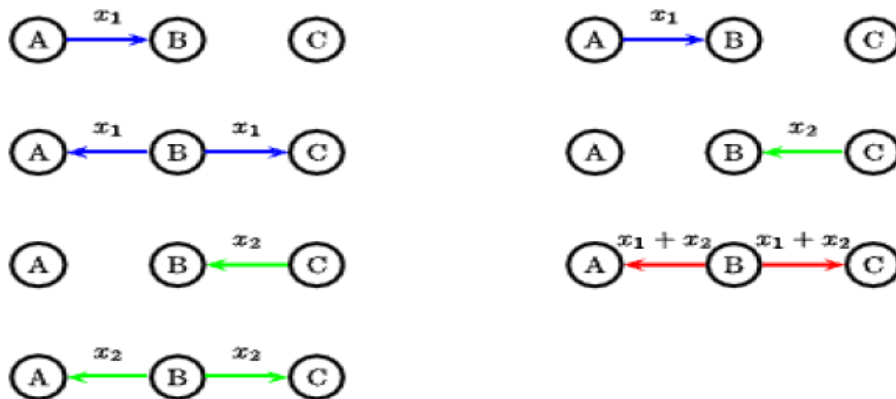
Όπου οι άγνωστοι είναι τα  $M_i$

Το παραπάνω σύστημα έχει  $m$  εξισώσεις με  $n$  αγνώστους. Για να είναι σε θέση ο κόμβος να ανακτήσει όλη τη πληροφορία που περιείχαν τα αρχικά πακέτα, θα πρέπει το  $m$  να είναι μεγαλύτερο ή ίσο του  $n$  ( $m \geq n$ ). Αυτό πρακτικά σημαίνει ότι ο αριθμός των ληφθέντων πακέτων θα πρέπει να είναι τουλάχιστον ίσος με τον αριθμό των αρχικών πακέτων.

## 1.3. Παραδείγματα Κωδικοποίησης

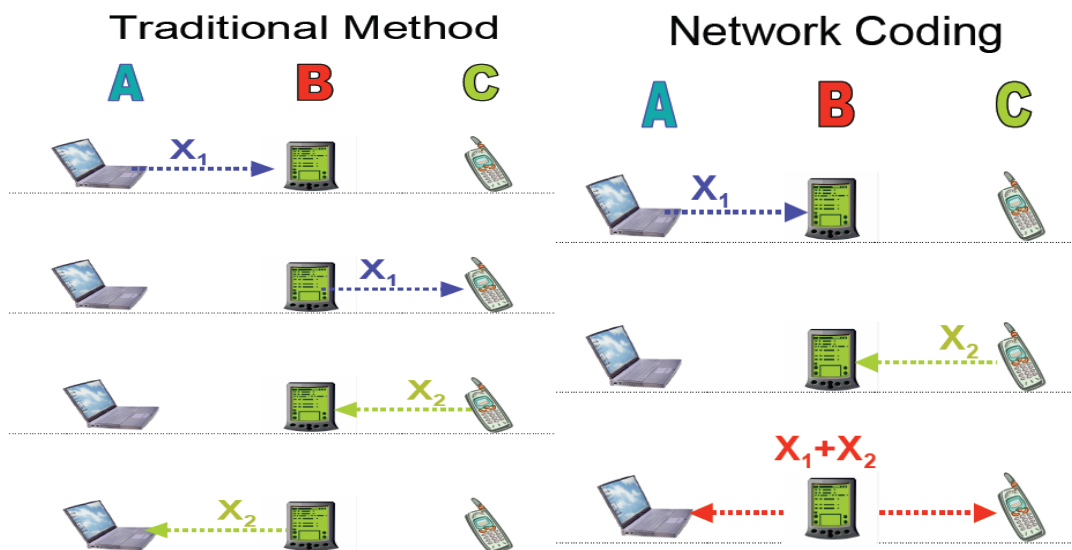
Λόγω της γενικότητας της τεχνικής αυτής και ενός φάσματος εφαρμογών της, η κωδικοποίηση δικτύου έχει προκαλέσει ιδιαίτερο ερευνητικό ενδιαφέρον στους τομείς της θεωρίας πληροφορίας και κωδικοποίησης, της δικτύωσης, των μεταγωγών, των ασύρματων επικοινωνιών, της θεωρίας πολυπλοκότητας, της κρυπτογραφίας και της θεωρίας πινάκων. Στα σχήματα που ακολουθούν παρουσιάζονται παραδείγματα των δυνατοτήτων αυτών. Να σημειωθεί ότι τα δίκτυα παρουσιάζονται ως κατευθυνόμενοι γράφοι όπου οι κορυφές αντιστοιχούν στα τερματικά (κόμβοι) και οι ακμές στις ζεύξεις μεταξύ των κόμβων.

### 1.3.1 Ασύρματο Δίκτυο εξοικονόμησης

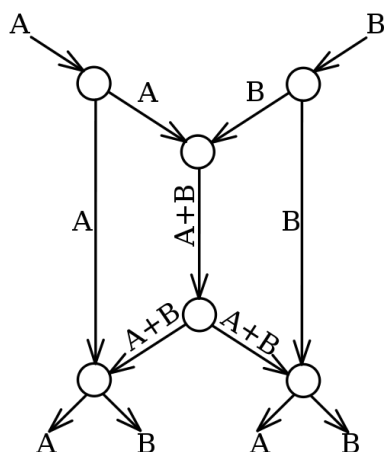


Σχήμα : Παράδειγμα εξοικονόμησης ασύρματων πόρων με εφαρμογή της κωδικοποίησης δικτύου

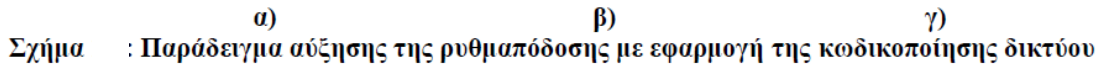
Στο δίκτυο του παραπάνω Σχήματος ο κόμβος A πρόκειται να στείλει το δυαδικό αρχείο  $x_1$  στον C και ο C το  $x_2$  στον A. Ο αναμεταδότης B δέχεται και τα δύο αρχεία. Χωρίς κωδικοποίηση δικτύου ο B μεταδίδει το  $x_1$  στον A και το  $x_2$  στον C. Υποθέτοντας ότι ο χρόνος διαιρείται σε σχισμές και ότι ένα τερματικό μπορεί να μεταδώσει ή να λάβει ένα αρχείο κατά τη διάρκεια μιας χρονικής σχισμής, για τη μετάδοση των δύο αρχείων απαιτούνται τέσσερις χρονικές σχισμές. Η κωδικοποίηση δικτύου εκμεταλλεύεται τη δυνατότητα ευρυεκπομπής των ασύρματων επικοινωνιών. Με χρήση κωδικοποίησης δικτύου ο B εκπέμπει το συνδυασμό  $x_1 + x_2$  των αρχείων οπότε απαιτούνται τρεις χρονικές σχισμές για τη μετάδοσή τους. Είναι φανερό ότι η κωδικοποίηση δικτύου επιτυγχάνει μείωση της καθυστέρησης, του χρόνου χρησιμοποίησης του ασύρματου διαύλου και των παρεμβολών, και εξοικονόμηση ενέργειας.



### 1.3.2 Δίκτυο πεταλούδα (The butterfly network example)



Το δίκτυο πεταλούδα χρησιμοποιείται συχνά για να γίνει κατανοητό πώς η γραμμική κωδικοποίηση του δικτύου μπορεί να ξεπεράσει τη δρομολόγηση. Δύο κόμβοι πηγής (στο επάνω μέρος της εικόνας) διαθέτουν πληροφορίες A και B και πρέπει να τις μεταδώσουν στους δύο κόμβους προορισμού (στο κάτω μέρος), όπου ο καθένας κόμβος προορισμού θέλει να γνωρίζει τόσο την πληροφορία A όσο και τη B. Κάθε ακμή μπορεί να μεταφέρει μόνο μία τιμή (μία άκρη μεταδίδει ένα bit ανά πεδίο του χρόνου). Εάν είχαμε μόνο τη δρομολόγηση σαν δυνατότητα μετάδοσης των A και B, τότε ο κεντρικός σύνδεσμος θα μπορούσε να μεταφέρει ή μόνο το A ή μόνο το B, αλλά όχι και τα δύο ταυτόχρονα. Εάν υποθέσουμε ότι στέλνεται μόνο το A μέσω του κεντρικού συνδέσμου. Στη συνέχεια ο αριστερός προορισμός θα λάβει το A δύο φορές ενώ το B καμία φορά. Ομοίως αν υποθέσουμε ότι στέλνεται μόνο το B μέσω του κεντρικού συνδέσμου. Τότε λέμε ότι η δρομολόγηση είναι ανεπαρκής, διότι δεν υπάρχει σύστημα δρομολόγησης το οποίο μπορεί να μεταδώσει το A και το B ταυτόχρονα προς τους δύο προορισμούς.

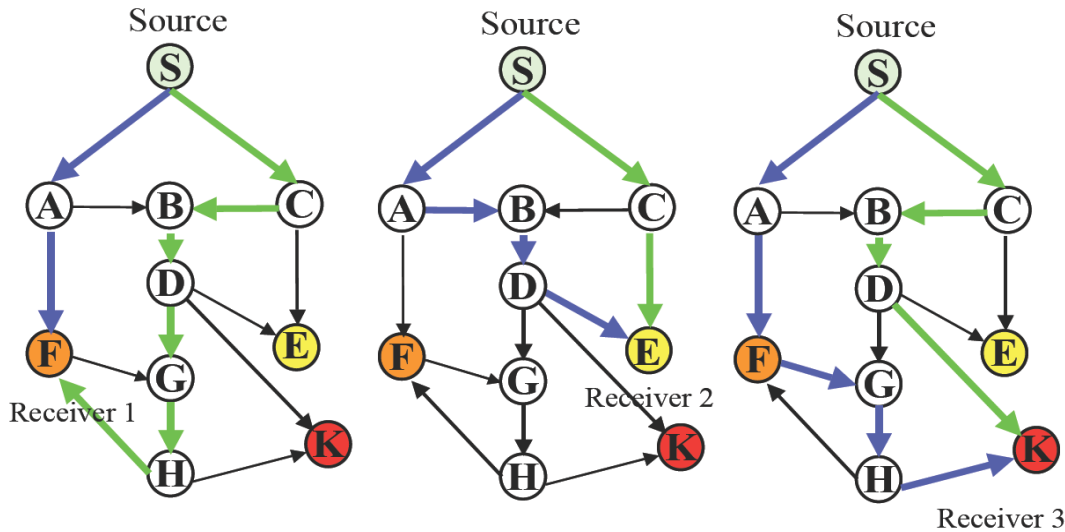


Με λίγα λόγια, χωρίς κωδικοποίηση δικτύου όταν τα πακέτα x1 και x2 φτάνουν ταυτόχρονα στον κόμβο C, ο κόμβος C θα πρέπει να αποφασίσει πιο από τα δύο πακέτα θα προωθήσει πρώτο στην τρέχουσα δρομολόγηση. Με την κωδικοποίηση του δικτύου καταφέρνουμε να προωθήσουμε και τα δύο πακέτα.



### 1.3.3 Multicasting (Πολυδιανομή)

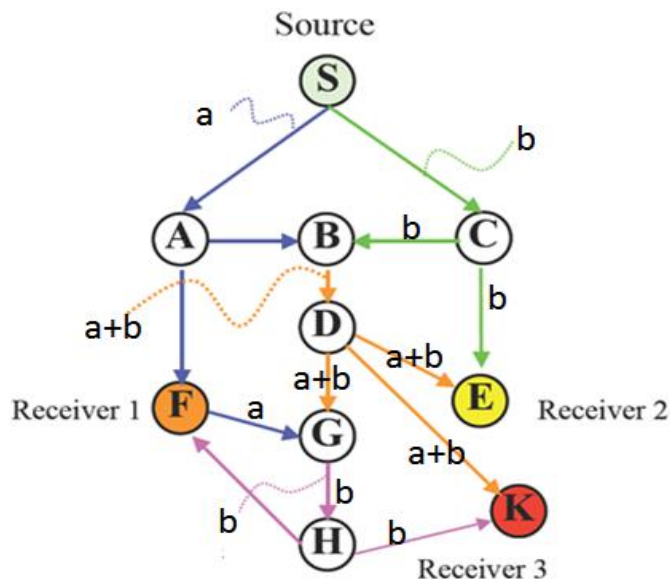
Θεωρούμε ένα δίκτυο, όπου η πηγή S θέλει κάνει Multicast σε τρεις δέκτες E, F και K. Ο ελάχιστος αριθμός κόμβων που μεσολαβούν μεταξύ S και κάθε δέκτης είναι 2. Οι πράσινες διαδρομές δεν μοιράζονται άκρα (Edges) με τις μπλε διαδρομές. Υποθέτουμε πως η δρομολόγηση έχει καθοριστεί σύμφωνα με τις κατευθύνσεις των βελών.



Για να βελτιστοποιήσουμε το multicasting χωρίς κωδικοποίηση δικτύου, πρέπει να λυθεί το πρόβλημα του Steiner tree όπου βρίσκει τις συντομότερες διασυνδέσεις μεταξύ των κόμβων. Αυτό ως γνωστό είναι δύσκολο και η λύση είναι προσεγγιστική. Ακόμη κι αν θα μπορούσαμε να λύσουμε αυτό, θα καταλήξουμε σε μια λύση η οποία είναι χειρότερη σε σύγκριση με την λύση όπου χρησιμοποιείται κωδικοποίηση δικτύου.

Πράγματι, στο παραπάνω παράδειγμα, όπως φαίνεται από την τοπολογία η καλύτερη δρομολόγηση των πακέτων ανάμεσα στους κόμβους δεν είναι σταθερή, δηλ. όταν υπάρχει μεταβίβαση πακέτων μεταξύ SF, SE και SK. Αυτό συμβαίνει διότι, τα πακέτα χρησιμοποιούν κοινούς κόμβους - πόρους, και για να προωθηθούν πρέπει να περιμένουν την προώθηση των πακέτων που προηγούνται.

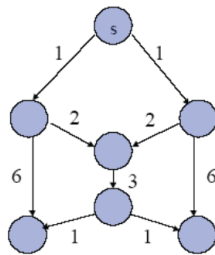
Η βέλτιστη σταθερότητα στις διασυνδέσεις (Steiner tree) επιτυγχάνεται μόνο όταν γίνεται χρήση κωδικοποίησης, διότι τα πακέτα προωθούνται ενιαία χωρίς να χρειάζεται να μεταβάλλουν την δρομολόγηση τους, δηλ. έχουν σταθερή διαδρομή χωρίς το ίδιο πακέτο να δεσμεύει κοινούς κόμβους με ένα άλλο διαφορετικό πακέτο (πχ μια υπόθεση που κάνουμε, οι διαδρομές μπλε και πράσινο δεν πρέπει να επικαλύπτονται).





Με την εφαρμογή κωδικοποίησης σε πολυδινομικό δίκτυο, ελαττώνεται το κόστος της δρομολόγησης των πακέτων. Για παράδειγμα, παρακάτω φαίνεται το κόστος για την αποστολή του κάθε πακέτου από S στον προορισμό του, με και χωρίς κωδικοποίηση.

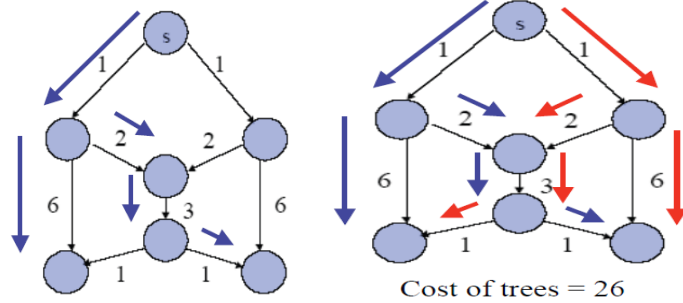
Κόστος από κόμβο σε κόμβο



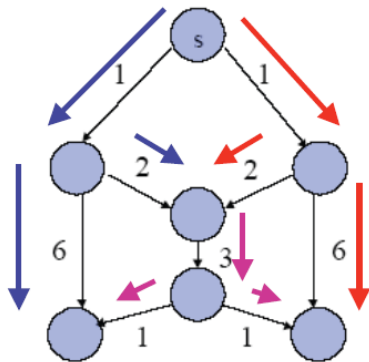
Κόστος χωρίς κωδικοποίηση ενός πακέτου

Μπλε :  $(1+6)+(2+3+1) = 13$

Κόκκινη :  $(1+6)+(2+3+1) = 13$

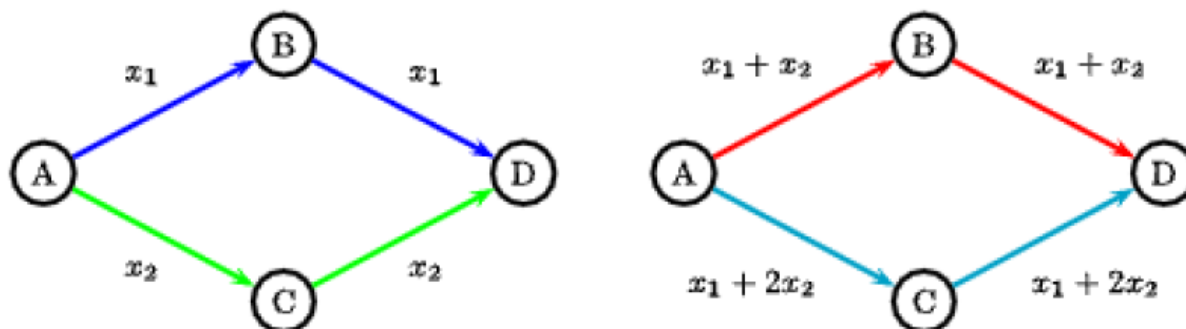


Κόστος με κωδικοποίηση δικτύου ενός πακέτου



Cost of network coding = 23

#### 1.3.4 Ασφάλειας δεδομένων με κωδικοποίηση δικτύου



**Σχήμα :** Παράδειγμα αποφυγής υποκλοπών με εφαρμογή της κωδικοποίησης δικτύου

Στο δίκτυο του παραπάνω Σχήματος παρουσιάζεται η περίπτωση που ο κόμβος A πρόκειται να στείλει δύο δυαδικά ψηφία στον κόμβο D. Υποθέτοντας ότι κάποιος με στόχο την υποκλοπή των αρχείων έχει πρόσβαση μόνο στη μία από τις δύο δυνατές διαδρομές από τον A στον D, ο A μπορεί να στείλει ένα διαφορετικό γραμμικό συνδυασμό των ψηφίων μέσω των δύο διαδρομών. Με αυτόν τον τρόπο κάποιος που έχει στόχο την υποκλοπή των ψηφίων έχει πιθανότητα 50% να υποκλέψει ένα από τα δύο ψηφία.

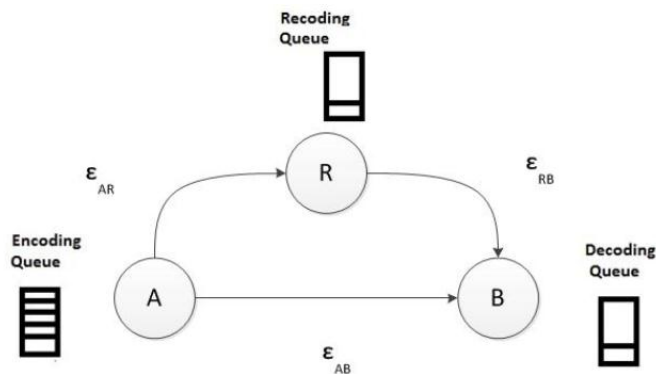
## 2. Η Τυχαία κωδικοποίηση δικτύου (Random Network Coding)

Η Τυχαία κωδικοποίηση δικτύου είναι ένα απλό αλλά ισχυρό σύστημα κωδικοποίησης, το οποίο σε συστήματα μετάδοσης επιτρέπει σχεδόν βέλτιστη απόδοση χρησιμοποιώντας έναν αποκεντρωτικό αλγόριθμο. Με λίγα λόγια η τυχαία γραμμική κωδικοποίηση δικτύου λειτουργεί ακριβώς όπως και η γραμμική κωδικοποίηση με την εξής διαφορά: οι κόμβοι μεταδίδουν τυχαίους γραμμικούς συνδυασμούς των πακέτων που λαμβάνουν, με συντελεστές που επιλέγονται από ένα πεπερασμένο πεδίο *Galois*. Ο σκοπός χρήσης ενός τέτοιου πεδίου είναι ο δέκτης (προορισμός του πακέτου) να αποκτήσει γραμμικά ανεξάρτητους συνδυασμούς πακέτων (και κατά συνέπεια περιλαμβάνει καινοτόμες πληροφορίες), με αποτέλεσμα η γραμμική ανεξαρτησία των λαμβανόμενων πακέτων να τείνει στην πιθανότητα 1.

Θα πρέπει ωστόσο να επισημανθεί ότι, αν και η τυχαία κωδικοποίηση δικτύου έχει εξαιρετική απόδοση όσον αφορά το throughput, αν ένας δέκτης δέχεται ανεπαρκή αριθμό πακέτων, είναι εξαιρετικά απίθανο να μπορεί να ανακτήσει κάποιο από τα αρχικά πακέτα. Αυτό μπορεί να αντιμετωπιστεί στέλνοντας επιπλέον τυχαίους γραμμικούς συνδυασμούς μέχρι ο δέκτης να αποκτήσει τον κατάλληλο αριθμό πακέτων.

### 2.1 Πώς δουλεύει η Random Linear Network Coding (RLNC)

RLNC in the project scenario:



- Η Alice (κόμβος A) παράγει διάφορα πακέτα
- Παραμένουν στον buffer μέχρι μια γενιά (ένας αριθμός από πακέτων) να συλλέγει στην ουρά
- Μόλις συλλέγεται η γενιά όλα αυτά τα πακέτα κωδικοποιούνται σε ένα πακέτο με το ίδιο μέγεθος χρησιμοποιώντας γραμμικούς συντελεστές που ανήκουν στο πεπερασμένο πεδίο *Galois*.
- Αυτό το πακέτο προωθείται
- Ο κόμβος αναμετάδοσης R λαμβάνει τα πακέτα, τα επανακωδικοποιεί αν χρειάζεται και τα προωθεί διατηρώντας, με τον τρόπο αυτό, τις πληροφορίες που μεταδίδονται στο δίκτυο. Εάν υπάρχουν πάρα πολλοί κόμβοι που μεσολαβούν η πιθανότητα λήψης των πακέτων αυξάνεται.
- Όταν ο Bob λαμβάνει κάποια πακέτα, απορρίπτει όσα επαναλαμβάνονται ή τα καταστραφεί και αρχίζει την αποκωδικοποίηση.

Διαδικασία Κωδικοποίησης (Encoding)

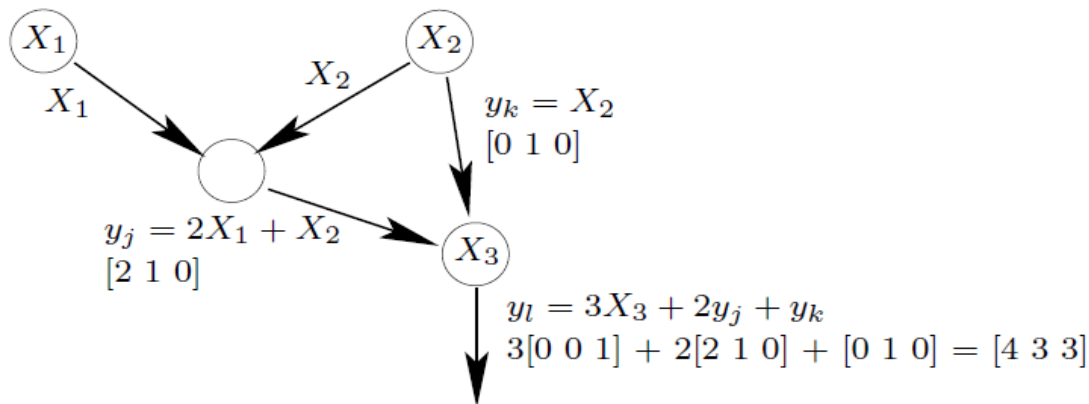
$$X_k = \sum_{i=1}^n g_i M_i^k$$

Όπου:

$X_k$ , η κωδικοποιημένη πληροφορία στον  $k$  κόμβο του δικτύου

$M_i^k$  αρχικά πακέτα  $M_1, \dots, M_n$  στον  $k$  κόμβο του δικτύου

$g_i$ , συντελεστές οι οποίοι επιλέγονται από ένα πεπερασμένο σύνολο (*finite field*) *Galois Field GF*



Διαδικασία Αποκωδικοποίησης (Decoding)

$$X^m = \sum_{i=1}^n g_i^j M^i$$

Όπου:

$X^m$ , διάνυσμα με  $m$  εξισώσεις και  $n$  αγνώστους

$n$ , είναι τα πακέτα που θέλουμε να βρούμε (αποκωδικοποιήσουμε)

Για να είναι σε θέση ο κόμβος να ανακτήσει όλη τη πληροφορία που περιείχαν τα αρχικά πακέτα, θα πρέπει το  $m$  να είναι μεγαλύτερο ή ίσο του  $n$  ( $m \geq n$ ). Αυτό πρακτικά σημαίνει ότι ο αριθμός των ληφθέντων πακέτων θα πρέπει να είναι τουλάχιστον ίσος με τον αριθμό των αρχικών πακέτων.

Η αποκωδικοποίηση επιτυγχάνεται με την μέθοδο απαλοιφής Gauss ή Gauss k Jordan

## 2.2 Χρησιμοποιώντας Matlab για RNCL

- Η Τυχαία κωδικοποίηση δικτύου είναι ένα απλό αλλά ισχυρό σύστημα κωδικοποίησης, το οποίο σε συστήματα μετάδοσης επιτρέπει σχεδόν βέλτιστη απόδοση.
- Λειτουργεί ακριβώς όπως και η γραμμική κωδικοποίηση με την εξής διαφορά: οι κόμβοι μεταδίδουν γραμμικούς συνδυασμούς των πακέτων που λαμβάνουν, με τυχαίους συντελεστές που επιλέγονται από ένα πεπερασμένο πεδίο *Galois*.
- Για να μπορεί ένα γραμμικό σύστημα με  $m$  εξισώσεις να λυθεί, δηλ. να αποκωδικοποιηθεί, πρέπει οι μεταβλητές του συστήματος να είναι ανεξάρτητες .
- π.χ. όταν ένας κόμβος δέχεται το παρακάτω γραμμικό σύστημα να λύσει:

$$\begin{aligned} 1x_1 + 7x_2 - 2x_3 \\ 4x_1 + 10x_2 + 1x_3 \\ 2x_1 - 4x_2 + 5x_3 \\ -3x_1 - 1x_3 - 4x_3 \end{aligned}$$

Μετά την απαλοιφή Gauss θα οδηγηθεί να φτάσει στο σημείο :

$x_1 = -3/2 x_3$ ,  $x_2 = 1/2 x_3$ , όπου  $x_3$  είναι αυθαίρετο.

Αυτό σημαίνει πως τα πακέτα εξαρτώνται μεταξύ τους και εάν το πακέτο  $x_3$  μπορεί να είναι οτιδήποτε τότε δεν μπορούμε να βρούμε τα πακέτα  $x_1, x_2$  και  $x_3$ .

- Π.χ. Ενώ όταν ένας κόμβος δέχεται το παρακάτω γραμμικό σύστημα να λύσει:

$$2x_1 + x_2 - x_3 = 8$$

$$-3x_1 - x_2 + 2x_3 = -11$$

$$-2x_1 + x_2 + 2x_3 = -3$$

Με την απαλοιφή Gauss ο πίνακας

θα έρθει στην μορφή:

$$2x_1 + x_2 - x_3 = 8$$

$$1/2x_2 + 1/2x_3 = 1$$

$$-x_3 = 1$$

Με οπισθοδρόμηση βρίσκουμε τα πακέτα:

$$x_3 = -1, x_2 = 3, x_1 = 2$$

Με την βοήθεια της matlab περνώντας τους συντελεστές του συστήματος σε έναν πίνακα, η συνάρτηση Gauss που δημιουργήσαμε περνάει τον πίνακα και τον απλοποιεί χρησιμοποιώντας την μέθοδο απαλοιφή Gauss.

```
>> C=[2 1 -1 8;-3 -1 2 -11;-2 1 2 -3]
```

```
C =
```

```

2     1    -1     8
-3    -1     2   -11
-2     1     2    -3
```

```
>> [a,xtrans] = Gauss(C)
```

```
a =
```

```

2.0000    1.0000   -1.0000    8.0000
0         0.5000    0.5000    1.0000
0         0       -1.0000    1.0000
```

```
xtrans =
```

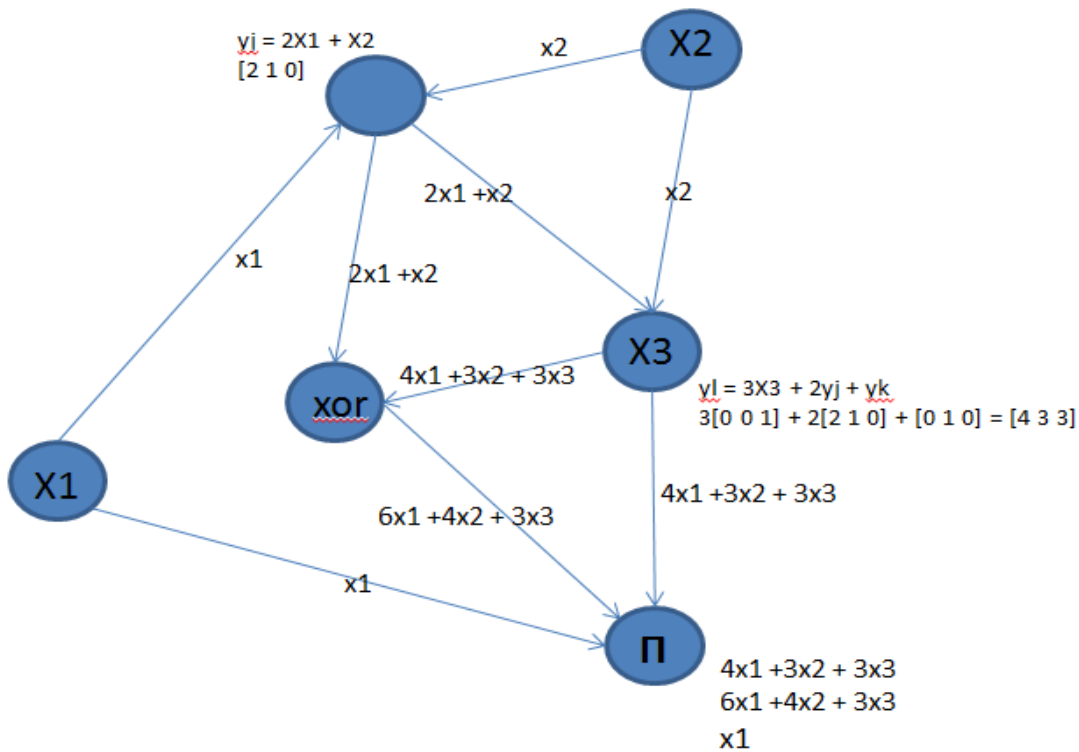
```

2
3
-1
```

Παρατηρούμε πως ο απλοποιημένος πίνακας είναι άνω τριγωνικός, άρα το σύστημα έχει λύσεις το διάνυσμα xtrans που φαίνεται ( $x_3 = -1, x_2 = 3, x_1 = 2$ )

- Όπως είδαμε, η ύπαρξη γραμμικής ανεξαρτησίας είναι σημαντική για την αποκωδικοποίηση δεδομένων. Όσες γραμμικές καινούργιες ανεξάρτητες εξισώσεις έρχονται για αποκωδικοποίηση, τόσο περισσότερη καινούργια πληροφορία έχουμε.
- Η τυχαία γραμμική κωδικοποίηση έχει δείξει πειραματικά και θεωρητικά πως, η γραμμική ανεξαρτησία των λαμβανόμενων πακέτων από τους κόμβους τείνει στην πιθανότητα 1.
- Για αυτόν τον λόγο, το RLNC αποτελεί ισχυρή τεχνική στον τομέα της κωδικοποίησης δικτύου και βρίσκει πληθώρα εφαρμογές στην χρήση του, παράδειγμα σε προσομοιώσεις και σε εφαρμογές πειραματικών δικτύων.

- Εδώ παρατηρούμε μια επιτυχής αποκωδικοποίηση στον κόμβο Π χρησιμοποιώντας απαλοιφή Gauss μέσω δοκιμών με matlab.



```
>> B = [4 3 3 0;6 4 3 0;1 0 0 0]
```

```
B =
```

```

4      3      3      0
6      4      3      0
1      0      0      0
```

```
>> [a,xtrans] = Gauss(B)
```

```
a =
```

```

4.0000    3.0000    3.0000         0
0    -0.5000   -1.5000         0
0         0     1.5000         0
```

```
xtrans =
```

```

0
0
0
```

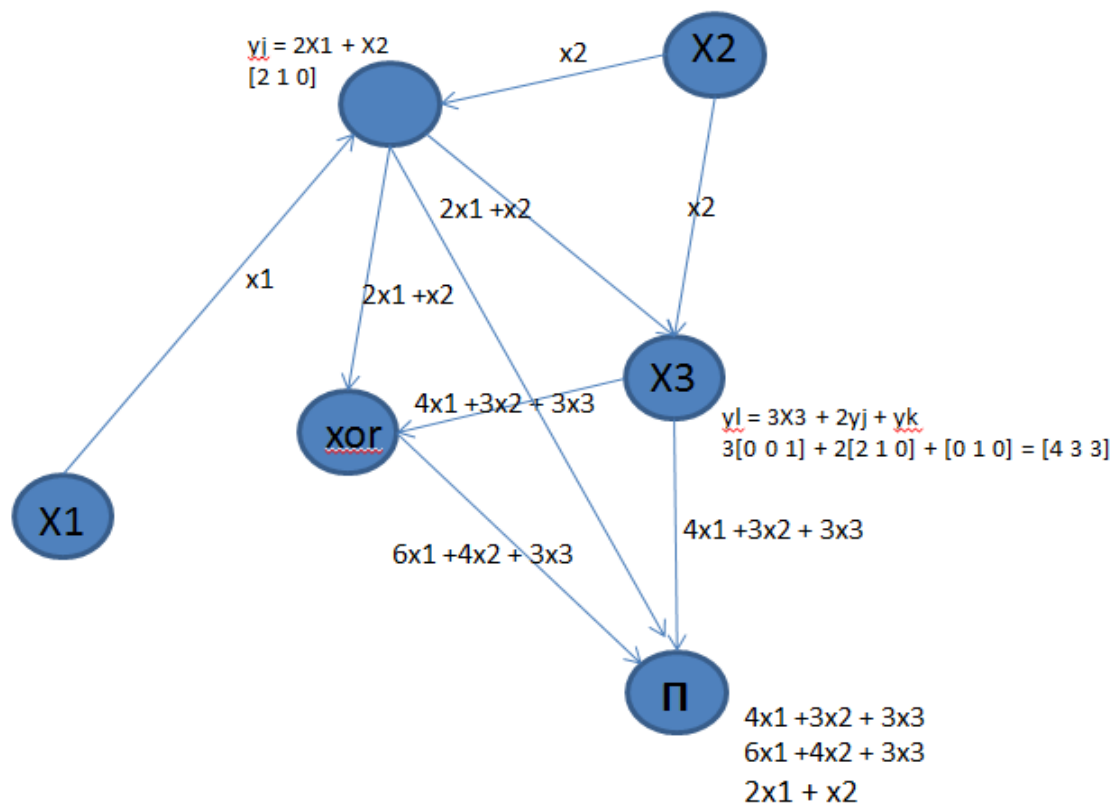
Παρατηρούμε πως ο απλοποιημένος πίνακας είναι άνω τριγωνικός , άρα το σύστημα έχει λύσεις. Δηλαδή τα πακέτα μεταξύ τους είναι γραμμικά ανεξάρτητα, διότι το διάνυσμα xtrans επέστρεψε μηδενικά όταν εξετάσαμε το παρακάτω σύστημα:

$$4x_1 + 3x_2 + 3x_3 = 0$$

$$6x_1 + 4x_2 + 3x_3 = 0$$

$$x_1 = 0$$

- Εδώ παρατηρούμε μια μη επιτυχής κωδικοποίηση στον κόμβο Π χρησιμοποιώντας απαλοιφή Gauss μέσω δοκιμών με matlab



```
>> B = [4 3 3 0;6 4 3 0;2 1 0 0]
```

```
B =
```

```

4      3      3      0
6      4      3      0
2      1      0      0

```

```
>> [a,xtrans] = Gauss(B)
```

```
a =
```

```

4.0000    3.0000    3.0000    0
0        -0.5000   -1.5000    0
0         0         0         0

```

```
xtrans =
```

```

NaN
NaN
NaN

```

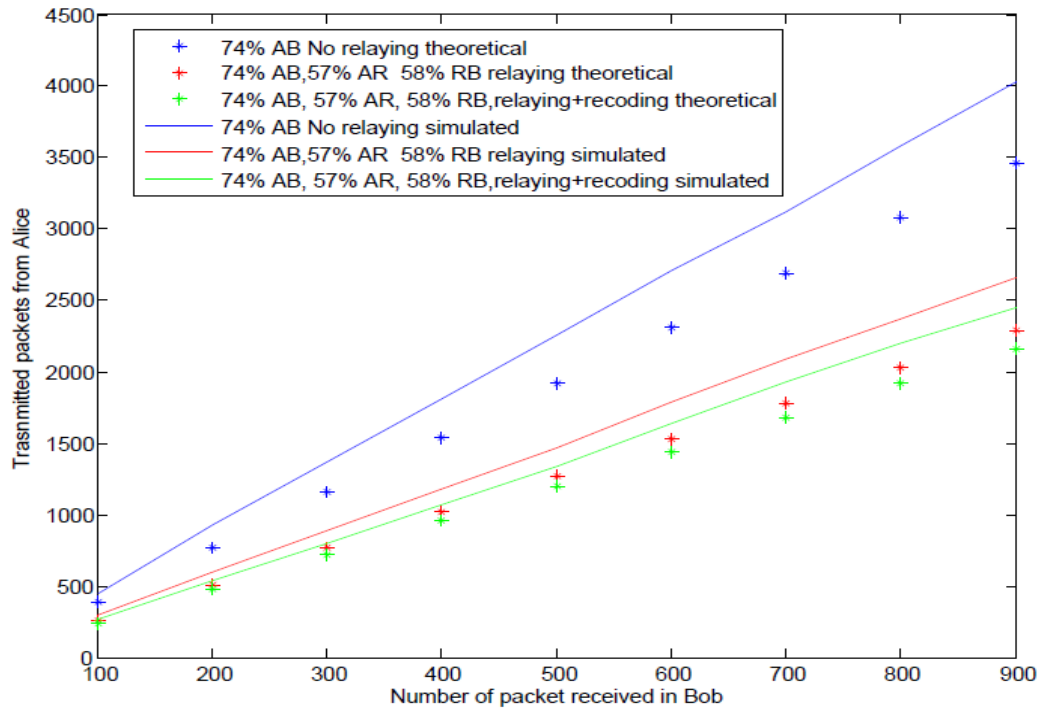
Παρατηρούμε πως ο απλοποιημένος πίνακας δεν είναι άνω τριγωνικός, άρα το σύστημα δεν έχει λύσεις. Δηλαδή τα πακέτα μεταξύ τους δεν είναι γραμμικά ανεξάρτητα, διότι το διάνυσμα xtrans επέστρεψε NaN όταν εξετάσαμε το παρακάτω σύστημα:

$$\begin{aligned}
 4x_1 + 3x_2 + 3x_3 &= 0 \\
 6x_1 + 4x_2 + 3x_3 &= 0 \\
 2x_1 + x_2 &= 0
 \end{aligned}$$



### 2.3 Σύγκριση: θεωρία - εφαρμογή

Για μια προσομοίωση που υλοποιήθηκε για την παραπάνω τοπολογία δικτύου Alice-Bob-Retransmitter , παρουσιάζονται τα παρακάτω αποτελέσματα.



#### Για τη θεωρητική ανάλυση:

Θεωρήθηκε ότι έχουμε 74% πιθανότητα σφάλματος στο κανάλι Alice-Bob και 57% στο κανάλι Alice-Relay-Bob.

Το θεωρητικό πλήθος των πακέτων που πρέπει να μεταδίδονται από την Alice ώστε να φτάσει ένα καθορισμένο πλήθος πακέτων στο Bob, εξαρτάται από :

- την πιθανότητα σφάλματος στο κύριο κανάλι μετάδοσης (σχήμα, μπλε \*).
- και εξαρτάται κι από την πιθανότητα σφάλματος στο Alice-Relay-Bob κανάλι (σχήμα, κόκκινο και πράσινο \*)

Πρέπει να αναφερθεί ότι η πράσινη \* έχει ληφθεί χρησιμοποιώντας επανακωδικοποίηση στην αναμετάδοση, με αποτέλεσμα την εξοικονόμηση κατά μέσο όρο 9% των μεταδόσεων.

#### Για την προσομοίωση ( μετά από 9 προσομοιώσεις):

Το πλήθος των μεταδιδόμενων πακέτων από την Alice και το πλήθος των λαμβανόμενων πακέτων από τον Bob εξαρτάται από :

- Την ποιότητα του καναλιού μεταξύ αυτών (σχήμα, μπλε),
- Την ποιότητα μεταξύ αυτών και του αναμεταδότη (σχήμα, κόκκινη) και από
- Την χρήση επανακωδικοποίησης στην αναμετάδοση (σχήμα, πράσινη)

Όταν ο αριθμός των ληφθέντων πακέτων αυξάνει στον Bob, αυξάνεται επίσης ο αριθμός των μεταδόσεων από την Alice. Από το σχήμα βλέπουμε ότι όταν το πλήθος των πακέτων που λαμβάνονται στο Bob είναι μικρό, το αποτέλεσμα της θεωρητικής ανάλυσης είναι κοντά στο αποτέλεσμα προσομοίωσης. Αυτό συμβαίνει επειδή έχουμε προσομοίωση πραγματικού δικτύου, όπου εάν ο αριθμός των πακέτων που ρέει στο δίκτυο είναι μεγάλος, θα υπάρχουν περισσότερα προβλήματα με τα πακέτα (όπως συγκρούσεις) και ως εκ τούτου, η Alice θα κάνει περισσότερες μεταδόσεις. Οι διαφορές μεταξύ των αναλυτικών-θεωρητικών αποτελεσμάτων και των αποτελεσμάτων της προσομοίωσης οφείλονται στους περισσότερους παράγοντες που περιλαμβάνονται και οι οποίοι μπορούν να επηρεάσουν τη συμπεριφορά του πακέτου. Το πλήθος

των μεταδόσεων από την Alice (κόκκινη γραμμή) μειώνεται για να λάβει τον ίδιο αριθμών πακέτων ο Bob, σε σύγκριση με (μπλε γραμμή) την περίπτωση, όπου η αναμετάδοση δεν χρησιμοποιείται. Επίσης χρησιμοποιώντας επανακωδικοποίηση κατά την αναμετάδοση, μπορεί να βελτιωθεί η απόδοση του κέρδους κατά 5,7% από την εξοικονόμηση μεταδόσεις. Τέλος όταν υπάρχουν περισσότερα πακέτα στο δίκτυο, η αναμετάδοση είναι πιο αποτελεσματική και μεταδίδονται τα πακέτα με την περισσότερη πληροφορία.

### 3. Τριγωνική κωδικοποίηση δικτύου (Triangular network coding)

Αναφέρουμε παρακάτω και την τεχνική της τριγωνικής κωδικοποίησης, όπου με απλά λόγια έχει σκοπό να ελαχιστοποιεί την πολυπλοκότητα αποκωδικοποίησης των πακέτων στους κόμβους προορισμού. Αυτό επιτυγχάνεται κωδικοποιώντας τα πακέτα πριν σταλούν με τέτοια τεχνική (τριγωνική), ώστε ο παραλήπτης να μην χρειάζεται να κάνει παραπάνω δυσκολότερες πράξεις για να αποκωδικοποιήσει τα πακέτα. Δηλ. η πολυπλοκότητα και κατά συνέπεια και ο χρόνος αποκωδικοποίησης μειώνεται. Η τεχνική αυτή είναι μια εντελώς καινούργια εύρεση στον τομέα της κωδικοποίησης δικτύου και μελετάται ακόμη για το πώς μπορεί να εφαρμοστεί πρακτικά στα σύγχρονα συστήματα δικτύων.

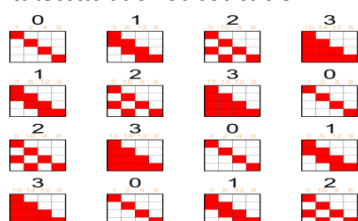
Στη θεωρία κωδικοποίησης, triangular network coding (TNC) είναι ένα δίκτυο κωδικοποίησης που βασίζεται σε ένα σύστημα κωδικοποίησης πακέτων που θεσπίστηκε από τους Qureshi, FOH & Cai (2012). Προηγουμένως, η κωδικοποίηση των πακέτων για την κωδικοποίηση δικτύου γινόταν χρησιμοποιώντας γραμμική κωδικοποίηση δικτύου (LNC) . Το μειονέκτημα του LNC σε μεγάλο πεπερασμένο πεδίο ή πεδίο Galois είναι ότι οδήγησε σε υψηλή κωδικοποίηση και αποκωδικοποίηση υπολογιστικής πολυπλοκότητας. Ενώ η γραμμική κωδικοποίηση και αποκωδικοποίηση στο σώμα  $GF(2)$  ελαττώνει το πρόβλημα της υψηλής υπολογιστικής πολυπλοκότητας, η κωδικοποίηση στο  $GF(2)$ , έχει ως συνέπεια την χαμηλή απόδοση όσον αφορά το throughput.

Triangular network coding, ως εκ τούτου αντιμετωπίζει κυρίως την υψηλή κωδικοποίηση και αποκωδικοποίηση υπολογιστικής πολυπλοκότητας, χωρίς να υποβαθμίζει την απόδοση throughput.

Η Τριγωνική κωδικοποίηση δικτύου (TNC), πραγματοποιείται σε δύο στάδια. Πρώτα προστίθενται επιπλέον "0" bits επιλεκτικά στην κεφαλή και την ουρά του κάθε πακέτου, έτσι ώστε όλα τα πακέτα να έχουν κοινό πλήθος από bit. Στη συνέχεια τα πακέτα κωδικοποιούνται με τη πράξη XOR, bit-by-bit. Τα "0" bits προστίθενται σε κάθε πακέτο κατά τέτοιο τρόπο ώστε στο τέλος να δημιουργείται ένα τριγωνικό πρότυπο (πίνακας) από "0".

Στην ουσία, η διαδικασία αποκωδικοποίησης TNC περιλαμβάνει απαλοιφή Gauss, όπως η διαδικασία αποκωδικοποίησης LNC. Ωστόσο, τα πακέτα σε TNC έχουν κωδικοποιηθεί με ένα τέτοιο τρόπο ώστε τα προκύπτοντα κωδικοποιημένα πακέτα έχουν ένα τριγωνικό πίνακα από "0". Έτσι η υπολογιστική διαδικασία Τριγωνοποίησης που έχει πολυπλοκότητα  $O(n^3)$ , όπου  $n$  είναι ο αριθμός των πακέτων, μπορεί να παρακαμφθεί και ο δέκτης τώρα να χρειάζεται μόνο να προβαίνει σε back-substitution (πίσω υποκατάσταση) με αποτέλεσμα η πολυπλοκότητα τελικά να είναι  $O(n^2)$  για κάθε θέση bit.

Η διαδικασία υπολογισμού των αγνώστων από ένα σύστημα που είναι στην άνω τριγωνική μορφή καλείται back substitution.



Ένα παράδειγμα κωδικοποίησης τεσσάρων πακέτων χρησιμοποιώντας TNC. Το bit  $b_{i,k} \in \{0,1\}$  είναι το  $i$ -οστό bit του  $k$ -οστού πακέτου. Κάθε πακέτο έχει αρχικό μήκος  $B$  Bits. Το κωδικοποιημένο πακέτο έχει μήκος  $B + 3$  bits. Πληροφορίες σχετικά με τον αριθμό των bits των επιπλέον '0' που προστέθηκαν στο κεφάλι του κάθε πακέτου περιλαμβάνονται στην επικεφαλίδα του κωδικοποιημένου πακέτου.

$b_{1,1}$	$b_{2,1}$	$b_{3,1}$	$b_{4,1}$	...	...	$b_{B,1}$	0	0	0
0	$b_{1,2}$	$b_{2,2}$	$b_{3,2}$	$b_{4,2}$	$b_{5,2}$	...	$b_{B,2}$	0	0
0	0	$b_{1,3}$	$b_{2,3}$	$b_{3,3}$	$b_{4,3}$	...	$b_{B,3}$	0	0
0	0	0	$b_{1,4}$	$b_{2,4}$	$b_{3,4}$	$b_{4,4}$	...	$b_{B,4}$	0

Η βασική ιδέα πίσω από τις μεθόδους της επίλυσης του συστήματος γραμμικών εξισώσεων είναι να τις μειώσουμε σε γραμμικές εξισώσεις όπου περιέχουν έναν μόνο άγνωστο, επειδή αυτές είναι εύκολο να λυθούν.

A. Οι πράξεις που υλοποιούνται είναι να πολλαπλασιάσουμε τα δύο μέλη μιας εξίσωσης με τον ίδιο αριθμό.

B. Να αναδιατάξουμε τις εξισώσεις, ανταλλάσσοντας και τις 2 πλευρές τις  $i^{\text{ης}}$  και  $j^{\text{ης}}$  εξίσωσης στο σύστημα.

Γ. Αντικαθιστώντας την εξίσωση  $i$  από το άθροισμα της εξίσωσης  $i$  με το γινόμενο ενός αριθμού με τις δύο πλευρές της εξίσωσης  $j$

Η Τρίτη πράξη είναι αυτή που χρησιμοποιείται πιο πολύ από όλες.

Η διαδικασία αυτή του υπολογισμού των αγνώστων από ένα σύστημα που είναι σε άνω τριγωνική (ή κάτω τριγωνική) μορφή είναι αυτό που καλείται "back substitution"

Σε Άνω τριγωνική μορφή είναι ένα σύστημα με  $n$  γραμμικές εξισώσεις και  $n$  αγνώστους εάν η  $i$  εξίσωση εξαρτάται μόνο από τους αγνώστους  $x_i, x_{i+1}, \dots, x_n$  για  $i=1,2,\dots,n$ .

Από την άλλη πλευρά αν πάρουμε τον επαυξημένο πίνακα  $Ax=b$  αντί του αρχικού συστήματος και τον κάνουμε σε άνω τριγωνική μορφή το αντίστοιχο σύστημα γραμμικών εξισώσεων μπορεί να λυθεί με back substitution όπως πριν. Η διαδικασία της εξάλειψης μεταβλητών από τις εξισώσεις, ή, ισοδύναμα, ο μηδενισμός των στοιχείων του πίνακα προκειμένου να φτιάξουμε το σύστημα σε άνω τριγωνική μορφή ονομάζεται απαλοιφή Gauss. Η απαλοιφή Gauss παραμένει η πιο γενικά εφαρμόσιμη μέθοδος των συστημάτων γραμμικών εξισώσεων προβλημάτων.

Ο αλγόριθμος της έχει ως εξής:

```

for  $j = 1, 2, \dots, n - 1$  do
  for  $i = j + 1, j + 2, \dots, n$  do
     $m_{ij} = a_{ij} / a_{jj}$ 
    for  $k = j + 1, j + 2, \dots, n$  do
       $a_{ik} = a_{ik} - m_{ij}a_{jk}$ 
    end
     $b_i = b_i - m_{ij}b_j$ 
  end
end
end

```

## 4. Το πλαίσιο των Δυνατοτήτων και των Ορίων της Τεχνικής Κωδικοποίησης

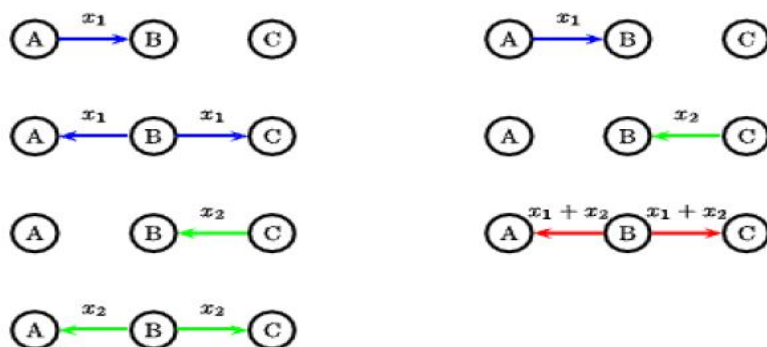
Σε αυτήν την ενότητα, θα δούμε πια είναι τα πλεονεκτήματα της Κωδικοποίησης Δικτύου, όπου η χρήση της συμβάλλει σε σημαντικές βελτιώσεις στα σύγχρονα δυναμικά και στατικά δίκτυα. Τονίζουμε, πως στην ενότητα 4.1 τα πλεονεκτήματα που αναφέρουμε, είναι οι σημαντικότεροι λόγοι που θεωρούνται αναγκαίοι, ώστε να εφαρμοστεί η κωδικοποίηση δικτύου και να αντικαταστήσει την παλιά τεχνική συστήματος χωρίς κωδικοποίηση. Βέβαια, η χρήση της κωδικοποίησης δεν αποδίδει πάντα με βέλτιστο τρόπο, για αυτό αναφέρουμε στην ενότητα 4.2 τα μειονεκτήματα που καθιστούν δύσκολα την εφαρμογή και την πρακτική χρήση της κωδικοποίησης, με αποτέλεσμα σαν σύνολο να μην συμφέρει να υλοποιηθεί και να εγκατασταθεί η τεχνική της κωδικοποίησης δικτύου διότι όπως έχουμε αναφερθεί σε παραπάνω ενότητες αυξάνουν την πολυπλοκότητα του συστήματος.

### 4.1 Πλεονεκτήματα της τεχνικής Network Coding

Η κωδικοποίηση δικτύου έχει τα εξής πλεονεκτήματα

- Αυξάνει η ρυθμαπόδοση
- Χρησιμοποιούνται αποδοτικότερα οι πόροι
- Μειώνεται η καθυστέρηση μετάδοσης
- Αυξάνεται η διάρκεια ζωής των κόμβων
- Γίνεται περισσότερο εύρωστο το δίκτυο
- Ελαχιστοποιούνται οι παρεμβολές
- Προστατεύεται το δίκτυο από επιθέσεις
- Αυξάνει την ασφάλεια των ροών δεδομένων στο δίκτυο

Σχήμα1



Η εφαρμογή της τεχνικής network coding έχει αρκετά πλεονεκτήματα. Το βασικό πλεονέκτημα της τεχνικής network coding είναι η αύξηση της διεκπεραιωτικής ικανότητας του δικτύου. Από τα παραπάνω παράδειγμα (ενότητα 1.3) είδαμε ότι οι εκπομπές πακέτων σε ένα δίκτυο μειώνονται. Στο συγκεκριμένο παράδειγμα 1.3.1 από 4 μειώνονται σε 3. Η μείωση των εκπομπών σημαίνει αυτόματα και μείωση των συγκρούσεων μεταξύ των κόμβων για την πρόσβαση στο μέσο. Το χρονικό κόστος της μετάδοσης συνίσταται κυρίως στην διαδικασία απόκτησης πρόσβασης στο μέσο και όχι στη μετάδοση αυτή καθαυτή. Ο χρόνος εντοπισμού και αντιμετώπισης των συγκρούσεων σε ασύρματα δίκτυα είναι πολύ μεγαλύτερος σε σχέση με το χρόνο μετάδοσης του πακέτου. Γίνεται λοιπόν, κατανοητό ότι η τεχνική network coding συμβάλλει καθοριστικά στην αύξηση της διεκπεραιωτικής ικανότητας του δικτύου με τον παραπάνω τρόπο.



## 4.2 Μειονεκτήματα της τεχνικής Network Coding

Ένα από τα σημαντικότερα μειονεκτήματα της τεχνικής είναι ότι εάν ένα πακέτο χαθεί κατά την μετάδοση, τότε αυτό συνεπάγεται πολλαπλές απώλειες για τον παραλήπτη. Αυτό συμβαίνει επειδή σε ένα πακέτο μπορεί να υπάρχει πληροφορία από πολλούς αποστολείς (πολλά πακέτα). Από τη στιγμή που χρειαζόμαστε  $n-1$  πακέτα για τη διαδικασία decoding, η απώλεια έστω και ενός κάνει αδύνατη την αποκωδικοποίηση του συνόλου των πακέτων. Ωστόσο, σε ένα δίκτυο με ικανό αριθμό κόμβων, τέτοιου είδους απώλειες είναι δύσκολο να συμβούν, αφού ένας κόμβος μπορεί να λάβει πακέτα από πολλούς διαφορετικούς αποστολείς, ειδικά αν μπορούν όλοι να επιτελέσουν τις λειτουργίες encode και decode.

Ένα άλλο μειονέκτημα είναι οι καθυστερήσεις που δημιουργούνται στο δίκτυο. Από τον ορισμό της τεχνικής, προκειμένου να πραγματοποιηθεί το decoding, είναι απαραίτητο να έχουμε στη διάθεσή μας όλη την πληροφορία που απαιτείται (δηλαδή και τα  $n-1$  πακέτα). Αυτό σημαίνει ότι ο παραλήπτης πρέπει να περιμένει να λάβει όλα αυτά τα πακέτα και μετά να προχωρήσει στη διαδικασία decoding. Επιπλέον καθυστέρηση προστίθεται και από τη διαδικασία encoding, αφού το access point που είναι υπεύθυνο να την εκτελέσει, δεν περιορίζεται σε μια επανεκπομπή των πακέτων που έλαβε, αλλά πρέπει να κάνει πρώτα τους απαραίτητους συνδυασμούς μεταξύ τους. Ένα μειονέκτημα που απορρέει από αυτού του είδους τις καθυστερήσεις αφορά εφαρμογές πραγματικού χρόνου. Σε αυτή την περίπτωση, οι καθυστερήσεις επηρεάζουν σε μεγάλο βαθμό την επίδοση του δικτύου και κατ'επέκταση της εφαρμογής. Είναι λοιπόν απαραίτητο να υπάρχει κάποιου είδους συγχρονισμός. Θα πρέπει να καθορίζεται προσεκτικά τόσο ο χρόνος αναμονής για εύρεση coding opportunities, όσο και ο χρόνος που θα περιμένει ο κάθε κόμβος για απάντηση.

Η τεχνική network coding απαιτεί από τη φύση της ευρεία εκπομπή από το access point, προκειμένου να μπορούν όλοι οι κόμβοι να λαμβάνουν τα κωδικοποιημένα πακέτα. Η ευρεία εκπομπή (multicast), δεν περιλαμβάνει επιβεβαίωση ότι το πακέτο που έχει σταλεί έφτασε στον προορισμό του. Έτσι οι κόμβοι του δικτύου δεν είναι σε θέση να γνωρίζουν αν τα πακέτα που έστειλαν έχουν φτάσει στον προορισμό τους. Για το λόγο αυτό, θα πρέπει να υπάρχει αρίθμηση των πακέτων που διακινούνται και φύλαξή τους σε κατάλληλες δομές, τόσο στον client όσο και στον server.

Τα μειονεκτήματα κατά την εφαρμογή της κωδικοποίησης δικτύου είναι κυρίως η πολυπλοκότητα που εισάγεται στο σύστημα, η διατήρηση του επιπέδου ασφαλείας σε συστήματα όπου η ασφάλεια είναι πολύ σημαντική απαίτηση και η ενσωμάτωσή της στην υπάρχουσα δομή. Ένα πολύ σημαντικό ζήτημα προς περαιτέρω έρευνα είναι η εύρεση της κατάλληλης σχέσης ανταλλαγής μεταξύ πολυπλοκότητας και επίδοσης του δικτύου.

Όσον αφορά την πολυπλοκότητα, για την εφαρμογή της κωδικοποίησης δικτύου οι κόμβοι πρέπει να επιτελούν πρόσθετες λειτουργίες. Στο παράδειγμα του Σχήματος στην ενότητα 1.3.1 (Ασύρματο Δίκτυο Εξοικονόμησης) ο κόμβος B πρέπει να διαθέτει επιπλέον μνήμη γιατί χρειάζεται να αποθηκεύσει το  $x_1$  αντί να το μεταδώσει αμέσως και να εκτελεί πράξεις για να προσδιορίζει το συνδυασμό των αρχείων. Επιπλέον, οι κόμβοι A και C πρέπει να διατηρήσουν αποθηκευμένη την πληροφορία που έστειλαν και να λύσουν ένα σύστημα γραμμικών εξισώσεων, αφού λάβουν το κωδικοποιημένο μήνυμα. Αυτό συμβαίνει διότι για να αποκωδικοποιήσουν τα πακέτα που λαμβάνουν οι κόμβοι A ή C πρέπει να γνωρίζουν τα  $n-1$  πακέτα που τους χρειάζονται για την αποκωδικοποίηση (σύστημα γραμμικών εξισώσεων).

Με την εφαρμογή της κωδικοποίησης δικτύου απαιτείται οι ενδιάμεσοι κόμβοι να εκτελούν πολύπλοκες πράξεις στα μηνύματα δεδομένων. Αυτό σημαίνει ότι η εφαρμογή της κωδικοποίησης, παρουσιάζει καθυστερήσεις λόγω των πολύπλοκων πράξεων στο δίκτυο, διότι πρέπει να εγγυάται την αυθεντικότητα της μεταδιδόμενης πληροφορίας.

Τέλος ένας τομέας που ερευνάται σήμερα είναι η ενσωμάτωση της κωδικοποίησης δικτύου στα υπάρχοντα πρωτόκολλα δικτύου και στις υπάρχουσες αρχιτεκτονικές δικτύων, πράγμα το οποίο καθιστά δυσκολίες στην συμβατότητά τους.

## 5. Εφαρμογές Κωδικοποίησης Δικτύου

Τα πλεονεκτήματα της κωδικοποίησης δικτύου έχουν μελετηθεί σε πληθώρα δικτύων και εφαρμογών όπως οι εξής:

- Διανομή ψηφιακών αρχείων : Content Distribution (CD) και Peer-to-Peer (P2P) διαμοιρασμός αρχείων.

Σε ένα σύστημα Peer-to-Peer, κάθε χρήστης λαμβάνει τα δεδομένα και βοηθά στην περαιτέρω διανομή τους σε άλλους κόμβους ενεργώντας ως εξυπηρετητής του συστήματος. Το αρχείο τεμαχίζεται και διαφορετικά τμήματά του μεταδίδονται μεταξύ χρηστών. Το σύστημα Microsoft Secure Content Distribution (MSCD), γνωστό και ως Avalanche, επιτρέπει στους χρήστες να παράγουν γραμμικούς συνδυασμούς των τμημάτων των αρχείων τα οποία βρίσκονται στην κατοχή τους. Οι συνδυασμοί αποστέλλονται μαζί με μία ετικέτα που περιλαμβάνει τους συντελεστές με τους οποίους πολλαπλασιάστηκαν τα τμήματα του συνδυασμού. Τα πλεονεκτήματα της εφαρμογής της κωδικοποίησης δικτύου σε ένα σύστημα διανομής ψηφιακών αρχείων είναι η αύξηση της ρυθμαπόδοσης και η αντιμετώπιση καταστάσεων όπως οι τυχαίες αφίξεις ή αναχωρήσεις χρηστών και η έλλειψη συνδεσιμότητας. Οι δυσκολίες της εφαρμογής της κωδικοποίησης δικτύου είναι πολυπλοκότητα που εισάγεται, η διατήρηση του επιπέδου ασφάλειας στο δίκτυο και η αντιμετώπιση της ετερογένειας των χρηστών. Η εφαρμογή αυτή έχει ομοιότητες με την τοπολογία ενός \*DNT δικτύου λόγω της ετερογένειας των χρηστών και των τυχαίων αφίξεων και αναχωρήσεων τους από το δίκτυο, οι οποίες έχουν ως αποτέλεσμα να μην υπάρχει πάντα εφικτή διαδρομή μεταξύ πηγής και προορισμού του μηνύματος.

\*[DNT](#) = Delay-tolerant networking (DTN), είναι μια αρχιτεκτονική δικτύου υπολογιστών που επιδιώκει προσεγγιστικά να αντιμετωπίσει τα τεχνικά ζητήματα σε ετερογενή δίκτυα που μπορεί να στερούνται συνεχούς σύνδεσης ή να υπάρχουν καθυστερήσεις με το δίκτυο. Παραδείγματα τέτοιων δικτύων είναι τα δίκτυα που λειτουργούν σε κινητές ή σε ακραία χερσαίο περιβάλλον, ή προβλεπόμενα δίκτυα στο χώρο.

- Ασύρματα δίκτυα
- Ευρυεκπομπή και πολυεκπομπή δεδομένων

Με την εφαρμογή της κωδικοποίησης δικτύου σε περιπτώσεις πολυεκπομπής αυξάνεται η χωρητικότητα και η ρυθμαπόδοση.

- Εναλλακτική στην κωδικοποίηση διαύλου (FEC: Forward Error Correction) και στην τεχνική του αυτόματου αιτήματος αναμετάδοσης (ARQ: Automatic repeat ReQuest) στα παραδοσιακά ασύρματα δίκτυα.

Έχει δειχθεί ότι η εφαρμογή της κωδικοποίησης δικτύου στα ασύρματα δίκτυα με απώλειες συμβάλλει στη μείωση του αριθμού των αναμεταδόσεων των μηνυμάτων

- Ad-hoc δίκτυα και Δίκτυα αισθητήρων

Στα δίκτυα αισθητήρων πόροι όπως η ενέργεια, ο χώρος αποθήκευσης της πληροφορίας και η υπολογιστική δυνατότητα είναι περιορισμένοι. Η κωδικοποίηση δικτύου μπορεί να συμβάλει στη μείωση της καθυστέρησης, της απασχόλησης της μνήμης και της κατανάλωσης ενέργειας, και συνεπώς στην αύξηση του χρόνου ζωής των κόμβων του δικτύου. Τα ασύρματα δίκτυα ad-hoc και τα δίκτυα αισθητήρων ως δίκτυα που διέπονται από λιγότερο αυστηρά πρωτόκολλα αναμένεται να προσφέρουν τις πρώτες εφαρμογές για της κωδικοποίησης δικτύου.



➤ Network monitoring

Η παρακολούθηση των απωλειών των ζεύξεων και των αλλαγών στην τοπολογία ενός δικτύου μπορεί να γίνει με είτε παθητικές είτε με ενεργητικές μετρήσεις. Οι παθητικές στηρίζονται στη μέτρηση της μεταφερόμενης κίνησης στο δίκτυο, ενώ οι ενεργητικές στην αποστολή ειδικών μηνυμάτων (probe) από ένα σύνολο πηγών σε ένα σύνολο παραληπτών. Η κωδικοποίηση δικτύου μπορεί να προσφέρει στην παρακολούθηση των απωλειών των ζεύξεων, εφόσον οι κόμβοι συνδυάζουν γραμμικά τα εισερχόμενα probe μηνύματα τους. Η απόφαση για το αν υπάρχει απώλεια σε κάποια ζεύξη λαμβάνεται όταν τα μηνύματα probe φθάσουν στον κόμβο όπου γίνεται η μέτρηση. Με βάση την τιμή των δεδομένων αυτών εξάγονται συμπεράσματα για το αν υπάρχει απώλεια ζεύξης και ποιό τμήμα του δικτύου που ενδεχομένως δεν λειτουργεί.

➤ Ασφάλεια δικτύου και ακεραιότητα δεδομένων

Όπως αναφερθήκαμε, η εφαρμογή της κωδικοποίησης δικτύου σε ένα δίκτυο μπορεί να οδηγήσει αφενός σε απόκρυψη σημαντικής πληροφορίας από τρίτους και αφετέρου σε περιβάλλον περισσότερο ευάλωτο για τους νόμιμους χρήστες. Δύο σημαντικοί τομείς έρευνας σήμερα είναι η χρήση της κωδικοποίησης δικτύου για να διασφαλιστεί η ασφάλεια του δικτύου από υποκλοπές και οι τόποι διασφάλισης της ακεραιότητας των δεδομένων μετά την εφαρμογή της κωδικοποίησης δικτύου στο δίκτυο.

## 5.1 Διανομή Ψηφιακού Περιεχομένου σε P2P

Τα Peer-to-peer (P2P) δίκτυα προσφέρουν μια εναλλακτική λύση για την διανομή ψηφιακού περιεχομένου. Αποτελούν μη-ιεραρχική δομή δικτύων υπολογιστών, που βασίζονται στην υπολογιστική ισχύ και στο εύρος ζώνης όλων των συμμετεχόντων κόμβων στο δίκτυο, και όχι σε ένα μικρό αριθμό των servers (διακομιστές) και των σχέσεων client-server. Σε ένα P2P δίκτυο, όλοι οι κόμβοι που λαμβάνουν πληροφορίες βοηθούν στην περαιτέρω διανομή του περιεχομένου σε άλλους κόμβους ενεργώντας οι ίδιοι ως διακομιστές. Έτσι το δίκτυο είναι εκ φύσεως επεκτάσιμο: οι κόμβοι που συμμετέχουν στο δίκτυο φέρνουν όχι μόνο νέες απαιτήσεις αλλά και πρόσθετη υπολογιστική ισχύ και bandwidth. Επιπλέον, δεν υπάρχει πλέον ένα ενιαίο σημείο αποτυχίας (συντρίβεια διακομιστή) στο σύστημα, καθώς η πληροφορία διανέμεται μεταξύ πολλαπλών κόμβων σε όλο το δίκτυο.

Έχοντας έτσι αντιμετωπιστεί το πρόβλημα της εξασφάλισης επαρκών πόρων στο δίκτυο, τα P2P εξακολουθούν να αντιμετωπίζουν προκλήσεις ή δυσκολίες στο πώς να χρησιμοποιούν βέλτιστα αυτούς τους πόρους με αποκεντρωμένο τρόπο και χαμηλής πολυπλοκότητας λειτουργία. Για παράδειγμα, η βέλτιστη δρομολόγηση πληροφορίας, είναι ένα δύσκολο πρόβλημα σε τέτοια δίκτυα μεγάλης κλίμακας που αλλάζουν πολύ γρήγορα με την πάροδο του χρόνου (χιλιάδες κόμβοι να εισέρχονται και να εξέρχονται μέσα σε σύντομο χρονικό διάστημα) και ειδικά όταν οι κόμβοι έχουν μόνο τοπικές πληροφορίες (δηλαδή βρίσκονται σε μια μικρή γεωγραφική περιοχή) σχετικά με το δίκτυο.

Το BitTorrent είναι ένα παράδειγμα ενός P2P συστήματος που χρησιμοποιεί τεχνικές εξάπλωσης για την ταυτόχρονη διάδοση διαφορετικών τμημάτων των πακέτων (fragments) ενός αρχείου μεταξύ των κόμβων (peers) που συμμετέχουν στο δίκτυο. Το πρόβλημα που υπάρχει είναι ότι, καθώς ο αριθμός των peers αυξάνεται, γίνεται πιο δύσκολη η διαδικασία της βελτιστοποίησης προγραμματισμού διανομής τμημάτων ή πακέτων στους παραλήπτες. Έτσι η πιθανότητα να ανακτηθούν καινούργια τμήματα πακέτων (ώστε να συλλέξει κάποιο περιεχόμενο) από τους δέκτες, μειώνεται ραγδαία ως προς την πιθανότητα να συλλέξει ήδη πακέτα που έχουν λάβει. Αυτό συμβαίνει διότι σπανιότερα πακέτα χάνονται και δεν φτάνουν ποτέ στον προορισμό τους. Μια πιθανή λύση είναι να χρησιμοποιηθεί και να δοθεί προτεραιότητα στην προώθηση σπανιότερων τμημάτων πακέτων που βρίσκονται σε τοπικό δίκτυο. Η ανίχνευση τέτοιων σπάνιων πακέτων (fragments) είναι δύσκολη και χρονοβόρα διαδικασία σε ένα τοπικό δίκτυο, πράγμα που καθιστά χειρότερη την κατάσταση σε μεγαλύτερης γεωγραφικής εμβέλειας (global) επίπεδα.

Η Microsoft Secure Content Distribution (MSCD), γνωστή επίσης ως Avalanche (Χιονοστιβάδα), είναι ένα παράδειγμα ενός συστήματος P2P προσπαθεί να δώσει λύσεις στα προβλήματα του BitTorrent με τη χρήση κωδικοποίησης δικτύου. Αντί για τη διανομή των τμημάτων πακέτων του αρχικού αρχείου, τα peers παράγουν γραμμικούς συνδυασμούς των τμημάτων που ήδη κατέχουν. Οι συνδυασμοί διανέμονται μαζί με μια ετικέτα που περιγράφει τους συντελεστές (coefficients) που δημιουργήσανε τον συνδυασμό. Ένας peer μπορεί να ανακτήσει μια αρχική πληροφορία όταν θα έχει συλλέξει αρκετά πακέτα γραμμικών ανεξάρτητων συνδυασμών. Στην ενότητα 1.2 για την αποκωδικοποίηση πακέτων, αναφέρουμε πως ο αριθμός των γραμμικών ανεξάρτητων συνδυασμών πρέπει να είναι μεγαλύτερος ή ίσος από τα άγνωστα πακέτα.

Ένα συχνό πρόβλημα στα P2P δίκτυα είναι το γεγονός ότι εισέρχονται νέοι κόμβοι και έχουν απαίτηση να παραλαμβάνουν πακέτα από τους γειτονικούς κόμβους. Η μέγιστη απόδοση δεν μπορεί να επιτευχθεί και μάλιστα η εφικτή είναι αρκετά μακριά από αυτή, λόγω δυσκολίας στην μετάδοση πακέτων και συνεχόμενη αλλαγή των κόμβων στο δίκτυο. Για παράδειγμα, μπορούμε να φανταστούμε ένα σενάριο στο οποίο ο κόμβος Α έχει κατεβάσει 80% του αρχείου, όταν ένας νέος κόμβος Β εισέρχεται στο δίκτυο, και δημιουργεί αίτηση να πάρει πακέτα του ίδιου αρχείου από γείτονές του. Ως αποτέλεσμα, τα πακέτα που ο Α έχει ήδη πάρει τα οποία τα κατέβαζε μέσω κάποιας δρομολόγησης, οδηγούν σε αυξημένη καθυστέρηση για τον κόμβο Α. Χρησιμοποιώντας κωδικοποίηση δικτύου μειώνει αυτό το πρόβλημα, δεδομένου ότι όλα τα μεταδιδόμενα πακέτα μπορούν να γίνουν χρήσιμες μεταφερόμενες πληροφορίες για ένα μεγάλο αριθμό κόμβων.

Με τη δυνατότητα να κωδικοποιήσουν οι ενδιαμέσσοι κόμβοι του δικτύου στην πραγματοποίηση μιας επικοινωνίας, μπορούμε να διαβιβάσουμε, αναπαράγουμε, και να κωδικοποιήσουν με εισερχόμενα πακέτα. Αυτή η ικανότητα έρχεται σε έντονη αντίθεση με τις παραδοσιακή ροή πακέτων, όπου η διαβίβαση μόνο επιτρέπεται. Για να εφαρμοστεί στην πράξη η κωδικοποίηση δικτύου, κάποιος πρέπει να αντιμετωπίσει τις προκλήσεις του υπολογισμού για την κωδικοποίηση

των συντελεστών που πρέπει να χρησιμοποιούνται από κάθε ενδιάμεσο κόμβο σε μια επικοινωνία, έτσι ώστε τα κωδικοποιημένα πακέτα στους δέκτες σίγουρα να αποκωδικοποιηθούν.

Παρόλο που αλγόριθμοι που κάνουν ντετερμινιστική κωδικοποίηση έχουν προταθεί και έχει αποδειχθεί ότι είναι αλγόριθμοι πολυωνυμικού χρόνου, απαιτούν ανταλλαγές των πακέτων με μεγάλο κόστος. Για αυτό έχουν προτείνει την έννοια της τυχαίας κωδικοποίησης δικτύου.

Η τυχαία κωδικοποίηση δικτύου μπορεί να εφαρμοστεί στον πραγματικό κόσμο των δικτύων, με τη διαίρεση του όγκου πληροφοριών σε γενιές, και εκτελώντας τυχαία γραμμική κωδικοποίηση σε κάθε γενιά. Η συντελεστές κωδικοποίησης μπορούν να μεταφέρονται από τα ίδια τα πακέτα πριν από τη μετάδοση. Έχει βγει το συμπέρασμα ότι η τυχαία κωδικοποίηση δικτύου είναι ανθεκτική στην απώλεια πακέτων, στην καθυστέρηση, καθώς και σε μεταβολές στην τοπολογία του δικτύου και την χωρητικότητα, και ότι επικοινωνίες με τυχαία κωδικοποίηση δικτύου μπορούν να πλησιάσουν κοντά στην θεωρητικά βέλτιστη απόδοση.

Μεγάλο μέρος συστημάτων διανομής περιεχομένου P2P, όπως το BitTorrent, βοηθούν τους peers να συνεργάζονται ο ένας με τον άλλο έτσι ώστε τα μεγάλα αρχεία να μπορούν να διανέμονται από τον ένα peer σε ένα μεγάλο αριθμό των συμμετεχόντων δεκτών, χωρίς τη βοήθεια των [dedicated servers](#). Μεγάλο μέρος των συστημάτων διανομής περιεχομένου P2P έχουν υιοθετήσει μια απλή σχεδιαστική φιλοσοφία: ένα αρχείο χωρίζεται σε μπλοκ, και οι peers συνδέονται ο ένας με τον άλλο σε μια τυχαία [τοπολογία πλέγματος](#), ανταλλάσσοντας τα μπλοκ με τυχαίο τρόπο. Στην επικοινωνία κάθε peer μεταδίδει ένα υποσύνολο των μπλοκ που έχει λάβει σε ένα υποσύνολο των γειτόνων του που επιλέγονται τυχαία χρησιμοποιώντας αλγορίθμους. Τέτοια τυχαία επικοινωνία για τυχαίες τοπολογίες πλέγματος είναι απλή στην εφαρμογή. Είναι φυσικό να δούμε μια πιθανή σχέση ανάμεσα στην τυχαία κωδικοποίηση δικτύου και στην τυχαία επικοινωνία, σε τυχαίες τοπολογίες πλέγματος. Λόγω της κοινής τυχαιοποιημένης φύσης τους, αναρωτιέται κανείς αν μπορεί να χρησιμοποιηθεί με ολοκληρωμένο τρόπο σε δίκτυα P2P. Στην ουσία, η [τυχαία επικοινωνία](#) μελετά την εξάπλωση ενός ενιαίου ή περισσότερων μπλοκ σε μια ομάδα συμμετεχόντων peers. Από την άλλη η τυχαία κωδικοποίηση δικτύου (με την σειρά της μελετά) με την ανάμιξη των μπλοκ όπου ο καθένας peer μεταδίδει, φαίνεται να μεγιστοποιεί την αποτελεσματικότητα της διάχυσης της πληροφορίας δεδομένου του περιορισμένου εύρους ζώνης.

### 5.1.1 Χρησιμοποιώντας Random Network Coding

Οι τοπολογίες δικτύου P2P σχηματίζεται από τους τελικούς hosts που συνδέονται ο ένας με τον άλλο, χρησιμοποιώντας [συνδέσεις υπέρθεσης](#), και αυτές οι τοπολογίες σχηματίζονται για ένα συγκεκριμένο στόχο. Ένας από τους στόχους είναι να διανείμουμε κάποιον όγκο ενός περιεχομένου, όπως ένα μεγάλο αρχείο, από έναν peer σε άλλους peers σε μια τοπολογία. Πιο τυπικά, ως θεωρήσουμε ένα δίκτυο με  $n$  peers οι οποίοι επιθυμούν να λάβουν ένα αντίγραφο ενός μεγάλου αρχείου που πρέπει να διαδοθεί. Το αρχείο διαιρείται σε  $K$  μπλοκ. Για λόγους απλότητας, ως υποθέσουμε επίσης ένα συγχρονισμένο πρότυπο στο οποίο ο χρόνος μετρείται σε κύκλους (rounds). Κάθε peer κάνει upload σε γείτονες που έχουν επιλεγεί τυχαία. Πόσοι κύκλοι απαιτούνται για όλους τους peer να λάβουν ένα αντίγραφο του αρχείου;

Εννοιολογικά, ο στόχος αυτός είναι παρόμοιος με το κλασικό πρόβλημα της τυχαίας επικοινωνίας, η οποία θεωρεί το πρόβλημα  $n$  ανθρώπων να εξαπλώνουν τη φήμη η οποία ήταν αρχικά στην κατοχή ενός μόνο ατόμου. Πόσοι κύκλοι απαιτούνται για τον καθένα να λάβει μια φήμη; Ο Pittel έχει δείξει ότι, εάν κάθε πρόσωπο που έχει ήδη λάβει την φήμη επικοινωνεί με ένα πρόσωπο που επιλέγεται τυχαία και ανεξάρτητα από όλες τις άλλες επιλογές που έκανε στο παρελθόν και στο παρόν, παίρνει  $\log_2 n + \log n + O(1)$  κύκλους για να φτάσει η φήμη σε όλα τα  $n$  άτομα. Ένα τέτοιο πρωτόκολλο, τυχαίας επιλογής δέκτη καλείται επίσης μοντέλο τυχαίας τηλεφωνικής κλήσης (random phone call). Η διαφορά μεταξύ της διανομής περιεχομένου P2P και του προβλήματος τυχαίας επικοινωνίας είναι ότι πολλαπλά μπλοκ πρέπει να διανέμονται, αντί για μία μόνο φήμη.

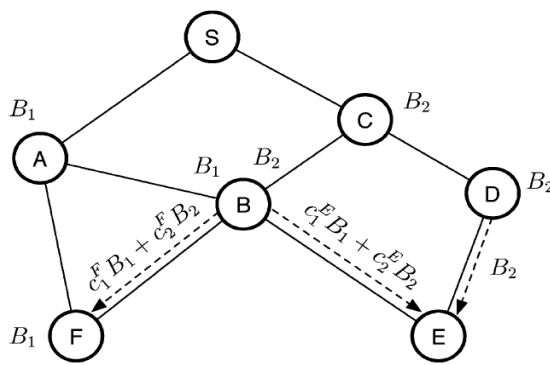
Ο Sanghani είναι μεταξύ των πρώτων όπου έχει μελετήσει το χρόνο που απαιτείται για να διαδοθούν πολλαπλά μπλοκ. Επέκτεινε το μοντέλο τυχαίας τηλεφωνικής κλήσης για να ενσωματώσει πολλαπλά μπλοκ, όπου σε κάθε γύρο, κάθε κόμβος επικοινωνεί με έναν άλλο όπου επιλεγεί ομοιόμορφα με τυχαίο τρόπο από ολόκληρο το δίκτυο, και κάθε κόμβος μπορεί να ανεβάσει το πολύ

ένα από τα μπλοκ που διαθέτει. Μέσα σε ένα τέτοιο μοντέλο, ακόμη και αν το centralized block scheduling επιτρέπεται, τουλάχιστον  $k + \log_2 N$  κύκλοι απαιτούνται για να διαδώσει όλα τα  $k$  μπλοκ από μια πηγή σε όλους τους  $n$  peers. Ο Sanghavi απέδειξε ότι με ένα αποκεντρωμένο πρωτόκολλο επιλογής μπλοκ, μπορεί κανείς να ολοκληρώσει τη διανομή των  $K$  μπλοκ από μία πηγή σε  $n$  κόμβους σε  $9(K + \log n)$  χρόνο, με μεγάλη πιθανότητα, για ένα μεγάλο αριθμό από τους peers.

Θα μπορούσε η χρήση της τυχαίας κωδικοποίησης δικτύου να μειώσει τον αριθμό των γύρων (rounds) που απαιτούνται για τη διανομή  $K$  μπλοκ με τυχαία επικοινωνία;

Ο Gkantsidis και ο Rodriguez, ήταν οι πρώτοι που ανέπτυξαν το σύστημα Avalanche, η οποία βασίστηκε στην τεχνική της τυχαίας κωδικοποίησης δικτύου, για τη διάδοση δεδομένων σε P2P δίκτυο όπου στηρίχτηκε στην ανταλλαγή των επιμέρους μπλοκ (π.χ. BitTorrent) λειτουργώντας με τρόπο αποκεντρωτικό.

Σύμφωνα με το Avalanche, αν οι κόμβοι μπορούν να συνδυάσουν γραμμικά όλα τα μπλοκ που έχουν ήδη λάβει, χρησιμοποιώντας τους συντελεστές τυχαίας κωδικοποίησης, και στη συνέχεια διαβιβάζουν τα εν λόγω κωδικοποιημένα μπλοκ σε άλλους κόμβους, η ποσότητα του χρόνου που απαιτείται για τη διανομή ενός μεγάλου αρχείου σε όλα τα peers στο δίκτυο μπορεί να μειωθεί.



**Fig. 1.** An example of distributing two blocks  $B_1$  and  $B_2$  with network coding.  $S$  is the source peer.

Ένα απλό παράδειγμα για τη διανομή δύο μπλοκ δίνεται στο ΣΧ. 1. Ας υποθέσουμε ότι ο peer B έχει λάβει το μπλοκ  $B_1$  και  $B_2$ , και ο peer D έχει λάβει το μπλοκ  $B_2$ . Αν και οι δύο peer, B και D μπορούν να εξυπηρετήσουν τον peer E σε αυτό το σημείο, μπορούν να καταλήξουν να μεταδώσουν το ίδιο μπλοκ  $B_2$  στον peer E, δεδομένου ότι δεν υπάρχει σύνδεση μεταξύ των peer B και D, και η μετάδοσή τους δύσκολα μπορεί να συντονιστεί. Στην περίπτωση αυτή, το εύρος ζώνης ανεβάσματος από τον peer B σπαταλιέται. Με τη χρήση της κωδικοποίησης δικτύου, ωστόσο, ο peer B μπορεί να μεταδώσει στον peer E ένα κωδικοποιημένο μπλοκ  $c_1^E B_1 + c_2^E B_2$  με συντελεστές  $c_1^E$  και  $c_2^E$  τυχαία επιλεγμένους. Ο peer E μπορεί να βρεί το  $B_1$  χρησιμοποιώντας τα μπλοκ  $B_2$  και  $c_1^E B_1 + c_2^E B_2$  που ήδη έλαβε. Με την κωδικοποίηση του δικτύου, ο peer B μπορεί να μεταδώσει στον peer F ένα άλλο τυχαία κωδικοποιημένο μπλοκ το  $c_1^F B_1 + c_2^F B_2$ , που είναι πάντα χρήσιμο στον F αν το  $C_1^F$  και  $C_2^F$  έχει κατάλληλα επιλεγεί. Διαισθητικά, η χρήση της τυχαίας κωδικοποίησης δικτύου έχει αυξήσει την ποικιλία των μπλοκ που μεταδίδονται.

Στην πράξη, ωστόσο, η υπολογιστική πολυπλοκότητα της κωδικοποίησης δικτύου κλιμακώνεται με τον αυξανόμενο αριθμό των μπλοκ. Για τη διαχείριση των εν λόγω πολυπλοκότητας, έχει προταθεί ότι πολλά μπλοκ σε ένα αρχείο να διαιρούνται σε πολλαπλές γενεές, και η κωδικοποίηση δικτύου εκτελείται μόνον εντός της ίδιας γενιάς. Πιο συγκεκριμένα, το αρχικό αρχείο με  $F$  bytes διαιρείται σε  $G$  γενιές, καθένα από τα οποία διαιρείται περαιτέρω σε  $m$  μπλοκ, που αναφέρεται ως το μέγεθος γενιάς. Υπάρχουν συνολικά  $M = G * m$  μπλοκ, το καθένα με μέγεθος  $k = F / M$  bytes.

Όταν ένα αρχείο πρόκειται να διανεμηθεί, η RNC εφαρμόζεται σε όλα τα μπλοκ μέσα σε μία γενιά. Θεωρείται ότι η γενιά  $i$ , περιέχει  $m$  αρχικά μπλοκ  $B^{(i)} = [B_1^i, B_2^i, \dots, B_m^i]$ . Ένα κωδικοποιημένο μπλοκ  $b$  από αυτή τη γενιά είναι ένας γραμμικός συνδυασμός των εν λόγω αρχικά μπλοκ στο πεδίο

Galois. Η κωδικοποίηση δικτύου είναι σαφές ότι δεν περιορίζει την πηγή: εάν ένας peer (συμπεριλαμβανομένης της πηγής) διαθέτει κωδικοποιημένα μπλοκ της γενιάς  $i$ , όταν προκύψει η ανάγκη να στείλει το νέο κωδικοποιημένο μπλοκ σε ένα γείτονα  $p$ , ανεξάρτητα και τυχαία επιλέγει ένα σύνολο συντελεστών κωδικοποίησης, και κωδικοποιεί όλα τα μπλοκ της γενιάς  $i$  που διαθέτει για να παράγει ένα κωδικοποιημένο μπλοκ  $x$  που είναι  $k$  bytes και  $x = \sum_{j=1}^L c_j^p * b_j^i$  (όπου  $c$  είναι η συντελεστής που παίρνουν τιμές από το πεδίο Galois και  $b$  είναι τα μπλοκ της ίδιας γενιάς).

Όταν η τυχαία κωδικοποίηση δικτύου εφαρμόζεται, προς όφελος της επιτυχούς αποκωδικοποίησης, ένα κωδικοποιημένο μπλοκ  $x$  είναι αυτόνομο, σε αυτή την κωδικοποίηση οι συντελεστές που χρησιμοποιούνται για την κωδικοποίηση των πρωταρχικών μπλοκ του  $x$  είναι ενσωματωμένοι στην κεφαλίδα του. Μόλις ένα peer λάβει συνολικά  $m$  κωδικοποιημένα μπλοκ από τη γενιά  $i$  που είναι γραμμικά ανεξάρτητα, θα είναι σε θέση να ανακτήσει όλα τα πρωτότυπα μπλοκ σε αυτή τη γενιά με Gaussian απαλοιφή, αξιοποιώντας την κωδικοποίηση των συντελεστών που είναι ενσωματωμένοι σε καθένα από τα  $m$  κωδικοποιημένα μπλοκ που έλαβε.

### Random Gossiping (τυχαία επικοινωνία) With Network Coding

Ο Deb έδειξε ότι, αν κάθε peer συνδυάσει γραμμικά όλα τα μπλοκ που έχει ήδη λάβει με χρήση τυχαίων συντελεστών και μεταδώσει αυτό το κωδικοποιημένο μπλοκ στον peer που θέλει, ο χρόνος για όλα τα  $n$  peer να λάβουν όλα τα  $k$  μπλοκ είναι  $ck + O(\sqrt{k} * \log k * \log n)$  κύκλους όπου  $c$  είναι μια σταθερά που παίρνει τιμές από το 3 έως το 6. Αυτό ουσιαστικά δείχνει ότι με την τυφλή μετάδοση κωδικοποιημένων μπλοκ και την επιλογή κόμβου επικοινωνίας τυχαία χωρίς καμία μορφή συμφωνίας μεταξύ των peers, ο χρόνος για να διαδώσει όλα τα  $k$  μπλοκ σε όλους τους peer είναι γραμμικός σε σχέση με το  $k$ .

### Optimality From a Trellis Graph Perspective

Έχει αποδειχθεί από τον Yeung με χρήση διακριτού χρόνου [trellis graph](#) ότι με την κωδικοποίηση δικτύου, επιτυγχάνονται οι βέλτιστοι χρόνοι εκπομπής, ανεξάρτητα από την τοπολογία του δικτύου και τον τρόπο μετάδοσης.

### 5.1.2 Περιορισμοί στην πρακτική εφαρμογή της Κωδικοποίησης Δικτύου

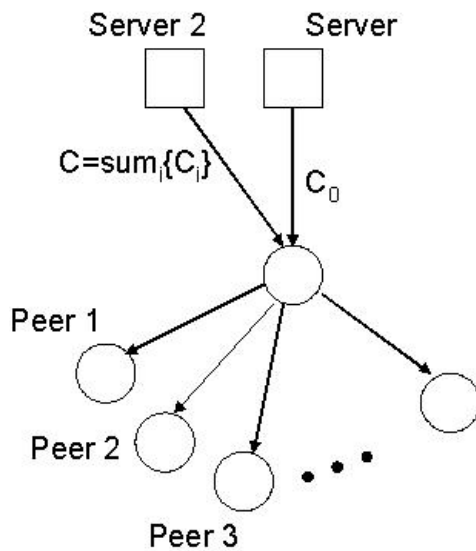
Υπάρχουν και περιορισμοί στα οφέλη που προσφέρει η τυχαία κωδικοποίηση δικτύου στα P2P πρωτόκολλα διανομής περιεχομένου. Η τυχαία κωδικοποίηση δικτύου μπορεί να πραγματοποιηθεί μόνο σε μπλοκ εντός της ίδιας γενιάς, η συμβατότητα (στην αποστολή) μεταξύ ενός ζεύγους γειτονικών peers μπορεί να εξακολουθήσει να είναι απαραίτητη σε όλη την γενιά. Με άλλα λόγια, αντί να συλλέγει μικρά μπλοκ, χρειάζεται μόνο ένας δέκτης για να συλλέξει όλες τις διακριτές γενιές που αποτελούν το αρχείο που έχει διανεμηθεί. Μετριάζει το πρόβλημα εντοπισμού των σπάνιων τμημάτων ενός αρχείου που μπορεί να είναι λιγότερο διαθέσιμο σε ολόκληρο το Δίκτυο P2P. Στην πράξη, μια τέτοια ανάγκη για ύπαρξη συνοχής ακόμη και σε μεγάλα τμήματα υποδιαίρεσης γενεών, μπορεί να επηρεάσει αρνητικά τα πλεονέκτημα που προσφέρει η τυχαία κωδικοποίηση δικτύου. όσο μεγαλύτερο είναι το μέγεθος της γενιάς, τόσο περισσότερη είναι η ποικιλία στα μπλοκ του συστήματος και τόσο ταχύτερα ολοκληρώνονται οι λήψεις.

Τα πρωτόκολλα που χρησιμοποιούν τυχαία κωδικοποίηση δικτύου είναι σε θέση να επιτύχουν την καλύτερη δυνατή απόδοση, αλλά η διαφορά απόδοσης μεταξύ της χρήσης κωδικοποίησης δικτύου και ενός καλά σχεδιασμένου πρωτόκολλου επιλογής μπλοκ δεν είναι σαφής. Ένα τέτοιο χάσμα μεταξύ των αποδόσεων μπορεί να είναι αρκετά μικρό όπως είναι στα πρωτόκολλα με μπλοκ χωρίς κωδικοποίηση δικτύου. Για παράδειγμα το BitTorrent, είναι σχεδιασμένο έτσι ώστε να κατεβαίνει το σπανιότερο μπλοκ πρώτο (με τη βοήθεια των συχνών ανταλλαγών buffer μεταξύ των peers, με σκοπό τον μετριασμό ορισμένων δυσμενών συνεπειών από τη διαδικασία εντοπισμού σπάνιων μπλοκ καθώς το αρχείο λήψης πλησιάζει στην ολοκλήρωσή του). Σε αντίθεση, η τυχαία κωδικοποίηση δικτύου χρησιμοποιεί επιπλέον υπολογιστική ισχύ για κάθε peer, η οποία δεν μπορεί να αιτιολογηθεί επαρκώς αν η απόδοση με τη χρήση της κωδικοποίησης δικτύου είναι μικρή σε μεγάλης κλίμακας P2P δίκτυα.

Εμπειρικές μελέτες έχουν αποδείξει ότι η χρήση της τυχαίας κωδικοποίησης δικτύου στην πράξη σε P2P σύστημα διανομής περιεχομένου, έχει ως αποτέλεσμα την ομαλή και γρήγορη λήψη και μάλιστα χωρίς πολλούς επιπρόσθετους υπολογισμούς. Ωστόσο, δεν είναι σαφές πώς οι διακριτές γενιές πρέπει να επιλέγονται και να συμβιβάζονται μεταξύ των peers. Δεν υπάρχουν επίσης συγκρίσεις με οποιοδήποτε από τα συστήματα διανομής περιεχομένου P2P που δεν χρησιμοποιούν κωδικοποίηση δικτύου σε μεγάλη κλίμακα. Μέχρι σήμερα, η τυχαία κωδικοποίηση δικτύου φαίνεται πολλά υποσχόμενη στις θεωρητικές μελέτες που έχουν γίνει και τα οφέλη της προσφέρουν πλεονεκτήματα σε πρακτικό επίπεδο.

Τονίζουμε, πως η χρήση κωδικοποίησης δικτύου δεν είναι ωφέλιμη σε τοπολογίες δικτύων αστερισμού. Όσον αφορά τη μέγιστη απόδοση, παρατηρείται ότι δεν υπάρχει όφελος από την κωδικοποίηση δικτύου στην δρομολόγηση των πακέτων. Η κωδικοποίηση δικτύου προσφέρει πλεονεκτήματα στην απόδοση μόνο σε multicast δικτύων.

Για παράδειγμα, στο παρακάτω δίκτυο αστερισμού, όλη η κίνηση και ο φόρτος του δικτύου προστίθεται στον κόμβο  $C_0$ , δεν υπάρχει multicasting (επικοινωνιακή σύνδεση πολλών κόμβων μεταξύ τους). Με την χρήση κωδικοποίησης δεν ωφελείται μεγάλη απόδοση, οπότε και για αυτό δεν υπάρχει και σκοπός να αυξήσουμε την πολυπλοκότητα του δικτύου.





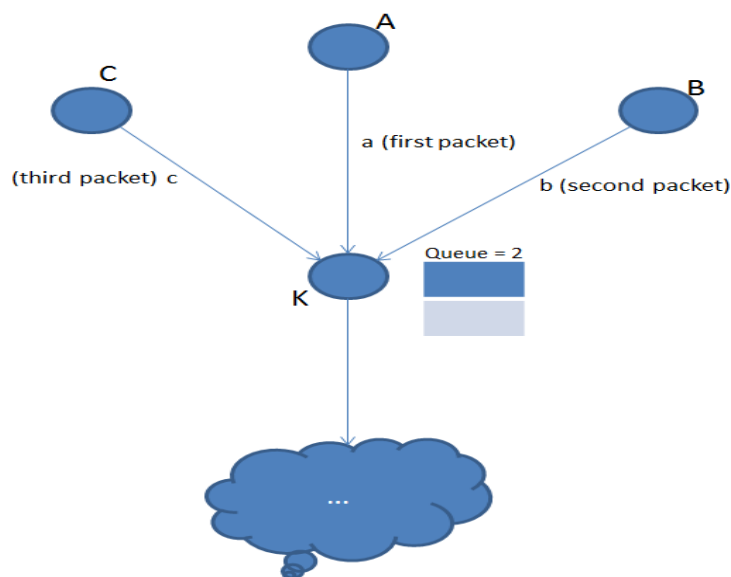
### 5.1.3 Αξιοπιστία σε P2P

Στα P2P δίκτυα, τα πακέτα χάνονται λόγω απωλειών μετάδοσής τους και από τους κόμβους αλλά και από σφάλματα κατά την μετάδοση στο δίκτυο με αποτέλεσμα να απορρίπτονται. Χωρίς κωδικοποίηση, μερικά κομμάτια του αρχείου που διανέμονται γίνονται σπάνια. Τέτοια κομμάτια (fragments) μπορεί να χαθούν για πάντα, εάν λίγοι κόμβοι που τους έχουν απενεργοποιηθούν ή αφήσουν το δίκτυο διανομής.

Με την κωδικοποίηση, λόγω του γραμμικού συνδυασμού (δηλ. όταν μεταφέρονται σε ένα πλαίσιο πακέτου συνδυασμός περισσότερων από ένα πακέτο με την πράξη xor), τα αρχικά block (πακέτο) αρχείων αντιπροσωπεύονται σε ένα μεγαλύτερο αριθμό πακέτων, και ως εκ τούτου η πιθανότητα μειώνεται για οποιοδήποτε συγκεκριμένο block να γίνει σπάνιο.

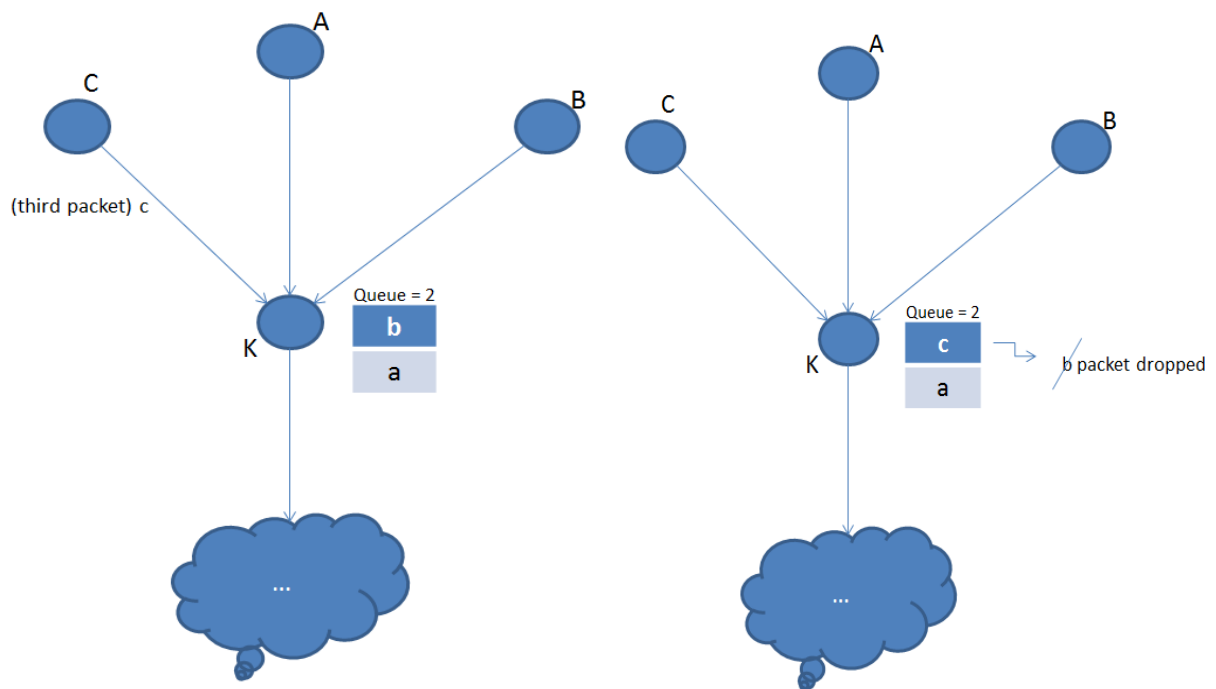
Για να καταλάβουμε διαισθητικά την απώλεια σπάνιων πακέτων που αναφέραμε παραπάνω, ας υποθέσουμε το παρακάτω P2P δίκτυο, όπου τα πακέτα που στέλνονται από τον Κόμβο Α έχουν μεγαλύτερη προτεραιότητα (π.χ. διότι θεωρείται πιο σημαντικός κόμβος και στέλνει περισσότερη χρήσιμη πληροφορία) προώθησης στον κόμβο Κ σε σύγκριση με την προτεραιότητα των πακέτων που στέλνονται από τους κόμβους C και B. Επίσης, τα πακέτα που στέλνονται από τον Κόμβο C έχουν μεγαλύτερη προτεραιότητα προώθησης σε σύγκριση με την προτεραιότητα των πακέτων που στέλνονται από τον κόμβο B. Για απλοποίηση, υποθέτουμε πως το πλήθος των θέσεων μνήμης στην ουρά προτεραιότητας πακέτων στον κόμβο Κ, είναι ίσον με δύο.

Θεωρούμε πως, η σειρά με την οποία τα πακέτα φτάνουν στον κόμβο Κ είναι πρώτα από τον κόμβο Α και έπειτα από τους κόμβους Β και C.

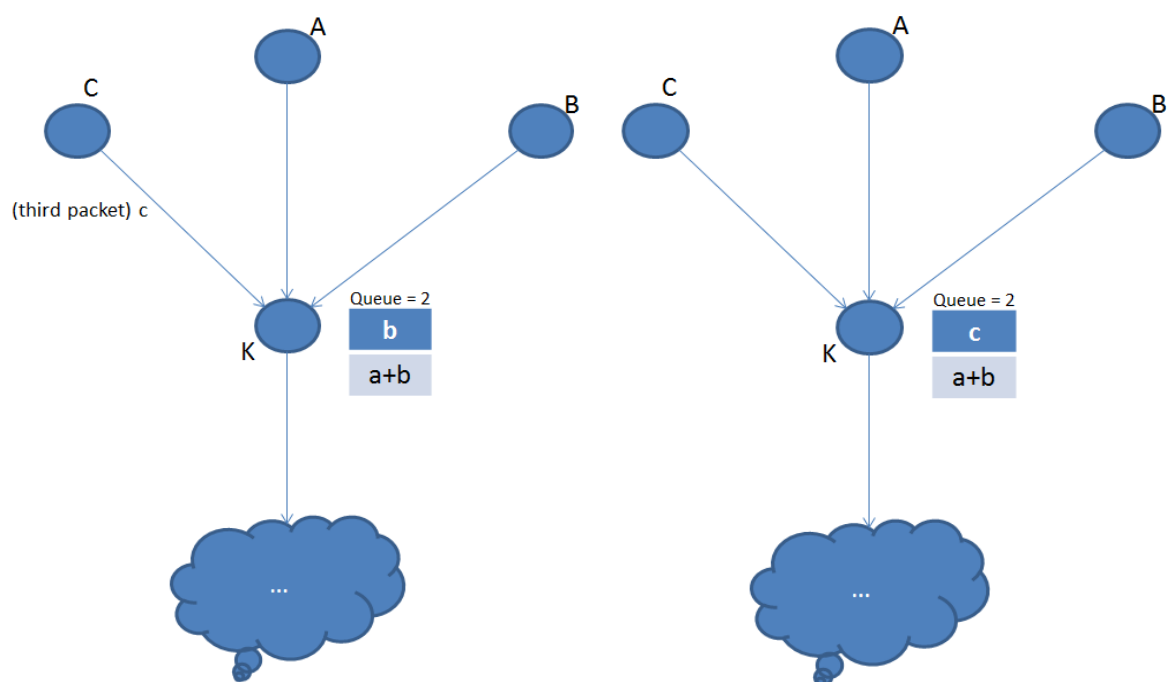


Θεωρούμε πως τα πακέτα a και b φτάνουν ταυτόχρονα και τοποθετούνται στην ουρά με την εξής προτεραιότητα, πρώτα το πακέτο a και μετά το πακέτο b. Πριν προωθηθεί το πακέτο a στους επόμενους κόμβους στο δίκτυο, φτάνει το πακέτο c, με αποτέλεσμα να γίνεται drop του πακέτου b λόγω της χαμηλότερης προτεραιότητας που έχει σε σύγκριση με το πακέτο c.





Η διαδικασία αυτή επαναλαμβάνεται, με συνέπεια το πακέτο b να χάνεται συνέχεια και να μην προωθείται ποτέ από τον κόμβο K. Έτσι τα πακέτα από τον κόμβο B γίνονται σπάνια. Με την χρήση της κωδικοποίησης, αυτό το πρόβλημα λύνεται διότι όταν φτάνουν τα πακέτα a και b στον K, κωδικοποιούνται με γραμμικό συνδυασμό και κατά συνέπεια ο συνδυασμός αυτός θα προωθηθεί. Δηλ. ο γραμμικός συνδυασμός που προωθείται είναι αποτέλεσμα του πακέτου a και b. Αυτό σημαίνει πως πλέον , μεταφέρεται και το πακέτο b που αποτελούσε σπάνια πληροφορία χωρίς κωδικοποίηση.



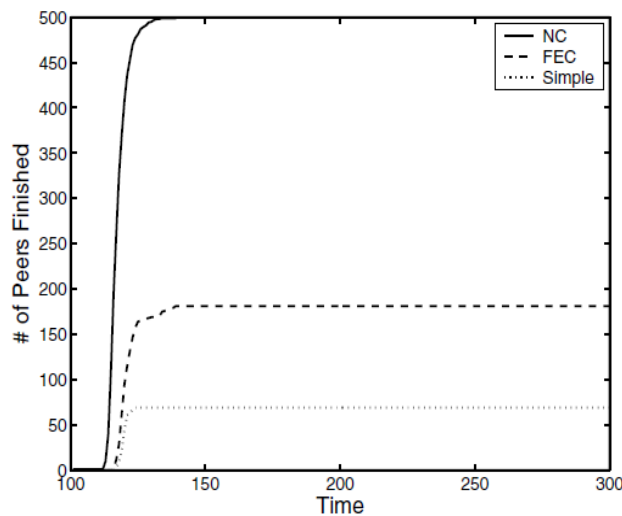
#### **5.1.4 Η Πρακτική Βελτίωση που προσφέρει η Κωδικοποίηση Δικτύου πάνω στην μελέτη μιας προσομοίωσης**

Για μια προσομοίωση που μελετήθηκε, το παρακάτω σχήμα παρουσιάζει την εξέταση κατά πόσοι peers είχαν την δυνατότητα να ολοκληρώσουν το κατέβασμα ενός αρχείου, στην περίπτωση όπου ο κάθε peer αποσυνδεόταν από το δίκτυο διανομής, όταν μετέδιδε μόνο μια φορά όλα τα πακέτα ενός ολόκληρου αρχείου που είχε στην διάθεσή του.

Τα αποτελέσματα της προσομοίωσης συγκρίνει τρία συστήματα:

- ένα που απασχολεί κωδικοποίησης δικτύου (NC),
- μια όπου ο peer στέλνει πακέτο κωδικοποιημένα με μοντέλο forward error correction (FEC), αλλά διαβιβάζει απλά πακέτα στους επόμενους peers
- και ένα "απλό" σύστημα, όπου τα δεδομένα στέλνονται ακωδικοποίητων στους peers

Παρατηρείται ότι, σε αντίθεση με την κωδικοποίηση του δικτύου, στα άλλα δύο συστήματα η πλειοψηφία των κόμβων δεν είναι σε θέση να ολοκληρώσει το κατέβασμα.



Αριθμός κόμβων που είναι σε θέση να ολοκληρώσουν το κατέβασμα ενός ολόκληρου αρχείου, σε ένα σύστημα όπου ο κάθε peer αφήνει το δίκτυο μετά από την μετάδοση όλο του αρχείου που διαθέτει. Συνολικός αριθμός των peers είναι 500.

## 5.2 Εφαρμογή σε ασύρματη διάδοση και Multi- channel ασύρματη διάδοση

Multi- channel = έχει την σημασία του δίαυλου επικοινωνίας μεταξύ των κόμβων.

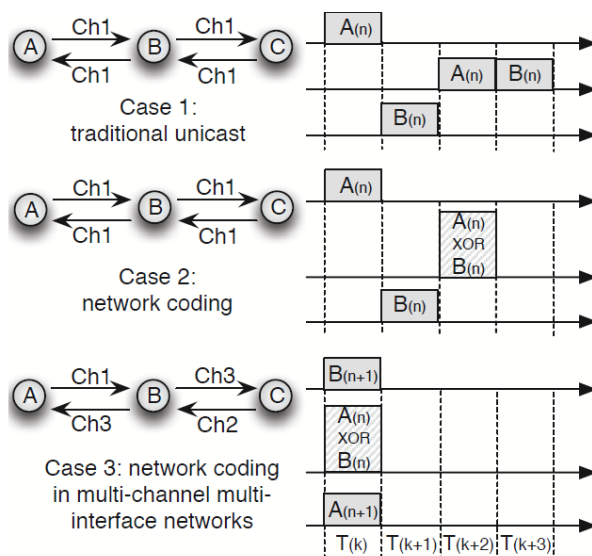
multi-channel multi-interface wireless mesh networks\_:

Η κωδικοποίηση δικτύου, είναι σε θέση να αυξήσει περαιτέρω τη χωρητικότητα των δικτύων πλέγματος πολλαπλών καναλιών. Ως εκ των προτέρων αξιολόγηση, θεωρούμε σαν απλούστερη μορφή της κωδικοποίησης δικτύου, την κωδικοποίηση πάνω στο  $GF(2)$  (πεδίο Galois με δυο στοιχεία) η οποία επιτρέπει στους ενδιάμεσους κόμβους αναμετάδοσης να κάνουν ευκαιριακά XOR εισερχόμενων πακέτων που κατευθύνονται προς άλλους, αυτοί βασίζονται σε προγενέστερη γνώση της αποκωδικοποίησης στους προοριζόμενους μεταγενέστερους κόμβους. Οι κόμβοι κωδικοποίησης μεταδίδουν τα κωδικοποιημένα πακέτα σε όλους τους μεταγενέστερους κόμβους, έτσι έχουμε μείωση του αριθμού των μεταδόσεων σε σύγκριση με τις παραδοσιακές δρομολόγησης. Ως μια διαισθητική αιτιολόγηση της κωδικοποίησης δικτύου στα πολυκάναλα ασύρματα δίκτυα πλέγματος, εξετάστε το σενάριο στο σχήμα. 1, όπου οι κόμβοι A και C σκοπεύουν να ανταλλάξουν τα πακέτα ο ένας με τον άλλον μέσω ενός κοινού ενδιάμεσου διαβιβαστή B. Με την παραδοσιακή δρομολόγηση, έχουμε 4 slots στον χρόνο που απαιτούνται για να ολοκληρωθεί η ανταλλαγή πακέτων. Χρησιμοποιώντας XOR κωδικοποίηση δικτύου, απαιτούνται μόνο 3 slots στον χρόνο. Κατά την εφαρμογή κωδικοποίησης δικτύου στα πολυκάναλα ασύρματα δίκτυα πλέγματος, ωστόσο, ο χρόνος μετάδοσης είναι μόνο 1 slot αφού η μετάδοση των πακέτων από τον A και C μπορεί να επικαλύπτεται με τη μετάδοση των προηγούμενων κωδικοποιημένων πακέτων.

Στην 1<sup>η</sup> περίπτωση: η διασύνδεση μεταξύ του κόμβου A - B και B - C γίνεται με την χρήση εξυπηρέτησης ενός διαύλου επικοινωνίας.

Στην 2<sup>η</sup> περίπτωση: είναι η ίδια με την 1<sup>η</sup> περίπτωση με εφαρμογή network coding

Στην 3<sup>η</sup> περίπτωση: η διασύνδεση μεταξύ του κόμβου A - B και B - C γίνεται με την χρήση εξυπηρέτησης τριών διαύλων επικοινωνίας και με εφαρμογή network coding.



Σχ. 1. Το άνωθεν σενάριο αποδεικνύει τα οφέλη της κωδικοποίησης δικτύου σε ευρυεκπομπή πολλαπλής διασύνδεσης σε ασύρματα δίκτυα πλέγματος.

### 5.3 Η χρησιμότητα της κωδικοποίησης δικτύου σε δίκτυα Wimax

Η Hybrid Automatic Repeat reQuest ([HARQ](#)) χρησιμοποιείται για να μεταδώσει τα πακέτα δεδομένων με αξιοπιστία. Ωστόσο, θυσιάζει την ανθεκτικότητα σε χρονικά μεταβαλλόμενα κανάλια, και μπορεί να αξιοποιήσει το ασύρματο μέσο στις περιπτώσεις των multi-path και multi-hop μεταδόσεων.

Η Τυχαία κωδικοποίηση δικτύου αποτελεί βασικό συστατικό στο σχεδιασμό του MRNC (MAC-layer Random Network Coding. A simple MAC-layer protocol) και λόγω αυτής διαμορφώνονται κάποια πλεονεκτήματα που δεν προσφέρει το HARQ.

#### πώς χρησιμοποιείται η κωδικοποίηση δικτύου σε MRNC;

Θα Δειχθεί ότι η τυχαία κωδικοποίηση δικτύου είναι πράγματι χρήσιμη όταν εφαρμόζεται σε WiMAX συστήματα στο πλαίσιο των τριών διαφορετικά σεναρίων: μεταδόσεις single-hop, handovers, και μεταδόσεις multi-hop.

**Single-hop Transmissions:** Στο [HARQ](#) οι πληροφορίες είναι οι πρώτες που κωδικοποιούνται. Ο αποστολέας μεταδίδει μόνο τα bits που πρέπει κανονικά να μεταδοθούν, και όταν λαμβάνει από τον δέκτη αρνητική ανάδραση (δηλαδή ότι υπήρξε κάποιο σφάλμα στο πακέτο που δέχτηκε) μεταδίδει ξανά το πακέτο. Μετά την παραλαβή του πακέτου χωρίς σφάλμα πραγματοποιείται συνδυασμός μεταξύ του “πακέτου με το σφάλμα” και του “πακέτου χωρίς σφάλμα”. Αυτή η διαδικασία συνεχίζεται έως ότου το πακέτο αποκωδικοποιηθεί σωστά ή επιτευχθεί ο μέγιστος αριθμός αναμεταδόσεων.

Το HARQ έχει επιβάρυνση στην κυκλοφορία των πακέτων λόγω των αναμεταδόσεων των πακέτων και των πακέτων ACK/NACK. Στο WiMAX, ο κινητός σταθμός μπορεί να έχει υψηλό βαθμό κινητικότητας, οδηγώντας έτσι σε διακυμάνσεις ποιότητας του καναλιού με την πάροδο του χρόνου. Τα ACK/NACK πακέτα μπορεί επίσης να εμφανίζουν σφάλματα και καθυστερήσεις που οφείλονται σε κακές συνθήκες του καναλιού. Σφάλματα και απώλειες στα (ACK) πακέτα οδηγούν σε πρόσθετες περιττές μεταδόσεις πακέτων. Για να διασφαλίσει την αξιοπιστία του το HARQ μειώνει την ανθεκτικότητά του σε πραγματικά κανάλια με κυμαινόμενη ποιότητα στην πάροδο του χρόνου. Η τυχαία κωδικοποίηση δικτύου προσφέρει μια απλή λύση σε αυτά τα προβλήματα.

Επειδή οι τυχαίοι γραμμικοί κώδικες δεν καθορίζουν το ρυθμό μετάδοσης των δεδομένων, το MRNC είναι σε θέση να προσαρμόζει το ρυθμό μετάδοσης δεδομένων ώστε να συμπίπτει με το διαθέσιμο εύρος ζώνης που καθορίζεται από τις συνθήκες του δικτύου με την πάροδο του χρόνου. Με το MRNC, ο αποστολέας εκπέμπει κωδικοποιημένα μπλοκ, και ο δέκτης πρέπει μόνο να «κρατήσει ένα κάδο» για να “συλλέξει” η γραμμικά ανεξάρτητα μπλοκ, έτσι ώστε να είναι σε θέση να ανακτήσει τα αρχικά δεδομένα που στάλθηκαν. Ο δέκτης δεν είναι απαραίτητο να μεταδώσει τα ACK / NACK πακέτα με κάθε κωδικοποιημένο μπλοκ και ο αποστολέας δεν είναι απαραίτητο να μεταδώσει επιπλέον πακέτα όταν συμβαίνουν σφάλματα. Το MRNC είναι σε θέση να προσφέρει ανθεκτικές μεταδόσεις, λόγω της εγγενούς ανθεκτικότητας σε λάθη που έχει από τους τυχαίους γραμμικούς κώδικες που δεν καθορίζουν το ρυθμό μετάδοσης των δεδομένων. Ακόμα κι αν ένα συγκεκριμένο κωδικοποιημένο πακέτο χαθεί, το επόμενο κωδικοποιημένο που θα ληφθεί φέρει εξίσου πληροφορία και είναι εξίσου χρήσιμο.

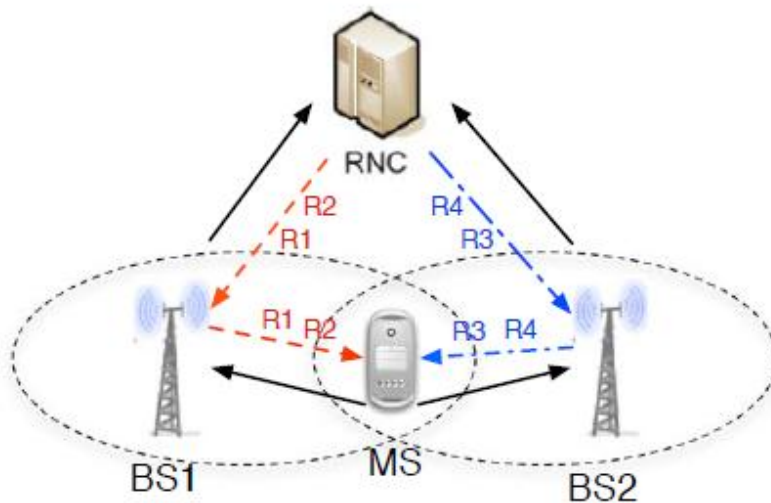
**Handovers:** Η [Μεταπομπή](#) αποτελεί μια βασική λειτουργία των WiMAX και συμβάλλει στην αντιμετώπιση προβλημάτων που προκύπτουν από την κίνηση των χρηστών. Είναι μια διαδικασία όπου ένας κινητός σταθμός μεταφέρεται από μια [διασύνδεση](#) ενός σταθμού βάσης σε μια άλλη διασύνδεση που παρέχεται από άλλο σταθμό βάσης. Πρόσφατα έγινε εφικτό ένας κινητός σταθμός να συνδέεται ταυτόχρονα με δύο ή περισσότερους κινητούς σταθμούς κατά τη διάρκεια μιας κλήσης(**Soft handover**), το λεγόμενο Macro Diversity Handover (MDHO).

Οι κινητοί σταθμοί που υποστηρίζουν MDHO, διατηρούν σύνδεση με ένα ενεργό σύνολο από σταθμούς βάσης που εμπλέκονται στο MDHO. Όταν η ισχύς ενός ορισμένου σταθμού βάσης του σήματος ξεπερνά ένα όριο (H\_Add), αυτός ο σταθμός βάσης προστίθεται στο ενεργό σύνολο των κινητών σταθμών. Από την άλλη πλευρά, ένας σταθμός βάσης θα πρέπει να αφαιρεθεί από το ενεργό σύνολο των κινητών σταθμών εάν η ισχύς του γίνει μικρότερη από μία ορισμένη τιμή κατωφλίου (H\_Delete). Με το μηχανισμό αυτό, ο κινητός σταθμός ενημερώνει το ενεργό σύνολο των σταθμών περιοδικά ελέγχοντας την ισχύ του σήματος. Στην περιοχή μεταπομπής, ο κινητός σταθμός συνεργάζεται με όλους τους σταθμούς βάσης που ανήκουν στο ενεργό σύνολο και ορίζει [συνδέσεις](#)

καθόδου με αυτούς τους σταθμούς βάσης μέσω ξεχωριστών καναλιών που υποστηρίζονται από OFDM / OFDMA σε WiMAX φυσικό επίπεδο. Η σύνδεση ανόδου (uplink) επικοινωνίας ορίζεται από το ίδιο κανάλι σε όλους τους σταθμούς βάσης που σχετίζονται με τον κινητό σταθμό. Κάθε τέτοια σύνδεση ανόδου του κινητού σταθμού αναμεταδίδεται ταυτόχρονα από τους σταθμούς βάσης σε ένα Radio Network Controller (RNC), το οποίο συνδέεται με όλους τους σταθμούς βάσης. Οι μεταδόσεις πρέπει να συγχρονιστούν έχοντας όλοι οι σταθμοί βάσης το ίδιο MAC / PHY PDUs για να μεταδώσουν στον κινητό σταθμό ταυτόχρονα.

Με την τυχαία κωδικοποίηση δικτύου αξιοποιούμε πλήρως το διαθέσιμο εύρος ζώνης κάθε σταθμού βάσης, και βελτιώνονται οι ρυθμοί ταυτόχρονης μετάδοσης καθοδικής σύνδεσης στον κινητό σταθμό. Με την τυχαία κωδικοποίηση δικτύου, μπορούν να αποφευχθούν οι προσπάθειες συγχρονισμού, αφού όλα τα κωδικοποιημένα πακέτα θεωρούνται ότι μεταφέρουν εξίσου χρήσιμη πληροφορία. Αξιοποιώντας τις ιδιότητες του OFDM / OFDMA σε WiMAX, κάθε υποκανάλι μπορεί να χρησιμοποιηθεί ξεχωριστά για την μετάδοση διαφορετικών κωδικοποιημένων πακέτων χωρίς να συμβεί καμία σύγκρουση. Στην περίπτωση αυτή, όλοι οι υποδίαυλοι μπορούν να αξιοποιηθούν πλήρως και αυτό ακριβώς είναι και το πλεονέκτημα της κωδικοποίησης δικτύου σε τυπικές περιπτώσεις πολυκάναλης επικοινωνίας (multi-path communication.).

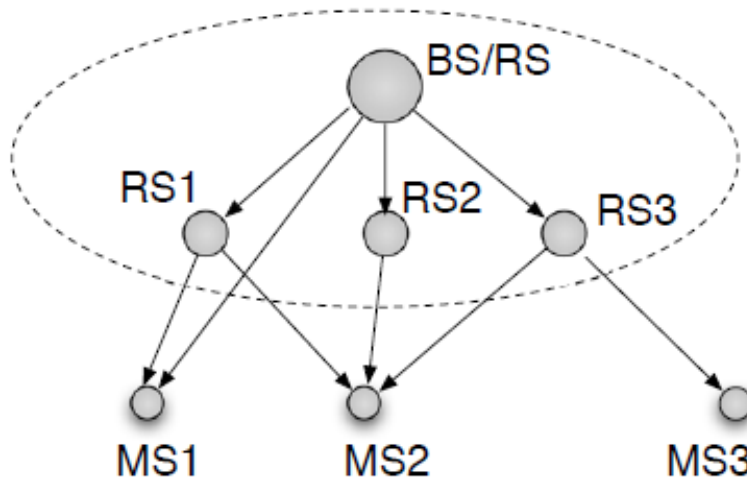
**Το πλεονέκτημα της τυχαίας κωδικοποίησης δικτύου σε ένα WiMAX δίκτυο αμφίδρομης μεταπομπής πακέτων:**



Αφού ο κινητός σταθμός εισέλθει στην περιοχή μεταπομπής, συνδέεται και με τους δύο σταθμούς βάσης (BS1, BS2), στον καθένα μέσω ενός μοναδικού υποδιαύλου που έχει προγραμματιστεί από τον κάθε σταθμό βάσης. Η κωδικοποίηση υλοποιείται στο Radio Network Controller (RNC) και διάφορα γραμμικά ανεξάρτητα κωδικοποιημένα πακέτα στέλνονται στους δύο σταθμούς βάσης ταυτόχρονα. Και οι δύο σταθμοί βάσης στέλνουν τα κωδικοποιημένα πακέτα στον κινητό σταθμό ταυτόχρονα. Ο κινητός σταθμός λαμβάνει αυτά τα κωδικοποιημένα πακέτα και από τους δύο σταθμούς βάσης και απαντά με ένα ACK μέσω του κοινού καναλιού ανερχόμενης ζεύξης αφού έχει λάβει έναν επαρκή αριθμό γραμμικά ανεξάρτητων κωδικοποιημένων πακέτων. Με τον τρόπο αυτό, η τυχαία κωδικοποίηση δικτύου βοηθά να αξιοποιηθεί πλήρως η καθοδική ζεύξη καναλιού κι από τους δύο σταθμούς βάσης.

**Multi-hop Transmissions:** Παρόμοια με την περίπτωση των handovers, όταν ο κινητός σταθμός κινείται σε περιοχή κάλυψης του σταθμού βάσης και του σταθμού αναμετάδοσης (RS, Relay Station), ο κινητός σταθμός είναι σε θέση να επικοινωνεί απευθείας με το σταθμό βάσης, έμμεσα με το σταθμό βάσης μέσω του σταθμού αναμετάδοσης ή και άμεσα και έμμεσα με το σταθμό βάσης.

**Το πλεονέκτημα από τη χρήση τυχαίας κωδικοποίησης δικτύου σε wimax multi-hop transmissions:**



Το HARQ που προτείνεται ειδικά για τη λειτουργία multi-hop στο WiMAX, εκτελείται μεταξύ του σταθμού βάσης (BS) και σταθμού αναμετάδοσης (RS), μεταξύ του σταθμού βάσης (BS) και των κινητών σταθμών (MS), και μεταξύ του σταθμού αναμετάδοσης (RS) και των κινητών σταθμών (MS).

Οι μεταδόσεις επειδή πραγματοποιούνται σε όλες τις συνδέσεις μπορεί να προκαλέσουν πρόσθετη επιβάρυνση στο δίκτυο, καθώς επίσης δεν αξιοποιούνται πλήρως και οι διαθέσιμοι πόροι μέσω των καναλιών μετάδοσης.

Επεκτείνοντας την περίπτωση που αναφέρθηκε παραπάνω για Handovers όλοι οι σταθμοί βάσης και οι σταθμοί αναμετάδοσης με ισχύ μεγαλύτερη του σήματος (H\_Add) διατηρούνται στο ενεργό σύνολο των κινητών σταθμών, οι σταθμοί βάσης και οι σταθμοί αναμετάδοσης με ισχύ μικρότερη του σήματος αφαιρούνται (H\_Delete) από το ενεργό σύνολο περιοδικά.

Με την εφαρμογή τυχαίας κωδικοποίησης δικτύου, ο κινητός σταθμός είναι σε θέση να λαμβάνει κωδικοποιημένα πακέτα από διαφορετικά κανάλια και να δημιουργεί έτσι συνδέσεις με όλους τους σταθμούς βάσης και με όλους τους σταθμούς αναμετάδοσης και μάλιστα με αρκετά ισχυρά σήματα, μέσω των οποίων μεταδίδονται ταυτόχρονα διαφορετικά κωδικοποιημένα πακέτα. Όλες οι μεταδόσεις μέσω των υπο-καναλιών μπορούν να χρησιμοποιηθούν πλήρως και αυτό έχει σαν συνέπεια την αύξηση της απόδοσης. Συνεπώς όλα τα ληφθέντα κωδικοποιημένα πακέτα φέρουν εξίσου χρήσιμη πληροφορία και δεν απαιτείται ούτε συγχρονισμός, ούτε αναμετάδοση.



## **5.4 Τεχνικές μετάδοσης VoIP με κωδικοποίηση δικτύου σε Ασύρματα Δίκτυα Πολλών Αλμάτων**

Ένα πρωτόκολλο δικτύωσης στο οποίο υλοποιήθηκε κωδικοποίηση δικτύου είναι το πρωτόκολλο COPE το οποίο είναι το πρώτο πρωτόκολλο δρομολόγησης που ενσωμάτωσε την κωδικοποίηση δικτύου. Η κωδικοποίηση δικτύου γρήγορα προσέλκυσε το ενδιαφέρον πολλών ερευνητών λόγω των σημαντικών ωφελειών του στην εξοικονόμηση πόρων. Σημαντικοί πόροι όπως το εύρος ζώνης ενός δικτύου αλλά και η ενέργεια των κόμβων εξοικονομούνται με την τεχνική της κωδικοποίησης δικτύου.

### **5.4.1 Τα βασικά χαρακτηριστικά της κωδικοποίησης δικτύου καθώς και το πως αυτή εφαρμόζεται στην πράξη στα ασύρματα δίκτυα:**

Αρχικά οι πρώτες ερευνητικές εργασίες που ασχολήθηκαν με την κωδικοποίηση δικτύου ήταν σε θεωρητικό επίπεδο. Οι περισσότερες από αυτές είχαν ως στόχο να επιτύχουν μέγιστη χωρητικότητα πολυδιανομής σε ασύρματα δίκτυα με την χρησιμοποίηση της κωδικοποίησης δικτύου. Στην συνέχεια αρκετές εργασίες εστίασαν στην πρακτική εφαρμογή της κωδικοποίησης δικτύου σε ασύρματα δίκτυα. Οι εργασίες αυτές ασχολήθηκαν κυρίως με τη βελτίωση ζητημάτων όπως είναι η δρομολόγηση, η ευρεία εκπομπή και η βελτίωση της ρυθμαπόδοσης του δικτύου. Στις εργασίες αυτές χρησιμοποιείται η κωδικοποίηση δικτύου με δύο διαφορετικές κυρίαρχες προσεγγίσεις.

Οι αλγόριθμοι που ακολουθούν την πρώτη προσέγγιση εφαρμόζουν την κωδικοποίηση /αποκωδικοποίηση των πακέτων από άκρο-σε- άκρο του δικτύου και οι αλγόριθμοι που ακολουθούν την δεύτερη προσέγγιση εφαρμόζουν κωδικοποίηση/αποκωδικοποίηση σε κάθε άλμα.

Στην κωδικοποίηση/αποκωδικοποίηση από άκρο σε άκρο η φιλοσοφία της τεχνικής βασίζεται στην εξάπλωση όσο το δυνατόν περισσότερων κωδικοποιημένων πακέτων σε όλο το δίκτυο με στόχο την παράδοση στους ενδεχόμενους παραλήπτες όσο το δυνατόν περισσότερων κωδικοποιημένων πακέτων. Βασική υπόθεση της προσέγγισης αυτής αποτελεί ότι ο καθένας παραλήπτης με τη συγκέντρωση επαρκούς αριθμού κωδικοποιημένων πακέτων θα είναι σε θέση να αποκωδικοποιήσει τα αρχικά πακέτα που προορίζονται γι' αυτόν. Σ' αυτού του είδους τις τεχνικές επιτρέπεται η περαιτέρω κωδικοποίηση ήδη κωδικοποιημένων πακέτων στους ενδιάμεσους κόμβους με σκοπό την αύξηση του κέρδους από την κωδικοποίηση. Οι περισσότεροι αλγόριθμοι που έχουν προταθεί με κωδικοποίηση από άκρο σε άκρο στηρίζονται στη γνώση της τοπολογίας του δικτύου για την λειτουργία τους. Αυτό το χαρακτηριστικό καθιστά την τεχνική αυτή δύσκολα εφαρμόσιμη σε ασύρματα δίκτυα όπου υπάρχει κινητικότητα ([MANETs](#)). Σε τέτοιου είδους δίκτυα χρησιμοποιείται κυρίως η τεχνική κωδικοποίησης/ αποκωδικοποίησης σε κάθε άλμα.

Η τεχνική κωδικοποίησης/ αποκωδικοποίησης σε κάθε άλμα βασίζεται στην απαίτηση κάθε κωδικοποιημένο πακέτο να μεταδίδεται μόνο για ένα άλμα. Ωστόσο, η αποκωδικοποίηση σε αυτό το άλμα θα πρέπει να είναι εγγυημένη για όλους τους επόμενους κόμβους. Κάθε ενδιάμεσος κόμβος του δικτύου όταν αποκωδικοποιήσει τα πακέτα σωστά μπορεί να δημιουργήσει νέες κωδικοποιήσεις πακέτων ενός άλματος. Η τεχνική αυτή βασίζεται στην ύπαρξη πολλαπλών ροών πακέτων σε ενδιάμεσους κόμβους με διαφορετικούς παραλήπτες. Πακέτα των ροών αυτών μπορεί να κωδικοποιηθούν σε κάποιον ενδιάμεσο κόμβο με την προϋπόθεση ότι είναι διαφορετικά τα μονοπάτια τους στο επόμενο άλμα. Στον κόμβο του επόμενου άλματος είναι αναγκαία η αποκωδικοποίηση τους. Εάν δεν συμβεί η αποκωδικοποίηση υπάρχει η πιθανότητα προώθησης πακέτων σε μέρη του δικτύου που δεν υπάρχει ενδιαφερόμενος παραλήπτης, σπαταλώντας άσκοπα το εύρος ζώνης του δικτύου.

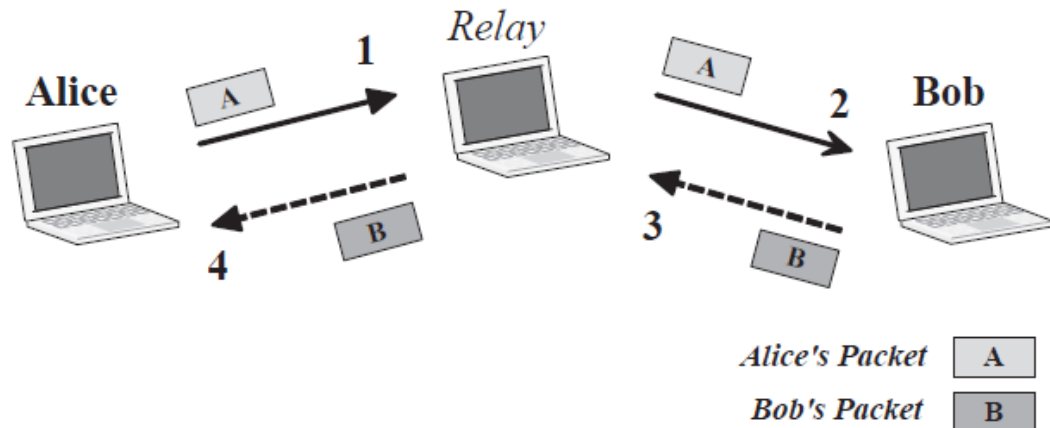
Στην τεχνική κωδικοποίησης/αποκωδικοποίησης σε κάθε άλμα στηρίζεται και ο αλγόριθμος COPE. Ο αλγόριθμος αυτός είναι ο πρώτος που ενσωμάτωσε την κωδικοποίηση δικτύου για βελτίωση της δρομολόγησης σε ένα MANET. Στη συνέχεια γίνεται μία λεπτομερής περιγραφή του αλγορίθμου αυτού και του τρόπου με τον οποίο υλοποιεί την κωδικοποίηση δικτύου.

Η πρώτη απόπειρα να μεταφέρουν την κωδικοποίηση δικτύου από την θεωρία στην πράξη στα ασύρματα δίκτυα (Κωδικοποίηση/Αποκωδικοποίηση σε κάθε άλμα):

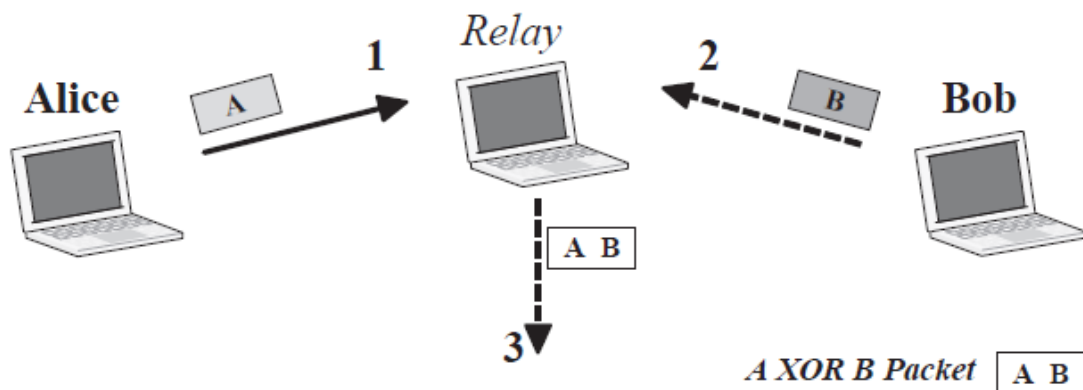
Ο αλγόριθμος που παρουσιάζεται στοχεύει στη μεγιστοποίηση της ρυθμαπόδοσης ενός ασύρματου δικτύου. Αυτό το καταφέρνει χρησιμοποιώντας την κωδικοποίηση των πακέτων στους κόμβους του



δικτύου όπως φαίνεται στο παρακάτω σχήμα. Σε αυτό το σχήμα παρουσιάζεται ένα απλό παράδειγμα επικοινωνίας δύο κόμβων ανταλλάσσοντας πακέτα με την βοήθεια ενός ενδιάμεσου δρομολογητή.



**Σχήμα (α):** Αποστολή μηνυμάτων μεταξύ της Alice και του Bob με την παραδοσιακή επικοινωνία



**Σχήμα (β):** Αποστολή μηνυμάτων μεταξύ της Alice και του Bob με το COPE

Στην παραδοσιακή επικοινωνία, σχήμα (α), η Alice στέλνει το πακέτο της στον δρομολογητή, ο οποίος το προωθεί στον Bob. Ο Bob με την σειρά του στέλνει το πακέτο του στον δρομολογητή, ο οποίος το προωθεί στην Alice. Για την ολοκλήρωση της επικοινωνίας απαιτούνται τεσσερις ξεχωριστές μεταδόσεις. Ας θεωρήσουμε τώρα την προσέγγιση με την χρήση της κωδικοποίησης δικτύου όπως το σχήμα (β). Η Alice και ο Bob στέλνουν σε ξεχωριστές μεταδόσεις ο καθένας το πακέτο στον δρομολογητή. Ο δρομολογητής με τη σειρά του συνδυάζει τα πακέτα με την πράξη XOR και στη συνέχεια στέλνει με broadcast μετάδοση το κωδικοποιημένο πακέτο. Η Alice και ο Bob αποκτούν τα πακέτα που προορίζονται για αυτούς χρησιμοποιώντας την πράξη XOR στο κωδικοποιημένο και το δικό τους πακέτο. Σε αυτήν την περίπτωση οι μεταδόσεις που χρειάζονται είναι τρεις. Οι μεταδόσεις που εξοικονομούνται μπορούν να χρησιμοποιηθούν για την αποστολή νέων πακέτων, αυξάνοντας έτσι την ρυθμαπόδοση του ασύρματου δικτύου. Ο αλγόριθμος COPE χρησιμοποιεί την τεχνική συνδυασμού πακέτων bitwise XOR. Επίσης ενσωματώνει τρεις βασικές τεχνικές για την λειτουργία του, οι οποίες περιγράφονται παρακάτω:

Opportunistic Listening: Λόγω της φύσης του κοινού μέσου κάθε κόμβος έχει την ευκαιρία να κρυφακούει πακέτα που μεταδίδονται στο δίκτυο. Το COPE θέτει τους κόμβους σε λειτουργία promiscuous, όπου ο κάθε κόμβος ακούει πακέτα που μεταδίδονται μεταξύ των κόμβων στην εμβέλεια του. Τα πακέτα αυτά αποθηκεύονται για ένα μικρό χρονικό διάστημα ( $T=0.5$  sec). Σκοπός είναι κάθε κόμβος να συλλέξει αρκετά πακέτα ώστε να μεγιστοποιήσει την δυνατότητα αποκωδικοποίησης ενός πακέτου. Επιπλέον κάθε κόμβος μεταδίδει σε όλους τους γείτονές του μία

σύνοψη των πακέτων που έχει καταγράψει (reception reports). Τα reception reports αποστέλλονται είτε με την χρησιμοποίηση κανονικών πακέτων(big-gyback) είτε με την χρήση περιοδικών μηνυμάτων ελέγχου.

Opportunistic Coding: Το ζητούμενο κατά την κωδικοποίηση είναι η εύρεση των πακέτων που πρέπει να συνδυαστούν ώστε να μεγιστοποιηθεί η ρυθμαπόδοση. Ένας κόμβος μπορεί να έχει πολλαπλές επιλογές συνδυασμού πακέτων. Ωστόσο, θα πρέπει να στοχεύει στην μεγιστοποίηση του αριθμού των απλών (native) πακέτων που κωδικοποιούνται εξασφαλίζοντας παράλληλα ότι κάθε κόμβος παραλήπτης έχει επαρκή πληροφορία για την αποκωδικοποίηση. Ο αλγόριθμος κωδικοποίησης θα πρέπει να εγγυάται ότι όλοι οι κόμβοι που είναι παραλήπτες κάποιου από τα πακέτα που περιέχονται στο κωδικοποιημένο πακέτο μπορούν να αποκωδικοποιήσουν και να ανακτήσουν το πακέτο που τους ενδιαφέρει. Αυτό επιτυγχάνεται ακολουθώντας τον παρακάτω απλό κανόνα:

Για να μεταδοθούν  $n$  πακέτα,  $p_1, \dots, p_n$ , σε  $n$  nexthops,  $r_1, \dots, r_n$  ένας κόμβος μπορεί να συνδυάσει μαζί τα  $n$  πακέτα με XOR, μόνο εάν κάθε nexthop  $r_i$  γνωρίζει όλα τα  $n-1$  πακέτα  $p_j$  με  $j \neq i$

Γίνεται φανερό ότι κάθε φορά που ένας κόμβος έχει την ευκαιρία για μετάδοση, στόχος του είναι η εύρεση του μεγαλύτερου  $n$  που ικανοποιεί τον παραπάνω κανόνα ώστε να μεγιστοποιήσει το όφελος από την κωδικοποίηση.

Learning Neighbor State: είναι φανερό ότι για την κωδικοποίηση των πακέτων, ένας κόμβος θα πρέπει να γνωρίζει τα πακέτα που έχουν καταγράψει οι γείτονες του. Όπως αναφέρθηκε παραπάνω, αυτό γίνεται με την μετάδοση μηνυμάτων reception reports. Ωστόσο, σε περιπτώσεις που υπάρχει συμφόρηση στο δίκτυο τα μηνύματα αυτά μπορεί να χαθούν λόγω των συγκρούσεων ενώ σε περιπτώσεις όπου στο δίκτυο υπάρχει ελάχιστος φόρτος δικτύου, τα μηνύματα αυτά μπορεί να φτάσουν πολύ αργά δηλαδή όταν ένας κόμβος έχει πάρει ήδη μία απόφαση κωδικοποίησης, η οποία δεν είναι η καλύτερη. Γι' αυτό το λόγο οι κόμβοι δεν πρέπει να βασίζονται εξολοκλήρου στα reception reports αλλά χρειάζεται να προβλέπουν εάν ένας γείτονας τους γνωρίζει κάποιο συγκεκριμένο πακέτο. Για την πραγματοποίηση αυτής της πρόβλεψης με έξυπνο τρόπο χρησιμοποιούνται πληροφορίες από το πρωτόκολλο δρομολόγησης. Συγκεκριμένα, το COPE υπολογίζει την πιθανότητα ένας γείτονας ενός κόμβου να έχει ένα πακέτο ως την πιθανότητα παράδοσης του συνδέσμου(link) μεταξύ του προηγούμενου κόμβου του πακέτου και του γειτονικού κόμβου. Αυτή η πιθανότητα υπολογίζεται και χρησιμοποιείται από το πρωτόκολλο δρομολόγησης για κάθε link μετάδοσης στο ασύρματο δίκτυο. Μερικές φορές ένας κόμβος μπορεί να πραγματοποιήσει μία λάθος υπόθεση η οποία μπορεί να προκαλέσει με αποτυχία αποκωδικοποίησης σε κάποιον ενδιαμέσο κόμβο. Σε αυτές τις περιπτώσεις το native πακέτο επαναμεταδίδεται πιθανόν κωδικοποιημένο με ένα νέο σύνολο πακέτων.

Κατά τη λειτουργία του αλγόριθμου κωδικοποίησης στο COPE ακολουθούνται μερικές βασικές σχεδιαστικές αρχές. Καταρχήν, η κωδικοποίηση στηρίζεται στην παραδοχή ότι ποτέ τα πακέτα δεν καθυστερούνται σκόπιμα. Όταν ένας κόμβος κατέχει το δικαίωμα εκπομπής παίρνει το πρώτο πακέτο από την ουρά εξόδου. Στην συνέχεια ελέγχει ποιά άλλα πακέτα μπορούν να κωδικοποιηθούν με αυτό το πακέτο και όταν γίνει η κατάλληλη επιλογή τα πακέτα αυτά κωδικοποιούνται με XOR. Εάν δεν υπάρχουν ευκαιρίες κωδικοποίησης ή δεν υπάρχουν διαθέσιμα πακέτα στην ουρά εξόδου ο κόμβος δεν περιμένει για την άφιξη νέων πακέτων με σκοπό την κωδικοποίηση. Δεύτερο, το COPE δείχνει προτίμηση στην κωδικοποίηση πακέτων με ίδιο ή παρόμοιο μέγεθος έτσι ώστε να μεγιστοποιηθεί το όφελος από την κωδικοποίηση. Τέλος, το COPE δεν κωδικοποιεί μαζί πακέτα τα οποία προορίζονται στον ίδιο κόμβο του επόμενου άλματος επειδή ο κόμβος αυτός δεν θα μπορεί να πραγματοποιήσει την αποκωδικοποίηση αυτών των πακέτων.

#### 5.4.2 Ενσωμάτωση της κωδικοποίησης δικτύου στη μετάδοση VoIP

Η τεχνολογία VoIP τυγχάνει μεγάλης απήχησης για την πραγματοποίηση κλήσεων ομιλίας και την μετάδοση της φωνής. Εκτός από τα ενσύρματα δίκτυα σημαντικό κομμάτι στη μετάδοση VoIP έχουν και τα ασύρματα δίκτυα τα οποία αναπτύσσονται με ραγδαίους ρυθμούς. Είτε στα δίκτυα κορμού είτε μέχρι τον τελικό χρήστη τα ασύρματα δίκτυα συμβάλλουν στην μεταφορά VoIP με σκοπό να παρέχουν ευελιξία και χαμηλό κόστος στους παρόχους και τους τελικούς χρήστες. Προκύπτει πρόβλημα όταν μεταδίδονται πακέτα VoIP σε ασύρματα ad-hoc δίκτυα πολλών αλμάτων. Το χαρακτηριστικό μιας κλήσης VoIP είναι ότι η φωνή μεταδίδεται σε πολλά μικρά πακέτα τα οποία εισάγονται στο δίκτυο. Όταν οι κλήσεις αυξάνονται και τα πακέτα πληθαίνουν παρατηρείται συμφόρηση στους κόμβους ενός τέτοιου δικτύου. Το γεγονός αυτό δημιουργεί καθυστέρηση και απώλειες πακέτων. Αποτέλεσμα αυτού είναι η ποιότητα των κλήσεων ομιλίας να υποβαθμίζεται σημαντικά. Το πρόβλημα αυτό οφείλεται κυρίως στον μηχανισμό ανταγωνισμού για την πρόσβαση στο κοινό μέσο μεταξύ των κόμβων ενός δικτύου που επιθυμούν να μεταδώσουν. Με τον μηχανισμό αυτό οι κόμβοι σπαταλούν περισσότερο χρόνο μέχρι να αποφασίσουν ποιος θα μεταδώσει παρά για την πραγματική μετάδοση των δεδομένων φωνής. Μια σημαντική κατηγορία τεχνικών που έχουν προταθεί για τη βελτίωση του συγκεκριμένου προβλήματος είναι οι τεχνικές συνάθροισης των πακέτων. Οι τεχνικές αυτές έχουν ως στόχο τη μείωση του αριθμού των πακέτων που εκπέμπονται με τη συνάθροιση πολλαπλών πακέτων σε ένα. Αν και βελτιώνουν σημαντικά την μετάδοση VoIP σε ένα ασύρματο δίκτυο, ωστόσο οι τεχνικές αυτές έχουν περιορισμένη απόδοση λόγω της σημαντικής αύξησης που παρουσιάζουν στο μέγεθος των πακέτων που δημιουργούν.

Η περαιτέρω βελτίωση των αλγορίθμων μετάδοσης VoIP μπορεί να επιτευχθεί με την χρήση τεχνικών που προέρχονται από τη Θεωρία Πληροφορίας. Μια τέτοια τεχνική είναι η κωδικοποίηση δικτύου που προδιαγράφει ότι δύο ή περισσότερα πακέτα μπορούν να κωδικοποιηθούν, να μεταδοθούν μέσα από ένα δίκτυο και να αποκωδικοποιηθούν στον παραλήπτη με αποτέλεσμα την εξοικονόμηση πόρων. Παρουσιάζονται τρεις αλγόριθμοι που χρησιμοποιούν την κωδικοποίηση δικτύου για τη βελτίωση του προβλήματος μετάδοσης της φωνής. Οι αλγόριθμοι αυτοί είναι ο NCA(Network Coding - Aggregation), NCA-P (Network Coding – Aggregation - Progressive) και ο NCA-FS (Network Coding – Aggregation- Failure Salvation).

Network Coding – Aggregation: Ο αλγόριθμος NCA χρησιμοποιεί την κωδικοποίηση δικτύου για τη μείωση των μεταδόσεων με την κωδικοποίηση πολλαπλών πακέτων. Επιπλέον, ο NCA χρησιμοποιεί την τεχνική συνάθροισης πακέτων σε συνδυασμό με την κωδικοποίηση ώστε να καταφέρει να αυξήσει το κέρδος από τον συνδυασμό πολλών πακέτων σε περιπτώσεις που η εύρεση κωδικοποιήσεων περιορίζεται λόγω συγκεκριμένων συνθηκών του δικτύου. Μέσω πειραματικών μετρήσεων αποδείχθηκε ότι ο αλγόριθμος NCA έχει καλύτερη απόδοση σε σχέση με τον αλγόριθμο HHA, που είναι ο αποδοτικότερος αλγόριθμος συνάθροισης πακέτων για τα υπό μελέτη δίκτυα. Ο NCA καταφέρνει να υποστηρίξει περισσότερες ταυτόχρονες κλήσεις VoIP με ικανοποιητικά επίπεδα ποιότητας συνομιλίας. Επιπρόσθετα, αποδείχθηκε ότι ο αλγόριθμος NCA μπορεί να υποστηρίξει καλύτερα κλήσεις VoIP οι οποίες πραγματοποιούνται με καλύτερης ποιότητας κωδικοποιητές, οι οποίοι χρησιμοποιούν μεγαλύτερο μέγεθος πακέτου.

Network Coding – Aggregation – Progressive: Ο αλγόριθμος NCA-P επεκτείνει την λειτουργία του βασικού αλγορίθμου NCA έχοντας ως στόχο τη μείωση της καθυστέρησης που παρατηρείται κατά την αναμετάδοση των πακέτων φωνής. Ο NCA-P στοχεύει στην αποδοτικότερη αξιοποίηση του επιπέδου MAC και για τον σκοπό αυτό προτείνει ένα διαφορετικό τρόπο αναμετάδοσης των πακέτων. Αποτέλεσμα είναι η σημαντική μείωση στην μέση καθυστέρηση μετάδοσης. Μέσω πειραματικών μετρήσεων αποδείχθηκε ότι εκτός από τη μείωση της καθυστέρησης ο αλγόριθμος NCA-P καταφέρνει να αυξήσει την χωρητικότητα του δικτύου υποστηρίζοντας περισσότερες ταυτόχρονες κλήσεις από τον αλγόριθμο NCA.

Network Coding – Aggregation- Failure Salvation: Τέλος, μια επέκταση του NCA-P, είναι ο αλγόριθμος NCA-FS. Ο αλγόριθμος αυτός πραγματοποιεί αναμετάδοση των χαμένων πακέτων χωρίς ωστόσο να προκαλείται επιβάρυνση στο δίκτυο με την δημιουργία νέων μεταδόσεων. Ο NCA-FS ενσωματώνει πακέτα τα οποία δεν μεταδόθηκαν επιτυχώς σε νέα πακέτα των οποίων η μετάδοσή τους έχει προγραμματιστεί και αν το μέγεθος τους το επιτρέπει. Τα πειραματικά αποτελέσματα για τον αλγόριθμο αυτό δείχνουν ότι μειώνει σημαντικά το ποσοστό των πακέτων που χάνονται από συγκρούσεις χωρίς να προκαλεί σημαντική αύξηση στην μέση καθυστέρηση των πακέτων. Επίσης,

παρά το γεγονός ότι ο NCA-FS δεν αυξάνει την χωρητικότητα ενός δικτύου όσον αφορά τις ταυτόχρονες κλήσεις VoIP, ωστόσο βελτιώνει σημαντικά την ποιότητα των κλήσεων αυτών.

### **Συμπεράσματα Κωδικοποίηση δικτύου στο Μέλλον**

Τα μελλοντικά ασύρματα δίκτυα αναμένεται να προσφέρουν υψηλής ταχύτητας πρόσβαση στο internet οπουδήποτε και οποτεδήποτε. Η δημοσιότητα του iPhone και άλλα είδη έξυπνων τηλεφώνων επιταχύνουν αναμφίβολα αυτή την τάση και δημιουργούν νέες απαιτήσεις όσον αφορά την κυκλοφορία. Οι τρέχουσες κυψελοειδής ασύρματες ευρυζωνικές τεχνολογίες αδυνατούν να ανταποκριθούν στην αυξανόμενη ζήτηση για τον όγκο των δεδομένων, την κάλυψη, των νέων υπηρεσιών και του αριθμού των χρηστών. Η κωδικοποίηση δικτύου έχει αναδειχθεί ως ένα πολλά υποσχόμενο εργαλείο για τον σχεδιασμό των μελλοντικών ασύρματων δικτύων. Εργάζονται συστηματικά για τον σχεδιασμό νέων συστημάτων κωδικοποίησης δικτύων για τα μελλοντικά ασύρματα κυψελοειδή δίκτυα και νέους αλγορίθμους επεξεργασίας σήματος, ικανούς να επιτύχουν σημαντικές βελτιώσεις στο throughput του δικτύου, την ενεργειακή απόδοση και την αξιοπιστία.

Η Κωδικοποίηση δικτύου είναι μια αναδυόμενη περιοχή θεωρίας κωδικοποίησης που βασίζεται στους υπολογιστές και σε προβλήματα δικτύου επικοινωνίας. Οι πρόσφατες εργασίες για την κωδικοποίηση του δικτύου καθιστά μια νέα άποψη σχετικά με την πολυεκπομπή σε ένα δίκτυο. Η ανάπτυξη της κωδικοποίησης δικτύου μπορεί να συμβάλει στη βελτίωση των επιδόσεων των δικτύων και να βοηθήσει στην καλύτερη αξιοποίηση των διαθέσιμων πόρων. Είναι μια περιοχή η οποία πρόκειται να προσελκύσει μεγάλο ερευνητικό ενδιαφέρον. Σε σύγκριση με τις παραδοσιακές τεχνικές δρομολόγησης, η κωδικοποίηση δικτύου προσφέρει πρόσθετα οφέλη, δηλαδή καταναλώνονται λιγότεροι πόροι δικτύου και προσφέρει ευκολία διαχείρισης και αντοχή. Υπάρχουν ακόμα κάποιες δυσκολίες που πρέπει να ξεπεραστούν πριν από την εμπορική εφαρμογή της κωδικοποίησης δικτύου, ειδικά όταν χρησιμοποιούνται σε ένα πραγματικό περιβάλλον όπως είναι το Διαδίκτυο. Ωστόσο, η κωδικοποίηση του δικτύου φαίνεται να προσφέρει πολλές δυνατότητες για βελτίωση και εξέλιξη των δικτύων των ηλεκτρονικών υπολογιστών.

Μέχρι σήμερα, η τυχαία κωδικοποίηση δικτύου φαίνεται πολλά υποσχόμενη στις θεωρητικές μελέτες που έχουν γίνει και τα οφέλη της προσφέρουν πλεονεκτήματα σε πρακτικό επίπεδο.

## **Βιβλιογραφική Αναφορά**

Από επιστημονικές εργασίες (papers):

- Network Coding: An Introduction, Tracey Ho Desmond S. Lun
- Network Coding and its Applications in Communication Networks, Alex Sprintson, Texas A&M University, College Station, Texas, USA
- Network Coding: Theory and Reality, Mohit Saxena, Department of Computer Science Purdue University
- Linear Network Coding to Increase TCP Throughput , Alex Britt 2013/4/23
- Network Coding for the Internet and Wireless Networks, Philip A. Chou and Yunnan Wu June 2007 MSR-TR-2007-70
- Simulation of Random Linear Network Coding in Ad-Hoc Networks, ALLBORT UNISVERSITET, department of electronic system, 31st May 2012 Supervisors: Stephan Rein, Frank Fitzek, Morten V. Pedersen
- Random Network Coding in Peer-to-Peer Networks: From Theory to Practice, By Baochun Li and Di Niu
- How Practical is Network Coding?, Mea Wang, Baochun Li
- Can Network Coding Help in P2P Networks?, Dah Ming Chiu, Raymond W Yeung, Jiaqing Huang\_ and Bin Fan Chinese University of Hong Kong
- Is Random Network Coding Helpful in WiMAX? , Jin Jin, Baochun Li, Department of Electrical and Computer Engineering, University of Toronto
- Adaptive Random Network Coding in WiMAX, Jin Jin, Baochun Li, Department of Electrical and Computer Engineering, University of Toronto
- On Practical Network Coding for Wireless Environments, Dina Katabi, Sachin Katti, Wenjun Hu, Hariharan Rahul, and Muriel Medard , Massachusetts Institute of Technology
- Network Coding: An Overview, Author: Axel Davidian, Advisor: Ioannis Oikonomidis, Date : 21.01.2005
- Cache Content Placement Using Triangular Network Coding, Cong Liu
- Gaussian Elimination and Back Substitution, Jim Lambers
- Network Coding Applications, Christina Fragouli and Emina Soljanin
- Simulation algorithms for Network Coding, UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH, School of Telecommunications Engineering of Barcelona
- Network Coding Techniques for Wireless and Sensor Networks, Pouya Ostovari, Jie Wu, and Abdallah Khreishah
- On the Benefits of Network Coding in Multi-Channel Wireless Networks, Xinyu Zhang, Baochun Li , Department of Electrical and Computer Engineering, University of Toronto

Από Διπλωματικές:

- Κωδικοποίηση δικτύου σε δίκτυα ανθεκτικά σε καθυστέρηση, ΕΜΠ, Χριστίνα Γ. Βλάχου
- Τεχνικές μετάδοσης VoIP με κωδικοποίηση Δικτύου σε Ασύρματα Δίκτυα Πολλών Αλμάτων, Καραγιαννίδης Πέτρος
- Υλοποίηση και αξιολόγηση της τεχνικής network coding σε ασύρματα δίκτυα, Βασίλειος Μπούργος

Απο το διαδίκτυο:

- <http://www.hindawi.com/journals/ijdmb/2011/857847/>
- [http://www.digplanet.com/wiki/Triangular\\_network\\_coding](http://www.digplanet.com/wiki/Triangular_network_coding)