
**Εθνικό Μετσόβιο Πολυτεχνείο**

**Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών**

Τομέας Τεχνολογίας Πληροφορικής και Υπολογιστών

Εργαστήριο Λογικής & Επιστήμης Υπολογισμών (Corelab)


ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ

---

# Αξιόπιστη Επικοινωνία υπό Συνθήκες Περιορισμένης Γνώσης

---


*του*

Δημήτρη Κ. Σακαβάλα


***Επιβλέπων**: Αριστείδης Παγουρτζής*
Αν. Καθηγητής ΕΜΠ

---

Αθήνα, Ιούλιος 2016

**ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ**
ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ
ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΤΕΧΝΟΛΟΓΙΑΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ
ΕΡΓΑΣΤΗΡΙΟ ΛΟΓΙΚΗΣ ΚΑΙ ΕΠΙΣΤΗΜΗΣ ΥΠΟΛΟΓΙΣΜΩΝ

# Αξιόπιστη Επικοινωνία υπό Συνθήκες Περιορισμένης Γνώσης

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ

του

**Δημήτρη Κ. Σακαβάλα**

**Συμβουλευτική Επιτροπή**: Αριστείδης Παγουρτζής
Ευστάθιος Ζάχος
Δημήτριος Φωτάκης

Εγκρίθηκε από την επταμελή εξεταστική επιτροπή:

| | | |
|---|---|---|
| ..... | ..... | ..... |
| Αριστείδης Παγουρτζής<br>Αν. Καθηγητής ΕΜΠ | Ευστάθιος Ζάχος<br>Καθηγητής ΕΜΠ | Δημήτριος Φωτάκης<br>Επ. Καθηγητής ΕΜΠ |
| ..... | ..... | ..... |
| Άγγελος Κιαγιάς<br>Αν. Καθηγητής ΕΚΠΑ | Βασίλης Ζήκας<br>Επ. Καθηγητής RPI | Ευριπίδης Μάρκου<br>Επ. Καθηγητής ΠΘ |

.....
Αντώνιος Συμβώνης
Καθηγητής ΕΜΠ

Αθήνα, Ιούλιος 2016.

……
**Δημήτρης Κ. Σακαβάλας**
Διδάκτωρ Ε.Μ.Π.

# Περίληψη

Καθώς τα σύγχρονα δίκτυα επικοινωνιών αυξάνονται σε μέγεθος, γίνονται συνεχώς πιο ευάλωτα σε δυσλειτουργίες των συστατικών τους. Τα δίκτυα αυτά αποτελούνται από οντότητες (συμμετέχοντες ή παίκτες) που αλληλεπιδρούν μεταξύ τους για την επίτευξη κάποιου κοινού στόχου. Τα κατανεμημένα συστήματα χρησιμοποιούνται ευρέως στις σημερινές δικτυακές υποδομές, καθώς είναι ιδανικά για την μοντελοποίηση τέτοιων περιπτώσεων συνεργατικών υπολογισμών. Επομένως, οι παρεχόμενες λύσεις πρέπει να είναι σε θέση να αντιμετωπίσουν εσφαλμένες και κακόβουλες συμπεριφορές εκ μέρους των συμμετεχόντων. Τα ζητήματα ασφάλειας και αξιοπιστίας που προκύπτουν, αποτελούν αντικείμενο μελέτης στους τομείς των Ασφαλών Υπολογισμών πολλών Συμμετεχόντων και των Κατανεμημένων Υπολογισμών. Η παρούσα εργασία, συμβάλλει στην μελέτη θεμελιωδών αρχών επικοινωνίας (Αξιόπιστη Εκπομπή και Αξιόπιστη Μετάδοση Μηνύματος) σε μη αξιόπιστα κατανεμημένα συστήματα, με τη διερεύνηση των επιπτώσεων της δομής του δικτύου και της τοπολογικής γνώσης των συμμετεχόντων στον βαθμό που μπορούν αν επιτευχθούν αυτές οι βασικές εργασίες. Θεωρούμε την χειρότερη περίπτωση αντιπάλου (Βυζαντινός αντίπαλος), ο οποίος διαφθείρει μέρος των συμμετεχόντων και τους αναγκάζει να αποκλίνουν αυθαίρετα από τους προκαθορισμένους κανόνες.

Αρχικά, θεωρούμε ότι το μοντέλο t-τοπικά περιορισμένου αντιπάλου, το οποίο εισήχθη το 2004 από Koo, όπου ο αριθμός των διεφθαρμένων παικτών στην γειτονιά κάθε παίκτη περιορίζεται από ένα άνω φράγμα. Διερευνούμε την σχέση μεταξύ του επιπέδου της τοπολογικής γνώσης και της επιλυσιμότητας του προβλήματος αναπτύσσοντας μιας ευέλικτη τεχνική που μας επιτρέπει την εξαγωγή αναγκαίων συνθηκών που καθιστούν το πρόβλημα επιλύσιμο, για κάθε επίπεδο γνώσης της τοπολογίας. Ο έλεγχος της ισχύος αυτών των συνθηκών αποδεικνύεται ότι είναι NP-δύσκολο πρόβλημα, αλλά στην πορεία προτείνουμε ένα αποδοτικό 2-προσεγγιστικό αλγόριθμο για την περίπτωση των δικτύων άγνωστης τοπολογίας (ad hoc). Ως προς την επίλυση του προβλήματος, γενικεύουμε την αλγοριθμική ιδέα στην οποία στηρίζεται ο απλός αλλά ιδιαίτερα χρήσιμος Αλγόριθμος Πιστοποιημένης Διάδοσης (CPA), που προτάθηκε από τον Koo το 2004, και σχεδιάζουμε αλγορίθμους οι οποίοι επιλύουν το πρόβλημα όποτε ισχύουν οι αναγκαίες συνθήκες ("μοναδικοί" αλγόριθμοι) σε κάθε περίπτωση τοπολογικής γνώσης. Έτσι, επιτυγχάνουμε τον ακριβή χαρακτηρισμό των γραφημάτων στα οποία είναι δυνατή η αξιόπιστη επικοινωνία σε σχέση με το επίπεδο γνώσης της τοπολογίας. Προκειμένου να επιτευχθούν τα παραπάνω, εισάγουμε το Μοντέλο Μερικής Γνώσης, στο οποίο κάθε παίκτης γνωρίζει ένα οποιοδήποτε τμήμα του δικτύου που αναπαρίσταται

από ένα υπογράφημα. Στη μελέτη μας, καταφέρνουμε να απαντήσουμε στο ανοιχτό ερώτημα των Pelc και Peleg (2005) καταφατικά, αποδεικνύοντας την μοναδικότητα του CPA σε δίκτυα άγνωστης τοπολογίας, δηλαδή, ότι ο CPA μπορεί να ανεχθεί όσες τοπικές διαφθορές ανέχεται και οποιοσδήποτε άλλος αλγόριθμος.

Επιπλέον, καταφέρνουμε να γενικεύσουμε τα αποτελέσματά μας στο μοντέλο Γενικού Αντιπάλου των Hirt και Maurer (1997), το οποίο αποτελεί γενίκευση όλων των γνωστών μοντέλων αντιπάλου, με την προσαρμογή των τεχνικών και αλγορίθμων μας από το μοντέλο t-τοπικά φραγμένου αντιπάλου. Έτσι, σχεδιάζουμε τους πρώτους αλγορίθμους βέλτιστης ανεκτικότητας, που πετυχαίνουν αξιόπιστη επικοινωνία υπό περιορισμένη τοπολογική γνώση και ύπαρξη γενικού αντιπάλου. Μελετάμε επίσης την αποδοτικότητα πρωτοκόλλων αξιόπιστης επικοινωνίας, εισάγοντας μια αλγοριθμική ιδιότητα που δηλώνει ότι ένα αλγοριθμικό σχήμα είναι όσο αποδοτικό όσο και οποιοδήποτε άλλο ως προς πολυωνυμικές παραμέτρους. Για την εξαγωγή των τελευταίων συμπερασμάτων, χρησιμοποιούμε, μεταξύ άλλων , μια νέα έννοια συνδυασμού γνώσης σχετικά με την δομή του αντιπάλου, κατάλληλες έννοιες διαχωριστών σε μη αξιόπιστα δίκτυα και μια ιδιότητα αυτο-αναγωγής του προβλήματος.

Τέλος, μελετάμε την ενεργειακά αποδοτική εκπομπή σε ασύρματα δίκτυα, όπου ταυτόχρονες μεταδόσεις οδηγούν σε παρεμβολή σήματος η οποία αποτρέπει την διάδοση του μηνύματος. Συγκεκριμένα, εξετάζουμε το ασύρματο μοντέλο δικτύου k-μεταδόσεων, στο οποίο δίνεται ένα άνω φράγμα k στον αριθμό των μεταδόσεων του κάθε παίκτη. Σε αυτό το μοντέλο αποδεικνύουμε ένα κάτω φράγμα στο χρόνο που απαιτείται για το διαμοιρασμό του μηνύματος σε όλο το δίκτυο από οποιοδήποτε πρωτόκολλο.

**Λέξεις-κλειδιά:** αξιόπιστη εκπομπή, αξιόπιστη μετάδοση μηνύματος, βυζαντινός αντίπαλος, μερική γνώση, γενικός αντίπαλος, ελλιπή δίκτυα, δίκτυα άγνωστης τοπολογίας, κατανεμημένα συστήματα, τοπολογική γνώση, ασύρματα δίκτυα, ενεργειακή αποδοτικότητα, εκπομπή $k$-μεταδόσεων.

# Abstract

As communication networks grow in size, they become increasingly vulnerable to component failures. These networks consist of numerous interacting entities (agents). Since distributed systems have become popular and widely used in contemporary networking, the provided solutions need to cope with erroneous and malicious components in the underlying communication network. Security and reliability issues that arise have been objects of extensive research in the fields of Secure Multiparty Computations and Distributed Computing. In our work we contribute to the realization of fundamental communication primitives (Reliable Broadcast and Reliable Message Transmission) in an adversarial distributed environment, by investigating the impact of the network structure and the agents' topology knowledge level on the achievability of these tasks. We consider a worst-case (Byzantine) adversary, which makes the agents misbehave arbitrarily,

Initially, we consider the t-locally bounded adversary model, introduced in 2004 by Koo, where a fixed upper bound on the number of corruptions in each agent's neighborhood is imposed. We explore the tradeoff between the level of topology knowledge and the solvability of the problem by developing a versatile technique which allows us to obtain impossibility results for every level of topology knowledge. Checking the necessary conditions for the solvability of the problem proves to be NP-hard but along the way we obtain an efficient 2-approximation algorithm for the ad hoc case (where agents only know their local neighborhood). On the positive, we generalize the algorithmic idea behind the simple, yet powerful Certified Propagation Algorithm (CPA), also introduced by Koo in 2004, and propose algorithms, that match the obtained bounds (unique algorithms) in every case. Thus, we exactly characterize the classes of graphs in which reliable communication is possible with respect to topology knowledge. In order to achieve these we introduced the Partial Knowledge Model in which each agent knows a part of the network, namely a connected subgraph containing itself. As a part of the latter contribution, we manage to settle an open question of Pelc and Peleg (2005) in the affirmative, by showing that in ad hoc networks, CPA is unique, that is, it can tolerate as many local corruptions as any other Broadcast algorithm.

Furthermore, we manage to generalize our results in the General Adversary model of Hirt and Maurer (1997), which subsumes earlier models by adapting our techniques and algorithms from the t-locally bounded model. Thus, we devise the first optimally resilient algorithms for Reliable Broadcast/Message transmission under restricted knowledge and general adversaries.

We also study the efficiency of RMT protocols by introducing an algorithmic property which implies that a protocol scheme is as efficient as any other for a certain problem with respect to polynomial time. To obtain our latter results we employ, among others, a novel notion of joining operation on adversary structures, appropriate notions of separators in unreliable networks, and a self-reducibility property of the RMT problem.

Finally, we study energy-efficient Broadcast in wireless networks, where simultaneous transmissions lead to signal interference which prevents message propagation. In particular, we examine the $k$-shot wireless network model, in which a bound $k$ on the number of transmissions for every player is given. We prove a lower bound on the Broadcast time of any protocol.

**Keywords:** reliable broadcast, reliable message transmission, byzantine adversary, partial knowledge, general adversary, incomplete networks, ad hoc networks, distributed computing, topology knowledge, wireless networks, energy efficiency, $k$-shot Broadcast

# Πρόλογος

Η παρούσα διατριβή εκπονήθηκε στο Εργαστήριο Λογικής και Επιστήμης Υπολογισμών (Corelab) της Σχολής Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Εθνικού Μετσόβιου Πολυτεχνείου [1]. Το εργαστήριο διαθέτει πολυετή εμπειρία σε αλγοριθμικά θέματα κατανεμημένων συστημάτων και ασφάλειας δικτύων. Η συνεργασία μου με το εργαστήριο ξεκίνησε με την εκπόνηση της μεταπτυχιακής μου εργασίας στα πλαίσια του Δ.Π.Μ.Σ "Εφαρμοσμένες Μαθηματικές Επιστήμες", την άνοιξη του 2010. Στη συνέχεια, είχα την τιμή να γίνω δεκτός ως υποψήφιος διδάκτορας υπό την επίβλεψη του Αναπληρωτή Καθηγητή ΕΜΠ κ. Αριστείδη Παγουρτζή και από το φθινόπωρο του 2010 ξεκίνησα να εργάζομαι στην περιοχή που τώρα, αποτελεί το αντικείμενο αυτής της διατριβής.

## Σκοπός και εφαρμογές της διατριβής

Η ταχεία ανάπτυξη των δικτύων επικοινωνιών και η πληθώρα των εφαρμογών που τη συνοδεύει δημιουργούν συνεχώς νέες ανάγκες και προκλήσεις. Τα δίκτυα επικοινωνιών συνήθως αποτελούνται από ένα πολυάριθμο σύνολο οντοτήτων - συμμετεχόντων που αλληλεπιδρούν μεταξύ τους. Αυτές οι οντότητες συχνά επιθυμούν να συνεργαστούν για την διεκπεραίωση εργασιών, οι οποίες ποικίλλουν από βασικές εργασίες, όπως για παράδειγμα η διανομή του ψηφιακού περιεχομένου και κοινή λήψη αποφάσεων, μέχρι πιο περίπλοκες, που θα βασίζονται στις προηγούμενες· ένα τέτοιο παράδειγμα είναι η ηλεκτρονική ψηφοφορία. Ενώ η συμπεριφορά των συμμετεχόντων αναμένεται γενικά να είναι έντιμη, ακολουθώντας κάποιους συμφωνηθέντες κανόνες, υπάρχει η πιθανότητα εμφάνισης προβληματικών ή ακόμα και κακόβουλων συμμετεχόντων στο δίκτυο, οι οποίοι επιθυμούν να παραβιάσουν αυτούς τους κανόνες με στόχο να εξυπηρετήσουν τα δικά τους συμφέροντα, εις βάρος των καλόβουλων συμμετεχόντων. Τέτοιες θεωρήσεις αναδεικνύουν την ανάγκη μελέτης ασφάλειας στα κατανεμημένα συστήματα, με τα οποία μοντελοποιείται ακριβώς η κατάσταση στην οποία πολλοί συμμετέχοντες επιχειρούν να επιτύχουν κάποιον κοινό στόχο δεδομένης της απουσίας μιας κεντρικής αρχής συντονισμού.

Οι πραγματικές εφαρμογές σήμερα, αφορούν δίκτυα με ιδιαίτερα πολύπλοκη δομή. Επομένως, η ανάγκη ανάπτυξης σαφούς και συμπαγούς θεωρητικής θεμελίωσης για την υποστήριξη της αξιόπιστης επικοινωνίας μεταξύ τμημάτων του δικτύου αυξάνεται, καθώς η μαθηματική μοντελοποίηση αυτών των δομών γίνεται συνεχώς πιο απαιτητική. Είναι σύνηθες στη βιβλιογραφία, η έρευνα να εστιάζεται σε απλουστευμένες δικτυακές δομές και ισχυρές παραδοχές ως προς τη γνώση των συμμετεχόντων, έτσι ώστε να προκύψουν τα ανάλογα αποτελέσματα που αφορούν την δυνατότητα διεκπεραίωσης ορισμένων εργασιών. Στην παρούσα μελέτη

[1]Το μεγαλύτερο μέρος της χρηματοδότησης μου, κατά τη διάρκεια των διδακτορικών μου σπουδών, προήλθε από την υποτροφία για διδακτορικές σπουδές που έλαβα από τον Ειδικό Λογαριασμό Κονδυλίων Έρευνας (ΕΛΚΕ) του Ε.Μ.Π.

ασχολούμαστε συγκεκριμένα με τη δομή του δικτύου και την “εκ των προτέρων” γνώση που κατέχουν οι συμμετέχοντες αναφορικά με αυτήν και εξετάζουμε πως αυτές οι παράμετροι επηρεάζουν την ορθότητα βασικών διαδικασιών ανταλλαγής πληροφορίας. Με αυτόν τον τρόπο συνεισφέρουμε στην ανακάλυψη των ελάχιστων δομικών απαιτήσεων από πλευράς δικτύου, και στο ελάχιστο επίπεδο γνώσης τα οποία καθιστούν επιλύσιμα προβλήματα ασφάλειας και αξιοπιστίας στα εν λόγω κατανεμημένα συστήματα. Τα αποτελέσματα μας έχουν άμεση εφαρμογή στην σχεδίαση δικτύων τα οποία μπορούν να υποστηρίξουν, με τον βέλτιστο τρόπο, την χρήση πρωτοκόλλων αξιόπιστης επικοινωνίας παρά την ύπαρξη συμμετεχόντων που παρεκκλίνουν από την τήρηση των κανόνων. Ένα άλλο πρακτικό πλεονέκτημα που προκύπτει από αυτή τη δουλειά είναι το ότι οι εν λόγω τεχνικές μπορούν να χρησιμοποιηθούν για τον ακριβή προσδιορισμό των χειρότερων σεναρίων παρεκκλίνουσας συμπεριφοράς που μπορεί να γίνει ανεκτή σε ήδη υπάρχουσες δικτυακές υποδομές. Οι παραπάνω μελέτες μπορούν να εφαρμοστούν ιδανικά σε εφαρμογές κρίσιμης σημασίας, όπως συστήματα ελέγχου πτήσης, πυρηνικών σταθμών παραγωγής ηλεκτρικής ενέργειας και στρατιωτικές επιχειρήσεις, όπου η υποδομή επικοινωνίας πρέπει να είναι σε θέση να αντιμετωπίσει βλάβες ή ακόμα χειρότερα κακόβουλες διαφθορές ορισμένων συσκευών. Σε εφαρμογές τέτοιας φύσης, συχνά χρησιμοποιούνται συσκευές περιορισμένων δυνατοτήτων ως προς τη μνήμη, τη διαθέσιμη ενέργεια και την υπολογιστική ισχύ, όπως ασύρματοι αισθητήρες κ.α., με ικανοποιητικά αποτελέσματα. Συνεπώς, είναι απαραίτητη η χρήση οντοτήτων-συσκευών με χαμηλές απαιτήσεις ως προς τη συνδεσιμότητα και τη γνώση που μπορούν να έχουν αποθηκευμένη σε μορφή δεδομένων.

Τα προβλήματα της αξιόπιστης εκπομπής και αξιόπιστης μετάδοσης μηνύματος, που μελετώνται εκτενώς στην παρούσα εργασία, αποτελούν θεμελιώδη δομικά στοιχεία για την επίτευξη πιο σύνθετων εργασιών σε ασθενώς συνδεδεμένα δίκτυα και μοντέλα περιορισμένης γνώσης των συμμετεχόντων. Η ανάγκη μελέτης μοντέλων περιορισμένης γνώσης υπαγορεύεται από εφαρμογές σε δίκτυα ευρείας κλίμακας (π.χ. το διαδίκτυο), όπου η εκτίμηση του βαθμού δυσλειτουργίας μπορεί να γίνει με σχετική ακρίβεια από τον κάθε συμμετέχοντα στα πλαίσια της γειτονιάς του, ενώ μια συνολική εκτίμηση μπορεί να είναι δύσκολο να επιτευχθεί λόγω γεωγραφικών περιορισμών και περιορισμών δικαιοδοσίας. Επιπλέον, η εγγύτητα κόμβων σε κοινωνικά δίκτυα συχνά συσχετίζεται με αυξημένη ποσότητα διαθέσιμης πληροφορίας, γεγονός που δικαιολογεί περαιτέρω την ευστάθεια του μοντέλου. Η εισαγωγή ενός συμπαγούς μοντέλου για τον περιορισμό της γνώσης όπως παρουσιάζεται σε αυτήν την εργασία, συμβάλλει στη θεμελίωση μιας πιο ρεαλιστικής θεώρησης για τα σύγχρονα δίκτυα επικοινωνιών και την αξιοπιστία τους.

Η ανάδυση της κοινωνικής δικτύωσης, του ηλεκτρονικού εμπορίου και των ηλεκτρονικών ψηφοφοριών μπορεί δυνητικά να έχει τεράστια επίδραση στη διασφάλιση της οικονομικής και κοινωνικής ευημερίας σε έναν ανοικτό και διασυνδεδεμένο ψηφιακό κόσμο. Για την επίτευξη του σκοπού αυτού, απαραίτητη προϋπόθεση είναι η οικοδόμηση της εμπιστοσύνης του κοινού σε αυτές τις διαδικασίες. Το τελευταίο μπορεί να επιτευχθεί με την εξασφάλιση της αξιοπιστίας των διαδικασιών και την προστασία των συμμετεχόντων από κακόβουλες συμπεριφορές. Αυτά τα ζητήματα μπορούν να διευθετηθούν μόνο με αυστηρή θεωρητική ανάλυση στο πλαίσιο συναφών επιστημονικών πεδίων, όπως αυτά των Κατανεμημένων Υπολογισμών

και της Κρυπτογραφίας. Ιδανικά, η αξιοπιστία των εν λόγω ηλεκτρονικών υπηρεσιών θα καθιερωθεί και θα οδηγήσει σε αυξημένη συμμετοχή ατόμων, ανεξάρτητα από οικονομικούς και κοινωνικούς παράγοντες, δεδομένου ότι η πρόσβαση σε αυτές τις διαδικασίες μπορεί να είναι πολύ προσιτή σε όλους. Το τελευταίο μπορεί να οδηγήσει σε αμεσοδημοκρατικές διαδικασίες που διέπονται από τις αρχές της ισότητας και της δικαιοσύνης.

Τέλος, η έρευνα μας μπορεί να ερμηνευθεί ως μια μελέτη για την διάδοση της γνώσης σε έναν γενικό πλαίσιο όπου η επικοινωνία μεταξύ των συμμετεχόντων αυξάνει την ποσότητα των πληροφοριών που κατέχει ο καθένας. Εστιάζοντας σε παραλλαγές της δομής του δικτύου και της αρχικής γνώσης των συμμετεχόντων, παρέχουμε τα ανάλογα όρια για τη διάδοση της γνώσης σε διαφορετικά μοντέλα. Χαλαρώνοντας τις απαιτήσεις ως προς τη γνώση του κάθε συμμετέχοντα με πιθανοτικό τρόπο, έτσι ώστε κάποιος να είναι σίγουρος για την ισχύ ενός γεγονότος με κάποια πιθανότητα, μπορούν να χρησιμοποιηθούν παρόμοιες τεχνικές για την εξαγωγή ανάλογων αποτελεσμάτων στους τομείς της διάδοσης πεποίθησης ή άποψης σε δίκτυα. Μεταξύ άλλων, αυτό θα παρείχε τη δυνατότητα εντοπισμού "κρίσιμων" μερών του δικτύου επικοινωνίας, ο έλεγχος των οποίων θα είχε ως αποτέλεσμα την ευρεία διάδοση συγκεκριμένων απόψεων στο δίκτυο. Το παραπάνω θα μπορούσε προφανώς να φανεί χρήσιμο σε στρατηγικές διαφήμισης, αλλά από την άλλη πλευρά θα μπορούσε να χρησιμοποιηθεί για την προστασία δικτύων επικοινωνιών έναντι σε διάδοση ψευδών πληροφοριών.

## Ευχαριστίες

Πρώτα απ'όλα, θα ήθελα να ευχαριστήσω τον επιβλέπων καθηγητή μου κ. Αριστείδη Παγουρτζή, ο οποίος με μεγάλη υπομονή και ηρεμία με εισήγαγε στον κόσμο της έρευνας δίνοντας μεγάλη σημασία στη δημιουργικότητα και στην ελευθερία που είναι απαραίτητο να έχει κανείς για να πετύχει κάτι ουσιαστικό. Μου συμπαραστάθηκε και με καθοδήγησε κατά τη διάρκεια των διδακτορικών μου σπουδών, σε επαγγελματικό και προσωπικό επίπεδο, δείχνοντας μου εμπιστοσύνη που αποτέλεσε για μένα βασική πηγή έμπνευσης.

Τα μέλη της τριμελούς συμβουλευτικής επιτροπής μου, κ. Στάθης Ζάχος και κ. Δημήτρης Φωτάκης, με στήριξαν με ειλικρινές ενδιαφέρον και με βοήθησαν ουσιαστικά να ασχοληθώ δημιουργικά με αυτό που πάντα ήθελα να κάνω. Με διαφορετικό ύφος ο καθένας, μου δώσανε συμβουλές στις οποίες θα μπορώ πάντα να στηρίζομαι. Παράλληλα, αποτέλεσε ιδιαίτερη τιμή για μένα η συμμετοχή του Άγγελου Κιαγιά, Βασίλη Ζήκα, Ευριπίδη Μάρκου και Αντώνη Συμβώνη στην επταμελή εξεταστική επιτροπή του διδακτορικού μου.

Η παρούσα εργασία περιλαμβάνει παρουσίαση αποτελεσμάτων που προέκυψαν από τη συνεργασία μου με τον Γιώργο Παναγιωτάκο και τον Χρήστο Λίτσα. Θα ήθελα να τους ευχαριστήσω για τις, επαγγελματικές και μη, εποικοδομητικές συζητήσεις που είχαμε και πιστεύω, μας εμπνεύσανε όλους. Η δουλειά που κάναμε μαζί δεν διαχωριζόταν και πολύ από την καλοπέρασή μας, γιαυτό και προέκυψαν ενδιαφέρουσες ιδέες.

Τα μέλη του Corelab, ήταν όλα αυτά τα χρόνια ιδανικοί συνεργάτες και τους ευχαριστώ για την ατμόσφαιρα που δημιούργησαν στο εργαστήριο. Οι χαλαρές συζητήσεις που κάναμε με

την Χριστίνα, τη Ματούλα, τον Αντώνη, την Πέλη και την Τζέλα, αναγκαίες για να ισορροπήσουμε, θα είναι πάντα αναπόσπαστο κομμάτι των αναμνήσεων αυτών των χρόνων. Ιδιαίτερα θέλω να ευχαριστήσω αυτούς με τους οποίους παίξαμε μαζί μουσική, χαλαρώσαμε, καθαρίσαμε τα κεφάλια μας και πάνω απ'όλα περάσαμε καλά και κάναμε πλάκα. Ελπίζω λοιπόν αυτή η κομπανία, οι "Μεγάλες Τρίτες" όπως την είπαμε, να μαζεύεται που και που και κάθε φορά να περνάμε όσο καλά περάσαμε και τις προηγούμενες. Ευχαριστώ λοιπόν τον Θανάση, τη Ναταλία, το Γιώργο, τους Μανώληδες, την Ελένη και τον Πέτρο.

Ευχαριστώ την Ειρήνη που είχε πάντα τον τρόπο της να με φέρνει σε ισορροπία και να μου θυμίζει τι είναι πραγματικά σημαντικό. Η περίοδος αυτή θα ήταν για μένα πιο δύσκολη χωρίς αυτήν.

Τέλος, οφείλω ένα τεράστιο ευχαριστώ στην οικογένειά μου που ποτέ δεν σταμάτησε να με στηρίζει με κάθε τρόπο. Η αδερφή μου, η μάνα μου και ο πατέρας μου, μου δίνανε πάντα έναν λόγο να συνεχίζω και να προσπαθώ να εξελιχθώ.

Δημήτρης Σακαβάλας

Αθήνα, Ιούλιος 2016

# Περιεχόμενα

# Κατάλογος σχημάτων

# Κεφάλαιο 1

# Εισαγωγή

Καθώς τα δίκτυα επικοινωνιών αυξάνονται σε μέγεθος, γίνονται ολοένα και πιο ευάλωτα σε βλάβες των στοιχείων που τα απαρτίζουν. Αυτά τα δίκτυα αποτελούνται από διασυνδεδεμένες οντότητες που επικοινωνούν μεταξύ τους. Στη συνέχεια θα αναφερόμαστε σε αυτές τις οντότητες ως *παίκτες*. Τα κατανεμημένα συστήματα υπολογισμών γίνονται συνεχώς πιο δημοφιλή λόγω της ευρείας εφαρμογής που βρίσκουν στις σύγχρονες δικτυακές υποδομές. Επομένως είναι σημαντικό, οι λύσεις που παρέχονται να είναι σε θέση να αντιμετωπίσουν την εμφάνιση βλαβών και κακόβουλων ενεργειών στο υποκείμενο δίκτυο. Η λειτουργικότητα των κατανεμημένων συστημάτων επιτυγχάνεται με αποκεντρωμένο τρόπο· οι αυτόνομες οντότητες που απαρτίζουν το δίκτυο συνεργάζονται για να εκτελέσουν εργασίες όπως απαιτητικούς υπολογισμούς, διανομή ψηφιακού υλικού ή λήψη κοινών αποφάσεων, δεδομένης της απουσίας μιας κεντρικής αρχής συντονισμού.

Η μελέτη της συμπεριφοράς κατανεμημένων συστημάτων υπό την παρουσία βλαβών, περιλαμβάνει το σχεδιασμό αλγορίθμων οι οποίοι επιτυγχάνουν το ζητούμενο στόχο, παρά την ύπαρξη *διεφθαρμένων* παικτών στο δίκτυο, η ταυτότητα μάλιστα των οποίων θεωρείται άγνωστη. Για να μοντελοποιήσουμε τη διαφθορά των παικτών, θεωρούμε έναν κεντρικό *αντίπαλο*, ο οποίος ελέγχει εν μέρει τη συμπεριφορά των παικτών, τους οποίους έχει καταφέρει να διαφθείρει. Οι παίκτες οι οποίοι δεν βρίσκονται υπό την επιρροή του αντιπάλου θα ονομάζονται *τίμιοι*. Διάφοροι τύποι διαφθοράς έχουν προταθεί στη σχετική βιβλιογραφία. Ανάμεσα σε αυτούς τους τύπους αντιπάλου, ο *Βυζαντινός ή Ενεργός* (Byzantine or Active) αντίπαλος, μοντελοποιεί τη χειρότερη περίπτωση αποκλίνουσας συμπεριφοράς. Συγκεκριμένα, θεωρείται ότι οι παίκτες που ελέγχονται από τον αντίπαλο, μπορούν να συμπεριφερθούν με αυθαίρετο τρόπο, σταματώντας τη ροή ή αλλάζοντας τη δρομολόγηση και το περιεχόμενο της πληροφορίας που πρέπει να μεταδώσουν με τρόπο που μπορεί να αποβεί καταστροφικός για την ορθότητα της οποιασδήποτε διαδικασίας απαιτεί επικοινωνία μεταξύ των συμμετεχόντων.

## 1.1 Το πρόβλημα της Αξιόπιστης Εκπομπής

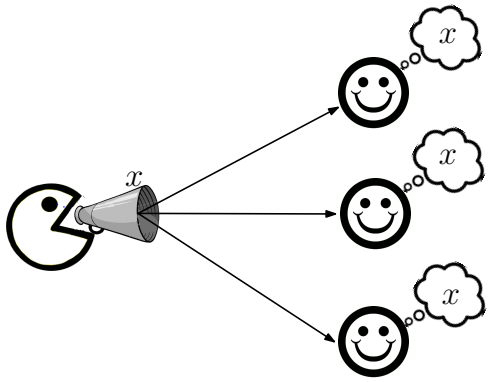
Ένα θεμελιώδες πρόβλημα στον τομέα των κατανεμημένων συστημάτων είναι αυτό της *Αξιόπιστης Εκπομπής* (Reliable Broadcast) ή αλλιώς το *πρόβλημα των Βυζαντινών Στρατηγών* (Byzantine Generals)· παρουσιάστηκε για πρώτη φορά από τους Lamport, Shostak and Pease [LSP82] το 1982. Στο πρόβλημα αυτό, ο στόχος είναι η ορθή μετάδοση ενός μηνύματος από έναν καθορισμένο *παίκτη-διανομέα* σε όλο το δίκτυο ανεξάρτητα από την ύπαρξη ενός Βυζαντινού αντιπάλου. Σε αυτήν την περίπτωση, ο αντίπαλος μπορεί να ελέγχει διάφορους παίκτες-κόμβους του δικτύου, και είναι ικανός να τους επιβάλει να αποκλίνουν από τους κανόνες του πρωτοκόλλου με αυθαίρετο τρόπο. Κατά κύριο λόγο, τα προβλήματα συμφωνίας έχουν μελετηθεί στη βιβλιογραφία στα πλαίσια του *μοντέλου φραγμένου αντιπάλου* (threshold adversary model), όπου υπάρχει η υπόθεση ύπαρξης ενός άνω ορίου $t$ στον αριθμό των διεφθαρμένων παικτών. Σε αυτό το μοντέλο, έχει αποδειχθεί ήδη από το [LSP82], ότι αξιόπιστη εκπομπή μπορεί να επιτευχθεί αν και μόνον αν $t < n/3$, όπου $n$ είναι ο συνολικός αριθμός των παικτών που συμμετέχουν. Το πρόβλημα της αξιόπιστης εκπομπής, έχει μελετηθεί εκτενώς σε πλήρη δίκτυα υπό το μοντέλο φραγμένου αντιπάλου από το 1982 έως το 1998, όπου οι Garay και Moses [GM98] παρουσίασαν το πρώτο *πλήρως πολυωνυμικό* πρωτόκολλο το οποίο ήταν βέλτιστο ως προς την πολυπλοκότητα γύρων και ανεχόταν τον μέγιστο αριθμό διαφθορών $t < n/3$. Η δυσκολία σχεδιασμού μιας λύσης για το πρόβλημα πρωτίστως μπορεί να συνοψιστεί στο σενάριο όπου ο κόμβος-διανομέας είναι διεφθαρμένος. Όπως φαίνεται στο Σχήμα 1.1, σε πραγματικά δίκτυα όπου ο διανομέας συνδέεται μέσω διαφορετικών καναλιών επικοινωνίας με κάθε παίκτη, ο διανομέας μπορεί να στείλει αντικρουόμενες τιμές στους παίκτες. Σε αυτήν την περίπτωση, απαιτούμε τελικά οι παίκτες να συμφωνήσουν σε μια κοινή τιμή.

Ο σκοπός ενός πρωτοκόλλου αξιόπιστης εκπομπής είναι να προσομοιώσει μια ιδανική εκπομπή, όπου όλοι λαμβάνουν την ίδια τιμή από τον διανομέα την ίδια χρονική στιγμή, μέσω της επικοινωνίας των παικτών. Ουσιαστικά απαιτείται να παρακαμφθούν οι λανθασμένες συμπεριφορές, χωρίς να χαθεί η ομοφωνία στο σύστημα. Ακολουθεί ο τυπικός ορισμός του προβλήματος της Αξιόπιστης Εκπομπής.

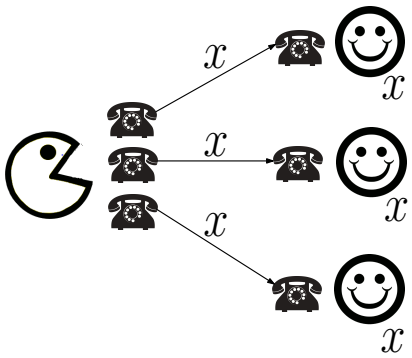
***Ορισμός* 1.1** (Πρόβλημα Αξιόπιστης Εκπομπής). *Έστω $V = \{p_1, p_2, \cdots, p_n\}$ ένα σύνολο $n$ παικτών, $X$ ο πεπερασμένος χώρος των μηνυμάτων και $D \in V$ ο κόμβος-διανομέας. Έστω επίσης ένα πρωτόκολλο $\Pi$ μεταξύ των παικτών $V$ με τιμές μηνυμάτων στο $X$, όπου ο $D$ έχει αρχική τιμή $x_D \in X$ και κάθε παίκτης $p_i$ τελικά αποφασίζει σε μια τιμή $y_i \in X$. Το πρωτόκολλο $\Pi$ ονομάζεται πρωτόκολλο Αξιόπιστης Εκπομπής αν και μόνον αν ικανοποιεί τις ακόλουθες συνθήκες:*

1. Ορθότητα: *Αν ο κόμβος-διανομέας $D$ είναι τίμιος, τότε όλοι οι τίμιοι παίκτες τελικά αποφασίζουν στην τιμή $x_D$.*
2. Συνέπεια: *Όλοι οι τίμιοι παίκτες τελικά αποφασίζουν στην ίδια τιμή, δηλαδή, $\forall p_i, p_j$ που είναι τίμιοι, ισχύει ότι $y_j = y_i$.*

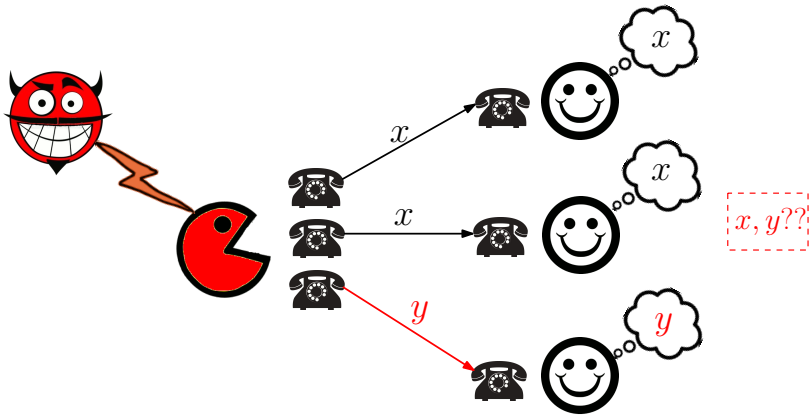
Σε ελλιπή δίκτυα, όπου ο διανομέας δεν είναι άμεσα συνδεδεμένος με όλους τους παίκτες, το πρόβλημα παρουσιάζει μια επιπλέον δυσκολία· ακόμα και στην περίπτωση που ο κόμβος-διανομέας είναι ένας τίμιος παίκτης, ο αντίπαλος μπορεί να διαφθείρει ένα κρίσιμο μέρος




(α′) Ιδανική Εκπομπη




(β′) Πραγματική Εκπομπη

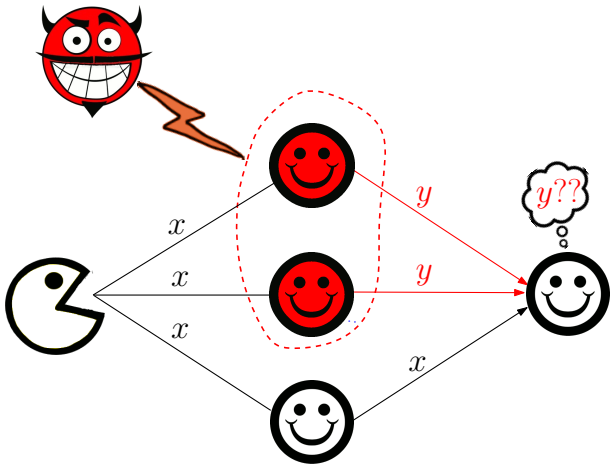



(γ′) Πραγματική Εκπομπη με διεφθαρμένο διανομέα

Σχήμα 1.1: Ιδανική και Πραγματική Αξιόπιστη Εκπομπή

του δικτύου έτσι ώστε να καταστήσει αδύνατη την απόφαση στην σωστή τιμή για κάποιους τίμιους παίκτες. Το σενάριο αυτό απεικονίζεται στο Σχήμα 1.2.

Η περίπτωση της Αξιόπιστης Εκπομπής σε ελλιπή δίκτυα έχει μελετηθεί σε πολύ μικρότερο βαθμό. Μετά την αρχική μελέτη του Dolev [Dol82] η οποία αντιμετώπιζε ρητά το συγκεκριμένο πρόβλημα, ακολούθησαν άλλες δουλειές [Dol82, DDWY93, KGSR02] όπου ουσιαστικά αντιμετωπίζουν το πρόβλημα κυρίως μέσω πρωτοκόλλων για *αξιόπιστη και ασφαλή μετάδοση μηνύματος*. Από τα τελευταία προκύπτουν και πρωτόκολλα Αξιόπιστης Εκπομπής για ελλιπή δίκτυα, αφού μπορούν να χρησιμοποιηθούν για την προσομοίωση αξιόπιστων καναλιών επικοινωνίας (όπως ορίζονται στην Ενότητα 1.2 ) για κάθε ζεύγος παικτών. Όπως είναι φυσικό, εκτός από το φράγμα $t < n/3$, απαιτείται να τηρούνται επιπλέον περιορισμοί ως προς τη συνδεσιμότητα του δικτύου για να είναι το πρόβλημα επιλύσιμο. Για παράδειγμα, στην περίπτωση του φραγμένου αντιπάλου, το πολύ $t < c/2$ διαφθορές παικτών μπορούν να γίνουν ανεκτές, όπου $c$ είναι η συνδεσιμότητα του δικτύου και αυτό το όριο είναι ακριβές, όπως απο-




Σχήμα 1.2: Αξιόπιστη Εκπομπή σε ελλιπή δίκτυα

δείχθηκε στο [Dol82].

### Αξιόπιστη Επικοινωνία

Στην εργασία αυτή ασχολούμαστε με το πρόβλημα της *Αξιόπιστης Εκπομπής με τίμιο κόμβο-διανομέα* σε γενικά (ελλιπή) δίκτυα. Στη συνέχεια, για λόγους συντομίας, θα αναφερόμαστε σε αυτό το πρόβλημα πιο απλά ως *Πρόβλημα Εκπομπής*. Όπως θα δούμε στο κεφάλαιο 3.7, η περίπτωση αυτή αποτυπώνει ουσιαστικά τη δυσκολία του γενικού προβλήματος, όπου ακόμη και ο διανομέας μπορεί να διαφθαρεί. Αυτό προκύπτει, γιατί δοθείσας μίας λύσης στο απλούστερο αυτό πρόβλημα, μπορούμε να με προσομοιάσουμε τις μεταδόσεις ενός πρωτοκόλλου Αξιόπιστης Εκπομπής για πλήρη δίκτυα. Ο ορισμός του προβλήματος ακολουθεί.

**Πρόβλημα Εκπομπής (με τίμιο κόμβο-διανομέα).** Το δίκτυο μοντελοποιείται ως ένα γράφημα $G = (V, E)$, όπου $V$ είναι το σύνολο των παικτών και το σύνολο ακμών $E$ αντιπροσωπεύει κανάλια επικοινωνίας μεταξύ των παικτών. Υποθέτουμε την ύπαρξη ενός καθορισμένου, τίμιου κόμβου-διανομέα $D$, η αρχική τιμή του οποίου $x_D \in X$, όπου είναι ο χώρος των μηνυμάτων, πρέπει να διαδοθεί σε όλους τους παίκτες του δικτύου. Ένα κατανεμημένο πρωτόκολλο Π, ονομάζεται πρωτόκολλο Εκπομπής αν μετά το τέλος αυτού του πρωτοκόλλου, κάθε τίμιος παίκτης του δικτύου έχει αποφασίσει στην τιμή του διανομέα $x_D$, δηλαδή είναι σε θέση να εξάγει την τιμή $x_D$ που στάλθηκε αρχικά από τον διανομέα.

Όπως έχουμε τονίσει προηγουμένως, το πρόβλημα έχει τετριμμένη λύση σε πλήρη δίκτυα· έτσι, εδώ θα εξετάσουμε την περίπτωση ελλιπών δικτύων επικοινωνίας.

Παρατηρούμε ότι η επίτευξη Εκπομπής, όπως ορίστηκε παραπάνω, είναι στην πραγματικότητα ισοδύναμη με την επίτευξη ορθής (αξιόπιστης) μετάδοσης μηνύματος από τον κόμβο-

διανομέα $D$ σε όλους τους παίκτες. Η υπόθεση του τίμιου κόμβου-διανομέα είναι ιδιαίτερης σημασίας στην περίπτωση των ασύρματων δικτύων. Σε αυτό το μοντέλο, λόγω της επικοινωνίας μέσω τοπικών εκπομπών, ο διανομέας ουσιαστικά δεσμεύεται να στείλει την ίδια αρχική τιμή σε όλους του γείτονες του, και έτσι να δεσμευτεί σε αυτήν την τιμή.

Στην παρούσα εργασία, εξετάζουμε επίσης το συγγενές πρόβλημα της *Αξιόπιστης Μετάδοσης Μηνύματος* (Reliable Message Transmission–RMT), όπου ο κόμβος-διανομέας $D$ επιθυμεί να μεταδώσει ένα μήνυμα σε έναν άλλον κόμβο-παραλήπτη. Στην πραγματικότητα, μια λύση του προβλήματος RMT για κάθε ζεύγος $(D, v), v \in V$, συνεπάγεται μια λύση του προβλήματος Εκπομπής. Ο τυπικός ορισμός του προβλήματος ακολουθεί.

**Πρόβλημα Αξιόπιστης Μετάδοσης Μηνύματος (RMT).** Υποθέτουμε την ύπαρξη ενός καθορισμένου, κόμβου-διανομέα $D$, η αρχική τιμή του οποίου $x_D \in X$, όπου  είναι ο χώρος των μηνυμάτων, πρέπει να διαδοθεί σε έναν καθορισμένο παίκτη $R$ που ονομάζεται *παραλήπτης*. Ένα κατανεμημένο πρωτόκολλο, ονομάζεται πρωτόκολλο Αξιόπιστης Μετάδοσης Μηνύματος αν μετά το τέλος αυτού του πρωτοκόλλου, ο παραλήπτης $R$ έχει αποφασίσει στην τιμή του διανομέα $x_D$, δηλαδή είναι σε θέση να εξάγει την τιμή $x_D$ που του στάλθηκε αρχικά από τον διανομέα.

## 1.2 Το μοντέλο επικοινωνίας

Ένα δίκτυο επικοινωνίας αναπαρίσταται από ένα γράφημα $G = (V, E)$. Οι κόμβοι $V$ του γραφήματος αντιπροσωπεύουν τους παίκτες και οι ακμές $E$ τα μεταξύ τους κανάλια επικοινωνίας. Στη συνέχεια θα χρησιμοποιούμε τους όρους *παίκτης-κόμβος*, για να αναφερόμαστε στους συμμετέχοντες του συστήματος. Γενικά, ο κάθε παίκτης μπορεί να έχει κάποια αρχική πληροφορία/είσοδο στην αρχή του πρωτοκόλλου. Η ανταλλαγή πληροφορίας μεταξύ των παικτών συντελείται μέσω των καναλιών επικοινωνίας. Τα κανάλια που χρησιμοποιούνται σε ένα τέτοιο δίκτυο μπορούν να ταξινομηθούν ανάλογα με τον βαθμό αξιοπιστίας και ασφάλειας που τα χαρακτηρίζει. Οι διάφορες κατηγορίες καναλιών επικοινωνίας φαίνονται παρακάτω.

- **Αξιόπιστα κανάλια (Authenticated)**: Τα μηνύματα που μεταδίδονται μέσω τέτοιων καναλιών δεν μπορούν να παραποιηθούν από τον αντίπαλο αλλά ο αντίπαλος μπορεί να υποκλέψει το περιεχόμενο. Επιπλέον χρησιμοποιώντας αξιόπιστα κανάλια ο παραλήπτης ενός μηνύματος γνωρίζει πάντα την πραγματική ταυτότητα του αποστολέα.
- **Εμπιστευτικά κανάλια (Confidential)**: Τα μηνύματα που μεταδίδονται μπορούν να παραποιηθούν από τον αντίπαλο αλλά δεν γίνεται να υποκλαπεί το περιεχόμενό τους.
- **Ασφαλή κανάλια (Secure)**: Αξιόπιστα και εμπιστευτικά κανάλια.

Επίσης ως προς την καθυστέρηση μετάδοσης των μηνυμάτων έχουμε τις εξής κατηγορίες.

- **Σύγχρονα κανάλια (Synchronous)**: Η καθυστέρηση της μετάδοσης των μηνυμάτων στο κανάλι φράσσεται από μια γνωστή σταθερά.
- **Ασύγχρονα κανάλια (Asynchronous)**: Η καθυστέρηση, αν και πεπερασμένη, δεν φράσσεται από κάποια γνωστή σταθερά.

Η τοπολογία του δικτύου μπορεί να είναι *πλήρης* ή *ελλιπής*. Στη δεύτερη περίπτωση κάποια ζεύγη παικτών δεν μοιράζονται κάποιο κανάλι επικοινωνίας για να ανταλλάξουν μηνύματα μεταξύ τους.

Σε αυτήν την εργασία θα εστιάσουμε κυρίως σε σύγχρονα, ελλιπή δίκτυα με αξιόπιστα κανάλια.

## 1.3 Το μοντέλο του αντιπάλου

Όπως αναφέραμε και προηγουμένως, η αποκλίνουσα συμπεριφορά κάποιων παικτών μοντελοποιείται με έναν *κεντρικό αντίπαλο* ο οποίος τους διαφθείρει. Για παράδειγμα, ο αντίπαλος σε ένα πραγματικό σενάριο θα μπορούσε να αντιπροσωπεύει έναν hacker, ο οποίος έχει καταφέρει να αποκτήσει τον έλεγχο των μηχανημάτων που χειρίζονται οι παίκτες.

### 1.3.1 Είδος της διαφθοράς

Διαφορετικά μοντέλα αντιπάλου μπορούν να προσδιοριστούν σε σχέση με την ικανότητα διαφθοράς του αντιπάλου· η χειρότερη περίπτωση αντιπάλου, την οποία μελετάμε στην παρούσα δουλειά, είναι ο *Βυζαντινός ή Ενεργός* (Byzantine or Active) αντίπαλος.

**Βυζαντινός ή Ενεργός Αντίπαλος**: Οι διεφθαρμένοι παίκτες βρίσκονται υπό τον πλήρη έλεγχο του αντιπάλου και η συμπεριφορά τους μπορεί να παρεκκλίνει από το πρωτόκολλο με αυθαίρετο τρόπο.

### 1.3.2 Υπολογιστική δύναμη του αντιπάλου

Το μοντέλο αντιπάλου προσδιορίζει επίσης την υπολογιστική του ισχύ. Οι πιο συνηθισμένες υποθέσεις σε ότι αφορά το προηγούμενο είναι ότι ο αντίπαλος είτε είναι *υπολογιστικά περιορισμένος*, οπότε θεωρείται ότι περιορίζεται σε υπολογισμούς που διαρκούν πολυωνυμικό χρόνο ως προς κάποια παράμετρο ασφάλειας, είτε δεν έχει κανέναν περιορισμό ως προς την υπολογιστική του δύναμη και καλείται αντίπαλος *απεριόριστης υπολογιστικής ισχύος*.

Στη παρούσα εργασία, ασχολούμαστε με πρωτόκολλα που πετυχαίνουν τον στόχο τους ακόμα και υπό την παρουσία ενός Βυζαντινού αντιπάλου απεριόριστης υπολογιστικής ισχύος. Τα αποτελέσματα που παρουσιάζονται προφανώς ισχύουν και για άλλους τύπους αντιπάλου

αφού το μοντέλο που χρησιμοποιούμε αποτελεί ένα σενάριο χειρότερης περίπτωσης ως προς επίπτωση της διαφθοράς στο σύστημα.

### 1.3.3 Ευάλωτοι παίκτες

Τέλος, τα είδη αντιπάλου μπορούν να διακριθούν σε σχέση με τα σύνολα των παικτών που μπορεί να διαφθείρουν. Το μοντέλο του *$t$-φραγμένου αντιπάλου* που έχει μελετηθεί εκτενώς στη βιβλιογραφία αντιστοιχεί στην κατάσταση όπου ο αντίπαλος μπορεί να διαφθείρει το πολύ $t$ παίκτες στο δίκτυο. Σε αυτήν την εργασία εστιάζουμε στα ακόλουθα μοντέλα αντιπάλου ως προς το εύρος των παικτών που μπορούν να διαφθείρουν.

**$t$-Τοπικά Φραγμένος Αντίπαλος.** Ο αντίπαλος μπορεί να διαφθείρει το πολύ $t$ κόμβους-παίκτες στην γειτονιά κάθε κόμβου. Το μοντέλο αυτό προτάθηκε από τον Koo [Koo04] το 2004.

Η σημασία αυτού του μοντέλου προέρχεται, μεταξύ άλλων, από τους τοπικούς περιορισμούς που επιβάλλονται στον αντίπαλο, η οποία μπορεί να χρησιμοποιηθεί για τον σχεδιασμό κριτηρίων, τα οποία μπορούν να χρησιμοποιηθούν σε δίκτυα άγνωστης τοπολογίας όπου ο κάθε παίκτης γνωρίζει μόνο τους άμεσους γείτονές του με τους οποίους επικοινωνεί. Το μοντέλο τοπικά φραγμένου αντιπάλου είναι ιδιαίτερα σημαντικό στις σύγχρονες πρακτικές εφαρμογές. Για παράδειγμα, στα κοινωνικά δίκτυα είναι πιο πιθανό για έναν παίκτη να έχει μια αρκετά ακριβή εκτίμηση του μέγιστου αριθμού των κακόβουλων παικτών που μπορούν να εμφανιστούν στη γειτονιά του, παρά να έχει μια τέτοια εκτίμηση για ολόκληρο το δίκτυο. Στην πραγματικότητα, αυτό το σενάριο ισχύει για όλα τα είδη των δικτύων, όπου κάθε κόμβος θεωρείται ότι είναι σε θέση να εκτιμήσει το μέγεθος της διαφθοράς στην άμεση γειτονιά του. Είναι επίσης φυσικό το φράγμα των διεφθαρμένων παικτών να ποικίλει σε διάφορα τμήματα του δικτύου. Παρακινούμενοι από τέτοιες θεωρήσεις, σε επόμενα κεφάλαια εισάγουμε μια γενίκευση του $t$-τοπικά φραγμένου αντιπάλου όπου ο αντίπαλος έχει διαφορετικό φράγμα ως προς τους παίκτες που μπορεί να διαφθείρει σε κάθε γειτονιά.

Το μοντέλο γενικού αντιπάλου προτάθηκε και καθιερώθηκε από τους Hirt και Maurer στο [HM97], και εμπεριέχει όλα τα τα γνωστά μοντέλα αντιπάλου, συμπεριλαμβανομένων και τον προαναφερθέντων. Ακολουθεί η τυπική περιγραφή του μοντέλου.

**Μοντέλο Γενικού Αντιπάλου.** Ο αντίπαλος μπορεί να διαφθείρει οποιοδήποτε σύνολο παικτών σε μια δεδομένη οικογένεια συνόλων $\mathcal{Z}$ που ονομάζεται *δομή αντιπάλου*. Μια δομή $\mathcal{Z}$ για το σύνολο των παικτών $V$ είναι μια *μονότονη* οικογένεια υποσυνόλων του $V$, δηλαδή μια οικογένεια συνόλων όπου κάθε υποσύνολο συνόλου της οικογένειας ανήκει σε αυτήν, δηλαδή:

$$\mathcal{Z} \subseteq 2^V, \text{ έτσι ώστε } \forall Z \in \mathcal{Z}, \forall Z' \subseteq Z, Z' \in \mathcal{Z}$$

## 1.4 Τοπολογική Γνώση

Όσον αφορά την αρχική γνώση που οι παίκτες διαθέτουν για την τοπολογία του δικτύου, επί το πλείστον έχουν μελετηθεί στη σχετική βιβλιογραφία οι επόμενες δύο περιπτώσεις.

- ***Ad Hoc* Δίκτυα (ή δίκτυα άγνωστης τοπολογίας)** : Κάθε παίκτης γνωρίζει μόνο τις ταυτότητες (ids) των άμεσων γειτόνων του.
- **Δίκτυα Γνωστής τοπολογίας**: Κάθε παίκτης γνωρίζει την τοπολογία ολόκληρου του δικτύου (ταυτότητες κόμβων και αντίστοιχες ακμές).

### 1.4.1 Μοντέλο μερικής γνώσης

Σε αυτήν την εργασία εισάγουμε επίσης το *Μοντέλο Μερικής Γνώσης*, στο οποίο κάθε παίκτης γνωρίζει μόνο την τοπολογία ενός αυθαίρετου υπογραφήματος του δικτύου στο οποίο ο ίδιος περιλαμβάνεται. Τυπικός ορισμός του μοντέλου αυτού ακολουθεί σε επόμενο κεφάλαιο.

Όπως μπορεί να δει κανείς στα επόμενα κεφάλαια της εργασίας, η γνώση ενός παίκτη ως προς τα πιθανά σύνολα διεφθαρμένων παικτών, συσχετίζεται φυσιολογικά με την τοπολογική γνώση που αυτός κατέχει. Η ανάγκη μελέτης μοντέλων περιορισμένης γνώσης υπαγορεύεται από εφαρμογές σε δίκτυα ευρείας κλίμακας (π.χ. το διαδίκτυο), όπου η εκτίμηση του βαθμού δυσλειτουργίας μπορεί να γίνει με σχετική ακρίβεια από τον κάθε συμμετέχοντα στα πλαίσια της γειτονιάς του, ενώ μια συνολική εκτίμηση μπορεί να είναι δύσκολο να επιτευχθεί λόγω γεωγραφικών περιορισμών και περιορισμών δικαιοδοσίας. Επιπλέον, η εγγύτητα κόμβων σε κοινωνικά δίκτυα συχνά συσχετίζεται με αυξημένη ποσότητα διαθέσιμης πληροφορίας, γεγονός που δικαιολογεί περαιτέρω την ευστάθεια του μοντέλου.

## 1.5 Αποδοτικότητα Κατανεμημένων Πρωτοκόλλων

Η πολυπλοκότητα ενός κατανεμημένου πρωτοκόλλου μπορεί να αναλυθεί με βάση το μέγιστο ποσό υπολογισμών που κάθε παίκτης πρέπει να εκτελέσει τοπικά (*τοπική πολυπλοκότητα χειρότερης περίπτωσης*) και με βάση το συνολικό ποσό πληροφορίας που απαιτείται να ανταλλαχθεί μεταξύ των παικτών κατά τη διάρκεια του πρωτοκόλλου. Επιπλέον, ο αριθμός των γύρων επικοινωνίας που απαιτούνται για την ολοκλήρωση του πρωτοκόλλου είναι ένα άλλο μέτρο το οποίο πρέπει να ληφθεί υπόψη. Σε σύγχρονα δίκτυα, με τα οποία ασχολούμαστε σε αυτή την εργασία, υποθέτουμε ότι κατά τη διάρκεια κάθε γύρου επικοινωνίας, όλοι οι κόμβοι παράλληλα λαμβάνουν τα τελευταία μηνύματα από τους γείτονές τους, εκτελούν τους τοπικούς υπολογισμούς που υπαγορεύονται από το πρωτόκολλο, και τελικά στέλνουν κάποια νέα μηνύματα στους γείτονές τους. οι παράγοντες που εξετάζονται προς βελτιστοποίηση σε ένα κατανεμημένο πρωτόκολλο είναι οι ακόλουθοι:

- **Πολυπλοκότητα Επικοινωνίας (Bit/Communication Complexity)**: Ο μέγιστος συνολικός αριθμός bits που στέλνονται από όλους τους τίμιους παίκτες κατά τη διάρκεια του πρωτοκόλλου, μεταξύ όλων των πιθανών εκτελέσεων αυτού. Θα χρησιμοποιήσουμε επίσης τον όρο **Πολυπλοκότητα Μηνυμάτων** για τον συνολικό αριθμό των μηνυμάτων που αποστέλλονται από όλους τους τίμιους παίκτες.
- **Πολυπλοκότητα Γύρων (Round Complexity)**: Ο μέγιστος αριθμός διαδοχικών γύρων επικοινωνίας, που χρειάζεται έτσι ώστε όλοι οι τίμιοι παίκτες να τερματίσουν το πρωτόκολλο, μεταξύ όλων των πιθανών εκτελέσεων αυτού.
- **Τοπική Υπολογιστική Πολυπλοκότητα (Local Computations Complexity)**: Η μέγιστη τοπική πολυπλοκότητα χειρότερης περίπτωσης μεταξύ όλων των παικτών και των πιθανών εκτελέσεων του πρωτοκόλλου.

Ένα κατανεμημένο πρωτόκολλο για το οποίο όλοι οι παραπάνω παράγοντες παραμένουν πολυωνυμικοί ονομάζεται **Πλήρως Πολυωνυμικό Πρωτόκολλο** (Fully Polynomial protocol).

# Κεφάλαιο 2

# Εκπομπή σε *Ad Hoc* Δίκτυα με Τοπικά Φραγμένο Αντίπαλο

Σε αυτό το κεφάλαιο θα εξετάσουμε το πρόβλημα Εκπομπής σε ελλιπή δίκτυα. Μελετάμε την ανοχή (απέναντι σε σφάλματα) του αλγορίθμου Certified Propagation Algorithm (CPA) [Koo04], ο οποίος είναι κατάλληλος για *ad hoc* δίκτυα. Αντιμετωπίζουμε το ζήτημα του προσδιορισμού του μέγιστου αριθμού των διεφθαρμένων παικτών $t_{\max}^{\text{CPA}}$ που ο CPA μπορεί να ανεχθεί στο μοντέλο του $t$-τοπικά φραγμένου αντιπάλου, στο οποίο ο αντίπαλος μπορεί να διαφθείρει το πολύ $t$ παίκτες στην γειτονιά του κάθε παίκτη. Για κάθε γράφημα $G$ και διανομέα $D$ παρέχουμε άνω και κάτω φράγματα για το $t_{\max}^{\text{CPA}}$, τα οποία μπορούν να υπολογιστούν αποδοτικά μέσω μιας γραφοθεωρητικής παραμέτρου που παρουσιάζουμε σε αυτό το κεφάλαιο. Στην πορεία αυτής της μελέτης σχεδιάζουμε έναν αποδοτικό 2-προσεγγιστικό αλγόριθμο για τον υπολογισμό του $t_{\max}^{\text{CPA}}$. Επιπλέον εισάγουμε δύο ακόμα γραφοθεωρητικές παραμέτρους, μία εκ των οποίων αντιστοιχεί ακριβώς στην παράμετρο $t_{\max}^{\text{CPA}}$. Η προσέγγισή που ακολουθούμε, μας επιτρέπει να απαντήσουμε καταφατικά στο ανοιχτό πρόβλημα, από το 2005, της *Μοναδικότητας του CPA* [PP05].

## 2.1 Εισαγωγή

Στην περίπτωση ενός έντιμου διανομέα, ιδιαίτερα χρήσιμης σε ασύρματα δίκτυα λόγω των αξιόπιστων τοπικών εκπομπών, το αναγκαίο φράγμα $t < n/3$ για την επιλυσιμότητα του προβλήματος της Αξιόπιστης Εκπομπής δεν ισχύει· για παράδειγμα, σε πλήρη δίκτυα το πρόβλημα γίνεται τετριμμένο. Ωστόσο, σε ελλιπή δίκτυα η κατάσταση είναι διαφορετική. Ένας μικρός αριθμός των προδοτών (διεφθαρμένοι παίκτες) μπορούν να καταφέρουν να αλλοιώσουν το αποτέλεσμα του πρωτοκόλλου, ελέγχοντας ένα κρίσιμο μέρος του δικτύου, π.χ. αν οι διεφθαρμένοι παίκτες αποτελούν ένα *διαχωριστή* του δικτύου, δηλαδή ένα σύνολο κόμβων που η αφαίρεσή τους από το γράφημα το καθιστά μη συνεκτικό. Είναι επομένως λογικό να ορι-

στούν κριτήρια, βασισμένα στη δομή του γραφήματος (σε γραφοθεωρητικές παραμέτρους), ώστε να φράσσεται ο αριθμός ή να περιοριστεί η κατανομή προδοτών στο δίκτυο.

Μια προσέγγιση προς αυτή την κατεύθυνση είναι η εξέταση τοπολογικών περιορισμών ως προς την ικανότητα διαφθοράς του αντιπάλου. Η σημασία των τοπικών περιορισμών έγκειται, μεταξύ άλλων, στο γεγονός ότι αυτοί οι περιορισμοί μπορούν να χρησιμοποιηθούν για την εξαγωγή τοπικών κριτηρίων τα οποία οι παίκτες μπορούν να χρησιμοποιήσουν για την επίτευξη Εκπομπής σε *ad hoc* δίκτυα. Ένα τέτοιο παράδειγμα είναι το μοντέλο *$t$-τοπικά φραγμένου αντιπάλου* που προτάθηκε από τον Koo στο [Koo04], στο οποίο το πολύ $t$ διαφθορές μπορούν να εμφανιστούν στη γειτονιά κάθε κόμβου.

Ο Koo [Koo04] πρότεινε ένα απλό, αλλά με μεγάλες δυνατότητες πρωτόκολλο για την Εκπομπή στο μοντέλο τοπικά φραγμένου αντιπάλου. Το πρωτόκολλο αυτό, ονομάστηκε αργότερα από τους Pelc, Peleg [PP05] *Certified Propagation Algorithm*(CPA) και μελετήθηκε από τον Koo σε δίκτυα ειδικής τοπολογίας (δίκτυα πλέγματος). Το 2005, οι Pelc και Peleg [PP05] μελέτησαν το μοντέλο $t$-τοπικά φραγμένου αντιπάλου σε γραφήματα γενικής τοπολογίας και πρότειναν μια ικανή τοπολογική συνθήκη υπό την οποία ο CPA μπορεί να επιτύχει εκπομπή σε κάθε δίκτυο. Επίσης παρείχαν ένα άνω φράγμα, που περιγράφεται από μια γραφοθεωρητική παράμετρο, για τον αριθμό των διεφθαρμένων παικτών $t$ που μπορεί να γίνει ανεκτός τοπικά από οποιοδήποτε πρωτόκολλο Εκπομπής. Η εξαγωγή ακριβέστερων φραγμάτων αφέθηκε από τους Pelc, Peleg σαν ανοικτό πρόβλημα. Σε αυτήν την κατεύθυνση, προτάθηκε από τους Ichimura and Shigeno [IS10] μια αποδοτικά υπολογίσιμη γραφοθεωρητική παράμετρος η οποία δίνει τελικά έναν καλύτερο, αλλά όχι ακριβή, χαρακτηρισμό της οικογένειας των γραφημάτων στην οποία ο CPA πετυχαίνει Εκπομπή. Έχει παραμείνει ανοικτό πρόβλημα από το 2005 η εξαγωγή μιας παραμέτρου η οποία αποκαλύπτει τον ακριβή αριθμό προδοτών $t$ για τον οποίο ο CPA είναι *$t$-ανεκτικός*, δηλαδή ο αριθμός $t$ ο οποίος μπορεί να γίνει τοπικά ανεκτός από τον CPA για οποιοδήποτε γράφημα $G$ με διανομέα $D$.

Πολύ πρόσφατα οι Tseng,Vaidya και Bhandari [TVB15] ανεξάρτητα από την παρούσα δουλειά, προτείνανε μια ικανή και αναγκαία συνθήκη για την Εκπομπή μέσω CPA. Εδώ, παρέχουμε μια αναγκαία και ικανή συνθήκη, που περιγράφεται από μια νέα παράμετρο όπως εξηγείται παρακάτω. Η προσέγγισή αυτή, μας επιτρέπει να παρέχουμε μια καταφατική απάντηση στο ανοιχτό πρόβλημα της *μοναδικότητας του CPA* [PP05].

## 2.2 Διάρθρωση του κεφαλαίου

Μελετάμε τη συμπεριφορά του CPA σε γενικά (ελλιπή) δίκτυα, όπου ο παίκτης-διανομέας είναι τίμιος. Όπως θα δούμε στην Ενότητα 2.10, η περίπτωση αυτή αποτυπώνει ουσιαστικά τη δυσκολία του γενικού προβλήματος όπου ακόμα και ο διανομέας μπορεί να είναι διεφθαρμένος. Η αρχική μας συνεισφορά είναι ο ακριβής προσδιορισμός του μέγιστου αριθμού των διεφθαρμένων παικτών $t^{\text{CPA}}_{\max}(G, D)$ ο οποίος μπορεί να γίνει τοπικά ανεκτός από τον CPA, για οποιοδήποτε γράφημα $G$ με διανομέα $D$. Καταφέρνουμε αυτό αναπτύσσοντας τις ακόλουθες τρεις γραφοθεωρητικές παραμέτρους:

- Η παράμετρος $\mathcal{K}(G, D)$ προσδιορίζεται μέσω μιας κατάλληλης *διάταξης-επιπέδων* των κόμβων του γραφήματος. Δείχνουμε ότι η συνθήκη $t < \mathcal{K}(G, D)/2$ είναι ικανή για να είναι ο CPA to be $t$-τοπικά ανεκτικός και ότι η $t < \mathcal{K}(G, D)$ αναγκαία συνθήκη, γεγονός που υποδηλώνει ότι $\lceil \mathcal{K}(G, D)/2 \rceil - 1 \leq t^{\text{CPA}}_{\text{max}} < \mathcal{K}(G, D)$. Αποδεικνύουμε ότι η παράμετρος αυτή συμπίπτει με την παράμετρο $\widetilde{\mathcal{X}}(G, D)$ που παρουσιάζεται στο [IS10]. Επιπλέον προτείνουμε έναν αποδοτικό αλγόριθμο για τον υπολογισμό της παραμέτρου $\mathcal{K}(G, D)$, ο οποίος είναι χαμηλότερης χρονικής πολυπλοκότητας από τον αλγόριθμο που προτείνεται στο [IS10] για τον υπολογισμό της $\widetilde{\mathcal{X}}(G, D)$. Σημειώνεται ότι αυτό μας παρέχει άμεσα έναν αποδοτικό 2-προσεγγιστικό αλγόριθμο για τον υπολογισμό του $t^{\text{CPA}}_{\text{max}}$ και παρέχουμε ένα παράδειγμα που δείχνει ότι ο λόγος προσέγγισης 2 είναι ακριβής για αυτόν τον αλγόριθμο.

- Η παράμετρος $\mathcal{M}(G, D, t)$, που εξαρτάται από την τιμή $t$, είναι μια παράμετρος που μπορεί να χρησιμοποιηθεί για να απαντήσουμε στο εάν ο CPA είναι $t$-τοπικά ανεκτικός για ένα γράφημα $G$ με διανομέα $D$, ελέγχοντας απλά εάν ισχύει το $\mathcal{M}(G, D, t) \geq t+1$. Επομένως, μέσω αυτής της παραμέτρου, παρέχουμε μία αναγκαία και ικανή συνθήκη έτσι ώστε ο CPA να είναι $t$-τοπικά ανεκτικός. Μια τέτοια συνθήκη δεν ήταν γνωστή στην βιβλιογραφία μέχρι πολύ πρόσφατα, όπου ανεξάρτητα από την παρούσα εργασία παρουσιάστηκε μία αναγκαία και ικανή συνθήκη στο [TVB15]. Ωστόσο, ο τρόπος με τον οποίο ορίζεται η συνθήκη στο [TVB15], υπονοεί έναν υπερεκθετικό αλγόριθμο για τον έλεγχο της (στην πραγματικότητα δεν παρουσιάζεται κάποιος αλγόριθμος στο [TVB15]). Από την άλλη πλευρά, θα δούμε ότι ακόμη και ένας αφελής αλγόριθμος για τον υπολογισμό της παραμέτρου $\mathcal{M}(G, D, t)$ απαιτεί εκθετικό χρόνο.

- Τέλος, η παράμετρος $\mathcal{T}(G, D) = \max\{t \in \mathbb{N} \mid \mathcal{M}(G, D, t) \geq t + 1\}$, μας δίνει ακριβώς το μέγιστο αριθμό διεφθαρμένων παικτών που μπορεί να ανεχθεί ο CPA σε κάθε γειτονιά, επομένως ταυτίζεται με την παράμετρο $t^{\text{CPA}}_{\text{max}}(G, D)$.

Επιπλέον, χρησιμοποιώντας την παράμετρο $\mathcal{M}(G, D, t)$ αποδεικνύουμε πως ο CPA είναι τελικά *μοναδικός* μεταξύ *ad hoc* αλγορίθμων Εκπομπής. Δηλαδή, αν ένας *ad hoc* αλγόριθμος Εκπομπής είναι $t$-ανεκτικός για ένα γράφημα $G$ με διανομέα $D$, τότε και ο CPA είναι $t$-ανεκτικός για τα $G, D$. Με αυτόν τον τρόπο, παρέχουμε μια καταφατική απάντηση στο ανοιχτό ερώτημα της μοναδικότητας του CPA που είχε τεθεί στο [PP05].

## 2.3 Ορισμός μοντέλου και προβλήματος

Σε αυτή την ενότητα, ορίζουμε τυπικά το πρόβλημα και το μοντέλο στο οποίο θα μελετηθεί, καθώς και μερικές χρήσιμες έννοιες που διευκολύνουν την παρουσίαση αυτής της εργασίας. Όπως αναφέρθηκε προηγουμένως, ο στόχος της Αξιόπιστης Εκπομπής είναι να επιτρέψουμε σε κάποιον καθορισμένο παίκτη, που ονομάζεται διανομέας, να διαμοιράσει συνεπώς την αρχική του τιμή σε όλους τους άλλους παίκτες του δικτύου, ακόμη και στην περίπτωση παρουσίας ενός κεντρικού αντιπάλου που διαφθείρει κάποιους παίκτες και να τους ελέγχει σε

κάποιο βαθμό. Κατά συνέπεια, η αποτελεσματικότητα ενός πρωτοκόλλου Αξιόπιστης Εκπομπής θα πρέπει να μελετάται σε σχέση με τις δυνατότητες διαφθοράς του αντιπάλου, οι οποίες ορίζονται ακριβώς από το *μοντέλο αντιπάλου.*

**Μοντέλο αντιπάλου $\mathcal{T}$.** Ένα μοντέλο αντιπάλου $\mathcal{T}$ ορίζει τα σύνολα των παικτών που μπορούν να διαφθαρούν από έναν $\mathcal{T}$-αντίπαλο (πιθανά/επιτρεπτά σύνολα διαφθοράς) καθώς και την πιθανή συμπεριφορά των διεφθαρμένων παικτών, δηλαδή, όλες τις πιθανές ενέργειες που εκτελούνται από αυτούς. Η συμπεριφορά του αντιπάλου σε μία εκτέλεση ενός κατανεμημένου πρωτοκόλλου, μπορεί να περιγραφεί με ακρίβεια από το σύνολο και τις ενέργειες των διεφθαρμένων παικτών· πιο συγκεκριμένα, μπορούμε να θεωρήσου ότι το $\mathcal{T}$ είναι ένα σύνολο ζευγών $T = (C, \Pi_C)$ όπου $C$ είναι το σύνολο των διεφθαρμένων παικτών και $\Pi_C$ είναι το κατανεμημένο πρωτόκολλο που αυτοί εκτελούν. Θεωρούμε το μοντέλο Βυζαντινού αντιπάλου το οποίο δεν επιβάλει κανέναν περιορισμό στην συμπεριφορά των διεφθαρμένων παικτών.Όσον αφορά τα πιθανά σύνολα διαφθοράς, σε αυτό το κεφάλαιο, λαμβάνουμε υπόψιν το μοντέλο $t$-τοπικά φραγμένου αντιπάλου το οποίο θα οριστεί τυπικά παρακάτω.

Η μοντελοποίηση του δικτύου επικοινωνίας μέσω του οποίου οποίο συνδέονται οι παίκτες ακολουθεί.

**Μοντελοποίηση του δικτύου.** Υποθέτουμε ότι το σύνολο των παικτών $V$ και τα κανάλια μεταξύ τους επικοινωνίας, ορίζουν ένα δίκτυο επικοινωνίας το οποίο αναπαρίσταται με το γράφημα $G = (V, E)$ όπου $E$ είναι το σύνολο των μη κατευθυνόμενων και αξιόπιστων καναλιών επικοινωνίας μεταξύ ζευγών παικτών.

Θα συμβολίζουμε με $\mathcal{N}(v)$ τη γειτονιά ενός κόμβου $v$ στο $G$, επίσης θα συμβολίζουμε τους κόμβους ενός γραφήματος $G$ με $V(G)$.

Σε αυτό το κεφάλαιο ασχολούμαστε με το πρόβλημα της *Αξιόπιστης Εκπομπής με τίμιο διανομέα* σε γενικά (πιθανώς ελλιπή) δίκτυα. Για λόγους συντομίας θα αναφερόμαστε σε αυτό απλώς ως *πρόβλημα Εκπομπής*. Η λύση του προβλήματος είναι τετριμμένη σε πλήρη δίκτυα; οι μελέτες που παρουσιάζονται σε αυτήν την εργασία απευθύνονται στην γενικότερη περίπτωση των ελλιπών δικτύων. Όπως θα δούμε στην Ενότητα 2.10, η περίπτωση τίμιου διανομέα ουσιαστικά αποτυπώνει και τη δυσκολία του γενικού προβλήματος, όπου ακόμα και ο διανομέας μπορεί να διαφθαρεί. Ένα πρωτόκολλο για τη γενική περίπτωση μπορεί να κατασκευαστεί προσομοιώνοντας την ανταλλαγή μηνυμάτων που χρησιμοποιείται σε πρωτόκολλα αξιόπιστης εκπομπής για πλήρη δίκτυα, τα οποία έχουν μελετηθεί εκτενώς. Τέλος, θεωρούμε ντετερμινιστικά πρωτόκολλα για την επίλυση του προβλήματος.

***Ορισμός* 2.1** (Αξιόπιστη Εκπομπή με τίμιο διανομέα/Εκπομπή). *Έστω $V = \{v_1, \ldots, v_n\}$ το σύνολο των $n$ παικτών που συνδέονται μέσω του δικτύου επικοινωνίας $G = (V, E)$ όπως αυτό περιγράφηκε παραπάνω και $X$ ένα πεπερασμένο πεδίο τιμών. Θεωρούμε ένα κατανεμημένο πρωτόκολλο $\Pi$ μεταξύ των παικτών $V$, όπου ο παίκτης $D \in V$ (που ονομάζεται* διανομέας*) έχει τιμή εισόδου $x_D \in X$ και κάθε παίκτης $v \in V$ τελικά αποφασίζει σε μια μοναδική τιμή εξόδου $y_v \in X$. Επίσης υποθέτουμε οποιοδήποτε μοντέλο αντιπάλου $\mathcal{T}$ τέτοιο ώστε ο διανομέας δεν μπορεί να διαφθαρεί. Το*

*πρωτόκολλο* $\Pi$ *πετυχαίνει Εκπομπή στο* $(G, D)$ *υπό το μοντέλο αντιπάλου* $\mathcal{T}$ *εάν για κάθε πιθανό σύνολο διαφθοράς* $T$ *και κάθε πιθανή συμπεριφορά αυτού σύμφωνα με το μοντέλο* $\mathcal{T}$*, όλοι οι τίμιοι παίκτες αποφασίζουν στην τιμή εισόδου του διανομέα, δηλαδή,* $\forall v \in V \setminus T, y_v = x_D$.

Ο *τερματισμός* του πρωτοκόλλου συνήθως απαιτείται στον καθιερωμένο ορισμό της Εκπομπής, δηλαδή, δηλαδή, πρέπει να εξασφαλιστεί ότι όλοι οι τίμιοι παίκτες τελικά τερματίζουν το πρωτόκολλο. Όπως συνηθίζεται στη σχετική βιβλιογραφία, παραλείπουμε τη μελέτη τερματισμού, η οποία συχνά προκύπτει άμεσα από την ορθότητα των αλγορίθμων. Συζητάμε το ζήτημα του τερματισμού με συντομία στην Ενότητα 3.8.

Στη συνέχεια, θα χρησιμοποιήσουμε ανεπίσημα τον όρο *πρωτόκολλο Εκπομπής* (ή αλγόριθμο) για κάθε κατανεμημένο αλγόριθμο που αποσκοπεί στην επίτευξη Εκπομπής, ανεξάρτητα αν είναι επιτυχής ή όχι.

Η μελέτη που παρουσιάζεται σε αυτό το κεφάλαιο αφορά το μοντέλο $t$-τοπικά φραγμένου αντιπάλου που εισήγαγε ο Koo στο [Koo04]. Η οικογένεια των *$t$-τοπικών* συνόλων (όπως ορίζεται παρακάτω) είναι σημαντική για τη μελέτη μας, δεδομένου ότι συμπίπτει με την οικογένεια των πιθανών συνόλων διαφθοράς.

***Ορισμός*** **2.2** ($t$-τοπικό σύνολο). *Δεδομένου ενός γραφήματος* $G = (V, E)$ *και ενός φυσικού* $t \in \mathbb{N}$*, ένα σύνολο* $C \subseteq V$ *ονομάζεται* $t$-τοπικό *εάν έχει την ιδιότητα:*

$$\forall u \in V,\ |\mathcal{N}(u) \cap C| \leq t.$$

**Μοντέλο $t$-τοπικά περιορισμένου αντιπάλου.** Σε αυτό το μοντέλο, ο αντίπαλος μπορεί να διαφθείρει μόνο ένα $t$-τοπικό σύνολο παικτών κατά τη διάρκεια της εκτέλεσης ενός πρωτοκόλλου στο σύστημα.

Στο μοντέλο του $t$-φραγμένου αντιπάλου, που έχει μελετηθεί εκτενώς στη βιβλιογραφία (βλ. [LSP82]), δίνεται ένα φράγμα για τον συνολικό αριθμό των διαφθορών. Αντιθέτως, στο μοντέλο $t$-τοπικά φραγμένου αντιπάλου, οι διαφθορές στην γειτονιά κάθε τίμιου παίκτη φράσσονται από μια σταθερά $t$. Η θεώρηση αυτή μοντελοποιεί μια κατάσταση όπου οι διεφθαρμένοι παίκτες κατανέμονται ομοιόμορφα, υπό κάποια έννοια, σε όλο το δίκτυο. Άλλωστε, η ύπαρξη ενός φράγματος στον συνολικό αριθμό των διαφθορών, δεν είναι τόσο ενδιαφέρουσα σε ελλιπή δίκτυα δεδομένου ότι ένας αντίπαλος θα μπορούσε απλώς να διαφθείρει τους γείτονες ενός συγκεκριμένου τίμιου παίκτη και ως εκ τούτου, να εμποδίσει κάθε μετάδοση μηνύματος σε αυτόν.

### 2.3.1 Ιδιότητες πρωτοκόλλων

Στη συνέχεια ορίζουμε κάποιες ιδιότητες πρωτοκόλλων, μερικές από τις οποίες προτάθηκαν στο [PP05], οι οποίες διευκολύνουν την παρούσα μελέτη και θα χρησιμοποιηθούν σε όλη την εργασία.

***Ορισμός*** **2.3** ($t$-τοπικά ανεκτικός αλγόριθμος για το $(G, D)$). *Ένας αλγόριθμος που πετυχαίνει Εκπομπή στο γράφημα $G$ με διανομέα $D$ για κάθε $t$-τοπικό σύνολο διαφθορών $T$ και κάθε πιθανή συμπεριφορά του $T$ ονομάζεται* $t$-τοπικά ανεκτικός αλγόριθμος για το $(G, D)$.

Σύμφωνα με τον ορισμό του προβλήματος της Εκπομπής, ένας τοπικά ανεκτικός αλγόριθμος για το $(G, D)$ είναι ένας αλγόριθμος ο οποίος πετυχαίνει Εκπομπή στο $(G, D)$ υπό το μοντέλο $t$-τοπικά φραγμένου αντιπάλου.

***Ορισμός*** **2.4** (Ασφαλής / $t$-τοπικά ασφαλής αλγόριθμος). *Ένας αλγόριθμος, μέσω του οποίου κανένας τίμιος παίκτης δεν αποφασίζει σε λάθος τιμή, για κάθε ζεύγος γραφήματος-διανομέα $(G, D)$, υπό οποιοδήποτε σύνολο διαφθορών και οποιαδήποτε συμπεριφορά αυτού (δηλαδή υπό οποιοδήποτε μοντέλο αντιπάλου), ονομάζεται ασφαλής.*

*Ένας αλγόριθμος, μέσω του οποίου κανένας τίμιος παίκτης δεν αποφασίζει σε λάθος τιμή, για κάθε ζεύγος γραφήματος-διανομέα $(G, D)$, υπό οποιοδήποτε $t$-τοπικό σύνολο διαφθορών και οποιαδήποτε συμπεριφορά αυτού (δηλαδή υπό το μοντέλο $t$-τοπικά φραγμένου αντιπάλου), ονομάζεται $t$-τοπικά ασφαλής.*

Σημειώνεται ότι ένας ασφαλής αλγόριθμος θα μπορούσε να αποτύχει, συγκεκριμένα παραδίδοντας εσφαλμένα (ή καθόλου) το μήνυμα σε όλους τους κόμβους του δικτύου. Με τον όρο εσφαλμένη παράδοση εδώ, εννοούμε οι πληροφορία που λαμβάνονται από έναν παίκτη δεν επαρκεί για να αποφασίσει. Ουσιαστικά, ένας ασφαλής αλγόριθμο Εκπομπής, εξασφαλίζει ότι ένας παίκτης θα αποφασίσει σε μία τιμή μόνο στην περίπτωση μόνο στην περίπτωση που μπορεί να συμπεράνει από την πληροφορία που έχει λάβει, ότι αυτή είναι η πραγματική τιμή του διανομέα.

Παρατηρείστε ότι κάποιος αλγόριθμος είναι $t$-τοπικά ασφαλής εφόσον ικανοποιεί την επιθυμητή ιδιότητα για κάθε στιγμιότυπο $(G, D)$. Από την άλλη, ο αλγόριθμος είναι $t$-τοπικά ανεκτικός για το $(G, D)$ αν ικανοποιεί την επιθυμητή ιδιότητα για το συγκεκριμένο στιγμιότυπο $(G, D)$. Ως εκ τούτου, υπάρχουν περιπτώσεις όπου ένας αλγόριθμος είναι $t$-τοπικά ανεκτικός γαι το $(G, D)$, αλλά δεν είναι $t$-τοπικά ασφαλής, ακόμη και αν η πρώτη ιδιότητα συνεπάγεται τετριμμένα ότι η ιδιότητα της ασφάλειας ισχύει για το στιγμιότυπο $(G, D)$.

Η σημασία της ασφάλειας ενός αλγορίθμου επισημαίνεται στο [PP05], όπου θεωρείται ως βασική προϋπόθεση που πρέπει να ικανοποιεί ένας αλγόριθμος Εκπομπής· εγγυάται ότι ακόμη και αν όλοι οι παίκτες δεν έχουν επαρκείς πληροφορίες για να αποφασίσουν σχετικά με την τιμή του διανομέα, κανείς δεν θα αποφασίσει τελικά σε μια λανθασμένη τιμή ή ψευδή δεδομένα. Παρακάτω ορίζουμε τυπικά την έννοια της *μοναδικότητας* ενός αλγορίθμου.

***Ορισμός*** **2.5** (Μοναδικότητα αλγορίθμου). *Έστω $\mathcal{A}$ μία οικογένεια αλγορίθμων. Ένας αλγόριθμος $A$ ονομάζεται μοναδικός (για το πρόβλημα της Εκπομπής) μεταξύ αλγορίθμων στην οικογένεια $\mathcal{A}$ (ή μοναδικός στην οικογένεια $\mathcal{A}$ ), εάν η ύπαρξη ενός αλγορίθμου της οικογένειας $\mathcal{A}$ ο οποίος πετυχαίνει Εκπομπή σε ένα στιγμιότυπο $(G, D)$ συνεπάγεται ότι ο $A$ πετυχαίνει Εκπομπή στο $(G, D)$.*

Ένας μοναδικός αλγόριθμος $A$ στην οικογένεια $\mathcal{A}$, ορίζει φυσιολογικά την κλάση των στιγμιοτύπων $(G, D)$ στα οποία το πρόβλημα είναι επιλύσιμο από $\mathcal{A}$-αλγόριθμους, δηλαδή ακριβώς αυτά τα στιγμιότυπα στα οποία ο $A$ πετυχαίνει Εκπομπή.

## 2.4 Ο Αλγόριθμος CPA

Όπως εξηγήσαμε προηγουμένως, θεωρούμε ένα δίκτυο όπου μπορούν να εμφανιστούν το πολύ $t$ διαφθορές στην γειτονιά κάθε κόμβου. Κάθε σύνολο με την παραπάνω ιδιότητα λοιπόν είναι ένα πιθανό σύνολο διεφθαρμένων παικτών.

Στον αλγόριθμο CPA, οι παίκτες χρησιμοποιούν μόνο τοπικές πληροφορίες. Αυτό καθιστά τον CPA ιδανικό για *ad hoc* δίκτυα, όπου η τοπολογική γνώση του κάθε παίκτη περιορίζεται στην γειτονιά του. Ο CPA είναι πιθανώς ο μόνος γνωστός αλγόριθμος Εκπομπής για το μοντέλου τοπικά φραγμένου αντιπάλου, ο οποίος δεν χρησιμοποιεί γνώση της τοπολογίας του δικτύου ή υπορουτίνες ανακάλυψης της τοπολογίας.

---

**Πρωτόκολλο 1**: ***Certified Propagation Algorithm (CPA)***

---

***Είσοδος:***
(Για κάθε παίκτη $v$) Ταυτότητα του διανομέα $D$, ταυτότητες γειτόνων του $v$, παράμετρος αντιπάλου $t$.
(Για τον διανομέα $D$) Αρχική τιμή $x_D$.
*Μορφή μηνυμάτων*: Τιμή $x \in X$, όπου $X$ ο χώρος μηνυμάτων.

**Κώδικας του** $D$: Στείλε $x_D \in X$ σε όλους τους γείτονες, αποφάσισε στο $x_D$ και τερμάτισε.

**Κώδικας του** $v \in \mathcal{N}(D)$: Αφού λάβεις την τιμή $x_D$ από τον διανομέα, αποφάσισε στο $x_D$, στείλε το $x_D$ σε όλους τους γείτονές σου και τερμάτισε.

(* *κανόνας πιστοποιημένης διάδοσης* *)

**Κώδικας του** $v \notin \mathcal{N}(D) \cup D$: Αν λάβεις $t+1$ μηνύματα με την ίδια τιμή $x$ από $t+1$ διαφορετικούς γείτονες, αποφάσισε στο $x$, στείλε το $x$ σε όλους τους γείτονές σου και τερμάτισε.

---

Στο [Koo04], αποδείχθηκε ότι ο CPA είναι $t$-τοπικά ασφαλής αλγόριθμος Εκπομπής. Παρακάτω παρουσιάζουμε την απόδειξη για λόγους πληρότητας.

***Θεώρημα* 2.1**. *Ο αλγόριθμος CPA είναι $t$-τοπικά ασφαλής.*

*Απόδειξη.*
Θα δείξουμε ότι αν ένας παίκτης αποφασίσει στην τιμή $x$ μέσω του CPA τότε $x = x_D$. Υποθέτουμε ότι υπάρχει ένα σύνολο παικτών $V' \subseteq V$ οι οποίοι αποφασίζουν σε τιμές διαφορετικές του $x_D$. Έστω $v$ ο παίκτης του $V'$ που αποφασίζει στον μικρότερο γύρο μεταξύ όλων των παικτών του $V'$, δηλαδή, ο πρώτος παίκτης που θα αποφασίσει σε μια λάθος τιμή, έστω την $x \neq x_D$. Ο $v$ δεν μπορεί να είναι γείτονας του διανομέα γιατί όλοι οι γείτονες του διανομέα αποφασίζουν στην τιμή $x_D$ όπως φαίνεται στον αντίστοιχο κανόνα απόφασης του CPA. Επομένως ο $v$ έλαβε $t+1$ μηνύματα με την τιμή $x$ από $t+1$ διαφορετικούς γείτονές του. Αφού το πολύ $t(v)$ γείτονές του μπορεί να είναι διεφθαρμένοι, τουλάχιστον ένας τίμιος παίκτης αποφάσισε στην τιμή $x \neq x_D$ πριν τον $v$. Άτοπο, αφού υποθέσαμε ότι ο $v$ είναι ο πρώτος παίκτης

που αποφάσισε σε λανθασμένη τιμή. □

Στην συνέχεια, ορίζουμε την ποσότητα, ο υπολογισμός της οποίας είναι ο κεντρικός στόχος αυτού του κεφαλαίου, συγκεκριμένα, το μέγιστο αριθμό τοπικών διαφθορών που μπορεί να γίνει ανεκτός από τον CPA.

***Ορισμός* 2.6** (Μέγιστη ανοχή του CPA). *Για ένα γράφημα $G$ και διανομέα $D$, $t^{\text{CPA}}_{\max}(G, D)$ το μέγιστο $t$ τέτοιο ώστε ο CPA είναι $t$-τοπικά ανεκτικός.*

Όποτε τα $G$ και $D$ εννοούνται από τα συμφραζόμενα, θα γράφουμε απλά $t^{\text{CPA}}_{\max}$ αντί για $t^{\text{CPA}}_{\max}(G, D)$.

**Φράγματα και συνθήκες.**

Ας κάνουμε τώρα μια απλή αλλά χρήσιμη παρατήρηση: Έστω μια γραφοθεωρητική παράμετρος $X$, δείχνοντας ότι η συνθήκη $t < X$ είναι μια ικανή τοπολογική συνθήκη για να είναι ο CPA $t$-τοπικά ανεκτικός, παρέχει άμεσα ένα κάτω φράγμα $\lceil X \rceil - 1$ για το $t^{\text{CPA}}_{\max}$. Αντίστοιχα, αναγκαίες συνθήκες παρόμοιας μορφής συνεπάγονται άνω φράγματα για το $t^{\text{CPA}}_{\max}$. Θα χρησιμοποιηθεί συχνά αυτή η σχέση φραγμάτων και συνθηκών σε ολόκληρο το κεφάλαιο.

## 2.5 Κάτω φράγματα στην ανοχή του CPA

Οι Pelc και Peleg [PP05] ήταν οι πρώτοι που παρουσίασαν μια γραφοθεωρητική παράμετρο $\mathcal{X}(G, D)$, η οποία σχετίζει τον μέγιστο ανεκτό αριθμό από τοπικές διαφθορές με την τοπολογία του γραφήματος. Αυτή η παράμετρος αντιπροσωπεύει τον μέγιστο αριθμό $b$ έτσι ώστε κάθε κόμβος $v$ να έχει τουλάχιστον $b$ γείτονες με απόσταση από τον $D$ μικρότερη από εκείνη του . Δίνουν μια ικανή συνθήκη σχετική με την ανοχή του CPA, συγκεκριμένα $\mathcal{X}(G, D) \geq 2t + 1$. Η συνθήκη αυτή υπονοεί ότι οι κόμβοι του γραφήματος $G$ μπορούν να διαταχθούν σε επίπεδα ως προς την απόστασή τους από τον διανομέα· με το πρώτο επίπεδο να είναι οι γειτονιά του διανομέα, και κάθε κόμβο στο επίπεδο $k$ να έχει τουλάχιστον $2t + 1$ γείτονες στο επίπεδο $k - 1$.

Αυτό με τη σειρά του συνεπάγεται ότι κάθε κόμβος σε απόσταση $k$ από τον $D$ (επίπεδο $k$) αποφασίζει στον $k$-οστό γύρο, επειδή σίγουρα θα λάβει τουλάχιστον $t + 1$ ορθές τιμές από τίμιους παίκτες του επιπέδου $k - 1$. Ωστόσο, όπως αποδεικνύεται στην ίδια δουλειά αυτή η συνθήκη δεν είναι αναγκαία, επειδή ένας κόμβος στο επίπεδο $k$ μπορεί επίσης να συλλέξει ορθές τιμές από γείτονές του στο επίπεδο $k$ ή $k+1$, και έτσι να συμπληρώσει τον απαραίτητο αριθμό των $t+1$ αντιγράφων τις ίδιας τιμής. Με άλλα λόγια, η τιμή $\lceil \mathcal{X}/2 \rceil - 1$ είναι ένα κάτω φράγμα για την μέγιστη ανοχή του CPA αλλά όχι ακριβές (το μέγιστο κάτω φράγμα).

### 2.5.1 Νέα παράμετρος-φράγμα για τη Μέγιστη Ανοχή του CPA

Σκοπεύοντας να εξάγουμε ακριβέστερα φράγματα για το $t_{\max}^{\text{CPA}}$ εισάγουμε την έννοια της *ελάχιστης $k$-διάταξης επιπέδων* ενός γραφήματος, η οποία οριζόταν έμμεσα στο [PP05]. Διαισθητικά μια ελάχιστη $k$-διάταξη επιπέδων είναι μια διαμέριση των κόμβων σε αριθμημένα επίπεδα-σύνολα, τέτοια ώστε κάθε κόμβος έχει τουλάχιστον $k$ γείτονες σε προηγούμενα επίπεδα και ανήκει στο ελάχιστο επίπεδο για το οποίο ικανοποιείται αυτή η ιδιότητα. Τυπικά έχουμε:

***Ορισμός* 2.7**. *Μία* Ελάχιστη $k$-Διάταξη Επιπέδων $\mathcal{L}_k(G, D)$ *ενός γραφήματος* $G = (V, E)$ *με διανομέα* $D$ *είναι μια διαμέριση* $V \setminus \{D\} = \bigcup_{i=1}^{m} L_i,\ m \in \mathbb{N}$ *τ.ώ.,*

$$\begin{aligned} L_1 =& \mathcal{N}(D), \\ L_2 =& \{v \in V \setminus\ L_1 : |\mathcal{N}(v) \cap L_1| \geq k\} \\ &\vdots \\ L_m =& \{v \in V \setminus \bigcup_{j=1}^{m-1} L_j : |\mathcal{N}(v) \cap \bigcup_{j=1}^{m-1} L_j| \geq k\} \end{aligned}$$

Στη συνέχεια ορίζουμε την έννοια της *ασθενούς $k$-διάταξης επιπέδων* η οποία είναι χρήσιμη για την απλότητα των αποδείξεων, καταργώντας την απαίτηση να ανήκουν οι κόμβοι στο ελάχιστο επίπεδο που δίνει τις επιθυμητές ιδιότητες.

***Ορισμός* 2.8**. *Μία* Ασθενής $k$-Διάταξη Επιπέδων *ενός γραφήματος* $G = (V, E)$ *με διανομέα* $D$ *είναι μια διαμέριση* $V \setminus \{D\} = \bigcup_{i=1}^{m} L_i,\ m \in \mathbb{N}$ *τ.ώ.,*

$$L_1 = \mathcal{N}(D), \qquad \forall v \in L_i : |\mathcal{N}(v) \cap \bigcup_{j=1}^{i-1} L_j| \geq k$$

#### Ιδιότητες των $k$-διατάξεων επιπέδων.

Σημειώνεται ότι ενώ μπορεί να υπάρχουν πολλές διαφορετικές ασθενείς $k$-διατάξεις επιπέδων ενός γραφήματος, η ελάχιστη $k$-διάταξη επιπέδων είναι μοναδική, όπως μπορεί να δειχθεί εύκολα με επαγωγή. Παρατηρούμε επίσης ότι μία ασθενής $k$-διάταξη επιπέδων μπορεί εύκολα να μετατραπεί στην ελάχιστη· για να δείξουμε αυτό χρησιμοποιούμε την έννοια του *αργοπορημένου κόμβου*:

Έστω μία ασθενής $k$-διάταξη επιπέδων $\mathcal{L}$: $V = \bigcup_{i=1}^{m} L_i,\ m \in \mathbb{N}$, θα ονομάζουμε έναν κόμβο $u \in L_h \in \mathcal{L}$ *αργοπορημένο κόμβο* της $\mathcal{L}$ αν $\exists\, d$ with $1 < d < h \leq m$ τ.ώ. $|\mathcal{N}(u) \cap \bigcup_{j=1}^{d-1} L_j| \geq k$. Το παρακάτω πόρισμα συνεπάγεται άμεσα από τους προηγούμενους ορισμούς.

***Πόρισμα* 2.2**. *Μια ασθενής $k$-διάταξη επιπέδων χωρίς αργοπορημένους κόμβους είναι ελάχιστη $k$-διάταξη επιπέδων.*

Λόγω του παραπάνω πορίσματος, για οποιαδήποτε ασθενή $k$-διάταξη επιπέδων $\mathcal{L}$ μπορούμε να κατασκευάσουμε μια ελάχιστη $k$-διάταξη επιπέδων $\mathcal{L}_k$ μετακινώντας επαναλαμβανόμενα κάθε αργοπορημένο κόμβο στο χαμηλότερο επίπεδο έτσι ώστε η διαμέριση να παραμένει ασθενής $k$-διάταξη επιπέδων. Επομένως ισχύει το παρακάτω.

***Πρόταση* 2.3**. *Έστω ένα γράφημα $G$ με διανομέα $D$, για κάθε $k \in \mathbb{N}$, αν υπάρχει ασθενής $k$-διάταξη επιπέδων για τα $G, D$ τότε υπάρχει μοναδική ελάχιστη $k$-διάταξη επιπέδων για τα $G, D$.*

*Απόδειξη.*

Αποδεικνύουμε ότι αν αλλάξουμε την διαμέριση με συγκεκριμένο τρόπο τότε αυτή παραμένει ασθενής $k$-διάταξη επιπέδων και τελικά κατασκευάζεται μία ελάχιστη $k$-διάταξη επιπέδων $\mathcal{L}_k(G, D)$. Θα χρησιμοποιήσουμε τον ακόλουθο ισχυρισμό,

Αρχικά παρατηρούμε ότι αν υπάρχει μαι ασθενής $k$-διάταξη επιπέδων $\mathcal{L}$: $V = \bigcup_{i=1}^{m} L_i$, $m \in \mathbb{N}$ με $1 < d < h \leq m$, τότε για τυχαίο $u \in L_h$ (αργοπορημένο κόμβο) με $|\mathcal{N}(u) \cap \bigcup_{j=1}^{d-1} L_j| \geq k$, η διαμέριση $\mathcal{L}'$ :

$$V = L_1 \cup L_2 \cup \ldots \cup \{L_d \cup \{u\}\} \cup \cdots \cup \{L_h \setminus \{u\}\} \cup \cdots \cup L_m = \bigcup_{i=1}^{m} L'_i$$

είναι επίσης μία ασθενής $k$-διάταξη επιπέδων.

Στηριζόμενοι στην προηγούμενη παρατήρηση, δοθείσας μιας οποιασδήποτε ασθενούς $k$-διάταξης επιπέδων $\mathcal{L}$ μπορούμε να κατασκευάσουμε μία ελάχιστη $k$-διάταξη επιπέδων $\mathcal{L}_k$, μετακινώντας όλους τους αργοπορημένους κόμβους στο ελάχιστο επίπεδο για το οποίο η διαμέριση παραμένει ασθενής $k$-διάταξη επιπέδων. Συγκεκριμένα,

Δοθείσας μίας ασθενούς $k$-διάταξης επιπέδων $\mathcal{L} : V = \bigcup_{i=1}^{m} L_i$, για κάθε κόμβο $v$, μετακινούμε τον $v$ στο σύνολο $L_i$ τ.ώ.

$$i = \min \left\{ d \in \{1, \ldots, m\} \;\middle|\; |\mathcal{N}(v) \cap \bigcup_{j=1}^{d-1} L_j| \geq k \right\}$$

Επιπλέον, όποτε μετακινούμε έναν αργοπορημένο κόμβο πρέπει να ελέγξουμε όλους τους υπόλοιπους κόμβους που μπορεί να μετατράπηκαν σε αργοπορημένους λόγω αυτής της κίνησης. Η διαδικασία αυτή τερματίζει σε πολυωνυμικό αριθμό βημάτων και η τελική διαμέριση δεν περιέχει αργοπορημένους κόμβους. Επομένως η διαμέριση που προκύπτει είναι μία ελάχιστη $k$-διάταξη επιπέδων σύμφωνα με το πόρισμα.

Ως προς την μοναδικότητα της ελάχιστης $k$-διάταξης επιπέδων $\mathcal{L}_k$, υποθέτουμε ότι για το γράφημα $G$ με διανομέα $D$ υπάρχουν δύο διαφορετικές ελάχιστες $k$-διατάξεις επιπέδων $\mathcal{L} = \{L_1, \cdots, L_m\}, \mathcal{L}' = \{L'_1, \cdots, L'_h\}$. Από τον ορισμό ισχύει ότι $L_1 = L'_1$. Έστω ότι $i$ είναι ο ελάχιστος ακέραιος ώστε $L_i \neq L'_i$ και υποθέτουμε χωρίς βλάβη της γενικότητας ότι $\exists v$, τ.ώ. $v \in L_i$ και $v \notin L'_i$. Τότε είναι προφανές ότι ο $v$ είναι ένας αργοπορημένος κόμβος της $L'_i$, και έτσι η $L'_i$ δεν είναι ελάχιστη $k$-διάταξη επιπέδων, το οποίο είναι άτοπο.

□

***Ορισμός* 2.9** (Παράμετρος $\mathcal{K}$). *Για γράφημα $G$ με διανομέα $D$,*

$$\mathcal{K}(G,D) \stackrel{def.}{=} \max\{k \in \mathbb{N} \mid \exists \text{ ελάχιστη } k\text{-διάταξη επιπέδων } \mathcal{L}_k(G,D)\}$$

***Θεώρημα* 2.4** (Ικανή συνθήκη). *Για κάθε γράφημα $G$ με διανομέα $D$ και $t \in \mathbb{N}$, αν $t < \mathcal{K}(G,D)/2$ τότε ο CPA είναι $t$-τοπικά ανεκτικός.*

*Απόδειξη.*
Παρατηρούμε ότι από το $2t < \mathcal{K}(G,D)$ συνεπάγεται η ύπαρξη μιας ελάχιστης $(2t+1)$-διάταξης επιπέδων $\mathcal{L}_{2t+1}(G,D)$. Έστω $\mathcal{L}_{2t+1}(G,D)$ η διαμέριση $\{L_1,\ldots,L_m\}$ του $V$, δηλαδή, $V = \bigcup_{i=1}^{m} L_i$. Αρκεί να δείξουμε ότι για $1 \leq i \leq m$, κάθε τίμιος παίκτης $v \in L_i$ αποφασίζει στην τιμή του διανομέα $x_D$. Με ισχυρή επαγωγή στο $i$ έχουμε :

Κάθε τίμιος παίκτης $v \in L_1 = \mathcal{N}(D)$ αποφασίζει τετριμμένα στην τιμή του διανομέα $x_D$ μόλις λάβει αυτή την τιμή. Αν όλοι οι τίμιοι παίκτες $u \in L_i, 1 \leq i \leq h$, αποφασίζουν στην $x_D$ σε κάποιο γύρο, τότε κάθε τίμιος παίκτης $v \in L_{h+1}$ λαμβάνει $|\bigcup_{j=1}^{h} L_j \cap \mathcal{N}(v)| \geq 2t+1$ μηνύματα από τους γείτονες του που έχουν ήδη αποφασίσει και ανήκουν σε προηγούμενα επίπεδα. Τουλάχιστον $t+1$ από αυτούς είναι τίμιοι. Επομένως ο $v$ αποφασίζει στην τιμή $x_D$.

□

***Πόρισμα* 2.5** (Κάτω φράγμα). *Για κάθε γράφημα $G$ με διανομέα $D$ ισχύει $t_{\max}^{\text{CPA}} \geq \lceil \mathcal{K}(G,D)/2 \rceil - 1$.*

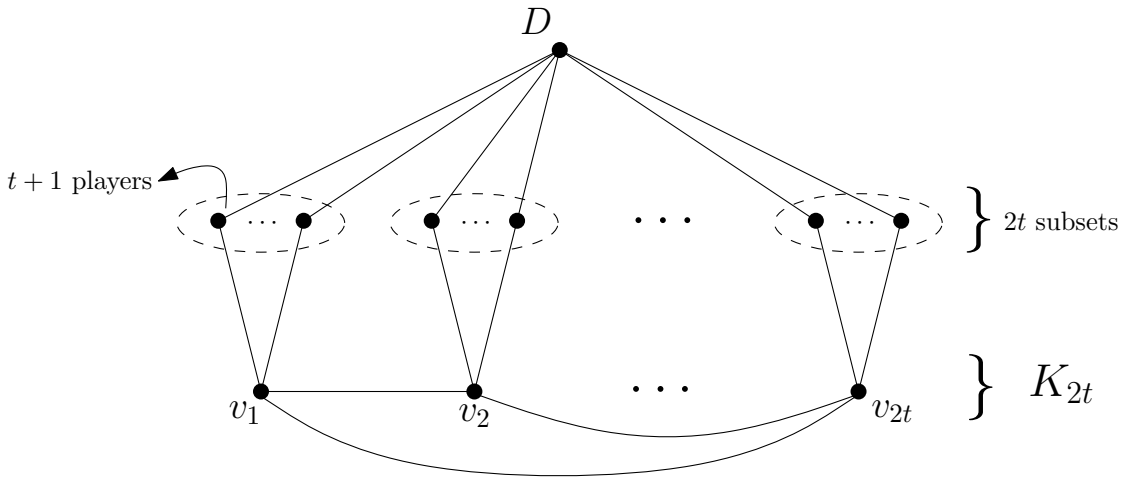
### 2.5.2 Ακρίβεια του κάτω φράγματος

Στο Θεώρημα 2.4 δείξαμε ότι η συνθήκη $t < \mathcal{K}(G,D)/2$ είναι ικανή για να είναι ο CPA $t$-τοπικά ανεκτικός· στη συνέχεια αποδεικνύουμε ότι η συνθήκη αυτή δεν είναι και αναγκαία. Διαισθητικά, ο λόγος είναι ότι η τοπολογία του γραφήματος μπορεί να είναι τέτοια ώστε να εμποδίζεται ο αντίπαλος να διαφθείρει ακριβώς $t$ παίκτες σε *κάθε* γειτονιά του γραφήματος και επομένως μερικοί παίκτες θα αποφασίσουν σωστά εκτελώντας τον CPA ακόμα και αν έχουν μόνο $t+1$ γείτονες σε προηγούμενα επίπεδα.

***Πρόταση* 2.6**. *Υπάρχει μια οικογένεια στιγμιοτύπων $(G,D)$, τέτοια ώστε ο CPA είναι $(\mathcal{K}(G,D)-1)$-τοπικά ανεκτικός για το $(G,D)$.*

*Απόδειξη.*

Στο Σχήμα 2.1 βλέπουμε μια τέτοια οικογένεια στιγμιοτύπων για κάθε τιμή του $t$. Σε αυτό το στιγμιότυπο, η γειτονιά του $D$ αποτελείται από $2t^2+2t$ κόμβους, οι κόμβοι $v_1,\ldots,v_{2t}$ αποτελούν μια κλίκα μεγέθους $2t$ και είναι συνδεδεμένοι με κόμβους στο σύνολο $\mathcal{N}(D)$ όπως




Σχήμα 2.1: Γράφημα με $\mathcal{K}(G, D) = t+1$, για το οποίο ο CPA είναι $t$-τοπικά ανεκτικός.

φαίνεται στο σχήμα. Εύκολα ελέγχουμε ότι $t = \mathcal{K}(G, D) - 1$. Αν τρέξουμε τον CPA στο $G$ τότε κάθε παίκτης $v_i \in \{v_1, \ldots, v_{2t}\}$ λαμβάνει $M$ ορθά μηνύματα, με

$$M = M_A + M_B \tag{1}$$

όπου, $M_A$ : ο αριθμός των μηνυμάτων που έλαβε από το σύνολο $\mathcal{N}(D)$ και
$M_B$ : ο αριθμός των μηνυμάτων που έλαβε από το σύνολο $B = \{v_1, \ldots, v_{2t}\} \setminus \{v_i\}$.

Έστω $T_i = T \cap \mathcal{N}(D) \cap \mathcal{N}(v_i)$ το σύνολο των προδοτών οι οποίοι είναι κοινοί γείτονες των $D$ and $v_i$. Τότε,

$$M_A = |\mathcal{N}(D) \cap \mathcal{N}(v_i) \setminus T_i| = t + 1 - |T_i| \tag{2}$$

Για να υπολογίσουμε τον αριθμό των ορθών μηνυμάτων που λαμβάνει ο $v_i$ από άλλους παίκτες στο $B$, ορίζουμε τα σύνολα:

$$C_{B_1} = \{v \in B \mid v \text{ έλαβε το πολύ } t \text{ μηνύματα από το } \mathcal{N}(D)\ \}$$
$$C_{B_2} = \{v \in B \mid v \text{ είναι διεφθαρμένος}\ \}$$
$$C_B = C_{B_1} \cup C_{B_2}$$

Παρατηρούμε ότι το $C_{B_1}$ γίνεται μέγιστης πληθικότητας αν ο αντίπαλος διαφθείρει ακριβώς ένα παίκτη σε κάθε σύνολο $\mathcal{N}(v_j) \cap \mathcal{N}(D), \forall v_j \in B$. Επομένως,

$$\max_{T:t\text{-τοπικό}} |C_{B_1}| = \max_{T:t\text{-τοπικό}} |T \cap (\mathcal{N}(D) \setminus \mathcal{N}(v_i))| = t - |T_i|$$

Επίσης $|C_{B_2}| \leq t - |T_i|$ επειδή τα $B$ και $\mathcal{N}(v_i) \cap \mathcal{N}(D)$ σχηματίζουν τη γειτονιά του $v_i$ όπου οι διαφθορές μπορεί να είναι το πολύ $t$. Στη συνέχεια υπολογίζουμε ένα άνω φράγμα για το $C_B$.

$$|C_B| = |C_{B_1} \cup C_{B_2}| \leq |C_{B_1}| + |C_{B_2}| \leq (t - |T_i|) + (t - |T_i|) = 2t - 2|T_i|$$

άρα,

$$M_B = 2t - 1 - |C_B| = 2t - 1 - 2t + 2|T_i| = 2|T_i| - 1 \quad (3)$$

Τελικά υπολογίζουμε τον συνολικό αριθμό μηνυμάτων $M$,

$$(1), (2), (3) \Rightarrow M = M_A + M_B \geq t + 1 - |T_i| + 2|T_i| - 1 = \\ = t + |T_i|$$

Για οποιοδήποτε $v_i$, αν $|T_i| > 0$ τότε $M \geq t + 1$. Αλλιώς θα ισχύει $|T_i| = 0$ και ο $v_i$ θα λάβει $t + 1$ ορθά μηνύματα από το $\mathcal{N}(D)$. Επομένως ο CPA πετυχαίνει Εκπομπή στο στιγμιότυπο $(G, D)$.

□

## 2.6 Άνω φράγμα για την ανοχή του CPA

Στην προηγούμενη ενότητα δείξαμε ότι $t_{\max}^{\text{CPA}} \geq \lceil \mathcal{K}(G, D)/2 \rceil - 1$, επίσης παρουσιάσαμε περιπτώσεις όπου $\mathcal{K}(G, D) - 1$ προδότες μπορούν να γίνουν ανεκτοί από τον CPA. Σε αυτήν την ενότητα θα δείξουμε ότι ο αριθμός αυτός είναι και ο μέγιστος που μπορεί να γίνει ανεκτός, δηλαδή, δείχνουμε ότι η τιμή $\mathcal{K}(G, D) - 1$ είναι ένα άνω φράγμα στον τοπικό αριθμό προδοτών για κάθε $G$ και $D$. Το πετυχαίνουμε το προηγούμενο αποδεικνύοντας μία αναγκαία συνθήκη για να είναι ο CPA $t$-τοπικά ανεκτικός.

***Θεώρημα* 2.7** (Αναγκαία συνθήκη). *Για κάθε γράφημα $G$ με διανομέα $D$ και $t \geq \mathcal{K}(G, D)$, ο CPA δεν είναι $t$-τοπικά ανεκτικός.*

*Απόδειξη.*
Υποθέτουμε ότι ο CPA είναι $t$-τοπικά ανεκτικός, με $t \geq \mathcal{K}(G, D)$. Αφού ο CPA είναι $t$-τοπικά ανεκτικός πρέπει να υπάρχει θετικός ακέραιος $s$, τέτοιος ώστε ο αλγόριθμος τερματίζει μετά από $s$ βήματα στο στιγμιότυπο $(G, D)$. Περιγράφουμε την λειτουργία του CPA στο γράφημα $G$ με σύνολα κόμβων που αποφασίζουν. Έστω $L_i$ το σύνολο των κόμβων που αποφασίζουν στον $i$-στό γύρο. Αφού κάθε κόμβος $v \in L_i$ αποφασίζει στον $i$-στό γύρο ισχύει ότι ο $v$ έχει τουλάχιστον $t + 1$ γείτονες στα σύνολα $L_1, \ldots, L_{i-1}$. Δηλαδή,

$$\forall v \in L_i \Rightarrow |\mathcal{N}(v) \cap \bigcup_{j=1}^{i-1} L_j| \geq t + 1.$$

Παρατηρούμε ότι η παραπάνω ακολουθία συνόλων είναι μία ασθενής $(t + 1)$-διάταξη επιπέδων για τα $G$, $D$. Από αυτήν την παρατήρηση και την Πρόταση 2.3 έχουμε ότι πρέπει να υπάρχει μια ελάχιστη $(t + 1)$-διάταξη επιπέδων για τα $G$, $D$. Αυτό όμως μας οδηγεί σε αντίφαση αφού υποθέσαμε ότι $t \geq \mathcal{K}(G, D)$.

□

***Πόρισμα* 2.8** (Άνω φράγμα για το $t^{\text{CPA}}_{\max}$). *Για κάθε γράφημα $G$ με διανομέα $D$ ισχύει ότι* $t^{\text{CPA}}_{\max} < \mathcal{K}(G, D)$

### 2.6.1 Σύγκριση με την παράμετρο των Ichimura-Shigeno

Στην εργασία [IS10], οι Ichimura και Shigeno εισάγουν την γραφοθεωρητική παράμετρο $\widetilde{\mathcal{X}}(G, D)$ η οποία μπορεί να χρησιμοποιηθεί για την εξαγωγή μιας ικανής συνθήκης για την ανοχή του CPA. Για ένα γράφημα $G = (V, E)$ με διανομέα $D$, θεωρούν μια ολική διάταξη των κόμβων $\sigma = (v_1, v_2, \ldots)$ του συνόλου $V \setminus (\mathcal{N}(D) \cup D)$, και χρησιμοποιούν τη συνάρτηση $\delta(W_i, v)$ για τον αριθμό των γειτόνων του κόμβου $v$ στο σύνολο $\mathcal{N}(D) \cup \{v_1, \ldots, v_{i-1}\}$. Η ολική διάταξη $\sigma$ έχει την ιδιότητα $\forall i, j,$ τ.ώ. $1 \leq i < j \leq |V \setminus (\mathcal{N}(D) \cup D)|$ ισχύει ότι $\delta(W_{i-1}, v_i) \geq \delta(W_{i-1}, v_j)$. Αυτή η διάταξη αναφέρεται επίσης στη βιβλιογραφία [NI08] σαν *max-back* διάταξη. Έπειτα ορίζουν την παράμετρο $\widetilde{\mathcal{X}}(G, D) = \min\{\delta(W_{i-1}, v_i) \mid i = 1, 2, \ldots\}$. και αποδεικνύουν ότι είναι μοναδική , δηλαδή, είναι η ίδια για όλες τις max-back διατάξεις. Ουσιαστικά, με όρους που παρουσιάζονται στην παρούσα εργασία, αποδεικνύουν ότι, [1]

$$\lceil \widetilde{\mathcal{X}}(G, D)/2 \rceil - 1 \leq t^{\text{CPA}}_{\max} < \widetilde{\mathcal{X}}(G, D). \tag{1}$$

Ως εκ τούτου, η παράμετρός τους δίνει παρόμοια φράγματα με τη δικιά μας. Στη συνέχεια δείχνουμε παρά τους διαφορετικούς ορισμούς των παραμέτρων $\mathcal{K}(G, D)$ και $\widetilde{\mathcal{X}}(G, D)$, αποδεικνύεται ότι αυτές είναι ίσες.

***Πρόταση* 2.9**. $\mathcal{K}(G, D) = \widetilde{\mathcal{X}}(G, D)$

*Απόδειξη.*
Θεωρούμε την max-back διάταξη $\sigma = (v_1, v_2, \ldots)$. Παρατηρούμε ότι η ακολουθία $\{L_1 = \mathcal{N}(D), L_2 = \{v_1\}, L_3 = \{v_2\}, \ldots\}$ είναι τετριμμένα μια ασθενής $\widetilde{\mathcal{X}}(G, D)$-διάταξη επιπέδων, γιατί η ελάχιστη συνδεσιμότητα μεταξύ ενός επιπέδου και των προηγούμενών του είναι $\widetilde{\mathcal{X}}(G, D)$. Άρα, λόγω της Πρότασης 2.3, υπάρχει μια ελάχιστη $\widetilde{\mathcal{X}}(G, D)$-διάταξη επιπέδων και επομένως $\mathcal{K}(G, D) \geq \widetilde{\mathcal{X}}(G, D)$. Έτσι, συνδυάζοντας την τελευταία ανισότητα με την ανισότητα $(1)$ δείχνουμε το ακόλουθο:

$$t^{\text{CPA}}_{\max} < \widetilde{\mathcal{X}}(G, D) \leq \mathcal{K}(G, D)$$

Αφού η Πρόταση 2.6 υπονοεί ότι υπάρχει ένα γράφημα γαι το οποίο ο CPA είναι $(\mathcal{K}(G, D)-1)$-τοπικά ανεκτικός η παραπάνω σχέση συνεπάγεται την ισότητα των παραμέτρων $\mathcal{K}(G, D)$ και $\widetilde{\mathcal{X}}(G, D)$. Αν αυτό δεν ίσχυε τότε το $\widetilde{\mathcal{X}}(G, D) < \mathcal{K}(G, D)$ θα σήμαινε ότι $t^{\text{CPA}}_{\max} < \mathcal{K}(G, D)-1$, το οποίο είναι άτοπο.

□

[1] Παρατηρούμε ότι η συνθήκη $t \leq \widetilde{\mathcal{X}}(G, D)$ παρουσιάζεται σαν αναγκαία στο [IS10]· ωστόσο η απόδειξή τους μπορεί εύκολα να μετατραπεί για να αποδειχθεί το πιο ακριβές φράγμα $t < \widetilde{\mathcal{X}}(G, D)$, όπως φαίνεται στο δεξί μέλος της $(1)$.

Παρόλο που οι δύο παράμετροι $\mathcal{K}(G, D)$ και $\widetilde{\mathcal{X}}(G, D)$ αποδεικνύονται ίσες, το γεγονός ότι η $\mathcal{K}(G, D)$ είναι ορισμένη με διαφορετικό τρόπο οδηγεί σε βελτιωμένη πολυπλοκότητα υπολογισμού της, όπως θα δούμε στην επόμενη ενότητα.

## 2.7 Προσέγγιση της μέγιστης ανοχής του CPA

Ας εξετάσουμε τώρα την προσεγγισιμότητα της *Μέγιστης ανοχής του CPA*· θα σχεδιάσουμε έναν αποδοτικό 2-προσεγγιστικό αλγόριθμο. Αρχικά δείχνουμε πως μπορούμε να ελέγξουμε την ύπαρξη μιας ελάχιστης $m$-διάταξης επιπέδων, για ένα γράφημα $G$ με διανομέα $D$, χρησιμοποιώντας μια παραλλαγή του κλασικού αλγόριθμου BFS. Στη συνέχεια, πετυχαίνουμε την προσέγγιση υπολογίζοντας την παράμετρο $\mathcal{K}(G, D)$, μέσω επαναλήψεων του παραπάνω ελέγχου. Ο λόγος προσέγγισης αποδεικνύεται, συνδυάζοντας τα Πορίσματα 2.5 και 2.8.

**Έλεγχος ύπαρξης ελάχιστης $m$-διάταξης επιπέδων για τα $(G, D)$**

Για είσοδο $(G, D, m)$ κάνουμε τα ακόλουθα:

1. Αναθέτουμε ένα μετρητή σε κάθε κόμβο αρχικοποιημένο στο 0.
2. Εισάγουμε σε μία ουρά τον κόμβο-διανομέα και όλους τους γείτονές του.
3. Εξάγουμε έναν κόμβο από την ουρά και αυξάνουμε κατά 1 τους μετρητές όλων των γειτόνων του. Εισάγουμε έναν τέτοιο γείτονα στην ουρά μόνον αν ο μετρητής του είναι τουλάχιστον $m$.
4. Επαναλαμβάνουμε το βήμα 3 μέχρι να αδειάσει η ουρά.
5. Αν όλοι οι κόμβοι έχουν εισαχθεί στην ουρά τότε δίνουμε έξοδο '*Αληθές*' (υπάρχει μία ελάχιστη $m$-διάταξη επιπέδων), αλλιώς δίνουμε έξοδο '*Ψευδές*'.

Παρατηρούμε ότι ο παραπάνω αλγόριθμος μπορεί να τροποποιηθεί για να υπολογίζει την ελάχιστη $m$-διάταξη επιπέδων $\mathcal{L}_m(G, D)$.

**2-Προσέγγιση της παραμέτρου $t_{\max}^{\text{CPA}}$**

1. Υπολόγισε την παράμετρο $\mathcal{K}(G, D)$: Αφού $\mathcal{K}(G, D) < \min_{v \in V \setminus (\mathcal{N}(D) \cup D)} \deg(v) = \delta$, η ακριβής τιμή της παραμέτρου $\mathcal{K}(G, D)$ υπολογίζεται με $\log \delta$ επαναλήψεις του ελέγχου ύπαρξης, χρησιμοποιώντας δυαδική αναζήτηση.
2. Επέστρεψε $\lceil \mathcal{K}(G, D)/2 \rceil - 1$

Το $t \geq \mathcal{K}(G, D)$ σημαίνει ότι ο CPA δεν είναι $t$-τοπικά ανεκτικός, επομένως ισχύει ότι $t_{\max}^{\text{CPA}} < \mathcal{K}(G, D)$, συνεπώς, η επιστρεφόμενη τιμή είναι τουλάχιστον $\lceil t_{\max}^{\text{CPA}}/2 \rceil - 1$.

Ένα *ακριβές παράδειγμα* (tight example) για το λόγο προσέγγισης αυτού του αλγορίθμου στην πραγματικότητα δίνεται από την οικογένεια στιγμιοτύπων που παρουσιάστηκε νωρίτερα στο Σχήμα 2.1 στο οποίο παρουσιάσαμε ένα γράφημα $G$ για το οποίο $\mathcal{K}(G, D) = t + 1$ και ο CPA είναι $t$-τοπικά ανεκτικός.

Η πολυπλοκότητα του παραπάνω προσεγγιστικού αλγορίθμου δίνεται προφανώς από την πολυπλοκότητα υπολογισμού του $\mathcal{K}(G, D)$. Όπως εξηγήσαμε παραπάνω, ο αλγόριθμος χρειάζεται το πολύ $\log \delta$ εκτελέσεις του ελέγχου ύπαρξης ελάχιστης διάταξης επιπέδων. Το τελευταίο απαιτεί πολυπλοκότητα χρόνου $O(|E|)$ (ίδια πολυπλοκότητα με τον αλγόριθμο BFS). Συνολικά, έχουμε ότι η πολυπλοκότητα χρόνου του αλγορίθμου είναι της τάξης $O(|E| \log \delta)$, η οποία είναι σημαντικά βελτιωμένη σε σχέση με την πολυπλοκότητα υπολογισμού της ισοδύναμης παραμέτρου $\widetilde{\mathcal{X}}(G, D)$, η οποία είναι $O(|V|(|V| + |E|))$ όπως αναφέρεται στο [IS10] .

## 2.8 Ακριβής προσδιορισμός του $t_{\max}^{\text{CPA}}$

Σε αυτήν την ενότητα παρουσιάζουμε μια διαδικασία για τον ακριβή υπολογισμό του $t_{\max}^{\text{CPA}}$. Για τον σκοπό αυτό εισάγουμε δύο νέες γραφοθεωρητικές παραμέτρους. Για ένα πιθανό σύνολο διεφθαρμένων παικτών ($t$-τοπικό) $T$ και γράφημα $G = (V, E)$ θα συμβολίζουμε με $G_{\bar{T}} = (V \setminus T, E')$ το επαγόμενο υπογράφημα (node induced) του $G$ στο σύνολο κόμβων $V \setminus T$.

***Ορισμός* 2.10**. *Για γράφημα $G$ με διανομέα $D$ και θετικό ακέραιο $t$, το $t$-όριο ασφαλείας είναι η ποσότητα* $\mathcal{M}(G, D, t) = \min_{T:\ t\text{-τοπικό}} \mathcal{K}(G_{\bar{T}}, D)$.

***Θεώρημα* 2.10** (Αναγκαία και ικανή συνθήκη). *Για γράφημα $G = (V, E)$ και διανομέα $D$, ο CPA είναι $t$-τοπικά ανεκτικός αν και μόνον αν $\mathcal{M}(G, D, t) \geq t + 1$.*

*Απόδειξη.*

($\Leftarrow$) Έστω $\mathcal{M}(G, D, t) \geq t+1$ και $T \subseteq V \setminus D$ ένα οποιοδήποτε $t$-τοπικό σύνολο διεφθαρμένων κόμβων. Από τον ορισμό ισχύει $\mathcal{K}(G_{\bar{T}}, D) \geq t + 1$. Επομένως υπάρχει μία ελάχιστη $(t + 1)$-διάταξη επιπέδων $\mathcal{L}_{t+1}(G_{\bar{T}}, D) = \{L_1, \ldots, L_m\}$. Άρα οποιοσδήποτε τίμιος παίκτης $v$ έχει τουλάχιστον $t + 1$ τίμιους γείτονες σε επίπεδα προηγούμενα του $\mathcal{L}_{t+1}(G_{\bar{T}}, D)\cdot$ με μια απλή επαγωγή δείχνουμε ότι ο $v$ θα αποφασίσει στην τιμή του διανομέα $x_D$.

($\Rightarrow$) Εάν ο CPA είναι $t$-τοπικά ανεκτικός τότε για οποιοδήποτε $t$-τοπικό σύνολο διεφθαρμένων $T$ ισχύει ότι κάθε τίμιος παίκτης στο υπογράφημα $G_{\bar{T}}$ αποφασίζει στο $x_D$. Έστω ότι ο συνολικός αριθμός γύρων μέχρι τον τερματισμό του πρωτοκόλλου είναι $m \in \mathbb{N}$. Ορίζουμε την ακολουθία συνόλων $L_i = \{v \in V \setminus T \mid v \text{ αποφασίζει στον γύρο } i \text{ του CPA }\}$, $i \in \{1, \ldots, m\}$. Δείχνουμε με επαγωγή ότι η ακολουθία $(L_i)_{i=1}^m$ είναι η (μοναδική) ελάχιστη $(t + 1)$-διάταξη επιπέδων του γραφήματος $G_{\bar{T}}$ με διανομέα $D$. Αρχικά σημειώνουμε ότι $L_1 = \mathcal{N}(D) \setminus T$ γιατί οι παίκτες που αποφασίζουν στον γύρο 1 είναι ακριβώς αυτοί που ανήκουν στη γειτονιά του διανομέα. Για τη βάση της επαγωγής, παρατηρούμε ότι

$L_2 = \{v \in V \setminus T \mid \mathcal{N}(v) \cap L_1 \geq t+1\}$ καθώς οι παικτες που αποφασίζουν στον γύρο 2 είναι ακριβώς αυτοί που θα λάβουν $t+1$ όμοια μηνύματα από παίκτες που έχουν αποφασίσει στον γύρο 1. Υποθέτουμε ότι $L_k = \{v \in V \setminus \{T \cup \bigcup_{j=1}^{k-1} L_j\} : |\mathcal{N}(v) \cap \bigcup_{j=1}^{k-1} L_j| \geq t+1\}$ και παρατηρούμε ότι ισχύει το

$$L_{k+1} = \{v \in V \setminus \{T \cup \bigcup_{j=1}^{k} L_j\} : |\mathcal{N}(v) \cap \bigcup_{j=1}^{k} L_j| \geq t+1\}$$

λόγω του ότι οι παίκτες που αποφασίζουν στον γύρο $k+1$ είναι ακριβώς οι παίκτες που λαμβάνουν τουλάχιστον $t+1$ μηνύματα από παίκτες πυ έχουν αποφασίσει σε προηγούμενα επίπεδα. Αφού τα παραπάνω ισχύουν για κάθε $T$, ο ισχυρισμός αποδεικνύεται.

□

Για τον ακριβή προσδιορισμό της Μέγιστης Ανοχής του CPA $t_{\max}^{\text{CPA}}$ εισάγουμε την παράμετρο,

$$\mathcal{T}(G, D) = \max\{t \in \mathbb{N} \mid \mathcal{M}(G, D, t) \geq t+1\}$$

Από την παραπάνω συζήτηση θα πρέπει να είναι σαφές ότι $\mathcal{T}(G, D)$ ταυτίζεται με την Μέγιστη Ανοχή του CPA.

***Πόρισμα* 2.11.** $t_{\max}^{\text{CPA}}(G, D) = \mathcal{T}(G, D)$

Ένας απλός αλγόριθμος για να υπολογίσουμε το $t$-όριο ασφαλείας $\mathcal{M}(G, D, t)$ απαιτεί εκθετικό χρόνο καθώς πρέπει να λάβουμε υπόψιν όλα τα $t$-τοπικά σύνολα και να υπολογίσουμε το $\mathcal{K}(G_{\bar{T}}, D)$ όπως αυτό φαίνεται στην Ενότητα 2.7). Σημειώνεται ότι μια διαφορετική ικανή και αναγκαία συνθήκη για να είναι ο CPA $t$-τοπικά ανεκτικός δόθηκε ανεξάρτητα στο [TVB15]. Ωστόσο, μόνο ένας αλγόριθμος υπερεκθετικού χρόνου υπονοείται για τον έλεγχο αυτής της συνθήκης (δεν δίνεται αλγόριθμος στο [TVB15]).

Επιπλέον, για τον υπολογισμό του $t_{\max}^{\text{CPA}} = \mathcal{T}(G, D)$ αρκεί να εκτελεστούν το πολύ $\log \delta$ υπολογισμούς της παραμέτρου $\mathcal{M}(G, D, t)$ όπου, $\delta$ είναι ο ελάχιστος βαθμός μεταξύ όλων των κόμβων στο σύνολο $V \setminus (\mathcal{N}(D) \cup D)$.

## 2.9 Μοναδικότητα του CPA σε *Ad Hoc* δίκτυα

Βασιζόμενοι στην ικανή και αναγκαία συνθήκη για την $t$-τοπική ανεκτικότητα του CPA στο γράφημα $G$με διανομέα $D$ μπορούμε τώρα να αποδείξουμε την *Εικασία της Μοναδικότητας του CPA* για *ad hoc* δίκτυα, που είχε τεθεί σαν ανοιχτό πρόβλημα στο [PP05]. Η εικασία αναφέρει ότι δεν υπάρχει αλγόριθμος Εκπομπής που να μπορεί να ανεχθεί περισσότερες τοπικές διαφθορές από τον CPA σε δίκτυα άγνωστης τοπολογίας (*ad hoc*).

Λαμβάνουμε υπόψιν μόνο την κλάση των $t$-*τοπικά ασφαλών* αλγορίθμων Εκπομπής μέσω των οποίων κανένας παίκτης δεν αποφασίζει ποτέ σε λάθος τιμή υπό οποιοδήποτε $t$-τοπικό σύνολο διαφθοράς (βλέπε [PP05]).

Εργαζόμαστε στο μοντέλο *ad hoc* δικτύων, π.χ. [PP05]. Συγκεκριμένα υποθέτουμε ότι οι κόμβοι γνωρίζουν μόνο τις δικές τους ταυτότητες, τις ταυτότητες των γειτόνων τους και την ταυτότητα του διανομέα. Ένας κατανεμημένος αλγόριθμος Εκπομπής που λειτουργεί κάτω από αυτές τις παραδοχές ονομάζεται *ad hoc αλγόριθμος.*

***Θεώρημα* 2.12**. *Έστω $\mathcal{A}$ ένας ad hoc αλγόριθμος $t$-τοπικά ασφαλής. Αν ο $\mathcal{A}$ είναι $t$-τοπικά ανεκτικός για γράφημα $G$ με διανομέα $D$ τότε ο CPA είναι $t$-τοπικά ανεκτικός για τα $G, D$.*

*Απόδειξη.*
Από το Θεώρημα 2.10 έχουμε ότι, αν ο CPA δεν είναι $t$-τοπικά ανεκτικός στο $(G, D)$ τότε, $\mathcal{M}(G, D, t) = \min_{T:\ t\text{-τοπικό}} \mathcal{K}(G_{\bar{T}}, D) \leq t$ το οποίο συνεπάγεται ότι υπάρχει ένα $t$-τοπικό σύνολο $T$ τ.ώ. στο υπογράφημα $G_{\bar{T}}$ δεν υπάρχει ελάχιστη $(t+1)$-διάταξη επιπέδων. Από τον ορισμό της $(t+1)$-διάταξης επιπέδων έχουμε ότι δοθείσας μιας ακολουθίας υποσυνόλων του συνόλου κόμβων $V_{\bar{T}} = V \setminus (T \cup \{D\})$,

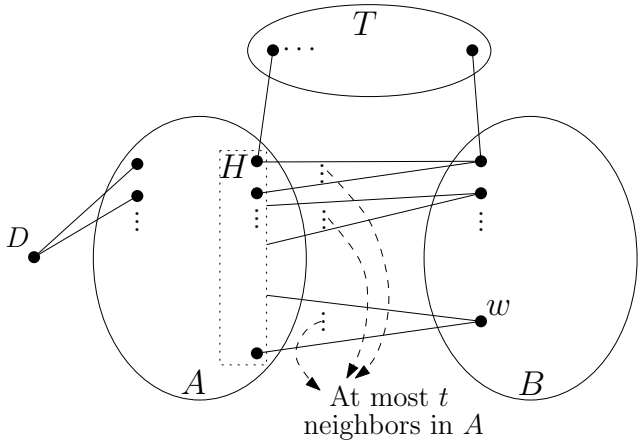
$$L_1 = \mathcal{N}_{G_{\bar{T}}}(D),\ \ L_i = \{v \in V_{\bar{T}} \setminus \bigcup_{j=1}^{i-1} L_j : |\mathcal{N}_{G_{\bar{T}}}(v) \cap \bigcup_{j=1}^{i-1} L_j| \geq t+1\}, 2 \leq i \leq m$$

υπάρχει $h \in \mathbb{N}$ s.t. $\forall j \geq h,\ L_j = \emptyset$ και $\bigcup_{i=1}^{h} L_i \subsetneq V_{\bar{T}}$. Συμβολίζουμε με $h_{\min}$ το ελάχιστο $h \in \mathbb{N}$ με την παραπάνω ιδιότητα. Χωρίς βλάβη της γενικότητας μπορούμε να υποθέσουμε ότι $h_{\min} \geq 2$, επειδή $h = 1$ συνεπάγεται ότι στο γράφημα $G_{\bar{T}}$ ο διανομέας $D$ δεν είναι συνδεδεμένος με το υπόλοιπο γράφημα το οποίο με τη σειρά του τετριμμένα συνεπάγεται ότι κανένας αλγόριθμος δεν μπορεί να πετύχει Εκπομπή υπό την διαφθορά του συνόλου $T$.

Έστω $A = \bigcup_{i=1}^{h_{\min}} L_i$ και $B = V_{\bar{T}} \setminus A$. Είναι προφανές από τον ορισμό της ελάχιστης $(t+1)$-διάταξης επιπέδων ότι $\forall w \in B,\ |\mathcal{N}_{G_{\bar{T}}}(w) \cap A| \leq t$. Επιπλέον, το $\bigcup_{i=1}^{h_{\min}} L_i \subsetneq V_{\bar{T}}$ σημαίνει ότι $B \neq \emptyset$. Τελικά χρησιμοποιούμε τον συμβολισμό $H = \bigcup_{w \in B} (\mathcal{N}_{G_{\bar{T}}}(w) \cap A)$ και παρατηρούμε ότι το $H$ συνιστά ένα διαχωριστή (τομή-κόμβων) στο γράφημα $G_{\bar{T}}$ που χωρίζει τον διανομέα $D$ από το υπογράφημα $B$. Η διαμέριση του γραφήματος $G$ στα τρία υπογραφήματα $A, B, T$ απεικονίζεται στο Σχήμα 3.1.

Έστω το γράφημα $G'$ το οποίο προκύπτει από το $G$ αν αφαιρέσουμε ακμές $(u, v)$ από το σύνολο $E' = \{(u, v) | u, v \in A \cup T\}$ τέτοιες ώστε το σύνολο $H$ γίνεται $t$-τοπικό στο $G'$ (π.χ. μπορούμε να αφαιρέσουμε όλες τις ακμές μεταξύ κόμβων του συνόλου $A \cup T$). Η ύπαρξη συνόλου ακμών που εγγυάται αυτήν την ιδιότητα προκύπτει από το γεγονός ότι $\forall w \in B,\ |\mathcal{N}_{G_{\bar{T}}}(w) \cap H| \leq t$.

Η συνέχεια της απόδειξης γίνεται με απαγωγή σε άτοπο. Υποθέτουμε ότι υπάρχει ένας $t$-τοπικά ασφαλής αλγόριθμος Εκπομπής . $\mathcal{A}$ ο οποίος είναι $t$-τοπικά ανεκτικός στο γράφημα $G$ με διανομέα $D$. Θεωρούμε τις ακόλουθες εκτελέσεις $\sigma$ και $\sigma'$ του αλγορίθμου $\mathcal{A}$,



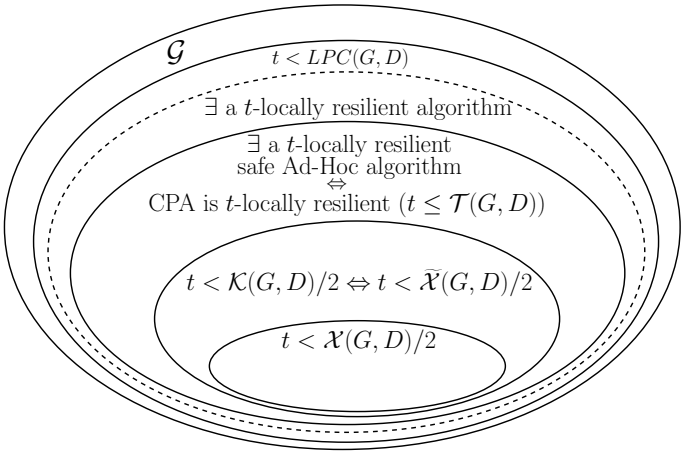

Σχήμα 2.2: Διαμέριση του $G$ στα υπογραφήματα $A, B, T$

- Η εκτέλεση $\sigma$ συμβαίνει στο γράφημα $G$ με διανομέα $D$, για την τιμή του διανομέα έχουμε ότι $x_D = 0$, το σύνολο διεφθαρμένων παικτών είναι το $T$ και σε κάθε γύρο, όλοι οι παίκτες αυτού του συνόλου στέλνουν τα ίδια μηνύματα που θα στέλνανε στον αντίστοιχο γύρο της εκτέλεσης $\sigma'$ όπου το σύνολο $T$ είναι ένα σύνολο τίμιων παικτών.

- Η εκτέλεση $\sigma'$ συμβαίνει στο γράφημα $G'$ με διανομέα $D$, για την τιμή του διανομέα έχουμε ότι $x_D = 1$, το σύνολο διεφθαρμένων παικτών είναι το $H$ και σε κάθε γύρο, όλοι οι παίκτες αυτού του συνόλου στέλνουν τα ίδια μηνύματα που θα στέλνανε στον αντίστοιχο γύρο της εκτέλεσης $\sigma$ όπου το σύνολο $H$ είναι ένα σύνολο τίμιων παικτών.

Σημειώνουμε ότι τα σύνολα $T, H$ είναι πιθανά σύνολα διαφθοράς στα γραφήματα $G, G'$ αντίστοιχα καθώς είναι $t$-τοπικά. Παρατηρούμε ότι το σύνολο $H \cup T$ είναι ένας διαχωριστής που αποσυνδέει τον διανομέα $D$ από το υπογράφημα $B$ και στα δύο γραφήματα $G$ και $G'$ και οι ενέργειες που εκτελούν όλοι οι κόμβοι αυτού του συνόλου-διαχωριστή είναι ακριβώς οι ίδιες και στις δύο εκτελέσεις $\sigma, \sigma'$. Συνεπώς, οι ενέργειες κάθε τίμιου παίκτη $w \in B$ θα είναι πανομοιότυπες και στις δύο εκτελέσεις. Από την υπόθεση μας έχουμε ότι ο αλγόριθμος $\mathcal{A}$ είναι $t$-τοπικά ανεκτικός στο $G$ με διανομέα $D$, άρα ο $w$ θα αποφασίσει στην τιμή του διανομέα 0 κατά την εκτέλεση $\sigma$ στο $G$. Από τα προηγούμενα, πρέπει να αποφασίσει στην ίδια τιμή και στην εκτέλεση $\sigma'$ στο γράφημα $G'$. Ωστόσο, στην τελευταία εκτέλεση η τιμή του διανομέα είναι 1. Αυτό μας δίνει μια αντίφαση αφού υποθέσαμε ότι ο $\mathcal{A}$ είναι $t$-τοπικά ασφαλής αλγόριθμος. □

Παρατηρούμε ότι αν παραλείψουμε την απαίτηση να είναι ο αλγόριθμος $t$-τοπικά ασφαλής, τότε το θεώρημα δεν ισχύει. Διαισθητικά, μπορούμε να χρησιμοποιήσουμε ένα πρωτόκολλο το οποίο χρησιμοποιεί παραδοχές για της τοπολογικές ιδιότητες του δικτύου έτσι ώστε το πρωτόκολλο αυτό να είναι $t$-τοπικά ανεκτικό σε μια οικογένεια γραφημάτων που έχουν τις συγκεκριμένες τοπολογικές ιδιότητες.




Σχήμα 2.3: Επισκόπηση συνθηκών σχετιζόμενες με την ύπαρξη $t$-τοπικά ανεκτικών αλγορίθμων. Οι παράμετροι $LPC(G, D)$ και $\mathcal{X}(G, D)$ ορίζονται στο [PP05] και η $\widetilde{\mathcal{X}}(G, D)$ στο [IS10]. Οι συνεχείς γραμμές δείχνουν γνήσια υποσύνολα. Οι αντίστοιχοι αγγλικοί όροι χρησιμοποιούνται ως εξής· $t$-τοπικά ανεκτικός αλγόριθμος: $t$-locally resilient και ασφαλής αλγόριθμος: safe algorithm

Πιο τυπικά, στο [PP05], οι Pelc και Peleg εισήγαγαν έναν άλλον αλγόριθμο, με την ονομασία *Relaxed Propagation Algorithm*(RPA) ο οποίος χρησιμοποιεί γνώση της τοπολογίας του δικτύου και απέδειξαν ότι υπάρχει ένα γράφημα $G$ με διανομέα $D$ για το οποίο ο RPA είναι 1-τοπικά ανεκτικός ενώ ο CPA δεν είναι. Έτσι, αν χρησιμοποιήσουμε τον RPA στο *ad hoc* μοντέλο υποθέτοντας ότι το δίκτυο είναι στην πραγματικότητα το $G$ τότε αυτός ο αλγόριθμος θα είναι 1-τοπικά ανεκτικός για το $G$ με διανομέα $D$ ενώ ο CPA δεν θα είναι. Το γεγονός ότι ο RPA δεν είναι $t$-τοπικά ασφαλής αλγόριθμος είναι εύκολο να αποδειχθεί. Αυτή η απλή παρατήρηση μας δείχνει ότι το θεώρημα δεν ισχύει αν λάβουμε υπόψιν αλγορίθμους οι οποίοι δεν είναι $t$-τοπικά ασφαλείς.

## 2.10 Συμπεράσματα κεφαλαίου

Από τη στιγμή που η ύπαρξη ενός $t$-τοπικά ανεκτικού αλγόριθμου Εκπομπής σε ένα γράφημα $G$ με διανομέα $D$ προφανώς εξαρτάται από την τοπολογία του $G$, για δοθέντα αριθμό $t$ μπορούμε να ορίσουμε και να συγκρίνουμε οικογένειες γραφημάτων (με καθορισμένο κόμβο-διανομέα) που καθορίζονται από τις ιδιότητες και τις τοπολογικές συνθήκες που έχουν εμφανιστεί έως τώρα στην βιβλιογραφία συμπεριλαμβανομένων αυτών που ορίστηκαν σε αυτό το κεφάλαιο. Μια επισκόπηση των αντίστοιχων οικογενειών και της μεταξύ τους σχέσης απεικονίζεται στο Σχήμα 3.4.

**Η γενική περίπτωση του προβλήματος (Διαφθαρμένος κόμβος-διανομέας).** Όπως αναφέραμε, η ορθότητα του CPA στηρίζεται στην υπόθεση ότι ο διανομέας είναι τίμιος. Προκειμένου να αντιμετωπιστεί η περίπτωση στην οποία ο διανομέας είναι διεφθαρμένος μπορούμε να παρατηρήσουμε ότι εάν ο συνολικός αριθμός των προδοτών είναι αυστηρά μικρότερος του $n/3, n = |V|$, και ο αριθμός των προδοτών σε κάθε γειτονιά είναι φραγμένος από το $\min_{D \in V} \mathcal{T}(G, D)$ τότε μπορούμε να πετύχουμε Εκπομπή προσομοιώνοντας οποιοδήποτε πρωτόκολλο για πλήρη γραφήματα ως εξής: Κάθε μετάδοση ενός παίκτη σε πολλούς (ή ακόμη και ενός παίκτη σε έναν άλλον) αντικαθίσταται από μαι εκτέλεση του CPA. Παρατηρούμε ότι η συνθήκη $\min_{D \in V} \mathcal{T}(G, D)$ μπορεί να μην είναι ακριβής σε αυτήν την περίπτωση. Μπορούμε να πάρουμε ένα καλύτερο φράγμα αν ορίσουμε την παράμετρο $\mathcal{M}(G, D, t)$ λαμβάνοντας υπόψιν μόνο πιθανά σύνολα διεφθαρμένων παικτών με πληθικότητα αυστηρά μικρότερη του $n/3$. Συνεπώς, εξάγουμε ένα άνω φράγμα για Εκπομπή με διεφθαρμένο κόμβο-διανομέα, δηλαδή $t \leq \min\left(\lceil n/3 \rceil - 1, \min_{D \in V} \mathcal{T}(G, D)\right)$. Η εξαγωγή ενός ακριβούς φράγματος για τον αριθμό των διαφθορών όπως και η μελέτη για πιο αποδοτικούς αλγορίθμους για το γενικό πρόβλημα είναι ενδιαφέροντα ανοιχτά ερωτήματα.

Άλλα ανοιχτά ερωτήματα που προκύπτουν από τη μελέτη που παρουσιάζεται σε αυτό το κεφάλαιο είναι τα εξής:
α) Ο ορισμός μιας αποδοτικά υπολογίσιμης παραμέτρου μέσω της οποίας μπορούν να εξαχθούν πιο ακριβή φράγματα από αυτά της παραμέτρου $\mathcal{K}(G, D)$ που θα οδηγήσουν σε μια προσέγγιση του $t_{\max}^{\text{CPA}}$ με λόγο μικρότερο του 2.
β) Ένα άλλο θέμα που δεν έχει μελετηθεί αρκετά είναι η ανάπτυξη τοπικά ανεκτικών πρωτοκόλλων για ασύρματα δίκτυα, όπου πρέπει να αντιμετωπιστεί και το ζήτημα της παρεμβολής συχνοτήτων όταν δύο κόμβοι εκπέμπουν ταυτόχρονα σε κάποιον άλλον (σύγκρουση). Σε αυτήν την κατεύθυνση θα πρέπει να ληφθούν υπόψιν μοντέλα στα οποία ο αντίπαλος δεν μπορεί να προκαλέσει απεριόριστο αριθμό συγκρούσεων, σε διαφορετική περίπτωση θα μπορούσε να εμποδίσει την παράδοση κάποιων μηνυμάτων επ'αόριστον. Η τελευταία περίπτωση έχει μελετηθεί εν μέρη στις εργασίες [Koo04, KKP01, KBKV06].

# Κεφάλαιο 3

# Μερική Γνώση και Φράγματα Διάδοσης

Σε αυτό το κεφάλαιο επεκτείνουμε τη μελέτη μας για το πρόβλημα της αξιόπιστης Εκπομπής σε ελλιπή δίκτυα υπό την παρουσία ενός βυζαντινού αντιπάλου. Εξετάζουμε το πρόβλημα υπό το μοντέλο *τοπικά φραγμένου αντιπάλου* του Koo (2004) και το μοντέλο *γενικού αντιπάλου* των Hirt και Maurer (1997) και ερευνούμε την σχέση μεταξύ του επιπέδου της τοπολογικής γνώσης και της επιλυσιμότητας του προβλήματος. Για να διερευνήσουμε τη σχέση αυτή, εισάγουμε το *μοντέλο μερικής γνώσης* το οποίο περιγράφει την κατάσταση όπου κάθε παίκτης έχει αυθαίρετη γνώση της τοπολογίας.

Επεκτείνουμε την τεχνική του *τοπικού διαχωριστή ζεύγους* (local pair cut) των Pelc και Peleg (2005), προκειμένου να εξάγουμε αποτελέσματα ως προς την επιλυσιμότητα του προβλήματος της Εκπομπής, για κάθε επίπεδο τοπολογικής γνώσης και κάθε είδος κατανομής των διαφθορών. Αναπτύσσουμε πρωτόκολλα για κάθε περίπτωση τοπολογικής γνώσης· για τις ακραίες περιπτώσεις των *ad hoc* δικτύων και της πλήρης γνώσης της τοπολογίας αποδεικνύουμε ότι τα πρωτόκολλα είναι βέλτιστης ανεκτικότητας, δηλαδή επιλύουν το πρόβλημα όποτε αυτό είναι δυνατό. Επομένως καταφέρνουμε να δώσουμε τον ακριβή χαρακτηρισμό των δικτύων στα οποία είναι δυνατή η επίτευξη Εκπομπής σε αυτές τις περιπτώσεις τοπολογικής γνώσης. Στο τέλος του κεφαλαίου, γενικεύουμε τα αποτελέσματά μας, για τις ακραίες περιπτώσεις του επιπέδου γνώσης, στο μοντέλο γενικού αντιπάλου των Hirt και Maurer (1997), του οποίου υποπεριπτώσεις είναι όλα τα γνωστά μοντέλα αντιπάλου. Το πετυχαίνουμε αυτό με την προσαρμογή των τεχνικών και των αλγορίθμων μας που αρχικά παρουσιάζονται στο μοντέλο του τοπικά φραγμένου αντιπάλου.

Μεταξύ άλλων, από την γενικευμένη τεχνική διαχωριστών ζεύγους που παρουσιάζουμε προκύπτει μία διαφορετική, από αυτή που παρουσιάζεται στο Κεφάλαιο 2, και περισσότερο διαισθητική απόδειξη για την εικασία της μοναδικότητας του CPA [PP05], η οποία αναφέρει ότι ο CPA μπορεί να ανεχτεί όσες τοπικές διαφθορές ανέχεται και οποιοσδήποτε άλλος ασφαλής αλγόριθμος. Όπως έχει αναφερθεί προηγουμένως, οι ασφαλείς αλγόριθμοι είναι αλγό-

ριθμοι που ποτέ δεν προκαλούν τη λήψη λανθασμένης απόφασης από έναν παίκτη. Σημειώνουμε ότι η απόδειξη της μοναδικότητας του CPA που παρουσιάζονται σε αυτό το κεφάλαιο είναι η πρώτη δημοσιευμένη απόδειξη για το πρόβλημα και εμφανίστηκε για πρώτη φορά στο [PPS14]. Τέλος, παρουσιάζουμε έναν νέο αλγόριθμο βασισμένο στον CPA, ο οποίος πετυχαίνει Εκπομπή στο μοντέλο γενικού αντιπάλου και αποδεικνύουμε την μοναδικότητα αυτού του αλγορίθμου σε αυτό το γενικότερο μοντέλο. Αυτός ο αλγόριθμος είναι ο πρώτος αλγόριθμος που έχουμε συναντήσει στη βιβλιογραφία και πετυχαίνει Εκπομπή σε *ad hoc* δίκτυα γενικής τοπολογίας με βέλτιστη ανεκτικότητα υπό το μοντέλο γενικού αντιπάλου.

## 3.1 Διάρθρωση του κεφαλαίου

Σε αυτό το κεφάλαιο θα μελετήσουμε την σχέση μεταξύ του επιπέδου τοπολογικής γνώσης και της επιλυσιμότητας του προβλήματος υπό διαφορετικά μοντέλα αντιπάλου. Κατά τη διάρκεια αυτής της μελέτης ασχολούμαστε με την οικογένεια των *ασφαλών αλγορίθμων* Εκπομπής, δηλαδή, με αλγόριθμους που ποτέ δεν προκαλούν λανθασμένη απόφαση από κάποιον παίκτη. Η σημασία αυτής της κατηγορίας αλγορίθμων έχει στηριχθεί στο [PP05] και αναλύονται περαιτέρω στο προηγούμενο κεφάλαιο.

Αρχικά, λαμβάνουμε υπόψιν μία φυσιολογική γενίκευση του μοντέλου $t$-τοπικά φραγμένου αντιπάλου, που το ονομάζουμε μοντέλο *$t$-τοπικά ανομοιόμορφα φραγμένου αντιπάλου* (ή μη ομοιόμορφο μοντέλο) και επεκτείνει το (ομοιόμορφο) μοντέλο που μελετήθηκε μέχρι τώρα. Αυτό το νέο μοντέλο επιτρέπει διαφορετικά φράγματα στον μέγιστο αριθμό των διαφθορών της κάθε γειτονιάς.

Στην Ενότητα 3.3, αντιμετωπίζουμε την περίπτωση της τοπικά ανθεκτικής *ad hoc* Εκπομπής στο μοντέλο ανομοιόμορφα φραγμένου αντιπάλου. Παρουσιάζουμε μια νέα ικανή και αναγκαία συνθήκη για να είναι ο CPA $t$-τοπικά ανεκτικός επεκτείνοντας την έννοια του *τοπικού διαχωριστή ζεύγους* των Pelc και Peleg [PP05] στην έννοια του *μερικού τοπικού διαχωριστή ζεύγους*. Παρά την ύπαρξη ισοδύναμων συνθηκών όπως αυτές παρουσιάζονται στα [TVB12, LPS13], η απλότητα της νέας συνθήκης, την καθιστά εξαιρετικά προσαρμόσιμη σε διαφορετικά μοντέλα αντιπάλου και γνώσης της τοπολογίας. Παρόλο που από την ισοδύναμη συνθήκη που παρουσιάζεται στο Κεφάλαιο 2 προκύπτουν κάποια ενδιαφέροντα αποτελέσματα ως προς την προσέγγιση της λύσης, η συνθήκη που παρουσιάζουμε σε αυτό το κεφάλαιο, μας επιτρέπει να επεκτείνουμε τα αποτελέσματα σχετικά με την επιλυσιμότητα του προβλήματος σε διαφορετικά μοντέλα. Παρουσιάζουμε επίσης μια εναλλακτική και πιο διαισθητική απόδειξη για το ανοιχτό πρόβλημα της μοναδικότητας του CPA [PP05], στο οποίο αναφέρεται ότι αν οποιοσδήποτε ασφαλής αλγόριθμος πετυχαίνει εκπομπή σε ένα *ad hoc* δίκτυο τότε πετυχαίνει και ο CPA. Επιπλέον δείχνουμε ότι ο υπολογισμός της ισχύος της συνθήκης είναι NP-δύσκολος και παρατηρούμε ότι αυτό το αρνητικό αποτέλεσμα έχει και μία θετική όψη, ότι ένας αντίπαλος ο οποίος είναι περιορισμένος σε πολυωνυμικούς υπολογισμούς, δεν δύναται να πραγματοποιήσει μια βέλτιστη επίθεση εκτός αν ισχύει ότι $\mathrm{P} = \mathrm{NP}$.

Στην Ενότητα 3.4, επικεντρωνόμαστε σε δίκτυα γνωστής τοπολογίας και προτείνουμε ένα

πρωτόκολλο βέλτιστης ανεκτικότητας (μοναδικό), το οποίο ονομάζουμε *Αλγόριθμο Διάδοσης Μονοπατιών* (Path Propagation Algorithm-PPA). Χρησιμοποιώντας τον PPA, δείχνουμε ότι η τοπολογική συνθήκη η οποία αποδείχθηκε στο [PP05] ότι είναι αναγκαία για την ύπαρξη αλγορίθμων Εκπομπής, είναι επίσης και ικανή. Με αυτόν τον τρόπο, δίνουμε έναν ακριβή τοπολογικό χαρακτηρισμό των δικτύων στα οποία το πρόβλημα της Εκπομπής επιδέχεται λύση. Από την άλλη πλευρά, στο [PPS14] αποδείξαμε ότι είναι NP-δύσκολο να υπολογιστεί η ορθότητα μιας συνθήκης του αλγορίθμου PPA, το οποίο υποδεικνύει ότι ο αλγόριθμος είναι ακατάλληλος για πρακτική χρήση. Ωστόσο, στην ίδια δουλειά παρείχαμε ενδείξεις ότι δεν υπάρχει κανένα αποδοτικό πρωτόκολλο βέλτιστης ανεκτικότητας, δείχνοντας ότι δεν υπάρχουν αποδοτικοί αλγόριθμοι, μέσω των οποίων οι παίκτες παίρνουν ακριβώς τις ίδιες αποφάσεις όπως αυτές που θα παίρνανε αν εκτελούσαν τον PPA, εκτός και αν $P \neq NP$.

Στη συνέχεια, κάνουμε ένα βήμα παραπάνω στην Ενότητα 3.5, εξετάζοντας ένα υβρίδιο μεταξύ *ad hoc* δικτύων και δικτύων γνωστής τοπολογίας: συγκεκριμένα υποθέτουμε ότι κάθε κόμβος γνωρίζει ένα μέρος του δικτύου, δηλαδή ένα συγκεκριμένο υπογράφημα που περιέχει τον εαυτό του. Προτείνουμε έναν αλγόριθμο που πετυχαίνει Εκπομπή σε αυτό το πλαίσιο, τον *Γενικευμένο Αλγόριθμο Διάδοσης Μονοπατιών* (Generalized Path Propagation Algorithm-GPPA). Χρησιμοποιούμε τον GPPA για να δείξουμε ότι αυτό το μοντέλο *μερικής γνώσης* επιτρέπει την ύπαρξη αλγορίθμων Εκπομπής αυξημένης ανεκτικότητας σε σχέση με την *ad hoc* περίπτωση.

Τέλος, στην Ενότητα 3.6, μελετάμε το μοντέλο γενικού αντιπάλου και δείχνουμε ότι μια κατάλληλη παραλλαγή του αλγορίθμου CPA μας δίνει έναν μοναδικό αλγόριθμο ενάντια σε έναν γενικό αντίπαλο σε *Ad Hoc* δίκτυα. Αυτός είναι ο πρώτος αλγόριθμος που έχουμε συναντήσει στην βιβλιογραφία και πετυχαίνει Εκπομπή σε για γενικά *ad hoc* δίκτυα ενάντια σε γενικό αντίπαλο. Επίσης, παρουσιάζουμε ένα ανάλογο αποτέλεσμα για δίκτυα γνωστής τοπολογίας, το οποίο όμως υπονοείται στο [KGSR02] όπως προαναφέραμε. Στο τέλος αυτού του κεφαλαίου ασχολούμαστε με την επέκταση των αποτελεσμάτων μας στην περίπτωση όπου και ο διανομέας μπορεί να διαφθαρεί· αυτό μπορεί να επιτευχθεί χρησιμοποιώντας πρωτόκολλα Εκπομπής για πλήρη δίκτυα όπου πετυχαίνουμε τις αξιόπιστες ανταλλαγές μηνυμάτων μέσω των πρωτοκόλλων που προτείνουμε σε αυτό το κεφάλαιο.

Ένα κεντρικό εργαλείο στην εργασία μας είναι μια εκλέπτυνση της τοπικής ζεύγους-cut τεχνική της Pelc και Φαλέγ cite PP05 η οποία αποδεικνύεται ότι είναι επαρκής για την ακριβή (στις περισσότερες περιπτώσεις) χαρακτηρισμό της κατηγορίας των γραφημάτων για τα οποία είναι δυνατόν Broadcast για κάθε επίπεδο γνώσεων τοπολογία και το είδος της κατανομής της διαφθοράς. Ένα χρήσιμο παραπροϊόν πρακτικό ενδιαφέρον είναι ότι οι εκλεπτυσμένη περικοπές μπορούν να χρησιμοποιηθούν για να καθορίσουν την ακριβή υπογράφημα στο οποίο Broadcast είναι δυνατόν κάτω από οποιοδήποτε σύνολο διαφθοράς.

Κεντρικής σημασίας εργαλείο στην παρούσα εργασία είναι η γενίκευση της τεχνικής των τοπικών διαχωριστών ζεύγους των Pelc και Peleg [PP05]. Η τεχνική αυτή αποδεικνύεται εξαιρετικά χρήσιμη για τον ακριβή χαρακτηρισμό της οικογένειας των γραφημάτων για την οποία είναι δυνατή η Εκπομπή σε κάθε επίπεδο γνώσης τοπολογίας και κατανομή των διεφθαρμένων παικτών. Μια παρατήρηση πρακτικού ενδιαφέροντος είναι ότι αυτή η γενικευμένη τεχνική τοπικών διαχωριστών ζεύγους μπορεί να χρησιμοποιηθεί για να καθοριστεί το υπογράφημα

στο οποίο είναι δυνατή η Εκπομπή είναι δυνατόν κάτω από οποιοδήποτε σύνολο διαφθοράς.

Για μεγαλύτερη σαφήνεια, επιλέξαμε να παρουσιάσουμε αρχικά τα αποτελέσματα στο μοντέλο του $t$-τοπικά φραγμένου αντιπάλου (Ενότητες 3.3,3.4, 3.5), στο οποίο οι αποδείξεις και τα πρωτόκολλα είναι απλούστερα και πιο διαισθητικά. Έπειτα, παρουσιάζουμε τα αποτελέσματα στο, πιο περίπλοκο, μοντέλο του γενικού αντιπάλου (Ενότητα 3.6).

Αυτό το κεφάλαιο περιλαμβάνει αποτελέσματα που παρουσιάστηκαν αρχικά στα [PPS14, PPS16b]

## 3.2 Προκαταρκτικοί ορισμοί

Στη συνέχεια θα ορίσουμε τυπικά το μοντέλο αντιπάλου γενικεύοντας τις έννοιες που αναπτύχθηκαν αρχικά στα [Koo04, PP05] και παρουσιάζονται στο κεφάλαιο 2. Θα ορίσουμε επίσης, βασικές έννοιες και την ορολογία που θα χρησιμοποιηθεί σε αυτό το κεφάλαιο. Θα Αναφερόμαστε στους συμμετέχοντες ενός πρωτοκόλλου με τους όρους *κόμβος* και *παίκτης* εναλλακτικά.

**Συνάρτηση διαφθοράς.** Λαμβάνοντας υπόψη ότι κάθε παίκτης θα μπορούσε να εκτιμήσει το δικό του άνω φράγμα για τον αριθμό των διαφθορών στη γειτονιά του, όπως αναφέρθηκε νωρίτερα, εισάγουμε ένα μοντέλο στο οποίο ο μέγιστος αριθμός των διαφθορών μπορεί να είναι διαφορετικός σε διαφορετικές γειτονιές. Ως εκ τούτου, γενικεύουμε το κλασσικό μοντέλο $t$-τοπικά φραγμένου αντιπάλου [Koo04] στο οποίο υπάρχει ένα ενιαίο άνω φράγμα στον τον αριθμό των τοπικών διαφθορών. Εδώ θεωρούμε την $t : V \to \mathbb{N}$ να είναι μία *συνάρτηση διαφθοράς* με πεδίο ορισμού το σύνολο των παικτών $V$.

**Μοντέλο $t$-τοπικά ανομοιόμορφα φραγμένου αντιπάλου.** Το δίκτυο αναπαρίσταται από ένα γράφημα $G = (V, E)$ και ο διανομέας είναι ένας παίκτης $D \in V$ όπως εξηγήθηκε προηγουμένως. Δίνεται επίσης μια συνάρτηση διαφθοράς $t : V \to \mathbb{N}$ η οποία ορίζει ότι ο αντίπαλος μπορεί να διαφθείρει το πολύ $t(u)$ παίκτες στην γειτονιά $\mathcal{N}(u)$ οποιουδήποτε κόμβου $u \in V$. Θα αναφερόμαστε σε αυτό το μοντέλο και ως *μη ομοιόμορφο μοντέλο.* Η οικογένεια των *$t$-τοπικών* συνόλων (όπως ορίζεται παρακάτω) είναι αυξημένης σημασίας στη μελέτη μας αφού συμπίπτει με την οικογένεια των πιθανών συνόλων διεφθαρμένων παικτών.

***Ορισμός* 3.1** ($t$-τοπικά σύνολα). *Έστω ένα γράφημα $G = (V, E)$ και μια συνάρτηση $t : V \to \mathbb{N}$, ένα $t$-τοπικό σύνολο είναι ένα σύνολο $C \subseteq V$ για το οποίο $\forall u \in V,\ |\mathcal{N}(u) \cap C| \leq t(u)$. Για $V' \subseteq V$ ένα $t$-τοπικό σύνολο ως προς το $V'$ είναι ένα σύνολο $C \subseteq V$ για το οποίο $\forall u \in V',\ |\mathcal{N}(u) \cap C| \leq t(u)$.*

**Σύγκριση με το ομοιόμορφο μοντέλο.** Είναι φανερό ότι το αρχικό μοντέλο $t$-τοπικά φραγμένου αντιπάλου αντιστοιχεί στην ειδική περίπτωση όπου το $t$ είναι μια σταθερή συ-

νάρτηση. Στη συνέχεια, θα αναφερόμαστε στο αρχικό μοντέλο $t$-τοπικά φραγμένου αντιπάλου ως *ομοιόμορφο μοντέλο* σε αντίθεση με το *μη ομοιόμορφο* που εισήχθη παραπάνω. Επειδή η μελέτη αυτού του κεφαλαίου επικεντρώνεται στο μη ομοιόμορφο μοντέλο θα αναφερόμαστε σε αυτό απλά ως το μοντέλο $t$-τοπικά φραγμένου αντιπάλου, υπονοώντας ότι το $t$ είναι η συνάρτηση διαφθοράς όπως ορίστηκε παραπάνω.

Στη μελέτη μας, θα κάνουμε συχνά χρήση διαχωριστών του γραφήματος που χωρίζουν κάποιους παίκτες από τον διανομέα, δηλαδή, διαχωριστές οι οποίοι δεν περιλαμβάνουν τον διανομέα. Από εδώ και πέρα, θα χρησιμοποιούμε απλά τον όρο *διαχωριστής* για να υποδηλώνουμε έναν διαχωριστή τέτοιας μορφής. Η έννοια του *$t$-τοπικού διαχωριστή ζεύγους* ($t$-local pair cut) εισήχθη στο [PP05] και είναι κεντρικής σημασίας για τον καθορισμό των ορίων στα οποία η ορθή διάδοση πληροφορίας σε ένα δίκτυο είναι εφικτή.

***Ορισμός* 3.2** ($t$-τοπικός διαχωριστής ζεύγους ). *Έστω ένα γράφημα $G = (V, E)$ και μια συνάρτηση $t : V \to \mathbb{N}$, ένα ζεύγος $t$-τοπικών συνόλων $C_1, C_2$ τέτοιο ώστε το $C_1 \cup C_2$ είναι διαχωριστής του $G$ ονομάζεται* $t$-τοπικός διαχωριστής ζεύγους.

Ο επόμενος ορισμός του *$t$-τοπικός μερικός διαχωριστής ζεύγους* ($t$-partial local pair cut) επεκτείνει την έννοια του $t$-τοπικού διαχωριστή ζεύγους και είναι ιδιαίτερα χρήσιμος για την περιγραφή της δυνατότητας Εκπομπής σε δίκτυα άγνωστης τοπολογίας (*ad hoc* δίκτυα) όπου η τοπολογική γνώση του κάθε παίκτη περιορίζεται στην γειτονιά του.

***Ορισμός* 3.3** ($t$-τοπικός μερικός διαχωριστής ζεύγους). *Έστω $C$ ένας διαχωριστής του $G$, που διαμερίζει το σύνολο $V \setminus C$ στα σύνολα $A, B \neq \emptyset$ τ.ώ. $D \in A$. Το $C$ είναι ένας is a* $t$-τοπικός μερικός διαχωριστής ζεύγους ($t$-plp διαχωριστής) *αν υπάρχει μια διαμέριση $C = C_1 \cup C_2$ όπου $C_1$ είναι $t$-τοπικό και $C_2$ είναι $t$-τοπικό ως προς το $B$.*

Στο ομοιόμορφο μοντέλο, χρησιμοποιήθηκε η παράμετρος *τοπική συνδεσιμότητα ζεύγους* (LPC($G, D$) [PP05] ενός γραφήματος $G$ με διανομέα $D$, η οποία ορίστηκε ως ο ελάχιστος ακέραιος $t$ τ.ώ. υπάρχει $t$-τοπικός διαχωριστής ζεύγους στο $(G, D)$. Για να ορίσουμε την αντίστοιχη έννοια στο μη ομοιόμορφο μοντέλο χρειάζεται να ορίσουμε μια μερική διάταξη μεταξύ των συναρτήσεων διαφθοράς. Παρ'όλα αυτά, όπως φαίνεται από τα Θεωρήματα 3.1 και 3.2, για τη μελέτη της δυνατότητας Εκπομπής αρκεί να λάβουμε υπόψιν μας το ακόλουθο πρόβλημα απόφασης:

***Ορισμός* 3.4** (Πρόβλημα $pLPC$). *Έστω ένα γράφημα $G$ με διανομέα $D$ και μία συνάρτηση διαφθοράς $t$, να αποφασιστεί αν υπάρχει ένας $t$-plp διαχωριστής στο $(G, D)$.*

### 3.2.1 Το Μοντέλο μερικής γνώσης

Στη συνέχεια εισάγουμε το *μοντέλο μερικής γνώσης* όπου κάθε παίκτης έχει αρχική γνώση ως προς ένα συγκεκριμένο υπογράφημα του πραγματικού γραφήματος $G$. Το μοντέλο μερικής γνώσης παρουσιάστηκε για πρώτη φορά στο [PPS14].

Η ανάγκη μελέτης μοντέλων περιορισμένης γνώσης υπαγορεύεται από εφαρμογές σε δίκτυα ευρείας κλίμακας (π.χ. το διαδίκτυο), όπου η εκτίμηση του βαθμού δυσλειτουργίας μπορεί να

γίνει με σχετική ακρίβεια από τον κάθε συμμετέχοντα στα πλαίσια της γειτονιάς του, ενώ μια συνολική εκτίμηση μπορεί να είναι δύσκολο να επιτευχθεί λόγω γεωγραφικών περιορισμών και περιορισμών δικαιοδοσίας. Επιπλέον, η εγγύτητα κόμβων σε κοινωνικά δίκτυα συχνά συσχετίζεται με αυξημένη ποσότητα διαθέσιμης πληροφορίας, γεγονός που δικαιολογεί περαιτέρω την ευστάθεια του μοντέλου.

Σε αυτό το μοντέλο, κάθε παίκτης $v$ έχει μόνο τοπολογική γνώση ενός συγκεκριμένου υπογραφήματος $G_v$ του δικτύου $G$ το οποίο συμπεριλαμβάνει και τον εαυτό του. Συγκεκριμένα, θεωρούμε την οικογένεια $\mathcal{G}$ όλων των υπογραφημάτων του $G$ και χρησιμοποιούμε την *συνάρτηση γνώσης* $\gamma : V(G) \to \mathcal{G}$, όπου $\gamma(v)$ αντιπροσωπεύει το υπογράφημα του οποίου η τοπολογία είναι γνωστή στον παίκτη $v$. Επεκτείνουμε το πεδίο ορισμού της $\gamma$ επιτρέποντας σαν όρισμα της συνάρτησης ένα σύνολο $S \subseteq V(G)$. Η τιμή της συνάρτησης στο $S$ θα αντιστοιχεί στην *από κοινού γνώση* όλων των κόμβων στο $S$. Πιο συγκεκριμένα, αν $\gamma(v) = G_v = (V_v, E_v)$, τότε $\gamma(S) = G_S = (\bigcup_{v \in S} V_v, \bigcup_{v \in S} E_v)$. Το *ad hoc* μοντέλο, που έχει μελετηθεί εκτενώς, είναι στην πραγματικότητα μια ειδική περίπτωση του μοντέλου μερικής γνώσης, όπου θεωρούμε ότι η τοπολογική γνώση του κάθε παίκτη περιορίζεται στην γειτονιά του, δηλαδή, $\forall v \in V(G),\ \gamma(v) = \mathcal{N}(v)$.

## 3.3 *Ad Hoc* Δίκτυα

### 3.3.1 Ο αλγόριθμος (CPA)

Στον αλγόριθμο CPA, οι παίκτες χρησιμοποιούν μόνο τοπικές πληροφορίες. Αυτό καθιστά τον CPA ιδανικό για *ad hoc* δίκτυα, όπου η τοπολογική γνώση του κάθε παίκτη περιορίζεται στην γειτονιά του. Ο CPA είναι πιθανώς ο μόνος γνωστός αλγόριθμος Εκπομπής για το μοντέλου τοπικά φραγμένου αντιπάλου, ο οποίος δεν χρησιμοποιεί γνώση της τοπολογίας του δικτύου ή υπορουτίνες ανακάλυψης της τοπολογίας.

Πιθανώς, ένας άλλος, πιο πολύπλοκος αλγόριθμος θα μπορούσε να κατασκευαστεί για αυτό το πλαίσιο χρησιμοποιώντας έναν αλγόριθμο ανακάλυψης τοπολογίας (π.χ. παραλλαγή του [NT09]), και στη συνέχεια να χρησιμοποιεί την γνώση της τοπολογίας για να εκτελέσει κάποιον γνωστό αλγόριθμο Εκπομπής ο οποίος απαιτεί μεγαλύτερο επίπεδο τοπολογικής γνώσης (π.χ. ο αλγόριθμος RPA που παρουσιάστηκε στο [PP05]).

Ο CPA δεν χρησιμοποιεί καμία υπορουτίνα ανακάλυψης τοπολογίας· παρά την απλότητά του και την ελάχιστη πολυπλοκότητα μηνυμάτων (ένας παίκτης διαδίδει μόνο την τιμή στην οποία αποφάσισε σε όλους τους γείτονές του) αποδεικνύεται ότι η ανεκτικότητα του είναι βέλτιστη (δηλαδή είναι *μοναδικός*). Το τελευταίο σημαίνει ότι δεν γίνεται να επιτύχουμε καλύτερη επιλυσιμότητα του προβλήματος με τη χρήση πιο πολύπλοκων αλγορίθμων. Επιπλέον, ο συνδυασμός των αποτελεσμάτων αυτού του κεφαλαίου με αυτά των Ενοτήτων 3.4, 3.5 υπονοεί ότι υπάρχουν στιγμιότυπα στα οποία το πρόβλημα δεν είναι επιλύσιμο στο *Ad Hoc* μοντέλο, αλλά είναι επιλύσιμο εάν υποθέσουμε υψηλότερο επίπεδο γνώσης της τοπολογίας. Αυτό υποδηλώνει ότι κανένας αλγόριθμος ανακάλυψης τοπολογίας στο *ad hoc* μοντέλο δεν μπορεί να

μας παρέχει κάποια χρήσιμη πληροφορία που θα επηρεάσει την επιλυσιμότητα του προβλήματος.

Το Πρωτόκολλο 2, που παρουσιάζεται στη συνέχεια, αποτελεί μια τροποποίηση του αρχικού CPA η οποία μπορεί να εφαρμοστεί στο γενικευμένο μοντέλο τοπικά φραγμένων διαφθορών που εισάγαμε σε αυτό το κεφάλαιο. Συγκεκριμένα, ένας κόμβος $v$, κατά την παραλαβή $t(v)+1$ μηνυμάτων με την ίδια τιμή $x$ από $t(v)+1$ διαφορετικούς γείτονες, αποφασίζει στο $x$, το στέλνει σε όλους του γείτονές του και τερματίζει. Ακολουθεί η περιγραφή του Πρωτοκόλλου:

---

**Πρωτόκολλο 2**: ***Certified Propagation Algorithm (CPA)***

---

***Είσοδος:***
(Για κάθε παίκτη $v$) Ταυτότητα του διανομέα $D$, ταυτότητες γειτόνων του $v$, παράμετρος αντιπάλου $t$.
(Για τον διανομέα $D$) Αρχική τιμή $x_D$.
*Μορφή μηνυμάτων*: Τιμή $x \in X$, όπου $X$ ο χώρος μηνυμάτων.

**Κώδικας του** $D$: Στείλε $x_D \in X$ σε όλους τους γείτονες, αποφάσισε στο $x_D$ και τερμάτισε.

**Κώδικας του** $v \in \mathcal{N}(D)$: Αφού λάβεις την τιμή $x_D$ από τον διανομέα, αποφάσισε στο $x_D$, στείλε το $x_D$ σε όλους τους γείτονές σου και τερμάτισε.

(* *κανόνας πιστοποιημένης διάδοσης* *)

**Κώδικας του** $v \notin \mathcal{N}(D) \cup D$: Αν λάβεις $t(v)+1$ μηνύματα με τη ν ίδια τιμή $x$ από $t(v)+1$ διαφορετικούς γείτονες, αποφάσισε στο $x$, στείλε το $x$ σε όλους τους γείτονές σου και τερμάτισε.

---

Όπως έχει ήδη δειχθεί στην Ενότητα 2.4, ο CPA είναι ένας $t$-τοπικά ασφαλής αλγόριθμος Εκπομπής. Η απόδειξη για το μη ομοιόμορφο μοντέλο είναι πανομοιότυπη με την απόδειξη που παρουσιάστηκε για το ομοιόμορφο μοντέλο.

### 3.3.2 Μοναδικότητα του CPA σε *Ad Hoc* δίκτυα

Στηριζόμενοι στους ορισμούς που δόθηκαν παραπάνω, θα δώσουμε τώρα μια εναλλακτική και περισσότερο διαισθητική απόδειξη για την την υπόθεση της *μοναδικότητας του CPA* σε *ad hoc* δίκτυα, η οποία τέθηκε σαν ανοιχτό πρόβλημα στο [PP05]. Υπενθυμίζουμε ότι η υπόθεση αναφέρει πως κανένας αλγόριθμος δεν μπορεί να ανεχτεί περισσότερες τοπικές διαφθορές από τον CPA σε *ad hoc* δίκτυα.

Λαμβάνουμε υπόψιν μόνο την οικογένεια των *$t$-τοπικά ασφαλών* αλγορίθμων Εκπομπής. Υποθέτουμε το μοντέλο *ad hoc* δικτύων όπου οι κόμβοι γνωρίζουν μόνο τα δικά τους αναγνωριστικά (ids) και τα αναγνωριστικά των γειτόνων τους. Ένας κατανεμημένος αλγόριθμο εκπομπής που λειτουργεί υπό αυτές τις προϋποθέσεις θα καλείται *ad hoc αλγόριθμος Εκπομπής*.

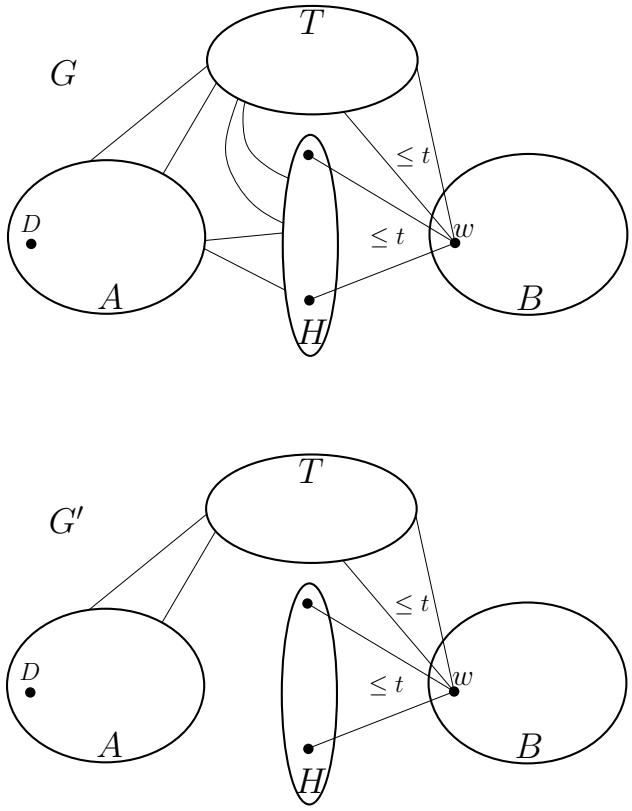
***Θεώρημα* 3.1** (Ικανή συνθήκη). *Έστω ένα γράφημα $G$, μια συνάρτηση διαφθοράς $t$ και ένας διανομέας $D$, εάν δεν υπάρχει $t$-plp διαχωριστής στο $(G, D)$, τότε ο CPA είναι $t$-τοπικά ανεκτικός για το $(G, D)$.*

*Απόδειξη.*
Υποθέτουμε ότι δεν υπάρχει $t$-plp διαχωριστής στο $G, D$. Υποθέτουμε μια εκτέλεση του CPA όπου το πραγματικό σύνολο διεφθαρμένων παικτών είναι το $T$. Από τον ορισμό, το $T$ είναι $t$-τοπικό επειδή έχουμε υποθέσει το μοντέλο $t$-τοπικά φραγμένου αντιπάλου· προφανώς το $T \cup \mathcal{N}(D)$ είναι ένας διαχωριστής του $G$ όπως ορίστηκε προηγουμένως(δηλ. περιέχει τον κόμβο $D$). Αφού το $T$ είναι $t$-τοπικό και $T \cup \mathcal{N}(D)$ δεν είναι ένας $t$-plp διαχωριστής πρέπει να υπάρχει $u_1 \in V \setminus (T \cup \mathcal{N}(D) \cup D)$ τ.ώ. $|\mathcal{N}(u_1) \cap (\mathcal{N}(D) \setminus T)| \geq t(u_1) + 1$. Αφού ο $u_1$ είναι τίμιος και όλοι οι παίκτες στο $\mathcal{N}(D) \setminus T$ θα αποφασίσουν τετριμμένα στην σωστή τιμή $x_D$ μέσω του CPA σαν άμεσοι γείτονες του διανομέα, ο $u_1$ θα λάβει $t(u_1)$ αντίγραφα του $x_D$ και θα αποφασίσει στην *σωστή* τιμή του διανομέα $x_D$. Χρησιμοποιούμε τώρα το ίδιο επιχείρημα επαγωγικά για να δείξουμε ότι κάθε τίμιος παίκτης θα αποφασίσει τελικά στην σωστή τιμή $x_D$ μέσω του CPA. Έστω $C_k = (\mathcal{N}(D) \setminus T) \cup \{u_1, u_2, ..., u_{k-1}\}$ το σύνολο των τίμιων παικτών που έχουν αποφασίσει μέχρι ένα συγκεκριμένο γύρο του πρωτοκόλλου, και έστω ότι έχουν αποφασίσει στην σωστή τιμή $x_D$. Τότε το $C_k \cup T$ είναι ένας διαχωριστής. Αφού το $T$ είναι $t$-τοπικό, μέσω του ίδιου επιχειρήματος που χρησιμοποιήσαμε πριν προκύπτει ότι υπάρχει ένας κόμβος $u_k$ s.t. $|C_k \cap \mathcal{N}(u_k)| \geq t(u_k) + 1$ και ότι ο $u_k$ θα αποφασίσει στην σωστή τιμή $x_D$. Τελικά όλοι οι τίμιοι παίκτες ια αποφασίσουν στην σωστή τιμή $x_D$. Επομένως ο CPA είναι $t$-τοπικά ανεκτικός στο $(G, D)$. □

Σημειώνεται ότι η παραπάνω απόδειξη δεν χρησιμοποιεί ρητά το γεγονός ότι ο CPA είναι $t$-τοπικά ασφαλής. Αντί αυτού, δείχνουμε επαγωγικά ότι σε κάθε βήμα (πριν τερματίσουν όλοι οι κόμβοι), υπάρχουν κάποιοι κόμβοι που αποφασίζουν και ότι όλοι αποφασίζουν στην σωστή τιμή. Μια μικρή τροποποίηση της απόδειξης μπορεί μπορεί να χρησιμοποιηθεί σαν εναλλακτική απόδειξη για την $t$-τοπική ασφάλεια του CPA αφού στην επαγωγική υπόθεση θεωρούμε ότι όλοι οι αποφασισμένοι κόμβοι έχουν αποφασίσει στην σωστή τιμή.

***Θεώρημα* 3.2** (Αναγκαιότητα της συνθήκης). *Έστω $\mathcal{A}$ ένας $t$-τοπικά ασφαλής ad hoc αλγόριθμος Εκπομπής. Έστω ένα γράφημα $G$, μία συνάρτηση διαφθοράς $t$ και ο διανομέας $D$, εάν υπάρχει ένας $t$-plp διαχωριστής, τότε ο $\mathcal{A}$ δεν είναι $t$-τοπικά ανεκτικός στο $(G, D)$.*

*Απόδειξη.*
Υποθέτουμε τη διαμέριση του συνόλου $V$ στα σύνολα $A, B, T, H$ τέτοια ώστε $C = T \cup H$ είναι ένας $t$-plp διαχωριστής στο γράφημα $G$ με διανομέα $D$ ο οποίος αποσυνδέει τα σύνολα $A, B$ μεταξύ τους. Έστω το $T$ είναι $t$-τοπικό σύνολο και το $H$ $t$-τοπικό ως προς το σύνολο $B$ (Σχήμα 3.1). Έστω $G'$ το γράφημα που προκύπτει από το $G$ εάν αφαιρέσουμε όλες τις ακμές που συνδέουν κόμβους από το σύνολο $A \cup T \cup H$ με κόμβους στο $H$ έτσι ώστε το σύνολο $H$ μετατρέπεται σε $t$-τοπικό στο $G'$ (π.χ. μπορούμε να αφαιρέσουμε όλες τις ακμές που συνδέουν κόμβους στο $A \cup T \cup H$ με κόμβους στο $H$). Παρατηρείστε ότι η ύπαρξη ενός συνόλου ακμών




Σχήμα 3.1: Τα γραφήματα $G$ και $G'$

που μας εγγυάται την παραπάνω ιδιότητα υπονοείται από το γεγονός ότι το $H$ είναι $t$-τοπικό ως προς το $B$.

Η απόδειξη γίνεται με απαγωγή σε άτοπο. Υποθέτουμε ότι υπάρχει ένας $t$-τοπικά ασφαλής αλγόριθμος Εκπομπής $\mathcal{A}$ ο οποίος είναι $t$-τοπικά ανεκτικός στο γράφημα $G$ με διανομέα $D$. Θεωρούμε τις ακόλουθες εκτελέσεις $\sigma$ και $\sigma'$ του αλγορίθμου $\mathcal{A}$ :

- Η εκτέλεση $\sigma$ συμβαίνει στο γράφημα $G$ με διανομέα $D$, τιμή του διανομέα $x_D = 0$, και σύνολο διεφθαρμένων παικτών το $T$· σε κάθε γύρο κάθε διεφθαρμένος παίκτης στο $T$ εκτελεί τις ενέργειες τις οποίες θα εκτελούσε στον αντίστοιχο γύρο της εκτέλεσης $\sigma'$ (όπου $T$ είναι ένα σύνολο τίμιων παικτών).
- Η εκτέλεση $\sigma'$ συμβαίνει στο γράφημα $G'$ με διανομέα $D$, τιμή του διανομέα $x_D = 1$, και σύνολο διεφθαρμένων παικτών το $H$· σε κάθε γύρο κάθε διεφθαρμένος παίκτης στο $H$ εκτελεί τις ενέργειες τις οποίες θα εκτελούσε στον αντίστοιχο γύρο της εκτέλεσης $\sigma$ (όπου $H$ είναι ένα σύνολο τίμιων παικτών).

Σημειώνεται ότι τα σύνολα $T, H$ είναι επιτρεπτά σύνολα διαφθοράς στα $G, G'$ αντίστοιχα αφού είναι $t$-τοπικά στα αντίστοιχα γραφήματα. Είναι προφανές ότι το $H \cup T$ είναι ένας

διαχωριστής που αποσυνδέει τον $D$ από το σύνολο $B$ και στα δύο γραφήματα $G$ και $G'$ και ότι οι ενέργειες οποιουδήποτε κόμβου σε αυτόν τον διαχωριστή είναι ίδιες και στις δύο εκτελέσεις $\sigma, \sigma'$. Συνεπώς, οι ενέργειες κάθε τίμιου κόμβου $w \in B$ πρέπει να είναι ακριβώς οι ίδιες και στις δύο εκτελέσεις. Επειδή, από την υπόθεσή μας, ο αλγόριθμος $\mathcal{A}$ είναι $t$-τοπικά ανεκτικός στο $G$ με διανομέα $D$, ο $w$ πρέπει να αποφασίσει στην τιμή 0 του διανομέα στην εκτέλεση $\sigma$ στο $G$ με διανομέα $D$, και θα κάνει το ίδιο και στην εκτέλεση $\sigma'$ στο $G'$. Εντούτοις, στην εκτέλεση $\sigma'$ η τιμή του διανομέα είναι 1. Επομένως μέσω του αλγορίθμου $\mathcal{A}$ ο $w$ θα αποφασίσει σε λάθος τιμή στο $(G', D)$. Αυτό έρχεται σε αντίθεση με την υπόθεση ότι ο $\mathcal{A}$ είναι $t$-τοπικά ασφαλής. □

**Σημείωση για την απόδειξη του Θεωρήματος 3.2.** Παρά το γεγονός ότι το επιχείρημα με τις δύο ταυτόχρονες εκτελέσεις $\sigma, \sigma'$ είναι μία καθιερωμένη ιδέα στη βιβλιογραφία (π.χ. [Dol82, KGSR02, Koo04, PP05]), μπορεί να φαίνεται ότι ο ορισμός των ενεργειών των διεφθαρμένων παικτών είναι κυκλικός και γιαυτό οι ενέργειες δεν είναι καλώς ορισμένες. Για ευκολία της παρουσίασης θα συμβολίζουμε με $T, H$ τα σύνολα της εκτέλεσης $\sigma$ και με $T', H'$ τα αντίστοιχα σύνολα στην εκτέλεση $\sigma'$. Η κυκλικότητα του ορισμού μπορεί (ψευδώς) να εμφανιστεί στο ακόλουθο παράδειγμα: Οι ενέργειες του $T$ εξαρτώνται από τις ενέργειες του $T'$ που με τη σειρά τους μπορεί να εξαρτώνται από τα μηνύματα που λαμβάνουν οι παίκτες από το $H'$ τα οποία εξορισμού εξαρτώνται από τις ενέργειες του $H$ στην εκτέλεση $\sigma$ που τελικά μπορεί να εξαρτάται από τις ενέργειες του $T$. Για να ξεπεράσουμε αυτή την ασάφεια παρατηρούμε ότι οι ενέργειες όλων των παικτών είναι μοναδικά ορισμένες με έναν επαγωγικό τρόπο, δηλαδή, στον πρώτο γύρο και των δύο εκτελέσεων οι ενέργειες των τίμιων παικτών στα αντίστοιχα σύνολα $H, T'$ είναι μοναδικά ορισμένες από το ντετερμινιστικό πρωτόκολλο $\mathcal{A}$ και τις αρχικές τιμές τους, λόγω του ότι δεν έχουν ακόμη λάβει κανένα μήνυμα. Επομένως, οι ενέργειες που εκτελούνται στον πρώτο γύρο από τα αντίστοιχα διεφθαρμένα σύνολα $H', T$ είναι μοναδικά ορισμένες από τις ενέργειες των $H, T'$. Υποθέτοντας ότι οι ενέργειες (μηνύματα που ανταλλάσσονται) όλων των παικτών είναι μοναδικά ορισμένες μέχρι το τέλος του γύρου $k$, μπορούμε να παρατηρήσουμε ότι οι ενέργειες όλων των παικτών είναι μοναδικά ορισμένες και στον γύρο $k+1$ λόγω του γεγονότος ότι τα μηνύματα που διαδίδονται στον γύρο $k+1$καθορίζονται πλήρως από τις ενέργειες που εκτελούνται μέχρι τον γύρο $k$.

***Πόρισμα* 3.3** (Μοναδικότητα του CPA). *Για ένα γράφημα $G$ με διανομέα $D$, εάν υπάρχει ασφαλής ad hoc αλγόριθμος Εκπομπής ο οποίος είναι $t$-τοπικά ανεκτικός στο $(G, D)$, τότε και ο CPA είναι $t$-τοπικά ανεκτικός στο $(G, D)$.*

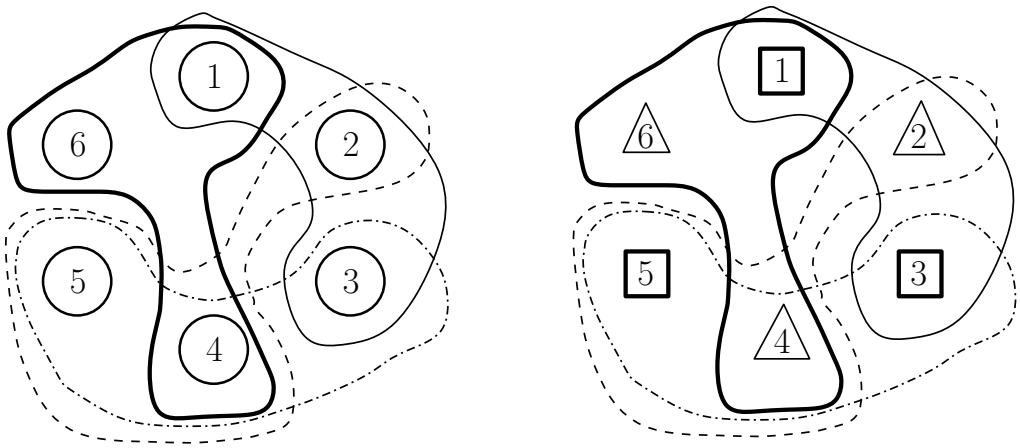
*Απόδειξη.*
Προκύπτει άμεσα από τα Θεωρήματα 3.1,3.2. □

Το παραπάνω, σύμφωνα με τον ορισμό της μοναδικότητας σημαίνει ότι ο CPA είναι μοναδικός μεταξύ των $t$-τοπικά ασφαλών αλγορίθμων.

### 3.3.3 Δυσκολία επίλυσης του προβλήματος $pLPC$

Οι Ichimura και Shigeno στο [IS10] απέδειξαν ότι το *πρόβλημα διαχωρισμού συνόλων* (set splitting problem), γνωστό ως NP-δύσκολο [GJ79], ανάγεται στο πρόβλημα του υπολογισμού του μικρότερου ακεραίου $t$ τέτοιου ώστε υπάρχει ένας $t$-τοπικός διαχωριστής ζεύγους στο γράφημα $G$. Έχοντας γενικεύσει την έννοια του $t$-τοπικού διαχωριστή ζεύγους σε αυτή του $t$-plp διαχωριστή έχουμε ορίσει το πρόβλημα $pLPC$. Παρουσιάζουμε μια απόδειξη σχεδόν πανομοιότυπη με αυτή του [IS10] για να δείξουμε ότι το $pLPC$ πρόβλημα είναι επίσης NP-δύσκολο.

***Θεώρημα* 3.4**. *Το πρόβλημα $pLPC$ είναι* NP*-δύσκολο.*




Σχήμα 3.2: Ένα στιγμιότυπο και η λύση του προβλήματος διαχωρισμού συνόλων με $X = \{1, 2, 3, 4, 5, 6\}$ και $S = \{\{1, 2, 3\}, \{3, 4, 5\}, \{1, 4, 6\}, \{2, 4, 5\}\}$. Η λύση απεικονίζεται με τα δύο σύνολα $X_1 = \{1, 3, 5\}$ και $X_2 = \{2, 4, 6\}$, τα στοιχεία των οποίων απεικονίζονται με τετράγωνα και τρίγωνα αντίστοιχα. Παρατηρείστε ότι όλα τα σύνολα του $S$ έχουν τουλάχιστον έναν κόμβο σε κάθε σύνολο $X_1, X_2$.

*Απόδειξη.*
Αρχικά ασχολούμαστε με μια παραλλαγή του προβλήματος pLPC στην οποία το ζητούμενο είναι ο προσδιορισμός ύπαρξης $t$-plp στο δίκτυο όπου ο διανομέας δεν είναι συγκεκριμένος, δηλαδή, εάν υπάρχει ένας $t$-plp διαχωριστής για οποιοδήποτε κόμβο-διανομέα στο σύνολο των κόμβων. Στο τέλος της απόδειξης δείχνουμε ότι αν αυτή η γενικότερη παραλλαγή του pLPC προβλήματος είναι NP-δύσκολη τότε είναι και το αρχικό pLPC πρόβλημα (με συγκεκριμένο διανομέα).

Αρχικά δείχνουμε ότι το *πρόβλημα διαχωρισμού συνόλων* το οποίο είναι γνωστό ως NP-δύσκολο [GJ79] ανάγεται στο γενικό pLPC πρόβλημα. Δοθείσας μιας συλλογής $S$ τριάδων οι οποίες είναι υποσύνολα του πεπερασμένου συνόλου $X$, στο πρόβλημα διαχωρισμού συνόλων ζητάμε αν υπάρχει μια διαμέριση του $X$ σε δύο σύνολα $X_1$ και $X_2$ τέτοια ώστε καμία τριάδα του $S$ δεν

περιέχεται εξολοκλήρου στο $X_1$ ή στο $X_2$. Ένα στιγμιότυπο αυτού του προβλήματος και η λύση του απεικονίζεται στο Σχήμα 3.2.

Προτείνουμε την ακόλουθη αναγωγή. Έστω $S+$ μια συλλογή που προκύπτει προσθέτοντας μονοσύνολα $\{v\}$ στο $S$ τέτοια ώστε η πληθικότητα του $\{s \in S+ : v \in s\}$ είναι τουλάχιστον 6 για κάθε $v \in X$. Ένα πλήρες γράφημα $S+$ και ένα αντίγραφο αυτού συμβολίζονται με $K_{S+}$ και ${K'}_{S+}$, αντίστοιχα. Συμβολίζουμε με $s' \in V({K'}_{S+})$ το αντίγραφο του κόμβου $s \in S+$. Κατασκευάζουμε ένα γράφημα $G_{SSP}$ (Σχήμα 3.3) με σύνολο κόμβων $V(G_{SSP}) = V(K_{S+}) \cup V({K'}_{S+}) \cup X$ και σύνολο ακμών

$$E(G_{SSP}) = E(K_{S+}) \cup E({K'}_{S+}) \cup \{(v, s), (v, s') : v \in X, s \in S+, v \in s\}$$

όπου ο κόμβος $s'$ είναι αντίγραφο του $s$ όπως προαναφέρθηκε.

Στη συνέχεια αποδεικνύουμε ότι υπάρχει μια ζητούμενη διαμέριση του $X$ αν και μόνον αν υπάρχει ένας 2-plp διαχωριστής $C$ στο $G_{SSP}$.

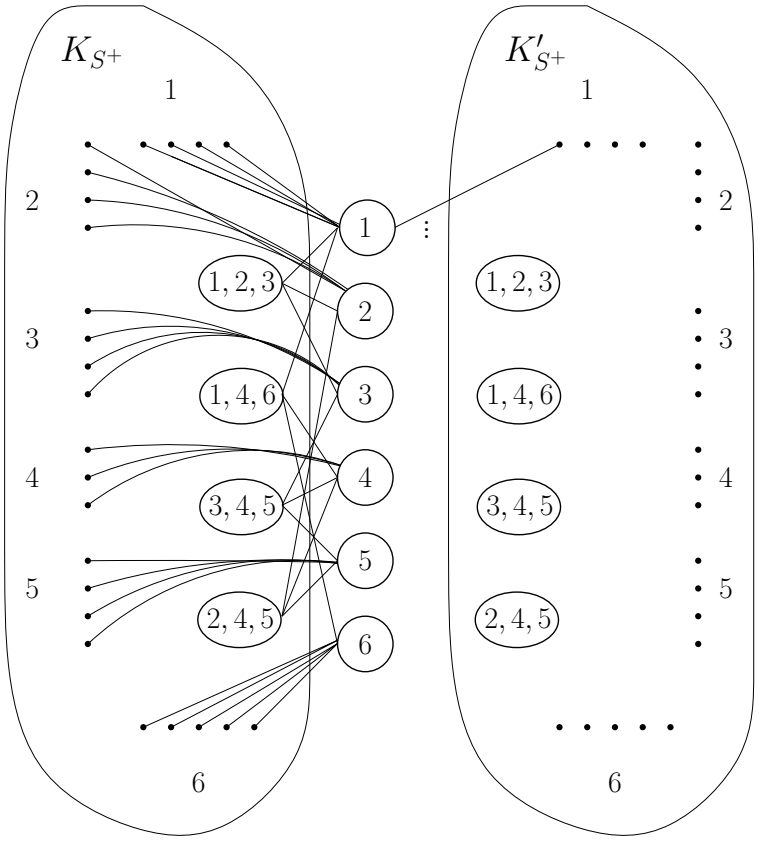
Για την κατεύθυνση "⇒"αρκεί να παρατηρήσουμε ότι μία διαμέριση $X = X_1 \cup X_2$ για την οποία κανένα σύνολο του $S$ δεν περιέχεται εξολοκλήρου σε κανένα από τα $X_1$, $X_2$, υπονοεί ότι καθένα από τα σύνολα $X_1, X_2$ θα περιέχει το πολύ δύο κόμβους (στοιχεία) τα οποία εμφανίζονται στη γειτονιά του κάθε κόμβου (συνόλου) στο $K_{S+}$ και στο ${K'}_{S+}$ και επομένως το σύνολο $X = X_1 \cup X_2$ είναι ένας 2-plp διαχωριστής.

Για την κατεύθυνση "⇐" εργαζόμαστε ως εξής. Θεωρώντας έναν 2-plp διαχωριστή $C$ στο $G_{SSP}$ διακρίνουμε δύο περιπτώσεις, την περίπτωση $X \setminus C \neq \emptyset$ και την περίπτωση $X \setminus C = \emptyset$. Στην πρώτη περίπτωση, παρατηρούμε πως αν το υπογράφημα του $G_{SSP}$ που προκύπτει από την αφαίρεση του $C$ από το $G_{SSP}$ αποτελείται από τουλάχιστον δύο συνδεδεμένα συστατικά, τότε το $C$ πρέπει να περιέχει το σύνολο $\mathcal{N}(v) \cap V(K_{S+})$ ή το σύνολο $\mathcal{N}(v) \cap V({K'}_{S+})$ για καθένα $v \in X \setminus C$. Αφού κάθε $v \in X$ έχει τουλάχιστον 6 γείτονες σε κάθε υπογράφημα $V(K_{S+})$ και $V({K'}_{S+})$, για κάθε διαμέριση του $C$, είτε κάθε κόμβος στο $V(K_{S+}) \setminus C$ ή κάθε κόμβος στο $V({K'}_{S+}) \setminus C$ έχει τουλάχιστον 3 γείτονες σε κάποιο κομμάτι της διαμέρισης. Επομένως, αφού το $C$ είναι ένας 2-plp διαχωριστής η περίπτωση $X \setminus C \neq \emptyset$ δεν μπορεί να ισχύει.

Απομένει να εξετάσουμε την περίπτωση ύπαρξης ενός ενός 2-plp διαχωριστή $C = C_1 \cup C_2$ όπου $X \setminus C = \emptyset$, το οποίο συνεπάγεται ότι $X \subseteq C$; σημειώνουμε ότι τα $C_1, C_2$ είναι τελικά 2-τοπικά λόγω συμμετρίας. Παρατηρούμε ότι το $X$ αποτελεί επίσης ένα διαχωριστή του $G_{SSP}$; επίσης, σε αυτήν την περίπτωση, και τα δύο σύνολα $X_i = C_i \cap X, i = 1, 2$, είναι 2-τοπικά (ως υποσύνολα των 2-τοπικών συνόλων $C_i, i = 1, 2$), επομένως το $X = X_1 \cup X_2$ είναι ένας 2-plp διαχωριστής. Συνεπώς, κανένα σύνολο $s \in S$ μπορεί να περιέχεται εξολοκλήρου σε κάποιο από τα $X_i, i = 1, 2$, επειδή $|s| = 3$, ως εκ τούτου ο αντίστοιχος κόμβος $s$ στο $K_{S+}$ (και ο $s'$ στο ${K'}_{S+}$) θα είχε 3 γείτονες στο $X_i$ δημιουργώντας αντίφαση με το γεγονός ότι το $X_i$ είναι 2-τοπικό σύνολο. Επομένως το πρόβλημα διαχωρισμού συνόλων $(S, X)$ έχει την λύση $X = X_1 \cup X_2$.

Ολοκληρώνουμε την απόδειξη δείχνοντας ότι η NP-δυσκολία του $pLPC(G, t)$ χωρίς διανομέα (γενική περίπτωση) συνεπάγεται την NP-δυσκολία στην περίπτωση που έχουμε συγκεκριμένο διανομέα $D$, δηλαδή, τη δυσκολία του προβλήματος $pLPC(G, t, D)$. Πράγματι, εάν

υπήρχε αλγόριθμος πολυωνυμικού χρόνου για το $pLPC(G, t, D)$ τότε λύνοντας το $pLPC(G, t, v)$ για κάθε κόμβο-διανομέα $v \in V$ θα αρκούσε για να κατασκευάσουμε έναν πολυωνυμικό αλγόριθμο για το $pLPC(G, t)$. Επομένως ο υπολογισμός του $pLPC(G, t, D)$ είναι NP-δύσκολος. □




Σχήμα 3.3: Το γράφημα $G_{SSP}$ για το πρόβλημα διαχωρισμού συνόλων που παρουσιάζεται στο Σχήμα 3.2. Οι ακμές στην δεξιά πλευρά είναι συμμετρικές με αυτές στην αριστερή και παραλείπονται για λόγους απλότητας.

Το προηγούμενο θεώρημα μας δείχνει ότι ο υπολογισμός τις αναγκαίας και ικανής συνθήκης για να πετύχει τον στόχο του ο CPA είναι NP-δύσκολο. Παρατηρούμε ότι αυτό το αρνητικό αποτέλεσμα έχει όμως και μια θετική χροιά, συγκεκριμένα υπονοεί ότι ένας αντίπαλος που είναι περιορισμένος σε υπολογισμούς πολυωνυμικού χρόνου δεν μπορεί να υπολογίσει πάντα μια βέλτιστη επίθεση εκτός και αν P = NP.

## 3.4 Δίκτυα γνωστής τοπολογίας

### 3.4.1 Ο Αλγόριθμος διάδοσης μονοπατιών

Θεωρώντας μόνο ασφαλείς αλγορίθμους Εκπομπής, η μοναδικότητα του CPA στο *ad hoc* μοντέλο υπονοεί ότι κάποιος αλγόριθμος που πετυχαίνει Εκπομπή σε περιπτώσεις που ο CPA δεν το κάνει, πρέπει να λειτουργεί σε ένα ασθενέστερο μοντέλο π.χ., να υποθέτει επιπλέον πληροφορία για την τοπολογία του δικτύου. Είναι επομένως λογικό να εξετάσουμε το μοντέλο όπου οι παίκτες έχουν πλήρη γνώση της τοπολογίας του δικτύου. Σε αυτήν την ενότητα προτείνουμε τον *Αλγόριθμο διάδοσης μονοπατιών* (Path Propagation Algorithm - PPA) και δείχνουμε ότι είναι βέλτιστης ανεκτικότητας στο μοντέλο πλήρους γνώσης. Για λόγους ευκολίας θα χρησιμοποιήσουμε τις ακόλουθες έννοιες:

***Ορισμός* 3.5** (Κάλυμμα μονοπατιών). *Ένα σύνολο $S \subseteq V \setminus D$ θα ονομάζεται* κάλυμμα *ενός συνόλου μονοπατιών $\mathcal{P}$ αν και μόνον αν $\forall p \in \mathcal{P},\ \exists s \in S$ τ.ώ. $s \in p$ (ο $s$ είναι κόμβος του $p$).*

Όπως μπορεί κανείς να δει στον αλγόριθμο, κάθε μονοπάτι που διαδίδεται, μεταδίδεται μαζί με μια τιμή που διαδίδει. Η τιμή αυτή αντιστοιχεί στην τιμή που είχε αρχικά αποσταλεί από τον πρώτο κόμβο του μονοπατιού (*πηγή* του μονοπατιού). Το άλλο τελικό σημείο του μονοπατιού, δηλαδή, ο τελευταίος κόμβος του μονοπατιού $p$ θα συμβολίζεται με τον όρο $tail(p)$. Όταν ένας κόμβος $v$ λειτουργεί ως αναμεταδότης της τιμής που έχει φτάσει σε αυτόν μέσω του μονοπατιού $p$, προσαρτά το αναγνωριστικό του $v$ στον τελευταίο κόμβο του $p$ και έτσι δημιουργεί ένα νέο μονοπάτι $p'$ με $tail(p') = v$, ενώ η πηγή των $p$ και $p'$ παραμένει η ίδια. Η περιγραφή του PPA ακολουθεί.

---

**Πρωτόκολλο 3**: ***Αλγόριθμος διάδοσης μονοπατιών (PPA)***

---

*Είσοδος* (γιια κάθε κόμβο $v$): αναγνωριστικό $D$ του διανομέα, γράφημα $G$, $t(v) =$ μέγιστος αριθμός διαφθορών στο $\mathcal{N}(v)$.
*Μορφή μηνύματος*: ζεύγος $(x, p)$, όπου $x \in X$ (χώρος μηνυμάτων), και το $p$ είναι ένα μονοπάτι του $G$ (μονοπάτι διάδοσης μηνύματος).

**Κώδικας του** $D$: στείλε το μήνυμα $(x_D, D)$ σε όλους τους γείτονες, αποφάσισε στο $x_D$ και τερμάτισε.

**Κώδικας του** $v \neq D$: Αρχικοποίηση $decision_v := \perp$.
κατά την παραλαβή του $(x, p)$ από τον κόμβο $u$ κάνε:

αν $(v \in p) \vee (tail(p) \neq u)$ τότε απέριψε το μήνυμα αλλιώς στείλε $(x, p||v)$ [1] σε

όλους του γείτονες.

αν $(decision_v = \perp) \wedge (\text{decision}(v) \neq \perp)$ τότε

[1] Με το $p||v$ συμβολίζουμε το μονοπάτι που αποτελείται από το μονοπάτι $p$ και τον κόμβο $v$, με τον τελευταίο κόμβο του $p$ συνδεδεμένο με τον $v$.

$decision_v :=$ decision$(v)$;
στείλε το μήνυμα $(decision_v, v)$ σε όλους τους γείτονες;
αποφάσισε στο $decision_v$.

**Συνάρτηση decision**$(v)$

(* *κανόνας διάδοσης διανομέα* *)
αν $v \in \mathcal{N}(D)$ και ο $v$ λαμβάνει $(x_D, D)$ τότε επέστρεψε $x_D$.
(* *κανόνας διάδοσης έντιμου μονοπατιού* *)
αν ο $v$ λαμβάνει τα μηνύματα $(x, p_1), \ldots, (x, p_m)$ και $\exists\, \mathcal{P} \subseteq \{p_1, \ldots, p_m\}$ που δεν έχει $t$-τοπικό κάλυμμα.
τότε επέστρεψε $x$ αλλιώς επέστρεψε $\perp$.

---

Όσον αφορά τον κανόνα διάδοσης έντιμου μονοπατιού του PPA, σημειώνεται ότι το $\mathcal{P}$, δεν είναι ολόκληρο το σύνολο από τα μονοπάτια που έχει συλλέξει ο $v$ αλλά οποιοδήποτε σύνολο από μονοπάτια μέσω των οποίων ο $v$ λαμβάνει την τιμή $x$. Επίσης παρατηρούμε ότι το κριτήριο είναι υπαρξιακό, και επομένως η ύπαρξη ενός συνόλου $\mathcal{P}$ με την επιθυμητή ιδιότητα αρκεί για να αποφασίσει ο παίκτης στην αντίστοιχη τιμή. Βλέπουμε ότι κάθε παίκτης μπορεί να ελέγξει την εγκυρότητα του κανόνα διάδοσης έντιμου μονοπατιού μόνο αν έχει γνώση της συνάρτησης διαφθοράς $t$ και της τοπολογίας του δικτύου. Στη συνέχεια μελετάμε την ασφάλεια του PPA.

***Θεώρημα* 3.5**. *Ο PPA είναι $t$-τοπικά ασφαλής.*

*Απόδειξη.*
Θα δείξουμε ότι αν ένας παίκτης αποφασίσει στην τιμή $x$ μέσω του PPA, τότε $x = x_D$. Υποθέτουμε προς άτοπο ότι υπάρχει ένα σύνολο παικτών $V' \subseteq V$ που αποφασίζει σε τιμές διαφορετικές του $x_D$. Έστω $v$ ο παίκτης του $V'$ που αποφασίζει στον μικρότερο γύρο μεταξύ όλων των παικτών του $V'$, δηλαδή, ο πρώτος παίκτης που παίρνει μια λανθασμένη απόφαση, και υποθέτουμε ότι ο $v$ αποφασίζει στην τιμή $x \neq x_D$. Ο παίκτης $v$ δεν πορεί να είναι γείτονας του διανομέα αφού όλοι οι γείτονες του διανομέα αποφασίζουν στην τιμή $x_D$ όπως φαίνεται από τον αντίστοιχο κανόνα απόφασης του PPA. Επομένως ο $v$ έχει αποφασίσει στη τιμή $x$ μέσω του κανόνα διάδοσης έντιμου μονοπατιού. Αυτό σημαίνει ότι ο $v$ έλαβε την τιμή $x$ από ένα σύνολο μονοπατιών $\mathcal{P}$ τέτοιο ώστε δεν υπάρχει ένα $t$-τοπικό κάλυμμα του $\mathcal{P}$. Επιπλέον, μέσω του ελέγχου $tail(p) \neq u$, εξασφαλίζουμε ότι τουλάχιστον ένας διεφθαρμένος κόμβος θα συμπεριληφθεί σε ένα μονοπάτι που περιέχει διεφθαρμένους κόμβους. Λόγω του τελευταίου, αποφεύγουμε την περίπτωση όπου όλοι οι διεφθαρμένοι κόμβοι κρύβουν το αναγνωριστικό τους σε ένα μονοπάτι αλλάζοντας το πραγματικό μονοπάτι διάδοσης; αυτή είναι μια ιδέα που χρησιμοποιείται συχνά στη σχετική βιβλιογραφία ακι παρουσιάστηκε πρώτη φορά στο [Dol82].

Αφού δεν υπάρχει ένα $t$-τοπικό κάλυμμα του $\mathcal{P}$, είναι τώρα προφανές ότι τουλάχιστον ένα μονοπάτι $p$ του $\mathcal{P}$ αποτελείται μόνο από τίμιους κόμβους και επομένως η τιμή $x$, η οποία

διαδίδεται μέσω του $p$, είναι η πραγματική τιμή στην οποία ο κόμβος-πηγή $w$ του $p$ έχει αποφασίσει. Συνεπώς, τουλάχιστον ένας τίμιος παίκτης έχει αποφασίσει στην τιμή$x \neq x_D$ πριν από τον $v$. Αυτό όμως αντιφάσκει στο γεγονός ότι ο $v$ είναι ο πρώτος παίκτης που έλαβε μια λανθασμένη απόφαση.

□

### 3.4.2 Μια ικανή και αναγκαία συνθήκη

Θα δείξουμε τώρα ότι η μη ύπαρξη $t$-τοπικού διαχωριστή ζεύγους είναι μια ικανή συνθήκη για την επίτευξη Εκπομπής από τον PPA σε δίκτυα άγνωστης τοπολογίας υπό το μοντέλο $t$-τοπικά φραγμένου αντιπάλου.

***Θεώρημα* 3.6** (ικανή συνθήκη). *Δοθέντος ενός γραφήματος $G$ με διανομέα $D$ και μια συνάρτηση διαφθοράς $t$, εάν δεν υπάρχει $t$-τοπικός διαχωριστής ζεύγους στο $(G, D)$ τότε όλοι οι τίμιοι παίκτες θα αποφασίσουν στην σωστή τιμή $x_D$ μέσω του PPA.*

*Απόδειξη.*

Όλοι οι παίκτες στο $\mathcal{N}(D)$ αποφασίζουν στο $x_D$ λόγω του *κανόνα διάδοσης διανομέα*, επειδή ο διανομέας είναι τίμιος. Στη συνέχεια δείχνουμε ότι όλοι οι τίμιοι παίκτες θα αποφασίσουν στο $x_D$ λόγω του *κανόνα διάδοσης έντιμου μονοπατιού*. Παρατηρούμε ότι αφού ο PPA είναι $t$-τοπικά ασφαλής, αρκεί να δείξουμε ότι, σε κάποιον γύρο,κάθε παίκτης θα λάβει τη σωστή τιμή $x_D$ μέσω ενός συνόλου μονοπατιών $\mathcal{P}$ το οποίο θα του επιτρέψει να αποφασίσει στο $x_D$ μέσω του κανόνα διάδοσης έντιμου μονοπατιού (αν δεν έχει ήδη αποφασίσει σε αυτή την τιμή σε κάποιο προηγούμενο γύρο).

Έστω ο $v$ οποιοσδήποτε παίκτης στο $V \setminus \mathcal{N}(D)$μ υποθέτουμε ότι δεν υπάρχει $t$-τοπικός διαχωριστής στο $(G, D)$. Έστω $T$ ένα $t$-τοπικό σύνολο και θεωρούμε οποιαδήποτε εκτέλεση $\sigma_T$ του PPA όπου το $T$ είναι ο πραγματικό σύνολο των διεφθαρμένων παικτών. Έστω $\mathcal{P}_{D,v}$ το σύνολο όλων των μονοπατιών που συνδέουν τον $D$ με τον $v$ και αποτελούνται εξ ολοκλήρου από κόμβους στο $V \setminus T$ (τίμιους κόμβους). Παρατηρούμε ότι ισχύει $\mathcal{P}_{D,v} \neq \emptyset$, αλλιώς το $T$ είναι ένας διαχωριστής που χωρίζει τον $D$ από τον $v$ και τότε ο $T$ είναι τετριμμένα ένας $t$-τοπικός διαχωριστής ζεύγους, άτοπο λόγω της υπόθεσης μη ύπαρξης $t$-τοπικού διαχωριστή ζεύγους. Εφόσον τα μονοπάτια στο $\mathcal{P}_{D,v}$ αποτελούνται εξ ολοκλήρου από τίμιους κόμβους, είναι εύκολο να δούμε ότι ο $v$ θα λάβει τη σωστή τιμή $x_D$ μέσω όλων των μονοπατιών στο $\mathcal{P}_{D,v}$. Αφού το $\mathcal{P}_{D,v}$ είναι ένα σύνολο μονοπατιών που διαδίδουν την ίδια τιμή στον $v$, ο παίκτης $v$ θα ελέγξει αν υπάρχει ένα $t$-τοπικό κάλυμμα γιαυτό, όπως υπαγορεύεται από τον κανόνα διάδοσης έντιμου μονοπατιού, δηλαδή, το $\mathcal{P}_{D,v}$ θα ταυτιστεί με το $\mathcal{P}$ όπως αυτό φαίνεται στον αλγόριθμο.

Στη συνέχεια δείχνουμε ότι δεν υπάρχει $t$-τοπικό κάλυμμα του $\mathcal{P}_{D,v}$. Έστω ότι $\exists T' : t$-τοπικό κάλυμμα του $\mathcal{P}_{D,v}$. Τότε προφανώς $T \cup T'$ είναι ένας διαχωριστής που χωρίζει τον $D$ από τον $v$, αφού κάθε μονοπάτι που συνδέει τον $D$ με τον $v$ περιέχει τουλάχιστον έναν κόμβο

στο $T \cup T'$. Επιπλέον ο διαχωριστής $T \cup T'$ μπορεί να διαμεριστεί σε δύο σύνολα $T \setminus T', T'$ τα οποία είναι τετριμμένα $t$-τοπικά και επομένως , $T \cup T'$ είναι ένας $t$-τοπικός διαχωριστής ζεύγους, άτοπο. Επομένως δεν υπάρχει $t$-τοπικό κάλυμμα του $\mathcal{P}_{D,v}$.

Συνεπώς, στην εκτέλεση $\sigma_T$, ο κόμβος $v$ θα λάβει την σωστή τιμή, σε κάποιο γύρο $k$, μέσω κάθε μονοπατιού στο $\mathcal{P}_{D,v}$ μαζί με το αντίστοιχο μονοπάτι διάδοσης. Εάν ο παίκτης $v$ έχει ήδη αποφασίσει μέχρι τον γύρο $k$ τότε θα έχει αποφασίσει σίγουρα στην τιμή $x_D$ λόγω της $t$-τοπικής ασφάλειας του PPA. Σε κάθε άλλη περίπτωση, ο $v$ θα αποφασίσει επίσης στην σωστή τιμή $x_D$ μέχρι το τέλος του γύρου $k$ λόγω του κανόνα διάδοσης έντιμου μονοπατιού, επειδή το σύνολο μονοπατιών $\mathcal{P}_{D,v}$ δεν καλύπτεται από κανένα $t$-τοπικό σύνολο.

□

Χρησιμοποιώντας τα ίδια επιχειρήματα όπως στην απόδειξη της αναγκαιότητας της συνθήκης $t < LPC(G, D)$ [PP05] μπορούμε να δείξουμε ότι η μη ύπαρξη ενός $t$-τοπικού διαχωριστή ζεύγους είναι μια αναγκαία συνθήκη για να πετύχει Εκπομπή οποιοσδήποτε αλγόριθμος στο μη ομοιόμορφο μοντέλο. Η απόδειξη χρησιμοποιεί παρόμοια επιχειρήματα με αυτά της απόδειξης του Θεωρήματος 3.2 αλλά είναι πολύ απλούστερη· η διαφορά είναι οι διαφορετικές εκτελέσεις του αλγορίθμου θεωρούνται στο ίδιο γράφημα. Στην προκειμένη περίπτωση δεν μπορούμε να θεωρήσουμε εκτελέσεις του αλγορίθμου σε διαφορετικά γραφήματα αφού η τοπολογία είναι γνωστή σε όλους τους παίκτες και επομένως οι παίκτες θα ήταν σε θέση να διακρίνουν τα δύο αυτά σενάρια. Η αναγκαιότητα της συνθήκης εκφράζεται με το παρακάτω Θεώρημα. Η απόδειξη παραλείπεται ως πανομοιότυπη με την αντίστοιχη του [PP05].

***Θεώρημα* 3.7** (Αναγκαιότητα της συνθήκης). *Δοθέντος ενός γραφήματος $G$ με διανομέα $D$ και μια συνάρτηση διαφθοράς $t$, αν υπάρχει ένας $t$-τοπικός διαχωριστής ζεύγους στο $(G, D)$ τότε δεν υπάρχει κανένας $t$-τοπικά ανεκτικός αλγόριθμος για το $(G, D)$.*

Επομένως η μη ύπαρξη ενός $t$-τοπικού διαχωριστή ζεύγους αποδεικνύεται ικανή και αναγκαία συνθήκη για την ύπαρξη ενός $t$-τοπικά ανεκτικού αλγορίθμου στο ομοιόμορφο και στο μη ομοιόμορφο μοντέλο. Ως εκ τούτου, προκύπτει η βέλτιστη ανεκτικότητα του PPA.

## 3.5 Το μοντέλο μερικής γνώσης

Έως τώρα έχουμε παρουσιάσει αλγορίθμους Εκπομπής βέλτιστης ανεκτικότητας για τις δύο ακραίες περιπτώσεις τοπολογικής γνώσης: το *ad hoc* μοντέλο και το μοντέλο πλήρους γνώσης. Προκύπτει επομένως μια φυσιολογική ερώτηση: υπάρχει κάποιος αλγόριθμος Εκπομπής που να πετυχαίνει βέλτιστη ανεκτικότητα σε ένα πλαίσιο όπου οι κόμβοι έχουν μερική γνώση της τοπολογίας;

Για να απαντήσουμε σε αυτήν την ερώτηση εισάγουμε το *μοντέλο μερικής γνώσης*, όπου κάθε παίκτης έχει περιορισμένη γνώση επί της τοπολογίας του δικτύου και σχεδιάζουμε έναν νέο αλγόριθμο, που αποτελεί ουσιαστικά γενίκευση του PPA και απαιτεί μόνο μερική γνώση της

τοπολογίας του δικτύου από τους παίκτες. Πιο συγκεκριμένα, όπως εξηγήσαμε στην Ενότητα 3.2.1 υποθέτουμε ότι κάθε παίκτης $v$ έχει γνώση της τοπολογίας μόνο ενός συγκεκριμένου υπογραφήματος $G_v$ του $G$, το οποίο περιλαμβάνει και τον ίδιο. Όπως ορίστηκε προηγουμένως, η ανάθεση αρχικής τοπολογικής γνώσης σε όλους τους παίκτες μοντελοποιείται από την *συνάρτηση γνώσης* $\gamma$ όπου $\gamma(v)$ αναπαριστά το υπογράφημα, την τοπολογία του οποίου γνωρίζει ο παίκτης $v$. Θα χρησιμοποιήσουμε επίσης την *από κοινού γνώση* $\gamma(S)$ ενός συνόλου παικτών $S$, η οποία επίσης ορίστηκε στην Ενότητα 3.2.1 και αναπαριστά το γράφημα που προκύπτει αν όλοι οι κόμβοι στο $S$ συνδυάσουν την τοπολογική τους γνώση. Ένας αλγόριθμος που πετυχαίνει Εκπομπή για οποιοδήποτε $t$-τοπικό σύνολο διαφθορών στο γράφημα $G$ με διανομέα $D$ και συνάρτηση γνώσης $\gamma$, θα καλείται $(\gamma, t)$-*τοπικά ανεκτικό* για το $(G, D)$.

**Ο αλγόριθμος GPPA**. Έστω μια συνάρτηση διαφθοράς $t$ και μια συνάρτηση γνώσης $\gamma$· ορίζουμε τον *Γενικευμένο Αλγόριθμο Διάδοσης Μονοπατιών* (Generalized Path Propagation Algorithm - GPPA) να λειτουργέι ακριβώς όπως ο PPA εκτός από μια φυσιολογική τροποποίηση του *κανόνα διάδοσης έντιμου μονοπατιού*. Ο τροποποιημένος αυτός κανόνας απόφασης θα καλείται *γενικευμένος κανόνας διάδοσης μονοπατιού* και παρουσιάζεται παρακάτω.

**Γενικευμένος κανόνας διάδοσης μονοπατιού**. Ο παίκτης $v$ λαμβάνει την ίδια τιμή $x$ από ένα σύνολο μονοπατιών $\mathcal{P}$ τα οποία περιέχονται εξολοκλήρου στο υπογράφημα $\gamma(v)$ και είναι σε θέση να συμπεράνει (από τη γνωστή του τοπολογία) ότι δεν υπάρχει $t$-τοπικό κάλυμμα του $\mathcal{P}$.

**Παρατήρηση**. Όπως είναι φανερό, ο GPPA γενικεύει και τους δύο αλγορίθμους CPA και PPA. Πράγματι, αν $\forall v \in V$, $\gamma(v) = \mathcal{N}(v)$, τότε ο GPPA στο στιγμιότυπο $(G, D, t, \gamma)$ συμπίπτει με τον CPA στο στιγμιότυπο $(G, D, t)$. Από την άλλη, αν, $\forall v \in V$, $\gamma(v) = G$ τότε ο GPPA στο $(G, D, t, \gamma)$ συμπίπτει με τον PPA στο $(G, D, t)$.

Σημειώνουμε επίσης ότι, φυσιολογικά, όσο η συνάρτηση $\gamma$ παρέχει περισσότερη πληροφορία για την τοπολογία του δικτύου, η ανεκτικότητα αυξάνεται, με τον CPA να είναι ελάχιστης ανεκτικότητας σε αυτήν την οικογένεια αλγορίθμων, και τον PPA να πετυχαίνει μέγιστη ανεκτικότητα.

Για να δείξουμε ικανές και αναγκαίες συνθήκες έτσι ώστε ο GPPA να είναι $t$-τοπικά ανεκτικός χρειάζεται να γενικεύσουμε την έννοια του of $t$-plp διαχωριστή όπως φαίνεται παρακάτω:

***Ορισμός* 3.6** ($(\gamma, t)$-plp διαχωριστής τύπου 1). *Έστω $C$ ένας διαχωριστής του $G$, που διαμερίζει το $V \setminus C$ σε δύο σύνολα $A, B \neq \emptyset$ τέτοια ώστε, $D \in A$. Το $C$ θα καλείται* $(\gamma, t)$-plp διαχωριστής τύπου 1 (plp1 διαχωριστής) *αν υπάρχει μαι διαμέριση $C = C_1 \cup C_2$ τέτοια ώστε το $C_1$ είναι $t$-τοπικό και το $C_2 \cap \gamma(B)$ είναι $t$-τοπικό στο γράφημα$\gamma(B)$.*

***Ορισμός* 3.7** ($(\gamma, t)$-plp διαχωριστής τύπου 2). *Έστω $C$ ένας διαχωριστής του $G$, που διαμερίζει το $V \setminus C$ σε δύο σύνολα $A, B \neq \emptyset$ τέτοια ώστε, $D \in A$.Το $C$ θα καλείται* $(\gamma, t)$-plp διαχωριστής τύπου ($t$-plp2 διαχωριστής) *αν υπάρχει μια διαμέριση $C = C_1 \cup C_2$ τέτοια ώστε $C_1$ είναι $t$-τοπικό και $\forall u \in B$, $C_2 \cap \mathcal{N}(u)$ είναι $t$-τοπικό στο γράφημα $\gamma(u)$.*

Μπορούμε τώρα αν αποδείξουμε τα δύο παρακάτω θεωρήματα. Οι αποδείξεις στηρίζονται στις τεχνικές που αναπτύχθηκαν για τους αλγορίθμους CPA και PPA.

***Θεώρημα* 3.8** (Ικανή συνθήκη). *Έστω $t$ μια συνάρτηση διαφθοράς και $\gamma$ μια συνάρτηση γνώσης, αν δεν υπάρχει $(\gamma, t)$-plp2 διαχωριστής στο $G$ με διανομέα $D$ τότε ο $GPPA(G, D, t, \gamma)$ είναι $(\gamma, t)$-τοπικά ανεκτικός για το $(G, D)$.*

*Απόδειξη.*
Υποθέτουμε ότι δεν υπάρχει $(\gamma, t)$-plp2 διαχωριστής. Έστω μια εκτέλεση του GPPA όπου το πραγματικό σύνολο διαφθοράς είναι το $T$. Εξ ορισμού, το $T$ είναι $t$-τοπικό, αφού εργαζόμαστε στο μοντέλο $t$-τοπικά φραγμένου αντιπάλου· προφανώς το $T \cup \mathcal{N}(D)$ είναι ένας διαχωριστής στο $G$ όπως αυτός ορίστηκε προηγουμένος (δηλαδή, χωρίς να περιέχει τον $D$). Εφόσον το $T$ είναι $t$-τοπικό και το $T \cup \mathcal{N}(D)$ δεν είναι $(\gamma, t)$-plp2 διαχωριστής πρέπει να υπάρχει ένας κόμβος $u_1 \in V \setminus (T \cup \mathcal{N}(D) \cup D)$ τέτοιος ώστε το $\mathcal{N}(D) \cap \mathcal{N}(u_1)$ δεν είναι $t$-τοπικό στο $\gamma(u_1)$. Αλλά αφού όλοι οι τίμιοι κόμβοι στο $\mathcal{N}(D) \cap \mathcal{N}(u_1)$ έχουν αποφασίσει σωστά σαν γείτονες του διανομέα, ο $u_1$ θα λάβει την τιμή $x_D$ από μονοπάτια μήκους 1, που ξεκινάνε από αυτούς τους κόμβους. Η εύρεση ενός $t$-τοπικού συνόλου διαφθορών που καλύπτει αυτό το σύνολο μονοπατιών είναι αδύνατη αφού θα έπρεπε να περιέχει όλους αυτούς τους κόμβους, και από τα παραπάνω, δεν θα ήταν $t$-τοπικό. Συνεπώς, ο $u_1$ θα αποφασίσει στην τιμή του διανομέα $x_D$. Μπορούμε να χρησιμοποιήσουμε το ίδιο επιχείρημα επαγωγικά για να δείξουμε ότι κάθε τίμιος κόμβος θα αποφασίσει τελικά στην σωστή τιμή $x_D$ μέσω του GPPA. Έστω $C_k = (\mathcal{N}(D) \setminus T) \cup \{u_1, u_2, ..., u_{k-1}\}$ το σύνολο των κόμβων που έχουν αποφασίσει μέχρι ένα συγκεκριμένο γύρο του πρωτοκόλλου και υποθέτουμε ότι έχουν αποφασίσει ορθά στο $x_D$. Τότε, το $C_k \cup T$ είναι ένας διαχωριστής. Εφόσον το $T$ είναι $t$-τοπικό επιχειρηματολογώντας όπως και πριν, βλέπουμε ότι υπάρχει ένας κόμβος που δεν έχει αποφασίσει $u_k$ τέτοιος ώστε $C_k \cap \mathcal{N}(u_k)$ δεν είναι $t$-τοπικό στο $\gamma(u_k)$. Χρησιμοποιώντας το ίδιο επιχείρημα όπως πριν, δείχνουμε ότι ο $u_k$ θα αποφασίσει στην σωστή τιμή. Τελικά όλοι οι τίμιοι παίκτες θα αποφασίσουν στην τιμή $x_D$. Συνεπώς, ο $GPPA$ είναι $t$-τοπικά ανεκτικός στο $(G, D)$. □

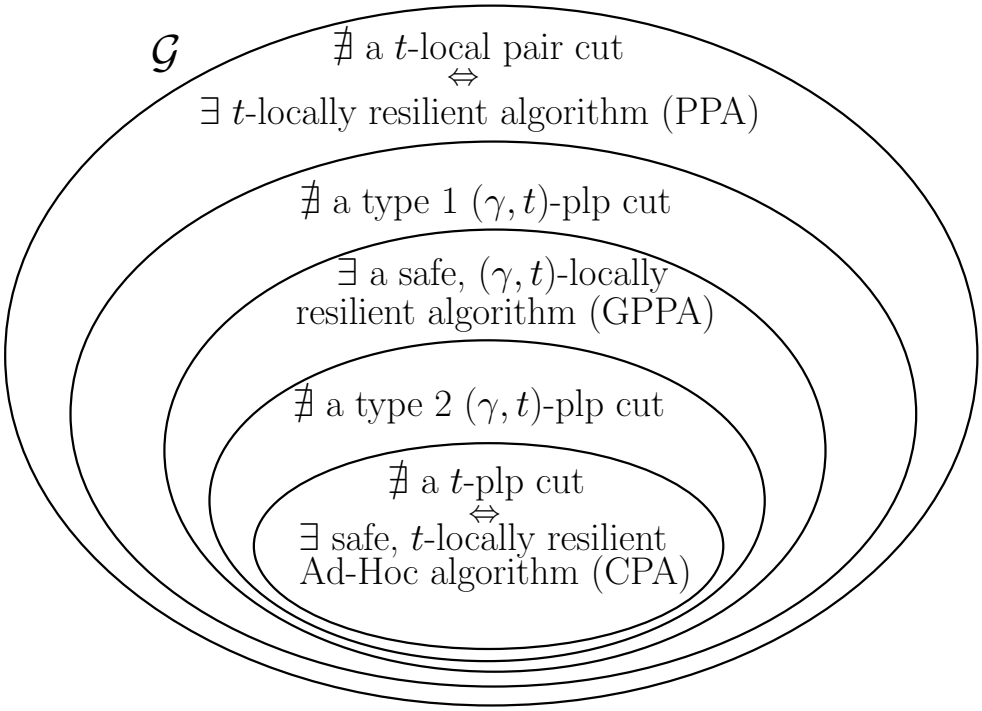
Όμοια με την απόδειξη του Θεωρήματος 3.1, παρατηρούμε ότι και σε αυτήν την απόδειξη δεν χρησιμοποιούμε το γεγονός ότι ο GPPA είναι ασφαλής αλλά αντί αυτού αποδεικνύουμε επαγωγικά ότι στην περίπτωση που μελετάμε, όλοι οι κόμβοι θα αποφασίσουν ορθά.

***Θεώρημα* 3.9** (Αναγκαία συνθήκη). *Έστω $t$ μια συνάρτηση διαφθοράς και $\gamma$ μια συνάρτηση γνώσης και $\mathcal{A}$ ένας $t$-τοπικά ασφαλής αλγόριθμος Εκπομπής. Αν υπάρχει ένας $(\gamma, t)$-plp1 διαχωριστής στο γράφημα $G$ με διανομέα $D$, τότε ο $\mathcal{A}$ δεν είναι $(\gamma, t)$-τοπικά ανεκτικός για το $(G, D)$.*

*Απόδειξη.*
Υποθέτουμε ότι υπάρχει ένας $(\gamma, t)$-plp1 διαχωριστής $C = T \cup H$ στο γράφημα $G$ με διανομέα $D$ και το $T$ είναι το $t$-τοπικό σύνολο της διαμέρισης του $C$ (Figure 3.1). Το υπογράφημα $\gamma(B)$ είναι η από κοινού γνώση των κόμβων στο $B$. Έστω, $G'$ το γράφημα που προκύπτει από το $G$ αν αφαιρέσουμε ακμές από το $A \setminus \gamma(B)$ έτσι ώστε το σύνολο $H$ γίνεται $t$-τοπικό στο $G'$. Η ύπαρξη ενός συνόλου ακμών, από την αφαίρεση των οποίων προκύπτει το παραπάνω, υπονοείται από την δεύτερη ιδιότητα του $(\gamma, t)$-plp1 διαχωριστή. Υποθέτουμε ότι υπάρχει ένας

$t$-τοπικά ασφαλής αλγόριθμος Εκπομπής $\mathcal{A}$ ο οποίος είναι $t$-τοπικά ανεκτικός στο γράφημα $G$ με διανομέα $D$. Μπορούμε πλέον να επιχειρηματολογήσουμε με τον ίδιο τρόπο όπως στο Θεώρημα 3.2 και να καταλήξουμε σε άτοπο. □

Μπορούμε να παρατηρήσουμε ότι η αθξημένη τοπολογική γνώση υπονοεί αυξημένη ανεκτικότητα του GPPA συγκριτικά με τον CPA· για παράδειγμα, η ικανή συνθήκη του GPPA ισχύει και σε περιπτώσεις όπου η ικανή συνθήκη του CPA δεν ισχύει. Μία επισκόπηση των αποτελεσμάτων μας σχετικά με το μοντέλο $t$-τοπικά φραγμένου αντιπάλου ώς προς το επίπεδο της τοπολογικής γνώσης παρουσιάζεται στο Σχήμα 3.4.




Σχήμα 3.4: Επισκόπηση των συνθηκών που αφορούν την ύπαρξη $t$-τοπικά ανεκτικών αλγορίθμων Εκπομπής ως προς το επίπεδο της τοπολογικής γνώσης. Σημειώνεται ότι το $\mathcal{G}$ αναφέρεται στην οικογένεια ζευγών $(G, D)$.

Παρατηρούμε ότι ο λόγος για τον οποίο ο GPPA δεν είναι αλγόριθμος βέλτιστης ανεκτικότητας, είναι ότι ότι οι κόμβοι στο $\gamma(v)$ δεν μοιράζονται την γνώση της τοπολογίας που κατέχουν. Ένας αλγόριθμος βέλτιστης ανεκτικότητας θα πρέπει επίσης να περιλαμβάνει και ανταλλαγή τοπολογικής γνώσης μεταξύ των παικτών. Ένα τέτοιο πρωτόκολλο θα παρουσιαστεί στο επόμενο κεφάλαιο και αποδεικνύεται πράγματι μοναδικό για το μοντέλο μερικής γνώσης.

## 3.6 Μοντέλο γενικού αντιπάλου

Στη συνέχεια, ασχολούμαστε με το μοντέλο *γενικού αντιπάλου* των Hirt και Maurer [HM97] προκειμένου να γενικεύσουμε τα αποτελέσματά μας.

**Μοντέλο γενικού αντιπάλου**. Οι Hirt και Maurer στο [HM97] μελετάνε την ασφάλεια πρωτοκόλλων υπολογισμών πολλών συμμετεχόντων ως προς μια *δομή αντιπάλου*, δηλαδή, μια οικογένεια υποσυνόλων των παικτών· θεωρείται ότι ο αντίπαλος είναι ικανός να διαφθείρει ένα από αυτά τα σύνολα της οικογένεια σε μία εκτέλεση. Πιο τυπικά,

Μία δομή $\mathcal{Z}$ για το σύνολο των παικτών $V$ είναι μια μονότονη οικογένεια υποσυνόλων του $V$, δηλαδή $\mathcal{Z} \subseteq 2^V$, όπου όλα τα σύνολα ενός υποσυνόλου $Z \in \mathcal{Z}$ περιέχονται επίσης στο $\mathcal{Z}$, (εναλλακτικά, $\forall Z \in \mathcal{Z}$, εάν $Z' \subseteq Z$ τότε ισχύει ότι $Z' \in \mathcal{Z}$).

Επαναπροσδιορίζουμε τώρα κάποιες έννοιες που έχουν εισαχθεί σε αυτό το κεφάλαιο προκειμένου να επεκτείνουμε τα αποτελέσματά μας με στην περίπτωση του γενικού αντιπάλου. Θα καλούμε έναν αλγόριθμο που πετυχαίνει Εκπομπή για κάθε σύνολο διαφθοράς $T \in \mathcal{Z}$ στο γράφημα $G$ με διανομέα $D$, *$\mathcal{Z}$-ανεκτικό* στο $(G, D)$.

Ένα κάλυμμα $S \in \mathcal{Z}$ ενός συνόλου μονοπατιών $\mathcal{P}$ θα καλείται $\mathcal{Z}$-κάλυμμα. Στη συνέχεια, γενικεύουμε την έννοια του $t$-τοπικού διαχωριστή ζεύγους.

***Ορισμός* 3.8** ($\mathcal{Z}$-διαχωριστής ζεύγους). *Ένας διαχωριστής $C$ του $G$ για τον οποίον υπάρχει μια διαμέριση $C = C_1 \cup C_2$ και $C_1, C_2 \in \mathcal{Z}$ καλείται* $\mathcal{Z}$-διαχωριστής ζεύγους *του $G$.*

### 3.6.1 Δίκτυα γνωστής τοπολογίας

Προσαρμόζουμε τον PPA προκειμένου να μελετήσουμε το πρόβλημα της Εκπομπής στο μοντέλο γενικού αντιπάλου. Ο γενικευμένος $\mathcal{Z}$-PPA αλγόριθμος προκύπτι από την τροποποίηση του κανόνα διάδοσης έντιμοου μονοπατιού του PPA (Protocol 3).

**$\mathcal{Z}$-PPA κανόνας έντιμου μονοπατιού**. Ο παίκτης $v$ λαμβάνει την ίδια τιμή $x$ από ένα σύνολο $\mathcal{P}$ μονοπατιών και είναι σε θέση να συμπεράνει ότιγια κάθε $T \in \mathcal{Z}$, το $T$ δεν είναι κάλυμμα του $\mathcal{P}$.

Επιπλέον, ισχύουν τα ακόλουθα θεωρήματα και οι αποδείξεις τους είναι ουσιαστικά πανομοιότυπες με τις αποδείξεις των Θεωρημάτων 3.6, και 3.7. Η μόνη τεχνική τροποποίηση στις αποδείξεις είναι ότι πρέπει να αντικατασταθούν οι έννοιες $t$-τοπικός διαχωριστής ζεύγους, $t$-τοπικό σύνολο, $t$-τοπικό κάλυμμα, με τις $\mathcal{Z}$-διαχωριστής ζεύγους, πιθανό σύνολο διαφθοράς (ή ένα σύνολο που ανήκει στο $\mathcal{Z}$) και $\mathcal{Z}$-κάλυμμα αντίστοιχα.

***Θεώρημα* 3.10** (Ικανή συνθήκη). *Έστω ένα γράφημα $G$, διανομέας $D$, και μία δομή αντιπάλου $\mathcal{Z}$, αν δεν υπάρχει ένας $\mathcal{Z}$-διαχωριστής ζεύγους, τότε όλοι οι τίμιοι οπ παίκτες θα αποφασίσουν στο $x_D$ μέσω του $\mathcal{Z}$-PPA.*

***Θεώρημα* 3.11** (Αναγκαία συνθήκη). *Έστω ένα γράφημα $G$, ένας διανομέας $D$, και μία δομή αντιπάλου $\mathcal{Z}$, αν υπάρχει ένας $\mathcal{Z}$-τοπικός διαχωριστής ζεύγους τότε δεν υπάρχει κανένας $\mathcal{Z}$-ανεκτικός αλγόριθμος Εκπομπής για το $(G, D)$.*

### 3.6.2 *Ad Hoc* Δίκτυα

Εφόσον στο *ad hoc* μοντέλο οι παίκτες γνωρίζουν μόνο τα δικά τους αναγνωριστικά και τα αναγνωριστικά των γειτόνων τους είναι λογικό να υποθέσουμε ότι κάποιος παίκτης έχει μόνο τοπική γνώση ως προς τη δομή του αντιπάλου $\mathcal{Z}$. Συγκεκριμένα, δοθείσας της πραγματικού δομής αντιπάλου $\mathcal{Z}$ υποθέτουμε ότι ο κάθε παίκτης $v$ γνωρίζει μόνο την *τοπική δομή αντιπάλου* $\mathcal{Z}_v = \{A \cap \mathcal{N}(v) : A \in \mathcal{Z}\}$. Μια παρόμοια υπόθεση χρησιμοποιείται και στο [TV13].

Όπως και στα δίκτυα γνωστής τοπολογίας, μπορούμε να περιγράψουμε μια γενικευμένη έκδοση $\mathcal{Z}$-CPA of CPA, ο οποίος είναι ένας *ad hoc* αλγόριθμος Εκπομπής για το μοντέλο γενικού αντιπάλου. Συγκεκριμένα, τροποποιούμε το βήμα (3) του CPA (Πρωτόκολλο 2) με τον ακόλουθο τρόπο.

**$\mathcal{Z}$-CPA κανόνας πιστοποιημένης διάδοσης.** Αν ένας κόμβος $v$ δεν είναι γείτονας του διανομέα, τότε αν λάβει την ίδια τιμή $x$ από όλου στου γείτονές του που βρίσκονται στο σύνολο $\mathcal{N} \subseteq \mathcal{N}(v)$ τέτοιο ώστε $N \notin \mathcal{Z}_v$, αποφασίζει στην τιμή $x$.

Η απόδειξη της ασφάλειας του $\mathcal{Z}$-CPA είναι ουσιαστικά η ίδια με την απόδειξη ασφάλειας του αρχικού αλγορίθμου CPA, όπως παρουσιάζεται στο Θεώρημα 2.1. Παρατηρούμε ότι ο $\mathcal{Z}$-CPA κανόνας πιστοποιημένης διάδοσης. Ουσιαστικά δηλώνει ότι αν κάποιος παίκτης λάβει την ίδια τιμή $x$ από ένα σύνολο γειτόνων του που δεν μπορούν να διαφθαρούν όλοι, τότε ο παίκτης μπορεί ασφαλώς να αποφασίσει στο μήνυμα, καθώς τουλάχιστον ένας από αυτούς του γείτονές του είναι σίγουρα τίμιος και στέλνει την σωστή τιμή.

Για να επιχειρηματολογήσουμε για τις τοπολογικές συνθήκες που επηρρεάζουν την αποτελεσματικότητα του $\mathcal{Z}$-CPA γενικεύουμε την έννοια του $t$-plp διαχωριστή.

***Ορισμός* 3.9** ($\mathcal{Z}$-μερικός διαχωριστής ζεύγους). *Έστω $C$ ένας διαχωριστής του $G$ που διαμερίζει το $V \setminus C$ στα σύνολα $A, B \neq \emptyset$ τέτοια ώστε $D \in A$. Το $C$ είναι ένας $\mathcal{Z}$-μερικός διαχωριστής ζεύγους ($\mathcal{Z}$-partial pair cut ($\mathcal{Z}$-pp cut) αν υπάρχει μια διαμέριση $C = C_1 \cup C_2$ με $C_1 \in \mathcal{Z}$ και $\forall u \in B$, $\mathcal{N}(u) \cap C_2 \in \mathcal{Z}_u$.*

Ανάλογα με την μοναδικότητα του CPA, μπορούμε τώρα να αποδείξουμε την μοναδικότητα του $\mathcal{Z}$-CPA στο μοντέλο γενικού αντιπάλου. Παρουσιάσουμε μία εναλλακτική απόδειξη, μια τροποποίηση της οποίας μπορεί να χρησιμοποιηθεί για την απόδειξη του Θεωρήματος 3.1.

***Θεώρημα* 3.12** (Ικανή συνθήκη). *Έστω ένα γράφημα $G$, διανομέας $D$, και μία δομή αντιπάλου $\mathcal{Z}$, αν δεν υπάρχει ένας $\mathcal{Z}$-pp διαχωριστής, τότε ο $\mathcal{Z}$-CPA είναι $\mathcal{Z}$-ανεκτικός.*

*Απόδειξη.*
Υποθέτουμε ότι ο $\mathcal{Z}$-CPA δεν είναι $\mathcal{Z}$-ανεκτικός. τότε υπάρχει ένα σενάριο όπου το σύνολο

$C$ είναι οι διεφθαρμένοι κόμβοι, $A$ είναι οι τίμιοι κόμβοι που έχουν αποφασίσει και $B$ είναι οι τίμιοι κόμβοι που δεν έχουν αποφασίσει. Όλοι οι κόμβοι στο $A$ έχουν αποφασίσει στην σωστή τιμή αφού ο $\mathcal{Z}$-CPA είναι ασφαλής. Εφόσον κάθε κόμβος στο $B$ δεν έχει αποφασίσει, έχουμε ότι $\forall u \in B : \mathcal{N}(u) \cap A \in \mathcal{Z}_u$, αλλιώς ο $u$ θα είχε αποφασίσει αφού ένα σύνολο κόμβων που δεν βρίσκονται στο $Z_u$ θα του είχε στείλει την ίδια τιμή. Αλλά τότε ισχύει ότι $C \cup A$ είναι ένας $\mathcal{Z}$-pp διαχωριστής το οποίο αντιφάσκει με την υπόθεση. Ως εκ τούτου, ο $\mathcal{Z}$-CPA είναι $\mathcal{Z}$-ανεκτικός. □

***Θεώρημα* 3.13** (Αναγκαία συνθήκη ). *Έστω $\mathcal{A}$ ένας ασφαλής ad hoc αλγόριθμος Εκπομπής. Για ένα γράφημα $G$, με διανομέα $D$, και δομή αντιπάλου $\mathcal{Z}$, αν υπάρχει ένας $\mathcal{Z}$-pp διαχωριστής τότε ο $\mathcal{A}$ δεν είναι $\mathcal{Z}$-ανεκτικός για το $G, D$.*

*Απόδειξη.*
Έστω $C = C_1 \cup C_2$ ένας $\mathcal{Z}$-pp διαχωριστής που χωρίζει το $V \setminus C$ στα σύνολα $A, B \neq \emptyset$ τέτοια ώστε $D \in A$. Έστω $\mathcal{Z}' = \{\bigcup_{u \in B} Z \cap \mathcal{N}(u) : Z \in \mathcal{Z}\} \cup \{C_2\}$.

Για κάθε κόμβο $u$ στο $B$ έχουμε:

$$\begin{aligned}
\mathcal{Z}'_u &= \{Z \cap \mathcal{N}(u) : Z \in \mathcal{Z}'\} \cup \{C_2 \cap \mathcal{N}(u)\} \\
&= \left\{ \left( \bigcup_{v \in B} Z \cap \mathcal{N}(v) \right) \cap \mathcal{N}(u) : Z \in \mathcal{Z} \right\} \cup \{C_2 \cap \mathcal{N}(u)\} \\
&= \{Z \cap \mathcal{N}(u) : Z \in \mathcal{Z}\} \cup \{C_2 \cap \mathcal{N}(u)\} \\
&= \mathcal{Z}_u
\end{aligned}$$

αφού $\forall u \in B : \mathcal{N}(u) \cap C_2 \in \mathcal{Z}_u$.

Μέχρι τώρα έχουμε διαπιστώσει ότι (α) οι κόμβοι στο $B$ δεν μπορούν να αποφανθούν αν το $\mathcal{Z}$ ή το $\mathcal{Z}'$ είναι η πραγματική δομή αντιπάλου επειδή $\forall u \in B : \mathcal{Z}_u = \mathcal{Z}'_u$ και (β) το σύνολο $C_2$ είναι ένα επιτρεπτό σύνολο διαφθοράς στο $\mathcal{Z}'$.

Υποθέτουμε ότι ένας κόμβος στο $B$ μπορεί να αποφασίσει σε κάποια τιμή σε μια εκτέλεση όπου το $\mathcal{Z}$ είναι η πραγματική δομή αντιπάλου. Τότε, χρησιμοποιώντας το καθιερωμένο επιχείρημα που παρουσιάζεται στο Θεώρημα 3.2,μπορούμε να φτάσουμε σε αντίφαση ως προς την ασφάλεια του αλγορίθμου θεωρώντας μία διαφορετική εκτέλεση όπου το $\mathcal{Z}'$ είναι η πραγματική δομή του αντιπάλου. Οι λεπτομέρειες της απόδειξης βασίζονται στην δυσκολία των τίμιων παικτών του $B$ να διακρίνουν σε ποια εκτέλεση συμμετέχουν, σε αυτήν με δομή αντιπάλου $\mathcal{Z}$ ή σε αυτή με δομή αντιπάλου $\mathcal{Z}'$. □

## 3.7 Η περίπτωση του διεφθαρμένου διανομέεα

Μελετήσαμε το πρόβλημα της Εκπομπής στην περίπτωση που ο διανομέας είναι τίμιος. Για αν μελετήσουμε το πρόβλημα στη γενική περίπτωση που ακόμα και ο διανομέας μπορεί να διαφθαρεί, παρατηρούμε ότι για δοθείσα δομή αντιπάλου $\mathcal{Z}$ και γράφημα $G$, $\mathcal{Z}$-ανεκτική Εκπομπή σε *ad hoc* δίκτυα μπορεί να επιτευχθεί αν ισχύουν και οι δύο ακόλουθες συνθήκες:

1. $\nexists Z_1, Z_2, Z_3 \in \mathcal{Z}$ τέτοια ώστε $Z_1 \cup Z_2 \cup Z_3 = V$.

2. $\forall v \in V$ δεν υπάρχει ένας $\mathcal{Z}$-pp διαχωριστής στο $G$ με διανομέα $v$.

Η συνθήκη 1 αποδείχθηκε από τους Hirt και Maurer [HM97] ικανή και αναγκαία για την ύπαρξη πρωτοκόλλων υπολογισμών πολλών συμμετεχόντων σε πλήρη δίκτυα. Μπορεί να επιτευχθεί $\mathcal{Z}$-ανεκτική Εκπομπή στην γενική περίπτωση, όπου το δίκτυο είναι ελλιπές, προσομοιώνοντας οποιοδήποτε πρωτόκολλο για πλήρη δίκτυα (π.χ. το πρωτόκολλο που παρουσιάζεται στο [FM98]) ακολούθως: κάθε διάδοση ενός παίκτη σε πολλούς άλλους αντικαθίσταται από μία εκτέλεση του $\mathcal{Z}$-CPA. Δεν είναι δύσκολο να δούμε ότι η σύζευξη των παραπάνω συνθηκών είναι αναγκαία και ικανή για να πετύχουμε Εκπομπή σε ελλειπή δίκτυα στην γενική περίπτωση όπου ο διανομέας μπορεί να διαφθαρεί. Ομοίως, σε δίκτυα γνωστής τοπολογίας υπάρχει ένας $\mathcal{Z}$-ανεκτικός αλγόριθμος Εκπομπής αν η συνθήκη 1 ισχύει και για κάθε $v \in V$ δεν υπάρχει $\mathcal{Z}$-διαχωριστής ζεύγους για το γράφημα $G$ με διανομέα $v$. Φυσικά, οι παραπάνω παρατηρήσεις ισχύουν και για την ειδική περίπτωση του μοντέλου $t$-τοπικά φραγμένου αντιπάλου.

## 3.8 Συμπεράσματα Κεφαλαίου

Όπως δείξαμε, στο μοντέλο $t$-τοπικά φραγμένου αντιπάλου και στο μοντέλο γενικού αντιπάλου η ιδέα του CPA, παρά την απλότητά της και το ελάχιστο ποσό διάδοσης μηνυμάτων (ένας παίκτης διαδίδει μόνο την τιμή που έχει αποφασίσει σε όλους τους γείτονές του) μας δίνει αλγορίθμους οι οποίοι είναι βέλτιστης ανεκτικότητας (μοναδικοί). Το τελευταίο σημαίνει ότι δεν είναι δυνατόν να πετύχουμε καλύτερη επιλυσιμότητα του προβλήματος χρησιμοποιώντας πιο πολύπλοκα σχήματα διάδοσης μηνυμάτων. Επιπλέον, τα αποτελέσματα αυτού του κεφαλαίου υπονοούν ότι υπάρχουν στιγμιότυπα στα οποία το πρόβλημα δεν είναι επιλύσιμο στο Ad Hoc μοντέλο, αλλά είναι επιλύσιμο εάν υποθέσουμε υψηλότερο επίπεδο γνώσης της τοπολογίας. Αυτό υποδηλώνει ότι κανένας αλγόριθμος ανακάλυψης τοπολογίας στο ad hoc μοντέλο δεν μπορεί να μας παρέχει κάποια χρήσιμη πληροφορία που θα επηρεάσει την επιλυσιμότητα του προβλήματος. Αφού ο CPA είναι βέλτιστης ανεκτικότητας, είναι φυσιολογικό αν μελετήσουμε εάν μας παρέχει και την πιο αποδοτική λύση για το πρόβλημα. Ασχολούμαστε με την τελευταία ερώτηση στο επόμενο κεφάλαιο.

Ένα ενδιαφέρον ανοιχτό πρόβλημα είναι να προσδιορίσουμε την μεγαλύτερη κλάση αλγορίθμων μεταξύ των οποίων ο CPA (αντίστοιχα και ο $\mathcal{Z}$-CPA) είναι μοναδικός. Προηγούμενα αποτελέσματα (βλέπε αλγόριθμος RPA [PP05]) συνδυασμένα με τη μελέτη που παρουσιάστηκε σε αυτό το κεφάλαιο υποδεικνύουν ότι για να πετύχουμε καλύτερη επιλυσιμότητα από τον CPA πρέπει να υποθέσουμε επιπλέον τοπολογική γνώση.

Αποδείξαμε ότι ο υπολογισμός της ισχύος των ικανών και αναγκαίων συνθηκών για επίτευξη Εκπομπής σε δίκτυα γνωστής και άγνωστης τοπολογίας είναι NP-δύσκολος. Επομένως ποια θα μπορούσε να είναι η καλύτερη επίθεση που μπορεί να πετύχει κάποιος αντίπαλος? Παρόμοια θέματα μπορεί να προκύψουν από τη σκοπιά των σχεδιαστών του συστήματος. Ο

καθορισμός ενός κατάλληλου μεγέθους προς βελτιστοποίηση σχετικό με την ανεκτικότητα του δικτύου είναι απαραίτητος για να απαντήσουμε τέτοια ερωτήματα απάντηση σε τέτοιου είδους ερωτήματα.

# Κεφάλαιο 4

# Μερική Γνώση και Αξιόπιστη Μετάδοση Μηνύματος

Μια θεμελιώδης αρχή στον τομέα των κατανεμημένων συστημάτων είναι η *Αξιόπιστη Μετάδοση Μηνύματος* (Reliable Message Transmission-RMT), η οποία αναφέρεται στην ορθή αποστολή ενός μηνύματος από έναν παίκτη σε κάποιον άλλο, παρά την ύπαρξη βυζαντινών διαφθορών. Σε αυτό το κεφάλαιο αντιμετωπίζουμε το πρόβλημα στο μοντέλο γενικού αντιπάλου των Hirt και Maurer, στο οποίο συμπεριλαμβάνονται προγενέστερα μοντέλα όπως τα μοντέλα καθολικά και τοπικά φραγμένου αντιπάλου. Αναφορικά με την τοπολογική γνώση, εργαζόμαστε στο *Μοντέλο Μερικής Γνώσης*, που εισήχθη στο προηγούμενο κεφάλαιο· όπως προαναφέραμε, το μοντέλο αυτό γενικεύει τα μοντέλα πλήρους και *ad hoc* γνώσης.

Οι συνεισφορές που παρουσιάζονται σε αυτό το κεφάλαιο είναι οι εξής: (α) Μία ικανή και αναγκαία συνθήκη για την επίτευξη RMT στο μοντέλο μερικής γνώσης υπό την επιρροή ενός γενικού αντιπάλου. Για να δείξουμε την ικανότητα της συνθήκης, προτείνουμε τον RMT-Αλγόριθμο Μερικής Γνώσης (RMT Partial Knowledge Algorithm ή RMT-PKA), έναν αλγόριθμο που επιλύει το RMT πρόβλημα όποτε αυτό είναι επιλύσιμο· αυτό τον καθιστά έναν *μοναδικό* αλγόριθμο για το πρόβλημα. Ο RMT-PKA είναι ο πρώτος αλγόριθμος που συναντήσαμε στη βιβλιογραφία για την επίλυση του RMT στο μοντέλο μερικής γνώσης. (β) Μία μελέτη της αποδοτικότητας στην περίπτωση των *ad hoc* δικτύων: Δείχνουμε ότι είτε το πρωτόκολλο $\mathcal{Z}$-CPA, που παρουσιάστηκε στο προηγούμενο κεφάλαιο, είναι πλήρως πολυωνυμικό είτε δεν υπάρχει πλήρως πολυωνυμικό RMT πρωτόκολλο· έτσι, εισάγουμε μια νέα έννοια μοναδικότητας ως προς την αποδοτικότητα την οποία ονομάζουμε *μοναδικότητα πολυωνυμικού χρόνου.*

Για την εξαγωγή των αποτελεσμάτων μας, χρησιμοποιούμε, μεταξύ άλλων, μία πράξη *ενοποίησης γνώσης* μεταξύ δομών αντιπάλου, μια νέα έννοια διαχωριστή (RMT-cut), κατάλληλη για το RMT σε αναξιόπιστα δίκτυα, και μία ιδιότητα αυτοαναγωγής του προβλήματος RMT, που δείχνουμε με τη βοήθεια σύνθεσης πρωτοκόλλων. Το τελευταίο είναι και το κεντρικό εργαλείο για την απόδειξη της μοναδικότητας πολυωνυμικού χρόνου του $\mathcal{Z}$-CPA.

## 4.1 Εισαγωγή

Η επίτευξη αξιόπιστης επικοινωνίας σε αναξιόπιστα δίκτυα είναι θεμελιώδης στον τομέα των κατανεμημένων συστημάτων. Προφανώς, η ύπαρξη ενός πιστοποιημένου καναλιού επικοινωνίας μεταξύ δύο παικτών μας εγγυάται την αξιόπιστη μεταξύ τους επικοινωνία. Εντούτοις, στα σύγχρονα δίκτυα επικοινωνίας συγκεκριμένοι παίκτες είναι μόνο έμμεσα συνδεδεμένοι, και χρειάζεται να χρησιμοποιηθούν ενδιάμεσοι παίκτες σαν αναμεταδότες για να διαδοθεί το μήνυμα στον πραγματικό παραλήπτη. Το πρόβλημα της *Αξιόπιστης Μετάδοσης μηνύματος* (Reliable Message Transmission-RMT) είναι το πρόβλημα της επίτευξης ορθής παράδοσης ενός μηνύματος $m$ από τον διανομέα (ή αποστολέα) $D$ στον παραλήπτη $R$ ακόμα και στην περίπτωση που κάποιοι ενδιάμεσοι κόμβοι είναι διεφθαρμένοι και δεν προωθούν το μήνυμα όπως έχει συμφωνηθεί. Σε αυτό το κεφάλαιο μελετάμε το πρόβλημα Αξιόπιστης Μετάδοσης Μηνύματος υπό την ύπαρξη ενός γενικού βυζαντινού αντιπάλου. Το πρόβλημα RMT μελετήθηκε αρχικά από τον Dolev [Dol82] στο πλαίσιο του συγγενούς προβλήματος της Αξιόπιστης Εκπομπής.

Το RMT ενάντια σε βυζαντινούς αντιπάλους έχει μελετηθεί εκτενώς σε διάφορες παραλλαγές: ασφαλής ή αξιόπιστη μετάδοση, υπό γενικό ή φραγμένο αντίπαλο, με την απαίτηση τέλειας ασφάλειας ή με την ανοχή μιας μικρής πιθανότητας σφάλματος. Εδώ επικεντρωνόμαστε στην τέλεια αξιόπιστη μετάδοση μηνύματος υπό έναν γενικό αντίπαλο και στο μοντέλο μερικής γνώσης. Πιο συγκεκριμένα, το RMT στο μοντέλο του φραγμένου αντιπάλου, μελετήθηκε αρχικά στα [DDWY93, DW02], όπου τέθηκαν επιπλέον περιορισμοί ως προς την ασφάλεια και στο [SGSR08] όπου επιτρεπόταν μια μικρή πιθανότητα λάθους. Αποτελέσματα για το RMT στο μοντέλο γενικού αντιπάλου [HM97], δόθηκαν στα [KGSR02, SR06, SPCR09]. Γενικά, πολύ λίγες μελέτες ασχολήθηκαν με το RMT ή συγγενή προβλήματα σε μοντέλα περιορισμένης γνώσης παρά το γεγονός ότι αυτή η κατεύθυνση είχε προταθεί το 2002 από στην δουλειά των Kumar *et al.* [KGSR02]. Μελετάμε λοιπόν το πρόβλημα RMT υπό το μοντέλο γενικού αντιπάλου και το μοντέλο μερικής γνώσης που εισήχθη στο προηγούμενο κεφάλαιο.

Η ισχύς των αποτελεσμάτων αυτού του κεφαλαίου κείται στον συνδυασμό αυτών των δύο πολύ γενικών μοντέλων (γενικού αντιπάλου και μερικής γνώσης), διαμορφώνοντας την πιο γενική θεώρηση που έχουμε συναντήσει έως τώρα στα πλαίσια του σύγχρονου και ντετερμινιστικού μοντέλου.

Όλα τα προαναφερθέντα αποτελέσματα για το πρόβλημα της Εκπομπής, που παρουσιάζονται στα προηγούμενα κεφάλαια, μπορούν να προσαρμοστούν τετριμμένα για το πρόβλημα RMT. Ο προσδιορισμός μιας αναγκαίας και ικανής συνθήκης για την πιο γενική περίπτωση του μοντέλου μερικής γνώσης δεν είχε επιτευχθεί πριν την παρούσα μελέτη. Επιπλέον η μελέτη στα προηγούμενα κεφάλαια επικεντρώθηκε στην επιλυσιμότητα του προβλήματος και όχι στην αποδοτικότητα των πρωτοκόλλων που το επιλύουν· γενικά δεν έχει διεξαχθεί κάποια γνωστή μελέτη για την πολυπλοκότητα του προβλήματος σε αυτό το πλαίσιο. Αυτά τα δύο ζητήματα μελετώνται και απαντώνται σε αυτό το κεφάλαιο.

### 4.1.1 Διάρθρωση του Κεφαλαίου

Μελετάμε το πρόβλημα RMT υπό την παρουσία ενός γενικού βυζαντινού αντίπαλου. Η συνεισφορά μας μπορεί να συνοψιστεί σε δύο κεντρικά σημεία:

- Επιλυσιμότητα του RMT στο μοντέλο μερικής γνώσης. Αποδεικνύουμε μια αναγκαία και ικανή συνθήκη για την επίτευξη RMT σε αυτό το πλαίσιο, και παρουσιάζουμε τον RMT-Αλγόριθμο Μερικής Γνώσης (RMT Partial Knowledge Algorithm ή RMT-PKA), έναν αλγόριθμο που πετυχαίνει RMT όποτε ισχύει αυτή η συνθήκη. Σύμφωνα με την ορολογία που χρησιμοποιήθηκε στα προηγούμενα κεφάλαια, αυτός είναι ένας *μοναδικός* αλγόριθμος για το πρόβλημα, με την έννοια ότι όποτε ένας αλγόριθμος πετυχαίνει RMT σε ένα συγκεκριμένο στιγμιότυπο τότε το πετυχαίνει και ο αλγόριθμός μας. Αυτό συμπληρώνει την μελέτη της επιλυσιμότητας που παρουσιάσαμε στο Κεφάλαιο 3. Ο RMT-PKA είναι και ο πρώτος αλγόριθμος γιαυτό το γενικό μοντέλο που συναντάμε στη σχετική βιβλιογραφία.

  Μία σημαντική έννοια που χρησιμοποιούμε είναι η έννοια της *από κοινού δομής αντιπάλου* ενός συνόλου παικτών η οποία ανταποκρίνεται στην χειρότερη περίπτωση δομής αντιπάλου που είναι συμβατή με την αρχική γνώση των παικτών; αυτή η έννοια είναι πολύ σημαντική για την εξαγωγή της αναγκαίας και ικανής συνθήκης που αναφέρεται παραπάνω, αφού μας παρέχει έναν τρόπο να αξιοποιήσουμε ασφαλώς την μέγιστη έγκυρη πληροφορία από τα μηνύματα που ανταλλάζονται. Επίσης χρησιμοποιούμε και αναπτύσσουμε την τεχνική των τοπικών διαχωριστών ζεύγους, που εισήχθη από τους Pelc και Peleg [PP05] στα πλαίσια της μελέτης του συγγενούς προβλήματος της Εκπομπής. Αυτή η τεχνική επεκτάθηκε στο Κεφάλαιο 3 για την εξαγωγή χαρακτηρισμών των κλάσεων των γραφημάτων για τα οποία η επίτευξη Εκπομπής είναι εφικτή για διάφορα επίπεδα τοπολογικής γνώσης και οποιοδήποτε τύπο κατανομής των διαφθορών. Ωστόσο, δεν παρουσιάσαμε μέχρι τώρα έναν ακριβή χαρακτηρισμό των στιγμιοτύπων όπου το πρόβλημα είναι επιλύσιμο για το μοντέλο μερικής γνώσης. Εδώ, απαντάμε αυτό το ερώτημα προτείνοντας μία κατάλληλη έννοια διαχωριστή ζεύγους για το μοντέλο μερικής γνώσης και έναν μοναδικό αλγόριθμο (RMT-PKA) για το RMT, τον πρώτο που έχει προταθεί γιαυτό το γενικό μοντέλο. Ο αλγόριθμος RMT-PKA είναι γενικός και συμπεριλαμβάνει στην περιγραφή του τους αλγορίθμους όπως ο CPA [Koo04], ο PPA και ο $\mathcal{Z}$-CPA [PPS14], που παρουσιάστηκαν σε προηγούμενα κεφάλαια, σαν ειδικές περιπτώσεις. Μία χρήσιμη παρατήρηση που προκύπτει από τη μελέτη μας και έχει πρακτικό ενδιαφέρον, είναι ότι η νέα αυτή έννοια διαχωριστή μπορεί να χρησιμοποιηθεί για τον προσδιορισμό του ακριβούς υπογραφήματος στο οποίο είναι εφικτό να επιτευχθεί RMT στην φάση του σχεδιασμού ενός δικτύου. Μία αξιοσημείωτη ιδιότητα του αλγορίθμου μας είναι η *ασφάλειά* του όπως αυτή ορίστηκε σε προηγούμενο κεφάλαιο: ακόμα και αν δεν είναι δυνατή η επίτευξη RMT ο παραλήπτης δεν θα πάρει ποτέ μια λανθασμένη απόφαση παρά τις αυξημένες δυνατότητες επίθεσης που έχει ο αντίπαλος, η οποίες περιλαμβάνουν, μεταξύ άλλων, την αναφορά ανυπόστατης τοπολογίας και ψευδούς αρχικής γνώσης.

- Αποδοτικότητα επίτευξης του RMT στο *Ad Hoc* μοντέλο. Μελετάμε την *ad hoc* περί-

πτωση ως προς την αποδοτικότητα γιατί ακόμη και σε αυτήν την απλή περίπτωση μερικής γνώσης, δεν είναι ξεκάθαρο αν υπάρχει ένα αποδοτικό (πλήρως πολυωνυμικό[1]) πρωτόκολλο.

Προτείνουμε μια προσαρμογή του $\mathcal{Z}$-CPA [PPS14] κατάλληλη για το πρόβλημα RMT. Αποδεικνύουμε ότι αυτό το πρωτόκολλο είναι μοναδικό για το RMT στο *Ad Hoc* μοντέλο, το πρώτο πρωτόκολλο με αυτή την ιδιότητα που έχουμε συναντήσει. Εξετάζουμε αν και πότε αυτό το πρωτόκολλο είναι πλήρως πολυωνυμικό. Δείχνουμε ότι δεν υπάρχει κανένα μοναδικό πλήρως πολυωνυμικό πρωτόκολλο για το RMT εάν ο $\mathcal{Z}$-CPA δεν είναι πλήρως πολυωνυμικός, και έτσι εισάγουμε την νέα, πρακτικής σημασίας έννοια της *μοναδικότητας πολυωνυμικού χρόνου*. Συγκεκριμένα, δείχνουμε ότι αν ο $\mathcal{Z}$-CPA δεν είναι πλήρως πολυωνυμικός σε οποιαδήποτε κλάση στιγμιοτύπων στην οποία το RMT είναι επιλύσιμο, τότε υπάρχει μια αντίστοιχη κλάση (απλούστερων) στιγμιοτύπων όπου το RMT είναι επιλύσιμο και οποιοδήποτε πρωτόκολλο που πετυχαίνει RMT δεν μπορεί να είναι πλήρως πολυωνυμικό. Εξάγουμε αυτό το αποτέλεσμα δείχνοντας ότι ο $\mathcal{Z}$-CPA μπορεί να χρησιμοποιηθεί σαν μια πολυωνυμική αυτοαναγωγή για το RMT πρόβλημα. Επομένως, ο $\mathcal{Z}$-CPA, παρά την απλότητα και την ελάχιστη διάδοση μηνυμάτων που τον χαρακτηρίζει, αποδεικνύεται ότι είναι τουλάχιστον όσο αποδοτικός (με την έννοια που περιγράφεται παραπάνω) είναι οποιοσδήποτε RMT αλγόριθμος

Διαισθητικά, ενισχύουμε την ιδιότητα της μοναδικότητας του $\mathcal{Z}$-CPA υπονοώντας ότι, όχι μόνο δεν μπορεί να επιτευχθεί καλύτερη επιλυσιμότητα του προβλήματος χρησιμοποιώντας πιο πολύπλοκα σχήματα διάδοσης μηνυμάτων, αλλά επίσης δεν μπορεί να επιτευχθεί σημαντικά καλύτερη πολυπλοκότητα με αυτόν τον τρόπο. Αυτός ο περιορισμός φαίνεται να είναι εγγενής στα *ad hoc* δίκτυα όπου η γνώση των παικτών εξαρτάται αυστηρά από την πληροφορία που λαμβάνουν από τους άμεσους γείτονές τους.

Τα αποτελέσματα αυτού του κεφαλαίου παρουσιάστηκαν για πρώτη φορά στα [PPS16a, PPS15].

### 4.1.2 Μοντέλο και βασικοί ορισμοί

Σε αυτό το κεφάλαιο αντιμετωπίζουμε το πρόβλημα της τέλεια αξιόπιστης μετάδοσης μηνύματος, το οποίο θα αναφέρεται στο εξής σαν RMT, υπό την επιρροή ενός γενικού βυζαντινού αντιπάλου. Στο μοντέλο μας οι παίκτες έχουν μερική γνώση της τοπολογίας του δικτύου και της δομής του αντιπάλου.

Υποθέτουμε ένα σύγχρονο δίκτυο $G$ που αποτελείται από το σύνολο παικτών (κόμβων) $V(G)$ και το σύνολο ακμών $E(G)$ οι οποίες αναπαριστούν πιστοποιημένα κανάλια επικοινωνίας μεταξύ παικτών. Το σύνολο των γειτόνων ενός παίκτη $v$ συμβολίζεται με $\mathcal{N}(v)$. Ακολουθεί ο ορισμός του προβλήματος.

[1]Ένα πλήρως πολυωνυμικό πρωτόκολλο είναι ένα πρωτόκολλο πολυωνυμικής πολυπλοκότητας γύρων, επικοινωνίας και πολυωνυμικής τοπικής υπολογιστικής πολυπλοκότητας.

**Αξιόπιστη Μετάδοση Μηνύματος**. Υποθέτουμε την ύπαρξη ενός ορισμένου παίκτη $D$, που τον ονομάζουμε *διανομέα*, ο οποίος στοχεύει στη διάδοση μιας συγκεκριμένης τιμής $x_D \in X$, όπου $X$ ο χώρος αρχικών τιμών, σε έναν άλλον ορισμένο παίκτη $R$, που ονομάζεται *παραλήπτης*. Ένα κατανεμημένο πρωτόκολλο πετυχαίνει (επιλύει το πρόβλημα) RMT εάν μέχρι το τέλος του πρωτοκόλλου, ο παραλήπτης $R$ έχει *αποφασίσει* στην τιμή $x_D$, δηλαδή, αν είναι σε θέση να δώσει σαν έξοδο την τιμή $x_D$ που στάλθηκε αρχικά από τον διανομέα.

Όπως και στην Ενότητα 3.6.2, υιοθετούμε την φυσιολογική υπόθεση ότ η γνώση ενός παίκτη ως προς την δομή του αντιπάλου περιορίζεται από την τοπολογική του γνώση; συγκεκριμένα, ο συνδυασμός του μοντέλου μερικής γνώσης και του μοντέλου γενικού αντιπάλου που προτείνουμε ως προς τη γνώση των παικτών περιγράφεται παρακάτω:

**Μερική γνώση και γενικοί αντίπαλοι**. Εξετάζοντας το μοντέλο μερικής γνώσης υπό την παρουσία ενός γενικού αντιπάλου επεκτείνουμε το μοντέλο της Ενότητας 3.6.2 και υποθέτουμε ότι δοθείσας της δομής αντιπάλου $\mathcal{Z}$ κάθε παίκτης $v$ έχει γνώση μόνο ως προς τα πιθανά σύνολα διαφθοράς που συμπίπτουν με την τοπολογική του γνώση, δηλαδή γνωρίζει μόνο την *τοπική δομή αντιπάλου* $\mathcal{Z}_v = \{A \cap V(\gamma(v)) \mid A \in \mathcal{Z}\}$.

Συμβολίζουμε ένα στιγμιότυπο του προβλήματος με την πεντάδα $\mathcal{I} = (G, \mathcal{Z}, \gamma, D, R)$. Ανάλογα με τις ιδιότητες πρωτοκόλλων που παρουσιάσαμε νωρίτερα, θα χρησιμοποιήσουμε τις παρακάτω έννοιες:

**Ιδιότητες πρωτοκόλλων**. Λέμε ότι ένα πρωτόκολλο RMT είναι *ανεκτικό* για ένα στιγμιότυπο $\mathcal{I}$ εάν πετυχαίνει RMT στο στιγμιότυπο $\mathcal{I}$ για κάθε πιθανό σύνολο διαφθοράς και κάθε πιθανή συμπεριφορά των διεφθαρμένων παικτών. Λέμε ότι ένα RMT πρωτόκολλο είναι *ασφαλές* εάν δεν προκαλεί στον παραλήπτη $R$ την απόφαση σε λανθασμένη τιμή, σε οποιοδήποτε στιγμιότυπο. Ένα πρωτόκολλο $A$ είναι μοναδικό (για το πρόβλημα RMT) μεταξύ αλγορίθμων της οικογένειας πρωτοκόλλων $\mathcal{A}$, αν η ύπαρξη ενός πρωτοκόλλου $\mathcal{A}$ που πετυχαίνει RMT σε ένα στιγμιότυπο $\mathcal{I}$ συνεπάγεται ότι το $A$ πετυχαίνει επίσης RMT στο $\mathcal{I}$.

Ομοίως με το προηγούμενο κεφάλαιο, χρησιμοποιούμε διαχωριστές οι οποίοι αποσυνδέουν τον παραλήπτη από τον διανομέα, επομένως, διαχωριστές οι οποίοι δεν περιλαμβάνουν τον διανομέα. Στο εξής, θα αναφερόμαστε σε αυτού του τύπου τους διαχωριστές απλά με τον όρο διαχωριστής.

## 4.2 Μερική γνώση και γενικοί αντίπαλοι

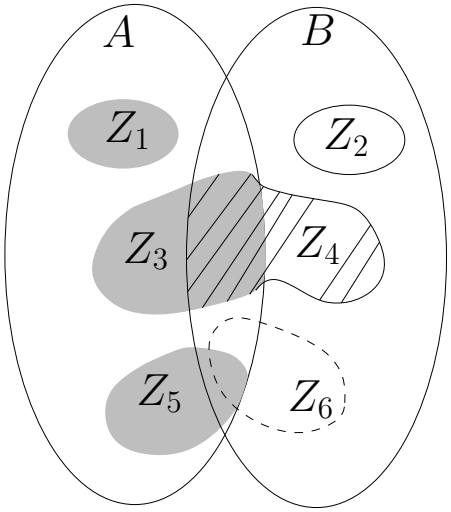
Λαμβάνοντας υπόψιν δύο παίκτες που έχουν μερική γνώση ως προς την δομή του αντιπάλου, είναι χρήσιμο να ορίσουμε μια πράξη για να υπολογίζουμε την *από κοινού γνώση* σχετικά με τον αντίπαλο. Για μια δομή αντιπάλου $\mathcal{E}$ και ένα σύνολο κόμβων $A$ συμβολίζουμε με $\mathcal{E}^A = \{Z \cap A \mid Z \in \mathcal{E}\}$ τον περιορισμό του $\mathcal{E}$ στο σύνολο $A$. Η από κοινού δομή αντιπάλου από δύο περιορισμένες δομές μπορεί να εξαχθεί μέσω της πράξης $\oplus$. Ορίζουμε την πράξη

σε δύο πιθανώς διαφορετικές δομές αντιπάλου $\mathcal{E}, \mathcal{F}$ έτσι ώστε η πράξη να είναι καλώς ορισμένη ακόμα και αν κάποιος διεφθαρμένος παίκτης παρέχει μια διαφορετική δομή από την πραγματική σε κάποιον τίμιο παίκτη.

***Ορισμός* 4.1**. *Έστω $\mathbb{T}^A = 2^{2^A}$ ο χώρος των δομών του αντιπάλου ως προς ένα σύνολο $A$. Για κάθε δύο σύνολα παικτών $A, B$ και δομές αντιπάλου $\mathcal{E}, \mathcal{F}$, η πράξη $\oplus : \mathbb{T}^A \times \mathbb{T}^B \to \mathbb{T}^{(A \cup B)}$, ορίζεται ακολούθως:*

$$\mathcal{E}^A \oplus \mathcal{F}^B = \{Z_1 \cup Z_2 | (Z_1 \in \mathcal{E}^A) \wedge (Z_2 \in \mathcal{F}^B) \wedge (Z_1 \cap B = Z_2 \cap A)\}$$

Διαισθητικά, η πράξη $\mathcal{E}^A \oplus \mathcal{F}^B$ ενοποιεί πιθανά σύνολα διαφθοράς από τα σύνολα $\mathcal{E}^A$ και $\mathcal{F}^B$ τα οποία 'συμφωνούν' στην τομή $A \cap B$. Στη συνέχεια, δείχνουμε ότι η πράξη $\oplus$ είναι αντιμεταθετική, προσεταιριστική και αυτοπαθής. Ένα απλό παράδειγμα της πράξης $\oplus$ απεικονίζεται στο Σχήμα 4.1.




Σχήμα 4.1: Υποθέτοντας ότι $Z_1, Z_3, Z_5 \in \mathcal{E}^A$ και $Z_2, Z_4, Z_6 \in \mathcal{F}^B$, παρατηρούμε ότι $\mathcal{E}^A \oplus \mathcal{F}^B$ πρέπει να περιέχει τα $Z_1 \cup Z_2, Z_3 \cup Z_4$ αλλά όχι το $Z_5 \cup Z_6$.

*Γεγονός.* Ένας ισοδύναμος ορισμός της πράξης $\oplus$ είναι ο παρακάτω:

$$\mathcal{E}^A \oplus \mathcal{F}^B = \{Z_1 \cup Z_2 \mid (Z_1 \in \mathcal{E}^A) \wedge (Z_2 \in \mathcal{F}^B) \wedge (Z_1 \cap B \subseteq Z_2) \wedge (Z_2 \cap A \subseteq Z_1)\}$$

Στη συνέχεια δείχνουμε κάποιες αλγεβρικές ιδιότητες της πράξης $\oplus$.

***Θεώρημα* 4.1**. *Η πράξη $\oplus$ είναι αντιμεταθετική.*

*Απόδειξη.*
Για δομές αντιπάλων $\mathcal{E}, \mathcal{F}$ και σύνολα κόμβων $A, B$:

$$\begin{aligned}\mathcal{E}^A \oplus \mathcal{F}^B &= \{Z_1 \cup Z_2 \mid (Z_1 \in \mathcal{E}^A) \wedge (Z_2 \in \mathcal{F}^B) \wedge (Z_1 \cap B = Z_2 \cap A)\} \\ &= \{Z_2 \cup Z_1 \mid (Z_2 \in \mathcal{F}^B) \wedge (Z_1 \in \mathcal{E}^A) \wedge (Z_2 \cap A = Z_1 \cap B)\} \\ &= \mathcal{F}^B \oplus \mathcal{E}^A\end{aligned}$$

Επομένως η πράξη $\oplus$ είναι αντιμεταθετική. □

***Θεώρημα* 4.2**. *Η πράξη $\oplus$ είναι αυτοπαθής.*

*Απόδειξη.*

$$\begin{aligned}\mathcal{E}^A \oplus \mathcal{E}^A &= \{Z_1 \cup Z_2 \mid (Z_1 \in \mathcal{E}^A) \wedge (Z_2 \in \mathcal{E}^A) \wedge (Z_1 \cap A = Z_2 \cap A)\} \\ &= \{Z_1 \cup Z_2 \mid (Z_1 \in \mathcal{E}^A) \wedge (Z_2 \in \mathcal{E}^A) \wedge (Z_1 = Z_2)\} \\ &= \{Z_1 | (Z_1 \in \mathcal{E}^A)\} \\ &= \mathcal{E}^A\end{aligned}$$

Επομένως η πράξη $\oplus$ είναι αυτοπαθής. □

***Θεώρημα* 4.3**. *Η πράξη $\oplus$ είναι προσεταιριστική.*

Η απόδειξη της προσεταιριστικότητας μπορεί να βρεθεί στο [PPS15].

Το επόμενο θεώρημα παρουσιάζει μια ιδιότητα της πράξης $\oplus$ ιδιαίτερα σημαντική για τη δουλειά μας.

***Θεώρημα* 4.4**. *Για δομές αντιπάλου $\mathcal{E}, \mathcal{F}$, σύνολα κόμβων $A, B$ και $\mathcal{H} = \mathcal{E}^A \oplus \mathcal{F}^B$, ισχύει ότι $\forall \mathcal{H}' \in \mathbb{T}^{A \cup B}$ : αν $\mathcal{H}'^A = \mathcal{E}^A$ και $\mathcal{H}'^B = \mathcal{F}^B$ τότε $\mathcal{H}' \subseteq \mathcal{H}$.*

*Απόδειξη.*
Υποθέτουμε ότι υπάρχει $\mathcal{H}'$ τέτοιο ώστε $\exists Z \in \mathcal{H}' : Z \notin \mathcal{H}$. Για $Z$ έχουμε $Z_1 = Z \cap A \in \mathcal{E}^A$ και $Z_2 = Z \cap B \in \mathcal{F}^B$. Επίσης $Z_1 \cap B = Z \cap A \cap B = Z_2 \cap A$. Αλλά τότε, ο Ορισμός 4.1 συνεπάγεται ότι $Z \in \mathcal{H}$, άτοπο. □

***Πόρισμα* 4.5**. *Για κάθε δομή αντιπάλου $\mathcal{Z}$ και σύνολο κόμβων $A, B$: $\mathcal{Z}^{(A \cup B)} \subseteq \mathcal{Z}^A \oplus \mathcal{Z}^B$.*

Το Πόρισμα 4.5 μας λέει ότι η πράξη $\oplus$ μας δίνει την μέγιστη (ως προς τον εγκλεισμό) πιθανή δομή αντιπάλου που είναι μη διακρίσιμη από δύο παίκτες που γνωρίζουν τα $\mathcal{Z}^A$ και $\mathcal{Z}^B$ αντίστοιχα, δηλαδή, που συμπέφτει με τη γνώση τους ως προς τη δομή αντιπάλου στα σύνολα $A$ και $B$ αντίστοιχα. Υπενθυμίζουμε ότι $\mathcal{Z}_u = \mathcal{Z}^{V(\gamma(u))}$. Θα προτιμήσουμε να χρησιμοποιούμε τον συμβολισμό $\mathcal{Z}_u$ για την τοπική δομή αντιπάλου ενός παίκτη $u$ και $\mathcal{Z}^{V(\gamma(u))}$ για να συμβολίζουμε τον αντίστοιχο περιορισμό της δομής αντιπάλου. Μπορούμε τώρα να

ορίσουμε την συνδυασμένη γνώση (*από κοινού γνώση*) ενός συνόλου κόμβων $B$ σχετικά με τη δομή αντιπάλου $\mathcal{Z}$ όπως φαίνεται στη συνέχεια. Για μια δομή αντιπάλου $\mathcal{Z}$, μια συνάρτηση γνώσης $\gamma$ και ένα σύνολο κόμβων $B$ ορίζουμε:

$$\mathcal{Z}_B = \bigoplus_{v \in B} \mathcal{Z}^{V(\gamma(v))}$$

Παρατηρούμε ότι το $\mathcal{Z}_B$ εκφράζει ακριβώς τη μέγιστη πιθανή δομή αντιπάλου, περιορισμένη στο $\gamma(B)$, που είναι σύμφωνη με την αρχική γνώση των παικτών στο $B$. Επίσης παρατηρούμε ότι από το Πόρισμα 4.5 έχουμε ότι $\mathcal{Z}^{V(\gamma(B))} \subseteq \mathcal{Z}_B$. Η ερμηνεία αυτού του εγκλεισμού στο πλαίσιό μας, είναι ότι αυτή η δομή που θεωρείται χειρότερη μη διακρίσιμη από τους παίκτες στο $B$, πάντα περιέχει την πραγματική δομή αντιπάλου.

## 4.3 Αξιόπιστη μετάδοση μηνύματος υπό μερική γνώση

Στο πρόβλημα RMT το ζητούμενο είναι η αποστολή ενός μηνύματος από τον διανομέα $D$ στον παραλήπτη $R$. Υποθέτουμε ότι ο διανομέας γνωρίζει την ταυτότητα του παραλήπτη $R$. Συμβολίζουμε ένα στιγμιότυπο του προβλήματος με την πεντάδα$(G, \mathcal{Z}, \gamma, D, R)$.Για να αναλύσουμε την επιλυσιμότητα του RMT εισάγουμε την έννοια του RMT-cut.

***Ορισμός* 4.2** (RMT-διαχωριστής). *Έστω $(G, \mathcal{Z}, \gamma, D, R)$ ένα στιγμιότυπο του RMT και $C = C_1 \cup C_2$ ένας διαχωριστής στο $G$, που χωρίζει το σύνολο $V \setminus C$ σε δύο σύνολα $A, B' \neq \emptyset$ όπου $D \in A$ και $R \in B'$. Έστω $B \subseteq B'$ το σύνολο κόμβων του συνδεδεμένου συστατικού του γραφήματος στο οποίο ανήκει ο $R$. Λέμε ότι το $C$ είναι ένας* RMT-διαχωριστής *αν και μόνον αν $C_1 \in \mathcal{Z}$ και $C_2 \cap V(\gamma(B)) \in \mathcal{Z}_B$.*

Στη συνέχεια αποδεικνύουμε ότι η μη ύπαρξη ενός RMT-διαχωριστή αποτελεί μια αναγκαία συνθήκη για την ύπαρξη ενός ασφαλούς RMT αλγορίθμου. Η απόδειξη συνδυάζει ιδέες από προηγούμενες αποδείξεις αναγκαιότητας με την πράξη $\oplus$ και ακολουθεί συνοπτικά.

***Θεώρημα* 4.6** (Αναγκαία συνθήκη). *Έστω $(G, \mathcal{Z}, \gamma, D, R)$ ένα στιγμιότυπο του RMT. Εάν υπάρχει RMT-διαχωριστής στο $G$ τότε δεν υπάρχει κανένας ασφαλής RMT αλγόριθμος ανεκτικός στο $(G, \mathcal{Z}, \gamma, D, R)$.*

*Απόδειξη.*
Έστω $C = C_1 \cup C_2$ ένας RMT-διαχωριστής που διαμερίζει το $V \setminus C$ στα σύνολα $A, B \neq \emptyset$ τ.ώ. $D \in A$ και $R \in B$. Χωρίς βλάβη της γενικότητας υποθέτουμε ότι το υπογράφημα που αντιστοιχεί στο σύνολο κόμβων $B$ είναι συνδεδεμένο. Εάν δεν είναι, τότε προσθέτοντας όλους τους κόμβους, που δεν ανήκουν στο συνδεδεμένο συστατικό που ανήκει ο $R$, στο $A$, προκύπτει ένας διαφορετικός RMT-διαχωριστής με τις επιθυμητές ιδιότητες. Θεωρούμε το στιγμιότυπο όπου $\mathcal{Z}' = \mathcal{Z}_B$ και όλες οι άλλες παράμετροι είναι οι ίδιες όπως στο αρχικό σενάριο. Τότε, όλοι οι κόμβοι στο $B$ έχουν την ίδια αρχική γνώση και στα δύο στιγμιότυπα, αφού $\mathcal{Z}_B = \mathcal{Z}'_B$.

Υποθέτουμε ότι ο $R$ μπορεί να αποφασίσει ορθά στην περίπτωση που το $\mathcal{Z}$ είναι η πραγματική δομή αντιπάλου. Τότε χρησιμοποιώντας το καθιερωμένο επιχείρημα με τις δύο εκτελέσεις που παρουσιάζεται στα προηγούμενα κεφάλαια, είναι πιθανή μια επίθεση στην ασφάλεια του αλγορίθμου και στην περίπτωση που το $\mathcal{Z}'$ είναι η πραγματική δομή αντιπάλου. Η κεντρική ιδέα είναι ότι κατασκευάζουμε δύο μη διακρίσιμα σενάρια, όπου η αρχική τιμή του διανομέα είναι διαφορετική. Οι λεπτομέρειες της απόδειξης είναι όμοιες με τις προηγούμενες αντίστοιχες αποδείξεις και στηρίζονται στην δυσκολία των τίμιων παικτών στο $B$ να διακρίνουν σε ποια εκτέλεση από τις δύο συμμετέχουν στην πραγματικότητα, ως προς τη δομή του αντιπάλου: αυτή με την δομή αντιπάλου $\mathcal{Z}$ ή αυτή με τη δομή $\mathcal{Z}'$. □

### 4.3.1 Ο RMT-Αλγόριθμος Μερικής Γνώσης (RMT- PKA)

Στην συνέχεια παρουσιάζουμε τον RMT-PKA, έναν RMT αλγόριθμο ο οποίος πετυχαίνει όποτε η συνθήκη του Θεωρήματος 4.6 (στην πραγματικότητα,η άρνησή της) ικανοποιείται. Αυτό το αποτέλεσμα καθιστά την συνθήκη αναγκαία και ικανή για την επιλυσιμότητα του RMT από ασφαλής αλγορίθμους. Για να αποδείξουμε το παραπάνω παρέχουμε κάποιες βοηθητικές έννοιες.

**Μηνύματα που ανταλλάσσονται στο Πρωτόκολλο 4.** Στο πρωτόκολλο RMT-PKA υπάρχουν δύο είδη μηνυμάτων που ανταλλάσσονται:

- Τα *μηνύματα τύπου 1* χρησιμοποιούνται για την διάδοση της τιμής του διανομέα και είναι της μορφής $(x, p)$ όπου $x \in X$ και το $p$ είναι ένα μονοπάτι.
- Τα *μηνύματα τύπου 2* που είναι της μορφής $((v, \gamma(v), \mathcal{Z}_v), p)$χρησιμοποιούνται για να διαδώσει ο κάθε κόμβος $v$ την αρχική του γνώση $\gamma(v), \mathcal{Z}_v$ σε όλο το γράφημα.

Έστω $M$ ένα υποσύνολο των μηνυμάτων τύπου 1 και 2 που λαμβάνει ο παραλήπτης $R$ σε κάποιο γύρο της εκτέλεσης του πρωτοκόλλου στο στιγμιότυπο $(G, \mathcal{Z}, \gamma, D, R)$. Θα γράφουμε $value(M) = x$ αν και μόνον αν όλα τα τύπου 1 μηνύματα του $M$ αναφέρουν την ίδια τιμή $x$ για τον διανομέα, δηλαδή, για κάθε μήνυμα $(y, p)$, ισχύει ότι $y = x$, για κάποιο $x \in X$. Παρατηρούμε ότι το $M$ μπορεί να αποτελείται από μηνύματα που περιέχουν αντιφατική πληροφορία. Στη συνέχεια ορίζουμε τη μορφή ενός συνόλου μηνυμάτων $M$ που δεν περιέχει αντιφατική πληροφορία στο πλαίσιο που εργαζόμαστε (ένα έγκυρο σύνολο $M$).

***Ορισμός* 4.3** (Έγκυρο σύνολο $M$). *Ένα σύνολο $M$ μηνυμάτων τύπων 1 και 2* αντιστοιχεί σε ένα έγκυρο σενάριο,*ή απλούστερα είναι* έγκυρο, *αν*

- $\exists x \in X$ *τ.ώ.* $value(M) = x$. *Αυτό σημαίνει ότι όλα τα μηνύματα τύπου 1 αναμεταδίδουν την ίδια τιμή $x$ως την τιμή του διανομέα.*
- $\forall m_1, m_2 \in M$ *τύπου 2,το πρώτο τους συστατικό είναι το ίδιο όταν αναφέρονται στον ίδιο κόμβο. Δηλαδή, αν* $m_1 = ((v, \gamma(v), \mathcal{Z}_v), p)$ *και* $m_2 = (((v', \gamma'(v), \mathcal{Z}'_v), p')$, *τότε το* $v = v'$ *συνεπάγεται ότι* $\gamma(v) = \gamma'(v)$ *και* $\mathcal{Z}_v = \mathcal{Z}'_v$.

Για κάθε έγκυρο $M$ μπορούμε να ορίσουμε το ζεύγος $(G_M, x_M)$ όπου $x_M = value(M)$. Για να ορίσουμε το $G_M$ υποθέτουμε ότι το $V_M$ είναι το σύνολο των κόμβων $u$ για τους οποίους η πληροφορία $\gamma(u), \mathcal{Z}_u$ περιέχεται στο $M$, συγκεκριμένα $V_M = \{v \mid ((v, \gamma(v), \mathcal{Z}_v), p) \in M$ για κάποιο μονοπάτι $p\}$. Τότε, το $G_M$ το επαγόμενο υπογράφημα του $\gamma(V_M)$ στο σύνολο κόμβων $V_M$. Επομένως, ένα έγκυρο σύνολο $M$ προσδιορίζει μοναδικά το ζεύγος $(G_M, x_M)$. Στη συνέχεια προτείνουμε δύο έννοιες που χρησιμοποιούμε για να ελέγξουμε αν ένα έγκυρο σύνολο $M$ περιέχει ορθή πληροφορία.

***Ορισμός* 4.4** (Πλήρες σύνολο μηνυμάτων). *Ένα* πλήρες *σύνολο μηνυμάτων $M$ είναι ένα έγκυρο σύνολο $M$ που περιέχει όλα τα $D - R$ μονοπάτια που εμφανίζονται στο $G_M$ σαν τμήμα των μηνυμάτων τύπου 1.*

***Ορισμός* 4.5** (Κάλυμμα αντιπάλου του συνόλου $M$). *Ένα σύνολο $C \subseteq V_M$ είναι ένα* κάλυμμα αντιπάλου *του συνόλου μηνυμάτων $M$ αν έχει την ακόλουθη ιδιότητα: το $C$ είναι ένας διαχωριστής μεταξύ των $D, R$ στο $G_M$ και αν $B$ είναι το σύνολο κόμβων του συνδεδεμένου συστατικού στο οποίο ανήκει ο $R$, τότε ισχύει ότι $(C \cap V(\gamma(B))) \in \mathcal{Z}_B$.*

---

**Πρωτόκολλο 4**: ***RMT-PKA***

---

*Είσοδος* (Για κάθε κόμβο $v$):αναγνωριστικό του διανομέα $D$, $\gamma(v)$, $\mathcal{Z}_v$.
*Μορφή μηνυμάτων*: τύπος 1: ζεύγος $(x, p)$ ή τύπος 2: ζεύγος $((u, \gamma(u), \mathcal{Z}_u), p)$, όπου $x \in X$ (χώρος μηνυμάτων), $u$ είναι το αναγνωριστικό κάποιου κόμβου, $\gamma(u)$ είναι η αρχική γνώση του $u$, $\mathcal{Z}_u$ είναι η τοπική δομή αντιπάλου του $u$, και $p$ είναι ένα μονοπάτι του $G$ (μονοπάτι διάδοσης μηνύματος).

**Κώδικας για τον** $D$: στείλε τα μηνύματα $(value : x_D, \{D\})$ και $((D, \gamma(D), \mathcal{Z}_D), \{D\})$ σε όλους τους γείτονες και τερμάτισε.

**Κώδικας για τον** $v \notin \{D, R\}$: στείλε το μήνυμα $((v, \gamma(v), \mathcal{Z}_v), \{v\})$ σε όλους τους γείτονες.
Μετά την παραλαβή ενός μηνύματος $(a, p)$ τύπου 1 ή 2 από τον κόμβο $u$ κάνε:

Αν $(v \in p) \vee (tail(p) \neq u)$[2] τότε απέριψε $(a, p)$ αλλιώς στείλε $(a, p||v)$ [3] σε όλους τους γείτονες.

**Κώδικας για τον** $R$: Μετά την παραλαβή του μηνύματος $(x, p)$ από τον $u$ κάνε:

αν απόφαση$\neq \perp$ τότε αποφάσισε στο απόφαση και τερμάτισε.

**Υπορουτίνα απόφαση**

(* *Κανόνας διάδοσης διανομέα* *)

αν $R \in \mathcal{N}(D)$ και ο $R$ λαμβάνει $(x_D, \{D\})$ τότε επέστρεψε $x_D$.

[2]Χρησιμοποιούμε το $tail(p)$ για να συμβολίσουμε τον τελευταίο κόμβο του μονοπατιού $p$. Ελέγχοντας αν $tail(p) \neq u$ εξασφαλίζουμε ότι τουλάχιστον ένας διεφθαρμένος κόμβος θα συμπεριληφθεί σε ένα μονοπάτι που διαδίδει μια εσφαλμένη τιμή.

[3]Με το $p||v$ συμβολίζουμε την παράθεση ενός κόμβου $v$ στο μονοπάτι $p$ $v$.

(* *κανόνας διάδοσης πλήρους συνόλου μονοπατιών* *)
αν ο $R$ λαμβάνει ένα πλήρες σύνολο $M$ με $value(M) = x$ και $\nexists$ ένα κάλυμμα αντιπάλου για το $M$

τότε επέστρεψε $x$ αλλιώς επέστρεψε $\perp$.

---

Στη συνέχεια δείχνουμε την μη αναμενόμενη ιδιότητα ασφάλειας του RMT-PKA, δηλαδή, ότι ο παραλήπτης δεν θα αποφασίσει ποτέ σε μια εσφαλμένη τιμή παρά τις αυξημένες δυνατότητες επίθεσης του αντιπάλου, οι οποίες συμπεριλαμβάνουν την αναφορά μη υπαρκτών κόμβων και γενικότερα ψευδούς τοπολογικής γνώσης.

***Θεώρημα* 4.7** (RMT-PKA Safety). *Ο RMT-PKA είναι ασφαλής αλγόριθμος.*

*Απόδειξη.*

Είναι προφανές ότι ο παραλήπτης $R$ δεν θα αποφασίσει σε μια λανθασμένη τιμή χρησιμοποιώντας τον κανόνα διάδοσης διανομέα (στην περίπτωση δηλαδή που $R \in \mathcal{N}(D)$) λόγω της υπόθεσης της εντιμότητας του διανομέα. Το δύσκολο κομμάτι της απόδειξης είναι να δείξουμε ότι ο παραλήπτης $R$ δεν θα αποφασίσει σε καμία τιμή $x \neq x_D$ χρησιμοποιώντας τον κανόνα διάδοσης πλήρους συνόλου μονοπατιών (στην περίπτωση που $R \notin \mathcal{N}(D)$). Έστω $T \in \mathcal{Z}$ ένα οποιοδήποτε πιθανό σύνολο διεφθαρμένων παικτών και έστω η εκτέλεση $e_T$ του RMT-PKA όπου $T$ είναι το πραγματικό σύνολο διαφθορών. Υποθέτουμε ότι σε κάποιο γύρο της εκτέλεσης $e_T$, ο $R$ λαμβάνει ένα πλήρες σύνολο $M'$ με $value(M') = x \neq x_D$. Αφού τα $D - R$ μονοπάτια του $G_{M'}$ διαδίδουν μια λανθασμένη τιμή $x$ σημαίνει ότι το $C = T \cap V_{M'}$ δημιουργεί έναν $D-R$ διαχωριστή στο γράφημα $G_{M'}$, αλλιώς θα υπήρχε ένα $D-R$ μονοπάτι στο $G_{M'}$ αποτελούμενο μόνο από τίμιους κόμβους που θα διέδιδε την τιμή $x_D$, αντίφαση γιατί $value(M') = x$. Εφόσον $C \in \mathcal{Z}$, ισχύει από τον ορισμό ότι $C \cap V(\gamma(S)) \in \mathcal{Z}_S,\ \forall S \subseteq V(G)$. Επομένως αν $B$ είναι το συνδεδεμένο συστατικό στο οποίο ανήκει ο $R$ υπό την διαμέριση που δημιουργεί ο διαχωριστής $C$ στο $G_{M'}$, ισχύει ότι $C \cap V(\gamma(B)) \in \mathcal{Z}_B$ λόγω του ότι το σύνολο $B$ περιέχει μόνο τίμιους κόμβους; πιο συγκεκριμένα, το $B$ δεν περιέχει κανέναν διεφθαρμένο κόμβο λόγω του ορισμού του $C$. Επιπλέον, ο αντίπαλος δεν μπορεί να εισάγει μη υπαρκτούς κόμβους στο $B$ γιατί το $T$ πρέπει να είναι ένας διαχωριστής μεταξύ του $R$ και κάθε μη υπαρκτού κόμβου που ισχυρίζεται ο αντίπαλος ότι υπάρχει. Οι τελευταίες παρατηρήσεις για το $B$ υπονοούν ότι ο $R$ μπορεί να υπολογίζει ορθά το $\mathcal{Z}_B$. Άρα, το $M'$ έχει ένα κάλυμμα αντιπάλου και ο $R$ δεν θα αποφασίσει σε μια τιμή $x \neq x_D$ μέσω του κανόνα διάδοσης πλήρους συνόλου μονοπατιών. □

***Θεώρημα* 4.8** (Ικανή συνθήκη). *Έστω $(G, \mathcal{Z}, \gamma, D, R)$ ένα στιγμιότυπο RMT. Αν δεν υπάρχει ένας RMT-διαχωριστής, τότε ο RMT-PKA πετυχαίνει RMT.*

*Απόδειξη.*
Παρατηρούμε ότι αν $R \in \mathcal{N}(D)$ τότε ο $R$ τετριμμένα αποφασίζει στο $x_D$ λόγω του *κανόνα*

*διάδοσης του διανομέα*, αφού ο διανομέας είναι τίμιος. Υποθέτοντας ότι δεν υπάρχει ένας RMT-διαχωριστής, θα δείξουμε ότι αν $R \notin \mathcal{N}(D)$ τότε ο $R$ θα αποφασίσει στην τιμή $x_D$ λόγω του *κανόνα διάδοσης πλήρους συνόλου μονοπατιών.*

Έστω $T \in \mathcal{Z}$ ένα πιθανό σύνολο διαφθορών και μια εκτέλεση $e_T$ του RMT-PKA όπου $T$ είναι το πραγματικό σύνολο διαφθοράς. Έστω $P$ το σύνολο μονοπατιών που συνδέουν τον $D$ με τον $R$ και αποτελούνται αποκλειστικά από κόμβους στο $V(G) \setminus T$ (τίμιους κόμβους). Παρατηρούμε ότι $P \neq \emptyset$, αλλιώς το $T$ είναι ένας διαχωριστής που χωρίζει τον $D$ από τον $R$ και είναι τετριμμένα ένας RMT-διαχωριστής, άτοπο.

Αφού τα μονοπάτια του $P$ αποτελούνται αποκλειστικά από τίμιους κόμβους, είναι προφανές ότι μέχρι το τέλος του γύρου $|V(G)|$, ο $R$ θα λάβει την τιμή $x_D$ μέσω όλων των μονοπατιών στο $P$ λαμβάνοντας το αντίστοιχο σύνολο τύπου 1 μηνυμάτων $M_1$. Επιπλέον, μέχρι τον γύρο $|V(G)|$, ο $R$ το σύνολο μηνυμάτων τύπου 2 $M_2$ το οποίο περιλαμβάνει πληροφορία για όλους τους κόμβους που συνδέονται με τον $R$ μέσω μονοπατιών που δεν περνάνε από κόμβους στο $T$. Αυτό περιλαμβάνει όλους τους κόμβους των μονοπατιών του συνόλου $P$. Συνεπώς, ο $R$ θα λάβει το πλήρες σύνολο μηνυμάτων $M = M_1 \cup M_2$ με $value(M) = x_D$.

Στη συνέχεια δείχνουμε ότι δεν υπάρχει κάλυμμα αντιπάλου για το $M$ και επομένως ο $R$ θα αποφασίσει στην τιμή $x_D$ μέσω του κανόνα διάδοσης του πλήρους συνόλου μονοπατιών $M$. Υποθέτουμε ότι υπάρχει ένα κάλυμμα αντιπάλου $C$ για το $M$. Αυτό, εξορισμού σημαίνει ότι το $C$ είναι ένας διαχωριστής μεταξύ των $D, R$ στο γράφημα $G_M$ και αν $B$ είναι το σύνολο κόμβων του συνδεδεμένου συστατικού στο οποίο ανήκει ο $R$, ισχύει ότι και το $(C \cap V(\gamma(B))) \in \mathcal{Z}_B$ (παρατηρούμε ότι ο $R$ μπορεί να υπολογίσει το $\mathcal{Z}_B$ χρησιμοποιώντας την πληροφορία που περιέχεται στο $M_2$ όπως ορίστηκε στην προηγούμενη παράγραφο). Τότε προφανώς το $T \cup C$ είναι ένας διαχωριστής στο $G$ που χωρίζει τον $D$ από τον $R$, αφού κάθε μονοπάτι του $G$ που συνδέει τον $D$ με τον $R$ περιέχει τουλάχιστον έναν κόμβο στο $T \cup C$. Έστω ο διαχωριστής $T \cup C$ που διαμερίζει το σύνολο $V(G) \setminus \{T \cup C\}$ στα σύνολα $A, B$ τέτοια ώστε $D \in A$. Τότε σαφώς το $T \cup C$ είναι ένας RMT διαχωριστής εξορισμού,άτοπο. Επομένως δεν υπάρχει ένα κάλυμμα αντιπάλου για το $M$ και ο $R$θα αποφασίσει στην τιμή $x_D$.

Επιπλέον, αφού ο RMT-PKA είναι ασφαλής, ο παραλήπτης δεν θα αποφασίσει σε καμία τιμή διαφορετική του $x_D$.

□

***Πόρισμα* 4.9** (Μοναδικότητα). *Ο RMT-PKA είναι μοναδικός μεταξύ ασφαλών αλγορίθμων, δηλαδή, δοθέντος ενός στιγμιότυπου RMT $(G, \mathcal{Z}, \gamma, D, R)$, εάν υπάρχει οποιοσδήποτε RMT αλγόριθμος ο οποίος είναι ανεκτικός για αυτό το στιγμιότυπο, τότε ο RMT-PKA επίσης πετυχαίνει RMT σε αυτό το στιγμιότυπο.*

## 4.4 RMT σε *ad hoc* δίκτυα

Σε αυτήν την ενότητα μελετάμε το πρόβλημα RMT σε *ad hoc* δίκτυα. Στο συγγενές πρόβλημα της Αξιόπιστης Εκπομπής με τίμιο διανομέα (ή απλώς πρόβλημα Εκπομπής) ο παραλήπτης

δεν είναι ένας μόνο κόμβος αλλά αντ'αυτού ολόκληρο το σύνολο των παικτών $V(G)$. Το πρόβλημα της Εκπομπής σε *ad hoc* δίκτυα υπό την παρουσία ενός γενικού αντιπάλου αρχικά μελετήθηκε στην Ενότητα 3.6.2 όπου παρουσιάστηκε ένας αλγόριθμος για αυτό το μοντέλο παρουσιάστηκε και αποδείχθηκε ότι είναι μοναδικός. Τα αποτελέσματα μπορούν τετριμμένα να προσαρμοστούν στην περίπτωση του προβλήματος RMT.

Ένα στιγμιότυπο του RMT στο *ad hoc* μοντέλο αποτελείται από μία τετράδα $(G, \mathcal{Z}, D, R)$ όπως παρουσιάζεται στην προηγούμενη ενότητα. Όσον αφορά το συγγενές πρόβλημα της Εκπομπής που μελετήθηκε στα προηγούμενα κεφάλαια, παρουσιάστηκε η έννοια του $\mathcal{Z}$*-pp διαχωριστή*και αποδείχθηκε ότι μία ικανή και αναγκαία συνθήκη για την επιλυσιμότητα του προβλήματος είναι ότι δεν υπάρχει ένας $\mathcal{Z}$-pp διαχωριστής στο στιγμιότυπο. Επιπλέον, το πρωτόκολλο $\mathcal{Z}$-CPA ($\mathcal{Z}$-αλγόριθμος πιστοποιημένης διάδοσης) παρουσιάστηκε και αποδείχθηκε ότι πετυχαίνει Εκπομπή σε κάθε στιγμιότυπο που το πρόβλημα είναι επιλύσιμο, δηλαδή, αποδείχθηκε η μοναδικότητά του.

Αφού στο πρόβλημα RMT ασχολούμαστε μόνο με την απόφαση του παραλήπτη $R$, παρουσιάζουμε μια μικρή τροποποίηση του $\mathcal{Z}$-pp διαχωριστή για να περιγράψουμε έναν ανάλογο διαχωριστή ($RMT$ $\mathcal{Z}$*-pp διαχωριστής*) ανάμεσα στον διανομέα $D$ και τον παραλήπτη $R$,

***Ορισμός* 4.6** ($RMT$ $\mathcal{Z}$-pp διαχωριστής). *Έστω $C$ ένας διαχωριστής του $G$ που διαμερίζει το $V \setminus C$ στα σύνολα $A, B \neq \emptyset$ τέτοια ώστε, $D \in A$ και $R \in B$. Το $C$ είναι ένας $RMT$ $\mathcal{Z}$-pp διαχωριστής αν υπάρχει μια διαμέριση $C = C_1 \cup C_2$ με $C_1 \in \mathcal{Z}$ και $\forall u \in B$, $\mathcal{N}(u) \cap C_2 \in \mathcal{Z}_u$.*

Ο αλγόριθμος $\mathcal{Z}$-CPA μπορεί να τροποποιηθεί τετριμμένα για την επίλυση του προβλήματος RMT. Σε αυτόν τον αλγόριθμο, αρχικά ο διανομέας στέλνει την αρχική του τιμή $x_D$ σε όλους τους γείτονές του και τερματίζει. Μετά από αυτό το βήμα, οι ενέργειες οποιουδήποτε παίκτη $v$ ορίζονται ακολούθως.

**RMT $\mathcal{Z}$-CPA κώδικας για τον $v \neq D$**

1. Αν $v \in \mathcal{N}(D)$ τότε μετά την παραλαβή της τιμής $x_D$ από τον διανομέα, αποφάσισε στην τιμή $x_D$.
2. Αν $v \notin \mathcal{N}(D)$ μετά την παραλαβή της ίδιας τιμής $x$από όλους τους γείτονες σε ένα σύνολο $N \subseteq \mathcal{N}(v)$ τέτοιο ώστε $N \notin \mathcal{Z}_v$, αποφάσισε στην τιμή $x$.
3. Αν $v = R$ και έχει αποφασίσει στο $x$ τότε δώσε έξοδο με τιμή $x$ και τερμάτισε, αλλιώς αν $v \neq R$ και έχει αποφασίσει στην τιμή $x$, στείλε $x$ σε όλους τους γείτονες $\mathcal{N}(v)$ και τερμάτισε.

Παρατηρούμε ότι ο $\mathcal{Z}$-CPA είναι ασφαλής αλγόριθμος, με την έννοια ότι, δεν προκαλεί ποτέ μια λανθασμένη απόφαση σε κάποιον παίκτη. Ακολουθώντας πανομοιότυπη ανάλυση με αυτή του προηγούμενου κεφαλαίου, όπου ο $\mathcal{Z}$-CPA αποδείχθηκε μοναδικός μεταξύ ασφαλών αλγορίθμων Εκπομπής, αποδεικνύεται η μοναδικότητα του $\mathcal{Z}$-CPA (τροποποιημένου όπως εξηγήθηκε) μεταξύ ασφαλών $RMT$ αλγορίθμων. Τα επόμενα θεωρήματα είναι ακριβώς ανάλογα

με αυτά που αποδεικνύουν την μοναδικότητα του $\mathcal{Z} - CPA$ για το πρόβλημα της Εκπομπής και οι αποδείξεις είναι ουσιαστικά πανομοιότυπες.

***Θεώρημα* 4.10** (Ικανή Συνθήκη). *Δοθέντος ενός στιγμιότυπου RMT $(G, \mathcal{Z}, D, R)$, αν δεν υπάρχει ένας $RMT$ $\mathcal{Z}$-pp διαχωριστής στο $G$, τότε ο $\mathcal{Z}$-CPA πετυχαίνει RMT στο $(G, \mathcal{Z}, D, R)$.*

***Θεώρημα* 4.11** (Necessary Condition). *Given an RMT instance $(G, \mathcal{Z}, D, R)$, if an $RMT$ $\mathcal{Z}$-pp cut exists on $G$ then no safe RMT algorithm exists for $(G, \mathcal{Z}, D, R)$.*

Επομένως, ο $\mathcal{Z}$-CPA, ο πρώτος αλγόριθμος που έχουμε συναντήσει για το πρόβλημα RMT σε γενικής τοπολογίας *ad hoc* δίκτυα υπό την παρουσία ενός γενικού αντιπάλου, αποδεικνύεται ότι είναι μοναδικός μεταξύ ασφαλών αλγορίθμων.

## 4.5 Μοναδικότητα πρωτοκόλλου ως προς την αποδοτικότητα

Μέχρι τώρα, έχουμε δει ότι ο $\mathcal{Z}$-CPA είναι μοναδικός μεταξύ ασφαλών *ad hoc* RMT αλγορίθμων. Ως προς την αποδοτικότητα, είναι ενδιαφέρον να εξετάσουμε αν ο $\mathcal{Z}$-CPA είναι επίσης και ο πιο αποδοτικός μεταξύ μοναδικών RMT αλγορίθμων ως προς πολυωνυμικές παραμέτρους. Θα ασχοληθούμε με την πολυπλοκότητα του πρωτοκόλλου ως προς το μέγεθος του γραφήματος $|G| = n$ μόνο, επειδή κυρίως ενδιαφερόμαστε για πρωτόκολλα *πλήρως πολυωνυμικά* (με πολυωνυμική πολυπλοκότητα γύρων, επικοινωνίας και τοπικών υπολογισμών) ανεξάρτητα από το μέγεθος της δομής του αντιπάλου. Παρατηρούμε ότι, αν η δομή αντιπάλου δίνεται ρητά τότε, ο $\mathcal{Z}$-CPA είναι τετριμμένα *πλήρως πολυωνυμικός* ως προς το συνολικό μέγεθος του στιγμιότυπου. Εντούτοις το $\mathcal{Z}$ μπορεί να είναι εκθετικού μεγέθους ως προς το $|G|$. Ο Υπολογισμός της πολυπλοκότητας του $\mathcal{Z}$-CPA δεν μπορεί να γίνει απευθείας αφού οι υπολογισμοί που εμπεριέχονται στο πρωτόκολλο δεν είναι ρητά ορισμένοι. Στην πραγματικότητα, ο $\mathcal{Z}$-CPA είναι ένα *σχήμα πρωτοκόλλων* που αναφέρεται σε μια "λειτουργικά ορισμένη" υπορουτίνα παρά σε μια συγκεκριμένη υλοποίηση αυτής της υπορουτίνας. Θα χρησιμοποιήσουμε τις ακόλουθες έννοιες για για να διευκολύνουμε την μελέτη μας σε κατανεμημένα σχήματα πρωτοκόλλων.

Αρχικά ορίζουμε την έννοια ενός σχήματος πρωτοκόλλων για το πρόβλημα $Q$; ουσιαστικά, αν ένα σχήμα πρωτοκόλλων $\mathcal{A}$ επιλύει το πρόβλημα $Q$ μέσω μιας υπορουτίνας που επιλύει το πρόβλημα $S$, τότε το $\mathcal{A}$ είναι μια αναγωγή από το $Q$ στο $S$ στο κατανεμημένο μοντέλο.

***Ορισμός* 4.7** (Protocol scheme). *Ένα* σχήμα πρωτοκόλλων $\mathcal{A}$ *είναι μια οικογένεια πρωτοκόλλων που περιέχει κλήσεις σε μια υπορουτίνα $X$ για την επίλυση ενός προβλήματος $S$. Ο υπολογισμός της $X$ δεν είναι ορισμένος, δηλαδή, η $X$ χρησιμοποιείται σαν μαύρο κουτί (black box). Επομένως, για κάθε αλγόριθμο $B$που επιλύει το πρόβλημα $S$ ένα διαφορετικό μέλος (πρωτόκολλο) $\mathcal{A}_B$ της $\mathcal{A}$ ορίζεται· δηλαδή, το $\mathcal{A}_B$ υλοποιεί την υπορουτίνα $X$ μέσω του αλγορίθμου $B$.*

**Πλήρως πολυωνυμικό σχήμα πρωτοκόλλων**. Λέμε ότι ένα *σχήμα πρωτοκόλλων* $\mathcal{A}$ *είναι πλήρως πολυωνυμικό* εάν υπάρχει αλγόριθμος $B$, που επιλύει το $S$, για τον οποίο το $\mathcal{A}_B$ είναι πλήρως πολυωνυμικό.

Παρατηρούμε ότι ο $\mathcal{Z}$-CPA είναι ένα σχήμα πρωτοκόλλων το οποίο περιλαμβάνει μια υπορουτίνα ελέγχου συμμετοχής (membership check) ($N \notin \mathcal{Z}_v$) που παρουσιάζεται στον δεύτερο κανόνα. Αναφορικά με την αποδοτικότητα του $\mathcal{Z}$-CPA, μπορούμε εύκολα να παρατηρήσουμε ότι είναι πολυωνυμικής πολυπλοκότητας γύρων και επικοινωνίας (λεπτομέρειες για αυτό παρουσιάζονται στην απόδειξη του Θεωρήματος 4.12). Για να επιχειρηματολογήσουμε σχετικά με την πολυπλοκότητα τοπικών υπολογισμών του σχήματος πρέπει να λάβουμε υπόψιν μας την πολυπλοκότητα της υπορουτίνας ελέγχου συμμετοχής. Πράγματι, το σχήμα $\mathcal{Z}$-CPA είναι πλήρως πολυωνυμικό εάν υπάρχει ένας αλγόριθμος $B$ μέσω του οποίου ο έλεγχος συμμετοχής εκτελείται σε πολυωνυμικό χρόνο σε σχέση με το μέγεθος του γραφήματος $|G|$. Στη συνέχεια εισάγουμε την έννοια της *μοναδικότητας πολυωνυμικού χρόνου*· ένα σχήμα πρωτοκόλλων που είναι πολυωνυμικά μοναδικό για κάποιο πρόβλημα, είναι με κάποια έννοια, βέλτιστα αποδοτικό ως προς πολυωνυμικούς παράγοντες.

***Ορισμός* 4.8** (Μοναδικότητα πολυωνυμικού χρόνου). *Καλούμε ένα σχήμα πρωτοκόλλων* $\mathcal{A}$ πολυωνυμικά μοναδικό *για κάποιο πρόβλημα* $\mathcal{P}$ *αν είναι μοναδικό (ως προς την επιλυσιμότητα) και η ύπαρξη ενός μοναδικού πλήρως πολυωνυμικού πρωτοκόλλου για το* $\mathcal{P}$ *συνεπάγεται ότι το* $\mathcal{A}$ *είναι επίσης πλήρως πολυωνυμικό για το* $\mathcal{P}$.

Με άλλα λόγια, είτε το $\mathcal{A}$ είναι πλήρως πολυωνυμικό πρωτόκολλο (σε όλα τα επιλύσιμα στιγμιότυπα) είτε δεν υπάρχει κανένας πλήρως πολυωνυμικός αλγόριθμος $\Pi$ που λύνει το $\mathcal{P}$ σε όλα τα επιλύσιμα στιγμιότυπα. Σχετικά με την έννοια της αναγωγής, η έννοια της μοναδικότητας πολυωνυμικού χρόνου ενός σχήματος πρωτοκόλλων $\mathcal{A}$ υπονοεί ότι το σχήμα $\mathcal{A}$ μπορεί να χρησιμοποιηθεί σαν αυτοαναγωγή του προβλήματος, όπως θα καταστεί σαφές στη συνέχεια.

Πιστεύουμε ότι η έννοια της μοναδικότητας πολυωνυμικού χρόνου είναι γενικότερου ενδιαφέροντος, αφού μπορεί να χρησιμοποιηθεί για να μελετηθεί το κατά πόσο ένα σχήμα πρωτοκόλλων είναι βέλτιστο ως προς την αποδοτικότητα και την αναγνώριση σημαντικών υποπροβλημάτων που είναι κρίσιμα για την επίλυση του αρχικού προβλήματος.

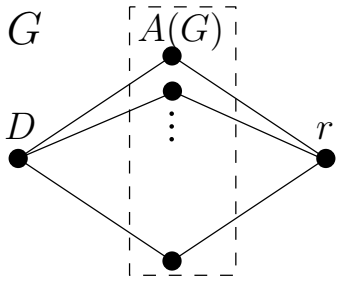
Στο κεντρικό θεώρημα αυτής της ενότητας αποδεικνύουμε ότι ρο σχήμα $\mathcal{Z}$-CPA είναι πολυωνυμικά μοναδικό για το πρόβλημα RMT, και έτσι δείχνουμε ότι το $\mathcal{Z}$-CPA σχήμα είναι τουλάχιστον όσο αποδοτικό, ως προς πολυωνυμικούς παράγοντες, όσο οποιοδήποτε άλλο RMT σχήμα πρωτοκόλλων. Για να το δείξουμε αυτό, κατασκευάζουμε μία αυτοαναγωγή του RMT βασισμένη στον $\mathcal{Z}$-CPA. Ουσιαστικά δείχνουμε ότι αν υπάρχει ένα μοναδικό, πλήρως πολυωνυμικό RMT πρωτόκολλο, τότε αυτό θα απαντάει και στον έλεγχο συμμετοχής σε πολυωνυμικό χρόνο ως προς το $|G|$ και επομένως μπορεί να χρησιμοποιηθεί σαν υπορουτίνα για να γίνει ο $\mathcal{Z}$-CPA πλήρως πολυωνυμικός.

## 4.6 Self-reducibility of RMT

Θεωρούμε την οικογένεια των στιγμιοτύπων $\mathcal{G}$ όπου είναι επιλύσιμο το RMT. Από τα θεωρήματα 4.10,4.11 έχουμε:

$$\mathcal{G} = \{(G, \mathcal{Z}, D, R) \mid \nexists RMT\ \mathcal{Z}\text{-pp cut in } G\ \}$$

Επίσης θεωρούμε την οικογένεια των *βασικών* στιγμιοτύπων $\mathcal{G}' \subseteq \mathcal{G}$ η οποία περιέχει τα στιγμιότυπα $(G, \mathcal{Z}, D, R)$ όπου το RMT είναι επιλύσιμο και το γράφημα $G$ είναι της μορφής που φαίνεται στο Σχήμα 4.2. Πιο συγκεκριμένα, το $G$ περιέχει δύο διαφορετικούς κόμβους $D, R$ και ένα "μεσαίο σύνολο" κόμβων το οποίο συμβολίζουμε με $A(G)$. Οι μόνες ακμές του $G$ είναι αυτές κάθε παίκτη στο σύνολο $A(G)$ με τον διανομέα $D$ και τον παραλήπτη $R$· επίσης, στο γράφημα που προκύπτει δεν υπάρχει $RMT\ \mathcal{Z}$-pp διαχωριστής. Τέλος, για κάθε $\mathcal{G}_1 \subseteq \mathcal{G}$




Σχήμα 4.2: Οικογένεια των στιγμιοτύπων $\mathcal{G}'$. Δεν υπάρχει $RMT\ \mathcal{Z}$-pp διαχωριστής.

ορίζουμε την οικογένεια των στιγμιοτύπων $\mathcal{I}(\mathcal{G}_1) \subseteq \mathcal{G}'$ η οποία αποτελείται από όλα τα στιγμιότυπα $(G', \mathcal{Z}', D', R') \in \mathcal{G}'$ τέτοια ώστε το μεσαίο σύνολο $A(G')$ του γραφήματος $G'$ είναι ένα υποσύνολο της γειτονιάς ενός κόμβου $v$ σε ένα γράφημα που περιέχεται στην οικογένεια $\mathcal{G}_1$, σαν τμήμα του στιγμιότυπου $(G, \mathcal{Z}, D, R)$, και $\mathcal{Z}' = \mathcal{Z}_v$ [4]. Ακριβέστερα,

$$\mathcal{I}(\mathcal{G}_1) = \{(G', \mathcal{Z}', D', R') \in \mathcal{G}' \mid \exists (G, \mathcal{Z}, D, R) \in \mathcal{G}_1,\ \exists v \in V(G) \setminus \{D\}, A(G') \subseteq \mathcal{N}(v), \mathcal{Z}' = \mathcal{Z}_v\}$$

Διαισθητικά, η παραπάνω οικογένεια δημιουργείται από την αποσύνθεση κάθε γραφήματος $G$ στην οικογένεια $\mathcal{G}_1$ σε "βασικά" γραφήματα της οικογένειας $\mathcal{G}'$ των οποίων τα μεσαία σύνολα εμφανίζονται στο $G$ σαν γειτονιές (ή τμήματα αυτών) των κόμβων, οι δομές αντιπάλου είναι υποσύνολα των αρχικών δομών, και το πρόβλημα RMT είναι επιλύσιμο.

[4] Σε αυτό το σημείο κάνουμε μια μικρή κατάχρηση της ορολογίας, για ευκολία της παρουσίασης, και χρησιμοποιούμε $\mathcal{Z}' = \mathcal{Z}_v$ αντί για $\mathcal{Z}' = \{S \cap A(G') \mid S \in \mathcal{Z}_v\}$. Η δεύτερη έκφραση είναι πιο ακριβής στην περίπτωση όπου $A(G') \subsetneq \mathcal{N}(v)$ γιατί έχουμε ορίσει το $\mathcal{Z}$ σαν υποσύνολο του δυναμοσυνόλου των κόμβων του στιγμιότυπου. Ωστόσο, αυτή η λεπτομέρεια δεν επηρεάζει την μελέτη μας γιατί μπορούμε να προσθέσουμε κάποιους επιπλέον κόμβους $\mathcal{N}(v) \setminus A(G')$ στο στιγμιότυπό μας $(G', \mathcal{Z}', D', R')$ σαν μεμονωμένους κόμβους.

Στη συνέχεια δείχνουμε ότι το πρόβλημα RMT σε οποιαδήποτε οικογένεια στιγμιοτύπων $\mathcal{G}_1 \subseteq \mathcal{G}$ (συμβολίζουμε με $RMT|_{\mathcal{G}_1}$), που επίσης καλείται και πρόβλημα RMT με *υποσχόμενο σύνολο* $\mathcal{G}_1$ (βλέπε [Gol08]), ανάγεται σε πολυωνυμικό χρόνο ως προς το μέγεθος του γραφήματος $n$ στο πρόβλημα $RMT|_{\mathcal{I}(\mathcal{G}_1)}$. Αυτό σημαίνει ότι εάν υπάρχει ένας πλήρως πολυωνυμικός αλγόριθμος για την επίλυση του RMT στην οικογένεια $\mathcal{I}(\mathcal{G}_1)$, μπορεί να χρησιμοποιηθεί σαν υπορουτίνα του $\mathcal{Z}$-CPA, για την επίλυση του RMT στην οικογένεια $\mathcal{G}_1$ σε πλήρως πολυωνυμικό χρόνο.Για λόγους ευκολίας, θα χρησιμοποιήσουμε τον ακόλουθο συμβολισμό σχετικά με τις εκτελέσεις των αλγορίθμων και την γνώση των παικτών.

**Εκτελέσεις και γνώση των παικτών**. Δοθείσας μιας εκτέλεσης $e$ ενός κατανεμημένου πρωτοκόλλου, η πληροφορία $view(v, e, k)$ ενός παίκτη $v$ περιγράφει τα μηνύματα που ανταλλάχθηκαν από $v$ και τους γείτονές του μέχρι τον γύρο $k$. Για λόγους απλότητας θα χρησιμοποιούμε τον συμβολισμό $view(v, e)$ για να αναφερόμαστε σε όλα τα μηνύματα που ανταλλάχθηκαν μεταξύ του $v$ και των γειτόνων του μέχρι το τέλος της εκτέλεσης $e$. Με το $view(v, e, k)|_A$ (και $view(v, e)|_A$) θα συμβολίζουμε την αντίστοιχη περιγραφή των μηνυμάτων που ανταλλάχθηκαν μεταξύ του $v$ και ενός συνόλου $A \subseteq \mathcal{N}(v)$. Η απόφαση ενός παίκτη $v$ στην εκτέλεση $e$ θα συμβολίζεται με $decision_e(v)$· για ντετερμινιστικά πρωτόκολλα, τα οποία λαμβάνουμε υπόψιν στην παρούσα εργασία, η συνάρτηση $decision_e(v)$ προσδιορίζεται πλήρως από την πληροφορία $view(v, e)$ του $v$ στην εκτέλεση $e$. Θα γράφουμε απλά $decision(v)$ όταν η εκτέλεση υπονοείται από τα συμφραζόμενα.

***Θεώρημα* 4.12**. *Αν υπάρχει ένας πλήρως πολυωνυμικός (ως προς το $n$) αλγόριθμος $\Pi$ που επιλύει το $RMT|_{\mathcal{I}(\mathcal{G}_1)}$ τότε υπάρχει ένας πλήρως πολυωνυμικός αλγόριθμος (ως προς το $n$) που επιλύει το $RMT|_{\mathcal{G}_1}$.*

Η απόδειξη του παραπάνω θεωρήματος παρουσιάζεται στο [PPS15].

Βασιζόμενοι στον ορισμό της μοναδικότητας πολυωνυμικού χρόνου και στο Θεώρημα 4.12, προκύπτει το ακόλουθο πόρισμα για τον $\mathcal{Z}$-CPA.

***Πόρισμα* 4.13**. *Το σχήμα πρωτοκόλλων $\mathcal{Z}$-CPA είναι πολυωνυμικά μοναδικό για το πρόβλημα RMT.*

## 4.7 Συμπεράσματα κεφαλαίου

Αναφορικά με το μοντέλο μερικής γνώσης, ο RMT-PKA περιέχει ανταλλαγή τοπολογικής γνώσης μεταξύ παικτών. Αν και η ανακάλυψη της τοπολογίας δεν είναι το κύριο κίνητρό μας, οι τεχνικές που χρησιμοποιούνται σε αυτό το κεφάλαιο (π.χ. η πράξη $\oplus$ ) μπορεί να εφαρμόζονται στο πρόβλημα της ανακάλυψης της τοπολογίας υπό την παρουσία βυζαντινών αντιπάλων ([NT09],[DLS13]). Από την σύγκριση με τις τεχνικές που χρησιμοποιούνται σε αυτόν τον τομέα θα μπορούσε να προκύψουν αποτελέσματα σχετικά με τη αποτελεσματική εξαγωγή ορθής πληροφορίας από κακόβουλα δημιουργημένα τοπολογικά δεδομένα.

Το μοναδικό πρωτόκολλο που παρουσιάστηκε για το μοντέλο μερικής γνώσης απαντά μόνο ερωτήματα σχετικά με την επιλυσιμότητα του προβλήματος. Μια φυσική ερώτηση είναι αν

και πότε μπορούμε να κατασκευάσουμε ένα μοναδικό αλγόριθμο ο οποίος είναι επίσης και αποδοτικός σε αυτό το πλαίσιο. Οι τεχνικές που έχουν χρησιμοποιηθεί έως τώρα στην σχετική βιβλιογραφία για τον περιορισμό της πολυπλοκότητας επικοινωνίας [KGSR02] δεν εφαρμόζονται άμεσα στο παρόν μοντέλο. Επομένως η μελέτη προς αυτή την κατεύθυνση μπορεί να δώσει ενδιαφέροντα αποτελέσματα ως προς την ανταλλαγή μηνυμάτων σε μοντέλα μερικής γνώσης της τοπολογίας.

Θα ήταν επίσης ενδιαφέρουσα η μελέτη της μοναδικότητας ως προς την αποδοτικότητα του RMT στο μοντέλο μερικής γνώσης επεκτείνοντας την ανάλυσή μας για την περίπτωση των *ad hoc* δικτύων.

Τέλος, μπορούμε να ορίσουμε έναν πιο ισχυρό τύπο πολυωνυμικής μοναδικότητας: ονομάζουμε ένα σχήμα πρωτοκόλλων $\mathcal{A}$ *ισχυρά μοναδικό ως προς πολυωνυμικό χρόνο* για το πρόβλημα $\Pi$ εάν η ύπαρξη οποιουδήποτε πλήρως πολυωνυμικού πρωτοκόλλου για μια κλάση στιγμιοτύπων $\mathcal{I}$ συνεπάγεται ότι το $\mathcal{A}$ είναι επίσης πλήρως πολυωνυμικό για την κλάση $\mathcal{I}$. Εικάζουμε ότι ο $\mathcal{Z}$-CPA είναι ισχυρά πολυωνυμικός ως προς πολυωνυμικό χρόνο για το πρόβλημα RMT στο *ad hoc* μοντέλο.

# Κεφάλαιο 5

# Εκπομπή $k$-μεταδόσεων σε ασύρματα δίκτυα

Ακόμα και όταν δεν παρατηρείται κακόβουλη ή εσφαλμένη συμπεριφορά κάποιων παικτών σε ένα κατανεμημένο σύστημα, πολλά διαφορετικά εμπόδια μπορεί να εμφανιστούν κατά τη διαδικασία μετάδοσης πληροφορίας που αφορούν πρακτικά προβλήματα ή και την ίδια τη φύση του δικτύου επικοινωνίας. Μελετάμε την περίπτωση των ασύρματων δικτύων όπου οι παίκτες είναι κάτοχοι ασύρματων συσκευών πομποδέκτη και επικοινωνούν μεταξύ τους με τοπικές ασύρματες εκπομπές. Η ίδια η φύση των ασύρματων δικτύων προσθέτει άλλον έναν παράγοντα δυσκολίας που αφορά την ορθότητα της διάδοσης του μηνύματος· συγκεκριμένα, απαιτείται η παρεμβολή σήματος να είναι χαμηλή για να διαδοθεί ένα μήνυμα στο δίκτυο. Αυτό το γεγονός συνήθως εκφράζεται υποθέτοντας ότι αν δύο γείτονες ενός παίκτη $v$ εκπέμψουν ταυτόχρονα προκύπτει μια σύγκρουση και ο $v$ δεν λαμβάνει κανένα μήνυμα.

Μελετάμε την επιλυσιμότητα του προβλήματος Εκπομπής με περιορισμένες μεταδόσεις από τους παίκτες σε ασύρματα *ad hoc* δίκτυα στην περίπτωση που όλοι οι παίκτες εκτελούν ορθά (έντιμα) το πρωτόκολλο. Πιο συγκεκριμένα, εξετάζουμε το *ασύρματο μοντέλο $k$-μεταδόσεων*, στο οποίο δίνεται ένα φράγμα $k$ και κάθε παίκτης μπορεί να μεταδώσει το πολύ $k$ φορές κατά τη διάρκεια εκτέλεσης ενός πρωτοκόλλου. Το κίνητρο για τη θεώρηση αυτή προέρχεται από ανάγκες ενεργειακής αποδοτικότητας που είναι σημαντικές για τα ευρέως χρησιμοποιούμενα δίκτυα ασύρματων αισθητήρων στα οποία κάθε παίκτης αντιπροσωπεύει μια συσκευή περιορισμένης ενέργειας (π.χ. υποστηριζόμενη από μπαταρία).

Κυρίως μελετάμε την γενικότερη περίπτωση των *προσαρμοστικών* αλγορίθμων Εκπομπής, οι οποίοι είναι αλγόριθμοι όπου οι ενέργειες του κάθε παίκτη ορίζονται λαμβάνοντας υπόψιν ολόκληρο το ιστορικό μεταδόσεών του. Αντιθέτως, σε έναν *μη προσαρμοστικό* αλγόριθμο Εκπομπής οι ενέργειες του κάθε παίκτη εξαρτώνται μόνο από το αναγνωριστικό του. Αποδεικνύουμε ένα κάτω φράγμα της τάξης του $\Omega\left(n^{\frac{1+k}{k}}\right)$ στην πολυπλοκότητα γύρων οποιουδήποτε πρωτοκόλλου Εκπομπής εισάγοντας την έννοια του *δέντρου μεταδόσεων* η οποία γενικεύει προηγούμενες προσεγγίσεις στη μελέτη του μοντέλου $k$-μεταδόσεων. Για να εξάγουμε

αυτό το κάτω φράγμα μελετάμε την πολυπλοκότητα γύρων οποιουδήποτε προσαρμοστικού αλγορίθμου Εκπομπής· αυτοί οι αλγόριθμοι αποδεικνύονται οι πιο αποδοτικοί σε αυτό το μοντέλο ως προς την πολυπλοκότητα γύρων. Τέλος, κατασκευάζουμε τον Αλγόριθμο Συντεταγμένων Μεταδόσεων (Coordinated Transmission Algorithm-CTA), έναν μη προσαρμοστικό αλγόριθμο για την συγκεκριμένη οικογένεια γραφημάτων όπου αποδεικνύεται το κάτω φράγμα. Η πολυπλοκότητα γύρων του αλγορίθμου είναι $\Omega\left(n^{\frac{1+k}{k}}\right)$ στην συγκεκριμένη οικογένεια και επομένως, διαφέρει από το κάτω φράγμα μόνο κατά ένα παράγοντα $k$.

## 5.1 Εισαγωγή

Η ενεργειακή αποδοτικότητα έχει αναδειχθεί σε κεντρικό ζήτημα στα ασύρματα δίκτυα, λόγω της συνεχώς αυξανόμενης χρήσης αυτόνομων συσκευών με περιορισμένες πηγές ενέργειας. Ένα μεγάλο μέρος της σύγχρονης έρευνας επικεντρώνεται στην επίτευξη ενεργειών επικοινωνίας με έναν ενεργειακά αποδοτικό τρόπο χωρίς να υποβιβάζεται αισθητά η γενική απόδοση του συστήματος. Αρκετές από τις μέχρι τώρα μελέτες έχουν επικεντρωθεί στο πρόβλημα της ρύθμισης της ακτίνας μετάδοσης των κόμβων έτσι ώστε το κόστος της ενέργειας να ελαχιστοποιείται.

Ωστόσο, αν οι κόμβοι εκπέμπουν σε προκαθορισμένο επίπεδο ισχύος είναι λογικό να θεωρήσουμε τον αριθμό των μεταδόσεων σαν ένα μέτρο κατανάλωσης ενέργειας. Μια τέτοια μελέτη ξεκίνησε από τους Gasieniec *et al.* στο [GKK$^+$08], όπου θεωρήθηκαν πρωτόκολλα Εκπομπής με περιορισμένες μεταδόσεις ανά κόμβο, για την περίπτωση των ασύρματων δικτύων γνωστής τοπολογίας. Εδώ, εξετάζουμε το πρόβλημα σε *ad hoc* ασύρματα δίκτυα, δηλαδή, δίκτυα στα οποία οι κόμβοι δεν έχουν καμία γνώση ως προς την τοπολογία του δικτύου.

Υποθέτουμε ότι ένα φράγμα $k$ δίνεται και ότι κάθε κόμβος μπορεί να μεταδώσει το πολύ $k$ φορές κατά τη διάρκεια της εκτέλεσης ενός πρωτοκόλλου Εκπομπής (*Εκπομπή $k$-μεταδόσεων*)· σημειώνεται ότι το φράγμα $k$ μπορεί κάλλιστα να αντιπροσωπεύει τον αριθμό των μεταδόσεων τον οποίο επιτρέπει η πηγή ενέργειας ενός παίκτη. Υποθέτουμε επίσης ότι η επικοινωνία είναι *σύγχρονη*, δηλαδή, όλοι οι κόμβοι λαμβάνουν ή μεταδίδουν ταυτόχρονα, ή αλλιώς, στον ίδιο γύρο. Σε κάθε οποιονδήποτε γύρο, κάθε κόμβος μπορεί να λειτουργήσει ως *πομπός* (αποστολέας) ή ως *δέκτης* (παραλήπτης). Όποτε εκπέμπει ένας κόμβος τότε το μήνυμά παραλαμβάνεται από όλους τους γείτονές του. Αν όμως, δύο γείτονες ενός κόμβου $v$ εκπέμψουν ταυτόχρονα τότε προκύπτει μια *σύγκρουση* και ο $v$ δεν λαμβάνει κανένα μήνυμα.

Μελετάμε δύο είδη πρωτοκόλλων: τα *προσαρμοστικά* και τα *μη προσαρμοστικά* πρωτόκολλα· τα πρώτα, είναι πρωτόκολλα στα οποία ένας κόμβος μπορεί να αποφασίσει αν θα μεταδώσει ή όχι λαμβάνοντας υπόψιν οποιαδήποτε πληροφορία έλαβε κατά τη διάρκεια των προηγούμενων γύρων, ενώ τα μη προσαρμοστικά είναι πρωτόκολλα όπου ο κάθε παίκτης αποφασίζει τις μεταδόσεις του χωρίς να λαμβάνει καθόλου υπόψιν το ιστορικό μεταδόσεων. Αν και τα μη προσαρμοστικά πρωτόκολλα είναι πιο ισχυρά, τα μη προσαρμοστικά είναι πιο εύκολα στην υλοποίηση και απαιτούν ελάχιστο χρόνο επεξεργασίας για κάθε κόμβο.

Μελετώντας κυρίως την περίπτωση των προσαρμοστικών πρωτοκόλλων, διερευνούμε τον τρόπο με τον οποίο ο περιορισμός στον αριθμό των μεταδόσεων επηρεάζει την πολυπλοκότητα γύρων των πρωτοκόλλων Εκπομπής.

### 5.1.1 Σχετική βιβλιογραφία

Η Εκπομπή σε ασύρματα δίκτυα άγνωστης τοπολογίας χωρίς περιορισμό στον αριθμό των μεταδόσεων έχει μελετηθεί εκτενώς στη βιβλιογραφία . Το πρόβλημα εισήχθη από τους Chlamtac και Kutten [CK85]. Οι Bar-Yehuda, Goldreich και Itai [BYGI87] παρουσίασαν το πρώτο πιθανοτικό πρωτόκολλο, το οποίο ολοκληρώνει την Εκπομπή σε $O(D \log n + \log^2 n)$ αναμενόμενο χρόνο όταν εκτελείται σε γραφήματα με $n$ κόμβους και διάμετρο $D$. Ακολούθησαν αρκετές εργασίες [CR03, KP03] που οδήγησαν στο ακριβές φράγμα $O(D \log(n/D) + \log^2 n)$.

Για την περίπτωση των ντετερμινιστικών πρωτοκόλλων, αποδείχθηκε από τους Brusci και Del Pinto στο [BP97], ένα κάτω φράγμα της τάξης του $\Omega(n \log n)$ για γενικά δίκτυα, το οποίο βελτιώθηκε (για μικρό $D$) σε $\Omega(n \log D)$ από τους Clementi *et al.* [CMS03]. Οι Chlebus *et al.* [CGG$^+$00] παρουσίασαν το πρώτο πρωτόκολλο Εκπομπής υπό-τετραγωνικής πολυπλοκότητας $O(n^{11/6})$. Αυτό το φράγμα βελτιώθηκε σε $O(n^{5/3} \log^3 n)$ από τους De Marco και Pelc [MP01] και στη συνέχεια από τους Chlebus *et al.* [CGÖR00], οι οποίοι παρουσίασαν έναν αλγόριθμο με πολυπλοκότητα $O(n^{3/2})$ βασισμένο σε πεπερασμένες γεωμετρίες. Οι Chrobak, Gąsieniec και Rytter [CGR00] βελτίωσαν επιπλέον το φράγμα σε $O(n \log^2 n)$. Τέλος, ο De Marco [Mar08] παρουσίασε το καλύτερο γνωστό άνω φράγμα της τάξης του $O(n \log n \log \log n)$, το οποίο έχει υπό-λογαριθμική ασυμπτωτική διαφορά με το κάτω φράγμα.

Όπως προαναφέρθηκε, η Εκπομπή με περιορισμένο αριθμό μεταδόσεων προτάθηκε για πρώτη φορά στο [GKK$^+$08]. επίσης μελετήθηκε στο [KP09], όπου προτάθηκαν πιθανοτικοί αλγόριθμοι για το πρόβλημα· και στις δύο περιπτώσεις, μελετήθηκε το πρόβλημα σε δίκτυα γνωστής τοπολογίας. Μια άλλη προσέγγιση για τον περιορισμό του αριθμού των μεταδόσεων παρουσιάστηκε στο [BCH09], όπου κατασκευάστηκαν αλγόριθμοι οι οποίοι χρησιμοποιούν μικρό αριθμό μεταδόσεων για κάθε κόμβο και πετυχαίνουν Εκπομπή σε σχεδόν βέλτιστο χρόνο.

Η προσέγγισή μας σε αυτό το κεφάλαιο αποτελεί φυσική συνέχεια της εργασίας των Koutris και Pagourtzis [KP11]. Σε αυτή την εργασία, οι συγγραφείς κάνουν το πρώτο βήμα για τη μελέτη της συμπεριφοράς των προσαρμοστικών πρωτοκόλλων Εκπομπής δείχνοντας ένα κάτω φράγμα της τάξης του $\Omega(n^2)$ για κάθε προσαρμοστικό πρωτόκολλο Εκπομπής 1-μετάδοσης και θέτουν σαν ανοιχτό πρόβλημα την γενίκευση του κάτω φράγματος για κάθε τιμή του $k$. Όσον αφορά την περίπτωση των μη προσαρμοστικών πρωτοκόλλων, στην ίδια δουλειά παρουσιάζεται ένα κάτω φράγμα της τάξης του $\Omega(n^2/k)$ στον χρόνο Εκπομπής οποιουδήποτε μη προσαρμοστικού αλγορίθμου $k$-μεταδόσεων. Τέλος, παρουσιάζουν ένα μη προσαρμοστικό πρωτόκολλο Εκπομπής το οποίο πετυχαίνει ένα άνω φράγμα που ταυτίζεται με το κάτω σε κάποιες περιπτώσεις, συγκεκριμένα $O(n^2/k)$, για κάθε $k \leq \sqrt{n}$ και $O(n^{3/2})$ για κάθε $k > \sqrt{n}$.

## 5.2 Προκαταρκτικές έννοιες

Θεωρούμε την περίπτωση των ασύρματων δικτύων, δηλαδή, δίκτυα στα οποία οι παίκτες κατέχουν συσκευές πομποδέκτη, τοποθετούνται σε κάποια φυσική επιφάνεια, και δύο κόμβοι μπορούν να επικοινωνήσουν μεταξύ τους αν είναι ο ένας μέσα στην ακτίνα μετάδοσης του άλλου και η παρεμβολή σήματος είναι χαμηλή. Μια συνήθης μοντελοποίηση είναι να θεωρήσουμε ότι το δίκτυο είναι ένα γράφημα και να υποθέσουμε (*υπόθεση συγκρούσεων*) ότι η επικοινωνία είναι εφικτή αν ένας κόμβος λαμβάνει ένα μήνυμα μόνο από έναν γείτονά του σε ένα συγκεκριμένο χρονικό σημείο.

**Δίκτυα άγνωστης τοπολογίας.** Μοντελοποιούμε ένα ασύρματο δίκτυο σαν ένα κατευθυνόμενο γράφημα. Συγκεκριμένα, αν ο παίκτης $v$ βρίσκεται εντός της ακτίνας εκπομπής ενός παίκτης $w$, το μοντελοποιούμε με την κατευθυνόμενη ακμή $(w, v)$. Επίσης, ότι οι κόμβοι έχουν μοναδικά αναγνωριστικά από το σύνολο $V = \{1, 2, \ldots, n\}$, όπου $n$ είναι ο αριθμός των κόμβων στο δίκτυο. Όσον αφορά την αρχική γνώση των παικτών, υποθέτουμε ότι στην αρχή του πρωτοκόλλου, ένας παίκτης γνωρίζει μόνο το δικό του αναγνωριστικό και το αν είναι ο διανομέας ή όχι. Αυτό σημαίνει ότι δεν έχει καθόλου γνώση, μερική ή ολική, ως προς την τοπολογία του δικτύου. Παρατηρούμε ότι σε αυτό το μοντέλο απαιτούμε ακόμα λιγότερη γνώση από το *ad hoc* μοντέλο όπως το έχουμε μελετήσει έως τώρα, αφού ο κάθε κόμβος δεν γνωρίζει ούτε τα αναγνωριστικά των γειτόνων του. Αυτή η υπόθεση είναι περισσότερο φυσική στο μοντέλο ασύρματων δικτύων, αφού στην πραγματικότητα ένας κόμβος εκπέμπει τοπικά ένα μήνυμα και δεν γνωρίζει την ύπαρξη καναλιών επικοινωνίας που αντιστοιχούν στους γείτονές του.

Επιπλέον, ότι οι κόμβοι δεν είναι σε θέση να κάνουν *ανίχνευση συγκρούσεων*, δηλαδή, αν μια προσπάθεια μετάδοσης μηνύματος στον κόμβο $v$ είναι ανεπιτυχής, τότε ο $v$ δεν παρατηρεί κάτι και άρα δεν μπορεί να ξεχωρίσει από την περίπτωση που δεν του έχει σταλεί κανένα μήνυμα.

Εφόσον υποθέτουμε ότι όλοι οι παίκτες είναι τίμιοι (δεν υπάρχει κάποιος αντίπαλος), λέμε ότι ένας αλγόριθμος πετυχαίνει Εκπομπή όταν όλοι οι κόμβοι του δικτύου έχουν λάβει το μήνυμα του διανομέα. Όμοια με πριν, η πολυπλοκότητα γύρων, ή αλλιώς ο *χρόνος εκτέλεσης* ενός αλγορίθμου Εκπομπής ορίζεται σαν τον αριθμό των γύρων που χρειάζονται, στην χειρότερη περίπτωση ως προς όλα τα πιθανά γραφήματα με $n$ κόμβους, για να επιτευχθεί Εκπομπή.

**Μη προσαρμοστικά πρωτόκολλα Εκπομπής** Ορίζουμε τώρα την έννοια του *μη προσαρμοστικού πρωτοκόλλου $k$-μεταδόσεων*. Όπως προαναφέρθηκε, ένα πρωτόκολλο είναι μη προσαρμοστικό αν οι κόμβοι δεν λαμβάνουν υπόψιν τους οποιαδήποτε πληροφορία μπορεί να έχουν λάβει κατά τη διάρκεια του πρωτοκόλλου. Πιο τυπικά, ένα μη προσαρμοστικό πρωτόκολλο μπορεί να περιγραφεί συνοπτικά σαν μια ακολουθία *συνόλων μετάδοσης*, τα οποία είναι υποσύνολα του συνόλου $V$. Από τη στιγμή που δεν χρησιμοποιείται από τους παίκτες κάποια επιπλέον πληροφορία, εκτός από το μήνυμα του διανομέα, είναι φυσιολογικό να υποθέσουμε ότι από τη στιγμή που ένας κόμβος λάβει το μήνυμα σε ένα βήμα $t$, ενεργοποιείται και μεταδίδει στους πρώτους $k$ γύρους μετά το $t$ στους οποίους εμφανίζεται στο σύνολο με-

τάδοσης. Αυτό το μοντέλο περιγράφει μια σημαντική κλάση αλγορίθμων Εκπομπής, αφού οι περισσότεροι γνωστοί ντετερμινιστικοί αλγόριθμοι Εκπομπής σε δίκτυα άγνωστης τοπολογίας εμπίπτουν σε αυτή την κλάση.

### 5.2.1 Προσαρμοστικά πρωτόκολλα Εκπομπής

Για τον ορισμό ενός προσαρμοστικού πρωτοκόλλου θα χρησιμοποιήσουμε a γενίκευση του μοντέλου που προτάθηκε από τους Kowalski και Pelc [KP04]. Στο μοντέλο που χρησιμοποιούμε για τους προσαρμοστικούς αλγορίθμους, επιτρέπουμε σε έναν κόμβο να εκπέμψει ένα μήνυμα στη γειτονιά του ακόμα και πριν αυτός λάβει το μήνυμα του διανομέα. Ένας αλγόριθμος μπορεί να χρησιμοποιήσει αυτήν την πληροφορία για την ανταλλαγή τοπολογικής γνώσης μεταξύ των παικτών η οποία μπορεί να επηρεάσει τις ενέργειες σε επόμενους γύρους. Συμβολίζουμε με $H_t(v)$ το ιστορικό αλληλεπίδρασης ενός κόμβου $v$ μέχρι το τέλος του γύρου $t$, δηλαδή, μία πλήρης περιγραφή όλων των μηνυμάτων που ;έλαβε (μαζί με το αντίστοιχο αναγνωριστικό του αποστολέα) έστειλε ο $v$ κατά τη διάρκεια του κάθε γύρου $1, \ldots, t$. Θα χρησιμοποιήσουμε την έννοια *εισερχόμενο ιστορικό* για την περιγραφή των ληφθέντων μηνυμάτων.

Ένα πρωτόκολλο Εκπομπής τώρα, μπορεί να οριστεί από μια συνάρτηση $\pi(v, t, H_{t-1}(v))$, η οποία έχει πεδίο τιμών το σύνολο {receive, transmit}. Μέσω της συνάρτησης αποφασίζεται αν ο κόμβος $v$ με ιστορικό $H_{t-1}(v)$ λειτουργεί σαν παραλήπτης (receive) ή σαν αποστολέας (transmit) στον γύρο $t$. Εάν ο $v$ λειτουργεί σαν αποστολέας στον γύρο $t$, τότε εκπέμπει ολόκληρο το ιστορικό του μέχρι τον γύρο $t-1$ μαζί με το αναγνωριστικό του, δηλαδή το μήνυμα $(v, H_{t-1}(v))$. Παρατηρούμε ότι η μέγιστη ανταλλαγή πληροφορίας προκύπτει όταν οι αποστολείς στέλνουν ολόκληρο το ιστορικό τους, αφού τότε ο παραλήπτης μπορεί να εξάγει οποιαδήποτε πληροφορία από αυτό. Για λόγους πληρότητας, υποθέτουμε ότι στη φάση αρχικοποίησης του πρωτοκόλλου (*γύρος 0*) κάθε παίκτης $v \in V \setminus \{s\}$ έχει το ιστορικό $H_0(v) = (\emptyset, \perp)$ που αντιπροσωπεύει την απουσία μιας αρχικής τιμής εισόδου. Θεωρούμε ότι ο διανομέας $D$ έχει την αρχική τιμή $H_0(s) = (\emptyset, m)$, όπου $m$ είναι η αρχική τιμή του $D$.

### 5.2.2 Διάρθρωση του κεφαλαίου

Σε αυτό το κεφάλαιο αντιμετωπίζουμε, κατά κύριο λόγο, το ανοιχτό ερώτημα που παρουσιάζεται στο [KP11], αναφορικά με τη γενίκευση του κάτω φράγματος και καταφέρνουμε να εξάγουμε ένα φράγμα για κάθε τιμή του $k$. Για να το πετύχουμε αυτό, αποδεικνύουμε ένα κάτω φράγμα στην πολυπλοκότητα γύρων οποιουδήποτε προσαρμοστικού αλγορίθμου Εκπομπής· εφόσον οι προσαρμοστικοί αλγόριθμοι επιτρέπουν τη χρήση οποιασδήποτε διαθέσιμης πληροφορίας αποδεικνύονται ότι είναι οι πιο ισχυροί αλγόριθμοι για το μοντέλο και επομένως το κάτω φράγμα ισχύει για οποιονδήποτε αλγόριθμο Εκπομπής.

Για να αποδείξουμε το φράγμα, εισάγουμε την κατασκευή του *δέντρου μεταδόσεων* το οποίο είναι ένας τρόπος αναπαράστασης των ενεργειών που εκτελούν οι παίκτες σε οποιονδήποτε αλγόριθμο Εκπομπής δοθέντος ενός συγκεκριμένου ιστορικού μεταδόσεων. Η κατασκευή μπο-

ρεί να χρησιμοποιηθεί για να προσδιοριστεί η ανάθεση αναγνωριστικών από την οποία προκύπτει η μεγαλύτερη καθυστέρηση της διάδοσης του μηνύματος σε ενδιάμεσα επίπεδα κόμβων, από την αρχή του πρωτοκόλλου μέχρι τον τερματισμό του. Η έννοια του δέντρου μεταδόσεων είναι και γενικότερου ενδιαφέροντος, αφού μπορεί να χρησιμοποιηθεί για να μελετηθεί η πολυπλοκότητα γύρων των αλγορίθμων σε αυτό το μοντέλο. Μελετάμε την οικογένεια γραφημάτων $\mathcal{G}$, μιας συγκεκριμένης τοπολογίας, για την εξαγωγή του κάτω φράγματος.

Τέλος, ασχολούμαστε με το κατά πόσο το κάτω φράγμα είναι βέλτιστο για την συγκεκριμένη οικογένεια $\mathcal{G}$, στην Ενότητα 5.4, κατασκευάζουμε ένα μη προσαρμοστικό πρωτόκολλο το οποίο πετυχαίνει Εκπομπή στην συγκεκριμένη οικογένεια με πολυπλοκότητα γύρων $\Omega\left(n^{\frac{1+k}{k}}\right)$, η οποία διαφέρει από το κάτω φράγμα κατά έναν παράγοντα $k$.

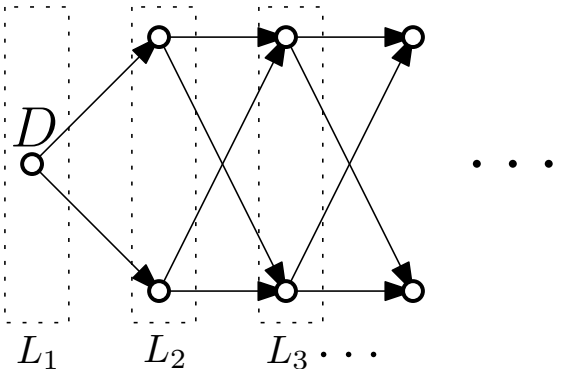
## 5.3 Πρωτόκολλα Εκπομπής και δέντρα μετάδοσης

Γενικεύοντας την προσέγγιση κάτω φράγματος της εργασίας [BP97] για κάθε αριθμό μεταδόσεων εισάγουμε μια κατασκευή, την οποία καλούμε *δέντρο μεταδόσεων*, η οποία επιτρέπει την εξαγωγή ενός κάτω φράγματος για την περίπτωση των $k$-μεταδόσεων. θεωρούμε την γενικότερη περίπτωση των προσαρμοστικών πρωτοκόλλων, και για κάθε τέτοιο πρωτόκολλο $\pi$ κατασκευάζουμε ένα δίκτυο στο οποίο η καθυστέρηση της ολοκλήρωσης της Εκπομπής με το πρωτόκολλο $\pi$αυξάνεται σημαντικά. Χρησιμοποιούμε την προσέγγιση των δέντρων μεταδόσεων για να μεγιστοποιήσουμε την καθυστέρηση στα ενδιάμεσα στάδια της επίτευξης Εκπομπής.

### 5.3.1 Οικογένεια των δικτύων

Η οικογένεια των δικτύων $\mathcal{G}$ που χρησιμοποιούμε για το επιχείρημα του κάτω φράγματος είναι γραφήματα συγκεκριμένης τοπολογίας, συγκεκριμένα, οι $n$ κόμβοι κάθε τέτοιου δικτύου μπορούν να διαμεριστούν σε $l$ επίπεδα· το πρώτο επίπεδο περιέχει μόνο τον διανομέα $D$, τα επόμενα $l-2$ περιέχουν 2 κόμβους το καθένα και το τελευταίο επίπεδο τους υπόλοιπους κόμβους (1 ή 2) για να ολοκληρωθεί η διαμέριση.Επιπλέον, κάθε κόμβος $v$ στο επίπεδο $i$ συνδέεται, με μια κατευθυνόμενη ακμή $(v, w)$, με κάθε κόμβο $w$ του επιπέδου $i+1$ και δεν υπάρχουν άλλες ακμές.

Πιο συγκεκριμένα, για ένα γράφημα $n$ κόμβων $G = (V, E) \in \mathcal{G}$, το σύνολο κόμβων $V$ μπορεί να διαμεριστεί σε $l = \lfloor n/2 \rfloor + 1$ επίπεδα $L_1, \ldots, L_l$ τέτοια ώστε $L_1 = \{s\}$, $|L_2| = \ldots = |L_{l-1}| = 2$ και $L_l = V \backslash \cup_{i=1}^{l-1} L_i$. Επιπλέον, $E = \{(w, v) \in L_i \times L_j \mid i, j \in \{1, \ldots l\}, j - i = 1\}$. Έχοντας προσδιορίσει την τοπολογία της οικογένειας γραφημάτων $\mathcal{G}$ τα διαφορετικά μέλη της οικογένειας διαφέρουν ως προς τον αριθμό των κόμβων και την ανάθεση των αναγνωριστικών. Η γενική τοπολογική δομή της οικογένειας $\mathcal{G}$ απεικονίζεται στο Σχήμα 5.1.




Σχήμα 5.1: Οικογένεια γραφημάτων $\mathcal{G}$.

### 5.3.2 Σχεδιάζοντας ένα "αργό" γράφημα

Θεωρούμε ένα οποιοδήποτε πρωτόκολλο Εκπομπής $k$-μεταδόσεων $\pi$ που πετυχαίνει Εκπομπή σε κάθε γράφημα με $n$ κόμβους. Θα κατασκευάσουμε ένα γράφημα $G_\pi \in \mathcal{G}$, αναθέτοντας αναγνωριστικά στους κόμβους, έτσι ώστε να υπάρχει σημαντική καθυστέρηση στην επίτευξη Εκπομπής. θα κατασκευάσουμε ένα γράφημα $G_\pi$ σταδιακά χρησιμοποιώντας τις οικογένειες γραφημάτων $\mathcal{G}_i$ όπως αυτές περιγράφονται στη συνέχεια.

**Μερική ανάθεση αναγνωριστικών.** Για μια τυχαία ανάθεση αναγνωριστικών $ID_i$ στα πρώτα $i$ ($i \in \{1, \ldots, l-1\}$) επίπεδα γραφημάτων τις οικογένειας $\mathcal{G}$, ορίζουμε την οικογένεια $\mathcal{G}_i \subseteq \mathcal{G}$ γραφημάτων με $n$ κόμβους η οποία έχει την ανάθεση $ID_i$ στα πρώτα $i$ επίπεδά της και επομένως τα μέλη της οικογένειας διαφέρουν μεταξύ τους σε $l-i$ επίπεδα. Έστω $S$ το σύνολο των αναγωριστικών που έχουν ανατεθεί και $A = V \setminus S$.

**Εισερχόμενο ιστορικό ενός επιπέδου.** Θεωρούμε την εκτέλεση ενός πρωτοκόλλου $\pi$ σε κάθε γράφημα της οικογένειας $G \in \mathcal{G}_i$. Παρατηρούμε ότι σε όλα τα γραφήματα $G \in \mathcal{G}_i$ οι κόμβοι στο επίπεδο $L_{i+1}$ λαμβάνουν από το επίπεδο $L_i$ το ίδιο εισερχόμενο ιστορικό $H_j$, για κάθε γύρο $j$ της εκτέλεσης. Η ακολουθία εισερχόμενου ιστορικού $(H_j) = (H_1, H_2, \ldots)$ μπορεί να προσδιοριστεί μέσω του πρωτοκόλλου $\pi$ καθώς η τοπολογία και τα αναγνωριστικά των πρώτων $i$ επιπέδων είναι γνωστά. Παρατηρούμε ότι σύμφωνα με τον ορισμό του ιστορικού μεταδόσεων ο όρος $H_j$ περιέχει όλη την πληροφορία που περιέχεται στους όρους $H_1, \ldots, H_{j-1}$. Διακρίνουμε μεταξύ του εισερχόμενου ιστορικού και του πλήρους ιστορικού γιατί στη συνέχεια θα μελετήσουμε τις ενέργειες που εκτελούν διαφορετικοί κόμβοι υπό την προϋπόθεση ότι λαμβάνουν τα ίδια μηνύματα (ίδιο ιστορικό εισερχομένων μηνυμάτων). Αφού το επίπεδο $L_i$ περιέχει όλους τους εισερχόμενους γείτονες των κόμβων στο $L_{i+1}$, και δεν υπάρχει κανένα κατευθυνόμενο μονοπάτι από κόμβους στο $L_{i+1}$ προς κόμβους στο $L_i$, εγγυόμαστε ότι το ιστορικό $(H_j)$ εκφράζει ολόκληρο το ιστορικό (εισερχομένων) μεταδόσεων των κόμβων στο επίπεδο $L_{i+1}$ και επομένως οι ενέργειές τους (transmit, receive) μπορούν να προσδιοριστούν για κάθε γύρο της εκτέλεσης.

**Εκπέμποντας και λαμβάνοντας υπό συγκεκριμένο εισερχόμενο ιστορικό**. Για να προσδιορίσουμε αν ένας κόμβος $v \in A$ εκπέμπει στον γύρο $t$υπό το εισερχόμενο ιστορικό $H_{t-1}$ (όντας στο επίπεδο $i+1$) μπορούμε να προσομοιώσουμε την εκτέλεση του πρωτοκόλλου $\pi$, όπου ο $v$ λαμβάνει το εισερχόμενο ιστορικό $H_{t-1}$ και να κατασκευάσουμε το πλήρες ιστορικό $H_{t-1}(v)$ του $v$ το οποίο μπορεί επιπρόσθετα να περιλαμβάνει μηνύματα σταλθέντα από τον $v$ [1]. Με αυτόν τον τρόπο μπορούμε να ορίσουμε τους κόμβους ενός συνόλου $A$ που εκπέμπουν $t$ με:

$$S_t^A = \{v \in A \mid \pi(v, t, H_{t-1}(v)) = \text{``transmit''}\}$$

και τους κόμβους που λαμβάνουν στον γύρο $t$ με:

$$R_t^A = \{v \in V \mid \pi(v, t, H_{t-1}(v)) = \text{``receive''}\}$$

.

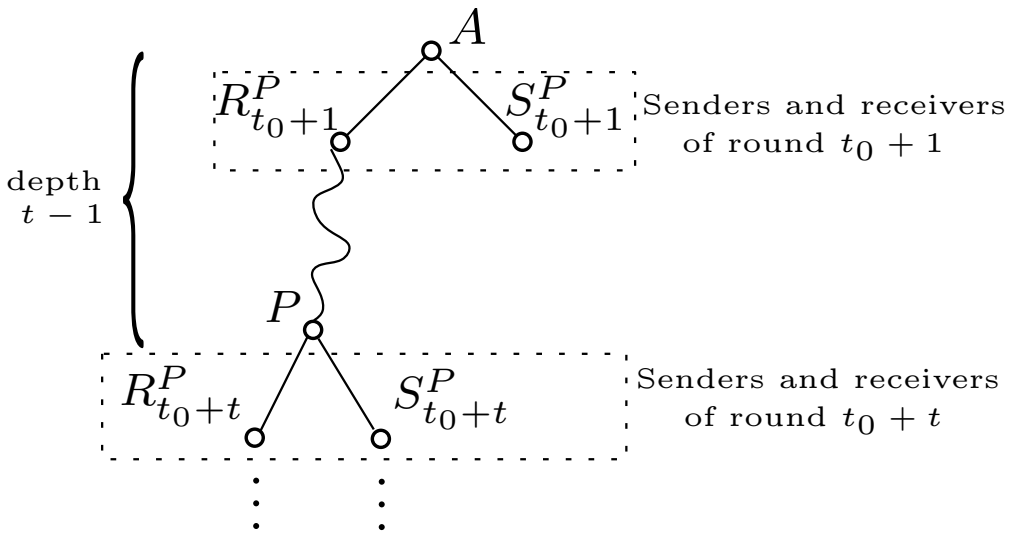
Δοθείσας μιας οικογένειας γραφημάτων $\mathcal{G}_i$ και ενός πρωτοκόλλου $\pi$ θα κατασκευάσουμε την οικογένεια γραφημάτων $\mathcal{G}_{i+1} \subseteq \mathcal{G}_i$ στην οποία μεγιστοποιείται η καθυστέρηση της μετάδοσης του μηνύματος από το επίπεδο $L_{i+1}$ στο επίπεδο $L_{i+2}$. Η προσέγγισή μας συνοψίζεται στην "χειρότερη" επιλογή των δύο αναγνωριστικών του επιπέδου $L_{i+1}$, έτσι ώστε είτε λόγω σύγκρουσης είτε λόγω μη εκπομπής το μήνυμα αποτυγχάνει να μεταδοθεί στο επίπεδο $L_{i+2}$ για τον μέγιστο αριθμό βημάτων.

### 5.3.3 Δέντρα μεταδόσεων

Στη συνέχεια εισάγουμε την έννοια του *δέντρου μεταδόσεων* which η οποία μπορεί να χρησιμοποιηθεί για τη μελέτη της ανάθεσης αναγνωριστικών που αποφέρει τη μέγιστη καθυστέρηση της μετάδοσης του μηνύματος σε ενδιάμεσα επίπεδα. Υπενθυμίζουμε ότι για την οικογένεια $\mathcal{G}_i$ (ορισμένη από την ανάθεση αναγνωριστικών $ID_i$) συμβολίζουμε με $A$ το σύνολο των αναγνωριστικών που δεν έχουν ανατεθεί. Επίσης, δοθέντος ενός πρωτοκόλλου $\pi$ και μιας οικογένειας $\mathcal{G}_i$ το εισερχόμενο ιστορικό $(H_j)$ των παικτών στο $L_{i+1}$ είναι καλώς ορισμένο όπως αναλύθηκε στην Ενότητα 5.3.2. Το δέντρο μεταδόσεων $T(\pi, \mathcal{G}_i, t_0)$ όπως ορίζεται παρακάτω, προσδιορίζει τα σύνολα μετάδοσης μετά τον γύρο $t_0$ υποθέτοντας ότι το εισερχόμενο ιστορικό τους είναι $(H_j)$, πιο συγκεκριμένα, προσδιορίζονται τα σύνολα πομπών και παραληπτών που αποτελούνται από κόμβους του συνόλου $A$ (υποψήφιοι για το επίπεδο $L_{i+1}$) για κάθε γύρο μετά τον γύρο $t_0$. Η κατασκευή απεικονίζεται στο Σχήμα 5.2

***Ορισμός* 5.1** (Δέντρο μεταδόσεων). *Ένα* δέντρο μεταδόσεων $T(\pi, \mathcal{G}_i, t_0)$ *για το πρωτόκολλο Εκπομπής $\pi$, την οικογένεια $\mathcal{G}_i$ και ένα γύρο $t_0$ είναι ένα δυαδικό δέντρο. Το αναγνωριστικό της ρίζας είναι το σύνολο κόμβων $A$ και το αναγνωριστικό του κάθε παιδιού είναι ένα υποσύνολο του αναγνωριστικού του πατέρα του. Τα αναγνωριστικά των παιδιών αποτελούν μια διαμέριση του αναγνωριστικού του πατέρα και όλα τα φύλλα είναι μονοσύνολα. Για έναν κόμβο $P$ σε βάθος $t-1$,*

[1] Προφανώς τα σταλθέντα μηνύματα του $v$ δεν έχουν καμία επίδραση στο εισερχόμενο ιστορικό λόγω της τοπολογίας (δεν υπάρχει κατευθυνόμενο μονοπάτι από κόμβους στο $L_{i+1}$ προς κόμβους στο $L_i$).




Σχήμα 5.2: Δέντρο μεταδόσεων $T(\pi, ID_i, t_0)$

*το αναγνωριστικό του αριστερού του παιδιού είναι $R^P_{t+t_0}$ ενώ το δεξί παιδί του $P$ έχει το αναγνωριστικό $S^P_{t+t_0}$, δηλαδή, τους κόμβους στο $P$ που λαμβάνουν (δεν εκπέμπουν), και αντίστοιχα εκπέμπουν, στον γύρο $t+t_0$ υποθέτοντας ότι το εισερχόμενο ιστορικό τους είναι το $(H_j)$.*

Παρατηρούμε ότι, δοθείσας μιας οικογένειας $\mathcal{G}_i$ (ή ισοδύναμα μιας ανάθεσης αναγνωριστικών $ID_i$) και μιας στιγμής έναρξης $t_i$, κάθε πρωτόκολλο Εκπομπής $\pi$ ορίζει ένα δέντρο μεταδόσεων $T(\pi, \mathcal{G}_i, t_i)$ το οποίο περιγράφει τις ενέργειες που εκτελούν οι παίκτες στο $A$, αν αυτοί λάβουν εισερχόμενο ιστορικό $(H_j)$, εκτελώντας το πρωτόκολλο $\pi$ μετά τον γύρο $t_i$.

Το μόνο μη τετριμμένο σημείο σε αυτήν την αντιστοιχία είναι το γιατί τα φύλλα πρέπει να είναι μονοσύνολα. Ο λόγος γιαυτό είναι ότι αν υπήρχε ένα φύλλο $P$ με $|P| \geq 2$ τότε το αντίστοιχο πρωτόκολλο δεν θα πετύχαινε Εκπομπή στην οικογένεια $\mathcal{G}_{i+1}$ με $L_{i+1} \subseteq P$.

***Ορισμός* 5.2** (Δέντρο $k$-μεταδόσεων ). *Ένα* Δέντρο $k$-μεταδόσεων *είναι ένα δέντρο μεταδόσεων στο οποίο κάθε κλαδί έχει το πολύ $k$ δεξιά παιδιά.*

Αυτό στην πραγματικότητα εξασφαλίζει ότι κάθε κόμβος θα εκπέμψει το πολύ σε $k$ γύρους όπως αυτό είναι επιθυμητό σε ένα πρωτόκολλο $k$-μεταδόσεων.

Στη συνέχεια ορίζουμε την έννοια του *μέγιστου βάθους ζεύγους* (maximum pair depth-mpd) ενός δέντρου $T(\pi, \mathcal{G}_i, t)$ το οποίο είναι σχετικό με την μέγιστη καθυστέρηση διάδοσης μεταξύ δύο επιπέδων. Παρατηρούμε ότι η ύπαρξη ενός εσωτερικού κόμβου με αναγνωριστικό που αποτελείται από ακριβώς 2 κόμβους, είναι εγγυημένο τετριμμένα από την δομή του δέντρου μεταδόσεων, και συγκεκριμένα από το γεγονός ότι όλα τα αναγνωριστικά των φύλλων είναι μονοσύνολα.

***Ορισμός* 5.3** (Μέγιστο βάθος ζεύγους). *Έστω ένα δέντρο μεταδόσεων $T$, το Μέγιστο βάθος ζεύγους (mpd) του δέντρου ορίζεται σαν το μέγιστο βάθος ενός κόμβου $P$ με $|P| = 2$. Στη συνέχεια θα*

*συμβολίζουμε αυτήν την ποσότητα με* $mpd(T)$.

Έστω μια οικογένεια $\mathcal{G}_i$ και ένα πρωτόκολλο $\pi$, με $t_i$, τον πρώτο γύρο όπου το μήνυμα του διανομέα διαδίδεται από το επίπεδο $L_i$ στο επίπεδο $L_{i+1}$ μέσω της εκτέλεσης του αλγορίθμου $\pi$. Παρατηρούμε ότι το $t_i$ είναι καλώς ορισμένο από τα $\mathcal{G}_i$ και $\pi$.

***Θεώρημα* 5.1**. *Έστω πρωτόκολλο Εκπομπής $\pi$ και οικογένεια γραφημάτων $\mathcal{G}_i$, τότε υπάρχει μια οικογένεια $\mathcal{G}_{i+1} \subseteq \mathcal{G}_i$ τέτοια ώστε η μετάδοση του μηνύματος από το επίπεδο $L_{i+1}$ στο επίπεδο $L_{i+2}$ σε όλα τα γραφήματα της $\mathcal{G}_{i+1}$ θα καθυστερήσει για τουλάχιστον $mpd(T(\pi, \mathcal{G}_i, t_i)) + 1$ γύρους, όπου $t_i$ είναι ο γύρος κατά τον οποίο το μήνυμα του διανομέα φτάνει για πρώτη φορά στο επίπεδο $L_{i+1}$.*

*Απόδειξη.*
Για την κατασκευή της οικογένειας $\mathcal{G}_{i+1}$ χρειάζεται μόνο να επιλέξουμε τα δύο αναγνωριστικά $v_1, v_2$ που θα ανατεθούν στο επίπεδο $L_{i+1}$. Η διάδοση ενός μηνύματος από το επίπεδο $L_{i+1}$ στο $L_{i+2}$ θα συμβεί στον πρώτο γύρο όπου ακριβώς ένας από τους $v_1, v_2$ θα εκπέμψει, σε άλλη περίπτωση είτε θα προκύψει μια φάση σύγκρουσης ή μία φάση που κανένας κόμβος από τους $v_1, v_2$ δεν θα εκπέμψει. Όπως δείξαμε νωρίτερα, υπάρχει ένας κόμβος $P$ με $|P| = 2$ και $depth(P) = mpd(T(\pi, \mathcal{G}_i, t_i))$. Επιλέγοντας τους κόμβους $L_{i+1} = \{v_1, v_2\} = P$, ο πρώτος γύρος όπου ακριβώς ένας από αυτούς εκπέμπει θα είναι ο γύρος $t \geq depth(P) + 1 = mpd(T(\pi, \mathcal{G}_i, t_i)) + 1$, συνεπώς, η διάδοση του μηνύματος στο επίπεδο $L_{i+2}$ θα καθυστερήσει μέχρι τον γύρο $mpd(T(\pi, \mathcal{G}_i, t_i)) + 1$.

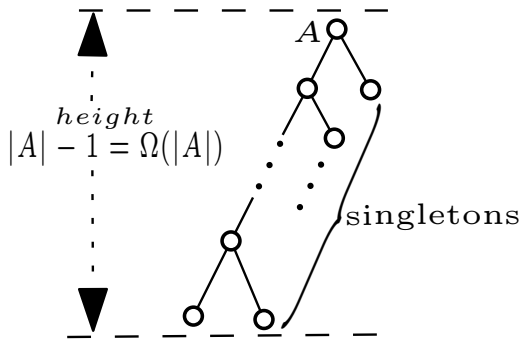
□

Έστω μια οικογένεια $\mathcal{G}_i$, θα θέλαμε να προσδιορίσουμε την ελάχιστη καθυστέρηση για την διάδοση μηνυμάτων από το επίπεδο $L_{i+1}$ στο επίπεδο $L_{i+2}$ ως προς όλα τα πρωτόκολλα Εκπομπής.

**Μέγιστο βάθος ζεύγους και ύψος δέντρου**. Χωρίς βλάβη της γενικότητας, για την μελέτη μας, μπορούμε να λάβουμε υπόψιν μόνο πρωτόκολλα Εκπομπής για τα οποία τα αντίστοιχα δέντρα μετάδοσης $T$ έχουν την ιδιότητα $mpd(T) + 1 = height(T)$. Μπορούμε να κάνουμε αυτή την απλουστευτική υπόθεση γιατί για κάθε τέτοιο δέντρο (ή πρωτόκολλο) το οποίο δεν έχει αυτή την ιδιότητα υπάρχει ένα άλλο δέντρο (πρωτόκολλο) λόγω του οποίου η διάδοση από το επίπεδο $L_{i+1}$ στο $L_{i+2}$ θα καθυστερήσει για τον ίδιο αριθμό γύρων και η ιδιότητα θα ισχύει. Το εν λόγω δέντρο προκύπτει αν απαιτήσουμε επιπλέον ότι κάθε κόμβος-μονοσύνολο του δέντρου είναι επίσης και φύλλο, και επομένως, τετριμμένα, είναι μικρότερου ύψους από το αρχικό δέντρο. Έτσι, για τον προσδιορισμό της ελάχιστης καθυστέρησης, αρκεί η εξαγωγή ενός κάτω φράγματος για το ελάχιστο ύψος των δέντρων $k$-μεταδόσεων.

***Θεώρημα* 5.2**. *Το ελάχιστο ύψος ενός δέντρου $k$-μεταδόσεων για την οικογένεια $\mathcal{G}_i$ με σύνολο μη ανατεθειμένων αναγνωριστικών $A$ με $|A| = a$ ως προς όλα τα πρωτόκολλα Εκπομπής $k$-μεταδόσεων $\mathcal{B}$ είναι*

$$\min_{\pi \in \mathcal{B}} height\left(T(\pi, \mathcal{G}_i, t_i)\right) = \Omega(a^{\frac{1}{k}})$$




Σχήμα 5.3: Δέντρο 1-μετάδοσης ελαχίστου ύψους

*Απόδειξη.*
Χωρίς βλάβη της γενικότητας μπορούμε να υποθέσουμε μόνο πρωτόκολλα που αντιστοιχούν σε δέντρα μεταδόσεων όπου κάθε εσωτερικός κόμβος έχει ένα δεξί παιδί. Ο λόγος γιαυτό είναι ότι αν ένα πρωτόκολλο $\pi$ αντιστοιχεί σε ένα δέντρο όπου ένας κόμβος $v$ έχει μόνο αριστερό παιδί (που δεν εκπέμπει) $w$, τότε διαγράφοντας αυτήν την ακμή μαζί με το αριστερό παιδί $w$ και συνδέοντας τα παιδιά του $w$ στον $v$ θα προκύψει ένα δέντρο μεταδόσεων μικρότερου ή ίσου ύψους και επομένως ένα πρωτόκολλο που θα πετυχαίνει πιο γρήγορη διάδοση.

Για την περίπτωση $k = 1$ μπορούμε να παρατηρήσουμε ότι κάθε παιδί $P$ θα περιέχει μόνο έναν κόμβο ($|P| = 1$) και θα είναι φύλλο. Αυτό είναι προφανές από τον ορισμό του δέντρου $k$-μεταδόσεων· αφού το κάθε κλαδί περιέχει το πολύ $k = 1$ δεξιά παιδιά και όλα τα φύλλα είναι μονοσύνολα, κάθε δεξί παιδί στο δέντρο πρέπει να είναι ένα μονοσύνολο-φύλλο. Επομένως το δέντρο ελαχίστου ύψους προκύπτει εάν η ρίζα και κάθε αριστερό παιδί έχει ένα δεξί παιδί που είναι και φύλλο. Συνεπώς για την περίπτωση $k = 1$,

$$\min_{\pi \in \mathcal{B}} T(\pi, \mathcal{G}_i, t) = a - 1 = \Omega(a)$$

Επομένως το θεώρημα ισχύει για $k = 1$. Το αντίστοιχο δέντρο ελάχιστου ύψους για αυτήν την περίπτωση απεικονίζεται στο Σχήμα 5.3

Υποθέτουμε ότι ο ισχυρισμός ισχύει για $k = i - 1$, θα αποδείξουμε ότι ισχύει για $k = i$. Αρχικά θεωρούμε ένα δέντρο $i$-μεταδόσεων $T$ και το ακραίο αριστερό κλαδί του $LB$ συμπεριλαμβανομένης και της ρίζας. Παρατηρούμε ότι κάθε δεξί παιδί $P$ οποιουδήποτε κόμβου στο $LB$ είναι στην πραγματικότητα μια ρίζα ενός δέντρου $(i-1)$-μεταδόσεων αφού όλοι οι κόμβοι στο $P$ έχουν μόνο $i - 1$ εναπομείνασες μεταδόσεις. Από την επαγωγική υπόθεση ότι το ελάχιστο ύψος κάθε τέτοιου δέντρου είναι $\Omega\left(|P|^{\frac{1}{i-1}}\right)$.

Για κάθε δέντρο $i$-μεταδόσεων $T$ υπάρχουν δύο περιπτώσεις (δύο είδη δέντρων μεταδόσεων):

1. Κάθε δεξί παιδί $P$ κόμβων στο $LB$ έχει πληθικότητα $|P| = O\left(a^{\frac{i-1}{i}}\right)$. Σε αυτήν την περίπτωση, το μήκος του $LB$ σε αυτό το δέντρο θα είναι της τάξης του:

$$|LB| = \frac{a}{O\left(a^{\frac{i-1}{i}}\right)} = \Omega\left(\frac{a}{a^{\frac{i-1}{i}}}\right) = \Omega(a^{1-\frac{i-1}{i}}) = \Omega(a^{1/i})$$

Αφού για κάθε ζεύγος κόμβων $P_r, P_{r+1}$ του $LB$ που βρίσκονται σε βάθος $r$ και $r+1$ αντίστοιχα, ισχύει ότι $|P_{r+1}| = |P_r| - O(a^{\frac{i-1}{i}})$.

Επιπλέον ισχύει ότι $height(T) \geq |LB| = \Omega(a^{\frac{1}{i}})$ και άρα

$$height(T) = \Omega(a^{\frac{1}{i}})$$

.

2. Υπάρχει ένα δεξί παιδί $P$ από κάποιον κόμβο στο $LB$ με πληθικότητα

$$|P| \neq O(a^{\frac{i-1}{i}}) \Leftrightarrow |P| = \omega(a^{\frac{i-1}{i}})$$

Από την επαγωγική υπόθεση, κάθε τέτοιο δέντρο $T_P$ με ρίζα $P$ θα έχει ελάχιστο ύψος της τάξης του:

$$height(T_P) = \Omega\left(\left(\omega(a^{(i-1)/i})\right)^{\frac{1}{i-1}}\right) = \Omega\left(a^{\frac{i-1}{i}\cdot\frac{1}{i-1}}\right) = \Omega\left(a^{\frac{1}{i}}\right)$$

Επιπλέον ισχύει ότι $height(T) \geq height(T_P) = \Omega(a^{\frac{1}{i}})$ και επομένως, και σε αυτήν την περίπτωση ισχύει ότι,

$$height(T) = \Omega(a^{\frac{1}{i}})$$

.

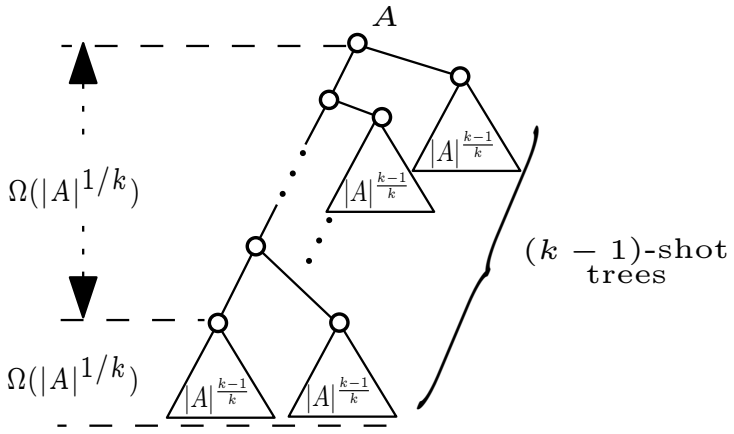
Συνεπώς το ελάχιστο ύψος του κάθε δέντρου $k$-μεταδόσεων είναι:

$$\min_{\pi\in\mathcal{B}} height\left(T(\pi, \mathcal{G}_i, t)\right) = \Omega(a^{\frac{1}{k}})$$

□

Ένα παράδειγμα δομής ενός δέντρου $k$-μεταδόσεων ελαχίστου ύψους απεικονίζεται στο Σχήμα 5.5. Όλα τα δεξιά υποδέντρα έχουν πληθικότητα ρίζας περίπου $|A|^{\frac{k-1}{k}}$.

***Θεώρημα* 5.3**. *Για κάθε προσαρμοστικό πρωτόκολλο $k$-μεταδόσεων $\pi$, υπάρχει ένα γράφημα $G \in \mathcal{G}$ $n$-κόμβων όπου το $\pi$ θα πετύχει Εκπομπή σε $\Omega(n^{\frac{1+k}{k}})$ γύρους.*




Σχήμα 5.4: Παράδειγμα ενός δέντρου $k$-μεταδόσεων ελαχίστου ύψους

*Απόδειξη.*
Εφαρμόζοντας επαναλαμβανόμενα τα Θεωρήματα 5.1,5.2 για $i = 1, \dots \lfloor n/2 \rfloor$ κατασκευάζουμε ένα γράφημα στο οποίο το πρωτόκολλο $\pi$ θα πετύχει Εκπομπή σε χρόνο ασυμπτωτικά μεγαλύτερο ή ίσο με

$$S_1 = (n-1)^{1/k} + (n-3)^{1/k} + \cdots + 2^{1/k}$$

στην περίπτωση που ο $n$ είναι περιττός και

$$S_2 = (n-1)^{1/k} + (n-3)^{1/k} + \cdots + 3^{1/k}$$

όταν ο $n$ είναι άρτιος.

Παρατηρούμε ότι στην περίπτωση που ο $n$ είναι περιττός το άθροισμα $S_1$ αποτελείται από $\lfloor n/2 \rfloor$ όρους και οι μισοί από αυτούς είναι μικρότεροι από $(n/2)^{\frac{1}{k}}$. Επομένως ισχύει ότι,

$$S_1 \geq \left\lfloor \frac{n}{4} \right\rfloor \cdot \left(\frac{n}{2}\right)^{\frac{1}{k}} > \left(\frac{n}{4} - 1\right) \cdot \left(\frac{n}{2}\right)^{\frac{1}{k}} \geq \frac{1}{8}(n-4)n^{\frac{1}{k}} \Rightarrow S_1 = \Omega\left(n^{\frac{1+k}{k}}\right)$$

όπου η τελευταία ανισότητα ισχύει γιατί $2^{\frac{1}{k}} \geq 2, k \in \mathbb{N}$. Χρησιμοποιώντας παρόμοια επιχειρήματα μπορούμε να δείξουμε ότι $S_2 = \Omega\left(n^{\frac{1+k}{k}}\right)$.

□

Το κάτω φράγμα που παρουσιάστηκε συμπίπτει με το φράγμα του [KP11] για την περίπτωση των πρωτοκόλλων 1-μετάδοσης.

## 5.4 Ένας μη προσαρμοστικός αλγόριθμος για την οικογένεια $\mathcal{G}$

Μελετώντας την ακρίβεια του κάτω φράγματος για την συγκεκριμένη οικογένεια $\mathcal{G}$, είναι ουσιώδες να μελετήσουμε αλγορίθμους γι αυτήν την συγκεκριμένη περίπτωση. Στην συνέχεια παρουσιάζουμε έναν απλό μη προσαρμοστικό αλγόριθμο Εκπομπής για την οικογένεια $\mathcal{G}$, η πολυπλοκότητα γύρων του οποίου διαφέρει από το κάτω φράγμα κατά έναν παράγοντα $k$. Απαιτούμε από αυτόν τον αλγόριθμο να επιλύει το πρόβλημα της Εκπομπής στην οικογένεια $\mathcal{G}$.

Υπενθυμίζουμε ότι ένας μη προσαρμοστικός αλγόριθμος $\mathcal{A}$ μπορεί να περιγραφεί σαν ακολουθία συνόλων μετάδοσης, δηλαδή, μια ακολουθία $s$ συνόλων αναγνωριστικών παικτών. Αν ένας παίκτης έχει ήδη λάβει το μήνυμα σε ένα γύρο $i$, το αναγνωριστικό του περιλαμβάνεται στο σύνολο $s_j$ με $j > i$ και έχει εκπέμψει λιγότερες από $k$ φορές μέχρι τον γύρο $j$, τότε λειτουργεί σαν πομπός στον γύρο $j$.

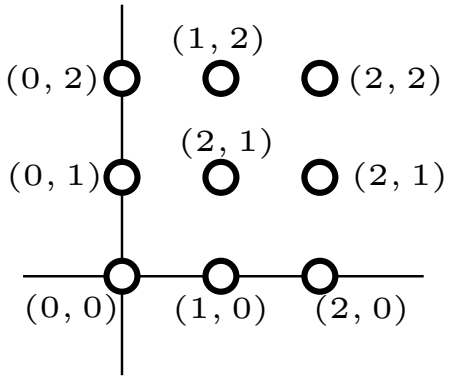
**Αλγόριθμος συντεταγμένων μεταδόσεων (CTA).** Υποθέτουμε έναν $k$-διάστατο κύβο $\left[0, \lceil n^{1/k} \rceil - 1\right]^k$, και αναπαριστούμε κάθε παίκτη σαν ακέραιο σημείο αυτού του κύβου. Συγκεκριμένα μπορούμε μπορούμε να υποθέσουμε ότι ο παίκτης $v$ αντιστοιχείται με ένα διάνυσμα συντεταγμένων $(x_1^v, \ldots, x_k^v)$ με $0 \leq x_1^v, \ldots, x_k^v \leq \lceil n^{1/k} \rceil - 1$, και $x_1^v, \ldots, x_k^v \in \mathbb{Z}$. Ο μη προσαρμοστικός αλγόριθμος CTA μπορεί πλέον να περιγραφεί από την ακολουθία $(s_i)_{i \in \mathbb{N}}$ συνόλων μετάδοσης όπως περιγράφεται παρακάτω:

$$\forall i \in \mathbb{N}, \text{ with } i \mod k\lceil n^{1/k} \rceil = j,$$
$$s_i = \{v \in V \mid x_{j \text{ div} \lceil n^{1/k} \rceil + 1} = j \mod \lceil n^{1/k} \rceil\}$$

Όπου το $a \mod b$ είναι το υπόλοιπο της διαίρεσης του $a$ με το $b$ και $a \text{ div } b$ συμβολίζει την ακέραια διαίρεση του $a$ με το $b$.

Περιγραφικά, σε κάθε γύρο, οι μόνοι παίκτες που εκπέμπουν είναι αυτοί που έχουν την ίδια τιμή σε κάποια συγκεκριμένη συντεταγμένη. Λεπτομερέστερα, σε κάθε γύρο $i = 0, \ldots, \lceil n^{1/k} \rceil - 1$, οι παίκτες που εκπέμπουν είναι ακριβώς οι παίκτες $v$ με $x_1^v = i$, σε κάθε γύρο $i = \lceil n^{1/k} \rceil, \ldots, 2\lceil n^{1/k} \rceil - 1$, οι παίκτες που εκπέμπουν είναι ακριβώς οι παίκτες $v$ με $x_2^v = i \mod \lceil n^{1/k} \rceil$ και ούτω καθεξής. Αυτή η ακολουθία εκπομπών επαναλαμβάνεται κάθε $k\lceil n^{1/k} \rceil$ γύρους όπου και όλες οι πιθανές τιμές για όλες τις συντεταγμένες έχουν ληφθεί υπόψιν. Ένα τετριμμένο παράδειγμα για την περίπτωση του $k = 2$ και $n = 9$ δίνεται στο Σχήμα 5.5. Σε αυτό το παράδειγμα έχουμε το ακόλουθο χρονοδιάγραμμα μεταδόσεων που επαναλαμβάνεται κάθε 6 γύρους:

- *Γύρος 0*: Πομποί $(0, 0), (0, 1), (0, 2)$
- *Γύρος 1*: Πομποί $(1, 0), (1, 1), (1, 2)$




Σχήμα 5.5: Παράδειγμα εκτέλεσης του CTA

- *Γύρος 2*: Πομποί $(2,0), (2,1), (2,2)$
- *Γύρος 3*: Πομποί $(0,0), (1,0), (2,0)$
- *Γύρος 4*: Πομποί $(0,1), (1,1), (2,1)$
- *Γύρος 5*: Πομποίers $(0,2), (1,2), (2,2)$

***Θεώρημα* 5.4.** *Ο αλγόριθμος CTA πετυχαίνει Εκπομπή στην οικογένεια $\mathcal{G}$ σε $O\left(k \cdot n^{\frac{1+k}{k}}\right)$ γύρους.*

*Απόδειξη.*
Αφού σε κάθε παίκτη ανατίθεται ένα μοναδικό διάνυσμα συντεταγμένων, σημαίνει ότι για κάθε ζεύγος παικτών $(v, w)$ υπάρχει μία συντεταγμένη στην οποία διαφέρουν, δηλαδή, $\exists i \in \{1, \ldots, k\}$ τέτοιο ώστε $x_i^v \neq x_i^w$. Συνεπώς, για κάθε διαδοχικό $k\lceil n^{1/k} \rceil$ ισχύει ότι για ένα ζεύγος παικτών $(v, w)$, ακριβώς ένας από τους δύο θα εκπέμψει σε τουλάχιστον ένα γύρο. Επιπλέον, κάθε παίκτης θα εκπέμψει σε ένα χρονικό διάστημα $k\lceil n^{1/k} \rceil \cdot$ συγκεκριμένα, κάθε παίκτης ο οποίος έχει ήδη παραλάβει το μήνυμα του διανομέα θα εκπέμψει ακριβώς $k$ φορές σε ένα χρονικό διάστημα διάρκειας $k\lceil n^{1/k} \rceil$ γύρων μετά την παραλαβή του μηνύματος. Τα προηγούμενα επιχειρήματα ισχύουν λόγω του γεγονότος ότι σε ένα χρονικό διάστημα $k\lceil n^{1/k} \rceil$ γύρων, θα έχουμε λάβει υπόψιν μας όλες τις τιμές για όλες τις συντεταγμένες.

Για οποιοδήποτε γράφημα $G \in \mathcal{G}$ υποθέτουμε ότι οι κόμβοι σε ένα επίπεδο $L_i$ λαμβάνουν το μήνυμα του διανομέα την χρονική στιγμή $T_i$ (υπενθυμίζουμε ότι και οι δύο κόμβοι του επιπέδου $L_i$ θα παραλάβουν το μήνυμα ταυτόχρονα). Σύμφωνα με την ανάλυση της προηγούμενης παραγράφου, είναι προφανές ότι μέχρι τον γύρο $T_i + k\lceil n^{1/k} \rceil$ υπάρχει τουλάχιστον ένας γύρος στον οποίον ακριβώς ένας από τους κόμβους του επιπέδου $L_i$ θα μεταδώσει το μήνυμα στο επόμενο επίπεδο $L_{i+1}$. Υποθέτοντας ότι ο διανομέας εκπέμπει το μήνυμά του στο επίπεδο $L_2$ στον αρχικό γύρο του πρωτοκόλλου ισχύει ότι ο CTA θα πετύχει Εκπομπή σε $O\left(k \cdot n^{\frac{1+k}{k}}\right)$ γύρους.

□

## 5.5 Συμπεράσματα κεφαλαίου

Σε αυτό το κεφάλαιο, μελετήσαμε την γενική περίπτωση των προσαρμοστικών πρωτοκόλλων Εκπομπής $k$-μεταδόσεων και καταφέραμε να εξάγουμε ένα κάτω φράγμα ως προς την πολυπλοκότητα γύρων του προβλήματος της Εκπομπής· αυτό καλύπτει εν μέρει το ανοιχτό ερώτημα του [KP11], αφού γενικεύουμε το κάτω φράγμα που παρουσιάστηκε εκεί για την περίπτωση $k = 1$ σε κάθε τιμή του $k$. Η έννοια του δέντρου μεταδόσεων, που εισάγαμε σε αυτό το κεφάλαιο και χρησιμοποιείται για την απόδειξη του φράγματος, θα μπορούσε να είναι και γενικότερου ενδιαφέροντος, αφού συσχετίζεται με την πολυπλοκότητα γύρων αλγορίθμων με μια γραφοθεωρητική παράμετρο αυτού του δέντρου. Επεκτείνουμε επίσης τη μελέτη της διαφοράς μεταξύ προσαρμοστικών και μη προσαρμοστικών αλγορίθμων κατασκευάζοντας τον αλγόριθμο CTA, η πολυπλοκότητα γύρων του οποίου διαφέρει από το κάτω φράγμα κατά ένα παράγοντα $k$.

Η περαιτέρω μελέτη της ακρίβειας του κάτω φράγματος είναι ιδιαίτερα ενδιαφέρουσα· προς αυτήν την κατεύθυνση θα ήταν λογικό να μελετηθούν διαφορετικές κλάσεις γραφημάτων ή ακόμα και ένας διαφορετικός τρόπος για την εξαγωγή του κάτω φράγματος για την συγκεκριμένη οικογένεια που θεωρήσαμε σε αυτό το κεφάλαιο. Κάνουμε ένα πρώτο βήμα προς τη μελέτη της σχέσης μεταξύ του χρόνου Εκπομπής των προσαρμοστικών και μη προσαρμοστικών αλγορίθμων· ωστόσο, το κύριο ερώτημα του αν τα προσαρμοστικά πρωτόκολλα παρέχουν πιο αποδοτικούς τρόπους για την επίτευξη Εκπομπής (ή άλλων κατανεμημένων εργασιών) από τους μη προσαρμοστικούς αλγορίθμους, παραμένει ακόμα ένα πολύ ενδιαφέρον ανοιχτό ερώτημα. Ουσιαστικά, η απάντηση αυτού του ερωτήματος εξαρτάται από το αν η χρήση της ανταλλαγής τοπολογικής γνώσης μπορεί να αποφέρει πιο αποδοτικούς αλγόριθμους στο πλαίσιο των δικτύων άγνωστης τοπολογίας. Το τελευταίο σημείο είναι επίσης και πρακτικής σημασίας αφού οι μη προσαρμοστικοί αλγόριθμοι είναι γενικά πιο απλοί στη σύλληψη και έχουν πολύ μικρές απαιτήσεις μνήμης από τους κόμβους.

# Βιβλιογραφία


[BCH09] Petra Berenbrink, Colin Cooper, and Zengjian Hu. Energy efficient randomised communication in unknown adhoc networks. *Theor. Comput. Sci.*, 410(27-29):2549–2561, 2009.

[BP97] Danilo Bruschi and Massimiliano Del Pinto. Lower bounds for the broadcast problem in mobile radio networks. *Distributed Computing*, 10(3):129–135, 1997.

[BYGI87] Reuven Bar-Yehuda, Oded Goldreich, and Alon Itai. On the time-complexity of broadcast in radio networks: An exponential gap between determinism and randomization. In *PODC*, pages 98–108, 1987.

[CGG+00] Bogdan S. Chlebus, Leszek Gasieniec, Alan Gibbons, Andrzej Pelc, and Wojciech Rytter. Deterministic broadcasting in unknown radio networks. In *SODA '00: Proceedings of the eleventh annual ACM-SIAM symposium on Discrete algorithms*, pages 861–870, Philadelphia, PA, USA, 2000. Society for Industrial and Applied Mathematics.

[CGÖR00] Bogdan S. Chlebus, Leszek Gasieniec, Anna Östlin, and John Michael Robson. Deterministic radio broadcasting. In Ugo Montanari, José D. P. Rolim, and Emo Welzl, editors, *ICALP*, volume 1853 of *Lecture Notes in Computer Science*, pages 717–728. Springer, 2000.

[CGR00] Marek Chrobak, Leszek Gasieniec, and Wojciech Rytter. Fast broadcasting and gossiping in radio networks. In *FOCS*, pages 575–581, 2000.

[CK85] I. Chlamtac and S. Kutten. On broadcasting in radio networks–problem analysis and protocol design. *Communications, IEEE Transactions on*, 33(12):1240–1246, dec. 1985.

[CMS03] Andrea E. F. Clementi, Angelo Monti, and Riccardo Silvestri. Distributed broadcast in radio networks of unknown topology. *Theor. Comput. Sci.*, 302(1-3):337–364, 2003.

[CR03] Artur Czumaj and Wojciech Rytter. Broadcasting algorithms in radio networks with unknown topology. In *FOCS*, pages 492–501. IEEE Computer Society, 2003.

[DDWY93] Danny Dolev, Cynthia Dwork, Orli Waarts, and Moti Yung. Perfectly secure message transmission. *J. ACM*, 40(1):17–47, January 1993.

[DLS13] Shlomi Dolev, Omri Liba, and Elad Michael Schiller. Self-stabilizing byzantine resilient topology discovery and message delivery - (extended abstract). In Vincent Gramoli and Rachid Guerraoui, editors, *NETYS*, volume 7853 of *Lecture Notes in Computer Science*, pages 42–57. Springer, 2013.

[Dol82] Danny Dolev. The byzantine generals strike again. *J. Algorithms*, 3(1):14–30, 1982.

[DW02] Yvo Desmedt and Yongge Wang. Perfectly secure message transmission revisited. In LarsR. Knudsen, editor, *Advances in Cryptology — EUROCRYPT 2002*, volume 2332 of *Lecture Notes in Computer Science*, pages 502–517. Springer Berlin Heidelberg, 2002.

[FM98] Matthias Fitzi and Ueli M. Maurer. Efficient byzantine agreement secure against general adversaries. In Shay Kutten, editor, *DISC*, volume 1499 of *Lecture Notes in Computer Science*, pages 134–148. Springer, 1998.

[GJ79] M. R. Garey and David S. Johnson. *Computers and Intractability: A Guide to the Theory of NP-Completeness*. W. H. Freeman, 1979.

[GKK+08] Leszek Gasieniec, Erez Kantor, Dariusz R. Kowalski, David Peleg, and Chang Su. Time efficient k-shot broadcasting in known topology radio networks. *Distributed Computing*, 21(2):117–127, 2008.

[GM98] Juan A. Garay and Yoram Moses. Fully polynomial byzantine agreement for $n > 3t$ processors in $t + 1$ rounds. *SIAM J. Comput.*, 27(1):247–290, 1998.

[Gol08] Oded Goldreich. *Computational Complexity: A Conceptual Perspective*. Cambridge University Press, New York, NY, USA, 1 edition, 2008.

[HM97] Martin Hirt and Ueli M. Maurer. Complete characterization of adversaries tolerable in secure multi-party computation (extended abstract). In James E. Burns and Hagit Attiya, editors, *PODC*, pages 25–34. ACM, 1997.

[IS10] Akira Ichimura and Maiko Shigeno. A new parameter for a broadcast algorithm with locally bounded byzantine faults. *Inf. Process. Lett.*, 110(12-13):514–517, 2010.

[KBKV06] Chiu-Yuen Koo, Vartika Bhandari, Jonathan Katz, and Nitin H. Vaidya. Reliable broadcast in radio networks: the bounded collision case. In Ruppert and Malkhi [RM06], pages 258–264.

[KGSR02] M V N Ashwin Kumar, Pranava R. Goundan, K Srinathan, and C. Pandu Rangan. On perfectly secure communication over arbitrary networks. In *Proceedings of the twenty-first annual symposium on Principles of distributed computing*, PODC '02, pages 193–202, New York, NY, USA, 2002. ACM.

[KKP01] Evangelos Kranakis, Danny Krizanc, and Andrzej Pelc. Fault-tolerant broadcasting in radio networks. *Journal of Algorithms*, 39(1):47 – 67, 2001.

[Koo04] Chiu-Yuen Koo. Broadcast in radio networks tolerating byzantine adversarial behavior. In Soma Chaudhuri and Shay Kutten, editors, *PODC*, pages 275–282. ACM, 2004.

[KP03] Dariusz R. Kowalski and Andrzej Pelc. Broadcasting in undirected ad hoc radio networks. In *PODC '03: Proceedings of the twenty-second annual symposium on Principles of distributed computing*, pages 73–82, New York, NY, USA, 2003. ACM.

[KP04] Dariusz R. Kowalski and Andrzej Pelc. Time of deterministic broadcasting in radio networks with local knowledge. *SIAM J. Comput.*, 33(4):870–891, 2004.

[KP09] Erez Kantor and David Peleg. Efficient k-shot broadcasting in radio networks. In Idit Keidar, editor, *DISC*, volume 5805 of *Lecture Notes in Computer Science*, pages 481–495. Springer, 2009.

[KP11] Paraschos Koutris and Aris Pagourtzis. Oblivious k-shot broadcasting in ad hoc radio networks. In Alex Potanin and Taso Viglas, editors, *Seventeenth Computing: The Australasian Theory Symposium, CATS 2011, Perth, Australia, January 2011*, volume 119 of *CRPIT*, pages 161–168. Australian Computer Society, 2011.

[LPS13] Chris Litsas, Aris Pagourtzis, and Dimitris Sakavalas. A graph parameter that matches the resilience of the certified propagation algorithm. In Jacek Cichon, Maciej Gebala, and Marek Klonowski, editors, *ADHOC-NOW*, volume 7960 of *Lecture Notes in Computer Science*, pages 269–280. Springer, 2013.

[LSP82] Leslie Lamport, Robert E. Shostak, and Marshall C. Pease. The byzantine generals problem. *ACM Trans. Program. Lang. Syst.*, 4(3):382–401, 1982.

[Mar08] Gianluca De Marco. Distributed broadcast in unknown radio networks. In Shang-Hua Teng, editor, *SODA*, pages 208–217. SIAM, 2008.

[MP01] Gianluca De Marco and Andrzej Pelc. Faster broadcasting in unknown radio networks. *Inf. Process. Lett.*, 79(2):53–56, 2001.

[NI08] Hiroshi Nagamochi and Toshihide Ibaraki. *Algorithmic Aspects of Graph Connectivity*. Cambridge University Press, 2008. Cambridge Books Online.

[NT09] Mikhail Nesterenko and Sébastien Tixeuil. Discovering network topology in the presence of byzantine faults. *IEEE Trans. Parallel Distrib. Syst.*, 20(12):1777–1789, 2009.

[PP05] Andrzej Pelc and David Peleg. Broadcasting with locally bounded byzantine faults. *Inf. Process. Lett.*, 93(3):109–115, 2005.

[PPS14] Aris Pagourtzis, Giorgos Panagiotakos, and Dimitris Sakavalas. Reliable broadcast with respect to topology knowledge. In Fabian Kuhn, editor, *Distributed Computing - 28th International Symposium, DISC 2014, Austin, TX, USA, October 12-15, 2014. Proceedings*, volume 8784 of *Lecture Notes in Computer Science*, pages 107–121. Springer, 2014.

[PPS15] Aris Pagourtzis, Giorgos Panagiotakos, and Dimitris Sakavalas. Reliable message transmission under partial knowledge. *IACR Cryptology ePrint Archive*, 2015:243, 2015.

[PPS16a] Aris Pagourtzis, Giorgos Panagiotakos, and Dimitris Sakavalas. Brief announcement: Reliable message transmission under partial knowledge and general adversaries. In George Giakkoupis, editor, *Proceedings of the 2016 ACM Symposium on Principles of Distributed Computing, PODC 2016, Chicago, IL, USA, July 25-28, 2016*, pages 203–205. ACM, 2016.

[PPS16b] Aris Pagourtzis, Giorgos Panagiotakos, and Dimitris Sakavalas. Reliable broadcast with respect to topology knowledge. *Distributed Computing*, pages 1–16, 2016.

[RM06] Eric Ruppert and Dahlia Malkhi, editors. *Proceedings of the Twenty-Fifth Annual ACM Symposium on Principles of Distributed Computing, PODC 2006, Denver, CO, USA, July 23-26, 2006*. ACM, 2006.

[SGSR08] Bhavani Shankar, Prasant Gopal, Kannan Srinathan, and C. Pandu Rangan. Unconditionally reliable message transmission in directed networks. In *Proceedings of the Nineteenth Annual ACM-SIAM Symposium on Discrete Algorithms*, SODA '08, pages 1048–1055, Philadelphia, PA, USA, 2008. Society for Industrial and Applied Mathematics.

[SPCR09] Kannan Srinathan, Arpita Patra, Ashish Choudhary, and C. Pandu Rangan. Unconditionally secure message transmission in arbitrary directed synchronous networks tolerating generalized mixed adversary. In *Proceedings of the 4th International Symposium on Information, Computer, and Communications Security*, ASIACCS '09, pages 171–182, New York, NY, USA, 2009. ACM.

[SR06] Kannan Srinathan and C. Pandu Rangan. Possibility and complexity of probabilistic reliable communication in directed networks. In Ruppert and Malkhi [RM06], pages 265–274.

[TV13] Lewis Tseng and Nitin H. Vaidya. Iterative approximate byzantine consensus under a generalized fault model. In Davide Frey, Michel Raynal, Saswati Sarkar, Rudrapatna K. Shyamasundar, and Prasun Sinha, editors, *Distributed Computing and Networking, 14th International Conference, ICDCN 2013, Mumbai, India, January 3-6, 2013. Proceedings*, volume 7730 of *Lecture Notes in Computer Science*, pages 72–86. Springer, 2013.

[TVB12] Lewis Tseng, Nitin H. Vaidya, and Vartika Bhandari. Broadcast using certified propagation algorithm in presence of byzantine faults. *CoRR*, abs/1209.4620, 2012.

[TVB15] Lewis Tseng, Nitin Vaidya, and Vartika Bhandari. Broadcast using certified propagation algorithm in presence of byzantine faults. *Information Processing Letters*, 115(4):512 – 514, 2015.