ΔΙΕΘΝΕΣ
ΠΑΝΕΠΙΣΤΗΜΙΟ
ΤΗΣ ΕΛΛΑΔΟΣ

Ασφάλεια Φυσικού Επιπέδου Για Ασύρματα Δίκτυα 5G

Χρήστος Χ. Οδοντόπουλος

ΠΜΣ: «Τηλεπικοινωνίες και Δίκτυα Ηλεκτρονικών Υπολογιστών»

Επιβλέπων Καθηγητής: Ευσταθίου Δημήτριος
Τμήμα Μηχανικών Πληροφορικής, Υπολογιστών και Τηλεπικοινωνιών, Διεθνές Πανεπιστήμιο της Ελλάδος

Σκοπός/Στόχος της εργασίας

- Ο υπολογισμός του ρυθμού σφαλμάτων bit BER (Bit Error Rate) στον νόμιμο δέκτη (Bob) και στον ωτακουστή (Eve)
- Το διάγραμμα αστερισμού για την κάθε διαμόρφωση
- Η σχέση μεταξύ του σηματοθορυβικού λόγου και του μέσου τετραγωνικού σφάλματος του καναλιού (channel mean square error)
- Να εξετάσουμε αν ο δέκτης του ωτακουστή παρουσιάζει μεγαλύτερο ποσοστό σφάλματος bit (BER), σε σύγκριση με τον νόμιμο δέκτη, ώστε ο νόμιμος πομπός να μπορεί να στείλει μεγαλύτερο ρυθμό πληροφορίας με ασφάλεια προς τον νόμιμο δέκτη
- Να εξετάσουμε αν το BER του Bob ελαττώνεται όσο αυξάνεται το SNR
- Να εξετάσουμε αν το BER της Eve μένει σταθερό για οποιαδήποτε τιμή του σηματοθορυβικού λόγου, για να μην μπορεί να αποδιαμορφώσει το σήμα που λαμβάνει
- Να εξετάσουμε αν το μέσο τετραγωνικό σφάλμα της εκτίμησης του ασύρματου του καναλιού του Bob μειώνεται και έτσι μπορεί να στείλει περισσότερη πληροφορία με ασφάλεια

Επισκόπηση Εργασίας

- Ασφάλεια Φυσικού Επιπέδου στις Ασύρματες Επικοινωνίες
- Πλεονεκτήματα των ασύρματων επικοινωνιών
- Είδη επιθέσεων ασύρματων επικοινωνιών
- Απαιτήσεις Ασφαλείας σε Ασύρματα Δίκτυα και Εργαλεία Ασφάλειας
- Βασικές Αρχές της Ασφάλειας Φυσικού Επιπέδου
- Εκτίμηση Ασύρματου Καναλιού σε Συστήματα OFDM
- Block Diagram of OFDM
- Διαμόρφωση και Αποδιαμόρφωση Σήματος
- Ανάλυση και Αποτελέσματα Προσομοίωσης

Ασφάλεια Φυσικού Επιπέδου στις Ασύρματες Επικοινωνίες

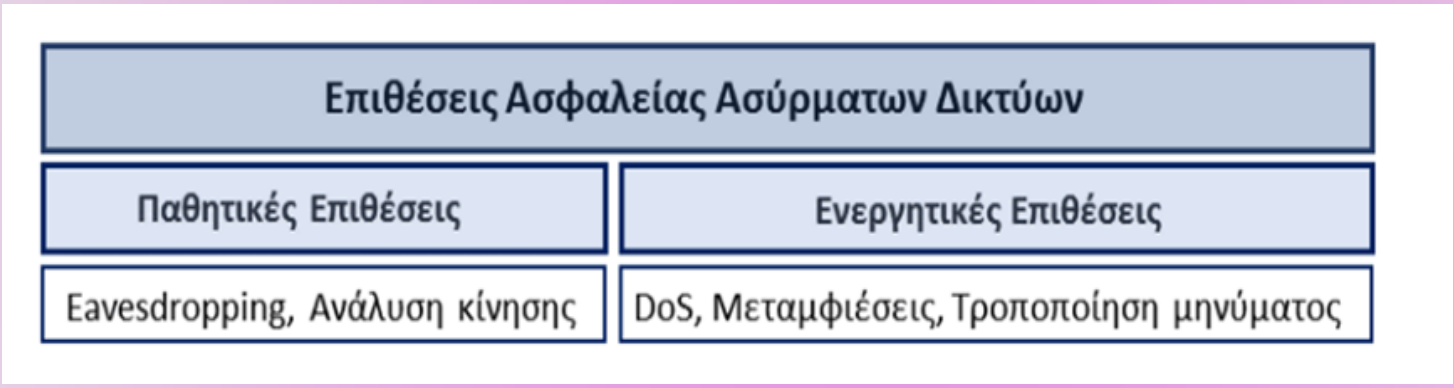
Στις μέρες μας η μετάβαση από τη βιομηχανική κοινωνία στην κοινωνία της πληροφορίας πραγματοποιείται μέσα από τη ραγδαία εξέλιξη των νέων τεχνολογιών πληροφορίας και τηλεπικοινωνίας. Η προστασία των δεδομένων και η παροχή ποιοτικών υπηρεσιών αποτελούν βασικά χαρακτηριστικά που αναζητούνται από τους νόμιμους χρήστες στα σύγχρονα τηλεπικοινωνιακά δίκτυα, ώστε να προστατεύονται από τους κακόβουλους χρήστες (υποκλοπείς)

Πλεονεκτήματα των ασύρματων επικοινωνιών

Οι ραγδαίες τεχνολογικές εξελίξεις δημιούργησαν όλο και περισσότερες προοπτικές για αύξηση της παραγωγής διαφόρων συσκευών ευρείας χρήσης ενώ το κόστος τους μειώθηκε αισθητά, με αποτέλεσμα την τελευταία δεκαετία τα ασύρματα δίκτυα να κατακτούν όλο και περισσότερο την καθημερινότητα μας. Οι τεχνολογίες υπολογιστών και ασυρμάτων επικοινωνιών έχουν καταστεί ένα πολύ σημαντικό κομμάτι της ζωής των ανθρώπων τις τελευταίες δεκαετίες, καθώς τα ασύρματα δίκτυα έχουν πολλά πλεονεκτήματα σε σχέση με τα ενσύρματα δίκτυα.

1. Ευκολία, ευελιξία και απλότητα εγκατάστασης
2. Κόστος
3. Ταχύτητες μετάδοσης
4. Εμβέλεια

Είδη επιθέσεων ασύρματων επικοινωνιών



Απαιτήσεις Ασφαλείας σε Ασύρματα Δίκτυα και Εργαλεία Ασφάλειας

Απαιτήσεις Ασφαλείας

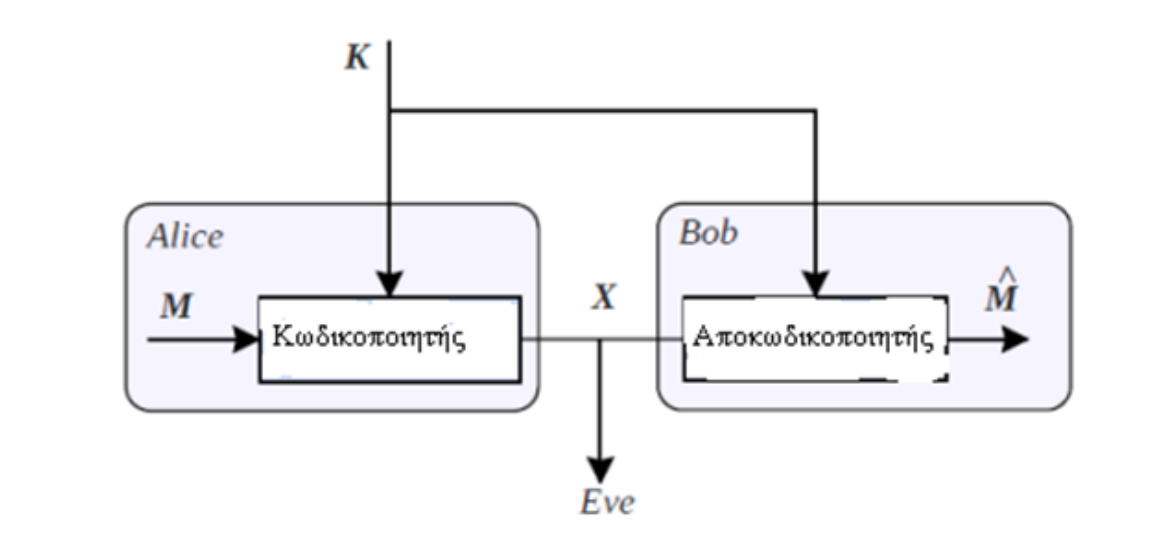
- Εμπιστευτικότητα (Confidentiality)
- Ακεραιότητα (Integrity)
- Αυθεντικοποίηση (Authentication)
- Διαθεσιμότητα (Availability)

Εργαλεία Ασφάλειας

- Τείχος Προστασίας (Firewall)
- Συστήματα Ανίχνευσης Εισβολής
- Κρυπτογραφικά Συστήματα

Βασικές Αρχές της Ασφάλειας Φυσικού Επιπέδου

- Στην πρωτοποριακή εργασία του Shannon αναφέρθηκαν για πρώτη φορά οι βασικές έννοιες της θεωρητικής ασφάλειας πληροφοριών
- Στην ασφάλεια της πληροφορίας ο πομπός αναφέρεται ως Alice, ο νόμιμος δέκτης ως Bob και ο ωτακουστής ως Eve



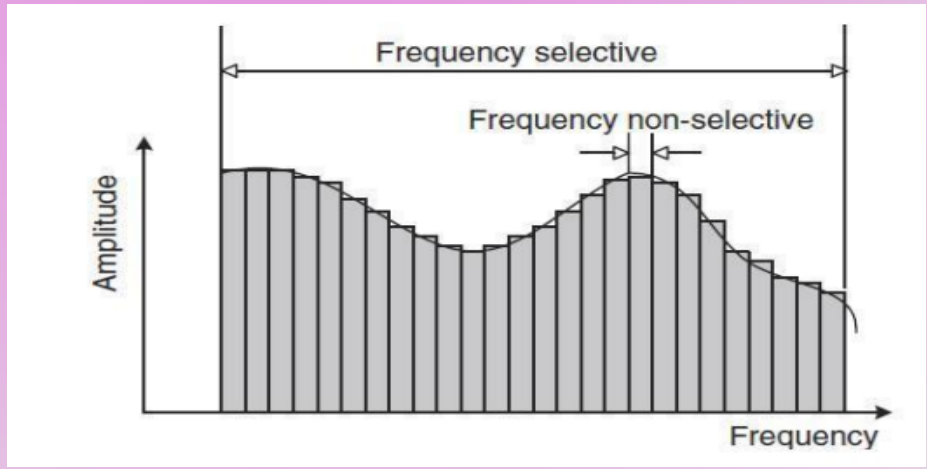
Εκτίμηση Ασύρματου Καναλιού σε Συστήματα OFDM

Η μέθοδος OFDM αποτελεί μία ευέλικτη μέθοδο πολύπλεξης καναλιών με αυξημένη χωρητικότητα που εφαρμόστηκε στις τηλεπικοινωνίες στα τέλη του προηγούμενου αιώνα, είναι η πιο διάσημη τεχνολογία στον χώρο των τηλεπικοινωνιών.

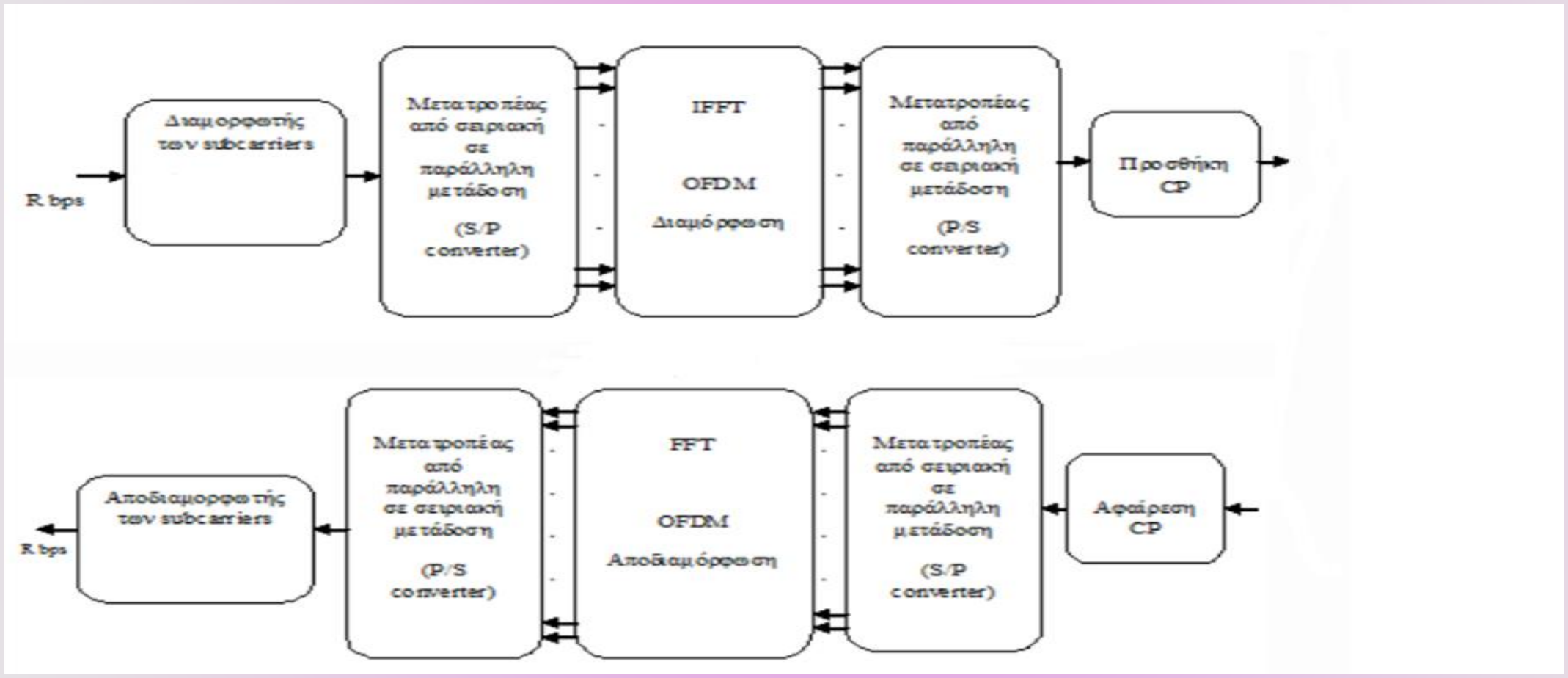
Στην τεχνική OFDM τα σήματα που στέλνονται πρέπει να είναι ορθογώνια και ανεξάρτητα μεταξύ τους, ώστε ο δέκτης να τα δέχεται χωρίς παρεμβολές. Με την χρήση των subcarriers, καταφέρνουμε την διατήρηση της ορθογωνιότητας και παράλληλα την μεγαλύτερη δυνατή εκμετάλλευση του φάσματος. Για να επιτευχθεί αυτό είναι απαραίτητες δύο προϋποθέσεις:

1. Ως προς το πεδίο του χρόνου

2. Ως προς το πεδίο συχνοτήτων



Block Diagram of OFDM



Διαμόρφωση και Αποδιαμόρφωση Σήματος

- Διαμόρφωση σήματος ονομάζεται η διαδικασία μετατροπής των δεδομένων, προκειμένου να διευκολύνεται η μεταφορά τους και να μεταδίδονται με επιτυχία στο μέσο. Οι σημαντικότεροι παράμετροι είναι το πλάτος, η συχνότητα και η φάση. Αντίθετα, αποδιαμόρφωση σήματος είναι η ανάστροφη διαδικασία, ώστε να ανακτηθεί το αρχικό σήμα

- Με τον όρο QPSK αναφερόμαστε στη διαμόρφωση μετατόπισης φάσης με ορθογωνισμό

- Η QAM συνδυάζει τη διαμόρφωση του πλάτους και τη διαμόρφωση της φάσης ταυτόχρονα, δηλαδή διαμορφώνεται μία ημιτονοειδής φέρουσα σε πλάτος και φάση. Κάθε σύμβολο είναι ένας συγκεκριμένος συνδυασμός τιμής πλάτους και φάσης

Ανάλυση και Αποτελέσματα Προσομοίωσης

- Το 5G ασύρματο δίκτυο που μελετά η συγκεκριμένη διπλωματική εργασία χρησιμοποιεί την τεχνική πολύπλεξη/διαμόρφωσης OFDM για την εκπομπή και λήψη του σήματος πληροφορίας

- Η κατανομή πιθανότητας (κατανομή Poisson) της θέσης των πιλοτικών υπομεταφορέων στο φάσμα του σήματος OFDM δημιουργείται μία φορά και γνωστοποιείται στο νόμιμο πομπό (Alice) και στο νόμιμο δέκτη (Bob) κατά τη φάση αυθεντικοποίησης

- Χρησιμοποιήθηκε το MATLAB (matrix laboratory), το οποίο είναι ένα περιβάλλον αριθμητικής υπολογιστικής

- Το πλήθος των bits που στάλθηκαν από τον πομπό στον δέκτη ορίστηκε ως NoBits= 2^{22}, καθώς χρειάζονται αρκετά bits προκειμένου να εμφανιστούν κάποια εσφαλμένα bits όταν ο σηματοθορυβικός λόγος SNR είναι υψηλός.

Ανάλυση και Αποτελέσματα Προσομοίωσης

- Στο πομπό με την χρήση του αντιστρόφου μετασχηματισμού Fourier (IFFT) πραγματοποιείται η μετατροπή του σήματος από το πεδίο συχνοτήτων στο πεδίο του χρόνου

- Ο γρήγορος μετασχηματισμός Fourier απαιτεί το πλήθος των σημείων να είναι δύναμη του 2, για αυτό το λόγο επιλέχθηκε στην εργασία το πλήθος των υποφορέων να είναι 256 (2^8)

- Στο πλήθος των 256 υποφορέων (subcarriers), τα 32 από αυτά μεταφέρουν την πληροφορία των πιλοτικών καναλιών, τα οποία μπαίνουν σε συγκεκριμένες θέσεις ακολουθώντας την κατανομή Poisson και χρησιμοποιούνται από το δέκτη για την αποδιαμόρφωση του σήματος

- Στην προσομοίωση χρησιμοποιήθηκαν οι διαμορφώσεις QPSK και 16-QAM.

- Ο νόμιμος δέκτης και ο ωτακουστής κινούνεται προς την ίδια κατεύθυνση με ταχύτητες 20, 40 και 80 km/h

- Ο σηματοθορυβικός λόγος (SNR) μεταβάλλεται από 0dB μέχρι 60dB με βήμα 5dB

Ανάλυση και Αποτελέσματα Προσομοίωσης

Αποτελέσματα της Προσομοίωσης:

- Ο υπολογισμός των ρυθμού σφαλμάτων bit BER (Bit Error Rate) στον νόμιμο δέκτη (Bob) και στον ωτακουστή (Eve)

$$BER = \frac{Αριθμός\ σφαλμάτων}{Αριθμός\ απεσταλμένων\ bits}$$

- Το διάγραμμα αστερισμού για την κάθε διαμόρφωση

$\log_2 M$

- Η σχέση μεταξύ του σηματοθορυβικού λόγου και του μέσου τετραγωνικού σφάλματος του καναλιού (channel mean square error)

$$CMSE = \sqrt{\sum_{i=1}^{n} \frac{(\hat{y_i} - y_i)^2}{n}}$$

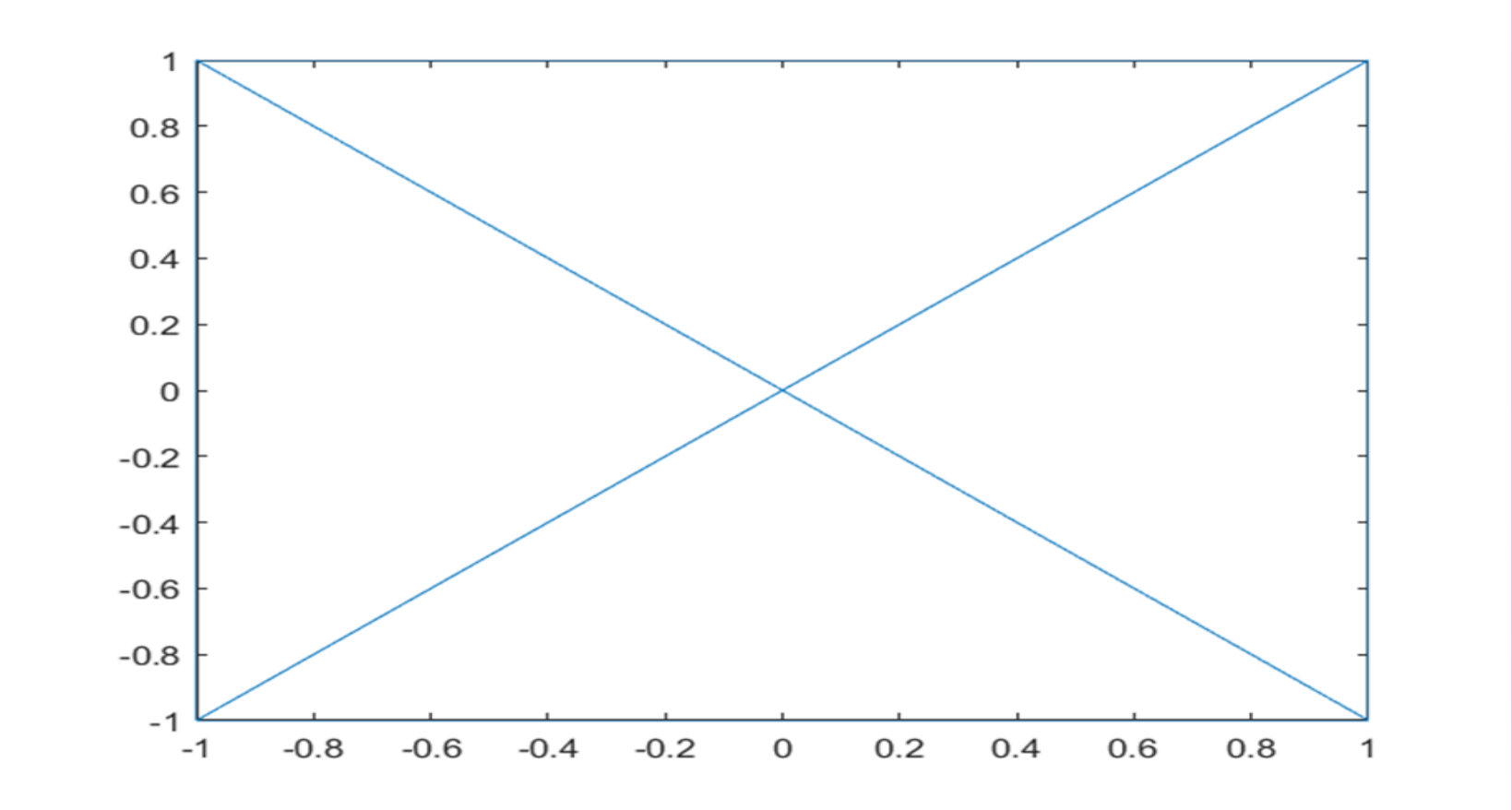
Παράμετροι προσομοίωσης για QPSK και 20 km/h

256 subcarriers		
Εύρος ζώνης (Bandwidth) = 3,5 MHz		
Η συχνότητα του carrier f = 3450 MHz ή 3450 * 10^6 Hz		
Η απόσταση μεταξύ των καναλιών Δf	0,015625	MHz ή 15,625 kHz
Η διάρκεια του συμβόλου OFDM είναι: T_OFDM = 1/Δf	0,064	ή 64 μsec
Η διάρκεια του κυκλικού προθέματος T_CP = 1/8 *T_OFDM	8	μsec
Υποθέτουμε ότι έχουμε εξάπλωση καθυστέρησης Δt = 7,5 μsec		
E_b/N_o = 0 dB μέχρι 60 dB με βήμα 5 dB		
c = λc * f (όπου c= 3*10^8 m/sec και f = 3450 *10^6 Hz)	0,086956522	δηλαδή λc= 0,09 m
v= F_D*λc (για v=20 km/h ή 5,55 m/sec και λc= 0,09 m βρίσκουμε το F_D)	61,66666667	δηλαδή F_D= 61,7 Hz
$F_T = 2*\pi*F_D*\Delta t$	0,00290607	
Συμπληρωματική του F_T είναι 1-0,0029 = 0,9971		

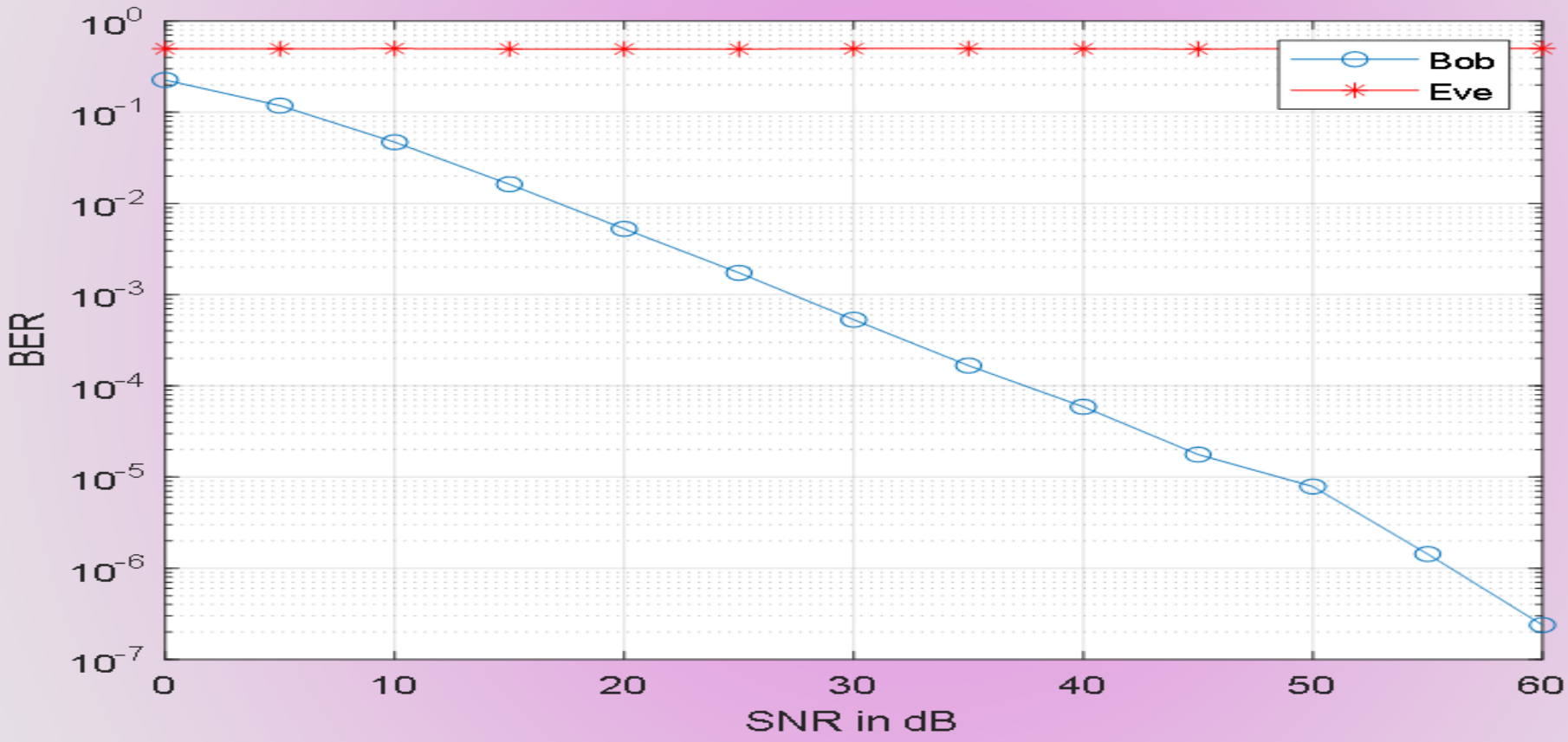
Αποτελέσματα προσομοίωσης QPSK (ταχύτητα 20 km/h)

SNR	BER_Bob	BER_Eve	ch_mse (Bob)	che_mse (Eve)
0	0,226114273	0,498007774	0,125320343	1,044680035
5	0,118266821	0,496880054	0,039809692	1,1697719
10	0,047021389	0,500254154	0,012548424	1,408124227
15	0,016249895	0,49434495	0,003958539	1,586838212
20	0,005268812	0,494142771	0,001237432	1,695060441
25	0,001734018	0,492940426	0,000393841	1,707809767
30	0,000530958	0,498539209	0,00012549	1,753897521
35	0,000166893	0,498727798	0,000039388	1,758463519
40	0,000058889	0,496805668	0,000012486	1,753585099
45	0,000017643	0,494473219	3,9655E-06	1,716586443
50	7,8678E-06	0,49684	1,2407E-06	1,746365509
55	1,4305E-06	0,494959354	3,9598E-07	1,723238671
60	2,3842E-07	0,50055337	1,239E-07	1,750885801

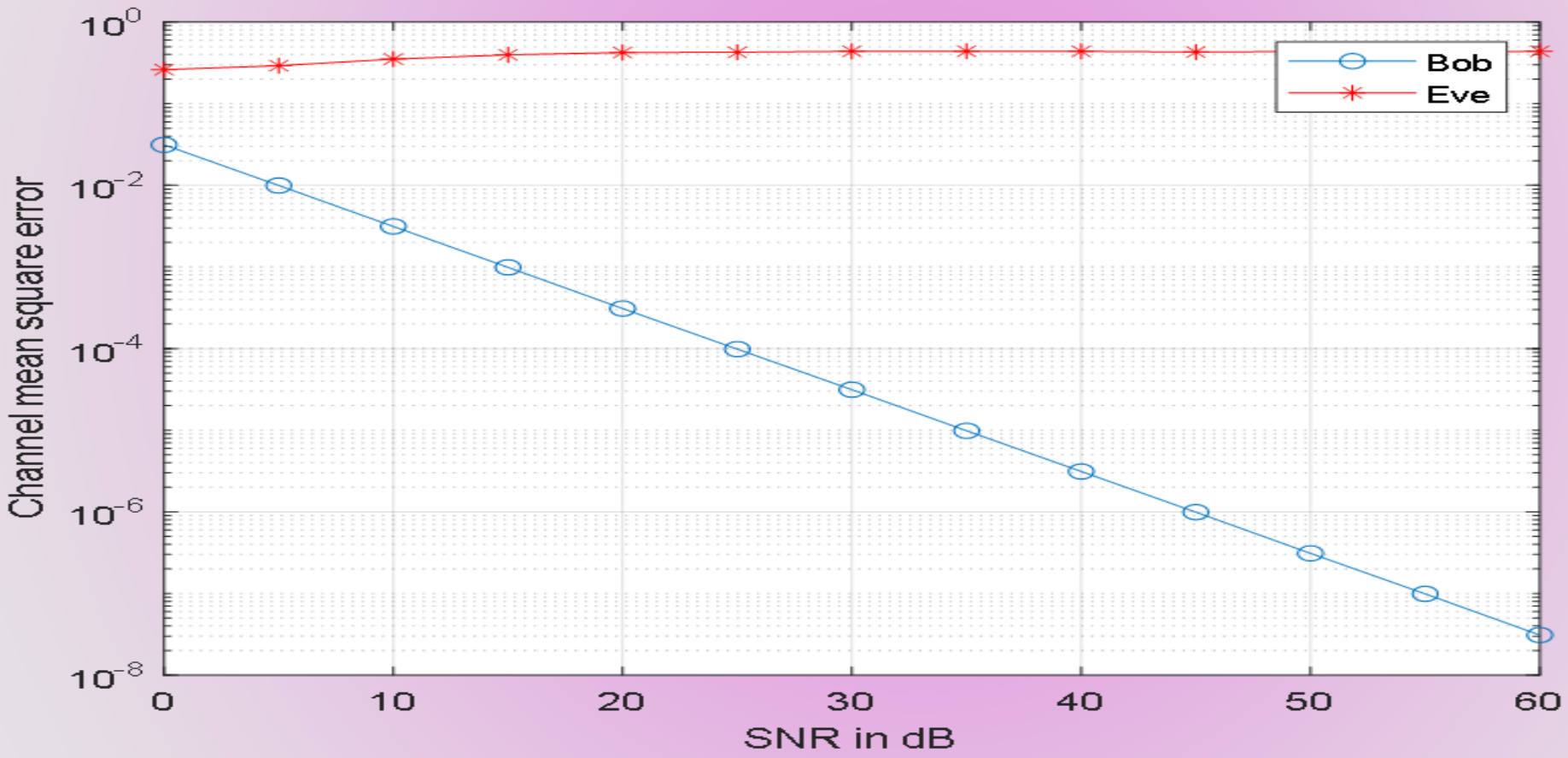
Διάγραμμα Αστερισμού της διαμόρφωσης QPSK



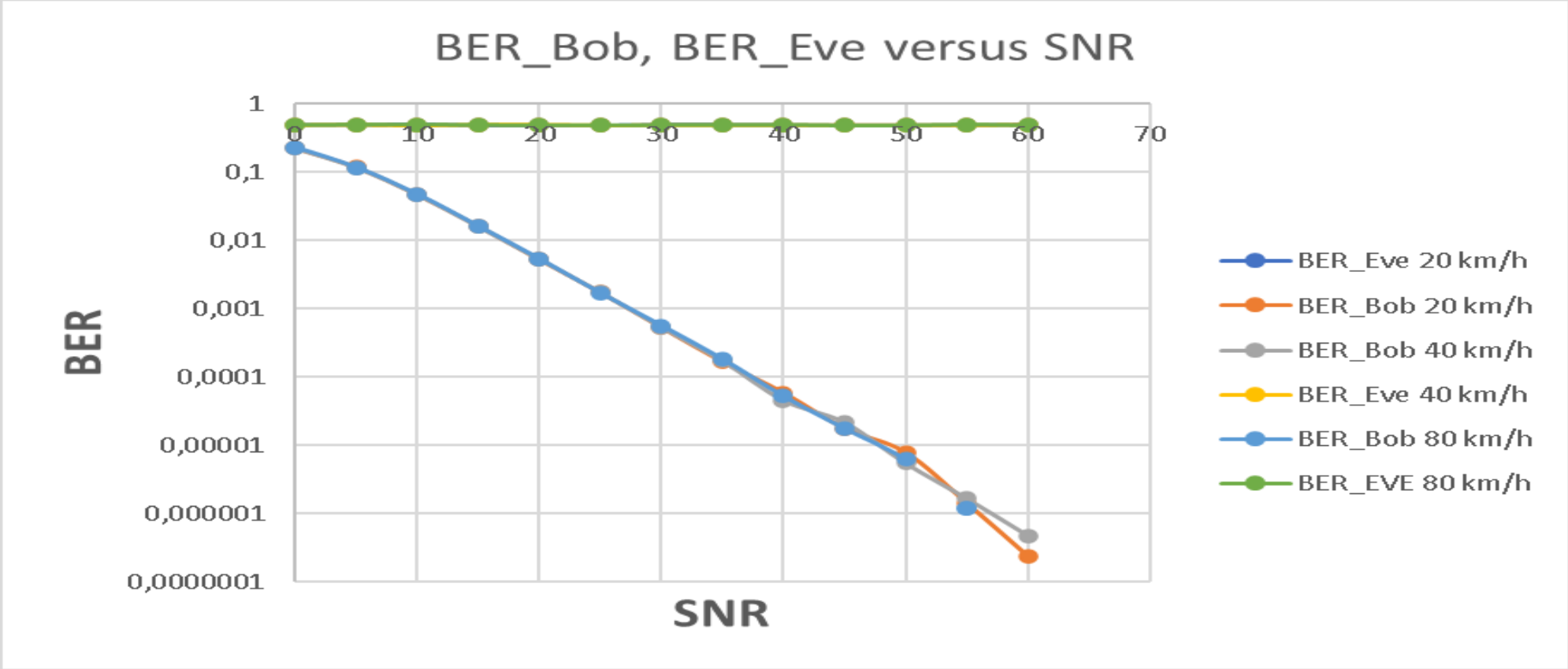
BER του Bob και Eve σε συνάρτηση με το SNR (20km/h)



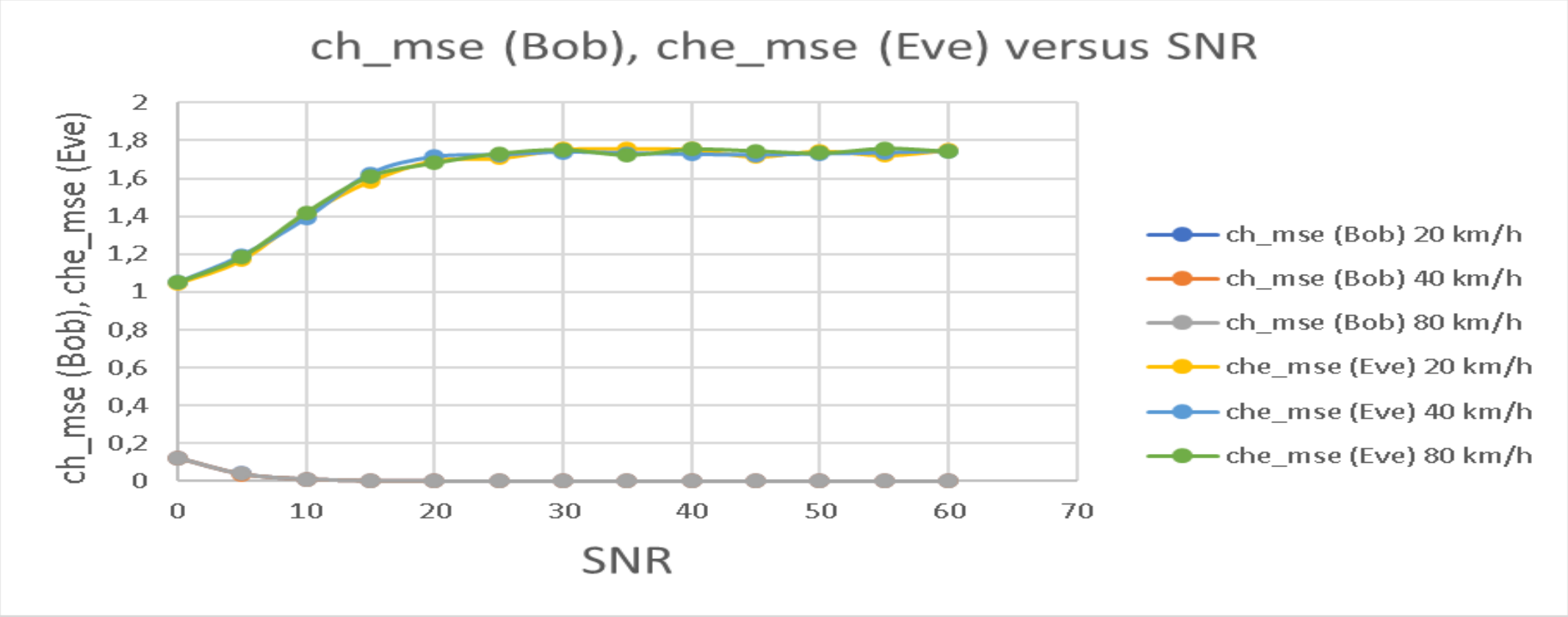
Μέσο τετραγωνικό σφάλμα της εκτίμησης του ασύρματου καναλιού σε συνάρτηση με το SNR (20km/h)



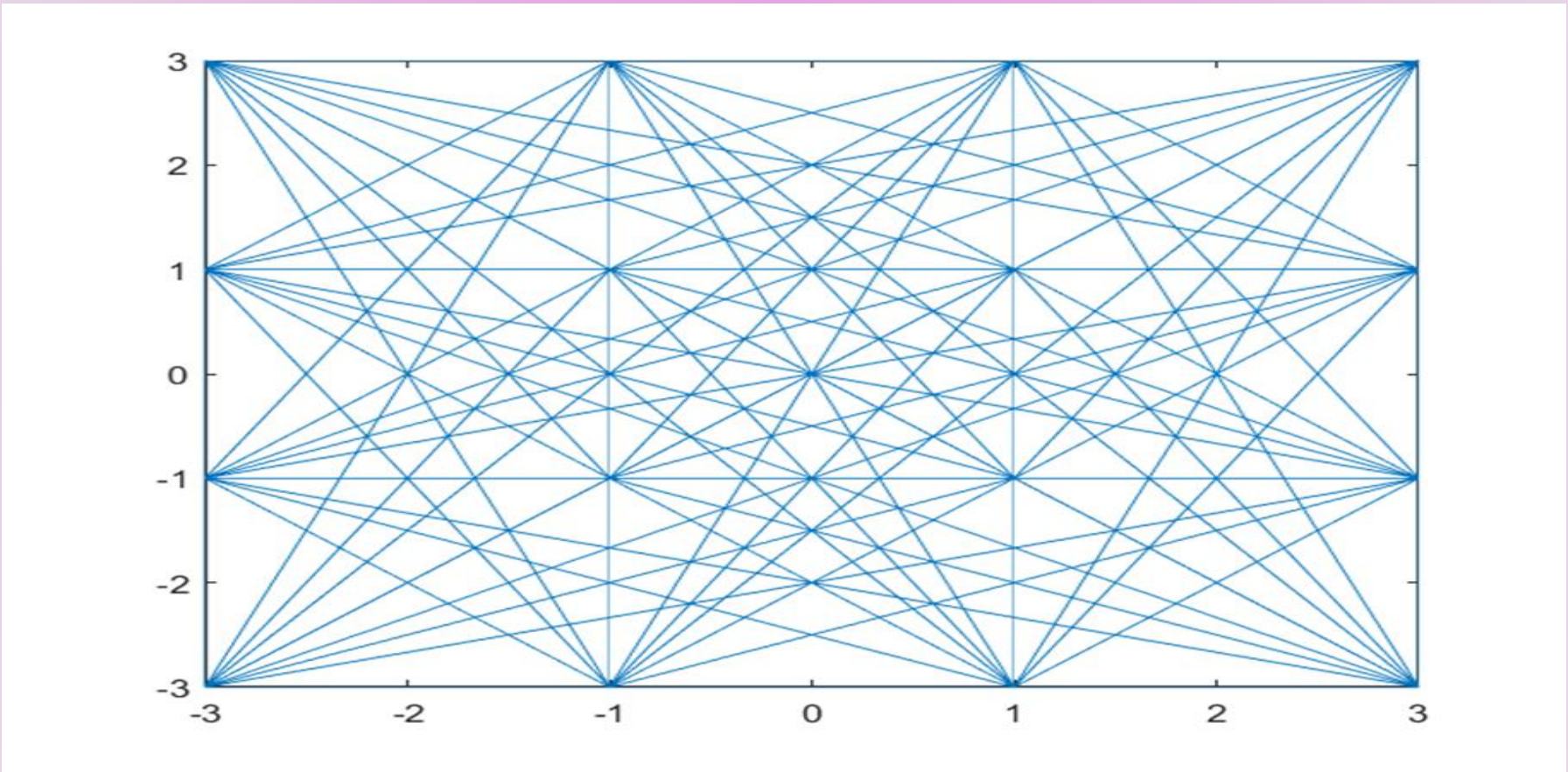
BER_Bob, BER_Eve versus SNR για QPSK



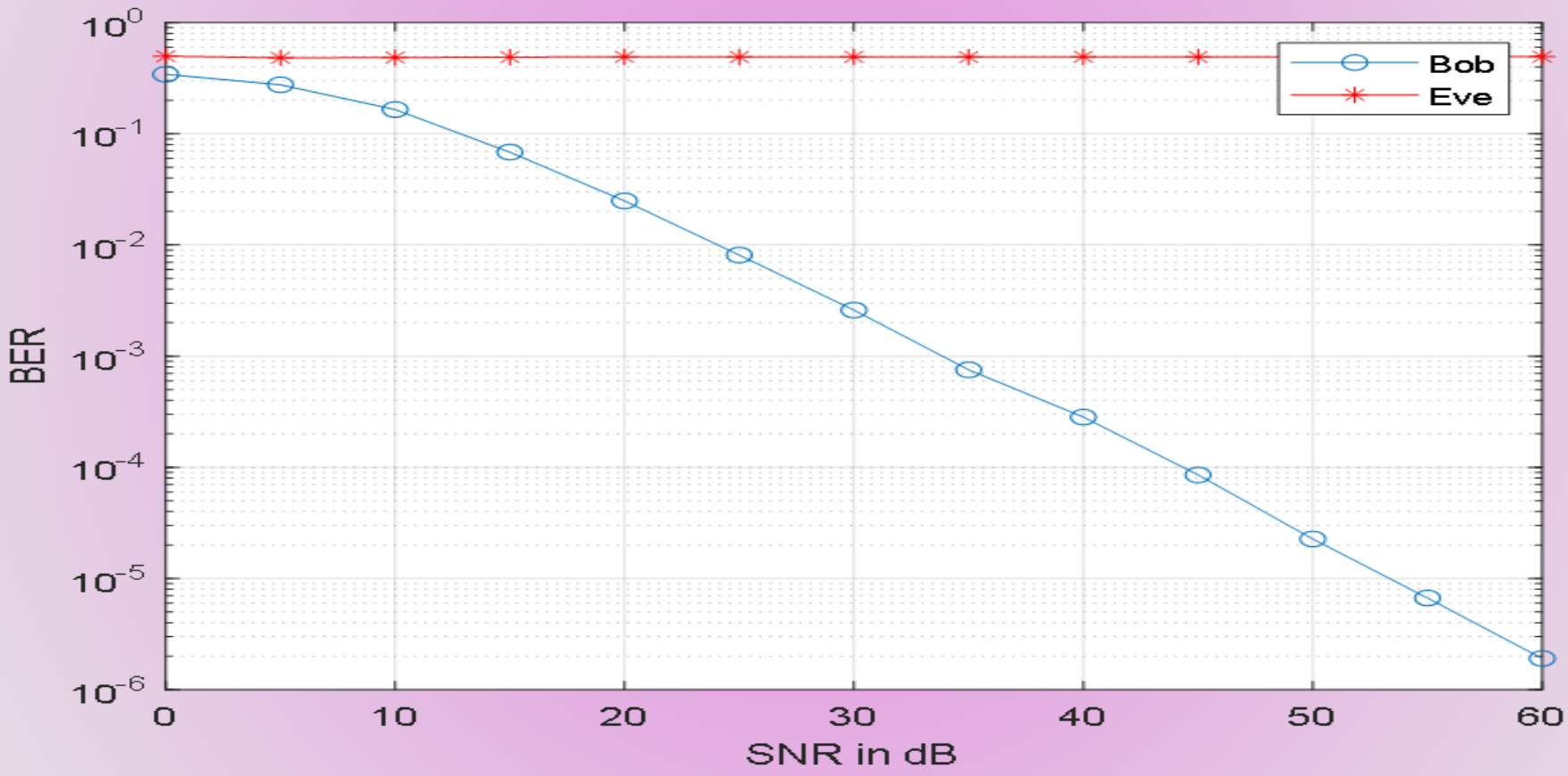
Μέσο τετραγωνικό σφάλμα της εκτίμησης του ασύρματου καναλιού σε συνάρτηση με το SNR για διαμόρφωση QPSK



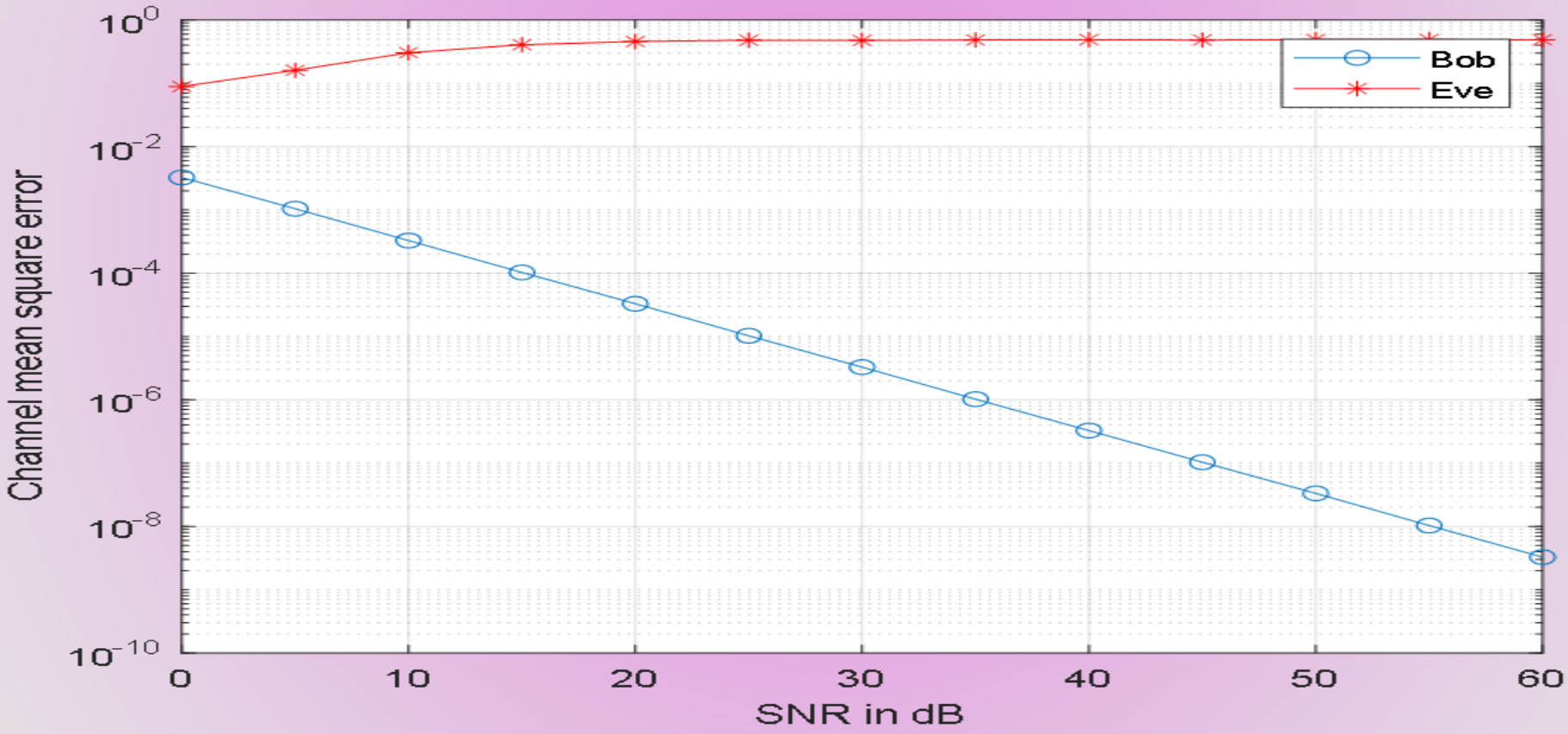
Διάγραμμα Αστερισμού της διαμόρφωσης 16-QAM



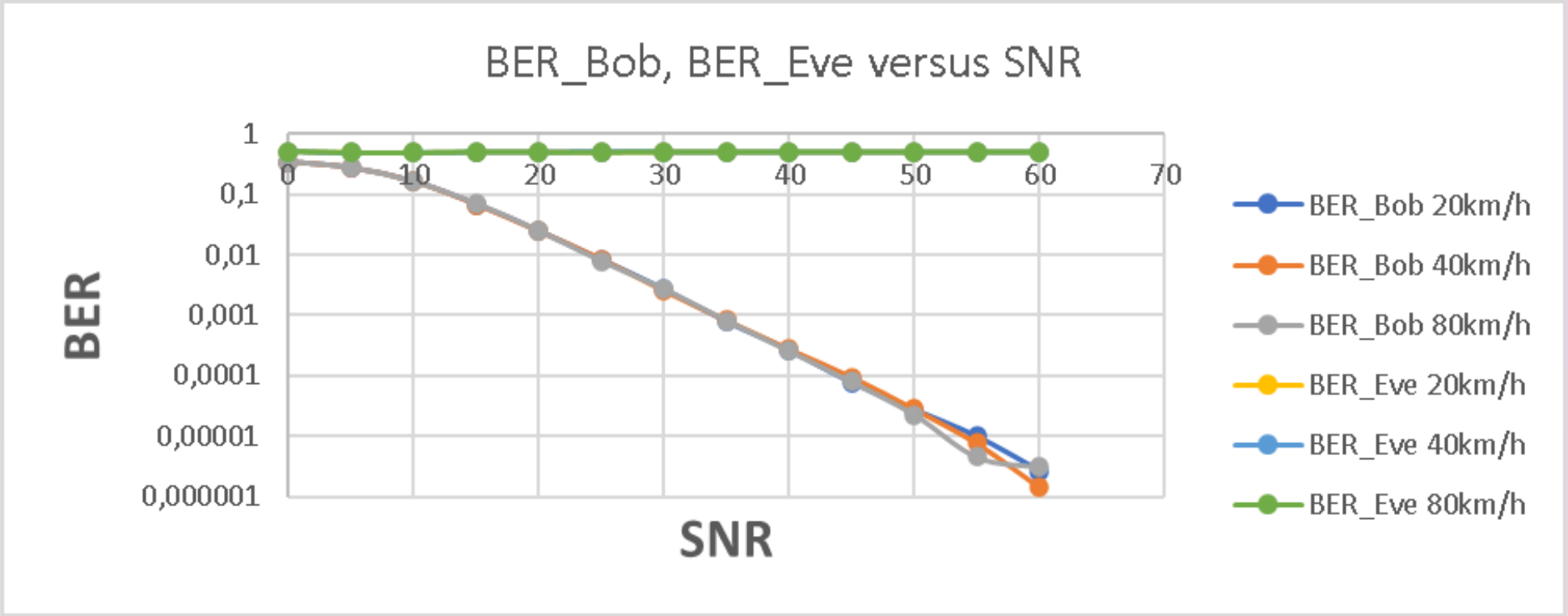
BER του Bob και Eve σε συνάρτηση με το SNR (20 km/h)



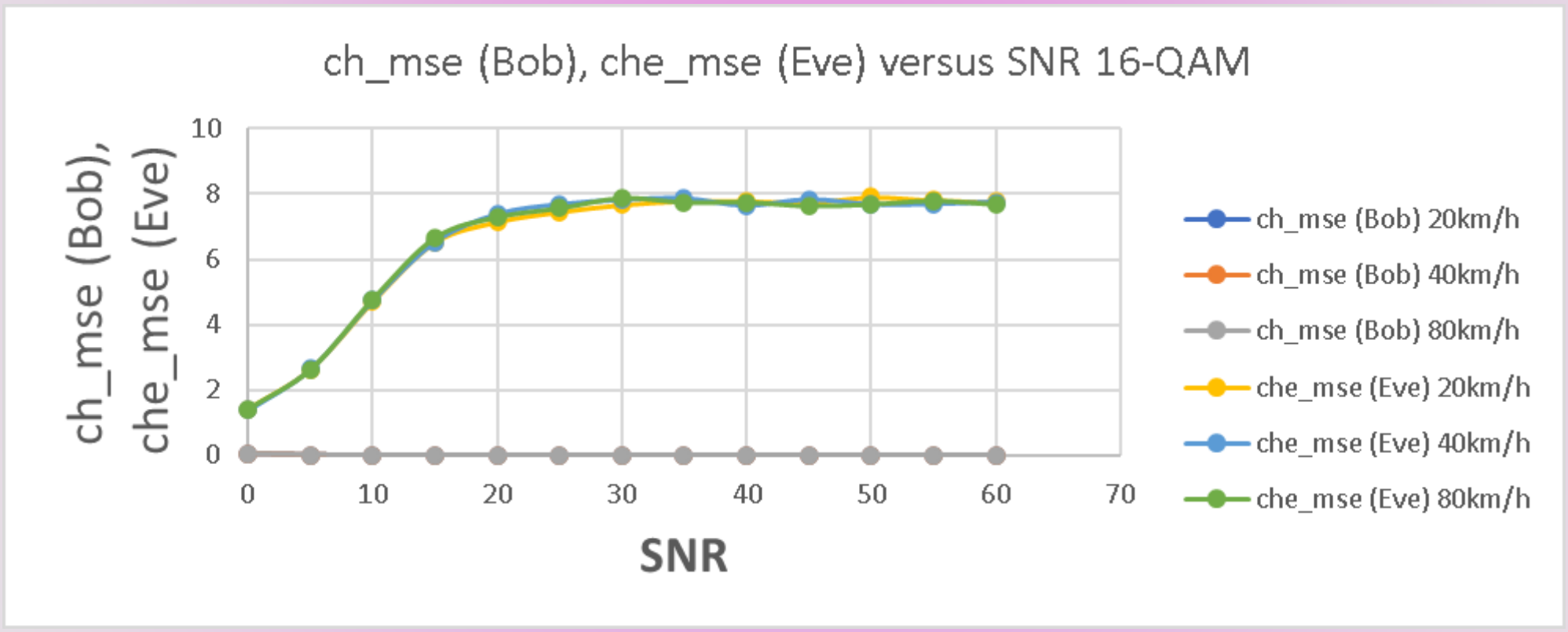
Μέσο τετραγωνικό σφάλμα της εκτίμησης του ασύρματου καναλιού σε συνάρτηση με το SNR για διαμόρφωση 16-QAM (20 km/h)



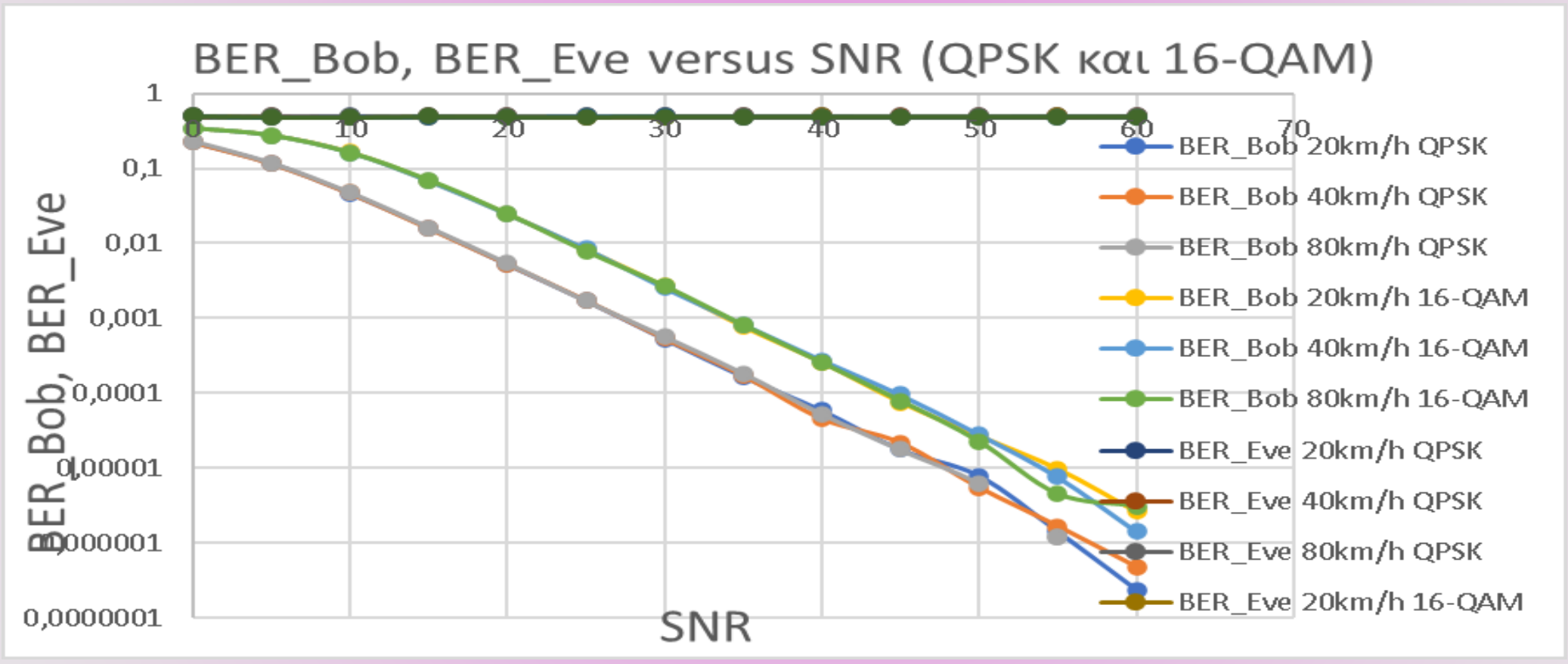
BER_Bob, BER_Eve versus SNR για 16-QAM



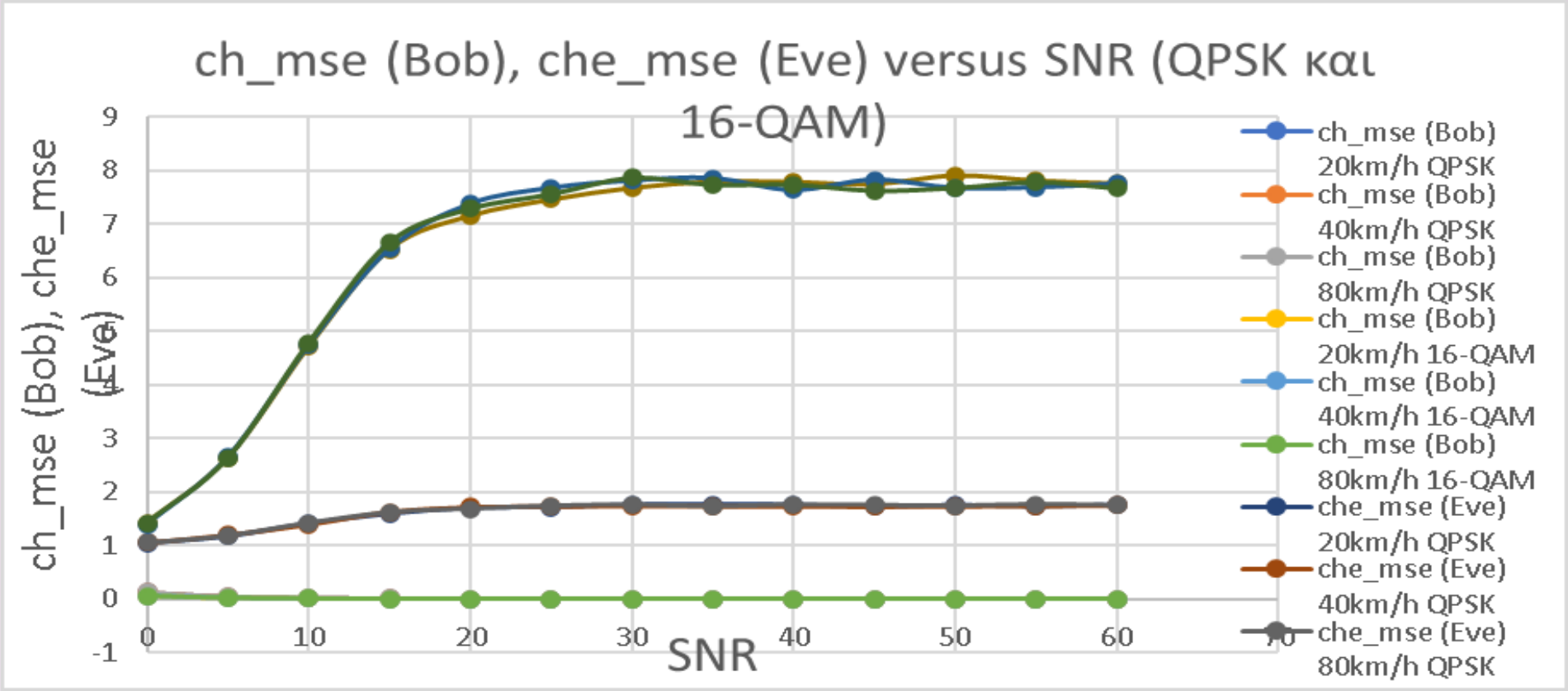
Μέσο τετραγωνικό σφάλμα της εκτίμησης του ασύρματου καναλιού σε συνάρτηση με το SNR για διαμόρφωση 16-QAM



BER_Bob, BER_Eve versus SNR για QPSK και 16-QAM



Μέσο τετραγωνικό σφάλμα της εκτίμησης του ασύρματου καναλιού σε συνάρτηση με το SNR για διαμόρφωση QPSK και 16-QAM



Συμπεράσματα προσομοίωσης

Μέσω της προσομοίωσης μπορούμε να εξάγουμε και να επιβεβαιώσουμε πολύ σημαντικά συμπεράσματα για τον τρόπο συμπεριφοράς του νόμιμου πομπού και δέκτη σε σχέση με τον ωτακουστή, όταν ο ωτακουστής δεν γνωρίζει τις θέσεις των πιλοτικών υποφορέων του OFDM συμβόλου:

- Η προσομοίωση πραγματοποιήθηκε αρκετές φορές, ώστε να επαληθευτούν με ακρίβεια τα αποτελέσματα
- Ο δέκτης του ωτακουστή παρουσιάζει μεγαλύτερο ποσοστό σφάλματος bit (BER), σε σύγκριση με τον νόμιμο δέκτη, οπότε ο νόμιμος πομπός μπορεί να στείλει μεγαλύτερο ρυθμό πληροφορίας με ασφάλεια προς τον νόμιμο δέκτη (χωρητικότητα μυστικότητας)
- Το BER του Bob ελαττώνεται όσο αυξάνεται το SNR, ενώ το BER της Eve μένει σταθερό για οποιαδήποτε τιμή του σηματοθορυβικού λόγου
- Το μέσο τετραγωνικό σφάλμα της εκτίμησης του ασύρματου του καναλιού του Bob μειώνεται και έτσι μπορεί να στείλει περισσότερη πληροφορία με ασφάλεια, ενώ για την Eve παραμένει σταθερή


thank you