ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΗΛΕΚΤΡΙΚΗΣ ΙΣΧΥΟΣ

Ανασκόπηση της κυβερνοασφάλειας συστημάτων βασισμένων σε αντιστροφείς με έμφαση στα μικροδίκτυα

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Αλέξανδρος, Π. Ασώματος

Επιβλέπων : Νικόλαος Χατζηαργυρίου

Ομ. Καθηγητής Ε.Μ.Π

Αθήνα, Ιούνιος 2025

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΗΛΕΚΤΡΙΚΗΣ ΙΣΧΥΟΣ

Ανασκόπηση της κυβερνοασφάλειας συστημάτων βασισμένων σε αντιστροφείς με έμφαση στα μικροδίκτυα

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Αλέξανδρος, Π. Ασώματος

Επιβλέπων : Νικόλαος Χατζηαργυρίου

Ομ. Καθηγητής Ε.Μ.Π

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 25η Ιουνίου 2025

Αθήνα, Ιούνιος 2025

.....	.....	.....
Ν. Χατζηαργυρίου	Γ. Κορρές	Α.Ε. Δημέας
Ομ. Καθηγητής Ε.Μ.Π	Καθηγητής Ε.Μ.Π	Επ. Καθηγητής Ε.Μ.Π

……..…

Αλέξανδρος, Π. Ασώματος

Διπλωματούχος Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π

Περίληψη

Η παρούσα διπλωματική εργασία αποτελεί μια εκτενή βιβλιογραφική μελέτη της κυβερνοασφάλειας σε συστήματα βασισμένα σε αντιστροφείς με ιδιαίτερη έμφαση στα μικροδίκτυα. Στον πυρήνα της, ο οποίος εστιάζει πάνω στον έλεγχο αυτών των συστημάτων, στα διάφορα είδη επιθέσεων που τα απειλούν και στους αμυντικούς μηχανισμούς που είναι αναγκαίο να υλοποιηθούν για την προστασία τους, συγκεντρώθηκαν, μελετήθηκαν και αναλύθηκαν τριάντα έξι συγγράμματα.

Αρχικά, αναφέρονται κάποια εισαγωγικά στοιχεία πάνω στις ανάγκες των εξελισσόμενων ηλεκτρικών δικτύων, στη σπουδαιότητα του αντιστροφέα ως διεπαφή μεταξύ ανανεώσιμων πηγών ενέργειας και δικτύου, στην ικανοποίηση αυτών των αναγκών, καθώς και στη δημιουργία προβλημάτων που προκύπτουν από τη δυνητική χρήση επικοινωνιακών υποδομών, η οποία είναι σημαντική στα ευφυή δίκτυα. Παρουσιάζεται η συνεισφορά της διπλωματικής εργασίας και πραγματοποιείται μια συνοπτική αναφορά του περιεχομένου των κεφαλαίων της.

Στη συνέχεια, παρουσιάζεται το τεχνικό υπόβαθρο των αντιστροφέων καθώς και των τοπολογιών ελέγχου, που συναντώνται, στη δυνητική ύπαρξη ενός ευφυούς δικτύου. Αναφέρονται τα χαρακτηριστικά των μικροδικτύων, τα τμήματα του ιεραρχικού ελέγχου τους, καθώς και οι συνήθεις τοπολογίες. Ακόμα, ορίζονται οι έννοιες της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας και ομαδοποιούνται διάφορα είδη επιθέσεων με βάση το ποια από αυτές προσπαθούν να υποβαθμίσουν.

Επιπλέον, προχωρώντας στο κομμάτι των κυβερνοεπιθέσεων, μελετάται το υλικό του αντιστροφέα και γίνεται κατηγοριοποίηση των επιθέσεων της βιβλιογραφίας ανάλογα με το ποιο τμήμα ελέγχου στοχοποιούν. Περιγράφονται τα σημαντικότερα χαρακτηριστικά τους συμπεριλαμβάνοντας, τη διαδικασία δράσης που ακολουθούν, τα τμήματα του δικτύου που εκμεταλλεύονται, τις λειτουργίες που επηρεάζουν καθώς και την αποτελεσματικότητα τους.

Ακόμα, έχοντας περιγράψει τις επιθέσεις, παρουσιάζονται τα συστήματα εντοπισμού και μετριασμού των επιπτώσεων, με βάση το τμήμα ελέγχου στο οποίο ανήκουν. Τονίζονται οι στρατηγικές άμυνας που ακολουθούνται μαζί με την αποτελεσματικότητα τους, περιγράφονται οι διαδικασίες δράσης τους, τα τμήματα που προστατεύουν, καθώς και εργαλεία που χρησιμοποιούν. Τέλος, παρουσιάζονται προτάσεις για επέκταση της μελέτης καθώς και τα συμπεράσματα της εργασίας.

Λέξεις κλειδιά: Κυβερνοασφάλεια, Αντιστροφέας, Μικροδίκτυο, Κατανεμημένοι ενεργειακοί πόροι, Πρωτογενής, Δευτερογενής, Συναίνεση, Έλεγχος, Κυβερνοεπιθέσεις, Άμυνα, FDI, DoS

ABSTRACT

This diploma thesis constitutes an extensive literature review on cybersecurity in inverter-based systems, with particular emphasis on microgrids. At its' core, which focuses on the control of these systems, the various types of attacks that threaten them, and the defense mechanisms necessary for their protection, thirty six research papers were collected, studied, and analyzed.

Initially, some introductory elements are presented regarding the needs of evolving electrical networks, the importance of inverters acting as interface between the renewable energy sources and the grid and the problems arising from the potential use of communication infrastructures, which are essential in smart grids. The contribution of the diploma thesis is outlined, followed by a brief overview of the content of its chapters.

Subsequently, the technical background of inverters and the control topologies, encountered in the potential existence of a smart grid, are presented. The characteristics of microgrids, the layers of their hierarchical control, and typical control topologies are discussed. Furthermore, the concepts of confidentiality, integrity, and availability are defined, and various types of attacks are categorized according to which of these properties they attempt to compromise.

On the section of cyberattacks, the inverter's hardware is examined, and the attacks found in the literature are categorized based on the control level they target. Their main characteristics are described, including the attack procedures they follow, the components they exploit, the functions they affect, and their effectiveness.

Having described the attacks, the intrusion detection and the impact mitigation systems are presented, according to the control level to which they belong. Defense strategies and their effectiveness are highlighted, along with the methods they employ, the components they protect and the tools they use. Finally, suggestions for further study and the conclusions of the diploma thesis are provided.

Keywords: Cybersecurity, Inverter, Microgrid, Distributed energy resources, Primary, Secondary, Consensus, Control, Cyberattacks, Defense, FDI, DoS

Ευχαριστίες

Στο σημείο αυτό, θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή μου, κ. Νικόλαο Χατζηαργυρίου, που μου έδωσε την ευκαιρία να ασχοληθώ με ένα πολύ ενδιαφέρον και σύγχρονο θέμα.

Επιπλέον, οφείλω ένα μεγάλο ευχαριστώ στην ερευνήτρια Άλκηστις Κοντού, για τη βοήθεια και καθοδήγηση που μου πρόσφερε, καθ' όλη τη διάρκεια εκπόνησης της εργασίας.

Τέλος, ευχαριστώ τους φίλους μου και φυσικά, την οικογένεια μου, που δε σταμάτησε να με βοηθάει και να με στηρίζει όλα αυτά τα χρόνια.

Πίνακας Περιεχομένων

Πίνακας Σχημάτων

Πίνακας Πινάκων

Κεφάλαιο 1

Εισαγωγή

Στο κεφάλαιο αυτό αναφέρονται λίγα λόγια για τις αλλαγές που συμβαίνουν στα δίκτυα με την ολοένα μεγαλύτερη απομάκρυνση από το παραδοσιακό ηλεκτρικό δίκτυο και τη σημασία του αντιστροφέα και της δυνητικής χρήσης μικροδικτύων. Επιπλέον, αναφέρεται η συνεισφορά της εργασίας στη βιβλιογραφία και τέλος παρουσιάζεται συνοπτικά η δομή της.

1.1 Γενικά

Με τις ολοένα αυξανόμενες ενεργειακές ανάγκες και την πίεση που ασκεί η κλιματική αλλαγή, έχουμε αλλαγές στο παραδοσιακό ηλεκτρικό δίκτυο, όπως η αύξηση στη χρήση ανανεώσιμων πηγών ενέργειας και κατανεμημένων ενεργειακών πόρων. Αναμένεται η εμφάνιση εκτενών υποδομών επικοινωνίας μεταξύ διαφόρων τμημάτων του δικτύου, γεγονός που θα διευκολύνει τον έλεγχο της κατανεμημένης παραγωγής και την αμφίδρομη ανταλλαγή πληροφορίας μεταξύ κόμβων, τα οποία βελτιώνουν διάφορους τομείς, όπως την οικονομική λειτουργία του δικτύου. Δυστυχώς, οι παραπάνω αλλαγές στο δίκτυο θα δημιουργήσουν προβλήματα στην ποιότητα ισχύος και θα επιφέρουν μείωση της αδράνειας στο συνολικό σύστημα, οι οποίες μπορεί να προκαλέσουν προβλήματα στην ευστάθεια [1], [2].

Η ευρεία χρήση ηλεκτρονικών ισχύος και η ύπαρξη επικοινωνιακού δικτύου, οδηγεί στην αναβάθμιση του παραδοσιακού δικτύου στο ευφυές δίκτυο. Οι αντιστροφείς αποτελούν σπουδαίο τμήμα του, καθώς έχουν τη δυνατότητα να λειτουργούν ως διεπαφές μεταξύ του ευφυούς δικτύου και κατανεμημένων ενεργειακών πόρων, όπως είναι τα φωτοβολταϊκά, προσφέροντας απαραίτητες βοηθητικές λειτουργίες, όπως η λειτουργία ρύθμισης της συχνότητας μέσω της ισχύος και η λειτουργία fault ride-through. Εδώ αξίζει να αναφερθεί, η σπουδαιότητα δυνητικής χρήσης μικροδικτύων βασισμένων σε αντιστροφείς, στα οποία θα εμβαθύνουμε περισσότερο αργότερα στην εργασία [3], [4].

Η ύπαρξη υποδομών επικοινωνίας στο επίπεδο που μελετάμε, παρά όλα τα θετικά της, θα δημιουργήσει και αισθητά περισσότερες ευκαιρίες για τη διεξαγωγή επιθέσεων κυβερνοασφάλειας, που μπορούν να οδηγήσουν σε καταστροφικές συνέπειες, όπως η πλήρης διακοπή λειτουργίας του δικτύου. Ένα σημαντικό παράδειγμα επίθεσης, είναι η επίθεση εισαγωγής ψευδών δεδομένων (FDI) που ακολούθησε μετά από phising emails και οδήγησε στη διακοπή ηλεκτροδότησης στην Ουκρανία για αρκετές ώρες το 2015 και έπληξε 225000 πελάτες [5]. Αυτά τα νέα προβλήματα στην ασφάλεια των δικτύων έχουν οδηγήσει κυβερνήσεις και οργανισμούς σε δράσεις για την προστασία τους. Υπάρχει ενδιαφέρον ασφαλώς και σε επίπεδο προστασίας μικροδικτύων και λόγω της σπουδαιότητας της δράσης αυτής, θα εμβαθύνουμε στη συνέχεια σε διάφορες περιπτώσεις επιθέσεων καθώς και των προσπαθειών, που έχουν γίνει, για την υλοποίηση επιμελών αμυντικών μηχανισμών.

1.2 Συνεισφορά και δομή της εργασίας

Μελετήθηκε το δημοσιευμένο υλικό που υπάρχει πάνω στον τομέα των ερευνών, των ανασκοπήσεων και των βιβλιογραφικών μελετών της κυβερνοασφάλειας πάνω σε συστήματα βασισμένα σε αντιστροφείς με ιδιαίτερη έμφαση στα μικροδίκτυα. Με βάση τις ελλείψεις που παρατηρήσαμε στον τρόπο προσέγγισης των επιθέσεων, των αμυντικών μηχανισμών και τις κατηγοριοποιήσεις αυτών, ακολουθεί η συνεισφορά αυτής της διπλωματικής εργασίας.

Αρχικά, αξίζει να αναφερθεί ότι στην εργασία, έγινε μια ειδική κατηγοριοποίηση για ένα πλήθος διαφορετικών ειδών επιθέσεων, που είναι γνωστές και στον τομέα της ασφάλειας πληροφορίας και επηρεάζουν τα ηλεκτρικά δίκτυα γενικά, καθώς και τα ευφυή δίκτυα συγκεκριμένα, με βάση το ποια από τις έννοιες της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας υποβαθμίζουν.

Επιπλέον στον τομέα των επιθέσεων, έχει γίνει μελέτη των FDI και DoS επιθέσεων σε διάφορες περιπτώσεις, παραθέτοντας και αναλύοντας μερικά συγγράμματα ως προς τις επιπτώσεις τους και τα συγκεκριμένα επιμέρους κομμάτια που στοχοποιούν. Εξ όσων γνωρίζουμε, δεν έχει γίνει κατηγοριοποίηση αυτών, με βάση συγκεκριμένα το επίπεδο ελέγχου που πλήττουν μέχρι και τον δευτερογενή έλεγχο. Κατόπιν παρατήρησης σημαντικών ομοιοτήτων μεταξύ περιπτώσεων που οι στόχοι ανήκουν στο ίδιο επίπεδο, πραγματοποιήθηκε η παραπάνω κατηγοριοποίηση. Επιπλέον, η εργασία αυτή, μπορούμε να πούμε μετά βεβαιότητας πως είναι η εκτενέστερη βιβλιογραφική μελέτη επιθέσεων πάνω σε συστήματα βασισμένα σε αντιστροφείς, εστιάζοντας στα μικροδίκτυα ειδικά στην απομονωμένη λειτουργία, καθώς έγινε μελέτη και ανάλυση τριάντα έξι συγγραμμάτων.

Στον τομέα της άμυνας απέναντι σε επιθέσεις, παρατηρήσαμε πως γίνεται συχνά κατηγοριοποίηση αυτών, με βάση τη λειτουργία τους και τον τρόπο που διαχειρίζονται το δίκτυο, καθώς και με βάση την ποιότητα των αποτελεσμάτων που παράγουν. Στην εργασία, προστέθηκε και η μεγαλύτερη ακριβής κατηγοριοποίηση με βάση το επίπεδο ελέγχου, στο οποίο εφαρμόζεται ο αμυντικός μηχανισμός κάθε φορά και δόθηκε ιδιαίτερη έμφαση στον διαχωρισμό τους, ανάλογα με το αν επιτελούν τον εντοπισμό της εισβολής, το μετριασμό των επιπτώσεών της στο σύστημα ή συνδυασμό τους. Αξίζει να αναφερθεί πως και σε αυτή την περίπτωση, η μελέτη των μηχανισμών ήταν ιδιαίτερα εκτενής, περιγράφοντας και αναλύοντας τις υλοποιήσεις τους σε είκοσι οχτώ περιπτώσεις των προαναφερθεισών συγγραμμάτων.

Παρακάτω παρουσιάζεται η δομή της εργασίας με βάση τα κεφάλαια στα οποία χωρίστηκε τα οποία είναι τα εξής:

- **Κεφάλαιο 1,** στο οποίο γίνεται μια σύντομη εισαγωγή στις αιτίες απομάκρυνσης

από το παραδοσιακό ηλεκτρικό δίκτυο και η είσοδος στα ευφυή και στη χρήση αντιστροφέων με υποδομές επικοινωνίας. Παρουσιάζεται ακόμα η προσφορά αυτής της βιβλιογραφικής μελέτης και η δομή της.

- **Κεφάλαιο 2,** στο οποίο περιγράφονται τα χαρακτηριστικά των μικροδικτύων, αναφέρονται τα πλεονεκτήματα και οι λόγοι δυνητικής χρήσης τους στα ευφυή δίκτυα, παρουσιάζονται τα είδη και οι τοπολογίες ελέγχου τους και γίνεται μια πρώτη κατηγοριοποίηση διαφόρων ειδών επιθέσεων με βάση το ποιες από τις έννοιες της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας υποβαθμίζουν.
- **Κεφάλαιο 3,** στο οποίο μελετάται η βιβλιογραφία με βάση τις επιθέσεις απέναντι στον αντιστροφέα, στον πρωτογενή έλεγχο του και στο δευτερογενή, δίνοντας ιδιαίτερη έμφαση στα τρωτά σημεία, στις διαδικασίες και στις επιπτώσεις των επιθέσεων σε συστήματα βασισμένα σε αντιστροφείς, με ιδιαίτερη έμφαση στα μικροδίκτυα
- **Κεφάλαιο 4,** στο οποίο περιγράφονται οι αμυντικοί μηχανισμοί που υλοποιούνται για την προστασία απέναντι στις επιθέσεις, επισημαίνοντας τα κύρια χαρακτηριστικά και τις ειδικές λειτουργίες του καθενός.
- **Κεφάλαιο 5,** στο οποίο δίνονται προτάσεις για επέκταση της συγκεκριμένης βιβλιογραφικής μελέτης καθώς και συμπεράσματα που προέκυψαν από την ανάλυση των διαφόρων περιπτώσεων επιθέσεων και αμυντικών διαδικασιών.

Κεφάλαιο 2

Υπόβαθρο αντιστροφέων και ελέγχου μικροδικτύων και επιπτώσεις στην κυβερνοασφάλεια

Σε αυτό το κεφάλαιο παρουσιάζονται οι δύο κατηγορίες αρχιτεκτονικής των αντιστροφέων που μελετήθηκαν ως βάσεις των μικροδικτύων καθώς και μια μελέτη των κύριων κατηγοριών ελέγχου, με βάση την επικοινωνία των ελεγκτών με τους επιμέρους κόμβους. Δίνεται έμφαση στα χαρακτηριστικά των μικροδικτύων μαζί με τον ιεραρχικό έλεγχο τους και τις συνήθεις τοπολογίες τους και τέλος, γίνεται μια σύντομη αναφορά στις έννοιες της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας μαζί με μια κατηγοριοποίηση των επιθέσεων προς ένα ευφυές δίκτυο με βάση το ποιες από αυτές στοχοποιούν.

2.1 Είδη αντιστροφέων

Οι αντιστροφείς που αποτελούν τον πυρήνα της λειτουργίας των συστημάτων που μελετήθηκαν, χωρίζονται σε δύο μεγάλες κατηγορίες με βάση τη λειτουργία τους, το ρόλο που επιτελούν για τις κατανεμημένες μονάδες παραγωγής (DGUs) και την κυκλωματική ανάλυσή τους. Οι κατηγορίες αυτές είναι οι εξής:

2.1.1 Grid-forming αντιστροφείς

Σε αυτή την περίπτωση, έχουμε χρήση του αντιστροφέα σε ένα κύκλωμα, με σκοπό τη δημιουργία και έλεγχο της τάσης και της συχνότητας για το δίκτυο αυτόνομα, γεγονός που κάνει και εμφανή το λόγο για τον οποίο έχουμε ευρεία χρήση τους σε μικροδίκτυα απομονωμένα, από το κεντρικό, δίκτυα. Μια πολύ σημαντική επίσης ιδιότητά τους, είναι το ότι μπορούν να φέρουν σε λειτουργία ένα δίκτυο χωρίς κάποια παροχή ισχύος, κάτι που είναι πολύ σημαντικό σε περιπτώσεις που έχουμε προβλήματα διαθεσιμότητας στο δίκτυο. Το απλοποιημένο κύκλωμα στη συγκεκριμένη περίπτωση, αποτελείται από έναν εξωτερικό βρόγχο τάσης και έναν εσωτερικό βρόγχο ρεύματος [6].

Όσον αφορά το συγχρονισμό με άλλες πηγές εναλλασσόμενου ρεύματος και το υπόλοιπο δίκτυο, κάνουμε χρήση του droop ελέγχου. Σε περιπτώσεις παράλληλα συνδεδεμένων αντιστροφέων, για λόγους συγχρονισμού κάνουμε χρήση των παρακάτω σχέσεων:

$$\omega_n = \omega_{ref} - m_p(P-P_n) \quad (1)$$

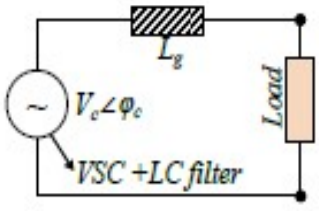
$$V_n=V_{ref}-n_p(Q-Q_n) \quad (2)$$

όπου ω_n, V_n, ω_{ref}, $V_{ref,}$ m_p, n_p, P, Q, P_n, Q_n είναι η συχνότητα και τάση αναφοράς, οι καθολικές τιμές συχνότητας και τάσης που δίνονται από τον δευτερεύοντα ελεγκτή, οι συντελεστές droop ενεργού και άεργου ισχύος, οι τιμές ενεργού και άεργου ισχύος που μετρήσαμε και οι τιμές αναφοράς ενεργού και άεργου ισχύος αντίστοιχα.

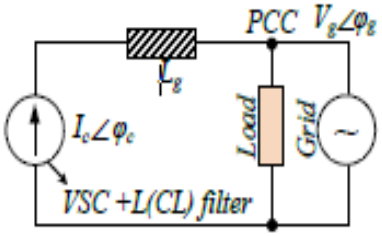
2.1.2 Grid-following αντιστροφείς

Σε αντίθεση με την κατηγορία των grid-forming αντιστροφέων, εδώ δεν έχουμε έλεγχο της τάσης του δικτύου, αλλά το κύκλωμα είναι υπεύθυνο για τον έλεγχο της ποσότητας ρεύματος που χρειάζεται να δοθεί στο δίκτυο ώστε να πληρούνται κάποιες ήδη καθορισμένες τιμές ισχύος. Λόγω αυτών των τιμών αναφοράς, ο αντιστροφέας μπορεί να λειτουργήσει ως grid-feeding αντιστροφέας, δίνοντας ισχύ ανεξάρτητα από τυχόν διακυμάνσεις σε συχνότητα και τάση. Μπορούν να χρησιμοποιηθούν επίσης για την προσαρμογή των καθορισμένων τιμών ενεργού και αέργου ισχύος σε περιπτώσεις τέτοιων διακυμάνσεων. Ένα μεγάλο μειονέκτημα αυτής της κατηγορίας είναι ότι δεν έχουν τη δυνατότητα, όπως οι grid-forming, να τροφοδοτήσουν το δίκτυο με ηλεκτρική αδράνεια, η οποία αναφέρεται στην ικανότητα να αντιδράσει το δίκτυο σε μια αλλαγή στη γωνία της φάσης της τάσης με μια ακαριαία μεταβολή στην ισχύ εξαιτίας της καθυστερημένης αντίδρασης του φασιθέτη της τάσης της γεννήτριας. Επιπλέον, συναντώνται χρονικές καθυστερήσεις στην τροφοδότηση ισχύος στο δίκτυο, εξαιτίας των καθυστερήσεων στην επαναρύθμιση των καθορισμένων τιμών ισχύος μετά από διακυμάνσεις στη συχνότητα, συγκριτικά με άλλες συσκευές που έχουν τη δυνατότητα να προσφέρουν αδράνεια στο δίκτυο [7].

Στην περίπτωση των grid-following αντιστροφέων, το απλοποιημένο κύκλωμα απεικονίζεται στο σχ. 1β. Όπως βλέπουμε, λόγω της κύριας λειτουργίας τους να εγχέουν ρεύμα στο δίκτυο, ο αντιστροφέας αναπαριστάται ως μια πηγή ρεύματος και το υπόλοιπο κύκλωμα αποτελείται από έναν εσωτερικό βρόγχο ελέγχου ρεύματος με ενσωματωμένη απόσβεση, μια μονάδα συγχρονισμού και έναν εξωτερικό βρόγχο ελέγχου τάσης [8].



Σχήμα 2.1: *Απλοποιημένο κύκλωμα grid-forming αντιστροφέα* [9]



Σχήμα 2.2: *Απλοποιημένο κύκλωμα grid-following αντιστροφέα* [9]

2.2 Τοπολογίες επικοινωνίας και ελέγχου σε ένα ευφυές δίκτυο

Σε ένα ευφυές δίκτυο μπορούμε να συναντήσουμε τριών ειδών τοπολογίες στο δίκτυο επικοινωνίας των διαφόρων κόμβων του και ο διαχωρισμός αυτών γίνεται με βάση το σύστημα ελέγχου και τον τρόπο που μια ομάδα κόμβων, όπως είναι κάποιοι αντιστροφείς που βρίσκονται σε επικοινωνία, μοιράζονται δεδομένα μεταξύ τους έτσι ώστε να έχουμε διατήρηση της ευστάθειας στο δίκτυο. Ανάλογα με τις παραμέτρους του δικτύου μας, παραδείγματος χάρη το μέγεθος του ή τον σκοπό που εξυπηρετεί, γίνεται κάθε φορά η επιλογή της κατάλληλης τοπολογίας, καθώς η καθεμία περίπτωση από τις τρεις έχει τα δικά της χαρακτηριστικά και επομένως τα δικά της πλεονεκτήματα και μειονεκτήματα. Τα είδη που αναφέρθηκαν είναι τα εξής:

- Κεντρικός έλεγχος: Στη συγκεκριμένη περίπτωση συναντάμε έναν κεντρικό κόμβο ο οποίος επικοινωνεί με όλους τους υπόλοιπους και έχει πλήρη έλεγχό πάνω στη λειτουργία τους και επομένως ελέγχει τη λειτουργία όλου του δικτύου. Αυτή η τοπολογία, ενώ προσφέρει μεγαλύτερη ευκολία στο συντονισμό των διαφόρων λειτουργιών του δικτύου, ευκολότερη χρήση βελτιστοποιήσεων στο σύνολο του δικτύου και γενικότερα μια πιο απλή και κατανοητή δομή που βοηθάει και στη λήψη αποφάσεων, ταυτόχρονα πάσχει από το γεγονός ότι μπορεί να καταρρεύσει, άμα το κεντρικό σημείο ελέγχου δεχτεί κάποια σοβαρή επίθεση και επιπλέον χρειάζεται εκτεταμένες και σύνθετες υποδομές κάτι που κάνει τη χρήση τους αρκετά κοστοβόρα, ειδικά όταν αναφερόμαστε σε μεγάλης κλίμακας δίκτυα. Το πιο διακεκριμένο κεντρικό σύστημα ελέγχου στην περίπτωση των ευφυών δικτύων, είναι το SCADA [10].
- Αποκεντρωμένος έλεγχος: Σε αυτή την περίπτωση, δεν έχουμε επικοινωνία μεταξύ των διάφορων κόμβων που απαρτίζουν ένα δίκτυο, με αποτέλεσμα να μην έχουμε ανταλλαγή πληροφοριών και μετρήσεων μεταξύ των επιμέρους κομματιών του ευρύτερου δικτύου. Όσον αφορά τα πλεονεκτήματα αυτής της κατηγορίας, σε αντίθεση με το προηγούμενο είδος τοπολογίας, εδώ δεν έχουμε το φόβο κατάρρευσης μεγάλου τμήματος του δικτύου λόγω κάποιας αδυναμίας του κόμβου κεντρικού ελέγχου, ενισχύοντας έτσι την ανθεκτικότητα του δικτύου και την ανοχή του σε σφάλματα και επιπλέον, γίνεται πιο βιώσιμη η δυνατότητα της επεκτασιμότητας του δικτύου. Δυστυχώς όμως, αυτή η κατηγορία συναντάει προβλήματα στο συντονισμό της λειτουργίας αποκεντρωμένων τμημάτων του ευρύτερου δικτύου, καθώς δεν έχουμε την ύπαρξη σταθερών υποδομών επικοινωνίας [11].

- Κατανεμημένος έλεγχος: Στην περίπτωση αυτή έχουμε ένα αποκεντρωμένο είδος ελέγχου, με τη διαφορά πως οι τοπικοί κατανεμημένοι ελεγκτές επικοινωνούν μεταξύ τους, ανταλλάσοντας δεδομένα απαραίτητα για τη λειτουργία του δικτύου. Αυτό το είδος, προσφέρει επεκτασιμότητα, ανθεκτικότητα σε αρνητικές μεταβολές και ταχύτερες τοπικές αποκρίσεις, θετικά που τον καθιστούν ιδανικό για μικροδίκτυα σε πολλές περιπτώσεις. Ούτε αυτή η περίπτωση όμως δεν είναι χωρίς αρνητικά χαρακτηριστικά, καθώς αυξάνει την πολυπλοκότητα στο συντονισμό των επιμέρους τοπικών κόμβων και εξαρτάται από την ύπαρξη επικοινωνιακού δικτύου [12].

2.3 Μικροδίκτυα και ο έλεγχός τους

Με τον όρο μικροδίκτυο αναφερόμαστε σε συστήματα ισχύος μικρότερου βεληνεκούς, η δυνητική χρήση των οποίων γίνεται όλο και πιο συμφέρουσα μέσα στα ευφυή δίκτυα λόγω της δυνατότητάς τους να μπορούν να λειτουργούν και απομονωμένα, αλλά και συνδεδεμένα στο υπόλοιπο δίκτυο διατηρώντας, σε κάθε περίπτωση, την ευσταθή λειτουργία τους, ενώ ταυτόχρονα επιτυγχάνουν διαφορετικούς στόχους. Με την όλο και μεγαλύτερη ενσωμάτωση κατανεμημένων ανανεώσιμων ενεργειακών πόρων, η οποία καθίσταται απαραίτητη λόγω των οφελών που έχει σε πολύ σημαντικούς τομείς, όπως είναι το περιβάλλον και η οικονομία [13], τα μικροδίκτυα βασισμένα σε ηλεκτρονικά ισχύος παρουσιάζουν άλλο έναν λόγο για τη δυνητική τους χρήση. Με βάση τον τύπο του ρεύματος που χρησιμοποιούν, τα μικροδίκτυα κατηγοριοποιούνται σε συνεχούς ρεύματος, εναλλασσόμενου ρεύματος και υβριδικά και εμείς εστιάζουμε κυρίως στην κατηγορία των εναλλασσόμενων χωρίς αυτό να σημαίνει ότι κάποια χαρακτηριστικά δεν είναι κοινά και για τις άλλες κατηγορίες. Κάποια από τα πλεονεκτήματά τους, πέρα από την πολύ σημαντική τους δυνατότητα να λειτουργούν απομονωμένα αλλά και συνδεδεμένα στο κεντρικό ηλεκτρικό δίκτυο, είναι τα εξής:

- Η μείωση της απόστασης από τα συνδεδεμένα φορτία σε ένα μικροδίκτυο θα οδηγήσει σε μεγάλη μείωση των απωλειών κατά τη μετάδοση ισχύος και συνολικά η χρήση τους βελτιώνει τη διαχείριση των απαιτήσεων ενέργειας που έχουν τα συνδεδεμένα φορτία.
- Η δυνατότητα τους να συνεχίζουν να λειτουργούν ομαλά, σε περίπτωση που χρειαστεί να αποκοπούν από το υπόλοιπο δίκτυο, χρησιμοποιώντας τον προστατευτικό εξοπλισμό

που έχουν στη διάθεσή τους, είναι πολύ σημαντική ειδικά σε περιπτώσεις που εξυπηρετούν τις ενεργειακές απαιτήσεις κρίσιμων φορτίων για το κοινωνικό σύνολο.

- Η ευρεία χρήση συστημάτων βασισμένων σε αντιστροφείς στα μικροδίκτυα, θα συμβάλλει και στην εξουδετέρωση αρμονικών συνιστωσών πέρα από την παροχή της απαιτούμενης τάσης.
- Μικροδίκτυα τα οποία είναι συνδεδεμένα στο κεντρικό δίκτυο, προσφέρουν τη δυνατότητα της απόκρισης-ζήτησης, γεγονός που σημαίνει πως μπορούν να προσαρμόζουν τις ενεργειακές τους απαιτήσεις, κάτι που συμβάλλει στην εύρυθμη λειτουργία του υπόλοιπου δικτύου και έχει οικονομικά οφέλη.

2.4 Επίπεδα ελέγχου με τις τοπολογίες που συναντώνται

Κάθε μικροδίκτυο καλείται, όπως αναφέραμε και προηγουμένως, να μπορεί να λειτουργήσει και συνδεδεμένο στο κεντρικό δίκτυο, αλλά και απομονωμένο ακόμα και σε περίπτωση που η αλλαγή λειτουργίας του πρέπει να γίνει απότομα. Η απομόνωση γίνεται με τη χρήση ενός διακόπτη απομόνωσης στο σημείο κοινής σύζευξης και το απομονωμένο πια δίκτυο πρέπει να μπορεί να συνεχίσει, να διατηρήσει την ευστάθεια του ως προς την τάση και τη συχνότητα, να προσαρμοστεί όσον αφορά το διαμοιρασμό ενεργού και άεργου ισχύος και να συνεχίσει να επιτυγχάνει αντιστάθμιση των ανεπιθύμητων αρμονικών συνιστωσών της τάσης [14].

Στην περίπτωση που ένα μικροδίκτυο λειτουργεί όσο είναι ακόμα συνδεδεμένο στο υπόλοιπο δίκτυο, ο έλεγχος του είναι λιγότερο σύνθετος ακολουθώντας την αρχιτεκτονική κεντρικού ελέγχου ενεργού/άεργου ισχύος, όπου οι αντιστροφείς του μικροδικτύου είναι συνήθως grid-following και παίζουν επομένως το ρόλο πηγών ρεύματος παρέχοντας ισχύ στο υπόλοιπο δίκτυο ακολουθώντας τη συχνότητα που δίνεται από αυτό, χρησιμοποιώντας ένα PLL(phase-locked loop) για το συγχρονισμό των φάσεων της τάσης του μικροδικτύου με αυτή του κύριου δικτύου στο οποίο παραμένει συνδεδεμένο. Ενώ είναι πιο συνηθισμένο στην περίπτωση που το μικροδίκτυο λειτουργεί απομονωμένο από το κύριο δίκτυο, μπορούμε και σε αυτή την περίπτωση να συναντήσουμε ένα σύστημα ελέγχου που χρησιμοποιεί droop έλεγχο και περιλαμβάνει απαραίτητα και grid-forming αντιστροφείς.

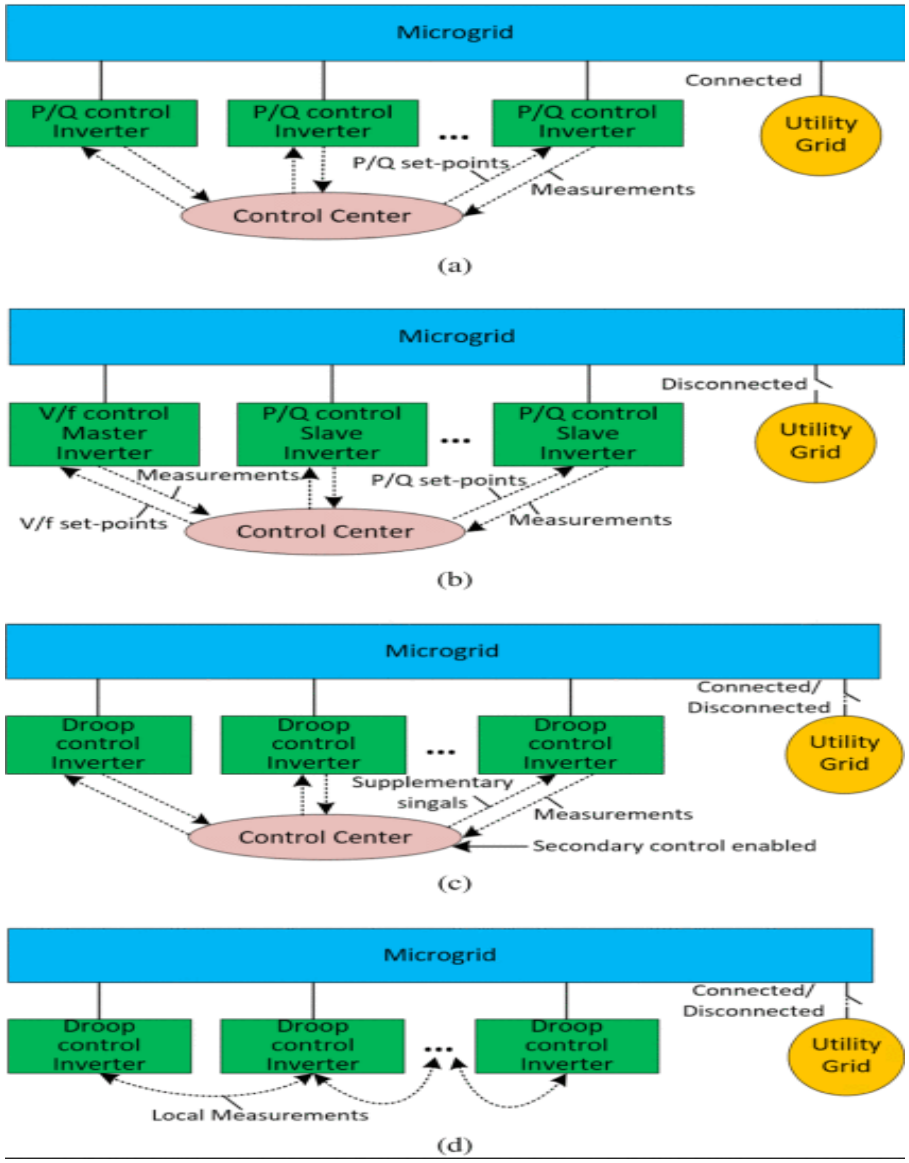
Μελετώντας τις περιπτώσεις που ένα μικροδίκτυο καλείται να λειτουργήσει αποσυνδεδεμένο από το κύριο δίκτυο, διαπιστώνουμε ότι ο έλεγχος στα μικροδίκτυα είναι συχνά πιο πολύπλοκος. Πιθανότατα, η πιο απλουστευμένη αρχιτεκτονική ελέγχου που συναντάμε στην αποσυνδεδεμένη

κατάσταση αποκαλείται αρχιτεκτονική master-slave (Αφέντη-Σκλάβου) όπου ένας grid-forming αντιστροφέας "δημιουργεί" το δίκτυο δίνοντας τις τιμές της τάσης και της συχνότητας του δικτύου, ενώ οι υπόλοιποι grid-following αντιστροφείς ακολουθούν, ενώ βρίσκονται σε λειτουργία ελέγχου ενεργού/άεργου ισχύος. Ο έλεγχος στην αποσυνδεδεμένη κατάσταση διακρίνεται στους βρόγχους ελέγχου ρεύματος και τάσης του αντιστροφέα, στον πρωτογενή, στον δευτερογενή και στον τριτογενή. Το πρωτογενές κομμάτι του ελέγχου αποτελείται από τον droop έλεγχο [15], ο οποίος μιμείται τα χαρακτηριστικά του droop των σύγχρονων γεννητριών και ρυθμίζει την τάση και τη συχνότητα με βάση τις τοπικές τιμές της άεργου και ενεργού ισχύος αντίστοιχα. Πέραν του απλού droop ελέγχου, αξίζει να σημειωθεί ότι υπάρχουν και άλλες μέθοδοι ελέγχου σε grid-forming αντιστροφείς είτε βασισμένες στο droop, είτε όχι [7]. Δυστυχώς, μετά το πέρας του πρωτογενούς ελέγχου, συναντούμε αποκλίσεις στις επιθυμητές τιμές της τάσης και της συχνότητας και εξαιτίας αυτών, κρίνεται απαραίτητη η εισαγωγή μεθόδων δευτερογενούς ελέγχου, οι οποίες στοχεύουν κυρίως στην εξάλειψη αυτών των αποκλίσεων, αλλά και βοηθούν στη βελτίωση της ποιότητας της τάσης απομακρύνοντας ανεπιθύμητες αρμονικές συνιστώσες.

Έχοντας αναφέρει τη μέθοδο του ελέγχου droop, μπορούμε να μιλήσουμε για ακόμα δύο κατηγορίες αρχιτεκτονικών μικροδικτύων που χρησιμοποιούν και αυτή τη μέθοδο ελέγχου. Στην πρώτη από αυτές κάθε κόμβος αντιστροφέα ορίζει αποκεντρωμένα τις τιμές στόχους για την ενεργό και άεργο ισχύ με βάση τις τοπικές τιμές της συχνότητας και της τάσης και στη συνέχεια γίνεται χρήση κεντρικού δευτερογενούς ελέγχου από το σύστημα των επιμέρους κόμβων του μικροδικτύου προκειμένου να εξαλειφθούν οι αποκλίσεις που προκαλούνται με το πέρας του πρωτογενούς ελέγχου.

Στην επόμενη κατηγορία βλέπουμε ένα κατανεμημένο σύστημα ελέγχου, όπου κάθε επιμέρους κόμβος επικοινωνεί απευθείας με ένα υποσύνολο όλων των υπόλοιπων, ανταλλάσσοντας δεδομένα, ακολουθώντας κάποια τεχνική δευτερογενή ελέγχου, όπως είναι αυτή που βασίζεται σε ένα σύστημα συναίνεσης. Ο κατανεμημένος έλεγχος με τη χρήση συναινετικού δευτερογενούς ελέγχου είναι ιδιαίτερα συνηθισμένος [16],[17],[18] και θα το συναντήσουμε σε διάφορα παραδείγματα στη συνέχεια. Στο Σχ.2.3 έχουμε μια απεικόνιση των προαναφερθεισών αρχιτεκτονικών [19]. Τέλος, το σχήμα ελέγχου στα μικροδίκτυα κλείνει με τον τριτογενή που μπορεί να υλοποιείται είτε κεντρικά, είτε αποκεντρωμένα. Το συγκεκριμένο επίπεδο ελέγχου ασχολείται με θέματα όπως είναι, η βελτιστοποίηση της διαχείρισης της ενέργειας συμπεριλαμβάνοντας αποφάσεις όπως το πότε να φορτιστεί ή να αποφορτιστεί ένα σύστημα αποθήκευσης ενέργειας (ESS), η ελαχιστοποίηση των διαφόρων λειτουργικών κοστών, η υλοποίηση στρατηγικών απόκρισης-ζήτησης με σκοπό τη διαχείριση κατανάλωσης ενέργειας σε διάφορα φορτία σύμφωνα με διακύμανση τιμών της αγοράς ή άλλους εξωτερικούς παράγοντες και

διάφορες άλλες περιπτώσεις σχετικές με τα οικονομικά και ενεργειακά χαρακτηριστικά ενός δικτύου. Κατανοούμε λοιπόν, πως το πεδίο εφαρμογής αυτού του επιπέδου ελέγχου, σε αντίθεση με τον πρωτογενή και τον δευτερογενή έλεγχο, απαιτεί πιο εκτενείς υποδομές επικοινωνίας από αυτές του μικροδικτύου, γεγονός που σημαίνει την ύπαρξη μεγαλύτερης ποικιλίας στις μεθόδους που ακολουθούνται, προκειμένου να οδηγηθούμε στη συνολική βελτιστοποίηση της λειτουργίας ενός δικτύου [20].



Σχήμα 2.3: *Τοπολογίες ελέγχου στα μικροδίκτυα* [19]

2.5 Εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα και κατηγοριοποίηση επιθέσεων με βάση αυτές

Εξαιτίας της αυξημένης πολυπλοκότητας των κυβερνοφυσικών ευφυών δικτύων, η οποία αποτελεί απόρροια των πολλών επιμέρους συστημάτων τα οποία χρειάζεται να είναι σε συνεχή επικοινωνία για να επιτελούν τις σύνθετες λειτουργίες για τις οποίες χρησιμοποιούνται, εμφανίζονται πολλά σημεία τα οποία είναι ευάλωτα σε επιθέσεις. Επομένως, ένα από τα σημαντικότερα στοιχεία αυτών των δομών, η διαλειτουργικότητα, είναι και μια από τις βασικές αιτίες δημιουργίας τρωτών σημείων σε διάφορα κομμάτια των δικτύων. Αυτές οι επιθέσεις, σε θεμελιώδες επίπεδο, έχουν ως στόχο την υποβάθμιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας (confidentiality, integrity, availability - CIA) των ηλεκτρικών δικτύων όπως συμβαίνει και γενικά στον τομέα της ασφάλειας πληροφοριών (InfoSec). Παρά το γεγονός ότι και στους δύο τομείς, ενδιαφερόμαστε για τη διασφάλιση των τριών εννοιών που προαναφέρθηκαν, υπάρχουν σημαντικές διαφορές και στην εφαρμογή της κάθε έννοιας στον κάθε τομέα αλλά και στη σπουδαιότητα του ρόλου που παίζει η καθεμία, στον κάθε τομέα ξεχωριστά. Οι διαφορές είναι οι εξής:

- **Εμπιστευτικότητα**: Με αυτόν τον όρο, στον τομέα της ασφάλειας πληροφοριών, αναφερόμαστε στην προστασία ευαίσθητων δεδομένων όπως είναι τα προσωπικά και περιουσιακά στοιχεία από τη μη εξουσιοδοτημένη πρόσβαση και αποκάλυψή τους. Έτσι, στον InfoSec τομέα, η εμπιστευτικότητα είναι πολύ μεγαλύτερης σπουδαιότητας απ' ότι στα ηλεκτρικά δίκτυα, όπου εστιάζουμε παραπάνω στην εξασφάλιση της μεταφοράς και διανομής του ηλεκτρικού ρεύματος. Παρά αυτό το γεγονός, συνεχίζει να είναι σημαντική η προστασία των δεδομένων των πελατών του ηλεκτρικού δικτύου όπως αυτά της κατανάλωσης, καθώς η μη εξουσιοδοτημένη γνωστοποίηση τους θα μπορούσε να οδηγήσει σε μεγάλα προβλήματα στην αγορά ηλεκτρικής ενέργειας [21].
- **Ακεραιότητα**: Η προστασία των δεδομένων από τη μη εξουσιοδοτημένη αλλοίωσή τους είναι ιδιαίτερα σημαντική και για τους δύο τομείς. Συγκεκριμένα στον τομέα των ηλεκτρικών δικτύων, αδυναμία προστασίας στοιχείων, όπως τα διάφορα σήματα ελέγχου, μπορεί να οδηγήσει στη μη ομαλή λειτουργία τμημάτων του ηλεκτρικού δικτύου ή ακόμα και στην παντελή αδυναμία διανομής ρεύματος σε περιοχές.
- **Διαθεσιμότητα**: Ενώ αποτελεί γεγονός, ότι η διαθεσιμότητα υπηρεσιών και η δυνατότητα πρόσβασης σε δεδομένα ανά πάσα στιγμή, κάτι που περιλαμβάνει και την προστασία κατά μιας μεγάλης κατηγορίας επιθέσεων (DoS), είναι μεγάλης σημασίας για τον InfoSec τομέα,

για τον τομέα ηλεκτρικών δικτύων η διαθεσιμότητα, είναι με διαφορά η σημαντικότερη από τις τρεις έννοιες. Η διαθεσιμότητα στα ευφυή δίκτυα σχετίζεται με την αδιάκοπη λειτουργία όλων των συστημάτων που εμπλέκονται στη λειτουργία του δικτύου όπως είναι τα SCADA συστήματα, συστήματα διαχείρισης της διανομής, κατανεμημένα κέντρα ελέγχου και όλα τα δίκτυα επικοινωνίας τους με εξωτερικά δίκτυα [22]. Η διασφάλιση της σταθερής παροχής ηλεκτρικού ρεύματος στους καταναλωτές αποτελεί προτεραιότητα για τους χειριστές των δικτύων, καθώς ακόμα και οποιαδήποτε αστάθεια, μπορεί να έχει σημαντικές συνέπειες στο κοινωνικό σύνολο.

Με βάση τις τρεις έννοιες που περιγράψαμε συντόμως παραπάνω (εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα), μπορούμε να κατηγοριοποιήσουμε και τους τύπους των επιθέσεων που είναι κοινοί μεταξύ του InfoSec τομέα και του ευρύτερου τομέα των δικτύων ηλεκτρικής ενέργειας.

1. **<u>Επιθέσεις εναντίον της εμπιστευτικότητας</u>**:

   - <u>Eavesdropping</u>: Σε αυτή την περίπτωση, συναντάμε τον υπεύθυνο για την επίθεση να έχει τη δυνατότητα να παρεμβληθεί, μεταξύ δύο τουλάχιστον επιμέρους μερών ενός δικτύου τα οποία βρίσκονται σε επικοινωνία, με σκοπό να λάβει πληροφορίες οι οποίες μπορούν αργότερα να χρησιμοποιηθούν για κακόβουλες δράσεις, όπως η χειραγώγηση της αγοράς (pricing attacks) ή και καταστολή της λειτουργίας του ηλεκτρικού δικτύου λόγω εύρεσης κάποιου τρωτού σημείου. Στο [23] αναφέρεται η σημασία προστασίας του δικτύου έναντι αυτών των επιθέσεων και προτείνεται ένας τρόπος άμυνας που έχει ώς στόχο την απόκρυψη των διάφορων μετρήσεων κατά τη μετάδοσή τους από το ένα σημείο στο άλλο εντός του δικτύου επικοινωνίας.
   - <u>Social engineering</u>: Αυτού του είδους οι επιθέσεις, αποτελούν έναν μεγάλο κίνδυνο για την ασφάλεια του δικτύου, καθώς αναφέρονται στην προσπάθεια χειραγώγησης εργαζομένων με στόχο είτε την αποκάλυψη ευαίσθητων δεδομένων, είτε ακόμα και τη διεξαγωγή κάποιας ενέργειας που μπορεί να επηρεάσει την ακεραιότητα και τη διαθεσιμότητα του δικτύου. Η συγκεκριμένη κατηγορία επιθέσεων περιλαμβάνει τις εξής υποκατηγορίες [24]:

     i. Phising
     ii. Pretexting
     iii. Επίθεση με τη χρήση δολώματος (baiting)
     iv. Ψυχολογική χειραγώγηση μέσω φόβου, κάποιου αισθήματος αναγκαιότητας ή και με το να προσποιηθεί ο επιτιθέμενος κάποιον ανώτερο του θύματος

v. Συλλογή στοιχείων από το διαδίκτυο για κάποιον υπάλληλο, με σκοπό το χτίσιμο μιας σχέσης εμπιστοσύνης ή και ακόμα και τον εκβιασμό του

vi. Χρήση κάποιου ανταλλάγματος (quid pro quo attacks)

- Ανάλυση της κίνησης: Ο επιτιθέμενος αναλύει την κίνηση μέσα στα κανάλια επικοινωνίας ενός δικτύου μεταξύ μερών του δικτύου όπως είναι οι αισθητήρες και οι μετρητές, χρησιμοποιώντας διάφορα εργαλεία λογισμικού, με στόχο τη συγκέντρωση πληροφοριών όπως τα διάφορα προφίλ φορτίου, την κατάσταση του εξοπλισμού που χρησιμοποιείται και ακόμα και αδυναμίες στα πρωτόκολλα που χρησιμοποιούνται και στην παραμετροποίηση του κάθε δικτύου.

2. Επιθέσεις εναντίον της ακεραιότητας:

- Εισαγωγή ψευδών δεδομένων (FDI): Αυτή η κατηγορία επιθέσεων αποτελεί μια από τις μεγαλύτερες κατηγορίες και ταυτόχρονα μια από τις πιο επικίνδυνες για ένα ηλεκτρικό δίκτυο με πιθανές καταστροφικές συνέπειες για το ανθρώπινο κοινωνικό σύνολο, όπως είναι η διακοπή δυνατότητας παροχής ηλεκτρικής ενέργειας και η καταστροφή του εξοπλισμού επιμέρους τμημάτων του δικτύου. Οι επιθέσεις της συγκεκριμένης κατηγορίας μπορούν να φέρουν την αλλοίωση σημαντικών παραμέτρων, όπως είναι οι διάφορες μετρήσεις επηρεάζοντας το αποτέλεσμα της διαδικασίας της εκτίμησης κατάστασης[25] που αποτελεί μια πολύ σημαντική λειτουργία των SCADA για την διατήρηση της ευστάθειας του δικτύου. Ακόμα, στο [26] έχουμε μελέτη επιθέσεων σε ευφυή δίκτυα οι οποίες έχουν στόχο τη διαδικασία, αυτή τη φορά, της μη γραμμικής εκτίμησης κατάστασης και στο [27] αναφέρεται η δυνατότητα αυτής της κατηγορίας επιθέσεων να ενεργοποιήσει την ακολουθία διακοπής λειτουργίας ενός επιμέρους κομματιού του δικτύου επηρεάζοντας και άλλα εξαρτώμενα κομμάτια οδηγώντας, λόγω κλιμάκωσης, σε διαδοχικές διακοπές ρεύματος. Επιπλέον, στο [28] συζητείται η περαιτέρω εκμετάλλευση της τοπολογίας επιμέρους κομματιών του δικτύου, με στόχο την πρόκληση κλιμακωτών επιπτώσεων στο δίκτυο. Αξίζει να αναφερθεί εδώ, μια πολύ σημαντική υποκατηγορία FDI επιθέσεων, οι επιθέσεις αναδιανομής φορτίου. Αυτή η κατηγορία αναφέρεται σε πιο ρεαλιστικά σενάρια επιθέσεων, καθώς μπορούν να επηρεαστούν μόνο μετρήσεις φορτίων κόμβων και ροής ισχύος γραμμής, ενώ μετρήσεις κεντρικών γεννητριών ή κόμβων μηδενικού φορτίου δε μπορούν να επηρεαστούν [29]. Όπως αναφέρεται και στις προαναφερθείσες πηγές, οι επιθέσεις αυτής της κατηγορίας είναι ακόμα πιο επικίνδυνες λόγω της ικανότητάς τους, σε κάποιες περιπτώσεις, να παρακάμπτουν ή να ξεγελούν τους αλγόριθμους ανίχνευσης ψεύτικων δεδομένων που είναι

εφαρμοσμένοι.

- Man in the Middle: Και σε αυτή την περίπτωση αναφερόμαστε σε μια πολύ ευρεία κατηγορία επιθέσεων για περιπτώσεις που συναντάμε επιμέρους κόμβους που χρειάζεται να ανταλλάξουν πληροφορίες. Ο επιτιθέμενος συνδέεται ως τρίτος κόμβος ανάμεσα στους δύο, που ανταλλάσσουν πληροφορίες, εν αγνοία τους, με τη δυνατότητα να αλλοιώσει τις συγκεκριμένες πληροφορίες πέρα από το να τις υποκλέψει [30]. Παραδείγματα τέτοιων κόμβων μπορεί να είναι δύο απλές συσκευές πεδίου, αλλά μπορεί να εμπλέκεται ακόμα και το σύστημα SCADA και ο ελεγκτής. Μία από τις πιο συνηθισμένες επιθέσεις MitM λέγεται ARP(address resolution protocol) spoofing, η οποία έχει ως στόχο τη σύνδεση της διεύθυνσης MAC του επιτιθέμενου με τη διεύθυνση IP του θύματος. Στα [30],[31] περιγράφονται δύο τέτοιες περιπτώσεις επιθέσεων χρησιμοποιώντας το ettercap λογισμικό για να επιτευχθεί το ARP spoofing. Οι spoofing επιθέσεις δεν έχουν ως στόχο μόνο το ARP. Στην περίπτωση που αποδέκτης της επίθεσης σε ένα δίκτυο είναι τα PMUs (phasor movement units), συναντάμε το GPS spoofing, κατά το οποίο χαρακτηρίζεται γενικά από παραγωγή τεχνητών GPS σημάτων. Για παράδειγμα, μπορούμε να ανταλλάξουμε τις δύο ομάδες μετρήσεων, που ανήκουν σε κανάλια δύο διαφορετικών PMUs, χωρίς να αλλαχθούν οι τιμές των μετρήσεων, αλλάζοντας τις πληροφορίες των τοποθεσιών από όπου παίρνονται αυτές οι μετρήσεις [32].
- Επαναποστολή πληροφοριών (replay attacks): Αυτές οι επιθέσεις στέλνουν ξανά στοιχεία, όπως διαφόρα είδη μετρήσεων, τα οποία έχουν υποκλαπεί από κάποιο κανάλι επικοινωνίας, δυσκολεύοντας την ανίχνευση τους, καθώς μιλάμε για δεδομένα τα οποία σε παλαιότερη στιγμή ήταν αυθεντικά. Συνεπώς, μπορούμε να έχουμε προβλήματα στη ροή ισχύος, χρονικές καθυστερήσεις και γενικά να έρθει το δίκτυο σε αστάθεια. Ο πολύ γνωστός ιός Stuxnet συνδέεται με τη συγκεκριμένη κατηγορία επιθέσεων [33]. Στα [34][35] μελετώνται κάποιες περιπτώσεις replay επιθέσεων και παρουσιάζονται και κάποια συστήματα άμυνας εναντίον τους, είτε μέσω πρόληψης, είτε μέσω αντιμετώπισης κατά τη διάρκεια εκτέλεσής τους.

3. **Επιθέσεις εναντίον της διαθεσιμότητας**:

- Denial of Service (DoS): Αυτή η κατηγορία επιθέσεων απέναντι σε διάφορα επιμέρους κομμάτια ενός ευφυούς δικτύου, είναι ιδιαίτερα σημαντική καθώς αποσκοπεί στη διακοπή της λειτουργίας κρίσιμων υποδομών του δικτύου, επηρεάζοντας έτσι άμεσα τη σημαντικότερη από τις τρεις έννοιες του CIA για ένα δίκτυο, τη διαθεσιμότητα, καθιστώντας πιθανή την αδυναμία παροχής ηλεκτρικού

ρεύματος σε κομμάτια του ανθρώπινου κοινωνικού συνόλου. Οι συγκεκριμένες επιθέσεις γίνονται ακόμα πιο ισχυρές και επικίνδυνες, όταν προέρχονται συντονισμένα και ταυτόχρονα από ένα πλήθος τερματικών, τα οποία συχνά είναι συσκευές, που εξαιτίας κάποιου προβλήματος ασφάλειας, βρίσκονται στην κατοχή του επιτιθέμενου δημιουργώντας έτσι τα λεγόμενα Botnets. Αυτή η ειδική υποκατηγορία επιθέσεων ονομάζεται Distributed Denial of Service (DDoS) [36].

Ένας τύπος DoS επιθέσεων είναι οι επιθέσεις πλημμύρας (flooding). Με το όνομα αυτό αναφερόμαστε στην παραγωγή πολύ μεγάλης ποσότητας κίνησης στους συνδέσμους στα κανάλια επικοινωνίας δύο ή περισσότερων επιμέρους κόμβων με στόχο την πρόκληση ασυνήθιστων καθυστερήσεων στη μετάδοση των σημαντικών πληροφοριών, οδηγώντας έτσι σε προβλήματα διαθεσιμότητας του ηλεκτρικού δικτύου [14],[37].

Άλλη μια υποκατηγορία είναι αυτή των επιθέσεων μπλοκαρίσματος (Jamming). Σε αυτή την περίπτωση, ο επιτιθέμενος δημιουργεί και αναμεταδίδει τυχαία σήματα με στόχο τη δημιουργία εμποδίων στην επικοινωνία των εξουσιοδοτημένων συσκευών, που προσπαθούν να επικοινωνήσουν, προκαλώντας έτσι καθυστερήσεις στην επικοινωνία και γενικότερα, προβλήματα στην ομαλή λειτουργία κομματιών του ευφυούς δικτύου [38][39].

Στο Σχ. 2.4 παραθέτουμε ένα ποσοτικό διάγραμμα των επιθέσεων της βιβλιογραφίας που μελετάται στη συνέχεια της εργασίας, ομαδοποιώντας τις με βάση τις κατηγορίες που περιγράφτηκαν. Παραλείπεται η κατηγορία των επιθέσεων εναντίον της εμπιστευτικότητας, καθώς αυτού του είδους οι επιθέσεις προηγούνται των βασικών επιθέσεων που βλάπτουν τα συστήματα, αφού έχουν ως σκοπό τη συλλογή των απαραίτητων πληροφοριών για τη διεξαγωγή τους.

Σχήμα 2.4: *Ποσοτικό διάγραμμα για τις επιθέσεις που μελετήθηκαν*

Κεφάλαιο 3

Κυβερνοεπιθέσεις σε συστήματα βασισμένα σε αντιστροφείς με έμφαση στα μικροδίκτυα

Στο κεφάλαιο αυτό γίνεται μελέτη των επιθέσεων σε συστήματα βασισμένα σε αντιστροφείς με κυριότερη μελέτη αυτών που στοχοποιούν μικροδίκτυα. Ομαδοποιούνται με βάση το επίπεδο ελέγχου, βλέποντας περιπτώσεις που αφορούν το υλικό του αντιστροφέα, τον πρωτογενή έλεγχο και τον δευτερογενή, δίνοντας έμφαση στα τρωτά σημεία που εκμεταλλεύονται, στη διαδικασία δράσης τους, στις λειτουργίες που επηρεάζουν και στα χαρακτηριστικά που τις κάνουν δύσκολο να αντιμετωπιστούν από συμβατικούς αμυντικούς μηχανισμούς.

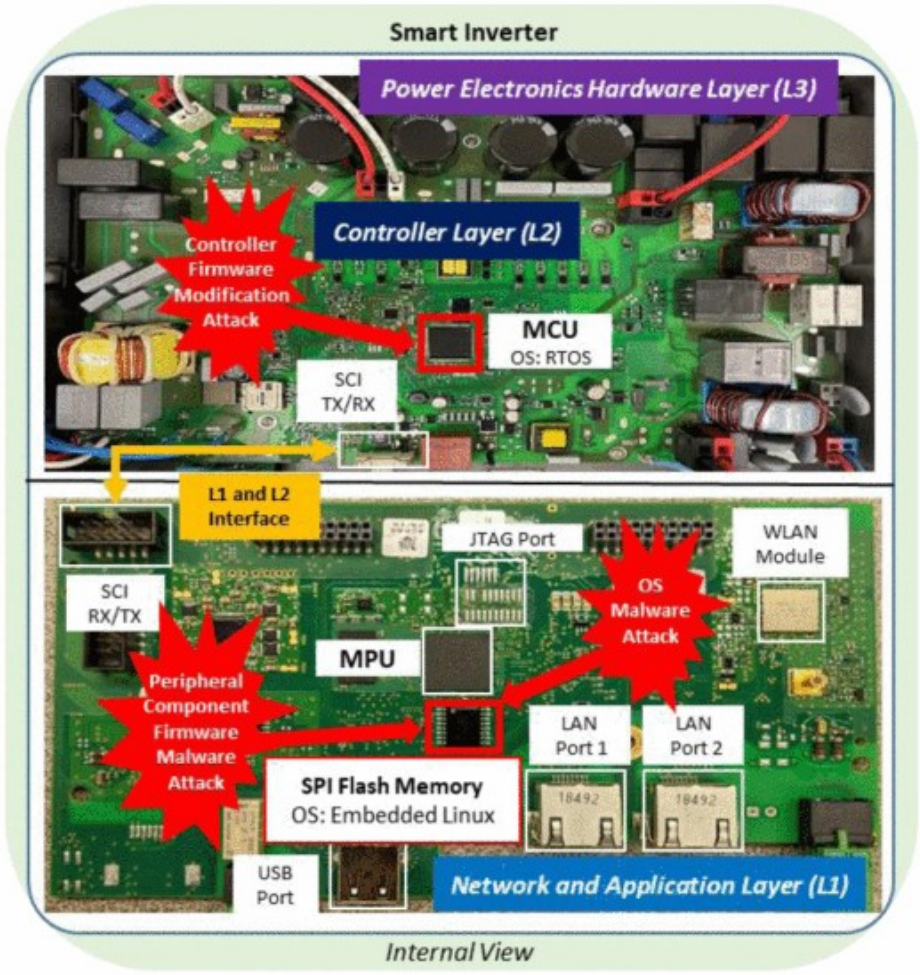
3.1 Υλικό αντιστροφέων ως στόχος επιθέσεων

Στο επίπεδο ευφυών δικτύων και μικροδικτύων, είναι απαραίτητη η χρήση ενσωματωμένων συστημάτων για την κατασκευή των ευφυών αντιστροφέων με τις επιθυμητές σε εμάς δυνατότητες, ειδικά αφού αυτοί οι αντιστροφείς θα συμμετέχουν σε ένα δίκτυο, όπου καλούνται να μπορούν να επικοινωνήσουν με άλλες κατανεμήμενες μονάδες, εξωτερικούς ελεγκτές κτλ. Το υλικό (**hardware**) αυτών των συστημάτων, παρά την λανθασμένη εντύπωση που επικρατούσε για καιρό ότι είναι ασφαλές, οπότε δε χρειάζεται να ακολουθούνται συγκεκριμένοι κανόνες και πρωτόκολλα για την προστασία του, δημιουργεί μια μεγάλη ομάδα από σημεία σε ένα δίκτυο τα οποία αποτελούν εν δυνάμει τρωτά σε επιθέσεις σημεία, όπως τα περιεχόμενα μνημών flash σε απομακρυσμένες τερματικές μονάδες [40]. Συνολικά σε ένα ευφυές δίκτυο που περιλαμβάνει συσκευές όπως, προγραμματιζόμενους λογικούς ελεγκτές, μονάδες μέτρησης φασιθετών, τερματικές μονάδες, συστήματα που επιβλέπουν τον έλεγχο και την απόκτηση πληροφοριών (SCADA) μεταξύ άλλων, εμφανίζονται πολλά σημεία στο υλικό των προαναφερθείσων συσκευών, τα οποία μπορούν να γίνουν στόχος, είτε επεμβατικών, είτε όχι επιθέσεων. Μια αιτία αυτού του προβλήματος είναι, πως συχνά χρησιμοποιούνται προϊόντα, τα οποία έχουν φτιαχτεί για εμπορική χρήση με κάποιες τροποποιήσεις, αντί για προϊόντα τα οποία φτιάχτηκαν ειδικά για το σκοπό που καλούνται να επιτελέσουν στο δίκτυο, κάτι που σημαίνει ότι μπορεί να εισάγουν τρωτά σημεία, που σχετίζονται με την κατασκευή τους, στο ευρύτερο ευφυές δίκτυο (**Commercial off-the-shelf**). Ο τύπος των επιθέσεων με στόχο το υλικό των παραπάνω συσκευών στα ενσωματωμένα συστήματα καθορίζεται και από το πόσο καταρτισμένος είναι, τι σκοπό και τι πόρους έχει ο επιτιθέμενος και ακόμα περισσότερο, από το τι είδους πρόσβαση μπορεί να έχει στη συσκευή που είναι ο στόχος της επίθεσης [41].

Ένα μικροδίκτυο, στο οποίο εστιάζει περισσότερο η εργασία αυτή, συγκριτικά με ένα ευρύ ευφυές δίκτυο, σίγουρα έχει λιγότερα συστήματα τα οποία μπορούν να γίνουν στόχοι επιθέσεων υλικού, αλλά ακόμα και στο φυσικό στρώμα μιας κατανεμημένης μονάδας και στον πρωτογενή της έλεγχο, συναντάμε αδυναμίες δεδομένου και του ότι έχουμε χρήση ευφυών αντιστροφέων οι οποίοι απαρτίζονται από ενσωματωμένα συστήματα. Ένας τέτοιος αντιστροφέας αποτελείται κυρίως από τα εξής τρία στρώματα [42]:

1. Το στρώμα δικτύου και εφαρμογής που περιλαμβάνει έναν μικροεπεξεργαστή με αρκετή υπολογιστική ισχύ για να επιτελέσει τις απαραίτητες λειτουργίες χρησιμοποιώντας και κάποια flash μνήμη. Επίσης, περιλαμβάνει τις απαραίτητες θύρες και περιφερειακά εξαρτήματα (JTAG, LAN, WLAN) για να μπορεί να επικοινωνήσει με άλλα κομμάτια του μικροδικτύου.

2. Το στρώμα ελέγχου, το οποίο έχει μια μονάδα μικροελέγχου, που με μικρότερη υπολογιστική ισχύ, συμβάλλει στην επεξεργασία σημάτων και στον έλεγχο του αντιστροφέα.
3. Το στρώμα υλικού των ηλεκτρονικών ισχύος, το οποίο περιλαμβάνει τα απαραίτητα εξαρτήματα ηλεκτρονικών ισχύος και τους απαραίτητους αισθητήρες.



Σχήμα 3.1: *Υλικό ευφυούς αντιστροφέα* [42]

3.1.1 Επιθέσεις στο Firmware

Μια συνήθης κατηγορία επιθέσεων στο υλικό ενός αντιστροφέα, στοχεύει το λογισμικό το οποίο είναι υπεύθυνο για τον έλεγχο του χαμηλότερου επιπέδου λειτουργίας του. Ο επιτιθέμενος πρέπει να μπορεί να εισάγει στη flash μνήμη του στρώματος εφαρμογής τη δική του πλαστή έκδοση του λογισμικού μέσω της οποίας μνήμης θα εκτελεστεί με σκοπό να επηρεάσει τα υπόλοιπα στρώματα και τη συνολική λειτουργία του αντιστροφέα [43]. Η εισαγωγή αυτού του κακόβουλου λογισμικού μπορεί να γίνει είτε επεμβατικά είτε όχι στην περίπτωση που ο επιτιθέμενος μπορεί να εκμεταλλευτεί απομακρυσμένα τη λειτουργία της αυτόματης ενημέρωσης του εν λόγω λογισμικού. Ακόμα, μπορούμε να έχουμε αντικατάσταση του λογισμικού, όταν οι κατασκευαστές των αντιστροφέων δημοσιοποιούν τα αρχεία του λογισμικού και όταν ο επιτιθέμενος μπορεί να τα ανακτήσει μόνος του από την εν λόγω συσκευή.

Στο [44] μελετώνται επιθέσεις αυτής της κατηγορίας σε έναν ηλιακό μικροαντιστροφέα, οι οποίες καταλήγουν να προσομοιάζουν δύο γνωστά σενάρια επιθέσεων, τις επιθέσεις DoS και τις επιθέσεις στην είσοδο του αλγορίθμου MPPT (maximum power point tracking), που οδηγούν στη μη βέλτιστη λειτουργία του συστήματος φωτοβολταϊκών. Τέλος, μέσω του λογισμικού μπορούν να επιτευχθούν και επιθέσεις εισαγωγής ψευδών δεδομένων, αλλάζοντας και το κέρδος απόκτησης των εσωτερικών αισθητήρων, επηρεάζοντας έτσι τις τιμές των μετρήσεων που συλλέγονται, αλλά και παραμέτρους σχετικές με τον έλεγχο, όπως τιμές αναφοράς διαφόρων μεταβλητών σχετικές με βοηθητικές λειτουργίες υποστήριξης του δικτύου. Τέτοιες λειτουργίες είναι η λειτουργία υποστήριξης της τάσης, η λειτουργία υποστήριξης της συχνότητας και λειτουργίες που αποτρέπουν την αποσύνδεση του αντιστροφέα από το δίκτυο, σε περιπτώσεις διαταραχής των τιμών της τάσης και της συχνότητας (fault ride-through). [9]

3.1.2 Επιθέσεις στους βρόγχους ελέγχου πριν τον πρωτογενή έλεγχο

Αν και οι βρόγχοι ελέγχου, που προηγούνται του πρωτογενούς, αποτελούν το πιο προστατευμένο τμήμα του ιεραρχικού ελέγχου κατανεμημένων μονάδων βασισμένων σε αντιστροφείς σε ένα σύστημα, δε σημαίνει ότι δε συναντούμε περιπτώσεις επιθέσεων που αξίζουν αναφορά. Αντιθέτως, επειδή στοχεύουν τμήματα που βρίσκονται σε καίρια τμήματα του συστήματος ελέγχου, είναι πολύ σημαντικές και αξίζουν προσοχή.

Στο [45] μελετάται ένα σύστημα LCC-HVDC και κάποιες περιπτώσεις FDI επιθέσεων σε

αυτό. Αρχικά, έχουμε επιθέσεις που στοχεύουν τον αντιστροφέα, είτε με μεταβολή της DC τάσης, είτε με μεταβολή της γωνίας κατάσβεσης. Με αύξηση της πραγματικής τάσης, έχουμε πτώση της γωνίας κατάσβεσης και με ικανή μείωσή της οδηγείται το σύστημα σε σφάλμα μεταγωγής, που αν επαναληφθεί αρκετά μπορεί να οδηγήσει σε διακοπή λειτουργίας. Με μείωση της πραγματικής τάσης, έχουμε αύξηση της γωνίας κατάσβεσης και αύξηση της ζήτησης άεργου ισχύος. Ακόμα, μελετώνται επιθέσεις εναντίον του ανορθωτή, που με αύξηση του DC ρεύματος, έχουμε μείωση της μεταφερόμενης ισχύος και πιθανά προβλήματα συχνότητας στην AC μεριά, ενώ με μείωση του ρεύματος έχουμε αύξηση της ισχύος, υπερβολική κατανάλωση άεργου ισχύος και τελικά πρόκληση αστάθειας στο σύστημα. Τέλος, μελετώνται συνδυασμοί των παραπάνω επιθέσεων που όπως είναι φυσικό οδηγούν σε μεγαλύτερα προβλήματα το σύστημα και πιθανά σε καταστροφή εξοπλισμού ή ολική διακοπή λειτουργίας του HVDC.

Στο [46] μελετάται μια υποκατηγορία FDI επιθέσεων, που ονομάζονται επιθέσεις εισαγωγής bias, απέναντι σε μετατροπείς ανεμογεννητριών στη μεριά σύνδεσης με το δίκτυο. Στο πλαίσιο που αφορά το κομμάτι του υλικού του αντιστροφέα πριν τον πρωτογενή έχουμε αρχικά, στοχοποίηση των παραμέτρων αναφοράς ρεύματος και τάσης, που προκαλούν αποκλίσεις από τις επιθυμητές τιμές της τάσης, επηρεάζουν τον έλεγχο της άεργου ισχύος και αυξάνουν τα ρεύματα στον μετατροπέα. Ακόμα, οι επιθέσεις στις μετρήσεις των αισθητήρων θεωρούνται επιθέσεις προς τους βρόγχους ρεύματος και τάσης, καθώς μεταβάλλουν άμεσα τις εισόδους τους, οδηγώντας σε μεταβολές ισχύος και προβλήματα στην απόσβεση που οδηγούν σε ταλαντώσεις τάσης και ρεύματος.

Στο [47] μελετάται μια υποκατηγορία FDI επιθέσεων που αναφέρονται ως επιθέσεις αντικατάστασης δεδομένων, επιθέσεις αλλαγής της τοπολογίας και επιθέσεις επαναποστολής, καθώς και συνδυασμού της πρώτης με την τρίτη κατηγορία επιθέσεων, απέναντι στους ελεγκτές αντιστροφέων σε ένα μικροδίκτυο. Η πρώτη κατηγορία στοχεύει τις παραμέτρους των ελεγκτών, υποβαθμίζοντας τη ρύθμιση συχνότητας και τάσης οδηγώντας πιθανώς το σύστημα σε αστάθεια. Η δεύτερη κατηγορία έχει ως στόχο την παρεμπόδιση ενός μικρού σήματος, που οι εξισώσεις του συστήματος που μελετάται χρησιμοποιούν για την ανίχνευση επιθέσεων. Ο μηδενισμός αυτού του σήματος δημιουργεί, εκτός από προβλήματα στον έλεγχο, περιπτώσεις που έχουμε μη δικαιολογημένη αποσύνδεση κάποιου κόμβου του μικροδικτύου. Η τρίτη κατηγορία πέρα από τη δυνατότητα της να κάνει την ανίχνευση άλλων επιθέσεων αδύνατη, μπορεί και μόνη της να υποβαθμίσει τη λειτουργία του συστήματος και να δημιουργήσει προβλήματα ευστάθειας, καθώς είναι υπεύθυνη για την επαναποστολή παλαιότερων μετρήσεων οι οποίες δεν είναι πια σωστές. Η περίπτωση συνδυασμού της πρώτης με την τρίτη κατηγορία επιθέσεων δημιουργεί τα προβλήματα της πρώτης δυσκολεύοντας ακόμα περισσότερο την ανίχνευσή της λόγω της τρίτης κατηγορίας.

3.1.3 Επιθέσεις στους αισθητήρες του αντιστροφέα

Οι αισθητήρες αποτελούν ένα ιδιαίτερα σημαντικό κομμάτι ενός οποιουδήποτε δικτύου ανεξαρτήτως βελησνεκούς, καθώς είναι υπεύθυνοι για τη συγκέντρωση μετρήσεων διαφόρων μεγεθών και τη μεταβίβαση τους στα αρμόδια συστήματα για την επεξεργασία και τη χρήση τους. Εξαιτίας της σπουδαιότητας τους και του γεγονότος ότι τα ελεγκτικά συστήματα, στα οποία μεταβιβάζονται οι μετρήσεις των αισθητήρων, εμπιστεύονται εγγενώς τα σήματα που προέρχονται από αυτούς, συναντάμε διάφορες περιπτώσεις επιθέσεων οι οποίες έχουν ως στόχο τους αισθητήρες είτε αλλοιώνοντας τις μετρήσεις τους είτε προσπαθώντας να τους απομονώσουν και να διακόψουν την επικοινωνίας τους με το υπόλοιπο δίκτυο [48].

Στο [48] μελετάται μια μη επεμβατική επίθεση υλικού, όπου το εργαλείο που εκτελεί την επίθεση μπορεί να παραμείνει κρυφό μέσα σε κάποιο δοχείο, σε μια συγκεκριμένη κατηγορία αισθητήρων με ευρεία χρήση στα ευφυή δίκτυα και όχι μόνο, τους Hall αισθητήρες και συγκεκριμένα σε ένα σύστημα ηλιακού αντιστροφέα συνδεδεμένου σε κάποιο δίκτυο. Χρησιμοποιείται εξοπλισμός χαμηλού κόστους για τη δημιουργία μαγνητικού πεδίου σε κοντινή απόσταση από τους αισθητήρες ώστε να μπορέσει να παραβιάσει την προστασία τους, με σκόπο την αλλοίωση των μετρήσεων της μεριάς συνεχούς/εναλλασσόμενου ρεύματος και τάσης του συστήματος του αντιστροφέα. Συγκεκριμένα, μια επίθεση διατηρώντας ένα σταθερό μαγνητικό πεδίο προσθέτει μια σταθερά στην τάση εξόδου του αντιστροφέα, ενώ κάποιο ημιτονοειδές μαγνητικό πεδίο προσθέτει ανεπιθύμητες αρμονικές στην τάση εξόδου και παρά τη διαφορετικές επιπτώσεις, έχουμε και στις δύο περιπτώσεις αποσύνδεση του αντιστροφέα από το δίκτυο γεγονός που μας δείχνει ότι αντιμετωπίζουμε περιπτώσεις DoS επιθέσεων.

Στο [49] βλέπουμε μια περίπτωση μη επεμβατικής επίθεσης σε αντιστροφέα φωτοβολταϊκών, στοχοποιώντας τους αισθητήρες που χρησιμοποιούνται στο σύστημα για τη συλλογή και μεταφορά μετρήσεων. Μέσω ελέγχου της συχνότητας ηλεκτρομαγνητικών παρεμβολών προς τους αισθητήρες, ο επιτιθέμενος μπορεί να καταφέρει να παρεισφρήσει στον έλεγχο του αντιστροφέα, αλλάζοντας τις τιμές των τάσεων αναφοράς κάτι που οδηγεί στη δυνατότητα ελέγχου της DC τάσης διαύλου. Αυτή η μελέτη δεν αφορά αποκλειστικά μόνο αισθητήρες Hall, αλλά αναφέρεται γενικά σε παρεμβολές εναντίον αισθητήρων σε φωτοβολταϊκά συστήματα.

3.2 Επιθέσεις στον πρωτογενή έλεγχο

Ο πρωτογενής έλεγχος σε ένα μικροδίκτυο ή γενικά σε ένα σύστημα βασισμένο σε αντιστροφείς υλοποιείται σε κάθε κατανεμημένη μονάδα παραγωγής με κέντρο έναν αντιστροφέα και περιλαμβάνει στη βασική του μορφή, είτε το συμβατικό droop είτε κάποια βελτίωση του, όπως αναφέραμε και προηγουμένως. Επιπλέον, έχουμε σε κάποιες περιπτώσεις προσθήκη ενός PLL και προσθήκη εικονικής αντίστασης χωρίς απώλειες και του ελέγχου αυτής, με στόχο τη βελτίωση της αποσύζευξης της ενεργού και της άεργου ισχύος [50].

Γνωρίζουμε ότι στην ιεραρχία του συνολικού συστήματος ελέγχου ενός μικροδικτύου, που περιλαμβάνει κατανεμημένες μονάδες παραγωγής, η καθεμία εκ των οποίων έχει στο κέντρο της λειτουργίας της κάποιον αντιστροφέα, ο πρωτογενής έλεγχος χαρακτηρίζεται από ταχύτερες αποκρίσεις συγκριτικά με το δευτερογενή και τον τριτογενή και γίνεται τοπικά στην κατανεμημένη μονάδα. Αναφερόμαστε λοιπόν σε διαδικασίες οι οποίες επιτυγχάνονται αποκεντρωμένα, χωρίς τη χρήση διαύλων επικοινωνίας, κάτι που κάνει τις επιθέσεις στο συγκεκριμένο κομμάτι λιγότερο συχνές, αλλά σε καμία περίπτωση αδύνατες.

3.2.1 Επιθέσεις στον droop έλεγχο

Στο [51] για παράδειγμα, έχουμε τη μελέτη συστημάτων που απαρτίζονται από grid-forming αντιστροφείς, τα οποία χρησιμοποιούν droop ελεγκτές στο πρωτογενές κομμάτι του συστήματος ελέγχου και αναλύονται δυναμικές επιθέσεις εισαγωγής ψευδών δεδομένων, οι οποίες έχουν ως στόχο την αλλαγή των τιμών των κερδών ή αλλιώς των συντελεστών κάποιου droop ελεγκτή με σκοπό τη μετατόπιση των ιδιοτιμών του συστήματος καταλήγοντας σε αλλαγή της περιοχής ευστάθειας κάποιου άλλου αντιστροφέα του ίδιου απομονωμένου μικροδικτύου. Τελικά, προτείνεται ένας αλγόριθμος για την αναγνώριση του τύπου της επίθεσης και την επιλογή του κατάλληλου τρόπου άμυνας.

Στο [52] έχουμε τη μελέτη δυναμικών, κρυφίων επιθέσεων εισαγωγής ψευδών δεδομένων εναντίον των πρωτογενών droop ελεγκτών σε ένα σύστημα αποτελούμενο από επιμέρους μικροδίκτυα απομονωμένα από το ευρύτερο δίκτυο, βασισμένα στη λειτουργία και grid-following και grid-forming αντιστροφέων και αποδεικνύεται ότι μέσω μιας οργανωμένης σειράς επιθέσεων σε αισθητήρες, μπορούμε να αλλοιώσουμε τις μετρήσεις τους και να παρακάμψουμε το σύστημα

ανίχνευσης λάθος δεδομένων (BDD) οδηγώντας το σύστημα σε πιθανή αστάθεια. Μελετώνται επιθέσεις που στοχεύουν ένα σημείο (single point attacks), αλλά και επιθέσεις που έχουν ταυτόχρονα ως στόχους πολλαπλά σημεία του δικτύου (multiple point attacks) και επισημαίνονται οι διαφορές στην προσέγγιση που ακολουθείται για την ανάλυση και αντιμετώπισή τους. Οι ακριβείς επιπτώσεις μελετώνται ως πρόβλημα βελτιστοποίησης και η λύση του δίνει το πάνω όριο στο σήμα επίθεσης εναντίον των αισθητήρων, όριο το οποίο αν ξεπεραστεί από τον επιτιθέμενο, έχουμε αποσταθεροποίηση των μικροδικτύων.

3.2.2 Επιθέσεις στο PLL

Μια επιπλέον κατηγορία επιθέσεων είναι αυτή που έχει ως στόχο το PLL του και επομένως στοχεύει να αλλάξει απευθείας την τιμή της ισχύος στην είσοδο του αντιστροφέα. Συναντάμε ένα PLL σε συστήματα βασισμένα σε αντιστροφείς, οι οποίοι είναι είτε αμιγώς grid-following, είτε έχουν κάποια υβριδική μορφή, που συνδυάζει λειτουργίες grid-following και grid-forming. Ο λόγος ύπαρξής του είναι να βοηθάει στο συγχρονισμό του αντιστροφέα με το υπόλοιπο δίκτυο, καθορίζοντας τη φάση του, είτε αυτό είναι άλλα αποκεντρωμένα συστήματα αντιστροφέων σε ένα μικροδίκτυο, είτε ένα σταθερό, ευρύ ηλεκτρικό δίκτυο.

Στο [53] μελετώνται περιπτώσεις δυναμικών και κρυφίων επιθέσεων εισαγωγής ψευδών δεδομένων με στόχο κάποιο PLL ενός κατανεμημένου ενεργειακού πόρου, με κέντρο λειτουργίας έναν grid-following αντιστροφέα. Με τη δημιουργία ψευδών θετικών παλμών τάσης, το χρονικό σημείο που η εναλλασσόμενη τάση γίνεται στιγμιαία ίση με το μηδέν στο σημείο κοινής σύζευξης, ο επιτιθέμενος οδηγεί το PLL στην παρουσίαση αλλοιωμένης γωνίας φάσης στην έξοδο του, οδηγώντας το σύστημα σε αστάθεια. Μέσα στις ανεπιθύμητες συνέπειες συμπεριλαμβάνονται καταστάσεις όπως, η υπέρταση, η αύξηση του ρυθμού αλλαγής συχνότητας και η αντιστροφή της ροής ισχύος.

Στο [54] έχουμε άλλη μια περίπτωση μελέτης δυναμικών, κρυφίων επιθέσεων, που έχουν ως στόχο το PLL κάποιου grid-following αντιστροφέα, οι οποίες μεταβάλλουν τις παραμέτρους ελέγχου του, κάτι που γίνεται δυνατό ειδικά, επειδή ο δράστης γνωρίζει πως ένα δίκτυο δε λειτουργεί σχεδόν ποτέ στην ονομαστική του συχνότητα. Τα σημεία, από όπου συνήθως ξεκινάει μια τέτοια επίθεση αναφέρεται ότι είναι πρώτον, κάποιο περιβάλλον χρήστη, που με τη χρήση κλεμμένων διαπιστευτηρίων του χειριστή του δικτύου, αποκτάει πρόσβαση μέσω SCADA σε κάποιον αντιστροφέα και δεύτερον, κάποιο κενό ασφαλείας του αντιστροφέα από την κατασκευή

του, το οποίο μπορεί να δημιουργήθηκε είτε ηθελημένα, είτε εξαιτίας κάποιου λάθους. Αναφέρονται, επίσης, οι άμεσες επιπτώσεις που έχουν αυτές οι επιθέσεις, οι οποίες μπορεί να είναι, η παραβίαση των ορίων ισχύος, η οποία είναι ικανή να οδηγήσει το ευρύτερο σύστημα σε αστάθεια, απώλειες εσόδων του χειριστή δικτύου, εξαιτίας της μειωμένης εξόδου ισχύος ενεργειακών πόρων βασισμένων στη χρήση ενός αντιστροφέα και αλλοίωση των επιπέδων της τάσης και των προφίλ τάσης που εν δυνάμει οδηγεί παραβίαση κανονισμών ως προς τις επιτρεπτές τιμές τάσης και ενεργού ισχύος.

Στο [55] μελετάται η περίπτωση επιθέσεων εισαγωγής ψευδών δεδομένων με στόχο τα SRF-PLL DFIG ανεμογεννητριών συνδεδεμένων στο δίκτυο. Έχουμε αλλοίωση των σημάτων που δέχεται το PLL από τον πίνακα ελέγχου της ανεμογεννήτριας, γεγονός που οδηγεί στην αλλοίωση της γωνίας φάσης εξόδου του PLL. Ακόμα και μια πολύ μικρή αλλοίωση των μετρήσεων που δέχεται σαν είσοδο το PLL, μπορεί να οδηγήσει σε προβλήματα σχετικά με την ποσότητα ενεργού ισχύος που εγχύει η ανεμογεννήτρια στο δίκτυο, καταλήγοντας σε αποσύνδεσή της και διαταραχή της ευστάθειας του ευρύτερου δικτύου.

Στο [56] έχουμε τη μελέτη κρυφίων επιθέσεων εισαγωγής ψευδών δεδομένων απέναντι σε μικροδίκτυα κατανεμημένων ενεργειακών πόρων συνδεδεμένα στο ευρύτερο δίκτυο. Έχουμε χρήση grid-following αντιστροφέων στα εν λόγω μικροδίκτυα, ενώ συγκεκριμένος στόχος των επιθέσεων είναι τα DSOGI (dual second-order generalized integrator) PLL με σκοπό τη διατάραξη της ευστάθειας του δικτύου. Με αλλοίωση των τιμών των παραμέτρων του PLL, παρατηρείται λανθασμένη γωνίας φάσης ως έξοδος του PLL γεγονός που διαταράσσει την τροφοδότηση ισχύος προς το δίκτυο οδηγώντας σε πιθανή αστάθεια.

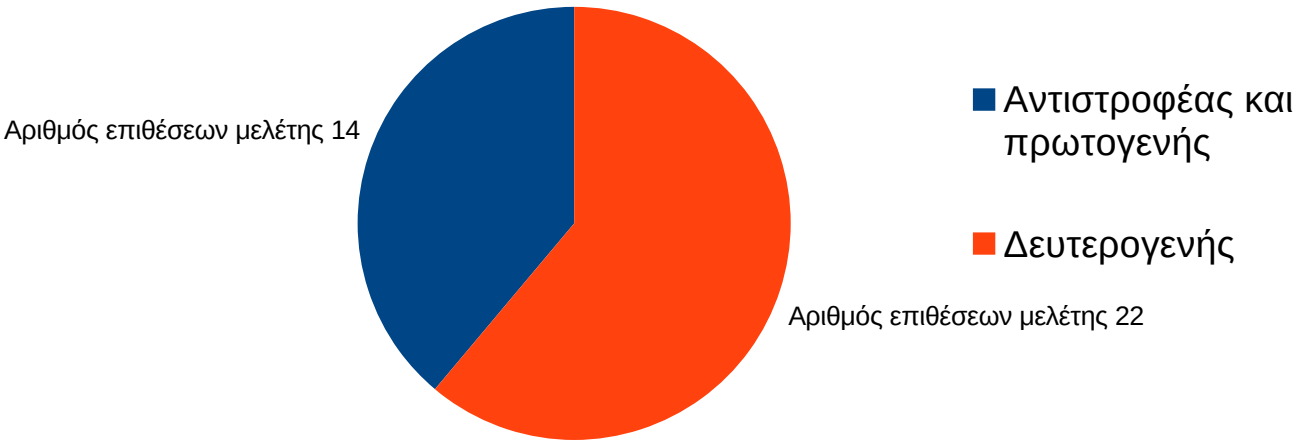
Στο [57] έχουμε GPS spoofing επιθέσεις με στόχο τη διαταραχή της σωστής λειτουργίας των DLL (delay lock loop) και PLL. Ο επιτιθέμενος δημιουργεί κάποιο αλλοιωμένο σήμα με μεγαλύτερη ένταση από το πραγματικό, με αποτέλεσμα τα DLL και PLL να ακολουθήσουν και να επεξεργαστούν το σήμα της επίθεσης ως πραγματικό.

Στο [58] μελετάται η περίπτωση διαταραχής της ευστάθειας της λειτουργίας ενός MMC (modular multi-level converter) που συνδέεται σε κάποιο μικροδίκτυο (weak grid connection). Αλλοίωση των τιμών των παραμέτρων που δέχεται το DSOGI PLL του MMC από το μικροδίκτυο, προκαλεί αλλαγή των τιμών των ρευμάτων αναφοράς που χρησιμοποιούνται στον βρόγχο ελέγχου του ρεύματος στον πρωτογενή έλεγχο. Προτείνονται κάποια βήματα βελτίωσης του εν λόγω PLL, με σκοπό την ομαλή λειτουργία του MMC κατά την παραμόρφωση της τάσης.

Οι επιθέσεις με στόχο ένα PLL απαιτούν ο επιτιθέμενος να είναι τεχνικά καταρτισμένος, να έχει γνώση του πως είναι δομημένο το δίκτυο στο οποίο ανήκει το PLL και αρκετές φορές να έχει

στη διάθεση του εξειδικευμένο εξοπλισμό μεγάλου κόστους για να φέρει σε πέρας την επίθεση, γεγονός που κάνει αυτή την κατηγορία επιθέσεων λιγότερο διαδεδομένη, αλλά ιδιαίτερα καταστροφική.

Στον Πίνακα 3.1 που ακολουθεί, παρουσιάζεται μια συνοπτική περιγραφή των περιπτώσεων επιθέσεων που περιγράφτηκαν προηγουμένως, ενώ στο Σχ. 3.2 βλέπουμε μια ποσοτική εμφάνιση των περιπτώσεων επιθέσεων που αναφέρθηκαν και αυτών που θα αναφερθούν στη συνέχεια για τον δευτερογενή έλεγχο.



Σχήμα 3.2: *Αριθμός επιθέσεων στα διαφορετικά τμήματα του ιεραρχικού ελέγχου*

Ref	*Είδος Inverter*	*Τύπος επίθεσης*	*Πρωτεύων στόχος επίθεσης*	*Αποτέλεσμα επίθεσης*	*Χαρακτηριστικά Επίθεσης*	*Islanded/Grid-tied Σύστημα*
[51]	Grid-Forming	FDI	Droop ελεγκτές	Μετατόπιση των ιδιοτιμών του συστήματος, αλλάζοντας τα κέρδη τάσης και συχνότητας n_i,m_i του ελεγκτή droop του i αντιστροφέα με αποτέλεσμα τη μετατόπιση της περιοχής ευστάθειας π.χ του i+1 αντιστροφέα	Δυναμική	Islanded μικροδίκτυο
[44]	Grid-following/Grid-forming	FDI, DoS	Firmware ηλιακού μικροαντιστροφέα	1)Απενεργοποίηση της λειτουργίας MPPT του ελεγκτή μέσω μιας DoS επίθεσης (επιτυγχάνεται με firmware modification) γεγονός που οδηγεί στη μείωση παραγωγής ισχύος. Αν συμβεί σε πολλαπλούς αντιστροφείς οδηγούμαστε σε επιδείνωση της οικονομικής λειτουργία του δικτύου. 2) Με DoS επιθέσεις φέρνουμε τον μικροαντιστροφέα εκτός λειτουργίας σε διαφορετικά χρονικά σημεία, γεγονός που δημιουργεί διακυμάνσεις στη συχνότητα του μικροδικτύου. Η αστάθεια του δικτύου μπόρει να οδηγήσει σε συνέπειες όπως η καταστροφή εξοπλισμού και η απώλεια ρεύματος. 3) Με αλλοίωση των τιμών των μετρήσεων τάσης και ρεύματος σε πραγματικό χρόνο οδηγούμε τον MPPT ελεγκτή σε αστάθεια επηρεάζοντας και την έξοδο του μικροαντιστροφέα και την ισχύ που πρέπει να παραχθεί για τις ανάγκες του μικροδικτύου. Πέρα από τις οικονομικές συνέπειες, μπορούμε να έχουμε ακόμα και διακοπές λειτουργίας του δικτύου.	Δυναμική, κρυφία	Islanded μικροδίκτυο
[52]	Grid-following/Grid-forming	FDI, DoS	Droop ελεγκτές	Εύρεση του ελάχιστου κέρδους του ελεγκτή ώστε να υπολογισθεί το σήμα επίθεσης που θα φέρει αστάθεια στο δίκτυο (single point attack -> χρήση Root-Locus – multiple point attack -> χρήση αλλοιωμένων μετρήσεων αισθητήρων και διαθέσιμων σημάτων ανατραφοδότησης του δικτύου)	Δυναμική, Κρυφία	Ομάδα μικροδικτύων απομονωμένων από το κεντρικό δίκτυο
[55]	Grid-Following	FDI	SRF-PLL	Αλλοίωση των τιμών που δέχεται το SRF-PLL από τον πίνακα ελέγχου της ανεμογεννήτριας, προσπερνώντας το τείχος προστασίας του	Δυναμική	Grid-tied ανεμογεννήτρια
[53]	Grid-Following	FDI	PLL	Κάνοντας την αποδοχή πως ο επιτιθέμενος μπορεί να πετύχει φυσικώς την έγχυση ψευδών παλμών τάσης σε σημείο κοντά στον αντιστροφέα, το PLL μπορεί να αναφέρει λάθος τιμή γωνίας φάσης στον κατανεμημένο ενεργειακό πόρο.	Δυναμική, Κρυφία	Grid-tied
[54]	Grid-Following	FDI	PLL	Αλλοίωση των τιμών των παραμέτρων ελέγχου (π.χ κάνοντας χρήση κλεμμένων διαπιστευτηρίων χειριστών του δικτύου) με αποτέλεσμα οικονομικές επιπτώσεις και την παραβίαση των ορίων της τάσης και της ευστάθειας του κυκλώματος ισχύος του αντιστροφέα αλλά και του ευρύτερου δικτύου	Δυναμική, Κρυφία	Weak/strong grid connection
[48]	Grid-Following ηλιακοί αντιστροφείς	Spoofing->DoS	Αισθητήρες HALL	Το μαγνητικό πεδίο της επίθεσης οδηγεί στην αλλαγή του σημείου λειτουργίας του PI ελεγκτή του αντιστροφέα -> σφάλμα στη λειτουργία των PLL και SVPWM -> παραμόρφωση της τάσης και της συχνότητας εξόδου -> παύση λειτουργίας του αντιστροφέα	Μη επεμβατική, Δυναμική, Κρυφία	Grid-tied
[45]	HVDC ανορθωτές and grid-forming/grid-following αντιστροφείς	FDI	Βρόγχοι ελέγχου ανορθωτή και αντιστροφέα	**Rectifier:** Σε κατάσταση ελέγχου συνεχούς DC ρεύματος αν η επίθεση αυξήσει το συνολικό DC ρεύμα, θα έχουμε μείωση της πραγματικής τιμής του ρεύματος -> αύξηση της DC τάσης και μείωση της κατανάλωσης άεργου ισχύος από το HVDC σύστημα-> βλάβη του θυρίστορ και προβλήματα στη συχνότητα στην AC μεριά του inverter. Αντίστροφα αποτελέσματα αν έχουμε μείωση του συνολικού ρεύματος. **Inverter:** Σε κατάσταση ελέγχου της συνεχούς DC τάσης, αύξηση της συνολικής τάσης -> μείωση της πραγματικής τιμής της DC τάσης -> αύξηση της γωνίας κατάσβεσης -> βλάβη θυρίστορ. Αν έχουμε μείωση της συνολικής τάσης με την επίθεση, οδηγούμαστε τελικά σε μείωση της γωνίας	Δυναμική, Κρυφία	LCC-HVDC

				κατάσβεσης η οποία οδηγεί σε προβλήματα επικοινωνίας στο σύστημα με τελικό αποτέλεσμα την αστάθεια στο σύστημα		
[49]	PV grid-following αντιστροφέας	EMI spoofing(FDI)	Αισθητήρες PV αντιστροφέα	Αν με την ηλεκτρομαγνητική παρεμβολή προκαλέσουμε πτώση της τάσης -> ανάλογη αύξηση της τάσης αναφοράς -> ταχύτερη φθορά του DC πυκνωτή ή ακόμα και ολική καταστροφή του αντιστροφέα. Αύξηση της τάσης στους αισθητήρες -> μείωση της τάσης αναφοράς -> παύση λειτουργίας αντιστροφέα αν υπάρχει σύστημα προστασίας κατά της υπέρτασης αλλιώς θα έχουμε έγχυση μεγάλων τιμών άεργου ισχύος στο δίκτυο αυξάνοντας το ρεύμα εξόδου καταστρέφοντας τον αντιστροφέα.	Δυναμική	Grid-tied μικροδίκτυο
[56]	Grid-following	FDI	DSOGI PLL	Αλλοίωση των παραμέτρων k_p,k_i του DSOGI PLL οδηγεί σε αλλοίωση της γωνίας φάσης και τελικά σε δημιουργία προβλημάτων στην έγχυση ισχύος στο δίκτυο που είναι συνδεδεμένο στον κατανεμημένο ενεργειακό πόρο	Κρυφία	Grid-tied
[57]	Grid-following	GPS Spoofing	DLL, PLL	Το σήμα του επιτιθέμενου είναι πιο δυνατό από το πραγματικό, γεγονός που οδηγεί τα DLL και PLL να επεξεργαστούν και να ακολουθήσουν αντίστοιχα, το αλλοιωμένο σήμα.	Κρυφία	Grid-tied
[58]	Grid-following	FDI	Βρόγχος ελέγχου ισχύος και PLL	Αλλοίωση του σήματος τάσης από το ασθενές δίκτυο στο οποίο είναι συνδεδεμένο το MMC σύστημα, δημιουργεί αλλοίωση των τιμών αναφοράς ρεύματος i_d,i_q που δέχεται ο βρόγχος ελέγχου ρεύματος	Δυναμική, Κρυφία	Weak grid connection
[46]	Grid-following/Grid-forming	FDI	Ελεγκτής αντιστροφέα	Αύξηση του ρεύματος αναφοράς στον έλεγχο του ρεύματος οδηγεί σε μείωση της τάσης γεγονός που οδηγεί το σύστημα τελικά να μειώσει εσφαλμένα την τιμή του ρεύματος αναφοράς. Παρόμοια αποτελέσματα συναντούμε στην περίπτωση αλλοίωσης των συνιστωσών d,q του ρεύματος που λαμβάνουν οι αισθητήρες. Τέλος, εκτελείται και μια επίθεση στα κέρδη διάφορων ελεγκτών τα οποία προκαλούν ταλαντώσεις στο σύστημα.	Δυναμική, Κρυφία	Islanded
[47]	Grid-following/Grid-forming	Τροποποίηση τοπολογίας, FDI(επίθεση αντικατάστασης δεδομένων), Επίθεση επαναποστολής δεδομένων μαζί με επίθεση αντικατάστασης δεδομένων	Εσωτερικός ελεγκτής μπαταρίας, Ελεγκτές εξωτερικών βρόγχων μπαταρίας και κυψέλης καυσίμου	Οι αλλαγές στις τάσεις εξόδου οδηγούν το μικροδίκτυο κατανεμημένων πόρων στην αποκοπή της μπαταρίας που δέχεται την επίθεση για την επαναφορά της ευστάθειας στο μικροδίκτυο. Η αστάθεια ισχύος επηρεάζει τους υπόλοιπους κατανεμημένους ενεργειακούς πόρους Η αύξηση και η μείωση των τιμών των μετρήσεων του μικροδικτύου οδηγεί σε επιδείνωση της λειτουργίας του και συγκεκριμένα σε αλλοίωση των τάσεων εξόδου. Με τις 2 ταυτόχρονες επιθέσεις (replay και επίθεση αντικατάστασης δεδομένων), έχουμε κατάρρευση του φωτοβολταϊκού που είναι ο στόχος, ενώ πρέπει να αντιμετωπιστεί η επίθεση replay για να ανιχνευθεί οποιαδήποτε άλλη.	Δυναμική, Κρυφία	Islanded σύμπλεγμα μικροδικτύων

Πίνακας 3.1: *Περίληψη των επιθέσεων στους αντιστροφείς και στον πρωτογενή έλεγχο*

3.3 Επιθέσεις στο δευτερογενή έλεγχο

Ο δευτερογενής έλεγχος σε ένα σύστημα βασισμένο στη λειτουργία αντιστροφέων, μπορεί να χωριστεί σε τρεις μεγάλες διαφορετικές κατηγορίες, με βάση τον τύπο του δικτύου επικοινωνίας, που χρησιμοποιείται για την ανταλλαγή δεδομένων μεταξύ των επιμέρους μονάδων παραγωγής και των κομματιών του δικτύου, που είναι υπεύθυνα για τη διεξαγωγή του δευτερογενούς ελέγχου. Είναι υπεύθυνος, κυρίως, για τη διόρθωση των αποκλίσεων στις τιμές της συχνότητας και της τάσης της κάθε τοπικής μονάδας, μετά το πέρας του πρωτογενούς ελέγχου. Η ύπαρξη του δικτύου επικοινωνίας και όλων των επιμέρους μονάδων, που χρησιμοποιούνται για την ανταλλαγή δεδομένων (αισθητήρες, ενεργοποιητές, ελεγκτές, δίαυλοι επικοινωνίας), δημιουργούν εύφορο έδαφος για τη διενέργεια επιθέσεων. Οι επιθέσεις αυτές παρουσιάζουν διαφορετικά χαρακτηριστικά και επιπτώσεις στο δίκτυο, ανάλογα με το σε ποια από τις τρεις κατηγορίες κατατάσσεται ο δευτερογενής έλεγχος, όπως θα δούμε και παρακάτω.

Η πρώτη κατηγορία είναι ο κεντρικός δευτερογενής έλεγχος όπου έχουμε έναν κεντρικό ελεγκτή, ο οποίος επικοινωνεί ταυτόχρονα με κάθε κατανεμημένη μονάδα παραγωγής και αφότου προβεί στους απαραίτητους υπολογισμούς, δεδομένων των μετρήσεων που έλαβε από την κάθε μονάδα μέσω κάποιου αισθητήρα, αποστέλλει την κατάλληλη εντολή ελέγχου στους ενεργοποιητές. Χρησιμοποιείται κυρίως για τη διαχείριση της ενεργού και της άεργου ισχύος [59], για την αποκατάσταση των τιμών της συχνότητας και της τάσης [60][61], για την εξάλειψη αρμονικών συνιστωσών [62][63] και για την επίλυση διαχειριστικών ζητημάτων με σκοπό την βελτίωση της επίδοσης του συστήματος[64][65].

Η δεύτερη κατηγορία είναι ο αποκεντρωμένος δευτερογενής έλεγχος, κατά τον οποίο έχουμε αποκατάσταση των μεγεθών της συχνότητας και της τάσης δίχως τη χρήση υποδομών επικοινωνίας για την ανταλλαγή μετρήσεων μεταξύ των κατανεμημένων μονάδων. Η αποκατάσταση επιτυγχάνεται ξεχωριστά τοπικά στην κάθε μονάδα. Αξίζει να αναφερθεί ότι, ακόμα και όταν σχεδιαστικά χρησιμοποιείται αυτός ο τύπος δευτερογενούς ελέγχου, σε υψηλότερο επίπεδο, όπως είναι αυτό του τριτογενούς ελέγχου και του κεντρικού ελεγκτή του μικροδικτύου, έχουμε χρήση δικτύου επικοινωνίας στο δίκτυό μας, καθώς χωρίς αυτό, λειτουργίες όπως η επαναφορά μέρους του δικτύου χωρίς κάποια εξωτερική πηγή ισχύος (black start) και ο έλεγχος τμημάτων του σε πραγματικό χρόνο δε θα ήταν δυνατές [66]. Τρεις κύριες κατηγορίες αποκεντρωμένου δευτερογενή ελέγχου είναι οι εξής:

1. Με τη χρήση ενός ζωνοπερατού φίλτρου χωρίς στατικό κέρδος (washout filter) και τη χρήση του θεωρήματος τελικής τιμής αποδεικνύεται ότι η συχνότητα και η τάση μπορούν να συγκλίνουν στις τιμές αναφοράς τους σε ένα ευσταθές μικροδίκτυο. Η υλοποίηση επιτυγχάνεται στο επίπεδο του droop ελέγχου [67][68].
2. Ακόμη, κάνοντας χρήση μεθόδων εκτίμησης μεταβλητών κατάστασης σε μικροδίκτυα έχουν σχεδιαστεί διάφορες τεχνικές αμιγούς αποκεντρωμένου δευτερογενή ελέγχου παρόλο που αυτές οι μέθοδοι εξαρτώνται πλήρως από τα χαρακτηριστικά μοντελοποίησης του κάθε συστήματος [69][70][71].
3. Τέλος, έχουμε περιπτώσεις οι οποίες με τη χρήση αποκλειστικά τιμών τοπικών μεταβλητών κάθε κατανεμημένης μονάδας επιτυγχάνουν την αποκατάσταση της συχνότητας και της τάσης χωρίς τη χρήση υποδομών επικοινωνίας [72][73].

Η τρίτη, τελική και συχνά πιο σημαντική κατηγορία για περιπτώσεις δευτερογενούς ελέγχου μικροδικτύων είναι αυτή του κατανεμημένου ελέγχου, καθώς έχουμε να κάνουμε με δίκτυα, τα οποία αποτελούνται από πολλαπλές, ξεχωριστές και συχνά ανομοιογενείς μονάδες. Η συγκεκριμένη κατηγορία συνδυάζει θετικά των δύο προηγούμενων, ενώ ταυτόχρονα αποφεύγει σημαντικά αρνητικά, όπως είναι διάφορα προβλήματα στη λειτουργία του δικτύου τα οποία οφείλονται στην αποτυχία ενός κεντρικού σημείου ελέγχου (single point of failure). Συναντάμε ένα δίκτυο επικοινωνίας, το οποίο είναι απαραίτητο για την επικοινωνία των κατανεμημένων μονάδων, που απαρτίζουν το μικροδίκτυο, χωρίς να σημαίνει ότι έχουμε ροή πληροφορίας από όλες τις μονάδες προς όλες τις μονάδες. Αυτό σημαίνει πως η τοπολογία διαφέρει από περίπτωση σε περίπτωση και παίζει σημαντικό ρόλο στη διεξαγωγή του ελέγχου. Οι κύριες ομάδες τεχνικών κατανεμημένου δευτερογενή ελέγχου είναι οι εξής:

1. Αρχικά, έχουμε μια ομάδα τεχνικών που βασίζεται στον υπολογισμό κάθε φορά του μέσου όρου των τιμών κάποιας παραμέτρου ενδιαφέροντος, που συλλέγονται από τις διάφορες κατανεμημένες μονάδες μέσω της επικοινωνίας τους. Το τελικό σήμα ελέγχου δημιουργείται μετά από τη σύγκριση του εν λόγω μέσου όρου με την ονομαστική τιμή της παραμέτρου και τη χρήση κάποιου ειδικά σχεδιασμένου ελεγκτή, με βάση την περίπτωση που μελετάται κάθε φορά [74][75].
2. Επιπλέον, μια άλλη ομάδα τακτικών κατανεμημένου δευτερογενή ελέγχου είναι αυτή που χρησιμοποιεί αλγόριθμους που επιδιώκουν τη συναίνεση μεταξύ των

διαφόρων κατανεμημένων μονάδων παραγωγής, μετά την ανταλλαγή πληροφοριών μεταξύ αυτών που επικοινωνούν. Σε αυτή την ομάδα, συναντάμε και περιπτώσεις που επιλέγεται να μην έχουν όλες οι κατανεμημένες μονάδες την ίδια σημασία στη διεξαγωγή του δευτερογενή ελέγχου. Σε αυτές τις περιπτώσεις μία κατανεμημένη μονάδα ορίζεται ως "ηγέτης", ενώ οι υπόλοιπες ως "ακόλουθοι" και αυτές ακολουθούν την αντικειμενική πορεία που καθορίζει η μονάδα-ηγέτης για το δίκτυο, χωρίς να έχουν οποιασδήποτε μορφής έλεγχο πάνω στην κατάστασή της. Σε δίκτυα που απαρτίζονται από πολλές κατανεμημένες μονάδες και επομένως παρουσιάζουν, σε αρκετές περιπτώσεις, πολύ δυναμική συμπεριφορά, χρειαζόμαστε παραπάνω από μια μονάδα ως ηγέτες. Αυτό περιπλέκει το πρόβλημα του ελέγχου δημιουργώντας ερωτήσεις όπως, ποιοι κόμβοι είναι οι βέλτιστες επιλογές για ηγέτες, ποιος είναι ο βέλτιστος αριθμός ακόλουθων για κάθε ηγέτη και άλλες. Σκοπός μας είναι να φέρουμε τις καταστάσεις, που βρίσκονται όλοι οι ακόλουθοι, εντός ενός συνόλου καταστάσεων που οριοθετείται από τους ηγέτες [76][77][78].

3. Τέλος, σε ορισμένες περιπτώσεις, η διαδικασία της ανταλλαγής πληροφορίας ανάμεσα στις κατανεμημένες μονάδες παραγωγής του μικροδικτύου δε συμβαίνει συνεχόμενα, γεγονός που περιορίζει την ποσότητα πληροφορίας που χρειάζεται να μεταφερθεί μέσω του δικτύου επικοινωνίας κάτι που είναι συχνά επιθυμητό. Συνήθως, η εκκίνηση της διαδικασίας της ανταλλαγής πληροφορίας ορίζεται, είτε από κάποιο ρολόι δηλαδή έχουμε εξάρτηση από το χρόνο, είτε από κάποιο γεγονός που την πυροδοτεί μέσω της αποστολής ενός σήματος, είτε από την κάθε κατανεμημένη μονάδα ξεχωριστά, μέσω της χρήσης της προηγούμενής της κατάστασης στον υπολογισμό του κανόνα ελέγχου που επιτρέπει την ανταλλαγή πληροφορίας [79][80][81]

3.3.1 FDI επιθέσεις στον δευτερογενή έλεγχο

Στο [82] μελετάται η περίπτωση διεξαγωγής FDI επιθέσεων εναντίον ενός μικροδικτύου, που λειτουργεί απομονωμένα από ένα χρονικό σημείο και μετά. Παρατηρούνται οι συνέπειες σε δύο διαφορετικές περιπτώσεις βλέποντας πως, στην περίπτωση που το σήμα της επίθεσης προς μια κατανεμημένη μονάδα ελέγχου έχει μικρό πλάτος, έχουμε σύγκλιση της συχνότητας και της τάσης σε διαφορετικές τιμές από τις επιθυμητές στους κατανεμημένους κόμβους του μικροδικτύου ενώ όταν αυξάνουμε το πλάτος στη δεύτερη περίπτωση, το σύστημα οδηγείται σε αστάθεια. Με τις

επιθέσεις αυτές διαταράσσονται οι λειτουργίες του καταμερισμού φορτίου και οι συνολικές απαιτήσεις ισχύος στο μικροδίκτυο.

Στο [83] έχουμε ένα απομονωμένο μικροδίκτυο τεσσάρων κατανεμημένων ενεργειακών πόρων, το οποίο δέχεται κάποιες επιθέσεις FDI σε διάφορες χρονικές στιγμές. Όταν στόχος των επιθέσεων είναι οι αισθητήρες, το σήμα επίθεσης στη συχνότητα είναι ημιτονοειδές, ενώ όταν στοχοποιούνται οι ενεργοποιητές, το σήμα επίθεσης είναι, είτε σταθερό, είτε εξαρτάται από το χρόνο. Όταν ο δευτερογενής έλεγχος είναι κάποιος συμβατικός έλεγχος συναίνεσης, παρατηρούνται διακυμάνσεις στις τιμές των συχνοτήτων των κατανεμημένων κόμβων οι οποίες προκαλούν αποσταθεροποίηση της λειτουργίας του συστήματος. Η λειτουργία που βάλλεται στη συγκεκριμένη περίπτωση, είναι αυτή του συγχρονισμού συχνότητας του δικτύου.

Στο [84] μελετάται ένα μικροδίκτυο που χρησιμοποιεί ένα είδος δευτερογενούς κατανεμημένου ελέγχου που ονομάζεται pinning συναίνεση, κατά τον οποίο μόνο ένα υποσύνολο κόμβων έχουν πρόσβαση στις τιμές αναφοράς της συχνότητας, ενώ οι υπόλοιποι κόμβοι τους ακολουθούν, λαμβάνοντας σήματα απ' αυτούς για να επιτευχθεί η λειτουργία της ρύθμισης της συχνότητας. Κατά τη διεξαγωγή FDI φραγμένων επιθέσεων στη συχνότητα σε έναν αριθμό απλών κόμβων ή στη συχνότητα αναφοράς στους pinned κόμβους, παρατηρούνται προβλήματα στην αποκατάσταση της συχνότητας (Frequency restoration) και στο διαμοιρασμό ισχύος (Power sharing) στο δίκτυο και στην περίπτωση που το άνω και κάτω φράγμα ξεπεράσει μια τιμή, το σύστημα καταρρέει μετά από σημαντικές ταλαντώσεις.

Στο [85] έχουμε ένα μικροδίκτυο αποτελούμενο από τέσσερα συστήματα αποθήκευσης ενέργειας (ESS) και ο δευτερογενής έλεγχος είναι κατανεμημένος έλεγχος συνεργασίας για συστήματα πολλαπλών κατανεμημένων μονάδων. Οι επιθέσεις FDI προκαλούν αποκλίσεις από την ονομαστική συχνότητα και ταλαντώσεις στην ενεργό ισχύ. Συγκεκριμένα, επηρεάζονται οι λειτουργίες του συστήματος που είναι υπεύθυνες για την ισορροπία της κατάστασης φόρτισης (State of charge), για το σωστό διαμοιρασμό της ισχύος και για την αποκατάσταση της συχνότητας

Στο [86] μελετάται η λειτουργία ενός μικροδικτύου αποτελούμενου από 4 κατανεμημένες γεννήτριες σε περιπτώσεις επιθέσεων εισαγωγής ψευδών δεδομένων κατά των αισθητήρων του και των συνδέσμων επικοινωνίας μεταξύ των επιμέρους κόμβων. Βλέπουμε την αδυναμία ενός συμβατικού αλγόριθμου συναίνεσης δευτερογενούς ελέγχου να διατηρήσει την ευστάθεια του συστήματος, ως προς τη συχνότητά του και ταυτόχρονα, δίνεται λύση στο πρόβλημα με την δημιουργία ενός εξελιγμένου observer-based αλγορίθμου στη θέση του συμβατικού.

Στο [87] μελετάται ένα απομονωμένο DC σύμπλεγμα μικροδικτύων με κατανεμημένο δευτερογενή έλεγχο συναίνεσης και η συμπεριφορά του κατά τη διάρκεια επιθέσεων FDI που

εισάγουν κάποιο ψευδές σήμα στο δευτερογενή ελεγκτή. Αυτό το σήμα δημιουργεί αποκλίσεις από τις επιθυμητές τιμές παραμέτρων, όπως η τάση εξόδου, που μεταφέρονται στους ενεργοποιητές από τη μονάδα ελέγχου, αποκλίσεις οι οποίες μπορούν να οδηγήσουν το σύστημα και σε αστάθεια. Έχουμε υποβάθμιση της λειτουργίας του δευτερογενή ελέγχου, με επιπτώσεις που βλέπουμε να μεταφέρονται στο επίπεδο των grid-forming και grid-following μετατροπέων.

Στο [88] βλέπουμε την περίπτωση ταυτόχρονων επιθέσεων FDI και DoS και την αύξηση στην απόκλιση της συχνότητας του συστήματος συγκριτικά με τη περίπτωση που έχουμε μονο DoS και ειδικά με την περίπτωση που έχουμε μόνο FDI. Έχουμε παρουσία FDI επιθέσεων με σκοπό την αλλοίωση του σήματος ελέγχου κατά μια ποσότητα στους actuators και παρουσία DoS στους συνδέσμους επικοινωνίας μεταξύ των κόμβων με σκοπό την παρεμπόδιση ανταλλαγής μετρήσεων. Προτείνεται ένας observer-based LFC (load frequency controller).

Στο [89] έχουμε άλλη μια περίπτωση που επικεντρώνεται στη δυσκολία της αντιμετώπισης συνδυαστικών επιθέσεων FDI και DoS. Με την αλλοίωση των μετρήσεων τάσης και συχνότητας στους αισθητήρες της κάθε κατανεμημένης γεννήτριας και της παρεμπόδισης της επικοινωνίας τους μέσω των διαύλων επικοινωνίας, το σύστημα οδηγείται σε αστάθεια. Για την αντιμετώπιση ενός τέτοιου συνδυασμού επιθέσεων, προτείνεται μια βελτιωμένη μορφή δευτερογενούς κατανεμημένου observer-based ελεκτή.

Στο [90] μελετάται η εισαγωγή ψευδών δεδομένων σε μικροδίκτυα μεταβλητού αριθμού επιμέρους κόμβων μέσω των actuators/sensors τους. Με την επιλογή αυθαίρετων σημάτων, που πληρούν κάποια κριτήρια, του επιτιθέμενου για αποστολή σε γειτονικούς κόμβους, προκαλείται αστάθεια στο σύστημα. Προτείνεται μια βελτιωμένη μορφή ενός consensus-based αλγόριθμου δευτερογενούς ελέγχου για την αντιμετώπιση των επιθέσεων αυτών που βασίζεται στο ότι κάθε φορά δε θα αντιμετωπίσει περισσότερους από 1 ή 2 (τίθεται από το σύστημα ως σταθερά) κακόβουλους γείτονες του κάθε υγιή κόμβου όταν οι χρονικές καθυστερήσεις του συστήματος είναι πεπερασμένες.

Στο [91] έχουμε ένα μικροδίκτυο που αποτελείται από επιμέρους κατανεμημένους πόρους βασισμένους στη λειτουργία αντιστροφέων. Παρατηρούνται οι αρνητικές συνέπειες στο συγχρονισμό των συχνοτήτων των επιμέρους κόμβων και στο διαμοιρασμό ενεργού ισχύος που έχουν γραμμικές και μη γραμμικές FDI επιθέσεις σε ενεργοποιητές, διαύλους επικοινωνίας, αισθητήρες και σε ελεγκτές. Παρουσιάζεται μια βελτιωμένη μορφή, βασισμένου στη συναίνεση, δευτερογενούς ελέγχου για την αντιμετώπιση των επιθέσεων αυτών.

Στο [92] μελετώνται οι επιπτώσεις που έχουν οι επιθέσεις εισαγωγής ψευδών δεδομένων σε κάποιον κατανεμημένο ενεργειακό πόρο (DER) σε δύο διαφορετικά συστήματα: σε ένα IEEE 34-

bus feeder που περιλαμβάνει έξι τέτοιους πόρους και σε ένα μικροδίκτυο με είκοσι. Και στα δύο συστήματα, όταν έχουμε αλλαγή της πραγματικής συχνότητας σε έναν κόμβο παρατηρούνται ταλαντώσεις, κατά την προσπάθεια αποκατάστασής της και απώλεια της επιθυμητής συναίνεσης, που επιδιώκει ο δευτερογενής έλεγχος. Οι ταλαντώσεις αυτές φτάνουν και στους κόμβους με τους οποίους επικοινωνεί ο κόμβος στον οποίο γίνεται η επίθεση. Παρεμφερείς επιπτώσεις συναντώνται και στην περίπτωση αλλοίωσης της τιμής της πραγματικής τάσης σε έναν κατανεμημένο ενεργειακό πόρο, όπου έχουμε ταλαντώσεις της τάσης και της άεργου ισχύος. Για την αντιμετώπιση των ανεπιθύμητων ταλαντώσεων στις παραπάνω περιπτώσεις, προτείνεται μια βελτίωση του συμβατικού αλγόριθμου συναίνεσης, με εισαγωγή εννοιών, όπως είναι το self-belief του κάθε κόμβου, το οποίο επηρεάζει τα επίπεδα εμπιστοσύνης γειτονικών κόμβων.

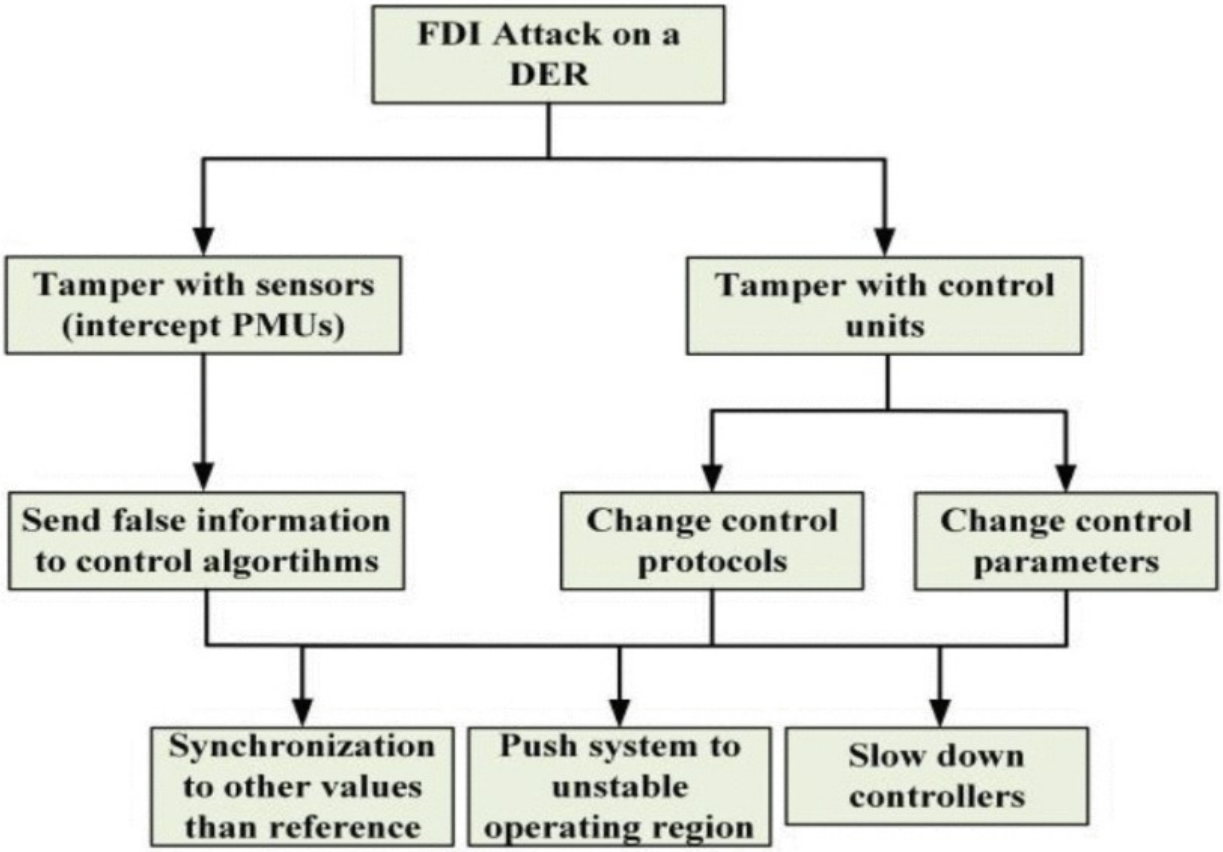
Στο [93] μελετώνται επιθέσεις εισαγωγής ψευδών δεδομένων σε ένα μικροδίκτυο που αποτελείται από πέντε κατανεμημένες μονάδες παραγωγής κατηγοριοποιώντας τις με βάση, το αν στοχεύουν στην επικοινωνούμενη μέτρηση μεταξύ δύο κόμβων μέσω του συνδέσμου επικοινωνίας τους, ή στην τιμή της πραγματικής παραμέτρου σε έναν από τους πέντε κόμβους. Στην πρώτη περίπτωση, η αλλοίωση της συχνότητας προκαλεί αλλαγές κυρίως στις τιμές της συχνότητας, της τάσης και της ενεργού ισχύος των κόμβων, ενώ η άεργος μένει σχεδόν ανεπηρέαστη. Η τάση δε, σχεδόν αποκλειστικά τις τιμές των τάσεων των κόμβων. Στην περίπτωση αλλοίωσης της συχνότητας μέσα στον ίδιο τον κόμβο, παρατηρούνται αλλαγές στις τιμές όλων των τεσσάρων παραμέτρων που προαναφέρθηκαν στους κόμβους του συστήματος, ενώ όσον αφορά την αλλαγή της τάσης, παρατηρούνται ταλαντώσεις κυρίως στις τάσεις των κόμβων. Στο σύστημα που μελετάται, χρησιμοποιείται ένα βελτιωμένος observer-based αλγόριθμος δευτερογενούς ελέγχου που στοχεύει στην παρουσίαση θετικών αποτελεσμάτων σε πεπερασμένο χρόνο.

Στο [94] έχουμε ένα μικροδίκτυο αποτελούμενο από 4 κατανεμημένες γεννήτριες των οποίων η λειτουργία είναι βασισμένη σε αντιστροφείς και μελετάται η ανταπόκριση του σε τρεις κατηγορίες επιθέσεων. Στην πρώτη κατηγορία, έχουμε αλλαγή της μέτρησης της τάσης αισθητήρα μιας κατανεμημένης μονάδας παραγωγής, γεγονός που δημιουργεί ταλαντώσεις στην τάση του και αλλαγές στην ενεργό και στην αέργο ισχύ παρά το μικρό χρονικό παράθυρο κατά το οποίο διεξάγεται η επίθεση κάτι που πιθανό να οδηγεί στην απομόνωση της εν λόγω μονάδας. Στη δεύτερη περίπτωση, με μια επίθεση που ανήκει σε ένα μοντέλο προσθετικών επιθέσεων (sparse additive attack) επηρεάζεται η είσοδος του ελεγκτή μιας κατανεμημένης μονάδας παραγωγής με τη χρήση ενός ημιτονοειδούς σήματος μικρού πλάτους γεγονός που δημιουργεί διακυμάνσεις σε όλες τις σχετικές παραμέτρους (συχνότητα, τάση, ενεργο και άεργο ισχύ). Μεγαλύτερες διαταραχές μπορούν να φέρουν το σύστημα σε αστάθεια.. Στην τρίτη και τελευταία περίπτωση, μελετώνται επιθέσεις αλλαγής των φορτίων οι οποίες προκαλούν ταλαντώσεις στη συχνότητα και αποκλίσεις

στην ενεργό και άεργο ισχύ, παρά το γεγονός ότι το σύστημα, λόγω της έλλειψης αδράνειας, έχει τη δυνατότητα να προσαρμοστεί άμεσα στις νέες ανάγκες ισχύος.

Στο [95] μελετάται ένα μικροδίκτυο αποτελούμενο από 4 αντιστροφείς, εκ των οποίων οι 2 είναι leaders, υπεύθυνοι για τις μέγιστες και ελάχιστες τιμές αναφοράς της συχνότητας και της τάσης και οι 2 είναι followers, οι οποίοι συμβάλλουν ο καθένας ανάλογα με το ρόλο του στο συνεργατικό κατανεμημένο δευτερογενή έλεγχο. Οι μη φραγμένες επιθέσεις εισάγουν ψευδή σήματα εξαρτώμενα από το χρόνο είτε 1) επηρεάζοντας τις τιμές αναφοράς που αποστέλλονται από τους leaders στους followers, είτε 2) παριστάνοντας πως είναι κάποιος γειτονικός αντιστροφέας στέλνοντας ψευδείς τιμές, είτε 3) αλλοιώνοντας τις τιμές των παραμέτρων που ανταλλάσονται μεταξύ γειτονικών αντιστροφέων, είτε 4) αλλοιώνοντας τις ίδιες τις μετρήσεις ενός αντιστροφέα. Οι διαταραχές που προκαλούνται στο μικροδίκτυο με τους παραπάνω τρόπους, καταστέλλουν κομβικές λειτουργίες του όπως η αποκατάσταση της συχνότητας και αποσταθεροποιούν το δίκτυο αν δεν αντιμετωπιστούν.

Στο Σχ. 3.2 παρουσιάζεται ένα συνοπτικό διάγραμμα ροής των FDI επιθέσεων σε συστήματα βασισμένα σε αντιστροφείς. Θεωρούμε ότι οι επιθέσεις σε διαύλους επικοινωνίας που έχουμε αναφέρει, παρόλο που δεν εμφανίζονται ρητά στο διάγραμμα αυτό, είναι μέρος του, καθώς αναφέρονται στις περιπτώσεις, που γίνεται εκμετάλλευσή τους για την αποστολή ψευδών δεδομένων.



Σχήμα 3.3: *Διάγραμμα ροής FDI επιθέσεων* [92]

3.3.2 DoS επιθέσεις στον δευτερογενή έλεγχο

Στο [96] παρουσιάζεται δύο περιπτώσεις επιθέσεων DoS με διαφορετικούς κύκλους λειτουργίας εναντίον ενός μικροδικτύου που αποτελείται από πολλαπλούς κατανεμημένους κόμβους συνδεδεμένους στο ευρύτερο ηλεκτρικό δίκτυο. Η διακοπή της επικοινωνίας κατά τη διάρκεια των επιθέσεων διαταράσσει τη λειτουργία του κατανεμημένου δευτερογενή ελέγχου που βασίζεται στην ανταλλαγή πληροφορίας και παρατηρούνται ανεπιθύμητες αρμονικές, διακυμάνσεις τιμών όπως ο συντελεστής ενεργούς ισχύος και αύξηση της συνολικής παραμόρφωσης ονομαστικού ρεύματος στο σημείο κοινής σύζευξης (PCC). Επισημαίνεται ως κύρια αιτία των παραπάνω, η απόκλιση της υπολειπόμενης χωρητικότητας RC (Residual Capacity) και του συντελεστή ενεργούς ισχύος φ από τις επιθυμητές τιμές.

Το [97] εστιάζει σε επιθέσεις DoS που διεξάγονται κατά ενός απομονωμένου μικροδικτύου το οποίο αποτελείται από πέντε κατανεμημένους ενεργειακούς πόρους. Οι επιθέσεις διαταράσσουν

την επικοινωνία μεταξύ των κόμβων αλλάζοντας την τοπολογία του δικτύου και επομένως τον πίνακα Laplace, προκαλώντας επιπτώσεις που αυξάνονται αναλογικά με τη διάρκεια και τη συχνότητα των επιθέσεων και κυμαίνονται από αποκλίσεις παραμέτρων όπως η συχνότητα από τις επιθυμητές τιμές έως και πρόκληση αστάθειας στο σύστημα. Συγκεκριμένα επηρεάζονται ο διαμοιρασμός ενεργού ισχύος και η λειτουργία της αποκατάστασης συχνότητας.

Στο [98] παρουσιάζονται περιπτώσεις που ένα μικροδίκτυο διαφορετικών αριθμών κατανεμημένων κόμβων, σε κάθε περίπτωση, δέχεται DoS επιθέσεις που διαταράσσουν την επικοινωνία. Κατά παρόμοιο τρόπο με την προηγούμενη περίπτωση, καταργώντας διαύλους επικοινωνίας μεταξύ κόμβων γεγονός που τροποποιεί τον πίνακα Laplace, παρουσιάζονται επιπτώσεις όπως απόκλιση από τις επιθυμητές τιμές της συχνότητας, της τάσης, της ενεργού και της άεργου ισχύος καθώς και σε πιο ακραίες περιπτώσεις, πρόκληση αστάθειας στο μικροδίκτυο. Έχουμε λοιπόν επιδείνωση της οικονομικής λειτουργίας του δικτύου καθώς και λειτουργιών όπως η αποκατάσταση συχνότητας και τάσης και ο διαμοιρασμός ισχύος.

Στο [84] πέρα από τις επιθέσεις FDI που αναφέρθηκαν στην προηγούμενη υποενότητα, έχουμε και την μελέτη επιθέσεων DoS προς το μικροδίκτυο των πέντε κατανεμημένων ενεργειακών πόρων. Όπως και στην προηγούμενη περίπτωση, έχουμε αλλοίωση της τοπολογίας του δικτύου με επιπτώσεις στον διαμοιρασμό ισχύος και στη δυνατότητα του δευτερογενούς ελέγχου για αποκατάσταση της συχνότητας και της τάσης. Επιπλέον, περιγράφεται ο συνδυασμός FDI και DoS επιθέσεων απέναντι στο απομονωμένο μικροδίκτυο, που όπως είναι αναμενόμενο αυξάνει την κλίμακα των προαναφερθεισών επιπτώσεων και αυξάνει τις πιθανότητες πρόκλησης αστάθειας στο σύστημα.

Στο [99] έχουμε τη μελέτη ενός απομονωμένου μικροδικτύου κατανεμημένων γεννητριών, που μέσω μιας σειράς DoS επιθέσεων στο δίκτυο επικοινωνίας του, καταλήγει να παρουσιάζει βίαιες ταλαντώσεις στις τιμές της τάσης και της συχνότητας των επιμέρους κόμβων λόγω της δυσκολίας ανταλλαγής μετρήσεων μεταξύ αυτών των κόμβων. Αυτές οι επιθέσεις DoS μπορεί να είναι από απλές περιοδικές και τυχαίες επιθέσεις jamming μέχρι και επιθέσεις εκμετάλλευσης συγκεκριμένων χαρακτηριστικών πρωτοκόλλων επικοινωνίας όπως το TCP. Παρουσιάζεται μια βελτίωση διακριτού χρόνου στον event-triggered αλγόριθμο δευτερογενούς ελέγχου για την αντιμετώπιση των DoS επιθέσεων που μειώνει ταυτόχρονα και τον απαιτούμενο όγκο δεδομένων που μεταφέρονται μεταξύ των κόμβων.

Στο [100] μελετάται ένα απομονωμένο δίκτυο που αποτελείται από AC και DC μικροδίκτυα που χρησιμοποιούν κατανεμημένο δευτερογενή έλεγχο κατά τη διαδικασία επικοινωνίας τους. Όταν η επικοινωνία ενός AC και ενός DC μικροδικτύου διακόπτεται εξαιτίας μιας DoS επίθεσης στον σύνδεσμο επικοινωνίας τους, παρατηρούνται ανεπιθύμητες διακυμάνσεις συχνότητας στη μεριά

των AC και τάσης στη μεριά των DC μικροδικτύων και η ακρίβεια της κατανομής ισχύος στα επιμέρους μικροδίκτυα υποβαθμίζεται αισθητά, ειδικά κατά τη χρονική στιγμή αλλαγής της ισχύος φορτίου. Για την εξασφάλιση της ευστάθειας του δικτύου ακόμα και κατά τη διάρκεια των παραπάνω φαινομένων, προτείνεται μια βελτίωση του event-triggered κατανεμημένου δευτερογενή ελέγχου με την εισαγωγή ενός προγνωστικού μοντέλου για τις στιγμές που η επικοινωνίας μεταξύ επιμέρους κόμβων έχει διακοπεί.

Στο [101] βλέπουμε ένα απομονωμένο μικροδίκτυο που αποτελείται από κατανεμημένες γεννήτριες των οποίων η λειτουργία είναι βασισμένη ως συνήθως, σε αντιστροφείς. Διεξάγοντας μια σειρά από DoS επιθέσεις ίσης διάρκειας σε διαφορετικά χρονικά σημεία και μια σειρά από επιθέσεις που ξεκινούν την ίδια χρονική στιγμή με διαφορετική διάρκεια, παρατηρούμε ταλαντώσεις των τιμών της συχνότητας, της τάσης και της ενεργού ισχύος των επιμέρους κόμβων που σε ορισμένες περιπτώσεις οδηγούν όλο το μικροδίκτυο σε αστάθεια. Μάλιστα, παρατηρείται ότι η διάρκεια των επιθέσεων είναι ο παράγοντας που επηρεάζει περισσότερο τις επιπτώσεις στο δίκτυο. Παρουσιάζεται μια βελτιωμένη εκδοχή του κεντρικού δευτερογενή ελεγκτή όπου το κέρδος του ελεγκτή δεν είναι παγιωμένο.

Στο [102] μελετάται ένα μικροδίκτυο αποτελούμενο από 4 επιμέρους μικροδίκτυα ή χωρίς βλάβη της γενικότητας, 4 επιμέρους κατανεμημένες γεννήτριες. Μέσω μιας σειράς τριών επιθέσεων DoS μεταξύ των επιμέρους τμημάτων 1-2, 3-4 και 2-3 στους συνδέσμους επικοινωνίας τους, αλλοιώνεται η ανταλλαγή μετρήσεων τους για κάποια συγκεκριμένα χρονικά διαστήματα. Αυτό το γεγονός, προκαλεί διακύμανση των τιμών της ενεργού και της αέργου ισχύος και στους κόμβους που πλήττονται σε κάθε χρονική στιγμή, αλλά και στους υπόλοιπους κόμβους με τους οποίους επικοινωνούν στο μικροδίκτυο κάτι που δημιουργεί πρόβλημα στον ομαλό διαμοιρασμό ισχύος που προσπαθεί να πετύχει ο δευτερογενής έλεγχος. Για την αποκατάσταση της ομαλής λειτουργίας ενός τέτοιου μικροδικτύου, υλοποιείται και προτείνεται στο δευτερογενές τμήμα ελέγχου, ένας αποκεντρωμένος ελεγκτής που χρησιμοποιεί κατανεμημένους παρατηρητές και εκτιμητές.

Στο [103] παρουσιάζεται ένα σύμπλεγμα 4 συνδεδεμένων μεταξύ τους μικροδικτύων που το καθένα έχει έναν αριθμό φορτίων και κατανεμημένων γεννητριών και έναν κεντρικό ελεγκτή. Στο δευτερογενές κομμάτι του ελέγχου, του εν λόγω δικτύου, χρησιμοποιείται ένας, βασισμένος στη συναίνεση, αλγόριθμος, η λειτουργία του οποίου βασίζεται στην ανταλλαγή μετρήσεων μεταξύ των επιμέρους μικροδικτύων. Στην περίπτωση αυτή, μελετάται μια σειρά από DoS επιθέσεις πολλών επιπέδων οι οποίες συγκεκριμένα, στοχοποιούν το επίπεδο των καναλιών επικοινωνίας μεταξύ των επιμέρους μικροδικτύων και σε κάθε επιμέρους μικροδίκτυο, τα επίπεδα της μεταφοράς μετρήσεων από τους αισθητήρες και των εισόδων ελέγχου στους ενεργοποιητές. Αυτές οι πολυεπίπεδες επιθέσεις, δημιουργούν ανεπιθύμητες ταλαντώσεις στις τιμές της συχνότητας και της ισχύος των

μικροδικτύων, γεγονός που δημιουργεί προβλήματα στη διεξαγωγή του συγχρονισμού συχνότητας και διαμοιρασμού ενεργού ισχύος στο δίκτυο. Συγκεκριμένα, μπορεί να παρατηρηθούν ενεργοποίηση προστατευτικών μηχανισμών του δικτύου, απόρριψη φορτίων και γενικευμένες διακοπες ρεύματος. Για την αντιμετώπιση αυτών των σύνθετων επιθέσεων, υλοποιείται ένα self-triggered σύστημα, βασισμένο στη συναίνεση, για τον κατανεμημένο δευτερογενή έλεγχο του δικτύου, ενώ τονίζεται η σπουδαιότητα άμυνας συγκεκριμένα απέναντι στο επίπεδο που αφορά τους ενεργοποιήτες, λόγω των μη αναγνωρίσιμων επιρροών που έχουν συγκριτικά με τα άλλα δύο επίπεδα που προαναφέρθηκαν.

Στον Πίνακα 3.2 έχουμε μια συνοπτική παρουσίαση των επιθέσεων στον δευτερογενή διακρίνοντας τα σημαντικότερα χαρακτηριστικά τους.

Ref	*Είδος Inverter*	*Τύπος επίθεσης*	*Σημείο εισόδου επίθεσης*	*Στόχος επίθεσης*	*Περιγραφή επίθεσης*	*Islanded/Grid-tied Μικροδίκτυο*	*Αλγόριθμος Δευτερογενούς Ελέγχου*
[82]	Grid-following/ Grid-forming	FDI	Μονάδες ελέγχου	Διατάραξη της λειτουργίας καταμερισμού φορτίου (**load sharing**) και των συνολικών απαιτήσεων ισχύος (**total power demand).**	Εξετάζονται δύο διαφορετικές στρατηγικές επίθεσης. Στην πρώτη περίπτωση έχουμε χρήση ψευδών σημάτων μικρού πλάτους κάτι που ενώ δεν οδηγεί το σύστημα σε αστάθεια, αλλάζει τις τιμές στις οποίες συγκλίνουν σημαντικές παράμετροι όπως η τάση και η συχνότητα του κάθε κόμβου του μικροδικτύου. Στη δεύτερη περίπτωση, με αυξημένο το πλάτος των σημάτων, το σύστημα οδηγείται σε αστάθεια, με αρκετά μεγαλύτερη απόκλιση των τιμών των παραμέτρων.	Islanded	Discreet averaging κατανεμημένος έλεγχος συναίνεσης
[96]	Grid-following/ Grid-forming	DoS	Δίαυλοι επικοινωνίας συγκεκριμένα στο σημείο κοινής σύζευξης	Απόκλιση της τιμής της υπολειπόμενης χωρητικότητας RC (**Residual Capacity**) στον αντιστροφέα και του συντελεστή ενεργού ισχύος φ από τις επιθυμητές τιμές.	Μελετώνται δύο περιπτώσεις DoS επιθέσεων με διαφορετικούς κύκλους λειτουργίας. Κατά τις περιόδους που η επίθεση είναι ενεργή έχουμε διακοπή της ανταλλαγής πληροφοριών μεταξύ των κόμβων αντιστροφέων κάτι που οδηγεί σε διαταραχή του δευτερογενούς ελέγχου και της βελτίωσης της ποιότητας ισχύος. Παρατηρούνται ανεπιθύμητες αρμονικές και διακυμάνσεις τιμών όπως ο συτεντελεστής ενεργούς ισχύος και αύξηση της total rated-current distortion στο PCC.	Grid-tied	Event-triggered κατανεμημένος έλεγχος
[97]	Grid-following/ Grid-forming	Time-varying latency και DoS	Δίκτυο επικοινωνίας κόμβων	Αποκατάσταση συχνότητας (**Frequency restoration)** και ο ακριβής διαμοιρασμός ενεργού ισχύος (**Active power sharing)**.	Στην περίπτωση των πιο απλών latency attacks έχουμε διακυμάνσεις στις τιμές παραμέτρων όπως η συχνότητα του συστήματος και η ενεργή ισχύς που παράγεται από τον κάθε κόμβο. Οι επιθέσεις DoS οδηγούν σε καταστροφή της τοπολογίας του μικροδικτύου αποσυνδέοντας διάφορους κόμβους (αλλοίωση του πίνακα γειτνίασης και επομένως του πίνακα Laplace) και ανάλογα με το πόσο μεγάλος είναι ο κύκλος λειτουργίας τους, αυξάνονται τα προβλήματα που δημιουργούν στην ευστάθεια του μικροδικτύου.	Islanded	Adaptive gain ελεγκτής Event-triggered κατανεμημένος έλεγχος
[83]	Grid-following/ Grid-forming	FDI	Αισθητήρες-Ενεργοποιητές	Η λειτουργία συγχρονισμού της συχνότητας (**frequency synchronization and tracking**) του δικτύου των αντιστροφέων.	Συναντώνται διακυμάνσεις στη συχνότητα των κόμβων των αντριστροφέων καθώς επηρεάζονται οι τιμές των παραμέτρων που είτε μεταδίδονται από τον κάθε κόμβο του μικροδικτύου (αισθητήρες), είτε παραλαμβάνονται από τον κάθε κόμβο (ενεργοποιητές). Πρόκληση αποσταθεροποίησης της λειτουργίας συγχρονισμού συχνότητας και εν τέλει του συστήματος αντιστροφέων.	Islanded	Observer-based κατανεμημένος έλεγχος
[98]	Grid-following/ Grid-forming	DoS	Δίκτυο επικοινωνίας κόμβων	Δημιουργία προβλημάτων στις λειτουργίες διαμοιρασμού άεργου ισχύος και ρύθμισης της τάσης.	Πρόκληση αλλαγών στην τοπολογία του δικτύου (αλλοίωση του πίνακα γειτνίασης και επομένως του πίνακα Laplace) με αποτέλεσμα τη διατάραξη του ελέγχου συχνότητας και του ελέγχου τάσης. Διακύμανση τιμών όπως η ενεργός ισχύς του κάθε κόμβου με αποτέλεσμα τη μη οικονομική λειτουργία του μικροδικτύου και σε κάποιες περιπτώσεις ακόμα και την πλήρη κατάρρευση του.	Both	Αναλογικός-ολοκληρωτικός έλεγχος κατανεμημένου μέσου όρου (DAPI)
[84]	Grid-following/ Grid-forming	(Stealthy) FDI, DoS	Κατανεμημένοι ενεργειακοί πόροι και δίκτυο επικοινωνίας	Αποκατάσταση συχνότητας (**Frequency restoration)** και ο ακριβής διαμοιρασμός ενεργού ισχύος (**Active power sharing)**.	**FDI**: Αλλοιώσεις των τιμών αναφοράς στους pinned κόμβους και των τιμών που ανταλλάσονται μεταξύ των διαφόρων κόμβων οδηγεί το σύστημα σε απόκλιση από τις επιθυμητές συνθήκες λειτουργίας καθώς εμποδίζεται η αποκατάσταση της	Islanded	Pinning κατανεμημένος έλεγχος συναίνεσης

					συχνότητας των κατανεμημένων ενεργειακών πόρων. Επίσης έχουμε επιπτώσεις στο διαμοιρασμό ισχύος μεταξύ των κόμβων. Μεγάλο άνω φράγμα στην τιμή των ψευδών δεδομένων οδηγεί το δίκτυο σε αστάθεια. **<u>DoS</u>**: Διακοπή ανταλλαγής μετρήσεων μεταξύ κόμβων του μικροδικτύου εξαιτίας της καταστροφής επικοινωνιακών διαύλων που οδηγεί στην αλλαγή της αρχικής τοπολογίας. Έχουμε αποκλίσεις από τις ζητούμενες τιμές συχνότητας και ενεργού ισχύος.		
[85]	Grid-following/ Grid-forming	FDI	ESS ενεργοποιητές	Ισορροπία SoC(State of charge), διαμοιρασμός ενεργού ισχύος και αποκατάσταση συχνότητας.	Η συχνότητα του μικροδικτύου αποκλίνει από την ονομαστική τιμή της και η ενεργός ισχύς του κάθε συστήματος αποθήκευσης ενέργειας παρουσιάζει ταλαντώσεις.	Islanded	Συνεργατικός έλεγχος για multi-agent συστήματα
[86]	Grid-following/ Grid-forming	FDI	Αισθητήρες-Ενεργοποιητές, Δίαυλοι επικοινωνίας	Επιδείνωση της λειτουργίας του συγχρονισμού συχνότητας του δικτύου.	Προβλήματα στην επαναφορά της συχνότητας στην ονομαστική τιμή της κατά τις επιθέσεις.	Islanded	Συμβατικός consensus, Observer-based κατανεμημένος έλεγχος με εικονικό στρώμα
[99]	Grid-following/ Grid-forming	DoS	Δίαυλοι επικοινωνίας	Παρεμπόδιση της λειτουργίας αποκατάστασης συχνότητας και τάσης, ακριβή διαμοιρασμού ενεργού ισχύος και αύξηση του κόστους για κάθε επιμέρους κόμβο ($/KWh).	Μείωση της ποιότητας επικοινωνίας των επιμέρους κόμβων του μικροδικτύου με τη διεξαγωγή πολλών επιθέσεων DoS ανά τακτά χρονικά διαστήματα με αποτέλεσμα την αύξηση του οικονομικού κόστους λειτουργίας του δικτύου αλλά και ακόμα και την πρόκληση αστάθειας στο σύστημα.	Islanded	Event triggered κατανεμημένος έλεγχος
[87]	Grid-forming/ Grid-following	FDI	Μονάδα ελέγχου	Υποβάθμιση της λειτουργίας του ελεγκτή του δευτερογενούς επιπέδου που οδηγεί σε προβλήματα τον διαμοιρασμό ισχύος, σε ταλάντωση την τάση και πιθανή αστάθεια το σύστημα	Το ψευδές σήμα που εισάγεται στον δευτερογενή έλεγκτη δημιουργεί προβλήματα στη ρύθμιση της τάσης και τα αλλοιωμένα σήματα, που δίνει ο ελεγκτής στους ενεργοποιητές του μικροδικτύου, υποβαθμίζουν το διαμοιρασμό ισχύος μεταξύ τους. Ταλαντώσεις της τάσης και του ρεύματος και καθυστέρηση στη σύγκλιση ή απόκλιση από τις επιθυμητές τιμές, μπορούν να οδηγήσουν σε αστάθεια.	Islanded microgrid cluster	Βασισμένος στη συναίνεση κατανεμημένος έλεγχος
[88]	Grid-following/ Grid-forming	FDI, DoS	Αισθητήρες-Ενεργοποιητές, Δίαυλοι επικοινωνίας	Επιδείνωση της λειτουργίας ελέγχου συχνότητας φορτίου (**Load frequency control**).	Αύξηση της απόκλισης της συχνότητας του συστήματος με αύξηση της μεταβλητής που χρησιμοποιείται στην H∞ για να δείξει τη δυνατότητα αναγνώρισης της επίθεσης FDI και με μείωση της μεταβλητής που δείχνει το χρόνο που μεσολαβεί μεταξύ των επιθέσεων DoS. Τα αποτελέσματα είναι σαφώς χειρότερα στο δίκτυο όταν έχουμε FDI και DoS επιθέσεις ταυτόχρονα.	Islanded	Observer-based κεντρικός έλεγχος
[89]	Grid-following/ Grid-forming	Hybrid attack (FDI + DoS)	Αισθητήρες-Ενεργοποιητές, Δίαυλοι επικοινωνίας	Διατάραξη του ελέγχου της απόκλισης συχνότητας και τάσης (**Frequency and voltage deviation control)**.	Μέσω της αλλοίωσης των μετρήσεων τάσης και συχνότητας στους sensors/actuators και της παρεμπόδισης ανταλλαγής πληροφορίας μέσω των διαύλων επικοινωνίας ανάμεσα σε επιμέρους κόμβους του μικροδικτύου, το σύστημα οδηγείται σε αστάθεια.	Islanded	Observer-based κατανεμημένος έλεγχος
[90]	Grid-following/ Grid-forming	FDI	Αισθητήρες-Ενεργοποιητές	Δημιουργία προβλημάτων στον οικονομικό έλεγχο του δικτύου και στη λειτουργία της ρύθμισης της συχνότητας (η οικονομία του σύστηματος συνδέεται κυρίως με την ενεργό ισχύ).	Ο επιτιθέμενος στέλνει αλλοιωμένες μετρήσεις σε κάποιον γειτονικό κόμβο του μικροδικτύου με αποτέλεσμα την απόκλιση από τις ζητούμενες στιγμές και την πρόκληση αστάθειας στο σύστημα.	Islanded	Βασισμένος στη συναίνεση κατανεμημένος έλεγχος

[100]	Grid-following/ Grid-forming	DoS	Δίαυλοι επικοινωνίας	Αύξηση του βάρους της επικοινωνίας μεταξύ των επιμέρους συμπλεγμάτων και επιδείνωση της αποκατάστασης της συχνότητας και του ακριβή διαμοιρασμού ενεργού ισχύος.	Λόγω μιας DoS επίθεσης στη σύνδεση μεταξύ ενός AC μικροδικτύου και ενός DC μικροδικτύου (τα μικροδίκτυα αυτά είναι μέρη ενός δικτύου από περισσότερα μικροδίκτυα συνδεδεμένα μεταξύ τους), παρατηρείται σημαντική απόκλιση στη συχνότητα, τάση και στην ακρίβεια του δικτύου για τη σωστή κατανομή ισχύος ανάμεσα στα επιμέρους μικροδίκτυά του.	Islanded δίκτυο από επιμέρους μικροδίκτυα	Event-triggered κατανεμημένος έλεγχος
[91]	Grid-following/ Grid-forming	State-dependent FDI	Αισθητήρες-Ενεργοποιητές, Δίαυλοι επικοινωνίας, Μονάδα ελέγχου	Αποσταθεροποίηση του μικροδικτύου και οδήγηση της πορείας του σε μη ασφαλή κατάσταση λειτουργίας παρεμποδίζοντας το συγχρονισμό σύχνότητας και το διαμοιρασμό ενεργού ισχύος.	Θεωρώντας επιθέσεις ταυτόχρονα σε ενεργοποιητές, διαύλους επικοινωνίας, αισθητήρες και τιμές αναφοράς σε ελεγκτές, ο συγχρονισμός της συχνότητας και ο ισότιμος διαμοιρασμός ενεργού ισχύος επηρεάζονται αρνητικά.	Islanded	Βασισμένος στη συναίνεση κατανεμημένος έλεγχος
[101]	Grid-following/ Grid-forming	Τυχαίες DoS	Δίαυλοι επικοινωνίας	Υποβάθμιση της ικανότητας του δικτύου για αποκατάσταση της συχνότητας, της τάσης και της ενεργού ισχύος στις επιθυμητές τιμές.	Προκαλούνται ταλαντώσεις στις τιμές της συχνότητας, τάσης και ενεργού ισχύος των κατανεμημένων πόρων του μικροδικτύου οι οποίες αυξάνονται ανάλογα με το χρονικό διάστημα που διαρκούν οι επιθέσεις DoS.	Islanded	Communication-based κεντρικός έλεγχος συχνότητας
[92]	Grid-following/ Grid-forming	FDI	Ελεγκτής κατανεμημένου ενεργειακού πόρου	Οδήγηση των μετρήσεων της συχνότητας και ενεργού ισχύος του δικτύου σε διαφορετικές τιμές από τις επιθυμητές και σημαντική απόκλιση της τιμής της σχετικής εντροπίας του κόμβου που δέχεται την επίθεση.	Η αλλοίωση της συχνότητας του κόμβου που δέχεται την επίθεση προκαλεί ταλαντώσεις στην τιμή της τάσης και της ισχύος όλων των προσβάσιμων, από τον αρχικό, κόμβων.	Islanded	Βασισμένος στη συναίνεση κατανεμημένος έλεγχος
[93]	Grid-following/ Grid-forming	FDI	Δίαυλοι επικοινωνίας, Κατανεμημένη μονάδα παραγωγής	Επιδείνωση του διαμοιρασμού ενεργού και άεργου ισχύος κατά την αποκατάσταση της συχνότητας και της τάσης αντίστοιχα.	**Link/node attacks:** Αλλοίωση συχνότητας/τάσης προκαλεί ταλαντώσεις των τιμών τους στους στόχους της επίθεσης αλλά και στους γειτονικούς κόμβους.	Islanded	Observer-based κατανεμημένος έλεγχος
[94]	Grid-following/ Grid-forming	FDI Control input Load deviation	Αισθητήρες-Ενεργοποιητές, Φορτία του μικροδικτύου	Δημιουργία προβλημάτων στις λειτουργίες διαμοιρασμού ενεργού ισχύος και ρύθμισης της συχνότητας.	**FDI:** Αλλαγή της τάσης απ' τον αισθητήρα προκαλεί ταλαντώσεις στην τάση και αποκλίσεις σε ενεργό και άεργο ισχύ. **Sparse additive:** Αλλαγές στα σήματα διαμόρφωσης του αντιστροφέα προκαλούν αλλοιώσεις σε όλες τις σχετικές τιμές. Αστάθεια συστήματος σε περίπτωση μεγάλων διαταραχών. **Load deviation:** Αλλαγές σε φορτία του συστήματος οδηγούν σε ταλαντώσεις στη συχνότητα. Πιθανή ζημιά σε εξοπλισμό και ενεργοποίση μηχανισμών απόρριψης φορτίων.	Islanded	Κεντρικός έλεγχος με κατανεμημένους ανιχνευτές στις κατανεμημένες μονάδες παραγωγής
[102]	Grid-following/ Grid-forming	DoS	Δίαυλοι επικοινωνίας	Μέσο τετραγωνικό σφάλμα των εκτιμητών διάφορο του μηδενός ώστε να έχουμε υποβάθμιση του διαμοιρασμού ισχύος στο μικροδίκτυο.	Διακυμάνσεις στις τιμές της ισχύος οδηγούν σε προβλήματα διαμοιρασμού ισχύος ανάμεσα σε όλες τις επιμέρους DGs.	Grid-tied	Observer-based αποκεντρωμένοι προσαρμοστικοί ελεγκτές με κατανεμημένους παρατηρητές και εκτιμητές
[103]	Grid-following/ Grid-forming	DoS	Αισθητήρες-Ενεργοποιητές	Ταλαντώσεις της συχνότητας και της ενεργού ισχύος, πιθανή	Ταλαντώσεις σε συχνότητα και ενεργό ισχύ οδηγούν σε προβλήματα στο συγχρονισμό συχνότητας και στο διαμοιρασμό	Islanded σύμπλεγμα μικροδικτύων	Self-triggered βασισμένος στη συναίνεση

			στο κάθε μικροδίκτυο, Δίαυλοι επικοινωνίας μεταξύ μικροδικτύων	ενεργοποίηση προστατευτικών μηχανισμών με διακοπές ρεύματος.	ισχύος στο δίκτυο με αποτέλεσμα τη γενικότερη επιδείνωση της λειτουργίας του δικτύου (ενεργοποίηση προστατευτικών μηχανισμών, απόρριψη φορτίου, διακοπές ρεύματος)		κατανεμημένος έλεγχος
[95]	Grid-following/Grid-forming	FDI	Δίαυλοι επικοινωνίας, Μονάδες ελέγχου	Επιδείνωση της λειτουργίας του συγχρονισμού συχνότητας του δικτύου.	Διακυμάνσεις σε συχνότητα και τάση οδηγούν σε απώλεια δυνατότητας συγχρονισμού στο δίκτυο.	Islanded	Leaders-followers συνεργατικός κατανεμημένος έλεγχος

Πίνακας 3.2: *Περίληψη των επιθέσεων στον δευτερογενή έλεγχο*

Κεφάλαιο 4

Άμυνα απέναντι στις κυβερνοεπιθέσεις σε συστήματα βασισμένα σε αντιστροφείς με έμφαση στα μικροδίκτυα

Στο κεφάλαιο αυτό γίνεται μελέτη την αμυντικών μηχανισμών που υλοποιούνται για να προστατεύσουν τα συστήματα από τις πιο σύγχρονες επιθέσεις που δε μπορούν να αντιμετωπιστούν με συμβατικούς τρόπους. Οι μηχανισμοί αυτοί περιγράφονται και μελετώνται δίνοντας έμφαση στους τρόπους με τους οποίους αναγνωρίζουν μια επίθεση και προσδιορίζουν τα χαρακτηριστικά τους, στη διαδικασία που ακολουθούν για τη μερική ή πλήρη αντιμετώπιση των επιπτώσεων αυτών των επιθέσεων στο δίκτυο και τα εργαλεία που χρησιμοποιούν για να επιτύχουν τα παραπάνω.

4.1 Εισαγωγικά στοιχεία της αμυντικής διαδικασίας

Έχοντας κάνει ανασκόπηση των περιπτώσεων των επιθέσεων, είναι φυσικά απαραίτητο να μελετήσουμε τους αμυντικούς μηχανισμούς και τις διαδικασίες που ακολουθούνται στη βιβλιογραφία, προκειμένου να προστατευτούν τα συστήματα. Στο Σχ. 4.1 παρουσιάζουμε ένα ενδεικτικό διάγραμμα με τα βήματα που ακολουθούνται ανάλογα με το αν το δίκτυο προστατεύεται από επιθέσεις με τη χρήση κάποιου συστήματος πρόληψης εισβολών ή όχι. Επειδή το σύστημα πρόληψης εισβολής δεν είναι συνηθισμένο, ειδικά στα μικροδίκτυα, λόγω των περισσότερων απαιτήσεων του σε πόρους και πιο εκτενείς υποδομές επικοινωνίας, εστιάζουμε στα βήματα της ανίχνευσης της εισβολής και του μετριασμού των επιπτώσεων.

Για την επαναφορά του συστήματος, που δέχεται την επίθεση, πάλι στην κανονική λειτουργία, το πρώτο βήμα είναι ο εντοπισμός της εισβολής. Αυτό το τμήμα είναι υπεύθυνο για την ανίχνευση και τον προσδιορισμό των χαρακτηριστικών της επίθεσης όπως είναι τα σήματα και οι κόμβοι-στόχοι της επίθεσης. Αυτή η διαδικασία μπορεί να κατηγοριοποιηθεί ως εξής:

1. **Anomaly-based** εντοπισμός εισβολής, που έχουμε όταν η ανίχνευση γίνεται συγκρίνοντας δεδομένα πραγματικού χρόνου με την αναμενόμενη στατιστικά συμπεριφορά χρησιμοποιώντας εργαλεία όπως μαθηματικά μοντέλα και ταξινομητές μηχανικής μάθησης.
2. **Observer-based** εντοπισμός εισβολής, που έχουμε όταν η ανίχνευση συμβαίνει συγκρίνοντας τις πραγματικές μετρήσεις με τις αναμενόμενες εξόδους του συστήματος, που προκύπτουν από τις εξισώσεις κατάστασής του, χρησιμοποιώντας εργαλεία όπως Kalman φίλτρα.
3. **Signature-based** εντοπισμός εισβολής, που έχουμε όταν η ανίχνευση πραγματοποιείται μέσω της σύγκρισης των εισόδων με βιβλιοθήκες γνωστών παλαιότερων επιθέσεων.

Αξίζει να σημειωθεί πως εστιάζουμε στις δύο πρώτες κατηγορίες, καθώς η τρίτη δε χρησιμοποιείται εξαιτίας του γεγονότος ότι είναι περιορισμένη σε γνωστές μόνο επιθέσεις. Τέλος, ο μηχανισμός του εντοπισμού είναι υπεύθυνος για την ενεργοποίηση του δεύτερου βήματος της αμυντικής διαδικασίας, αυτό του μετριασμού των επιπτώσεων.

Στον μετριασμό των επιπτώσεων, ο μηχανισμός είναι υπεύθυνος για τη μερική ή πλήρη αντιμετώπιση της επίθεσης και των επιπτώσεων της με μεγαλύτερο στόχο τη διατήρηση της διαθεσιμότητας που είναι υψίστης σημασίας για τα ηλεκτρικά δίκτυα. Σημαντικές στρατηγικές που

αξίζει να αναφερθούν με βάση τη βιβλιογραφική μελέτη είναι οι εξής:

1. **Observer-based εκτίμηση**, κατά την οποία συνήθως χρησιμοποιούνται κατανεμημένοι παρατηρητές οι οποίοι τοπικά προσπαθούν να εκτιμήσουν τις τιμές που, είτε αλλοιώθηκαν εξαιτίας κάποιας επίθεσης και απορρίφθηκαν γι' αυτό, είτε δε μπόρεσαν να μεταδοθούν λόγω διακοπής της επικοινωνίας μεταξύ δύο επιμέρους κόμβων.
2. **Υλοποίηση εικονικού στρώματος**, το οποίο είναι αδιάβλητο, συνδέεται με το πραγματικό δίκτυο μέσω ειδικών πινάκων και το επιβλέπει και αποστέλλει σήματα αντιστάθμισης όταν βλέπει να αποκλίνει από την επιθυμητή κατάσταση.
3. **Event-triggered** επικοινωνία, κατά την οποία η επικοινωνία μεταξύ των επιμέρους κόμβων ενεργοποιείται, μόνο όταν ικανοποιείται κάποια συνθήκη όπως όταν η διαφορά μεταξύ της τωρινής κατάστασης ενός κόμβου και της τελευταίας κατάστασης που μετάδωσε, είναι μεγαλύτερη από ένα δυναμικά μεταβαλλόμενο κατώφλι.

Σχήμα 4.1: *Συνοπτικό διάγραμμα ροής της αμυντικής διαδικασίας*

4.2 Μηχανισμοί ανίχνευσης εισβολής στον αντιστροφέα και στον πρωτογενή έλεγχο

Στο [44] σχεδιάζονται και υλοποιούνται ειδικά προσαρμοσμένοι μετρητές απόδοσης του υλικού (hardware performance counters) αντιστροφέων, οι οποίοι μαζί με τη βοήθεια ταξινομητών μηχανικής μάθησης, ανιχνεύουν επιθέσεις εναντίον του firmware. Αυτοί οι μετρητές παρακολουθούν τις ακολουθίες και τους τύπους εντολών (αριθμητική, λογική αποθήκευσης, φόρτωσης) που εκτελούνται και συγκρίνοντάς τα με τη βοήθεια των ταξινομητών, ανιχνεύουν ανωμαλίες στην αναμενόμενη συμπεριφορά του συστήματος. Αυτοί οι μετρητές έχουν μικρές απαιτήσεις και είναι ιδανικοί για ενσωματωμένα συστήματα τα οποία δεν έχουν πολλούς υπολογιστικούς πόρους να διαθέσουν.

Στο [53] υλοποιείται ένα σύστημα άμυνας για δίκτυα κατανεμημένων ενεργειακών πόρων απέναντι σε FDI επιθέσεις που χρησιμοποιεί ένα φίλτρο Kalman για την εκτίμηση του πλάτους και της γωνίας φάσης της τάσης και υπολογίζει την Ευκλείδεια απόσταση μεταξύ της εκτίμησης και της πραγματικής τιμής. Αν το αποτέλεσμα ξεπερνά κάποιο όριο, τότε το σύστημα δέχεται επίθεση. Ο μηχανισμός αυτός εφαρμόζεται και σε μια περίπτωση που ο στόχος της επίθεσης είναι ένα PLL και μπορεί με λίγες μικρές προσαρμογές να εφαρμοστεί σε περιπτώσεις που το σύστημα είναι κάποιο μικροδίκτυο.

Στο [54] το προτεινόμενο σύστημα άμυνας για ενεργειακά συστήματα βασισμένα σε αντιστροφείς, συνδυάζει την ανίχνευση της εισβολής με τον αντιμετώπιση των επιπτώσεων που έχει στο δίκτυο. Χρησιμοποιεί έναν δείκτη σοβαρότητας επίθεσης (ASI) που χρησιμοποιεί τοπικές μετρήσεις τάσης και εσωτερικές εκτιμήσεις του PLL ώστε να παράγει ένα σήμα σφάλματος για την ανίχνευση. Στη συνέχεια, για την αντιμετώπιση των επιπτώσεων προτείνεται μια προσαρμοσμένη εκδοχή ενός PLL που διαθέτει τις λειτουργίες της κανονικοποίησης του πλάτους και της αντιστάθμισης της φάσης ακόμα και κατά τη διάρκεια μιας επίθεσης διασφαλίζοντας την ευστάθεια στο σύστημα.

Στο [46] υλοποιείται ένα αμυντικό σύστημα που ανιχνεύει FDI επιθέσεις με κύριο στόχο τους ελεγκτές αντιστροφέων ανεμογεννητριών. Χρησιμοποιεί αρχικά ένα Unscented Kalman φίλτρο για την παραγωγή υπόλοιπων μεταξύ αναμενόμενης και πραγματικής συμπεριφοράς του συστήματος. Στη συνέχεια, εκτιμά τα υπόλοιπα αυτά και αποφαίνεται για την ύπαρξη ή όχι κάποιας ανωμαλίας στο σύστημα χρησιμοποιώντας είτε τη μέθοδο Cumulative Sum (CUSUM) με καλύτερη απόδοση σε ανωμαλίες που επιμένουν, είτε τη μέθοδο γενικευμένου λόγου πιθανοφάνειας (GLR) με καλύτερη απόδοση απέναντι σε απότομες μεταβολές.

Στο [47] υλοποιείται ένας αμυντικός μηχανισμός ανίχνευσης επιθέσεων που χρησιμοποιεί στον πυρήνα του δύο Duffing ταλαντωτές μαζί με έναν διαφορικό ταλαντωτή. Ο μηχανισμός αποστέλλει ένα ειδικά σχεδιασμένο να μην επεμβαίνει στην κανονική λειτουργία, δυναμικό σήμα μικρού πλάτους στους ελεγκτές των αντιστροφέων και ανάλογα με την απόκριση που θα λάβει, οι ταλαντωτές μπαίνουν σε διαφορετικές καταστάσεις οι οποίες δείχνουν αν υπάρχει επίθεση και τι είδους είναι αυτή. Οι καταστάσεις των ταλαντωτών είναι είτε γραμμικές, είτε περιοδικές, είτε ομοκλινικές, είτε χαοτικές, είτε κάποιος συνδυασμός αυτών. Τέλος, χρησιμοποιούνται επιπλέον συντελεστές σύζευξης για την ποσοτικοποίηση των αποκλίσεων από την κανονική λειτουργία του συστήματος

4.3 Μηχανισμοί μετριασμού επιπτώσεων στον αντιστροφέα και στον πρωτογενή έλεγχο

Στο [51] υλοποιείται ένας μηχανισμός για την αντιμετώπιση των επιπτώσεων FDI επιθέσεων σε μικροδίκτυα βασισμένα σε αντιστροφείς αλλά κατέχει και την ικανότητα της επεκτασιμότητας. Χρησιμοποιεί Adversarial Markov Decision Process (AMDP) αντί για MDP για τη δημιουργία της αλληλεπίδρασης μεταξύ της άμυνας επίθεση ώστε να έχει τη δυνατότητα προσαρμογής του μηχανισμού με βάση την επίθεση που εξελίσσεται με την πάροδο του χρόνου. Με τη χρήση του αλγόριθμου Twin Delayed Deep Deterministic Policy Gradient (TD3) βρίσκει την επίθεση που φέρνει αστάθεια στο σύστημα με την ελάσσονα προσπάθεια και προσαρμόζει τα κέρδη του droop για την επαναφορά της ευστάθειας. Θετικά στοιχεία του είναι πως δε χρειάζεται να ελέγχει όλες τις σχετικές με τον droop έλεγχο παραμέτρους και ότι παρουσιάζει δυναμικότητα, απέναντι σε μια επίθεση που προσαρμόζεται, με πολύ λίγες αλλαγές.

Στο [56] έχουμε υλοποίηση ενός delayed Dual Second-Order Generalized Integrator (DSOGI) Voltage Modulated Vector Current Control (VM-VCC) για την αντικατάσταση του DSOGI PLL που είναι ευάλωτο σε επιθέσεις που μεταβάλουν τα κέρδη του. Με τη μέθοδο αυτή, δε χρειάζεται πια να υπολογιστεί η γωνία φάσης όπως συνήθως και χρησιμοποιείται στη θέση της η τάση θετικής ακολουθίας για τους απαραίτητους μετασχηματισμούς και επιτυγχάνει απόρριψη ανεπιθύμητων αρμονικών με χρήση ενός χειριστή καθυστέρησης αντί για τον παραδοσιακό τρόπο μετατόπισης της φάσης. Για την ασφάλεια του, χρησιμοποιείται ένα ψηφιακό αντίγραφο του παραπάνω DSOGI που εγγυάται την ομαλή και ασφαλή λειτουργία του παραπάνω υλοποιημένου μηχανισμού.

Στο [57] αντιμετωπίζονται περιπτώσεις GPS spoofing με τη δημιουργία ενός σήματος που

παρεμβαίνει στη δράση του σήματος του επιτιθέμενου χρησιμοποιώντας αντιστροφή φάσης του κώδικα και αντιστροφή φάσης της φέρουσας συχνότητας. Με αυτόν τον τρόπο το σύστημα διορθώνει το σφάλμα που προκλήθηκε από το κακόβουλο σήμα στο DLL και αντιμετωπίζει διακυμάνσεις σε συχνότητα και φάση στο PLL.

Στο [58] υλοποιείται ένας μηχανισμός περιορισμού των dq συνιστωσών του ρεύματος σε συνδεδεμένα με το δίκτυο MMCs ανάλογα με το αν η επίθεση στοχοποιεί 1) τον εσωτερικό βρόγχο ρεύματος ή 2) το PLL και τους εξωτερικούς βρόγχους ελέγχου της ισχύος. Στην πρώτη περίπτωση αντιμετωπίζει ταλαντώσεις υψηλών συχνοτήτων αν ο δείκτης συνολικής αρμονικής παραμόρφωσης είναι πάνω από 5% για παραπάνω από 400ms, ενώ στη δεύτερη περίπτωση αντιμετωπίζει αποκλίσεις τιμών και περιπτώσεις αστάθειας όποτε το ρεύμα ξεπεράσει το 120% της ονομαστικής του τιμής.

Στον Πίνακα 4.1 γίνεται μια συνοπτική παρουσίαση των αμυντικών μηχανισμών των παραπάνω περιπτώσεων στο επίπεδο του αντιστροφέα και του πρωτογενούς ελέγχου τονίζοντας τα πιο σημαντικά χαρακτηριστικά τους.

Ref	*Κατηγορία επίθεσης*	*Στοχός επίθεσης*	*Στρατηγική λύσης του προβλήματος άμυνας*	*Κατηγορία αμυντικής στρατηγικής*	*Στόχος αμυντικής διαδικασίας*
[51]	FDI	Droop έλεγχος	Στοχαστική διαδικασία λήψης αποφάσεων (Adversarial Markov decision process)	Μετριασμός επιπτώσεων (Impact Mitigation)	Twin delayed deep deterministic policy gradient Εύρεση των κατάλληλων κερδών των ελεκτών droop ελαχιστοποιώντας τις επιπτώσεις της επίθεσης, οδηγώντας σε μια εύρωστη στρατηγική άμυνας
[44]	FDI, DoS	Firmware ηλιακού μικροαντιστροφέα	Υλοποίηση προσαρμοσμένων Hardware performance μετρητών Anomaly-based Intrusion Detection System (IDS)	Εντοπισμός εισβολής (Intrusion detection)	Ανίχνευση με τη βοήθεια machine learning κακόβουλου κώδικα μέσω του ελέγχου του αριθμού και των ακολουθιών των εντολών assembly
[53]	FDI	PLL	Υλοποίηση κατάλληλου πλαισίου για την ανάπτυξη testbeds κυβερνοασφάλειας Κυρίως observer-based IDS με στοιχεία anomaly-based	Εντοπισμός εισβολής	Αλγόριθμος ανίχνευσης επίθεσης βασισμένος σε ένα φίλτρο Kalman το οποίο χρησιμοποιείται για την εκτίμηση του πλάτους και της γωνίας φάσης της τάσης Χρήση των υπόλοιπων (διαφορά μεταξύ μέτρησης και εκτιμώμενης τιμής) που δημιουργούνται από το φίλτρο Kalman για την ανίχνευση
[54]	FDI	PLL	Χρήση του δείκτη δριμύτητας επίθεσης (ASI) για την ανίχνευση της επίθεσης. Βελτίωση του κυκλώματος του PLL για την αντιμετώπιση για την αντιμετώπιση επιθέσεων που επηρεάζουν άεργο ισχύ και τάση Anomaly-based IDS	Εντοπισμός εισβολής και μετριασμός επιπτώσεων	Ανίχνευση και αντιμετώπιση της επίθεσης ώστε να αποφευχθεί αστάθεια του συστήματος που μπορεί να οδηγήσει σε συνολική κατάρρευση εξαιτίας της αλλοίωσης της ενεργού και της άεργου ισχύος
[56]	FDI	DSOGI PLL	Υλοποίηση ενός DSOGI-based VM-VCC με προσθήκη χρονικής καθυστέρησης και ενός δεύτερου ίδιου DSOGI για τον ασφαλή έλεγχο της λειτουργίας του πρώτου	Μετριασμός επιπτώσεων	Αντιμετώπιση επιθέσεων αλλοίωσης μετρήσεων, εξαλείφοντας αρμονικές συνιστώσες της τάσης με στόχο την ελαχιστοποίηση των επιπτώσεων της παραμόρφωσης της τάσης στην έγχυση ρεύματος στο δίκτυο από τον κατανεμημένο ενεργειακό πόρο
[57]	GPS Spoofing	DLL, PLL	Εξάλειψη του καναλιού μέσω του οποίου γίνεται το spoofing κατά τη διαδικασία επεξεργασίας σήματος ή δημιουργία ενός ίσου και αντίθετου σήματος κατά τον έλεγχο RF φάσης	Μετριασμός επιπτώσεων	Επαναφορά των εξόδων των PLL και DLL φίλτρων στις επιθυμητές τιμές εξουδετερώνοντας το ψεύτικο σήμα με ένα αντίθετο σήμα δημιουργημένο ειδικά για την αντιμετώπιση της επίθεσης
[58]	FDI	Βρόγχος ελέγχου ισχύος, PLL	Δημιουργία ορίων στις τιμές αναφοράς του ρεύματος ανάλογα με τη χρονική κλίμακα στην οποία ανήκει το κάθε κομμάτι του κυκλώματος	Μετριασμός επιπτώσεων	Αν το ρεύμα στο πιο αργό κομμάτι του κυκλώματος ξεπεράσει το 120% της ονομαστικής τιμής του, έχουμε κατάσταση σφάλματος και ενεργοποιείται το όριο στο κομμάτι αυτό. Αν η ολική αρμονική παραμόρφωση, μετά από κάποιο χρόνο ενεργού ορίου στο πιο αργό κομμάτι, εξακολουθεί να είναι πιο πάνω από μια τιμή, έχουμε ενεργοποίση του ορίου αυτού του πιο γρήγορου κομματιού Εξάλειψη των ταλαντώσεων χαμηλών συχνοτήτων και αποκλίσεων προερχόμενων από το PLL και τον έλεγχο ισχύος με χρήση του ορίου ρεύματος αυτού του πιο αργού μέρους Εξάλειψη των ταλαντώσεων υψηλών συχνοτήτων που δημιουργούνται εξαιτίας της αστάθειας του εσωτερικού βρόγχου ρεύματος με χρήση του ορίου στο ρεύμα του εσωτερικού πιο συχνά επαναλαμβανόμενου μέρους

[46]	FDI	Ελεγκτής αντιστροφέα	Model-based ανίχνευση με τη χρήση ενός Unscented Kalman φίλτρου, Generalised Likelihood Ratio τεστ και του Cumulative Sum αλγόριθμου Observer-based IDS	Εντοπισμός εισβολής	Ανίχνευση αλλοιώσεων σε τιμές όπως τα κέρδη ελεγκτών και οι μετρήσεις αισθητήρων αλλά και σε παραμέτρους όπως τα σήματα ελέγχου με τη χρήση ενός Kalman φίλτρου για την παραγωγή υπολοίπου και τη χρήση GLR test και CUSUM αλγόριθμου για την αξιολόγηση αυτού του υπολοίπου Χρήση είτε του GLR τεστ είτε του CUSUM αλγόριθμου για την ανίχνευση.
[47]	Τροποποίηση τοπολογίας, FDI(επίθεση αντικατάστασης δεδομένων), Επίθεση επαναποστολής δεδομένων μαζί με επίθεση αντικατάστασης δεδομένων	Εσωτερικός ελεγκτής μπαταρίας, Ελεγκτές εξωτερικών βρόγχων μπαταρίας και κυψέλης καυσίμου	Model-free ανίχνευση με μικρή επιβάρυνση του συστήματος βασισμένη στη χρήση Duffing ταλαντωτών. Anomaly-based IDS	Εντοπισμός εισβολής	Ανάλογα με το αν το σύστημα δέχεται επίθεση και ανάλογα με τον τύπο αυτής, οι δύο Duffing ταλαντωτές μαζί με τον διαφορικό ταλαντωτή αλλάζουν καταστάσεις και ανάλογα με την κατάσταση έχουμε και προσδιορισμό των επιθέσεων.

Πίνακας 4.1: *Περίληψη αμυντικών μηχανισμών για τον αντιστροφέα και τον πρωτογενή έλεγχο*

4.4 Ανίχνευση εισβολής με μετριασμό επιπτώσεων στον δευτερογενή έλεγχο

Στην περίπτωση του δευτερογενούς ελέγχου, αξίζει να σημειωθεί πως η συντριπτική πλειοψηφία, ειδικά της πιο σύγχρονης βιβλιογραφίας, εστιάζει αποκλειστικά στους μηχανισμούς αντιμετώπισης των επιπτώσεων των επιθέσεων, καθώς λόγω της επικοινωνίας μεταξύ των επιμέρους κόμβων και γενικά των υπαρχόντων αλγόριθμων ελέγχου, η ανίχνευση μιας εισβολής είναι πιο απλή σχετικά με τον πρωτογενή και σε πολλές περιπτώσεις θεωρείται τετριμμένη.

Πάραυτα, παρακάτω μελετάμε κάποιες περιπτώσεις που υλοποιούν μηχανισμούς οι οποίοι συνδυάζουν τα δύο κύρια βήματα της αμυντικής διαδικασίας.

Στο [92] υλοποιείται ένα αμυντικό σύστημα στον κατανεμημένο δευτερογενή έλεγχο ενός μικροδικτύου το οποίο πρώτα ανιχνεύει μια εισβολή και προσδιορίζει τα χαρακτηριστικά της και στη συνέχεια αντιμετωπίζει τις επιπτώσεις της στο σύστημα. Αρχικά, χρησιμοποιείται η μέθοδος της Kullback-Leibler απόκλισης για την ανίχνευση στατιστικών ανωμαλιών σημάτων ελέγχου συχνότητας και τάσης και αν η απόκλιση βρεθεί μεγαλύτερη από ένα κατώφλι, το σύστημα αποφαίνεται ότι υπάρχει επίθεση. Στη συνέχεια, με βάση τις αποκλίσεις, κάθε κατανεμημένος κόμβος υπολογίζει κάποιες τιμές που δείχνουν το πόσο έμπιστος είναι ο ίδιος και το πόσο έμπιστος είναι κάθε γειτονικός του κόμβος. Αυτές οι τιμές χρησιμοποιούνται για να δοθεί, σε κάθε επικοινωνιακό δίαυλο, ένα βάρος, το οποίο χρησιμοποιείται για να κρίνει κάθε κόμβος ποια από τα δεδομένα που παίρνει μέσω κάθε διαύλου είναι ασφαλή και ποια όχι. Αυτά που κρίνονται μη ασφαλή, λαμβάνονται είτε λιγότερο υπόψη είτε καθόλου, εμποδίζοντας την κλιμάκωση των προβλημάτων. Με αυτόν τον τρόπο, εξασφαλίζεται η λειτουργία της αποκατάστασης συχνότητας και τάσης στο δίκτυο.

Στο [93] υλοποιείται ένας μηχανισμός που ανιχνεύει μια επίθεση μέσω εξισώσεις παρατηρητή σε κάθε κόμβο χρησιμοποιώντας τους κάθε φορά ανανεωμένους δείκτες εμπιστοσύνης των κόμβων για να εντοπιστούν ποιοι από τους κόμβους δεν είναι ασφαλείς. Στη συνέχεια, τα δεδομένα που μεταφέρονται από τους κόμβους, που κρίθηκαν μη ασφαλείς, δε λαμβάνονται υπόψη από τους άλλους κόμβους και το σύστημα προχωρά σε εκτιμήσεις με βάση τις μετρήσεις που ανταλλάσσονται μεταξύ των ασφαλών κόμβων. Ένα ιδιαίτερα σημαντικό χαρακτηριστικό αυτού του υλοποιημένου συστήματος είναι, πως εγγυάται αντιμετώπιση των αποκλίσεων συχνότητας και τάσης σε πεπερασμένο χρόνο μειώνοντας έτσι την πιθανότητα πρόκλησης μεγαλύτερων προβλημάτων όπως είναι η αστάθεια.

Στο [94] έχουμε υλοποίηση ενός μηχανισμού που ανιχνεύει και αντιμετωπίζει επιθέσεις

διαφόρων ειδών απέναντι σε μικροδίκτυα. Υπολογίζοντας υπόλοιπα μεταξύ πραγματικών και εκτιμώμενων τιμών και βλέποντας αν υπερβαίνουν κάποιο δυναμικά μεταβαλλόμενο κατώφλι, ο κεντρικός ελεγκτής αποφαίνεται για το αν υπάρχει επίθεση και ποιοι κόμβοι δεν είναι ασφαλείς. Στη συνέχεια για την αντιμετώπιση της επίθεσης, απομονώνονται οι κόμβοι που επηρεάζονται από την επίθεση, ώστε να ελαχιστοποιηθούν οι διαταραχές στο σύστημα. Στη συγκεκριμένη περίπτωση, ενώ το σύστημα δευτερογενούς ελέγχου είναι κεντρικό, έχουμε την ιδιαιτερότητα πως κατά την ανίχνευση, οι κατανεμημένοι κόμβοι μοιράζονται δεδομένα με τους γείτονές τους. Ιδιαίτερα σημαντικό χαρακτηριστικό της υλοποίησης είναι πως ο μηχανισμός δε χρειάζεται πλήρη γνώση του συστήματος και χρησιμοποιεί τη μέθοδο αναγνώρισης υποχώρου για να δημιουργήσει τις εξισώσεις κατάστασης του συστήματος όταν δεν υπάρχει κάποια επίθεση.

4.5 Μηχανισμοί μετριασμού επιπτώσεων στον δευτερογενή έλεγχο

Στο [96] υλοποιείται ένας αμυντικός μηχανισμός για μικροδίκτυο βασισμένο σε αντιστροφείς, το οποίο λειτουργεί συνδεδεμένο στο δίκτυο και περιλαμβάνει έναν ανθεκτικό, σε DoS επιθέσεις, event-triggered κατανεμημένο δευτερογενή έλεγχο. Κάθε αντιστροφέας υπολογίζει το ενεργειακό του υπόλοιπο και μέσω της επικοινωνίας μεταξύ τους, υπολογίζεται η συνολική υπολειπόμενη χωρητικότητα (residual capacity), ώστε τελικά να δοθεί τιμή αναφοράς του ρεύματος στο μικροδίκτυο των αντιστροφέων με βάση κανόνες δίκαιου διαμοιρασμού ισχύος. Έτσι, επιτυγχάνεται βελτίωση της ποιότητας ισχύος στο κοινό σημείο σύζευξης με το ευρύ δίκτυο ακόμα και κατά τη διάρκεια DoS επιθέσεων οι οποίες παρεμποδίζουν την επικοινωνία μεταξύ κόμβων. Αξίζει να αναφερθεί πως για να είναι αυτό δυνατό, ο event-triggered έλεγχος προσαρμόζεται ώστε να ενεργοποιεί την επικοινωνία όταν δεν είναι ενεργή η DoS επίθεση και μόνο αν υπάρχει μεγάλη απόκλιση μεταξύ της τωρινής κατάστασης και της κατάστασης την προηγούμενη τελευταία στιγμή που η επικοινωνία ήταν ενεργή.

Στο [97] έχουμε υλοποίηση ενός αμυντικού μηχανισμού για ένα απομονωμένο μικροδίκτυο του οποίου η επικοινωνία δέχεται Latency και DoS επιθέσεις. Ο μηχανισμός αυτός έχει δύο λειτουργίες ελέγχου που δουλεύουν συγχρονισμένα για να επιτύχουν την ομαλή λειτουργία του μικροδικτύου. Κατά την πρώτη λειτουργία, έχουμε έλεγχο προσαρμοζόμενου κέρδους, που εγγυάται τη στοχαστική ευστάθεια υπό τυχαίες καθυστερήσεις στην επικοινωνία, χρησιμοποιώντας έναν πίνακα προσαρμοζόμενων κερδών με βάση την καθυστέρηση και τη κατάσταση του δικτύου κάθε στιγμή. Βασίζεται στην ανάλυση Lyapunov–Krasovskii για την παραγωγή των συνθηκών

ευστάθειας και μοντελοποιείται ως ένα Time-Delayed Markov Jump Linear σύστημα. Κατά τη δεύτερη λειτουργία, έχουμε Event-Triggered Topology Reconfiguration έλεγχο που είναι υπεύθυνος για την αλλαγή της τοπολογίας λύνοντας ένα πρόβλημα βελτιστοποίησης, μεγιστοποιώντας τη συνδεσιμότητα και ελαχιστοποιώντας το κόστος στην επικοινωνία. Η δεύτερη λειτουργία ενεργοποιείται μόνο όταν η διάρκεια των καθυστερήσεων ξεπεράσει κάποιο κατώφλι.

Στο [83] υλοποιείται ένας observer-based αμυντικός μηχανισμός για προστασία μικροδικτύων εναντίον FDI επιθέσεων σε αισθητήρες και ενεργοποιητές. Οι κατανεμημένοι παρατηρητές είναι υπεύθυνοι για την εκτίμηση των σημάτων επίθεσης που εγχέονται στους αισθητήρες και ενεργοποιητές και στη συνέχεια, ένας κατανεμημένος ελεγκτής ανάδρασης εξόδου τύπου H∞ χρησιμοποιεί τις εκτιμήσεις αυτές, για να αντισταθμίσει τα σήματα. Ο τύπος H∞ είναι χρήσιμος γιατί επιβεβαιώνει την ανθεκτικότητα του συστήματος στη χειρότερη περίπτωση διαταραχών. Το σύστημα άμυνας αποκαθιστά τη συχνότητα σε επιθυμητές τιμές και διατηρεί ομαλή τη λειτουργία του μικροδικτύου χωρίς να χρειάζεται ιδιαίτερες γνώσεις για τις επιθέσεις όπως το ποιοι κόμβοι πλήττονται και ποια είναι τα πλάτη των σημάτων επίθεσης, παρά μόνο χρειάζεται να ξέρουμε ότι οι παράγωγοι είναι φραγμένες.

Στο [98] υλοποιείται ένα αμυντικό σύστημα για μικροδίκτυα, που δέχονται DoS επιθέσεις, το οποίο εστιάζει στην εξασφάλιση του γεγονότος πως το μικροδίκτυο έχει ένα έγκυρο σημείο λειτουργίας. Αυτό επιτυγχάνεται με τον μετασχηματισμό του κυβερνοφυσικού μικροδικτύου σε αμιγώς φυσικό, που μεταχειρίζεται τις επιθέσεις ως ενέργειες μεταβολής παραμέτρων όπως η έγχυση ισχύος. Κατά τη διαδικασία αυτή, δημιουργούνται καινούριες εξισώσεις ροής ισχύος συμπεριλαμβάνοντας τις αλλαγές από τις επιθέσεις, μοντελοποιούνται οι ζυγοί των αντιστροφέων ως PQ ζυγοί και τελικά αν μετά από αυτές τις αλλαγές, η λειτουργία του συστήματος είναι εφικτή για τη χειρότερη δυνατή περίπτωση, θα είναι δυνατή και για οποιαδήποτε άλλη.

Στο [84] υλοποιείται ένας αμυντικός μηχανισμός για μικροδίκτυα απέναντι σε επιθέσεις FDI και DoS, καθώς και συνδυασμό αυτών που βασίζεται στη συνεργασία δύο στρωμάτων ελέγχου. Το πρώτο είναι υπεύθυνο για τον τυπικό κατανεμημένο έλεγχο οπότε μόνο του είναι γρήγορο αλλά ευάλωτο στις επιθέσεις και το δεύτερο στρώμα είναι ασφαλές αλλά πιο αργό και είναι υπεύθυνο για την επίβλεψη του πρώτου μέσω εξισώσεων που τα συνδέουν και αποστολή σημάτων αντιστάθμισης σε περίπτωση που δημιουργούνται διαταραχές από επιθέσεις. Το σύστημα αυτό δε διαταράσσει την ομαλή λειτουργία του μικροδικτύου όταν δεν υπάρχουν επιθέσεις καθώς το δεύτερο στρώμα δεν επεμβαίνει και διασφαλίζει τις λειτουργίες της αποκατάστασης συχνότητας και διαμοιρασμού ενεργού ισχύος όταν υπάρχουν.

Στο [85] υλοποιείται ένα σύστημα προστασίας συστημάτων αποθήκευσης ενέργειας σε απομονωμένα μικροδίκτυα απέναντι σε επιθέσεις FDI. Αρχικά, γίνεται επαναληπτική εκτίμηση των

αγνώστων σημάτων επίθεσης ώστε να έχουμε σύγκλιση του σφάλματος στο μηδέν και στη συνέχεια με χρήση μιας βελτιωμένης μορφής του Round-Robin πρωτοκόλλου και εξασφαλίζουμε ότι κάθε στιγμή επικοινωνεί κάθε ESS μόνο με έναν γείτονα και εξασφαλίζουμε τελικά την αμφίδρομη επικοινωνία όλων των κόμβων με τους γείτονές τους. Ο ελεγκτής στον πυρήνα του αμυντικού μηχανισμού, μεταβάλλεται με βάση το χρόνο και οι εξισώσεις ελέγχου του εξαρτώνται από το κέρδος του, το οποίο είναι ρυθμιζόμενο για βελτιστοποίηση του συστήματος ανάλογα με διαφορετικές ρυθμίσεις του συστήματος, διαφορετικά σενάρια επιθέσεων και άλλες παραμέτρους. Με το παραπάνω σύστημα αποδεικνύεται η εξισορρόπηση SoC μεταξύ των ESSs, ο σωστός διαμοιρασμός ισχύος και η δυνατότητα αποκατάστασης της συχνότητας και της τάσης με μείωση του βάρους στις υποδομές επικοινωνίας.

Στο [86] έχουμε υλοποίηση ενός αμυντικού μηχανισμού για απομονωμένα μικροδίκτυα απέναντι σε FDI επιθέσεις, ο οποίος βασίζεται στη χρήση ενός προστατευμένου εικονικού στρώματος το οποίο αλληλεπιδρά με το πραγματικό σύστημα μέσω ειδικά σχεδιασμένων πινάκων. Το στρώμα αυτό επιτυγχάνει συγχρονισμό της συχνότητας στο δίκτυο ακόμα και αν όλοι οι κόμβοι του πραγματικού συστήματος δέχονται επίθεση και είναι καλύτερο από observer-based μηχανισμούς, καθώς όπως είπαμε δε χρειάζεται ένα υποσύνολο των κόμβων να είναι ασφαλείς. Τέλος, η ανθεκτικότητα του μηχανισμού αλλά και το υπολογιστικό κόστος αυξάνονται αναλογικά με την αύξηση της ρυθμιζόμενης παραμέτρου α γεγονός που προσφέρει παραπάνω ελευθερία προσαρμογής της άμυνας στις απαιτήσεις και στο μέγεθος της επίθεσης.

Στο [99] παρουσιάζεται ένας αμυντικός μηχανισμός για την προστασία μικροδικτύων, που λειτουργούν στην απομονωμένη κατάσταση, απέναντι σε DoS επιθέσεις. Χρησιμοποιείται κατανεμημένη στρατηγική ελέγχου, που αντί για συνεχή επικοινωνία μεταξύ των επιμέρους κατανεμημένων κόμβων και αποστολή ολόκληρης της ποσότητας πληροφορίας, χρησιμοποιεί διακριτή επικοινωνία ανταλλάσοντας μια απλοποιημένη μορφή των απαραίτητων δεδομένων χρησιμοποιώντας πεπερασμένο αριθμό bits μειώνοντας έτσι το επικοινωνιακό φορτίο. Επιπλέον, διακρίνει τη στρατηγική της επικοινωνίας πρώτον, στις περιπτώσεις που έχουμε ενεργή επίθεση DoS κατά τις οποίες οι κόμβοι επιχειρούν να επικοινωνήσουν περιοδικά και δεύτερον, όταν η επίθεση δεν είναι ενεργή, ακολουθείται μια event-triggered στρατηγική που ενεργοποιεί την επικοινωνία όποτε η κατάσταση ενός κόμβου έχει αλλάξει σημαντικά από την τελευταία του μετάδοση δεδομένων. Το κατώφλι που πρέπει να ξεπεραστεί, για να κριθεί “σημαντική” αυτή η αλλαγή, μικραίνει με την πάροδο του χρόνου ώστε να είναι πιο πιθανή η ενεργοποίηση της επικοινωνίας όσο το χρονικό διάστημα από την τελευταία φορά, που ήταν ενεργή, μεγαλώνει. Το αμυντικό σύστημα εγγυάται τη σύγκλιση της συχνότητας και της τάσης στις επιθυμητές τιμές και το βέλτιστο διαμοιρασμό ισχύος ενώ ταυτόχρονα μειώνει σημαντικά το βάρος στην επικοινωνία.

Στο [87] υλοποιείται ένας αμυντικός μηχανισμός για απομονωμένα συμπλέγματα μικροδικτύων που ακολουθούν Lyapunov-based συνεργατική στρατηγική ελέγχου απέναντι σε FDI επιθέσεις. Επιτυγχάνει ρύθμιση της τάσης και ακριβή διαμοιρασμό ισχύος ακόμα και κατά τη διάρκεια των επιθέσεων, βασίζοντας τη λειτουργία του αποκλειστικά σε τοπικές παραμέτρους των μικροδικτύων κάνοντας τον επεκτάσιμο ενώ ταυτόχρονα δε χρειάζεται πλήρη γνώση των μοντέλων του μικροδικτύων που προστατεύει.

Στο [88] παρουσιάζεται ένα σύστημα προστασίας απομονωμένων μικροδικτύων απέναντι ακόμα και σε ταυτόχρονη διεξαγωγή FDI και DoS επιθέσεων. Με τη χρήση κατανεμημένου παρατηρητή, που προσαρμόζει τη λειτουργία του με βάση το αν είναι ενεργή ή όχι η DoS επίθεση, γίνεται εκτίμηση της κατάστασης και του σήματος επίθεσης και με χρήση αυτών των στοιχείων από έναν κεντρικό ελεγκτή, δίνονται τα απαραίτητα σήματα αντιστάθμισης για την αντιμετώπιση των αποκλίσεων της συχνότητας σε worse-case scenario (H∞), εξαιτίας της FDI επίθεσης. Σε περίπτωση που η DoS επίθεση είναι ενεργή, χρησιμοποιούνται μόνο οι εκτιμήσεις των παρατηρητών τοπικά στις εξισώσεις ελέγχου, ενώ αν δεν είναι ενεργή, κάθε κατανεμημένος κόμβος λαμβάνει υπόψη του κανονικά ως είσοδο το σήμα που αποστέλλει ο κεντρικός ελεγκτής.

Στο [89] έχουμε υλοποίηση ενός αμυντικού μηχανισμού που προστατεύει απομονωμένα μικροδίκτυα απέναντι σε υβριδικές επιθέσεις που συνδυάζουν FDI με DoS. Αρχικά, κατανεμημένοι παρατηρητές χρησιμοποιούν μια επαναληπτική διαδικασία για τον προσδιορισμό των καταστάσεων της τάσης και της συχνότητας και των σημάτων των FDI επιθέσεων, με τα σφάλματα εκτίμησης να συγκλίνουν ασυμπτωτικά στο μηδέν, όταν το πλήθος των επαναλήψεων τείνει στο άπειρο και όσο οι ενεργές DoS επιθέσεις έχουν φραγμένη διάρκεια. Στη συνέχεια, χρησιμοποιείται από τον κατανεμημένο ελεγκτή ο μέσος όρος των εκτιμήσεων των FDI σημάτων για την παραγωγή των απαραίτητων σημάτων αντιστάθμισης και εξασφαλίζει πως τα σφάλματα της ρύθμισης της τάσης και της συχνότητας συγκλίνουν στο μηδέν. Τέλος, αξίζει να αναφερθεί ότι το σύστημα θεωρεί πως γνωρίζει από την αρχή τα χρονικά διαστήματα των DoS επιθέσεων και το υποσύνολο των συνδέσμων επικοινωνίας που πλήττονται κάθε φορά, ώστε να μπορεί να μηδενίσει μια μεταβλητή που κρίνει έναν σύνδεσμο ως σπασμένο, κάθε φορά που υπάρχει ενεργή DoS επίθεση σε αυτόν.

Στο [90] παρουσιάζεται μια περίπτωση συστήματος προστασίας απομονωμένων μικροδικτύων απέναντι σε FDI επιθέσεις που βασίζεται σε μια βελτιωμένη εκδοχή του Weighted Mean Subsequence Reduced (WMSR) αλγορίθμου για την απόρριψη, από κάθε κόμβο, των r πιο ακραίων μετρήσεων που έλαβε από τους γείτονές του σε αντίθεση με τον κλασικό αλγόριθμο που απορρίπτει 2r. Ο μηχανισμός εγγυάται τη σωστή κατανεμημένη οικονομική λειτουργία και την ανθεκτικότητα των μικροδικτύων, στην περίπτωση που ο κάθε κόμβος τους έχει τουλάχιστον r+1 γείτονες, χωρίς να χρειάζεται να γνωρίζει και να απομονώνει τους μη ασφαλείς κόμβους.

Στο [100] υλοποιείται ένας αμυντικός μηχανισμός προστασίας συνδεδεμένων μεταξύ τους AC/DC μικροδικτύων, τα οποία είναι απομονωμένα από το κύριο δίκτυο, απέναντι σε DoS επιθέσεις. Χρησιμοποιείται κατανεμημένος event-triggered έλεγχος που ενεργοποιεί την επικοινωνία μεταξύ δύο μικροδικτύων μόνο όταν η διαφορά της τωρινής κατάστασης και της τελευταίας κατάστασης που μετάδωσε, είναι μεγαλύτερη από ένα δυναμικά μεταβαλλόμενο κατώφλι και εγγυάται έτσι τον ακριβή διαμοιρασμό ισχύος και την αποκατάσταση της συχνότητας και της τάσης όταν το σύστημα δέχεται κάποια DoS επίθεση. Για να εκτιμήσει τις τιμές των μεταβλητών ελέγχου που δεν είναι δυνατό να μεταδοθούν κατά τη διάρκεια των επιθέσεων, το σύστημα χρησιμοποιεί ένα model-free σύστημα πρόβλεψης που βασίζεται πάνω σε ιστορικά δεδομένα εισόδων και εξόδων διατηρώντας την ευστάθεια όταν η επικοινωνία δεν είναι δυνατή.

Στο [91] παρουσιάζεται ένα σύστημα προστασίας απομονωμένων μικροδικτύων απέναντι σε FDI επιθέσεις που στοχοποιούν αισθητήρες, ενεργοποιητές, τιμές αναφοράς στον δευτερογενή κατανεμημένο ελεγκτή και παραμέτρους που ανταλλάσσονται μέσω των διαύλων επικοινωνίας. Χρησιμοποιεί ένα ασφαλές εικονικό στρώμα του οποίο η κατάσταση εξελίσσεται δυναμικά με βάση το τι συμβαίνει στο πραγματικό δίκτυο και μεταβάλει τον κανόνα ελέγχου αποστέλλοντας ένα σήμα αντιστάθμισης, για να εξουδετερώσει τις επιπτώσεις των επιθέσεων. Δε χρειάζεται ανίχνευση της εισβολής και το σύστημα προστατεύει τις λειτουργίες της αποκατάστασης της συχνότητας και του διαμοιρασμού ισχύος ακόμα και όταν όλοι οι κόμβοι με τους αντιστροφείς δέχονται επίθεση. Τέλος, αξίζει να αναφερθεί πως αυτό το εικονικό στρώμα αλληλεπιδρά με το μικροδίκτυο με κάποιους ειδικά σχεδιασμένους πίνακες για να εξασφαλίσει ασυμπτωτική ευστάθεια.

Στο [101] έχουμε υλοποίηση ενός αμυντικού μηχανισμού που προστατεύει απομονωμένα μικροδίκτυα εναντίον τυχαίων DoS επιθέσεων, οι οποίες διακόπτουν κάθε φορά την επικοινωνία μεταξύ του κεντρικού ελεγκτή και ενός υποσυνόλου των τοπικών ελεγκτών. Χρησιμοποιείται ένα Μαρκοβιανό γραμμικό σύστημα με άλματα για τη μοντελοποίηση του δικτύου με απότομες αλλαγές της δυναμικής του συστήματος όποτε αλλάζει η επίθεση και διακόπτει την επικοινωνία κάποιου άλλου υποσυνόλου τοπικών ελεγκτών με τον κεντρικό. Ανάλογα με την κατάσταση του πίνακα που περιγράφει ποιοι δίαυλοι επικοινωνίας είναι ενεργοί, ο κεντρικός ελεγκτής προσαρμόζει και το κέρδος του. Επιπλέον, ο αμυντικός μηχανισμός χρησιμοποιεί ένα δείκτη ευπάθειας για την ποσοτικοποίηση των επιπτώσεων των επιθέσεων στο σύστημα. Αποδεικνύεται τελικά, ότι το σύστημα άμυνας καταφέρνει να διατηρήσει τη συχνότητα και την τάση σε επιθυμητές τιμές και την ευστάθεια ισχύος στο μικροδίκτυο.

Στο [102] παρουσιάζεται ένας ιεραρχικός έλεγχος ασφάλειας που εστιάζει σε μικροδίκτυα για την αντιμετώπιση DoS επιθέσεων. Χρησιμοποιεί κατανεμημένους τοπικούς εκτιμητές για τον υπολογισμό φράγματος για την παράγωγο της μεταβαλλόμενης στο χρόνο τιμής αναφοράς της

ενεργού και της άεργου ισχύος και κατανεμημένους παρατηρητές για την αλλαγή μεταξύ κανονικής λειτουργίας και λειτουργίας υπό την επίδραση επίθεσης με βάση τη δυνατότητα επικοινωνίας. Επιπλέον, σχεδιάζονται αποκεντρωμένοι ελεγκτές βασισμένοι στη μέθοδο block backstepping για τους σωστούς υπολογισμούς των τιμών αναφοράς χωρίς ανάγκη για επικοινωνία. Το σύστημα εγγυάται ότι τα σφάλματα συγκλίνουν ασυμπτωτικά στο μηδέν όταν η επίθεση DoS είναι πεπερασμένη και ότι τα σφάλματα παραμένουν ομοιόμορφα φραγμένα σε ένα συμπαγές σύνολο όταν η επίθεση επιμένει.

Στο [103] υλοποιείται ένας αμυντικός μηχανισμός που βασίζεται σε self-triggered έλεγχο και εφαρμόζεται σε ένα δίκτυο που ο κάθε κόμβος είναι ένα διαφορετικό μικροδίκτυο. Η επικοινωνία του συστήματος μπορεί να επηρεάζεται από DoS επιθέσεις ταυτόχρονα σε διάφορα σημεία, όπως είναι, η επικοινωνία μεταξύ των κεντρικών ελεγκτών των επιμέρους μικροδικτύων, η επικοινωνία αισθητήρων κατανεμημένων ενεργειακών πόρων με τον ελεγκτή του κάθε μικροδικτύου εσωτερικά και η επικοινωνία των ενεργοποιητών με τον ελεγκτή του κάθε μικροδικτύου. Επιπλεόν, χρησιμοποιείται η έννοια της διατηρησιμότητας της ροής δεδομένων για την ποσοτικοποίηση της μη διαθεσιμότητας δεδομένων συνολικά στα πολλαπλά στρώματα επικοινωνίας. Ο κατανεμημένος έλεγχος είναι ασύγχρονος επιτρέπει στα μικροδίκτυα να ενημερώνουν μόνα τους και ανεξάρτητα τα σήματα ελέγχου με βάση τοπικά ρολόγια και ανάλογα με τον κάθε διαφορετικό γείτονά τους. Ακόμα, ο έλεγχος προσαρμόζει δυναμικά παραμέτρους ελέγχου όπως ο ρυθμός ενημέρωσης με βάση τους χρόνους των τελευταίων επιτυχημένων ανταλλαγών δεδομένων βελτιώνοντας τις περιπτώσεις των χειρότερων σεναρίων. Τέλος, ο τύπος της αντιμετώπισης των επιπτώσεων εξαρτάται από το αν η επίθεση μπορεί να αναγνωριστεί όπως αυτή μεταξύ αισθητήρων και τοπικού ελεγκτή, ή όχι όπως η επικοινωνία που σχετίζεται με τους ενεργοποιητές μετά την αποστολή του σήματος από τον τοπικό ελεγκτή. Το σύστημα εξασφαλίζει ομοφωνία ως προς τη συχνότητα και τον διαμοιρασμό ισχύος και βελτιώνει τα αποτελέσματα στα χειρότερα σενάρια συγκριτικά με άλλες ανθεκτικές, απέναντι σε DoS, στρατηγικές.

Στο [95] υλοποιείται ένας μηχανισμός προστασίας μικροδικτύων με αντιστροφείς απέναντι σε μη φραγμένες επιθέσεις, που χρησιμοποιεί πλήρως κατανεμημένο έλεγχο. Συναντάται, για άλλη μια φορά, η χρήση ενός εικονικού στρώματος το οποίο είναι προστατευμένο από επιθέσεις και υπολογίζει σήματα αντιστάθμισης για την αντιμετώπιση των επιπτώσεων των επιθέσεων τα οποία τα αποστέλλει στο πραγματικό δίκτυο μέσω ασφαλών καναλιών. Το αμυντικό σύστημα εξασφαλίζει τον κατανεμημένο δευτερογενή έλεγχο, απομονώνοντας ουσιαστικά την επίδραση των επιθέσεων στη λειτουργία αποκατάστασης της συχνότητας και της τάσης.

Στον Πίνακα 4.2, γίνεται μια συνοπτική παρουσίαση των αμυντικών μηχανισμών των παραπάνω περιπτώσεων στο επίπεδο του δευτερογενούς ελέγχου, τονίζοντας τα πιο σημαντικά

χαρακτηριστικά τους.

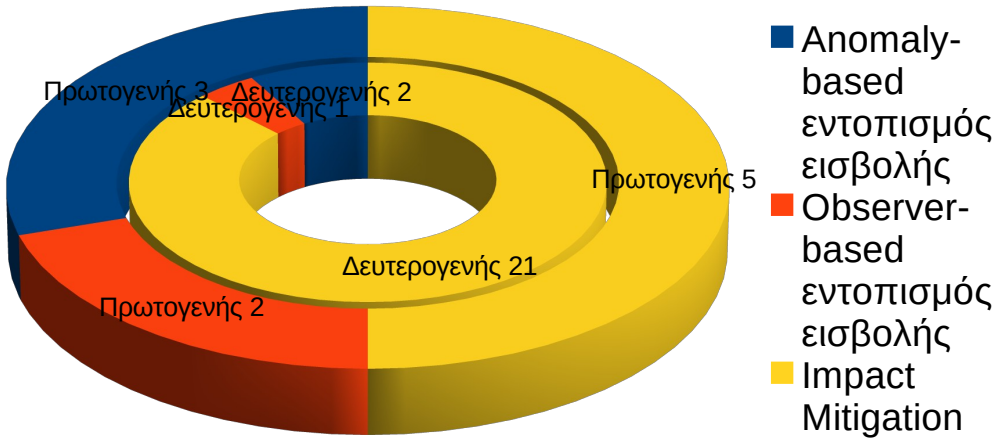
Τέλος, παρουσιάζουμε στο Σχ.4.2 μια ποσοτική απεικόνιση των αμυντικών μηχανισμών του συνόλου της βιβλιογραφίας, που μελετήθηκε με τις επιμέρους κατηγορίες τους

Ref	*Κατηγορία επίθεσης*	*Αδυναμία μικροδικτύου*	*Στρατηγική επίλυσης του προβλήματος άμυνας*	*Κατηγορία αμυντικής στρατηγικής*	*Μέθοδος και στόχος αμυντικής διαδικασίας*
[96]	DoS	Δίαυλοι επικοινωνίας συγκεκριμένα στο κοινό σημείο σύζευξης	Resilient event-triggered έλεγχος	Μετριασμός επιπτώσεων	Ορισμός επιθυμητού συντελεστή ενεργού ισχύος Ρύθμιση χωρητικότητας υπολοίπου του κάθε grid-tied αντιστροφέα ξεχωριστά Εκτίμηση συνολικής χωρητικότητας υπολοίπου στον κάθε αντιστροφέα Ρύθμιση της τιμής αναφοράς του ρεύματος αντιστάθμισης κάθε αντιστροφέα Αντιμετώπιση DoS επιθέσεων με στόχο τη βελτίωση της ποιότητας της ισχύος
[97]	Time-varying latency και DoS	Δίκτυο επικοινωνίας κόμβων	Resilient έλεγχος απέναντι σε κυβερνοεπιθέσεις με δύο λειτουργίες: Ελεγκτής προσαρμοζόμενου κέρδους και, Event-triggered ελεγκτής αναδιαμόρφωσης της τοπολογίας του μικροδικτύου	Μετριασμός επιπτώσεων	1)Αλγόριθμος resilient ελέγχου με προσαρμοζόμενο κέρδος και 2)αλγόριθμος αναδιαμόρφωσης της τοπολογίας του δικτύου. Το σύστημα περνάει από τον πρώτο αλγόριθμο στο δεύτερο άμα παραβιαστεί η συνθήκη ευστάθειας που έχει τεθεί και ικανοποιηθεί η συνθήκη event-trigger Όσο το δυνατόν ταχύτερη σταθεροποίηση του συστήματος κατά τη διάρκεια που δέχεται επιθέσεις χρονικών καθυστερήσεων και αναδιαμόρφωση της τοπολογίας του δικτύου στην περίπτωση που οι ζημιές είναι υπέρμετρες και κρίνεται απαραίτητο
[83]	FDI	Αισθητήρες-ενεργοποιητές	Observer-based resilient πλήρως κατανεμημένος έλεγχος συχνότητας	Μετριασμός επιπτώσεων	Μείωση των επιπτώσεων άγνωστων ποσοτικά επιθέσεων FDI σε αισθητήρες και ενεργοποιητές. Απαραίτητη η δημιουργία άνω και κάτω φραγμάτων στο σφάλμα των παρατηρητών για την εκτίμηση της συχνότητας γεγονός που επιτυγχάνεται με τη στρατηγική που ακολουθείται
[98]	DoS	Δίκτυο επικοινωνίας κόμβων	Μετατροπή ενός κυβερνοφυσικού συστήματος σε αμιγώς φυσικό υποβαθμίζοντας τις διαταραχές από τις DoS επιθέσεις στο να είναι ισάξιες με τις διαφοροποιήσεις των παραμέτρων του νέου φυσικού μοντέλου	Μετριασμός επιπτώσεων	Εύρεση ενός feasible point στο σύστημα παρά τις διαταραχές που προκαλούν οι DoS επιθέσεις οι οποίες μπορούν να κυμαίνονται από αποκλίσεις παραμέτρων όπως η συχνότητα από τις επιθυμητές τιμές, μέχρι και διακοπή λειτουργίας του δικτύου
[84]	FDI, DoS	Κατανεμημένοι ενεργειακοί πόροι και δίκτυο επικοινωνίας	Resilient έλεγχος πολλών στρωμάτων με διαφορετικές λειτουργίες και αδυναμίες κάτι που καθιστά ισχυρή τη συνεργασία τους	Μετριασμός επιπτώσεων	Το σημείο ισορροπίας του δικτύου είναι κατά τη διάρκεια των FDI επιθέσεων ασυμπτωτικά ευσταθές. Επίσης, κατά τις DoS επιθέσεις αποδεικνύεται η ευστάθεια κατά Lyapunov
[85]	FDI	Ενεργοποιητές ESS	Κατανεμημένος έλεγχος που εισάγει ένα κέρδος για τα ESS το οποίο ποικίλει με βάση το χρόνο. Επαναληπτική observer-based εκτίμηση με χρήση βελτιωμένου Round Robin αλγόριθμου	Μετριασμός επιπτώσεων	Επαναληπτική εκτίμηση των αγνώστων σημάτων επίθεσης. Το βελτιωμένο πρωτοκόλλο Round-Robin μειώνει το βάρος στην επικοινωνία εξασφαλίζοντας την αμφίδρομη επικοινωνία των γειτονικών ESS μέχρι το πέρας του. Το κέρδος του ελεγκτή είναι ρυθμιζόμενο για την επεκτασιμότητα του μηχανισμού Εξισορρόπηση SoC μεταξύ των ESSs, σωστός διαμοιρασμός ισχύος και δυνατότητα αποκατάστασης της συχνότητας και της τάσης
[86]	FDI	Αισθητήρες-Ενεργοποιητές, Δίαυλοι	Resilient κατανεμημένος έλεγχος με τη χρήση ενός επιπλέον κρυμμένου εικονικού	Μετριασμός επιπτώσεων	Με την προσθήκη του κρυμμένου εικονικού στρώματος που έχει τη δική του εσωτερική κατάσταση και συνδέεται με το πραγματικό σύστημα μέσω ειδικά φτιαγμένων πινάκων και την προσαρμογή των σχέσεων ελέγχου του συστήματος για να συμπεριλάβουμε αυτό το στρώμα, επιτυγχάνεται συγχρονισμός συχνότητας ακόμα και υπό την παρουσία επιθέσεων

		επικοινωνίας	στρώματος (hidden layer)		που αλλοιώνουν τις παραμέτρους του πραγματικού συστήματος. Η βέλτιστη λειτουργία αυτού του επιπλέον στρώματος εξαρτάται από την επιλογή κατάλληλων πινάκων και ειδικά από την επιλογή ικανά μεγάλης τιμής του κέρδους του α.
[99]	DoS	Δίαυλοι επικοινωνίας	Resilient event-triggered διακριτού χρόνου κατανεμημένος έλεγχος	Μετριασμός επιπτώσεων	Έχοντας επικοινωνία μεταξύ των κόμβων του μικροδικτύου και μεταφορά κβαντισμένων δεδομένων μόνο συγκεκριμένες στιγμές, οι οποίες καθορίζονται από την ικανοποίηση κάποιας συνθήκης, μειώνεται ο χρόνος επικοινωνίας άρα και η αδυναμία του συστήματος απέναντι σε DoS επιθέσεις. Κατά τις διακοπές επικοινωνίας έχουμε χρήση αποθηκευμένων δεδομένων και ενός μηχανισμού πρόβλεψης για την διατήρηση ευστάθειας. Δεδομένων κάποιων φραγμάτων στη συχνότητα και διάρκεια των επιθέσεων, έχουμε διατήρηση της ευστάθειας. Η επικοινωνία μεταξύ των κόμβων ενεργοποιείται είτε όταν η διαφορά της προηγούμενης κατάστασης που μεταδόθηκε με την τωρινή είναι μεγαλύτερη από ένα φθίνον κατώφλι, είτε μετά από έναν ελάχιστο χρόνο αναμονής
[87]	FDI	Μονάδα ελέγχου	Lyapunov-based resilient συνεργατικός έλεγχος	Μετριασμός επιπτώσεων	Έχουμε προστασία DC συμπλεγμάτων μικροδικτύων που λειτουργούν χωρίς τη βοήθεια του κυρίως δικτύου χωρίς να χρειάζεται ανίχνευση και απομόνωση της επίθεσης οδηγώντας το σύστημα σε ασυμπτωτική ευστάθεια και διατηρεί ομαλές τις λειτουργίες ρύθμισης της τάσης και διαμοιρασμού της ισχύος. Πολύ θετικό το χαρακτηριστικό της επεκτασιμότητας και η ανθεκτικότητα του απέναντι σε αβεβαιότητες για τη μοντελοποίηση των μικροδικτύων.
[88]	FDI, DoS	Αισθητήρες-Ενεργοποιητές, Δίαυλοι επικοινωνίας	Resilient observer-based κατανεμημένος έλεγχος	Μετριασμός επιπτώσεων	Με τη βοήθεια του εκπαιδευόμενου παρατηρητή έχουμε εκτίμηση ταυτόχρονα και της πραγματικής κατάστασης του συστήματος και του FDI σήματος επίθεσης είτε βρισκόμαστε στο χρονικό διάστημα επίθεσης DoS είτε όχι. Όταν δεν έχουμε επικοινωνία μεταξύ των κόμβων, ο παρατηρητής χρησιμοποιεί αποθηκευμένες τιμές παλαιότερων καταστάσεων, ενώ όταν η επικοινωνία είναι ενεργή, έχουμε ανανέωση των καταστάσεων των κόμβων που επικοινωνούν. Αυτές οι εκτιμήσεις χρησιμοποιούνται από τον νόμο ελέγχου του ελεγκτή ώστε να διατηρηθεί η ευστάθεια στο σύστημα
[89]	Υβριδικές επιθέσεις (FDI + DoS)	Αισθητήρες-Ενεργοποιητές, Δίαυλοι επικοινωνίας	Resilient estimator-based κατανεμημένος έλεγχος	Μετριασμός επιπτώσεων	Με τη χρήση ενός k-step εκτιμητή ο οποίος ανανεώνει επαναληπτικά τις εκτιμήσεις των καταστάσεων του συστήματος και των FDI σημάτων επίθεσης, έχουμε μετριασμό των ανακριβειών που οφείλονται στην απώλεια επικοινωνίας ανά διαστήματα λόγω των DoS επιθέσεων οι οποίες ανακρίβειες συγκλίνουν προς το μηδέν όσο αυξάνονται οι επαναλήψεις. Ο ελεγκτής με τη χρήση αυτών των εκτιμήσεων, αποζημιώνει το σύστημα για τις FDI επιθέσεις και βοηθάει στη διατήρηση της ευστάθειας.
[90]	FDI	Αισθητήρες-Ενεργοποιητές	Resilient consensus-based (modified WSMR) κατανεμημένος έλεγχος	Μετριασμός επιπτώσεων	Έχουμε χρήση μιας βελτιωμένης έκδοσης του αλγορίθμου Weighted Mean Subsequence Reduced (WMSR) στο consensus σύστημα που χρησιμοποιείται, με διαγραφή των σ μέγιστων και ελαχίστων τιμών που μεταδίδονται μεταξύ των κόμβων που επικοινωνούν στο μικροδίκτυο. Στη συνέχεια οι τιμές που μένουν χρησιμοποιούνται για την ενημέρωση της καινούριας κατάστασης του κάθε κόμβου ακολουθώντας ένα consensus πρωτόκολλο για τη διατήρηση της ευστάθειας στο σύστημα.
[100]	DoS	Δίαυλοι επικοινωνίας	Event-triggered κατανεμημένος έλεγχος με model-free predictive αλγόριθμο αντιστάθμισης	Μετριασμός επιπτώσεων	Η επικοινωνία μεταξύ κόμβων είναι ενεργή μόνο όταν η απόκλιση μεταξύ τωρινής και προηγούμενης κατάστασης ενός κόμβου ξεπερνά ένα προκαθορισμένο κατώφλι. Κατά τη διάρκεια των επιθέσεων DoS, χρησιμοποιείται ο αλγόριθμος πρόβλεψης κατάστασης που βασίζεται στη χρήση τιμών που είχαν μεταδοθεί μεταξύ κόμβων στο παρελθόν. Έχουμε βελτιώσεις στο διαμοιρασμό ισχύος, μείωση των αποκλίσεων συχνότητας και τάσης από τις επιθυμητές τιμές και του επικοινωνιακού βάρους κατά την αντιμετώπιση DoS επιθέσεων.
[91]	State-dependent FDI	Αισθητήρες-Ενεργοποιητές, Δίαυλοι επικοινωνίας, Μονάδα ελέγχου	Resilient consensus-based συνεργατικός κατανεμημένος έλεγχος με χρήση εικονικού στρώματος	Μετριασμός επιπτώσεων	Έχουμε βελτίωση ενός συνηθισμένου consensus-based συστήματος ελέγχου με την προσθήκη ενός εικονικού στρώματος με τη δική του εσωτερική κατάσταση το οποίο δε μπορεί να γίνει στόχος επίθεσης και γι' αυτό αποτελεί ένα ασφαλές σύστημα αναφοράς για τη διόρθωση της κατάστασης του πραγματικού συστήματος. Η διόρθωση αυτή έρχεται με αλλαγή του νόμου ελέγχου κατά μια τιμή ώστε να αντιμετωπιστεί το σήμα επίθεσης χωρίς να χρειάζεται να εντοπισθεί ποιοι κόμβοι του συστήματος δέχονται επίθεση. Μέσω αυτού του συστήματος άμυνας, έχουμε ευστάθεια συχνότητας και σωστό διαμοιρασμό ενεργού ισχύος.
[101]	Τυχαίες DoS	Δίαυλοι επικοινωνίας	Resilient frequency regulation χρησιμοποιώντας Μαρκοβιανό γραμμικό σύστημα με άλματα για τη μοντελοποίηση του μικροδικτύου	Μετριασμός επιπτώσεων	Το σύστημα χρησιμοποιεί ένα μαθηματικό μοντέλο που λέγεται Markovian jump linear system για την σωστή απεικόνιση του μικροδικτύου μετά τις αλλαγές που προκαλούνται στην επικοινωνία των διαφόρων κόμβων κάθε στιγμή εξαιτίας των τυχαίων DoS επιθέσεων. Ο δευτερογενής ελεγκτής προσαρμόζει τις τιμές των παραμέτρων του όπως το κέρδος του, ανάλογα με τη μορφή της DoS επίθεσης που δέχεται το σύστημα κάθε φορά, οδηγώντας στη μείωση του πλάτους ταλάντωσης της συχνότητας, της τάσης και της ενεργού ισχύος που προκαλούνται από τις τυχαίες επιθέσεις DoS. Το σύστημα διατηρεί την ευστάθεια του.

[92]	FDI	Ελεγκτής κατανεμημένου ενεργειακού πόρου	Resilient κατανεμημένος έλεγχος με self-belief factors Anomaly-based IDS	Εντοπισμός εισβολής και μετριασμός επιπτώσεων	Το σύστημα χρησιμοποιεί τη μέθοδο της Kullback-Leibler απόκλισης για να εντοπίσει μια επίθεση που σημαίνει ότι κάθε κόμβος συγκρίνει την κατανομή των σφαλμάτων συχνότητας και τάσης που δέχεται από τους γείτονές του με την κατανομή που θα έπρεπε να ακολουθούν και αν η διαφορά υπερβαίνει ένα κατώφλι, τότε το σύστημα δέχεται επίθεση. Ο παράγοντας εμπιστοσύνης καθορίζεται από τη μέθοδο KL και ο νόμος ελέγχου διαμορφώνεται με βάση το ποιοι κόμβοι έχουν υψηλούς παράγοντες, αγνοώντας τα δεδομένα που έρχονται από αυτούς με χαμηλούς παράγοντες. Έτσι διατηρείται η ευστάθεια ακόμα και υπό κρυφίων, επίμονων επιθέσεων.
[93]	FDI	Δίαυλοι επικοινωνίας, Κατανεμημένη μονάδα παραγωγής	Resilient κατανεμημένος observer-based έλεγχος καθορισμένου χρόνου Observer-based IDS	Εντοπισμός εισβολής και μετριασμός επιπτώσεων	Το σύστημα χρησιμοποιεί confidence και trust factors για τον εντοπισμό επιθέσεων και την αναγνώριση των εκτεθειμένων κόμβων αγνοώντας τα δεδομένα που στέλνουν. Έτσι, εγγυάται το σύστημα το ότι η συχνότητα και η τάση θα συγκλίνουν στις επιθυμητές τιμές σε πεπερασμένο χρονικό διάστημα, ακόμα και κατά τη διάρκεια επιθέσεων.
[94]	FDI Control input Load deviation	Αισθητήρες-Ενεργοποιητές, Φορτία του μικροδικτύου	Resilient model-free κεντρικός έλεγχος με κατανεμημένους detectors Anomaly-based IDS	Εντοπισμός εισβολής και μετριασμός επιπτώσεων	Χρησιμοποιείται η μέθοδος αναγνώρισης υποχώρου ώστε να μπορεί ο αμυντικός μηχανισμός να εντοπίσει τις απειλές και σε μικροδίκτυα που δεν έχουμε πλήρη γνώση της αρχιτεκτονικής τους. Αυτή η μέθοδος βασίζεται στη χρήση εισόδων και εξόδων του συστήματος ως δεδομένα για να μοντελοποιήσει το μικροδίκτυο. Χρησιμοποιείται μια τεχνική ανίχνευσης υπολοίπου μέσω της σύγκρισης της επιθυμητής κατάστασης του δικτύου και της πραγματικής. Αν ξεπερνάει κάποια τιμή το υπόλοιπο, τότε αντιμετωπίζουμε επίθεση και απομονώνουμε το εκτεθειμένο μέρος του δικτύου για την αποφυγή κλιμάκωσης και τη διατήρηση της ευστάθειας του συστήματος.
[102]	DoS	Δίαυλοι επικοινωνίας	Συνδυασμός αποκεντρωμένου ελέγχου με resilient κατανεμημένους παρατηρητές και εκτιμητές	Μετριασμός επιπτώσεων	Ο παρατηρητής διατηρεί τις τιμές αναφοράς της ενεργού και άεργου ισχύος στα επιθυμητά επίπεδα τα οποία καθορίζονται από τον εκτιμητή χωρίς να είναι απαραίτητη η συνεχής ροή δεδομένων μεταξύ των κατανεμημένων κόμβων (ιδιαίτερα χρήσιμο απέναντι σε επιθέσεις DoS). Ακόμα και σε περίπτωση που οι DoS επιμένουν, τα σφάλματα στις τιμές που παρακολουθούνται, παραμένουν περιορισμένες σε ένα αρκετά μικρό σύνολο τιμών. Το σύστημα εγγυάται την σωστή κατανομή ισχύος ανάμεσα στους κόμβους του μικροδικτύου.
[103]	DoS	Αισθητήρες-Ενεργοποιητές στο κάθε μικροδίκτυου, Δίαυλοι επικοινωνίας μεταξύ μικροδικτύων	Resilient self-triggered κατανεμημένος έλεγχος	Μετριασμός επιπτώσεων	Χρησιμοποιείται μια κοινή για όλο το δίκτυο παράμετρος για να είναι γνωστό αν κάθε στιγμή μπορεί να υπάρξει ομοφωνία παρά τις επιθέσεις. Κάθε κατανεμημένο μικροδίκτυο χρησιμοποιεί ασύγχρονη επικοινωνία με τα γειτονικά του μικροδίκτυα, μειώνοντας την εξάρτηση από τη συνεχή επικοινωνία μεταξύ τους και χρησιμοποιούνται χρονικές σημάνσεις για την αναγνώριση των στιγμών που η επικοινωνία ήταν επιτυχής. <u>DoS στην επικοινωνία μεταξύ μικροδικτύων και στην προώθηση μετρήσεων από τους αισθητήρες στον τοπικό ελεγκτή</u>: Καθυστερήσεις στις ενημερώσεις στον έλεγχο ώστε να μην έχουμε ενέργειες βασισμένες σε λανθασμένες ή παλιότερες εισόδους και διορθώσεις σε καθολικές παραμέτρους όπως σταθερές σχετικές με τους χρονικά διαστήματα συγχρονισμού. <u>DoS στην επικοινωνία μεταξύ ενεργοποιητή και κατανεμημένου ενεργειακού πόρου:</u> Προσάπτεται κάποια τιμή που ρυθμίζει την “ένταση” την εντολής που δίνεται, ώστε να έχουμε μικρότερες επιπτώσεις στην περίπτωση που δεν εφαρμοστεί σωστά και το σύστημα θεωρεί μέγιστη την καθυστέρηση στη διαδικασία της μεταφοράς της εντολής στον κατανεμημένο ενεργειακό πόρο ώστε να ελαχιστοποιηθεί η ποσότητα των εντολών που θα δωθούν όσο έχουμε DoS επίθεση. Το σύστημα διατηρεί σωστή κατανομή ισχύος και ρύθμιση της συχνότητας.
[95]	FDI	Δίαυλοι επικοινωνίας, Μονάδες ελέγχου	Resilient κατανεμημένος έλεγχος με τη χρήση εικονικού στρώματος	Μετριασμός επιπτώσεων	Με το εικονικό στρώμα να δρα ως παρατηρής και εκτιμητής ανεξάρτητα του συστήματος που δέχεται την επίθεση έχουμε μεταφορά σημάτων αποζημίωσης για τις επιθέσεις μέσα από κανάλια επικοινωνίας που καθίστανται ασφαλή χάρη σε συγκεκριμένο λογισμικό. Το σύστημα εγγυάται ευστάθεια και συγχρονισμό της συχνότητας και της τάσης με ελάχιστες αποκλίσεις από τις ονομαστικές επιθυμητές τιμές κάτα τη διάρκεια μη φραγμένων FDI επιθέσεων.

Πίνακας 4.2: *Περίληψη αμυντικών μηχανισμών στον δευτερογενή έλεγχο*



Σχήμα 4.2: *Ποσοτική απεικόνιση των αμυντικών μηχανισμών με τις επιμέρους κατηγορίες τους*

Κεφάλαιο 5

Επέκταση της έρευνας και συμπεράσματα

Στο κεφάλαιο αυτό δίνονται κάποιες κατευθύνσεις για συνέχεια της βιβλιογραφικής έρευνας που παρουσιάστηκε καθώς και κάποια τελικά συμπεράσματα, με βάση τη μελέτη και την ανάλυση που έγινε πάνω στην κυβερνοασφάλεια των συστημάτων βασισμένων σε αντιστροφείς με ιδιαίτερη έμφαση στα μικροδίκτυα.

5.1 Συμπεράσματα

Στη διπλωματική αυτή εργασία, πραγματοποιήθηκε εκτενής βιβλιογραφική μελέτη που έγινε πάνω σε τριάντα έξι συγγράμματα για τις επιθέσεις σε δίκτυα βασισμένα σε αντιστροφείς με μια ιδιαίτερη έμφαση σε απομονωμένα μικροδίκτυα και για τους αμυντικούς μηχανισμούς που προτείνονται ανάλογα με την κάθε διαφορετική περίπτωση στα τριάντα από αυτά. Παρατηρούμε και συμπεραίνουμε τη σπουδαιότητα που έχει η προσπάθεια για σφαιρική ανάλυση των συστημάτων και για την προστασία τους απέναντι σε επιθέσεις που διαφοροποιούνται και εξελίσσονται συνεχώς. Ταυτόχρονα τονίζουμε, ειδικά για τα πρώτα στάδια ελέγχου, την ανάγκη να κρατάμε το υπολογιστικό κόστος αυτών των μηχανισμών προστασίας χαμηλό, καθώς συχνά αποτελεί ένα σοβαρό περιορισμό.

Διακρίνουμε λοιπόν τα συμπεράσματά μας μεταξύ αυτών που αναφέρονται στο κομμάτι των επιθέσεων και αυτών που αναφέρονται στο κομμάτι της άμυνας απέναντι σε αυτές.

5.1.1 Επιθέσεις

Αρχικά θα αναφέρουμε τα συμπεράσματα μας με βάση τη μελέτη και την ανάλυση που έγινε πάνω στον τομέα των επιθέσεων που στοχεύουν γενικά το υλικό του αντιστροφέα, με ιδιαίτερη έμφαση στους βρόγχους ελέγχου ρεύματος και τάσης, τον πρωτογενή και τον δευτερογενή έλεγχο. Τα συμπεράσματά μας λοιπόν είναι τα εξής:

1. Το πλήθος των επιθέσεων που παρουσιάζονται και έχουν ως στόχο, κάποιο τμήμα του δευτερογενούς ελέγχου, είναι πολύ μεγαλύτερο από αυτές που στοχεύουν τμήματα πιο κοντά στη βάση του ιεραρχικού ελέγχου, καθώς ο δευτερογενής έλεγχος στην πλειοψηφία των περιπτώσεων που μελετώνται, περιλαμβάνει κάποιο δίκτυο επικοινωνίας. Αυτό δημιουργεί πολλά τρωτά σημεία, όπως τα σήματα ελέγχου που μεταδίδονται από τους ελεγκτές στους κόμβους-πόρους, που είναι βασισμένοι σε αντιστροφείς.
2. Οι επιθέσεις στους βρόγχους ελέγχου του αντιστροφέα και στον πρωτογενή έλεγχο, προκαλούν επιπτώσεις που εμφανίζονται πιο γρήγορα στη λειτουργία του δικτύου, λόγω της ταχύτερης χρονικής κλίμακας γεγονός που δημιουργεί έναν επιπλέον λόγο για ταχύτερο έλεγχο σε πραγματικό χρόνο. Οι επιπτώσεις που εμφανίζονται εξαιτίας

των επιθέσεων στον δευτερογενή έλεγχο, έχουν συχνά μεγαλύτερη διάρκεια, καθώς η πιο αργή φύση του οδηγεί σε πιο αργή αντιμετώπιση τους. Αυτό οξύνεται ακόμα περισσότερο, λόγω του ότι ο δευτερογενής έλεγχος βασίζεται συχνά στην επικοινωνία μεταξύ αποκεντρωμένων ελεγκτών, η οποία στοχοποιείται συχνά από επιθέσεις.

3. Τα προβλήματα που δημιουργούν επιθέσεις στον πρωτογενή και στο υλικό του αντιστροφέα, μπορούν να κλιμακωθούν σε όλο το δίκτυο, σε περισσότερες περιπτώσεις από ότι στον δευτερογενή έλεγχο**.** Για παράδειγμα, στην περίπτωση που ο δευτερογενής έλεγχος είναι κατανεμημένος, η δυνατότητα για διάδοση και κλιμάκωση των προβλημάτων είναι εμφανώς μικρότερη, γεγονός που αλλάζει όταν ο έλεγχος είναι κεντρικός.
4. Οι πιο διαδεδομένες κατηγορίες επιθέσεων είναι οι FDI και οι DoS, με τις πρώτες να έχουν λιγότερες απαιτήσεις για τη διεξαγωγή τους και να είναι πιο καθολικές ως προς την ομάδα των στόχων και των τμημάτων ελέγχου που μπορούν να πλήξουν. Αντίθετα, οι DoS έχουν συχνά περισσότερες απαιτήσεις από τον επιτιθέμενο, όπως η γνώση της τοπολογίας του δικτύου, στοχοποιούν σχεδόν αποκλειστικά τον δευτερογενή έλεγχο λόγω του επικοινωνιακού δικτύου και συχνά χρειάζονται μεγάλη διάρκεια και συχνότητα για να δημιουργήσουν σοβαρά προβλήματα στο δίκτυο.
5. Η συντριπτική πλειοψηφία των επιθέσεων στη βιβλιογραφία είναι δυναμικές και κρυφίες, γεγονός που τους προσφέρει ανθεκτικότητα απέναντι σε κλασικά συστήματα προστασίας των δικτύων και τις κάνει αισθητά λιγότερο ανιχνεύσιμες. Αυτά τα χαρακτηριστικά των επιθέσεων είναι κάποιοι από τους πιο σημαντικούς λόγους δημιουργίας της ανάγκης ολοένα και πιο σύνθετων αμυντικών μηχανισμών.
6. Σε μια προσπάθεια συγκεκριμενοποίησης των λειτουργιών που πλήττονται, καταλήγουμε στις εξής τρεις:
    i. Η αποκατάσταση της συχνότητας και της τάσης
    ii. Ο διαμοιρασμός ισχύος
    iii. Η οικονομική λειτουργία με ανεπιθύμητες μεταβολές σε ενεργειακά προφίλ.

5.1.2 Άμυνα

Η μελέτη αμυντικών μηχανισμών και η βελτίωση τους ειδικά για το μέλλον, αποτελεί όλο και πιο επιτακτική ανάγκη με την πάροδο του χρόνου και την εξέλιξη που βλέπουμε στις δυνατότητες των επιτιθέμενων. Έτσι, οφείλουμε να βγάλουμε συμπεράσματα με βάση τη βιβλιογραφία που αναλύθηκε και να τονίσουμε σημεία που πρέπει να δοθεί ιδιαίτερη έμφαση στο κομμάτι της άμυνας.

1. Στα επίπεδα του ελέγχου μέχρι και τον δευτερογενή έλεγχο, παρατηρούμε την έλλειψη συστημάτων για την πρόληψη εισβολών, παρόλο που είναι εξαιρετικής σημασίας λόγω της ικανότητάς τους να κρατάνε το σύστημα αδιάβλητο, καθώς αυτά τα συστήματα συχνά χρειάζονται εκτενείς υποδομές επικοινωνίας και περισσότερους υπολογιστικούς πόρους για την υλοποίηση τους.
2. Η ανίχνευση μιας εισβολής είναι αισθητά δυσκολότερη στους βρόγχους ελέγχου και στο πρωτογενές επίπεδο, εξαιτίας της ταχύτερης λειτουργίας και της έλλειψης επικοινωνίας, από ότι είναι στο δευτερογενές επίπεδο.
3. Στο κομμάτι της ανίχνευσης εισβολής, είναι πολύ πιο συνήθεις και εμφανίζονται πιο αποδοτικοί οι anomaly-based και observer-based μηχανισμοί σε αντίθεση με τους signature-based, καθώς οι βιβλιοθήκες γνωστών επιθέσεων δεν είναι επαρκείς, λόγω της ταχύτητας με την οποία διαφοροποιούνται οι επιθέσεις και εξελίσσονται με την πάροδο του χρόνου.
4. Είναι πολύ σημαντικό χαρακτηριστικό των αμυντικών μηχανισμών το να είναι model-free, επειδή αυτό αυξάνει την επεκτασιμότητά τους σε συστήματα με διαφορές στα χαρακτηριστικά τους. Παρατηρούμε ότι αυτό το χαρακτηριστικό δεν είναι σύνηθες στη βιβλιογραφία, κυρίως επειδή αυξάνει την πολυπλοκότητα των μηχανισμών.
5. Στο δεύτερο βήμα της άμυνας, αυτό του μετριασμού των επιπτώσεων, παρατηρούνται οι εξής τρεις επικρατούσες στρατηγικές:
    i. Observer-based έλεγχος
    ii. Υλοποίηση virtual layer
    iii. Event-triggered έλεγχος

Αξίζει επίσης να αναφερθεί, πως η τρίτη στρατηγική είναι η επικρατούσα στην άμυνα

απέναντι σε DoS επιθέσεις, καθώς αντιμετωπίζει πολύ εύστοχα τις διακοπές επικοινωνίας μεταξύ κόμβων που προκαλούν αυτές οι επιθέσεις, επειδή σε αυτή τη στρατηγική η επικοινωνία κατά κανόνα χρειάζεται να είναι ενεργή για μικρότερα χρονικά διαστήματα.

6. Στο επίπεδο του υλικού του αντιστροφέα και στον πρωτογενή έλεγχο, είναι ιδιαίτερα σημαντική η παρακολούθηση των συστημάτων σε πραγματικό χρόνο. Αξίζει να τονιστεί η προσοχή που πρέπει να δοθεί στο υλικό, καθώς έχει αναγνωριστεί πια ότι δεν είναι αδιάβλητο απέναντι σε κυβερνοεπιθέσεις.
7. Όσον αφορά το επίπεδο του δευτερογενούς ελέγχου, αξίζει να σημειωθούν, η έμφαση που πρέπει να δοθεί στον περιορισμό της χρονικής διάρκειας της επικοινωνίας, καθώς αποτελεί ένα πολύ σημαντικό τρωτό κομμάτι των συστημάτων και η σημασία της χρήσης κατανεμημένου ελέγχου, αντικαθιστώντας τον κεντρικό, ώστε να μπορεί να αποφευχθούν οι περιπτώσεις που ένα σημείο μπορεί να φέρει την κατάρρευση όλου του μικροδικτύου.

5.2 Προτάσεις για επέκταση

Η εργασία αυτή αποτελεί μια εκτενή βιβλιογραφική μελέτη της κυβερνοασφάλειας συστημάτων βασισμένα σε αντιστροφείς, με έμφαση στα μικροδίκτυα. Αναλύονται διαφόρων ειδών επιθέσεις σε αυτά και οι αμυντικοί μηχανισμοί που παρουσιάζονται για την προστασία τους, κατηγοριοποιώντας με βάση το επίπεδο που πλήττεται ή προστατεύεται σε κάθε περίπτωση.

Αρχικά, διατηρώντας αυτήν την κατηγοριοποίηση, θα μπορούσαν να συγκεντρωθούν και να μελετηθούν οι περιπτώσεις που αφορούν τον τριτογενή έλεγχο και να γίνει σύγκριση με τις περιπτώσεις που αφορούν τα τμήματα του ελέγχου μέχρι τον δευτερογενή, που μελετήθηκαν σε αυτή την εργασία. Ο τριτογενής έλεγχος είναι ένα πολύ σημαντικό κομμάτι του ιεραρχικού ελέγχου, καθώς κρίνεται απαραίτητος για τη βελτιστοποίηση της ανταλλαγής ισχύος μεταξύ του κυρίως δικτύου και συστημάτων βασισμένων σε αντιστροφείς, βελτιώνοντας έτσι την οικονομική λειτουργία του συστήματος. Ακόμα, συχνά αποφασίζει πότε ένα μικροδίκτυο θα λειτουργεί συνδεδεμένο στο δίκτυο και πότε απομονωμένο και επιβλέπει τη διαδικασία και τα αποτελέσματα του δευτερογενή ελέγχου.

Επιπλέον, η συντριπτική πλειοψηφία των επιθέσεων, που μελετήθηκαν στην εργασία, ανήκουν στις κατηγορίες των FDI και DoS επιθέσεων. Αξίζει να δοθεί προσοχή στις επιθέσεις που ανήκουν σε άλλες κατηγορίες, καθώς αν και δεν είναι τόσο συχνές, συνεχίζουν να αποτελούν,

δυνητικά, προβλήματα για τα συστήματα και να μελετηθούν οι επιπτώσεις που έχει καταγραφεί ότι επιφέρουν, καθώς και τα συστήματα που έχουν υλοποιηθεί ή πρέπει να υλοποιηθούν.

Ακόμα, στο κομμάτι των αμυντικών μηχανισμών στην εργασία ασχοληθήκαμε με τις καταγεγραμμένες περιπτώσεις πάνω στην ανίχνευση εισβολών και στο μετριασμό των επιπτώσεων. Επομένως, μπορεί να δοθεί έμφαση στο σύστημα της πρόληψης εισβολών, στον τρόπο εφαρμογής του και σε ποια τμήματα του ελέγχου έχει εφαρμοστεί σε μικροδίκτυα και γενικά σε συστήματα βασισμένα σε αντιστροφείς, καθώς η πρόληψη ενώ έχει περισσότερες απαιτήσεις από το σύστημα στο οποίο εφαρμόζεται, ταυτόχρονα προσφέρει στο δίκτυο το πλεονέκτημα να μη χρειαστεί να αντιμετωπίσει καμία διαταραχή της κανονικότητας του.

Βιβλιογραφία

[1] N. Hatziargyriou *et al*., "Definition and Classification of Power System Stability – Revisited & Extended," in *IEEE Transactions on Power Systems*, vol. 36, no. 4, pp. 3271-3281, July 2021, doi: 10.1109/TPWRS.2020.3041774.

[2] Q. Hou, E. Du, N. Zhang and C. Kang, "Impact of High Renewable Penetration on the Power System Operation Mode: A Data-Driven Approach," in *IEEE Transactions on Power Systems*, vol. 35, no. 1, pp. 731-741, Jan. 2020, doi: 10.1109/TPWRS.2019.2929276.

[3] H. Wang, M. Liserre and F. Blaabjerg, "Toward Reliable Power Electronics: Challenges, Design Tools, and Opportunities," in *IEEE Industrial Electronics Magazine*, vol. 7, no. 2, pp. 17-26, June 2013, doi: 10.1109/MIE.2013.2252958.

[4] B. Arbab-Zavar, E. J. Palacios-Garcia, J. C. Vasquez, and J. M. Guerrero, "Smart inverters for microgrid applications: A review," *Energies*, vol. 12, no. 5, 2019, Art. no. 840, doi: 10.3390/en12050840.

[5] G. Liang, S. R. Weller, J. Zhao, F. Luo and Z. Y. Dong, "The 2015 Ukraine Blackout: Implications for False Data Injection Attacks," in *IEEE Transactions on Power Systems*, vol. 32, no. 4, pp. 3317-3318, July 2017, doi: 10.1109/TPWRS.2016.2631891.

[6] F. de Bosio, L. A. de Souza Ribeiro, F. D. Freijedo, M. Pastorelli and J. M. Guerrero, "Effect of state feedback coupling and system delays on the transient performance of stand-alone VSI with LC output filter", *IEEE Trans. Ind. Electron.*, vol. 63, no. 8, pp. 4909-4918, Aug. 2016, doi: 10.1109/TIE.2016.2549990.

[7] P. Unruh, M. Nuschke, P. Strauß, and F. Welck, "Overview on Grid-Forming Inverter Control Methods," *Energies*, vol. 13, no. 10, p. 2589, May 2020, doi: 10.3390/en13102589.

[8] R. Teodorescu, M. Liserre and P. Rodriguez, Grid Converters for Photovoltaic and Wind Power Systems, Hoboken, NJ, USA:Wiley, 2011, doi: 10.1002/9780470667057.

[9] S. Sahoo, T. Dragičević and F. Blaabjerg, "Cyber Security in Control of Grid-Tied Power Electronic Converters—Challenges and Vulnerabilities," in *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 9, no. 5, pp. 5326-5340, Oct. 2021, doi: 10.1109/JESTPE.2019.2953480.

[10] A. R. Metke and R. L. Ekl, "Security Technology for Smart Grid Networks," in *IEEE Transactions on Smart Grid*, vol. 1, no. 1, pp. 99-107, June 2010, doi: 10.1109/TSG.2010.2046347.

[11] A. Ovalle, G. Ramos, S. Bacha, A. Hably and A. Rumeau, "Decentralized Control of Voltage Source Converters in Microgrids Based on the Application of Instantaneous Power Theory," in *IEEE Transactions on Industrial Electronics*, vol. 62, no. 2, pp. 1152-1162, Feb. 2015, doi:

10.1109/TIE.2014.2336638.
[12] Y. Sabri, N. El Kamoun and F. Lakrami, "A Survey: Centralized, Decentralized, and Distributed Control Scheme in Smart Grid Systems," 2019 7th Mediterranean Congress of Telecommunications (CMT), Fez, Morocco, 2019, pp. 1-11, doi: 10.1109/CMT.2019.8931370.
[13] C. Breyer et al., "On the History and Future of 100% Renewable Energy Systems Research," in IEEE Access, vol. 10, pp. 78176-78218, 2022, doi: 10.1109/ACCESS.2022.3193402.
[14] C. Carter, I. Onunkwo, P. Cordeiro and J. Johnson, "Cyber Security Assessment of Distributed Energy Resources," *2017 IEEE 44th Photovoltaic Specialist Conference (PVSC)*, Washington, DC, USA, 2017, pp. 2135-2140, doi: 10.1109/PVSC.2017.8366503.
[15] C. A. Plet, M. Brucoli, J. D. F. McDonald and T. C. Green, "Fault models of inverter-interfaced distributed generators: Experimental verification and application to fault analysis," 2011 IEEE Power and Energy Society General Meeting, Detroit, MI, USA, 2011, pp. 1-8, doi: 10.1109/PES.2011.6039183.
[16] J. Ni, H. Cao, X. Liu, L. Yang and L. Xiong, "Fixed-time leader-follower consensus based secondary voltage control for microgrid under directed communication graph," 2021 IEEE International Conference on Real-time Computing and Robotics (RCAR), Xining, China, 2021, pp. 566-571, doi: 10.1109/RCAR52367.2021.9517603.
[17] J. Qin, W. X. Zheng and H. Gao, "Coordination of Multiple Agents With Double-Integrator Dynamics Under Generalized Interaction Topologies," in IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), vol. 42, no. 1, pp. 44-57, Feb. 2012, doi: 10.1109/TSMCB.2011.2164523.
[18] B. Ning, Q. -L. Han, Z. Zuo, L. Ding, Q. Lu and X. Ge, "Fixed-Time and Prescribed-Time Consensus Control of Multiagent Systems and Its Applications: A Survey of Recent Trends and Methodologies," in IEEE Transactions on Industrial Informatics, vol. 19, no. 2, pp. 1121-1135, Feb. 2023, doi: 10.1109/TII.2022.3201589.
[19] Y. Li and J. Yan, "Cybersecurity of Smart Inverters in the Smart Grid: A Survey," in IEEE Transactions on Power Electronics, vol. 38, no. 2, pp. 2364-2383, Feb. 2023, doi: 10.1109/TPEL.2022.3206239.
[20] F. Nawaz, E. Pashajavid, Y. Fan and M. Batool, "A Comprehensive Review of the State-of-the-Art of Secondary Control Strategies for Microgrids," in IEEE Access, vol. 11, pp. 102444-102459, 2023, doi: 10.1109/ACCESS.2023.3316016.
[21] N. Komninos, E. Philippou and A. Pitsillides, "Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures," in *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 1933-1954, Fourthquarter 2014, doi: 10.1109/COMST.2014.2320093.
[22] Y. Yang, T. Littler, S. Sezer, K. McLaughlin and H. F. Wang, "Impact of cyber-security issues

on Smart Grid," *2011 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies*, Manchester, UK, 2011, pp. 1-7, doi: 10.1109/ISGTEurope.2011.6162722.

[23] Y. Jiang, S. Wu, X. Zhao, H. Luo, X. Li and Y. Wu, "A lightweight defense scheme for industrial data transmission against eavesdropping attacks and integrity attacks," *2021 4th IEEE International Conference on Industrial Cyber-Physical Systems (ICPS)*, Victoria, BC, Canada, 2021, pp. 461-466, doi: 10.1109/ICPS49255.2021.9468205.

[24] R. Salama, F. Al-Turjman, S. Bhatla and S. P. Yadav, "Social engineering attack types and prevention techniques- A survey," *2023 International Conference on Computational Intelligence, Communication Technology and Networking (CICTN)*, Ghaziabad, India, 2023, pp. 817-820, doi: 10.1109/CICTN57981.2023.10140957.

[25] Y. Liu, M. K. Reiter, and P. Ning, “False data injection attacks against state estimation in electric power grids,” *ACM Trans. Inf. Syst. Secur.*, vol. 14, no. 1, pp. 21–32, May 2009, doi: 10.1145/1952982.1952995.

[26] M. A. Rahman and H. Mohsenian-Rad, "False data injection attacks against nonlinear state estimation in smart power grids," *2013 IEEE Power & Energy Society General Meeting*, Vancouver, BC, Canada, 2013, pp. 1-5, doi: 10.1109/PESMG.2013.6672638.

[27] L. Che, X. Liu, Z. Li and Y. Wen, "False Data Injection Attacks Induced Sequential Outages in Power Systems," in *IEEE Transactions on Power Systems*, vol. 34, no. 2, pp. 1513-1523, March 2019, doi: 10.1109/TPWRS.2018.2871345.

[28] D. -T. Peng, J. Dong and Q. Peng, "Overloaded Branch Chains Induced by False Data Injection Attack in Smart Grid," in *IEEE Signal Processing Letters*, vol. 27, pp. 426-430, 2020, doi: 10.1109/LSP.2020.2974097.

[29] Y. Yuan, Z. Li and K. Ren, "Modeling Load Redistribution Attacks in Power Systems," in *IEEE Transactions on Smart Grid*, vol. 2, no. 2, pp. 382-390, June 2011, doi: 10.1109/TSG.2011.2123925.

[30] M. Conti, N. Dragoni and V. Lesyk, "A Survey of Man In The Middle Attacks," in *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 2027-2051, thirdquarter 2016, doi: 10.1109/COMST.2016.2548426.

[31] B. Kang *et al*., "Investigating cyber-physical attacks against IEC 61850 photovoltaic inverter installations," *2015 IEEE 20th Conference on Emerging Technologies & Factory Automation (ETFA)*, Luxembourg, Luxembourg, 2015, pp. 1-8, doi: 10.1109/ETFA.2015.7301457.

[32] Y. Cui, F. Bai, Y. Liu, P. L. Fuhr and M. E. Morales-Rodríguez, "Spatio-Temporal Characterization of Synchrophasor Data Against Spoofing Attacks in Smart Grids," in *IEEE Transactions on Smart Grid*, vol. 10, no. 5, pp. 5807-5818, Sept. 2019, doi: 10.1109/TSG.2019.2891852.

[33] Y. Mo, S. Weerakkody and B. Sinopoli, "Physical Authentication of Control Systems: Designing Watermarked Control Inputs to Detect Counterfeit Sensor Outputs," in *IEEE Control Systems Magazine*, vol. 35, no. 1, pp. 93-109, Feb. 2015, doi: 10.1109/MCS.2014.2364724.

[34] S. Hossain-McKenzie, A. Chavez, N. Jacobs, C. B. Jones, A. Summers and B. Wright, "Proactive Intrusion Detection and Mitigation System: Case Study on Packet Replay Attacks in Distributed Energy Resource Systems," *2021 IEEE Power and Energy Conference at Illinois (PECI)*, Urbana, IL, USA, 2021, pp. 1-6, doi: 10.1109/PECI51586.2021.9435231.

[35] J. Zhao, J. Wang and L. Yin, "Detection and Control against Replay Attacks in Smart Grid," *2016 12th International Conference on Computational Intelligence and Security (CIS)*, Wuxi, China, 2016, pp. 624-627, doi: 10.1109/CIS.2016.0151.

[36] Y. Guo, C. -W. Ten, S. Hu and W. W. Weaver, "Modeling distributed denial of service attack in advanced metering infrastructure," *2015 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, Washington, DC, USA, 2015, pp. 1-5, doi: 10.1109/ISGT.2015.7131828.

[37] P. Yi, T. Zhu, Q. Zhang, Y. Wu and J. Li, "A denial of service attack in advanced metering infrastructure network," *2014 IEEE International Conference on Communications (ICC)*, Sydney, NSW, Australia, 2014, pp. 1029-1034, doi: 10.1109/ICC.2014.6883456.

[38] K. Gai, M. Qiu, Z. Ming, H. Zhao and L. Qiu, "Spoofing-Jamming Attack Strategy Using Optimal Power Distributions in Wireless Smart Grid Networks," in *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2431-2439, Sept. 2017, doi: 10.1109/TSG.2017.2664043.

[39] J. Ma, Y. Liu, L. Song and Z. Han, "Multiact Dynamic Game Strategy for Jamming Attack in Electricity Market," in *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2273-2282, Sept. 2015, doi: 10.1109/TSG.2015.2400215.

[40] C. Konstantinou and M. Maniatakos, “A case study on implementing false data injection attacks against nonlinear state estimation,” in *Proc. 1st ACM Workshop Cyber-Physical Syst. Secur. Privacy (CPS-SPC)*, Vienna, Austria, Oct. 2016, pp. 81–92, doi: 10.1145/2994487.2994491.

[41] C. Konstantinou and M. Maniatakos, “Hardware-layer intelligence collection for smart grid embedded systems,” *J. Hardw. Syst. Secur.*, vol. 3, no. 1, pp. 1–14, Mar. 2019, doi: 10.1007/s41635-018-0063-0.

[42] S. R. B. Alvee, B. Ahn, S. Ahmad, K. -T. Kim, T. Kim and J. Zeng, "Device-Centric Firmware Malware Detection for Smart Inverters using Deep Transfer Learning," *2022 IEEE Design Methodologies Conference (DMC)*, Bath, United Kingdom, 2022, pp. 1-5, doi: 10.1109/DMC55175.2022.9906538.

[43] C. Konstantinou, A. Keliris and M. Maniatakos, "Taxonomy of firmware Trojans in smart grid devices," *2016 IEEE Power and Energy Society General Meeting (PESGM)*, Boston, MA, USA,

2016, pp. 1-5, doi: 10.1109/PESGM.2016.7741452.
[44] A. P. Kuruvila, I. Zografopoulos, K. Basu, and C. Konstantinou, “Hardware-assisted detection of firmware attacks in inverter-based cyberphysical microgrids,” *International Journal of Electrical Power & Energy Systems*, vol. 132, p. 107150, May 2021, doi: 10.1016/j.ijepes.2021.107150
[45] Q. Jiang, B. Li, T. Liu, F. Blaabjerg and P. Wang, "Study of Cyber Attack’s Impact on LCC-HVDC System With False Data Injection," in *IEEE Transactions on Smart Grid*, vol. 14, no. 4, pp. 3220-3231, July 2023, doi: 10.1109/TSG.2023.3266780.
[46] Á. M. Gómez, L. Navarro-Hilfiker and R. Wiśniewski, "Model-based Detection of Data-Injection Cyber-Attacks on Wind Turbine Controllers," *2024 10th International Conference on Control, Decision and Information Technologies (CoDIT)*, Vallette, Malta, 2024, pp. 1780-1785, doi: 10.1109/CoDIT62066.2024.10708323.
[47] Z. Jiang, P. Zhang and Y. Zhou, "Differential Duffing Oscillator-Based Cyberattack Detection for Inverters," in *IEEE Transactions on Smart Grid*, vol. 15, no. 1, pp. 1192-1195, Jan. 2024, doi: 10.1109/TSG.2023.3328160.
[48] A. Barua and M. A. Al Faruque, "Special Session: Noninvasive Sensor-Spoofing Attacks on Embedded and Cyber-Physical Systems," *2020 IEEE 38th International Conference on Computer Design (ICCD)*, Hartford, CT, USA, 2020, pp. 45-48, doi: 10.1109/ICCD50377.2020.00024.
[49] Z. Dan, F. Yang, K. Pan, C. Yan, X. Ji and W. Xu, "A Novel EMI Attack Exploiting the Control Vulnerability of Photovoltaic Inverters," *2022 IEEE 6th Conference on Energy Internet and Energy System Integration (EI2)*, Chengdu, China, 2022, pp. 1076-1080, doi: 10.1109/EI256261.2022.10116254.
[50] D. M. Vilathgamuwa, P. C. Loh and Y. Li, "Protection of Microgrids During Utility Voltage Sags," in IEEE Transactions on Industrial Electronics, vol. 53, no. 5, pp. 1427-1436, Oct. 2006, doi: 10.1109/TIE.2006.882006.
[51] Y. Wang and B. C. Pal, "Destabilizing Attack and Robust Defense for Inverter-Based Microgrids by Adversarial Deep Reinforcement Learning," in IEEE Transactions on Smart Grid, vol. 14, no. 6, pp. 4839-4850, Nov. 2023, doi: 10.1109/TSG.2023.3263243.
[52] H. Salehghaffari and M. Khodaparastan, "Dynamic Attacks Against Inverter-Based Microgrids," *2019 IEEE Power & Energy Society General Meeting (PESGM)*, Atlanta, GA, USA, 2019, pp. 1-5, doi: 10.1109/PESGM40551.2019.8973416.
[53] H. M. Albunashee *et al*., "A Test Bed for Detecting False Data Injection Attacks in Systems With Distributed Energy Resources," in *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 10, no. 1, pp. 1303-1315, Feb. 2022, doi: 10.1109/JESTPE.2019.2948216.
[54] A. Bamigbade, Y. Dvorkin and R. Karri, "Cyberattack on Phase-Locked Loops in Inverter-Based Energy Resources," in *IEEE Transactions on Smart Grid*, vol. 15, no. 1, pp. 821-833, Jan.

2024, doi: 10.1109/TSG.2023.3270348.
[55] M. Ansari, M. Ghafouri and A. Ameli, "Cybersecurity Vulnerabilities in Phase-Locked Loop (PLL) of DFIG-Based Wind Power Plants," *2023 IEEE 2nd Industrial Electronics Society Annual On-Line Conference (ONCON)*, SC, USA, 2023, pp. 1-6, doi: 10.1109/ONCON60463.2023.10431170.
[56] A. Bamigbade and F. d. León, "Secure Voltage-Modulated Vector Current Control of Distributed Energy Resources Using Delayed DSOGI Under Distorted and Unbalanced Grid Conditions," in *IEEE Transactions on Industry Applications*, doi: 10.1109/TIA.2024.3481214.
[57] T. -H. Kim, C. S. Sin, S. Lee and J. H. Kim, "Analysis of effect of anti-spoofing signal for mitigating to spoofing in GPS L1 signal," *2013 13th International Conference on Control, Automation and Systems (ICCAS 2013)*, Gwangju, Korea (South), 2013, pp. 523-526, doi: 10.1109/ICCAS.2013.6703992.
[58] X. Zha, Y. Liu and M. Huang, "Resilient Power Converter: A Grid-Connected Converter With Disturbance/Attack Resiliency via Multi-Timescale Current Limiting Scheme," in *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 11, no. 1, pp. 59-68, March 2021, doi: 10.1109/JETCAS.2021.3052252.
[59] A. Milczarek, M. Malinowski and J. M. Guerrero, "Reactive Power Management in Islanded Microgrid—Proportional Power Sharing in Hierarchical Droop Control," in *IEEE Transactions on Smart Grid*, vol. 6, no. 4, pp. 1631-1638, July 2015, doi: 10.1109/TSG.2015.2396639.
[60] S. Acharya, M. S. El-Moursi, A. Al-Hinai, A. S. Al-Sumaiti and H. H. Zeineldin, "A Control Strategy for Voltage Unbalance Mitigation in an Islanded Microgrid Considering Demand Side Management Capability," in *IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 2558-2568, May 2019, doi: 10.1109/TSG.2018.2804954.
[61] L. Meng, F. Tang, M. Savaghebi, J. C. Vasquez and J. M. Guerrero, "Tertiary Control of Voltage Unbalance Compensation for Optimal Power Quality in Islanded Microgrids," in *IEEE Transactions on Energy Conversion*, vol. 29, no. 4, pp. 802-815, Dec. 2014, doi: 10.1109/TEC.2014.2363687.
[62] X. Wang, J. M. Guerrero, F. Blaabjerg and Z. Chen, "Secondary voltage control for harmonics suppression in islanded microgrids," *2011 IEEE Power and Energy Society General Meeting*, Detroit, MI, USA, 2011, pp. 1-8, doi: 10.1109/PES.2011.6039871.
[63] Y. Han, P. Shen, X. Zhao and J. M. Guerrero, "An Enhanced Power Sharing Scheme for Voltage Unbalance and Harmonics Compensation in an Islanded AC Microgrid," in *IEEE Transactions on Energy Conversion*, vol. 31, no. 3, pp. 1037-1050, Sept. 2016, doi: 10.1109/TEC.2016.2552497.
[64] X. Yang, Y. Du, J. Su, L. Chang, Y. Shi and J. Lai, "An Optimal Secondary Voltage Control

Strategy for an Islanded Multibus Microgrid," in *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 4, no. 4, pp. 1236-1246, Dec. 2016, doi: 10.1109/JESTPE.2016.2602367.

[65] Y. Guan, J. C. Vasquez and J. M. Guerrero, "Coordinated Secondary Control for Balanced Discharge Rate of Energy Storage System in Islanded AC Microgrids," in *IEEE Transactions on Industry Applications*, vol. 52, no. 6, pp. 5019-5028, Nov.-Dec. 2016, doi: 10.1109/TIA.2016.2598724.

[66] Y. Khayat *et al*., "On the Secondary Control Architectures of AC Microgrids: An Overview," in *IEEE Transactions on Power Electronics*, vol. 35, no. 6, pp. 6482-6500, June 2020, doi: 10.1109/TPEL.2019.2951694.

[67] Y. Han, H. Li, L. Xu, X. Zhao and J. M. Guerrero, "Analysis of Washout Filter-Based Power Sharing Strategy—An Equivalent Secondary Controller for Islanded Microgrid Without LBC Lines," in *IEEE Transactions on Smart Grid*, vol. 9, no. 5, pp. 4061-4076, Sept. 2018, doi: 10.1109/TSG.2017.2647958.

[68] J. Lu, M. Savaghebi and J. M. Guerrero, "Second order washout filter based power sharing strategy for uninterruptible power supply," *IECON 2017 - 43rd Annual Conference of the IEEE Industrial Electronics Society*, Beijing, China, 2017, pp. 7854-7859, doi: 10.1109/IECON.2017.8217376.

[69] N. Xia, H. B. Gooi, S. Chen and W. Hu, "Decentralized State Estimation for Hybrid AC/DC Microgrids," in *IEEE Systems Journal*, vol. 12, no. 1, pp. 434-443, March 2018, doi: 10.1109/JSYST.2016.2615428.

[70] W. Gu, G. Lou, W. Tan and X. Yuan, "A Nonlinear State Estimator-Based Decentralized Secondary Voltage Control Scheme for Autonomous Microgrids," in *IEEE Transactions on Power Systems*, vol. 32, no. 6, pp. 4794-4804, Nov. 2017, doi: 10.1109/TPWRS.2017.2676181.

[71] K. Dehghanpour, Z. Wang, J. Wang, Y. Yuan and F. Bu, "A Survey on State Estimation Techniques and Challenges in Smart Distribution Systems," in *IEEE Transactions on Smart Grid*, vol. 10, no. 2, pp. 2312-2322, March 2019, doi: 10.1109/TSG.2018.2870600.

[72] Y. Khayat *et al*., "Communication-less Optimal Frequency Control of Islanded Microgrids," *2018 20th European Conference on Power Electronics and Applications (EPE'18 ECCE Europe)*, Riga, Latvia, 2018, pp. P.1-P.8.

[73] J. M. Rey, P. Martí, M. Velasco, J. Miret and M. Castilla, "Secondary Switched Control With no Communications for Islanded Microgrids," in *IEEE Transactions on Industrial Electronics*, vol. 64, no. 11, pp. 8534-8545, Nov. 2017, doi: 10.1109/TIE.2017.2703669.

[74] Q. Shafiee, T. Dragicevic, J. C. Vasquez, J. M. Guerrero, C. Stefanovic and P. Popovski, "A novel robust communication algorithm for distributed secondary control of islanded MicroGrids," *2013 IEEE Energy Conversion Congress and Exposition*, Denver, CO, USA, 2013, pp. 4609-4616,

doi: 10.1109/ECCE.2013.6647318.
[75] J. W. Simpson-Porco, Q. Shafiee, F. Dörfler, J. C. Vasquez, J. M. Guerrero and F. Bullo, "Secondary Frequency and Voltage Control of Islanded Microgrids via Distributed Averaging," in *IEEE Transactions on Industrial Electronics*, vol. 62, no. 11, pp. 7025-7038, Nov. 2015, doi: 10.1109/TIE.2015.2436879.
[76] E. A. Coelho *et al*., "Small-Signal Analysis of the Microgrid Secondary Control Considering a Communication Time Delay," in *IEEE Transactions on Industrial Electronics*, vol. 63, no. 10, pp. 6257-6269, Oct. 2016, doi: 10.1109/TIE.2016.2581155.
[77] S. Manaffam, M. Talebi, A. K. Jain and A. Behal, "Intelligent Pinning Based Cooperative Secondary Control of Distributed Generators for Microgrid in Islanding Operation Mode," in *IEEE Transactions on Power Systems*, vol. 33, no. 2, pp. 1364-1373, March 2018, doi: 10.1109/TPWRS.2017.2732958.
[78] W. Liu, W. Gu, Q. Huang, L. Chen and X. Yuan, "Pinning Group Consensus-Based Distributed Coordination Control for Active Distribution Systems," in *IEEE Access*, vol. 6, pp. 2330-2339, 2018, doi: 10.1109/ACCESS.2017.2782817.
[79] W. P. M. H. Heemels, M. C. F. Donkers and A. R. Teel, "Periodic Event-Triggered Control for Linear Systems," in *IEEE Transactions on Automatic Control*, vol. 58, no. 4, pp. 847-861, April 2013, doi: 10.1109/TAC.2012.2220443.
[80] J. Lu, M. Zhao, S. Golestan, T. Dragicevic, X. Pan and J. M. Guerrero, "Distributed Event-Triggered Control for Reactive, Unbalanced, and Harmonic Power Sharing in Islanded AC Microgrids," in *IEEE Transactions on Industrial Electronics*, vol. 69, no. 2, pp. 1548-1560, Feb. 2022, doi: 10.1109/TIE.2021.3057018.
[81] Y. Chen *et al*., "Distributed Self-Triggered Control for Frequency Restoration and Active Power Sharing in Islanded Microgrids," in *IEEE Transactions on Industrial Informatics*, vol. 19, no. 10, pp. 10635-10646, Oct. 2023, doi: 10.1109/TII.2023.3240738.
[82] H. Zhang, W. Meng, J. Qi, X. Wang and W. X. Zheng, "Distributed Load Sharing Under False Data Injection Attack in an Inverter-Based Microgrid," in *IEEE Transactions on Industrial Electronics*, vol. 66, no. 2, pp. 1543-1551, Feb. 2019, doi: 10.1109/TIE.2018.2793241.
[83] K. Ma, Y. Dong, P. Zhao and J. Yang, "Distributed Resilient Frequency Control Based on Estimation of Sensor and Actuator Attacks in AC Microgrids," *IECON 2022 – 48th Annual Conference of the IEEE Industrial Electronics Society*, Brussels, Belgium, 2022, pp. 1-6, doi: 10.1109/IECON49645.2022.9968390.
[84] Q. Zhou, M. Shahidehpour, A. Alabdulwahab, A. Abusorrah, L. Che and X. Liu, "Cross-Layer Distributed Control Strategy for Cyber Resilient Microgrids," in *IEEE Transactions on Smart Grid*, vol. 12, no. 5, pp. 3705-3717, Sept. 2021, doi: 10.1109/TSG.2021.3069331.

[85] S. Fan, D. Yue, H. Yan and C. Deng, "Distributed Round-Robin Protocol-Based Secondary Control for ESSs Under FDI Attacks," in *IEEE Transactions on Industrial Electronics*, vol. 71, no. 12, pp. 16493-16502, Dec. 2024, doi: 10.1109/TIE.2024.3390733.

[86] Y. Chen, D. Qi, H. Dong, C. Li, Z. Li and J. Zhang, "A FDI Attack-Resilient Distributed Secondary Control Strategy for Islanded Microgrids," in *IEEE Transactions on Smart Grid*, vol. 12, no. 3, pp. 1929-1938, May 2021, doi: 10.1109/TSG.2020.3047949.

[87] S. Tan *et al*., "Lyapunov-Based Resilient Cooperative Control for DC Microgrid Clusters Against False Data Injection Cyber-Attacks," in *IEEE Transactions on Smart Grid*, vol. 15, no. 3, pp. 3208-3222, May 2024, doi: 10.1109/TSG.2023.3332946.

[88] S. Hu, X. Ge, X. Chen and D. Yue, "Resilient Load Frequency Control of Islanded AC Microgrids Under Concurrent False Data Injection and Denial-of-Service Attacks," in *IEEE Transactions on Smart Grid*, vol. 14, no. 1, pp. 690-700, Jan. 2023, doi: 10.1109/TSG.2022.3190680.

[89] J. Zhang, S. Fan, C. Deng, B. Wang and X. Xie, "Distributed Resilient Secondary Control for AC Microgrids Against Hybrid Attacks," in *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 71, no. 11, pp. 5211-5220, Nov. 2024, doi: 10.1109/TCSI.2024.3449896.

[90] W. Zhang, T. Qian, X. Chen, K. Huang, W. Tang and Q. Wu, "Resilient Economic Control for Distributed Microgrids Under False Data Injection Attacks," in *IEEE Transactions on Smart Grid*, vol. 12, no. 5, pp. 4435-4446, Sept. 2021, doi: 10.1109/TSG.2021.3073874.

[91] M. Jamali, M. S. Sadabadi, M. Davari, S. Sahoo and F. Blaabjerg, "Resilient Cooperative Secondary Control of Islanded AC Microgrids Utilizing Inverter-Based Resources Against State-Dependent False Data Injection Attacks," in *IEEE Transactions on Industrial Electronics*, vol. 71, no. 5, pp. 4719-4730, May 2024, doi: 10.1109/TIE.2023.3281698.

[92] A. Mustafa, B. Poudel, A. Bidram and H. Modares, "Detection and Mitigation of Data Manipulation Attacks in AC Microgrids," in *IEEE Transactions on Smart Grid*, vol. 11, no. 3, pp. 2588-2603, May 2020, doi: 10.1109/TSG.2019.2958014.

[93] R. Lu, J. Wang and Z. Wang, "Distributed Observer-Based Finite-Time Control of AC Microgrid Under Attack," in *IEEE Transactions on Smart Grid*, vol. 12, no. 1, pp. 157-168, Jan. 2021, doi: 10.1109/TSG.2020.3017793.

[94] I. Zografopoulos and C. Konstantinou, "Detection of Malicious Attacks in Autonomous Cyber-Physical Inverter-Based Microgrids," in *IEEE Transactions on Industrial Informatics*, vol. 18, no. 9, pp. 5815-5826, Sept. 2022, doi: 10.1109/TII.2021.3132131.

[95] S. Zuo, O. A. Beg, F. L. Lewis and A. Davoudi, "Resilient Networked AC Microgrids Under Unbounded Cyber Attacks," in *IEEE Transactions on Smart Grid*, vol. 11, no. 5, pp. 3785-3794, Sept. 2020, doi: 10.1109/TSG.2020.2984266.

[96] S. Weng, D. Yue, J. Chen and C. Dou, "Distributed Resilient Event-Triggered Control for Power Quality Improvement in Grid-Tied Microgrid Under Denial-of-Service Attack," in *IEEE Systems Journal*, vol. 18, no. 2, pp. 860-871, June 2024, doi: 10.1109/JSYST.2024.3367307.

[97] W. Yao, Y. Wang, Y. Xu and C. Deng, "Cyber-Resilient Control of an Islanded Microgrid Under Latency Attacks and Random DoS Attacks," in *IEEE Transactions on Industrial Informatics*, vol. 19, no. 4, pp. 5858-5869, April 2023, doi: 10.1109/TII.2022.3191315.

[98] J. Liu, Y. Du, S. -i. Yim, X. Lu, B. Chen and F. Qiu, "Steady-State Analysis of Microgrid Distributed Control Under Denial of Service Attacks," in *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 9, no. 5, pp. 5311-5325, Oct. 2021, doi: 10.1109/JESTPE.2020.2990879.

[99] X. Cai, B. Gao, X. Nan and J. Yuan, "Resilient Discrete-Time Quantization Communication for Distributed Secondary Control of AC Microgrids Under DoS Attacks," in *IEEE Systems Journal*, vol. 18, no. 3, pp. 1798-1808, Sept. 2024, doi: 10.1109/JSYST.2024.3444049.

[100] H. Yang, T. Li, Y. Long and Y. Xiao, "Event-Triggered Distributed Secondary Control With Model-Free Predictive Compensation in AC/DC Networked Microgrids Under DoS Attacks," in *IEEE Transactions on Cybernetics*, vol. 54, no. 1, pp. 298-307, Jan. 2024, doi: 10.1109/TCYB.2022.3218026.

[101] S. Liu, Z. Hu, X. Wang and L. Wu, "Stochastic Stability Analysis and Control of Secondary Frequency Regulation for Islanded Microgrids Under Random Denial of Service Attacks," in *IEEE Transactions on Industrial Informatics*, vol. 15, no. 7, pp. 4066-4075, July 2019, doi: 10.1109/TII.2018.2885170.

[102] C. Deng, C. Wen, Y. Zou, W. Wang and X. Li, "A Hierarchical Security Control Framework of Nonlinear CPSs Against DoS Attacks With Application to Power Sharing of AC Microgrids," in *IEEE Transactions on Cybernetics*, vol. 52, no. 6, pp. 5255-5266, June 2022, doi: 10.1109/TCYB.2020.3029045.

[103] P. Ge, B. Chen and F. Teng, "Cyber-Resilient Self-Triggered Distributed Control of Networked Microgrids Against Multi-Layer DoS Attacks," in *IEEE Transactions on Smart Grid*, vol. 14, no. 4, pp. 3114-3124, July 2023, doi: 10.1109/TSG.2022.3229486.