Πανεπιστήμιο Δυτικής Μακεδονίας

Διπλωματική εργασία:

Κυβερνοεπιθέσεις σε συστήματα ηλεκτρικής ενέργειας

ΔΗΜΗΤΡΟΠΟΥΛΟΣ ΓΕΩΡΓΙΟΣ
Α.Μ: HN07236

Επιβλέπων Διδάσκων: Πασχάλης Γκαϊδατζής

Πίνακας περιεχομένων

Λίστα Εικόνων

Λίστα Ακρωνύμων

Αγγλικοί Όροι

BDD	Bad data Detection
BSI	Bundesamt fur sicherheit in der informationstechnik
CIP	Continuous improvement programme
DoE	Department of energy
DHS	Department of homeland security
ENTSO-E	European transmission system operators entity
ERCOT	Electric reliability council of texas
FDI	Foreign direct injection
GAO	Government accountability office
IoT	Internet of things
JPCERT/CC	Japan computer emergency responce
KCL	Kirchhoff current law
KTT	Karush-kuhn-tucker
KVL	Kirchhoff voltage law
LoRaWan	Long range wide area network
LPWAN	Low power wide area network
NERK	North American reliability corporation
PMU	Phasor measurement unit
SCADA	Supervisory control and data acquisition
SCED	Security constraint economic dispatch
3GPP	3rd generation partnership project

Ελληνικοί Όροι

ΕΨΔ	Έγχυση ψευδών Δεδομένων
ΣΗΕ	Συστήματα Ηλεκτρικής Ενέργειας

Περίληψη

Με την ταχεία ανάπτυξη των έξυπνων δικτύων και τα ολοένα και πιο ολοκληρωμένα δίκτυα επικοινωνίας, τα δίκτυα ηλεκτρικής ενέργειας αντιμετωπίζουν σοβαρά προβλήματα ασφάλειας στον κυβερνοχώρο. Αυτό το έγγραφο εξετάζει τις υπάρχουσες μελέτες σχετικά με τον αντίκτυπο των επιθέσεων την διάδοση ψευδών δεδομένων στα συστήματα ηλεκτρικής ενέργειας από τρεις πτυχές: Πρώτον, η έγχυση λανθασμένων δεδομένων μπορεί να επηρεάσει αρνητικά την οικονομική αποστολή αυξάνοντας το λειτουργικό κόστος του συστήματος ισχύος ή προκαλώντας διαδοχικές υπερφορτώσεις, ακόμη και διακοπές λειτουργίας. Δεύτερον, οι εισβολείς μπορούν να εισάγουν ψευδή δεδομένα στον εκτιμητή κατάστασης του συστήματος ηλεκτρικής ενέργειας, και αυτό θα εμποδίσει τους χειριστές να αποκτήσουν τις πραγματικές συνθήκες λειτουργίας του συστήματος. Τρίτον, οι επιθέσεις έγχυσης ψευδών δεδομένων μπορούν να υποβαθμίσουν τον διανεμημένο έλεγχο των διανεμημένων γεννητριών ή των μικροδικτύων προκαλώντας ανισορροπία ισχύος μεταξύ προσφοράς και ζήτησης.

Λέξεις-Κλειδιά: Συστήματα Ηλεκτρικής Ενέργειας, Κυβερνοεπίθεση, Κυβερνοασφάλεια

Abstract

Electricity networks are confronted with major cybersecurity issues due to the fast implementation of the smart grid and the growing integration of communication networks. This report takes a three-pronged approach to current research on the effect of fake data assaults on power systems. It is possible that injecting wrong data can lead to increased power system running expenses or perhaps downtime due to consecutive overloads and other consequences of improper data injection. The power system status estimator may also be hacked, allowing attackers to insert bogus data into the system and preventing operators from obtaining the true operating conditions. Distributed generation and microgrids might suffer from an imbalance of power supply and demand due to bogus data injection attacks.

Keywords: Power System protection, Cyberattack, Cybersecurity

Εισαγωγή

Οι κυβερνοεπιθέσεις είναι ανησυχητικές για το ηλεκτρικό δίκτυο όσο και οι φυσικές καταστροφές, και το πρόβλημα επιδεινώνεται καθώς αυτά τα δίκτυα γίνονται πιο συνδεδεμένα και πιο έξυπνα.

Σε αντίθεση με το παρελθόν, όταν μια διακοπή ρεύματος επηρέαζε μόνο την ηλεκτρική ενέργεια που παρέχεται σε σπίτια και επιχειρήσεις, τα δίκτυα ηλεκτρικής ενέργειας γίνονται βασικά στοιχεία των έξυπνων πόλεων, των υποδομών και των υπηρεσιών που σχετίζονται με την ασφάλεια. Χωρίς ισχύ, τίποτα από αυτά δεν λειτουργεί, και οι εξελιγμένες κυβερνοεγκληματικές ενέργειες μπορούν να κρατήσουν ομήρους μεγάλες περιοχές μέχρι να πληρώσουν τεράστια λύτρα ή να υποστούν άλλες απαιτήσεις.

Οι απειλές είναι επίσης παγκόσμιες. Καθώς η κερδοφορία από τις κυβερνοεπιθέσεις σε αυτά τα συστήματα αυξάνεται, αυξάνεται και ο αριθμός τους. Το Ευρωπαϊκό Δίκτυο Διαχειριστών Συστημάτων Μεταφοράς Ηλεκτρικής Ενέργειας (ENTSO-E), το οποίο αντιπροσωπεύει 42 ευρωπαϊκούς διαχειριστές συστημάτων μεταφοράς σε 35 χώρες, παραβιάστηκε το 2020. Ελλείψει σαφώς καθορισμένου πλαισίου ή σχετικών πληροφοριών που αφορούν μια παράβαση, είναι ανέφικτο να προσδιοριστεί επακριβώς μια συγκεκριμένη παράβαση που διαπράχθηκε από το Ευρωπαϊκό Δίκτυο Διαχειριστών Συστημάτων Μεταφοράς Ηλεκτρικής Ενέργειας (ENTSO-E). Οι πιθανές παραβάσεις περιλαμβάνουν τη μη τήρηση των κωδίκων και κανονισμών δικτύου, τον ανεπαρκή συντονισμό των διακρατικών συναλλαγών ηλεκτρικής ενέργειας, τον ανεπαρκή σχεδιασμό ή συντήρηση του συστήματος με αποτέλεσμα την αστάθεια του δικτύου ή τις διακοπές ρεύματος, ή τις παραβάσεις των μέτρων ασφάλειας στον κυβερνοχώρο. Τα ολοκληρωμένα δεδομένα είναι απαραίτητα για να διακρίνουμε την ακριβή παράβαση, δεδομένου του ευρέος φάσματος καθηκόντων που εμπίπτουν στην αρμοδιότητα του ENTSO-E και περιλαμβάνουν διάφορες πτυχές της μεταφοράς ηλεκτρικής ενέργειας και της λειτουργίας του συστήματος. Άλλες επιτυχημένες κυβερνοεπιθέσεις περιλαμβάνουν αυτές στο ρωσικό δίκτυο ηλεκτρικής ενέργειας το 2019 και στα πετροχημικά εργοστάσια της Saudi Aramco το 2017.

Το δίκτυο της Ουκρανίας δέχτηκε επίθεση το 2015, αφήνοντας 200.000 νοικοκυριά χωρίς ρεύμα. Μια παρόμοια επιχείρηση έγινε την επόμενη χρονιά. Και οι εγκληματίες του κυβερνοχώρου που παραβίασαν την Korea Hydro and Nuclear Power, τη νοτιοκορεατική πυρηνική και υδροηλεκτρική εταιρεία, το 2014 δημοσίευσαν σχέδια

και εγχειρίδια για δύο πυρηνικούς αντιδραστήρες στο διαδίκτυο και εξέθεσαν προσωπικά δεδομένα 10.000 εργαζομένων.

Σύμφωνα με την Ετήσια Έκθεση Αξιολόγησης Απειλών της Έκθεσης της Κοινότητας Πληροφοριών των ΗΠΑ (σελίδα 20), οι χώρες με δυνατότητες κυβερνοεπιθέσεων που στοχεύουν κρίσιμες υποδομές περιλαμβάνουν τη Ρωσία, την Κίνα, το Ιράν και τη Βόρεια Κορέα. Με άλλα λόγια, οι κυβερνοεπιθέσεις μπορούν να συμβούν οπουδήποτε και ανά πάσα στιγμή, και με αυτό το επίπεδο ικανότητας, καμία οντότητα δεν είναι απρόσβλητη.

Κεφάλαιο 1ο: «Η Προστασία και ο Έλεγχος των Σύγχρονων Συστημάτων Ηλεκτρικής Ενέργειας»

1.1 Εισαγωγή στα συστήματα ηλεκτρικής ενέργειας

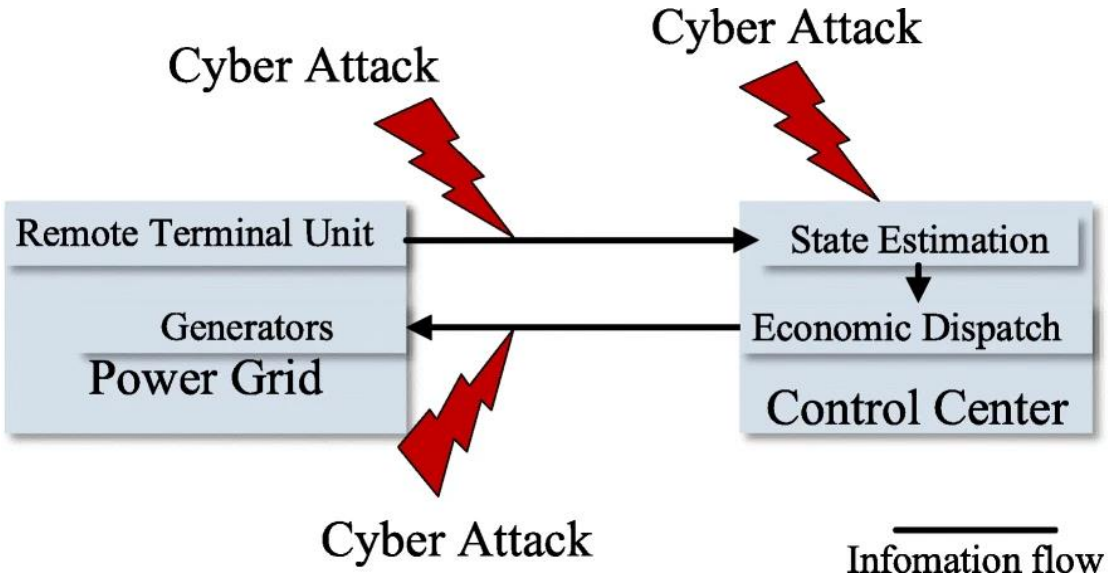
Με την εκτεταμένη ενσωμάτωση τεχνολογίας πληροφοριών και επικοινωνιών, τα συστήματα ισχύος εκτίθενται σε απειλές στον κυβερνοχώρο. Στοχεύοντας τη διαδικασία ανταλλαγής πληροφοριών, οι κακόβουλοι εισβολείς μπορούν να εισάγουν ψευδή δεδομένα για να προκαλέσουν διακοπή ρεύματος, οικονομική απώλεια και αστάθεια του συστήματος. Η έγχυση ψευδών δεδομένων (ΕΨΔ-false data injection-FDI) μπορεί επίσης να χρησιμοποιηθεί για την κάλυψη των υφιστάμενων βλαβών του ΣΗΕ. Αυτό θα επηρεάσει την ορατότητα του χειριστή στα σφάλματα και θα αποτρέψει τη λήψη κατάλληλων αντίμετρων.

Για παράδειγμα, το 2015, το ηλεκτρικό δίκτυο της Ουκρανίας δέχθηκε επίθεση και άνοιξαν διακόπτες υποσταθμού από κακόβουλες οντότητες [1]. Για να σχεδιαστούν κατάλληλα μέτρα προστασίας για τη βελτίωση της ανθεκτικότητας του συστήματος, είναι απαραίτητο να διερευνηθεί ο τρόπος με τον οποίο οι ΕΨΔ επηρεάζουν το σύστημα ηλεκτρικής ενεργειας (ΣΗΕ). Έτσι, έχει γίνει πολλή έρευνα σχετικά με τον επιθετικό μηχανισμό και την επίδραση των FDI .

Γενικά, τα μονοπάτια μέσω των οποίων οι FDI επηρεάζουν αρνητικά ένα ΣΗΕ μπορούν να ταξινομηθούν σε τρεις κατηγορίες, δηλαδή την εκτίμηση των καταστάσεων του συστήματος, τη δημιουργία εντολών ελέγχου και την ενεργοποίηση των ενεργειών ελέγχου, όπως φαίνεται στο Σχ. 1 .

Οι FDI μπορούν να προκαλέσουν τη δημιουργία ακατάλληλων εντολών ελέγχου στοχεύοντας άμεσα την οικονομική αποστολή. Τα λανθασμένα δεδομένα φορτίου εγχέονται σε οικονομική αποστολή με περιορισμούς ασφαλείας, γεγονός που προκαλεί τις ροές γραμμής να υπερβούν το όριο ενεργοποίησης υπερφόρτωσης, οδηγώντας σε διακοπή γραμμής και ακόμη και σε καταρράκτη αστοχία. Η οικονομική αποστολή επηρεάζεται σκόπιμα για την αύξηση του λειτουργικού κόστους ή για την απόκτηση παράνομου κέρδους από τις αγορές ηλεκτρικής ενέργειας. Οι FDI μπορούν επίσης να διεισδύσουν σε ένα ΣΗΕ επιτιθέμενοι στη μέτρηση και την εκτίμηση της κατάστασης του συστήματος και να προκαλέσουν βλάβη στην ακεραιότητα των πληροφοριών κατάστασης του συστήματος ισχύος. Οι FDI χρησιμοποιούνται ως εργαλείο για την

επίθεση στο σύστημα εποπτικού ελέγχου και απόκτησης δεδομένων (SCADA), ενώ περαιτέρω εισάγονται ψευδή δεδομένα στη μονάδα μέτρησης φάσης (PMU) για να παραπλανηθεί το κέντρο ελέγχου. Με αυτόν τον τρόπο, οι επιτιθέμενοι στον κυβερνοχώρο μπορούν να επηρεάσουν την ορατότητα του χειριστή στην πραγματική κατάσταση λειτουργίας του συστήματος, με αποτέλεσμα να αποτύχει ο χειριστής να λάβει τα κατάλληλα αντίμετρα. Μάλιστα, οι FDI χρησιμοποιούνται για την πρόκληση αυθαίρετων σφαλμάτων εκτίμησης του εκτιμητή κατάστασης, ενώ οι FDI εφαρμόζονται στη μη γραμμική εκτίμηση κατάστασης του ΣΗΕ και συζητούνται τα αντίστοιχα αντίμετρα. Επιπλέον, οι FDI μπορούν να τροποποιήσουν την είσοδο ελέγχου για το σύστημα, με αποτέλεσμα να επιδεινώνεται η σταθερότητα του συστήματος ισχύος. Το σήμα εισόδου για μια ακολούθως κατανεμημένη γεννήτρια έχει καταστραφεί από FDI, προκαλώντας τη διαφωνία μιας ομάδας κατανεμημένων γεννητριών. Οι FDI χρησιμοποιούνται για την πρόκληση ενός προβλήματος συγχρονισμού για νησιωτικά μικροδίκτυα, ενώ οι διακόπτες συστήματος ελέγχονται για να προκαλούν αστάθεια, και τα κέρδη των συσκευών ελέγχου τάσης μεταβάλλονται για να εκκινήσουν παροδική αστάθεια. Περαιτέρω, μια κακόβουλη επίθεση υλοποιείται μέσω προσομοίωσης ελέγχου αδράνειας για να προκαλέσει αστάθεια της συχνότητας του συστήματος.

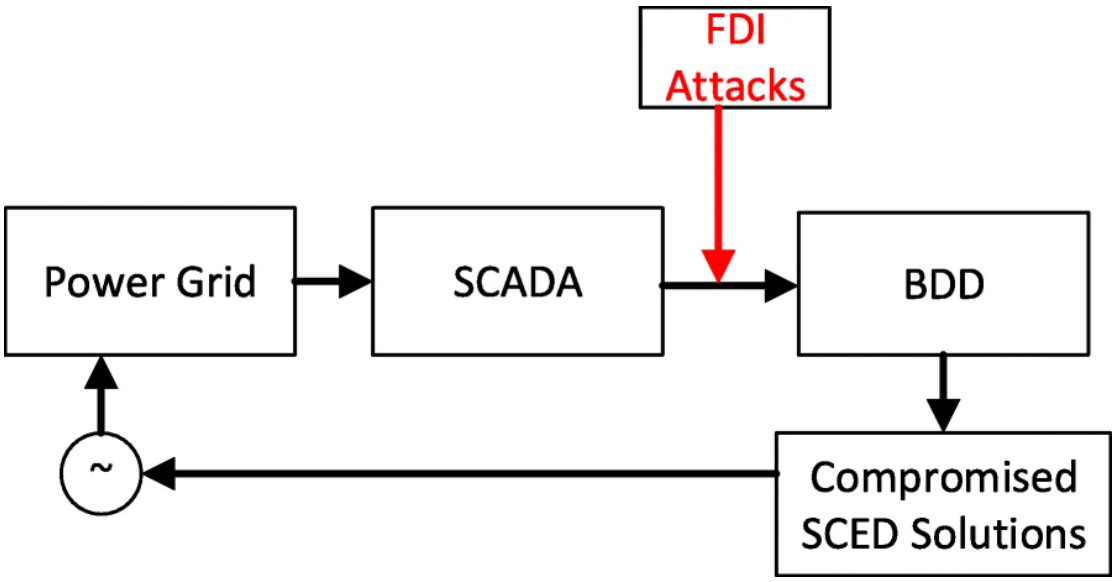


Εικόνα 1: Κυβερνο-επιθέσεις σε ένα σύστημα ηλεκτρικής ισχύος.

Προς το παρόν, η έρευνα για τον αντίκτυπο των FDI βασίζεται κυρίως στο μοντέλο FDI με ένα στιγμιότυπο ή/και στο μοντέλο του συστήματος ηλεκτρικής ενέργειας σταθερής κατάστασης, ενώ η έρευνα που εξετάζει τη μεταβατική διαδικασία ενός συστήματος ηλεκτρικής ενέργειας δεν είναι ενδελεχής και ολοκληρωμένη. Για να αποφευχθεί ο εντοπισμός ή η μείωση της κατανάλωσης ενέργειας κατά τη διαδικασία επίθεσης, οι έξυπνοι εισβολείς μπορούν να αλλάξουν τα δεδομένα που εισάγονται σε κάθε στιγμή επίθεσης. Η χρήση του μοντέλου συστήματος ηλεκτρικής ενέργειας σταθερής κατάστασης δεν είναι επίσης επαρκής για την ανάλυση του κινδύνου των FDI, καθώς τα πραγματικά συστήματα ισχύος είναι δικτυωμένα συστήματα ελέγχου. Παρόλο που η εκτίμηση της κατάστασης του συστήματος και η οικονομική αποστολή είναι ανθεκτικά στις FDI, οι επιτιθέμενοι μπορούν να διακόψουν την ασφαλή λειτουργία του συστήματος ισχύος επιτιθέμενοι στο αυτόματο σύστημα ελέγχου παραγωγής.

Για να αποκαλυφθεί ο κίνδυνος των FDI με ολοκληρωμένο τρόπο, η παρούσα εργασία εξετάζει την έρευνα σχετικά με τις επιθέσεις FDI στην οικονομική αποστολή, την εκτίμηση κατάστασης και τη δυναμική σταθερότητα των ΣΗΕ, όπως φαίνεται στο Σχ.1.

Σε ένα πραγματικό ΣΗΕ, οι γεννήτριες αποστέλλονται κάθε 5-15 λεπτά για να ελαχιστοποιηθεί το λειτουργικό κόστος. Τα δεδομένα φορτίου που υιοθετήθηκαν για οικονομική αποστολή με περιορισμούς ασφαλείας (Security Constraint Economic Dispatch-SCED) προέρχονται από τη βραχυπρόθεσμη πρόβλεψη φορτίου, η οποία χρησιμοποιεί τιμές μέτρησης ιστορικού φορτίου ή/και πραγματικού χρόνου ως είσοδο. Τα ψευδή δεδομένα που μπορούν να περάσουν την ανίχνευση κακών δεδομένων (BDD) μπορούν να εγχυθούν σκόπιμα για να τροποποιήσουν τις πληροφορίες φορτίου για το SCED και να τροποποιήσουν την επιβολή των ορίων ροής διακλάδωσης, όπως φαίνεται στο Σχ. 2 .



Εικόνα 2: Απεικόνιση επιθέσεων ΕΨΔ σε οικονομική αποστολή.

Έστω Δ D τα δεδομένα που εγχύθηκαν. Τα όρια για τις ροές γραμμής που επιβάλλονται από το SCED μπορούν να αντιπροσωπεύονται από [4, 5]:

$$P_{FDI} = S_F(K_P P^0 - K_D(D + \Delta D))$$

(1)

$$-r \leq P_{FDI} \leq r$$

(2)

όπου P FDI είναι το διάνυσμα ροής διακλάδωσης και D είναι το πραγματικό διάνυσμα φορτίου διαύλου. Τα K P και K D είναι οι πίνακες πρόσπτωσης γεννήτριας διαύλου και φορτίου διαύλου, αντίστοιχα. Το S F είναι ο πίνακας παράγοντα μετατόπισης παραγωγής και το r είναι η κανονική βαθμολογία χωρητικότητας των γραμμών. Επιπλέον, το πραγματικό φορτίο που χρησιμοποιείται στο SCED συμβολίζεται με D και η πραγματική ροή διακλάδωσης δίνεται ως:

$$P = \{S\}_F * (\{K\}_P * \{P\}^0 - \{K\}D * D) = \{P\}\{FDI\} + \{S\}_F * \{K\}_D * \Delta D$$

(3)

Ο συνδυασμός (1) και (3) δείχνει ότι η πραγματική ροή διακλάδωσης P ικανοποιεί τον περιορισμό ως:

$$r + S_F * K_D * \Delta D \leq P \leq r + S_F * K_D * \Delta D$$

(4)

Η εξίσωση (4) αποκαλύπτει ότι η πραγματική ροή γραμμής είναι μεγαλύτερη από τα όριά της, δηλαδή, $| P | \geq r$. Σε λειτουργία σε πραγματικό χρόνο, εάν μια γεννήτρια ακολουθήσει τις εντολές αποστολής που παράγονται από το SCED υπό επίθεση FDI, μπορεί να προκληθούν σοβαρές υπερφορτώσεις μετάδοσης, προκαλώντας ενέργειες ενεργοποίησης των συσκευών προστασίας.

Για να ξεκινήσει μια πρακτική επίθεση FDI, τα εγχυόμενα δεδομένα Δ D πρέπει να ικανοποιούν τους ακόλουθους περιορισμούς [6, 7]:

$$1^T \Delta D = 0$$

(5)

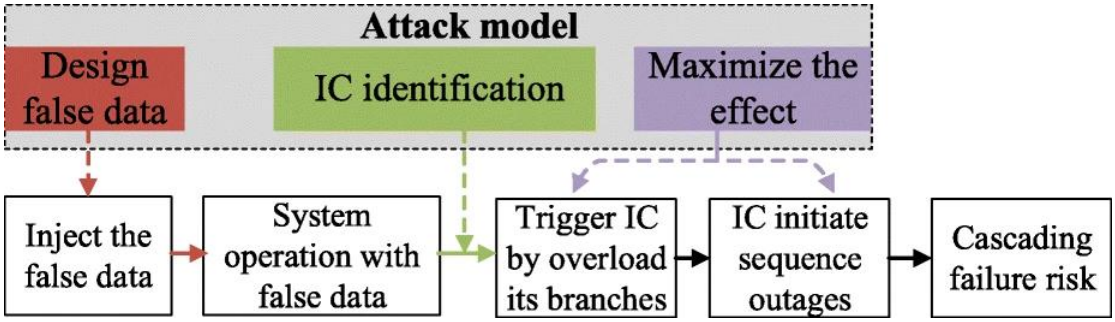
$$-\tau D \leq \Delta D \leq \tau D$$

(6)

Η εξίσωση (5) σημαίνει ότι το άθροισμα των αλλαγών του φορτίου είναι μηδέν για να εγγυηθεί το ισοζύγιο ισχύος, ενώ το (6) περιορίζει το μέγεθος της επίθεσης FDI σε έναν ζυγό φορτίου. Τέτοιοι περιορισμοί για μια επίθεση FDI χρησιμοποιούνται συνήθως στην υπάρχουσα βιβλιογραφία.

Το παραπάνω μοντέλο επίθεσης FDI αποκαλύπτει τους πιθανούς κινδύνους για την ασφαλή λειτουργία του συστήματος ισχύος, καθώς οι διακοπές ρεύματος σε ένα ηλεκτρικό δίκτυο προκαλούνται συνήθως από υπερφορτώσεις και διακοπές [21 , 22]. Όπως περιγράφεται στο [3], τρεις διαδοχικές απενεργοποιήσεις γραμμής μεταφοράς

και μετασχηματιστή ήταν οι κύριες αιτίες του Βορειοανατολικού Μπλακάουτ του 2003 και του Νοτιοδυτικού Μπλακάουτ του 2011, αντίστοιχα. Μόλις αναγνωριστεί ένα σύνολο κρίσιμων γραμμών που είναι γνωστό ως αρχικό ενδεχόμενο (IC) [24, 25], οι εισβολείς μπορούν σκόπιμα να προκαλέσουν αυτό το αρχικό ενδεχόμενο χρησιμοποιώντας μια επίθεση FDI. Δεδομένης της ικανότητας του IC, μπορούν να ξεκινήσουν διαδοχικές βλάβες και ακόμη και διαδοχικές αστοχίες, όπως φαίνεται στην Εικ. 3.



Εικόνα 3 Απεικόνιση κλιμακωτών αστοχιών που προκαλούνται απο FDI

1.2 Αύξηση του λειτουργικού κόστους που προκαλείται από επίθεση FDI

Οι εισβολείς μπορούν να αυξήσουν το λειτουργικό κόστος ενός συστήματος ισχύος διακόπτοντας το SCED και αλλάζοντας τα μεταδιδόμενα δεδομένα φορτίου. Το διάνυσμα επίθεσης μπορεί να βελτιστοποιηθεί μεγιστοποιώντας το λειτουργικό κόστος, το οποίο διαμορφώνεται ως πρόβλημα γραμμικού προγραμματισμού δύο επιπέδων ως:

$$c = \max_{\Delta D} c_g^T P + c_d^T J$$

(7)

$$\min_{P,J} c_g^T P + c_d^T J$$

(8)

$$1^T P = 1^T (DJ)$$

(9)

$$F = \{S\}\_F\{K\}\_PP - \{S\}\_F\{K\}\_D(D + \Delta DJ)$$

(10)

$$P_{\min} \leq P \leq P_{\max}$$

(11)

$$-f_{\max} \leq F \leq f_{\max}$$

(12)

$$0 \leq J \leq D + \Delta D$$

(13)

$$\Delta D\ (J \leq D + \Delta D).$$

(14)

όπου c g και c d είναι το διάνυσμα κόστους παραγωγής και απόρριψης φορτίου, αντίστοιχα. Το F είναι το υπολογισμένο διάνυσμα ροής γραμμής που περιέχει ψευδή δεδομένα, το f max είναι το διάνυσμα ορίου ροής διακλάδωσης και το J είναι το διάνυσμα απόρριψης φορτίου. Το P είναι το διάνυσμα ισχύος εξόδου της γεννήτριας και το P min και το P max είναι τα κάτω και άνω όρια για την έξοδο της γεννήτριας, αντίστοιχα.

Το ανώτερο επίπεδο (7), (8) δείχνει ότι τα ψευδή δεδομένα ΔD λαμβάνονται μεγιστοποιώντας την απόρριψη φορτίου μετά το SCED. Στο κατώτερο επίπεδο (9), (14), το λειτουργικό κόστος ελαχιστοποιείται με τα κατεστραμμένα δεδομένα φορτίου D + ΔD λαμβάνοντας υπόψη τα όρια ισχύος εξόδου της γεννήτριας (12), τα όρια ροής γραμμής μεταφοράς (13) και τα όρια απόρριψης φορτίου (14).

Οι μέθοδοι Karush-Kuhn-Tucker (KKT) και διπλής βάσης χρησιμοποιούνται ευρέως για την επίλυση του προαναφερθέντος προβλήματος βελτιστοποίησης δύο επιπέδων [4, 26]. Η προσέγγιση που βασίζεται στο KKT απαιτεί την εισαγωγή πρόσθετων

δυαδικών μεταβλητών για να σχηματιστούν οι λεγόμενοι περιορισμοί big-M, μειώνοντας την υπολογιστική απόδοση του αλγορίθμου. Όσον αφορά τη μέθοδο που βασίζεται στη δυαδικότητα, εμπλέκονται οι διγραμμικοί όροι των διπλών μεταβλητών και οι αντίστοιχες αρχικές μεταβλητές, και επομένως το πρόβλημα βελτιστοποίησης δεν είναι εύκολο να λυθεί.

Μια εναλλακτική λύση για τους εισβολείς για να κατασκευάσουν το διάνυσμα επίθεσης χρησιμοποιώντας μια γρήγορη προσέγγιση παρουσιάζεται στο [5]. Προκειμένου να αυξηθεί το λειτουργικό κόστος, τα επίπεδα φόρτωσης των κλάδων στο σετ Ω μεγιστοποιούνται μέσω της εισαγωγής ψευδών δεδομένων. Το προκύπτον πρόβλημα βελτιστοποίησης για τον προσδιορισμό των ψευδών δεδομένων Δ D περιγράφεται ως εξής:

$$\max_{\Delta D} \sum_{l \in \Omega} \delta_l \frac{-S_l K_D \Delta D}{f_l^{\max}}$$

(15)

$$h(\Delta D) \leq d$$

(16)

όπου l δηλώνει τη γραμμή μεταφοράς και S l είναι η l -η σειρά του SF .

Η αντικειμενική λειτουργία είναι η μεγιστοποίηση των επιπέδων φόρτωσης των γραμμών μεταφοράς στο σύνολο Ω. δ l = 1 εάν η ροή της ευθείας l είναι θετική, και δ l = − 1 διαφορετικά. Ο όρος − S l K D Δ D δηλώνει τη σταδιακή ροή ισχύος μέσω της γραμμής l που προκαλείται από τα εισαγόμενα ψευδή δεδομένα ΔD .

Τα λανθασμένα δεδομένα ΔD μπορούν να ληφθούν με την επίλυση του (15), βάσει του οποίου μπορεί εύκολα να λυθεί το πρόβλημα βελτιστοποίησης λειτουργικού κόστους (9) με περιορισμούς (10)–(14). Εφόσον το διάνυσμα επίθεσης καθορίζεται με την επίλυση του προβλήματος γραμμικού προγραμματισμού (15), ο χρόνος εκτέλεσης μειώνεται σημαντικά σε σύγκριση με τις προσεγγίσεις που βασίζονται στο KKT.

1.3 Εκτίμηση κατάστασης επιθέσεων στο σύστημα ηλεκτρικής ενέργειας

Για ένα σύγχρονο σύστημα ισχύος, πολλές έξυπνες συσκευές έχουν αναπτυχθεί για την απόκτηση δεδομένων σε πραγματικό χρόνο που σχετίζονται με τη λειτουργία του. Με την εκμετάλλευση αυτών των δεδομένων μέτρησης, οι χειριστές μπορούν να παρακολουθούν την κατάσταση λειτουργίας του συστήματος και να λαμβάνουν αποτελεσματικά μέτρα για τον μετριασμό των πιθανών κινδύνων. Ωστόσο, οι μετρήσεις πρέπει να μεταδοθούν στο κέντρο ελέγχου μέσω συνδέσεων επικοινωνίας και, ως εκ τούτου, τα συστήματα ισχύος αντιμετωπίζουν πιθανές επιθέσεις στον κυβερνοχώρο λόγω της ευπάθειας των τεχνολογιών επικοινωνίας. Για παράδειγμα, ένας κακόβουλος παράγοντας μπορεί να εισάγει ψευδή δεδομένα για να παρακινήσει τους χειριστές να λάβουν λάθος απόφαση σχετικά με την κατάσταση του συστήματος.

1.4 Επίθεση FDI με πλήρεις πληροφορίες δικτύου

Οι μετρήσεις χρησιμοποιούνται για την εκτίμηση της κατάστασης του συστήματος και λόγω της ύπαρξης σφαλμάτων μέτρησης, οι χειριστές προκαθορίζουν ένα όριο για τον εντοπισμό κακών δεδομένων. Σε περίπτωση υπέρβασης του ορίου, οι μετρήσεις θεωρούνται κακά δεδομένα. Ως εκ τούτου, εάν οι εισβολείς θέλουν να εξαπολύσουν μια επιτυχημένη επίθεση από FDI, τα εισαγόμενα ψευδή δεδομένα πρέπει να περάσουν τον εντοπισμό κακών δεδομένων. Η εκτίμηση της κατάστασης του συστήματος ισχύος μπορεί να εκφραστεί ως [11]:

$$\frac{d}{d\hat{x}} \|z - H\hat{x}\|_2 = 0$$

(17)

όπου x είναι το διάνυσμα κατάστασης και h{x} είναι το εκτιμώμενο διάνυσμα κατάστασης. z είναι η κατάσταση μέτρησης, Η ο Ιακωβιανός πίνακας του συστήματος ισχύος και ‖ · ‖ 2 ο Ευκλείδειος κανόνας.

Για τον εντοπισμό κακών δεδομένων, το υπόλειμμα r ορίζεται ως:

$$r = \|z - Hx\|_2$$

(18)

Ο όρος στη δεξιά πλευρά του (18) υποδηλώνει τη διαφορά μεταξύ των μετρούμενων και των πραγματικών τιμών. Αυτή η διαφορά προκαλείται από σφάλματα μέτρησης και διακοπές. Ένα όριο για το r είναι προκαθορισμένο από τον χειριστή και τα δεδομένα θεωρούνται κακά εάν ξεπεραστεί το όριο.

Για λόγους απεικόνισης, ένα ηλεκτρικό δίκτυο χωρίζεται σε περιοχές A και N με ένα σύνολο γραμμών σύνδεσης μεταξύ τους, ενώ οι μετρήσεις στην περιοχή A υποτίθεται ότι έχουν δεχτεί επίθεση από μια κακόβουλη οντότητα. Το διάνυσμα μέτρησης z αποσυντίθεται σε z 1 και z 2 , όπου το z 1 περιέχει όλες τις μετρήσεις στην στοχευόμενη περιοχή A χωρίς τις μετρήσεις ροής ισχύος στις γραμμές σύνδεσης και το z 2 συλλέγει τις υπόλοιπες μετρήσεις στην περιοχή A . Ομοίως, το διάνυσμα κατάστασης x χωρίζεται σε x 1 καιx 2 , όπου το x 1 συλλέγει όλα τα λεωφορεία στη στοχευμένη περιοχή A χωρίς τους οριακούς διαύλους και το x 2 περιέχει τα υπόλοιπα λεωφορεία.

Για να επιτεθούν στις μετρήσεις στην περιοχή A , οι εισβολείς πρέπει να σχεδιάσουν ένα διάνυσμα επίθεσης για να περάσουν την ανίχνευση κακών δεδομένων στην εκτίμηση κατάστασης. Αυτό σημαίνει ότι τα ψευδή δεδομένα που εισάγονται από τους εισβολείς θα πρέπει να αποτρέψουν την υπέρβαση του ορίου της υπολειπόμενης εκτίμησης κατάστασης. Ελλείψει των εγχυόμενων ψευδών δεδομένων, τα σφάλματα μέτρησης συμβάλλουν στο υπόλοιπο. Εάν οι μετρήσεις είναι χωρίς θόρυβο, το υπόλοιπο είναι ίσο ή κοντά στο μηδέν. Στην πραγματικότητα, η ανακρίβεια της μέτρησης προκαλεί ασυνεπείς μετρήσεις, οδηγώντας σε αύξηση του υπολειμματικού. Λιγότερη συνέπεια της μέτρησης συνεπάγεται υψηλότερο υπόλοιπο. Οι έξυπνοι εισβολείς ενδέχεται να κατασκευάσουν ψευδή δεδομένα που είναι σύμφωνα με τη φυσική ιδιότητα του συστήματος ισχύος.

Επομένως, τα ψευδή δεδομένα $z_1' = \frac{dz_1}{dt}$ που σχεδιάστηκαν από τους επιτιθέμενους είναι πιθανό να ακολουθούν τον νόμο περί ρεύματος του Kirchhoff (KCL) και τον νόμο τάσης του Kirchhoff (KVL), που δίνονται από:

$$z_1', x_1, \hat{x}_2, H_{11}, \text{and } H_{12}.$$

(19)

Οι μετρήσεις στην περιοχή χωρίς επίθεση παραμένουν αμετάβλητες.

Οι επιθετικοί μηχανισμοί των FDI στην εκτίμηση της κατάστασης του συστήματος ισχύος έχουν αποσαφηνιστεί στα άρθρα [8 , 9 , 10 , 12 , 13 , 14 , 15]. Όταν τα ψευδή δεδομένα δεν εισάγονται, η εξίσωση εκτίμησης κατάστασης δίνεται από:

$$\begin{bmatrix} z_1 \\ z_2 \end{bmatrix} = \begin{bmatrix} H_{11} & H_{12} \\ 0 & H_{22} \end{bmatrix} \begin{bmatrix} \hat{x}_1 \\ \hat{x}_2 \end{bmatrix} + \begin{bmatrix} e_1 \\ e_2 \end{bmatrix}$$

(20)

όπου e 1 και e 2 είναι τα σφάλματα μέτρησης των z 1 και z 2 , αντίστοιχα. Μπορεί να φανεί ότι το z 2 είναι μόνο συνάρτηση του x 2 . Στην περίπτωση εκτίμησης κατάστασης DC, τα H 11 , H 12 και H 22 είναι σταθερά, ενώ είναι συναρτήσεις του διανύσματος κατάστασης στην εκτίμηση κατάστασης AC. Όταν εισάγονται τα ψευδή δεδομένα, η μέτρηση z 1 αντικαθίσταται από το διάνυσμα επίθεσης $z_1' = \frac{dz_1}{dt}$. Τότε το υπόλοιπο αντιπροσωπεύεται από:

$$r' = \min \|z' - Hx'\|_2$$

(21)

Για να λάβετε μια εφικτή εκτίμηση του διανύσματος κατάστασης, πρέπει να ικανοποιηθεί ο ακόλουθος περιορισμός:

$$z' - (H_{11}x_1 + H_{12}\hat{x}_2)$$
$$z_2 - H_{22}\hat{x}_2$$

(22)

Η εξίσωση (22) αντικατοπτρίζει τη μείωση του συνολικού υπολείμματος καθώς εισάγονται τα ψευδή δεδομένα. Αυτό μπορεί να εξηγηθεί από το γεγονός ότι τα ψευδή δεδομένα που εγχύονται στην περιοχή επίθεσης υπακούουν στα KCL και KVL και ως εκ τούτου έχουν καλύτερη συνέπεια από τις αρχικές μετρήσεις. Θα πρέπει να διευκρινιστεί ότι το μειωμένο υπόλοιπο υπό επίθεση FDI δεν σημαίνει απαραίτητα ότι τα ψευδή δεδομένα είναι κοντά στην πραγματική τιμή [11]. Στην πραγματικότητα, οι επιτιθέμενοι μπορούν ταυτόχρονα να προκαλέσουν σοβαρές διαταραχές διατηρώντας ένα μικρό υπόλοιπο από τις FDI.

Για την κατασκευή του διανύσματος επίθεσης στο (19), οι ροές γραμμής στην περιοχή επίθεσης υπολογίζονται από:

$$p_{ij} = V_i^2 g_{ij} - V_i V_j \left(g_{ij}\cos(\theta_i - \theta_j) + b_{ij}\sin(\theta_i - \theta_j)\right)$$

(23)

$$q_{ij} = -V_i^2 b_{ij} - V_i V_j (g_{ij}\sin(\theta_i - \theta_j) - b_{ij}\cos(\theta_i - \theta_j))$$

(24)

όπου V i είναι το μέγεθος της τάσης στο ζυγό i . Τα b ij και g ij είναι η επιρροή και η αγωγιμότητα μεταξύ της γραμμής i - j , αντίστοιχα. Τα p ij και q ij είναι οι ροές ενεργού και αέργου ισχύος μεταξύ της γραμμής i - j .

Εφόσον το KCL εφαρμόζεται στο (19) για τους μη οριακούς διαύλους στην περιοχή επίθεσης, το αλγεβρικό άθροισμα των ροών των γραμμών που συνδέονται σε ένα ζυγό ισούται με την ισχύ που εγχέεται σε αυτόν τον ζυγό. Για τα οριακά λεωφορεία στην

περιοχή επίθεσης, τμήματα των γραμμών που συνδέονται με αυτό το λεωφορείο ανήκουν στην περιοχή χωρίς επίθεση (βλ. Εικ. 4). Επομένως, οι εξισώσεις ισοζυγίου ισχύος που προκύπτουν εκφράζονται ως:

$$p_i + \sum_{j \in S_{i,A}} p_{ij} + \sum_{j \in S_{i,N}} \hat{p}_{ij}:$$

(25)

$$p_i + \sum_{j \in S_{i,A}} p_{ij} + \sum_{j \in S_{i,N}} \hat{p}_{ij}:$$

(26)

$$\hat{V}_i \hat{V}_j \left(g_{ij} \cos(\hat{\theta}_i - \hat{\theta}_j) + b_{ij} \sin(\hat{\theta}_i - \hat{\theta}_j) \right):$$

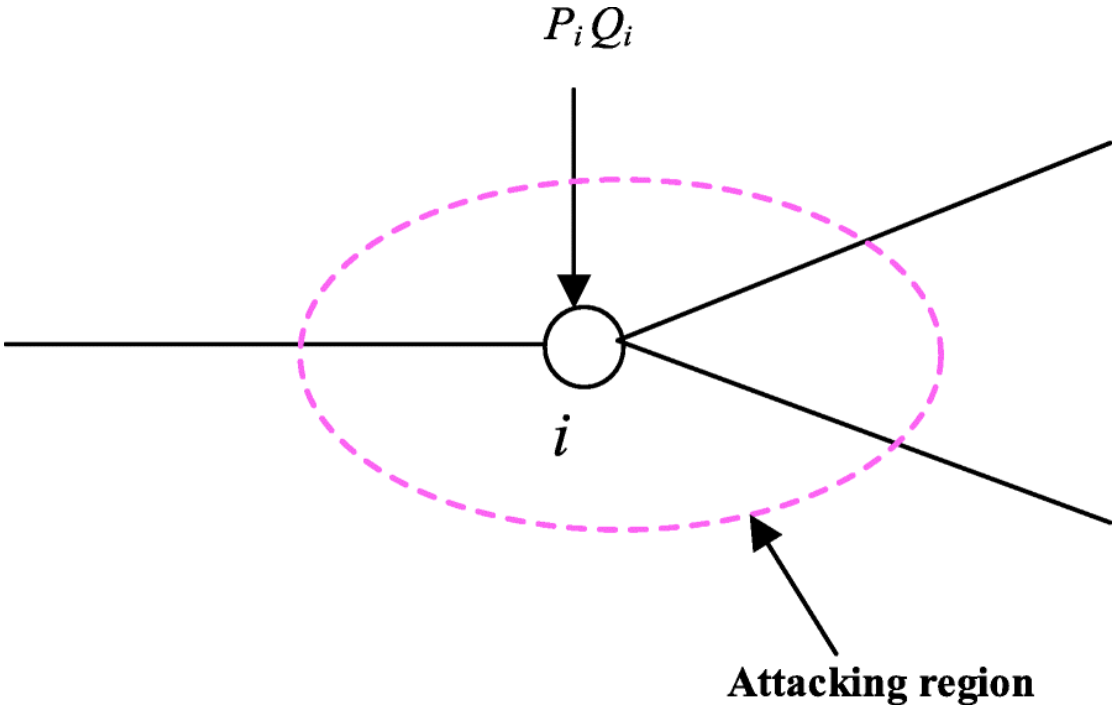
(27)

$$-\hat{V}_i \hat{V}_j \left(g_{ij} \sin(\hat{\theta}_i - \hat{\theta}_j) - b_{ij} \cos(\hat{\theta}_i - \hat{\theta}_j) \right)$$

(28)

όπου p i και q i είναι η ενεργός και άεργος ισχύς που εγχέεται στον ζυγό i . Τα p ij και q ij είναι οι ροές ενεργού και άεργου ισχύος της γραμμής i - j έξω από την περιοχή

επίθεσης.



Εικόνα 4. Ένα ζυγός οριοθέτησης στην επιτιθέμενη περιοχή

Από τις (27) και (28), βλέπουμε ότι οι μετρήσεις στην περιοχή χωρίς επίθεση δεν επιτίθενται. Έτσι, στις (25) και (26) είναι από τις δεδομένες τιμές, οι οποίες θα αλλάξουν στον Ιακωβιανό Πίνακα την ισχύ που εγχέεται στους οριακούς ζυγούς.

Ας σημειωθεί ότι το (17) έχει ως αποτέλεσμα τις μεταβλητές κατάστασης σε ένα στιγμιότυπο. Για να ληφθεί υπόψη η δυναμική συμπεριφορά των FDI, (17) μπορεί εύκολα να αναδιατυπωθεί ως άθροισμα z − Hx σε στιγμιότυπα T και το προκύπτον πρόβλημα βελτιστοποίησης μπορεί να λυθεί με παρόμοιο τρόπο. Οι λεπτομέρειες βρίσκονται στο [27].

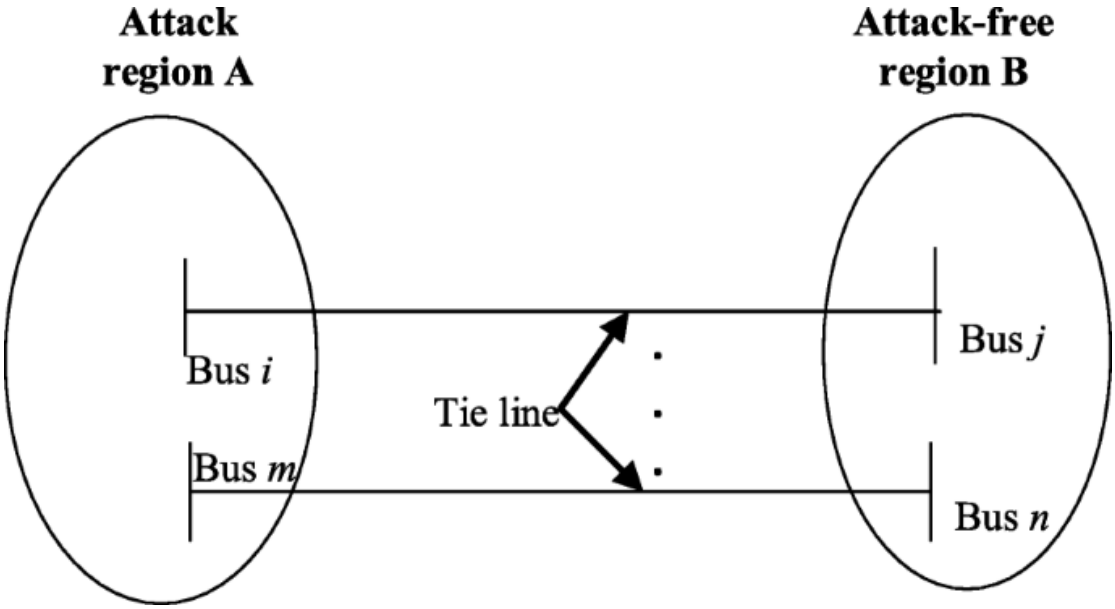
1.5 Επίθεση FDI με ελλιπείς πληροφορίες δικτύου

Η εξίσωση (19) δείχνει ότι το κατασκευασμένο διάνυσμα επίθεσης εξαρτάται από τις εκτιμήσεις των μεγεθών τάσης και των γωνιών φάσης των οριακών ζυγών στην περιοχή επίθεσης. Απαιτεί επίσης από τους εισβολείς να έχουν τις πληροφορίες τοπολογίας ολόκληρου του δικτύου ισχύος καθώς και τις παραμέτρους γραμμής [8,9,10,12,13,14 ,15]. Ωστόσο, οι πληροφορίες δικτύου ενός ηλεκτρικού δικτύου είναι εμπιστευτικές και οι εισβολείς είναι πιθανό να δυσκολευτούν να το αποκτήσουν. Επιπλέον, υπάρχουν

χιλιάδες ζυγοί και γραμμές σε ένα σύγχρονο σύστημα ηλεκτρικής ενέργειας. Αυτό σημαίνει ότι οι εισβολείς πρέπει να ασχοληθούν με εκτενείς πληροφορίες σχετικά με την τοπολογία του δικτύου. Επομένως, η υπόθεση ότι οι εισβολείς είναι σε θέση να αποκτήσουν τις εκτιμώμενες τιμές από την εκτίμηση κατάστασης δεν είναι πρακτική.

Για να κατασκευαστεί ένα πρακτικό μοντέλο επίθεσης έναντι εκτίμησης κατάστασης, οι παραπάνω συνθήκες είναι χαλαρές στο [11], στο οποίο το μοντέλο έγχυσης ψευδών δεδομένων απαιτεί μόνο τις πληροφορίες δικτύου της περιοχής επίθεσης (βλ. Εικ. 5) και όχι αυτού ολόκληρου του δικτύου ισχύος . Επιπλέον, το διάνυσμα επίθεσης στο [11] δεν βασίζεται άμεσα στις εκτιμήσεις των γωνιών φάσης αλλά μάλλον στις διαφορές γωνίας των γραμμών. Το μοντέλο επίθεσης FDI που χρησιμοποιείται στο [11] επαναδιατυπώνεται με τα ακόλουθα βήματα:

1) Αντικαταστήστε τις μετρούμενες τάσεις για τις εκτιμήσεις των μεγεθών τάσης στους οριακούς διαύλους στην περιοχή επίθεσης.
2) Αντικαταστήστε τις εκτιμήσεις των μεγεθών τάσης και των γωνιών φάσης με τις αντίστοιχες μετρήσεις για να προσδιορίσετε τις ροές στις γραμμές σύνδεσης.



Εικόνα 5. Ένα σύστημα ισχύος που αποσυντίθεται σε περιοχές χωρίς επίθεση και επιθέσεις

Κάνοντας τα παραπάνω, η εκτιμώμενη κατάσταση του συστήματος δεν απαιτείται πλέον στο σχεδιασμό του διανύσματος επίθεσης. Οι γωνίες φάσης στους οριακούς διαύλους στην περιοχή επίθεσης παίζουν ουσιαστικό ρόλο στην εφαρμογή του αναφερόμενου μοντέλου επίθεσης. Παρόλο που οι μετρήσεις των γωνιών φάσης είναι προσβάσιμες από το PMU, αυτό θα απαιτούσε την ανάπτυξη επαρκών PMU για την παροχή αυτών των πληροφοριών, και τέτοιες λύσεις μπορεί να είναι δύσκολο να κλιμακωθούν. Για να ξεκινήσει με επιτυχία μια επίθεση FDI σε ένα σύστημα ισχύος χωρίς επαρκή δεδομένα PMU, είναι επιθυμητό για τους εισβολείς να κατασκευάσουν ένα πιο πρακτικό μοντέλο επίθεσης χωρίς να απαιτούν τις μετρούμενες τιμές των γωνιών φάσης. Από την οπτική γωνία του αμυνόμενου, είναι επίσης υψίστης σημασίας να διερευνηθεί η πιθανότητα επίθεσης στην εκτίμηση κατάστασης χρησιμοποιώντας ένα τέτοιο μοντέλο επίθεσης.

Σύμφωνα με τις (23) και (24), η ροή γραμμής σε ένα σύστημα ισχύος υπολογίζεται χρησιμοποιώντας τη διαφορά γωνίας της γραμμής. Εάν είναι γνωστές οι διαφορές γωνίας μεταξύ των γραμμών, μπορούν να προσδιοριστούν οι ροές γραμμής. Αυτό σημαίνει ότι οι πραγματικές γωνίες φάσης στους οριακούς διαύλους δεν απαιτούνται για τον προσδιορισμό των ροών γραμμής και οι διαφορές γωνίας της γραμμής μπορούν να χρησιμοποιηθούν για τον υπολογισμό του διανύσματος επίθεσης στο (19) ακόμη και απουσία πραγματικών γωνιών φάσης διαύλου. Το παρακάτω διερευνά πώς να χρησιμοποιήσουμε διαφορές γωνίας γραμμής αντί για γωνίες φάσης διαύλου για να σχεδιάσουμε το διάνυσμα επίθεσης. Η εξίσωση (19) υπονοεί ότι οι γωνίες φάσης στους οριακούς διαύλους είναι σταθερές στις εκτιμήσεις του εκτιμητή κατάστασης. Αντίστοιχα, οι διαφορές γωνίας μεταξύ των λεωφορείων είναι επίσης σταθερές. Θεωρώντας την πραγματικά εκτιμώμενη γωνία φάσης στο ζυγό, ισχύει η ακόλουθη έκφραση:

$$\hat{\theta}_i - \hat{\theta}_j = \left(\hat{\theta}_i + \alpha\right) - \left(\hat{\theta}_j + \alpha\right)$$

(29)

Η εξίσωση (29) δείχνει ότι όταν οι γωνίες φάσης δύο οριακών διαύλων αλλάζουν κατά α, η αντίστοιχη διαφορά γωνίας παραμένει αμετάβλητη. Έτσι, οι γωνίες φάσης που χρησιμοποιούνται για τον υπολογισμό του διανύσματος επίθεσης μπορούν να ληφθούν με τα ακόλουθα βήματα [11]:

Βήμα 1. Επιλέξτε μια αυθαίρετη τιμή για έναν οριακό ζυγό.

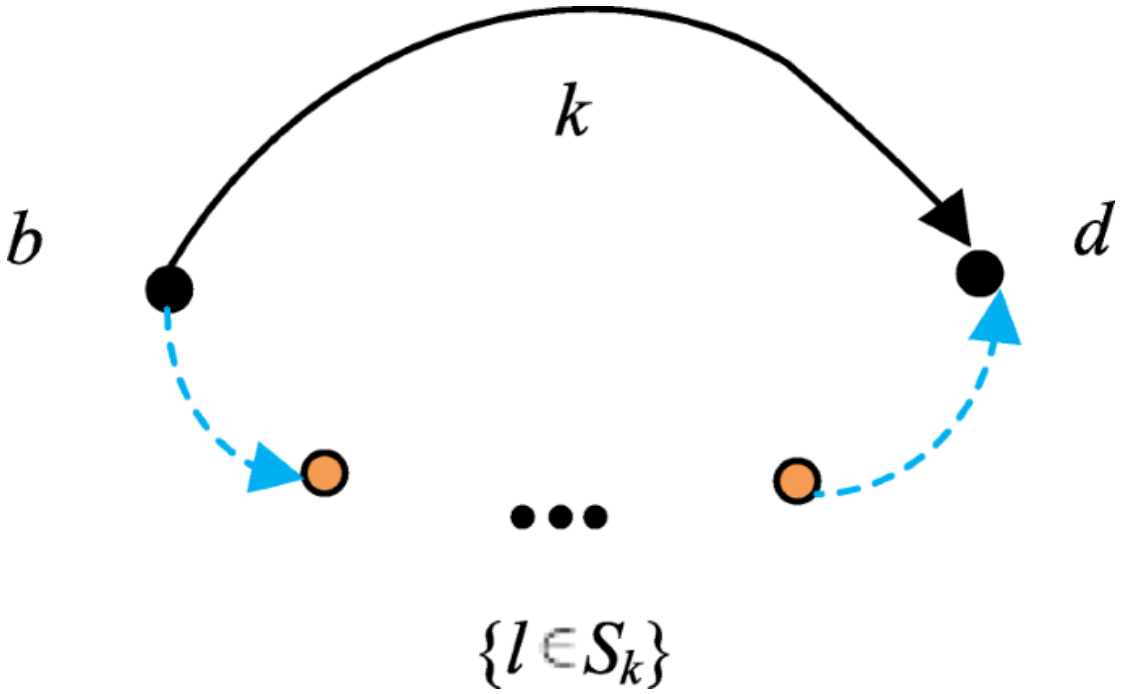
Βήμα 2. Επιλέξτε τις γωνίες φάσης για τους υπόλοιπους οριακούς διαύλους με βάση τις διαφορές γωνιών.

Λόγω της τυχαίας τιμής για τον οριακό ζυγό, οι γωνίες φάσης που λαμβάνονται από τα παραπάνω βήματα δεν αντιπροσωπεύουν τις πραγματικές. Ωστόσο, οι διαφορές γωνίας είναι ίδιες με τις πραγματικές, και έτσι οι ροές γραμμής παραμένουν αμετάβλητες. Επομένως, δεν υπάρχει ανάγκη για τους εισβολείς να αποκτήσουν τις πραγματικές τιμές των εκτιμώμενων γωνιών φάσης για να κατασκευάσουν το διάνυσμα επίθεσης και οι μόνες πληροφορίες που χρειάζονται είναι οι διαφορές των εκτιμώμενων γωνιών φάσης.

Υποθέτοντας ότι υπάρχει μια διαδρομή k που συνδέει δύο γειτονικούς διαύλους, όπως φαίνεται στο Σχ. 6 , μπορεί να αποδειχθεί ότι η ακόλουθη εξίσωση ισχύει για μια καθορισμένη κατεύθυνση:

$$\sum_{l \in S_k} \delta_l = \theta_b - \theta_d$$

(30)



Εικόνα 6. Ένα μονοπάτι που συνδέει δύο γειτονικά λεωφορεία

Από το (30), για τη διαδρομή { l ∈ S k } που συνδέει το ζυγό b και d , η διαφορά γωνίας μεταξύ των δύο διαύλων μπορεί να υπολογιστεί αθροίζοντας τις διαφορές γωνίας των γραμμών σε αυτή τη διαδρομή. Αυτό σημαίνει ότι οι επιτιθέμενοι δεν χρειάζεται να αποκτήσουν τις πραγματικές τιμές των εκτιμώμενων γωνιών φάσης στους οριακούς διαύλους. Για τον υπολογισμό της διαφοράς γωνίας χωρίς γνώση των πραγματικών γωνιών φάσης, λαμβάνονται υπόψη οι ακόλουθες προσεγγίσεις:

$$\begin{aligned}&\cos(\theta_i-\theta_j)\approx 1,\\&\sin(\theta_i-\theta_j)\approx \theta_i-\theta_j,\\&V_i\approx V_j\approx 1.\end{aligned}$$

(31)

Η αντικατάσταση του (31) σε (27) αποδίδει

$$p_{ij}\approx\frac{\theta_i-\theta_j}{x_{ij}}$$

(32)

Έτσι, η διαφορά γωνίας μπορεί να υπολογιστεί ως εξής:

$$\theta_i - \theta_j \approx x_{ij} p_{ij}$$

(33)

Η εξίσωση (33) δείχνει ότι η μέτρηση ισχύος γραμμής μπορεί να χρησιμοποιηθεί για τον υπολογισμό της διαφοράς γωνίας, ενώ το σφάλμα της διαφοράς γωνίας προκαλείται εν μέρει από τη χρήση των προσεγγίσεων στο (31). Επομένως, η ακρίβεια της διαφοράς γωνίας που προκύπτει από το (33) εξαρτάται από τις συνθήκες υπό τις οποίες ισχύει το (31). Είναι γνωστό ότι η διαφορά μειώνεται με την αύξηση του λόγου X/R μιας γραμμής. Έτσι, για να μειωθεί το σφάλμα που προκαλείται από το (31), μια βέλτιστη διαδρομή k στην περιοχή επίθεσης προσδιορίζεται μεγιστοποιώντας τη μέση αναλογία X/R του ρk ως [11]:

$$\begin{bmatrix} \theta \\ V \end{bmatrix} = \begin{bmatrix} \theta_0 \\ V_0 \end{bmatrix}$$

(34)

Όπως φαίνεται στο (22), για να αποφευχθεί η ανίχνευση από την ανίχνευση κακών δεδομένων, το συνολικό υπόλοιπο με τα εισαγόμενα ψευδή δεδομένα θα πρέπει να είναι μικρότερο από το προκαθορισμένο όριο. Επομένως, τα ψευδή δεδομένα μετά τα KCL και KVL εγχέονται στην περιοχή επίθεσης, ενώ οι ροές γραμμής υπολογίζονται από τα (23) και (24). Η εγχυόμενη ισχύς στον μη οριακό ζυγό είναι το άθροισμα των ροών στις γραμμές που συνδέονται με αυτόν τον ζυγό, ενώ η εγχυόμενη ισχύς στους οριακούς διαύλους λαμβάνεται από τα (25) και (26). Ο παρουσιαζόμενος αλγόριθμος για την κατασκευή του διανύσματος επίθεσης μπορεί να συνοψιστεί ως εξής.

Βήμα 1. Ορίστε τις αρχικές τιμές στο διάνυσμα κατάστασης ως

$$\begin{bmatrix} \theta \\ V \end{bmatrix} = \begin{bmatrix} \theta_0 \\ V_0 \end{bmatrix}$$

(35)

Βήμα 2. Λάβετε το διάνυσμα επίθεσης [pq PQ] T χρησιμοποιώντας το διάνυσμα τρέχουσας κατάστασης x = [θ V] T ;

Βήμα 3. Αξιολογήστε εάν η εγχυόμενη ισχύς σε ένα ζυγό και οι ροές ενεργού/ενεργού γραμμής περιορίζονται εντός και άνω ορίων, όπως:

$$\begin{cases} P_{\min} \le P \le P_{\max} \\ -p_{\max} \le p \le p_{\max} \\ -q_{\max} \le q \le q_{\max} \end{cases}$$

(36)

Αυτό μπορεί να μειώσει την πιθανότητα ανίχνευσης καθώς ο χειριστής μπορεί να έχει πρόσβαση στις πληροφορίες της διανομής ροής. Εάν ισχύουν οι συνθήκες, τερματίζεται. διαφορετικά, πηγαίνει στο επόμενο βήμα.

Βήμα 4. Υπολογίστε το αυξητικό Δ x = [Δ θ Δ V] T βελτιστοποιώντας την αντικειμενική συνάρτηση ως:

$$\min \sum_{t=1}^{10} 1^T S_t$$

(37)

$$\begin{bmatrix} \Delta p \\ \Delta q \\ \Delta P \\ \Delta Q \\ \Delta V \end{bmatrix} = \begin{bmatrix} H_1 & H_2 \\ H_3 & H_4 \\ H_5 & H_6 \\ H_7 & H_8 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} \Delta\theta \\ \Delta V \end{bmatrix}$$

όπου η χαλαρή μεταβλητή S t είναι μη αρνητική, και H 1 = ∂p / ∂θ , H 2 = ∂p / ∂V , H 3 = ∂q / ∂θ , H 4 = ∂q / ∂V , H 5 = ∂P / ∂θ , H 6 = ∂P / ∂V , H 7 = ∂Q / ∂θ , H 8 = ∂Q / ∂V . Οι εκφράσεις του H 1 - H 4 παρέχονται στο [28], ενώ οι εκφράσεις του H 5 - H 8 πρέπει να προσδιοριστούν. Το G αντιπροσωπεύει τη μήτρα μετάβασης που μετατρέπει το διάνυσμα γωνίας φάσης στο διάνυσμα διαφοράς γωνίας φάσης. Για τα οριακά λεωφορεία στην περιοχή επίθεσης, η χρήση του (26) οδηγεί σε:

$$(-g_{ij}\sin\theta_{ij} + b_{ij}\cos\theta_{ij})$$

(38)

Για τους μη οριακούς διαύλους στην περιοχή επίθεσης, οι μη μηδενικές εγγραφές μπορούν να προσδιοριστούν χρησιμοποιώντας παρόμοιο τρόπο με αυτόν που φαίνεται στο [28].

Βήμα 5. Ενημερώστε το διάνυσμα κατάστασης ως:

$$\begin{bmatrix} \theta \\ V \end{bmatrix} = \begin{bmatrix} \theta \\ V \end{bmatrix} + \begin{bmatrix} \Delta\theta \\ \Delta V \end{bmatrix}$$

(39)

και μετά επιστρέψτε στο Βήμα 2.

Χρησιμοποιώντας το Βήμα 1–5, οι εισβολείς μπορούν να επιτύχουν ένα διάνυσμα επίθεσης έναντι της εκτίμησης κατάστασης του συστήματος ισχύος. Αυτή η μέθοδος μπορεί να αποφύγει την ανίχνευση κακών δεδομένων, ενώ δεν απαιτεί πληροφορίες

σχετικά με την τοπολογία δικτύου ολόκληρου του συστήματος και τις γωνίες φάσης στους διαύλους.

1.6 Επιθέσεις στο σύστημα ελέγχου ισχύος

Το σύστημα ελέγχου ισχύος διαδραματίζει ζωτικό ρόλο στη διατήρηση της τροφοδοσίας σε ανταπόκριση στη ζήτηση των πελατών. Μια ανισορροπία μεταξύ προσφοράς και ζήτησης μπορεί να προκαλέσει αστάθεια της συχνότητας του συστήματος, απειλώντας τη λειτουργική ασφάλεια του συστήματος ηλεκτρικής ενέργειας. Ένα κεντρικό σύστημα ελέγχου χρησιμοποιείται συνήθως στα παραδοσιακά συστήματα ισχύος και το σχήμα περιλαμβάνει ένα ενιαίο κέντρο ελέγχου που συλλέγει πληροφορίες από και στέλνει εντολές ελέγχου σε όλους τους πράκτορες. Ωστόσο, μια τέτοια αρχιτεκτονική κεντρικού ελέγχου δεν ανταποκρίνεται πλέον στις ανάγκες των σημερινών συστημάτων ισχύος. Για παράδειγμα, οι γεωγραφικά διασκορπισμένες κατανεμημένες γεννήτριες ενσωματώνονται όλο και περισσότερο στο ηλεκτρικό δίκτυο. Αυτά δεν είναι κατάλληλα για συντονισμό από τον κεντρικό έλεγχο λόγω της απαίτησης λειτουργίας βύσματος και βύσματος [29 , 30]. Ο κεντρικός έλεγχος δεν εφαρμόζεται επίσης στη λειτουργία μικροδικτύου, όπου οι κατανεμημένες γεννήτριες απαιτούνται για την παροχή ρεύματος σε λειτουργία νησίδας [31]. Λόγω της αξιοπιστίας, της επεκτασιμότητας και της ευελιξίας του, ο κατανεμημένος έλεγχος προτιμάται έναντι του κεντρικού ελέγχου [32 , 33 , 34]. Ωστόσο, στον κατανεμημένο έλεγχο, οι τοπικοί ελεγκτές έχουν πρόσβαση σε τοπικές πληροφορίες και πληροφορίες για τους γείτονες και, ως εκ τούτου, είναι ευάλωτοι σε κυβερνοεπιθέσεις. Μια κακόβουλη οντότητα μπορεί να διακόψει την ανταλλαγή δεδομένων μεταξύ γειτονικών τοπικών ελεγκτών εξαπολύοντας επιθέσεις FDI [16 , 17 , 18 , 19 , 20].

1.7 Επίθεση FDI σε μονάδα διανεμημένης παραγωγής

Λαμβάνοντας υπόψη μια κατανεμημένη γεννήτρια βασισμένη σε μετατροπέα i , P i και P i, το μέγιστο είναι η ενεργή ισχύς εξόδου και η μέγιστη ισχύς, αντίστοιχα. Χρησιμοποιώντας τον μετασχηματισμό d - q, οι τάσεις των αξόνων d - και q - μπορούν να υπολογιστούν με U di = U i και U qi = 0. Υποθέτοντας ότι τα ρεύματα του άξονα d - και q - είναι I di και I qi , αντίστοιχα, τα ενεργά Η ισχύς εξόδου μπορεί να ληφθεί με:

$$P_i = U_{di} I_{di} + U_{qi} I_{qi} = U_i I_{di}$$

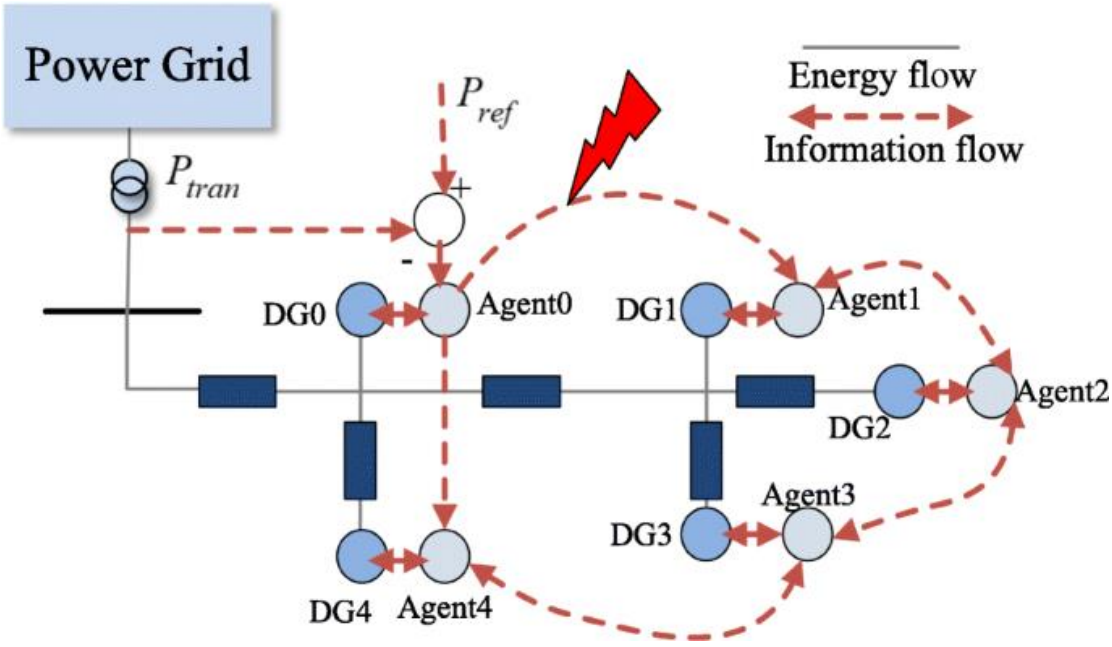
(40)

Εάν ο μετατροπέας ισχύος ελέγχεται από ένα σχήμα τροφοδοσίας δικτύου [31], το I di πρέπει να συγκλίνει στην τιμή αναφοράς του I di_ref σε μια περίοδο δειγματοληψίας T . Στην k η επανάληψη, το I di_ref μπορεί να προσδιοριστεί από

$$I_{di\_ref}(k) = \frac{P_{i,\max}\alpha_i(k)}{U_i(k)}$$

(41)

όπου η παράμετρος σχεδίασης α i υποδηλώνει την αναλογία χρήσης που ορίζεται από P i / P i, max . Όταν το I di συγκλίνει στο I di_ref στην k η επανάληψη, P i (k) = P i , max αi (k). Σύμφωνα με το (41), η ενεργός ισχύς εξόδου της κατανεμημένης γεννήτριας i μπορεί να ρυθμιστεί αλλάζοντας τον λόγο χρήσης α i . Δεδομένου ότι η ονομαστική ισχύς των κατανεμημένων γεννητριών που βασίζονται σε μετατροπείς είναι σχετικά μικρή, πολλαπλές κατανεμημένες γεννήτριες χρησιμοποιούνται σε ένα δίκτυο διανομής για αυξημένη χωρητικότητα. Ένα τέτοιο σύστημα μπορεί να θεωρηθεί ως εικονικό εργοστάσιο παραγωγής ενέργειας (VPP), όπως φαίνεται στο Σχ. 7 , όπου το P tran αντιπροσωπεύει τη συνολική ενεργή ισχύ που μεταδίδεται στο δίκτυο μεταφοράς.



Εικόνα 7. Ενδεικτικό διάγραμμα κατανεμημένου ελέγχου μονάδων διανεμημένης παραγωγής.

Για την παρακολούθηση της εντολής αποστολής P ref , η ομάδα των κατανεμημένων γεννητριών σε ένα VPP συντονίζεται χρησιμοποιώντας έναν συναινετικό αλγόριθμο αρχηγού-ακολούθου [16]:

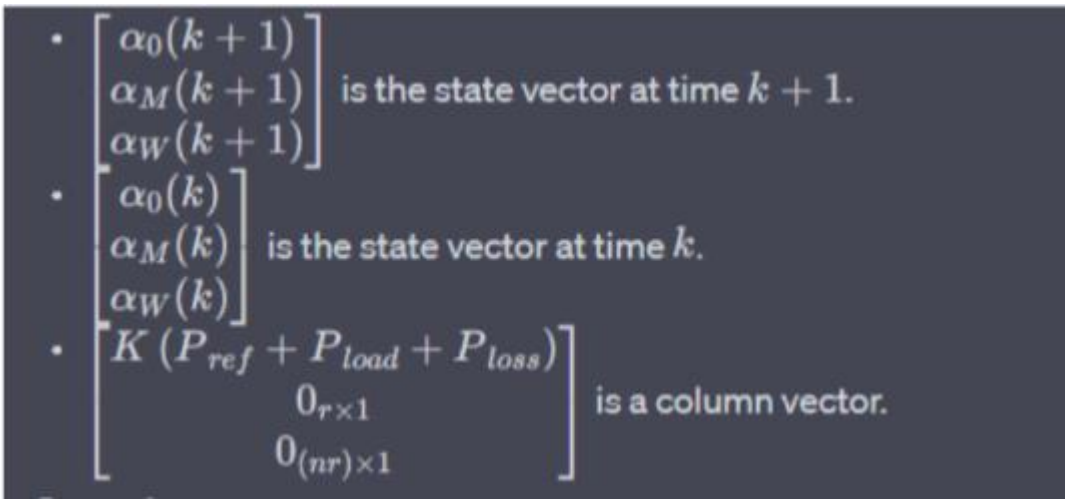
$$\alpha(k+1) = A\alpha(k) + BK\alpha(k) + KC$$

(42)

όπου α (k) = [α0(k), …, α n -1 (k)] T . B = [\(-{\hat{P}}_{\mathrm{max}} \) O n × (n -1)] T με \({\hat{P}}_{\mathrm{max}} \) =[P 0,max, …, P n -1,max] T και C = [P ref + P απώλεια + P φορτίο O 1 × (n-1)] T . A = [a ij] είναι ένας σταθμισμένος πίνακας με ij > 0. Το K είναι το κέρδος του ελεγκτή και το O είναι ο μηδενικός πίνακας. Το φορτίο P και η απώλεια P αντιπροσωπεύουν τη συνολική κατανάλωση ισχύος φορτίου και την απώλεια ισχύος στο VPP, αντίστοιχα. Επιλέγοντας τα σωστά A και K, μπορεί να αποδειχθεί η σύγκλιση του (4) [16]. Όταν επιτευχθεί σύγκλιση, οι δείκτες χρησιμοποίησης όλων των κατανεμημένων παραγωγών καταλήγουν σε συμφωνία καιΤο P tran κατευθύνεται στην προτιμώμενη τιμή του P ref .

Η εξίσωση (42) δείχνει ότι το δίκτυο επικοινωνίας μεταξύ των κατανεμημένων γεννητριών παίζει βασικό ρόλο στη ρύθμιση της ενεργού ισχύος εξόδου του VPP. Εάν ο τοπικός ελεγκτής μιας συγκεκριμένης κατανεμημένης γεννήτριας δεχθεί επίθεση από επιθέσεις FDI, ο λόγος χρήσης του θα αποτραπεί από τη σύγκλιση στη συναινετική τιμή, με αποτέλεσμα την αποτυχία παρακολούθησης του P tran στο P ref [35 , 36].

Οι εισβολείς μπορούν να επιτεθούν στον ελεγκτή μιας κατανεμημένης γεννήτριας εισάγοντας ψευδή δεδομένα στον ενεργοποιητή και αναγκάζοντάς τον να στείλει την ίδια εντολή ελέγχου στους γεωγραφικούς της γείτονες. Υποθέτοντας ότι r κατανεμημένες γεννήτριες υποβάλλονται σε επιθέσεις FDI και λαμβάνοντας υπόψη α M (k) ≡ α M = [αM ,. .., αM] T και α W (k) = [α r + 1 (k),. .., α r + n (k)] Τείναι τα διανύσματα αναλογίας χρήσης των κατανεμημένων γεννητριών με κακή συμπεριφορά και καλή συμπεριφορά, αντίστοιχα, ο αλγόριθμος (42) μπορεί να ξαναγραφτεί ως:

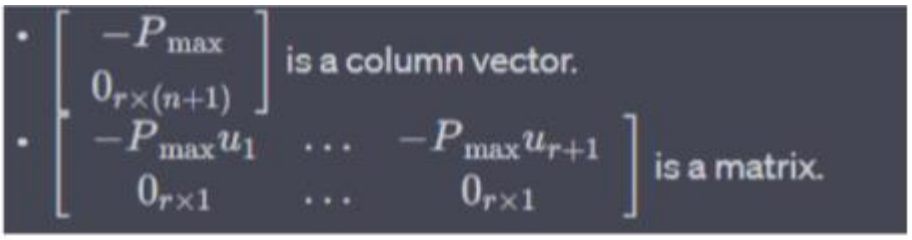


(43)

όπου I r × r είναι ο πίνακας ταυτότητας. Το [A 0 A M A W] ισούται με τις n - r σειρές του A + BK . P M ,max = [P 1,max ,. .., P r ,max] T , και P W ,max = [P (r + 1),max ,. .., P n ,max] T .

. Ως εκ τούτου, η θεωρία των διαταραχών μπορεί να χρησιμοποιηθεί για την ανάλυση της σταθερότητας του συστήματος [37].

Παρατηρείται ότι το \(\tilde{A} \) είναι ένας κατώτερος μπλοκ-τριγωνικός πίνακας με τις ιδιοτιμές λ i = 1 για i = 1,. .., r + 1, και οι ιδιοτιμές λ j για j = r + 2,. .., n - r . Εφόσον τα μπλοκ A 0 , A M και A W είναι ίδια με το αρχικό σύστημα στο (42), το λ j βρίσκεται στον ανοιχτό δίσκο μονάδας. Υποθέτοντας v r και u rείναι τα αντίστοιχα αριστερά και δεξιά ιδιοδιανύσματα με v r u r = 1, όταν το P είναι αρκετά μικρό, η διαταραχή στο λ i = 1 μπορεί να χαρακτηριστεί από το [16]:



(44)

Το V T Δ U έχει αρνητική ιδιοτιμή και ιδιοτιμή 0 με αλγεβρική πολλαπλότητα r . Αντίστοιχα έχει μια ιδιοτιμή 1 με αλγεβρική πολλαπλότητα r αν το P είναι αρκετά μικρό. Οι υπόλοιπες ιδιοτιμές βρίσκονται στον ανοιχτό δίσκο μονάδας. Αυτό

υποδηλώνει ότι είναι σταθερό. Είναι εύκολο να επαληθεύσετε ότι το σύστημα είναι σταθερό στη σταθερή κατάσταση

1. α_0^*:
   - α_0^* is defined as the minimum of two values:
     - The maximum of $\tilde{\alpha}_0$ and 0.
     - 1.1.
2. α_M^*:
   - α_M^* is simply equal to α_M.
3. α_W^*:
   - α_W^* is calculated using the formula:
     - $\alpha_W^* = (I_{nr} - A_W)^{-1} [A_0 \; A_M] \begin{bmatrix} \alpha_0^* \\ \alpha_M \end{bmatrix}$
4. $\tilde{\alpha}_0$:
   - $\tilde{\alpha}_0$ is calculated as:
     - $\tilde{\alpha}_0 = \frac{P_{ref}+P_{load}+P_{loss}-P_{M,\max}\alpha_M-P_{W,\max}\alpha_W^*}{P_{0,\max}}$

Τα αναλυτικά αποτελέσματα δείχνουν ότι οι κατανεμημένες γεννήτριες με καλή συμπεριφορά συγκλίνουν στον χώρο που εκτείνεται.Έτσι, όταν τα ψευδή δεδομένα εισάγονται από εισβολείς, οι αναλογίες χρήσης των κατανεμημένων γεννητριών δεν συμφωνούν, εμποδίζοντας την ενεργή έξοδο ισχύος ενός VPP να παρακολουθήσει την εντολή αποστολής. Επιπλέον, σύμφωνα με το [16], το ρυθμιζόμενο εύρος του P tran μπορεί να περιοριστεί από επιθέσεις FDI σε μια μεγάλη ομάδα κατανεμημένων γεννητριών. Αυτό υποβαθμίζει τη δυνατότητα ελέγχου του VPP.

- α_0^* is a scalar.
- α_M^* is a column vector.
- α_W^* is also a column vector.

- $\begin{bmatrix} \alpha_0^* \\ \alpha_M \end{bmatrix}$

1.8 Επίθεση FDI σε μικροδίκτυο

Σε ένα τυπικό μικροδίκτυο, ένας μετατροπέας ισχύος περιλαμβάνει μια πηγή ισχύος συνεχούς ρεύματος, γέφυρα μετατροπέα, μονάδα κοινής χρήσης ισχύος, φίλτρο εξόδου και βρόχους ελέγχου τάσης και ρεύματος. Η δυναμική ισχύος εξόδου του μετατροπέα i είναι:

$$\bullet \quad \frac{dP_i}{dt} = -\omega_{ci} P_i + \omega_{ci}(v_{odi} i_{odi} + v_{oqi} i_{oqi})$$

(46)

όπου v odi και v oqi είναι οι συνιστώσες του άξονα d - και q - της τάσης εξόδου. i odi και i oqi είναι οι συνιστώσες του άξονα d - και q - του ρεύματος εξόδου. Τα P i και Q i είναι η ενεργή και άεργη ισχύς εξόδου. ω ci είναι η συχνότητα αποκοπής του φίλτρου εξόδου.

Η δυναμική του μεγάλου σήματος του μετατροπέα δίνεται από το [38].

$$\begin{aligned} \frac{dx_i}{dt} &= f_i(x_i) + g(x_i)u_i \\ y_i &= h_i(x_i) \end{aligned}$$

(47)

όπου x i = [δ i , P i , Q i , ϕ di , ϕ qi , γ di , γ qi , i ldi , i lqi , v odi , v oqi , i odi , i oqi]. Το λεπτομερές μοντέλο του μετατροπέα βρίσκεται στο [38].

Η συνάρτηση κατανομής ισχύος πραγματοποιείται με τον έλεγχο droop που εκφράζεται ως [39,40 ,41 ,42 ,43]:

$$\begin{cases} \omega_i = \omega_{ni} - m_{pi} P_i \\ v_{\mathrm{mag},i} = V_{ni} - n_{qi} Q_i \end{cases}$$

(48)

όπου v mag,i και ω i είναι η τάση και η συχνότητα αναφοράς, αντίστοιχα. m pi και n qi είναι οι αντίστοιχοι συντελεστές πτώσης, και ω ni και V ni είναι τα σημεία ρύθμισης.

Ο έλεγχος Droop κάνει την τάση και τη συχνότητα να αποκλίνουν από τα καθορισμένα σημεία τους. Η συνεταιριστική δομή ελέγχου χρησιμοποιείται για την αλλαγή των ω ni και V ni στο (48) για να κατευθύνει την τάση και τη συχνότητα στις τιμές αναφοράς τους. Κάθε μετατροπέας μπορεί να ανταλλάσσει πληροφορίες με τους γείτονές του. Η διαφοροποίηση (48) αποδίδει:

$$\dot{\omega}_i = \dot{\omega}_{ni} - m_{pi}\dot{P}_i$$

(49)

Η είσοδος βοηθητικού ελέγχου ορίζεται ως:

$$\dot{\omega}_i = u_i$$

(50)

και ο νόμος συνεταιριστικού ελέγχου δίνεται από τα [44 , 45 , 46 , 47 , 48 , 49 , 50]:

$$\sum_{j \in N_i} a_{ij} \left(\omega_i(t) - \omega_j(t)\right)$$

(51)

όπου το N i περιέχει τους μετατροπείς του γειτονικού μετατροπέα i , και το g i αντιπροσωπεύει το μη μηδενικό κέρδος για τον μετατροπέα i .

Η βοηθητική είσοδος u i είναι:

$$u_i(t) = -c_\omega e_{\omega_i}(t)$$

(52)

όπου c ω είναι ένα κέρδος σύζευξης και το σημείο ρύθμισης στο (49) ικανοποιεί:

$$\omega_{ni} = \int \left(u_i + m_{pi} \dot{P}_i \right) dt$$

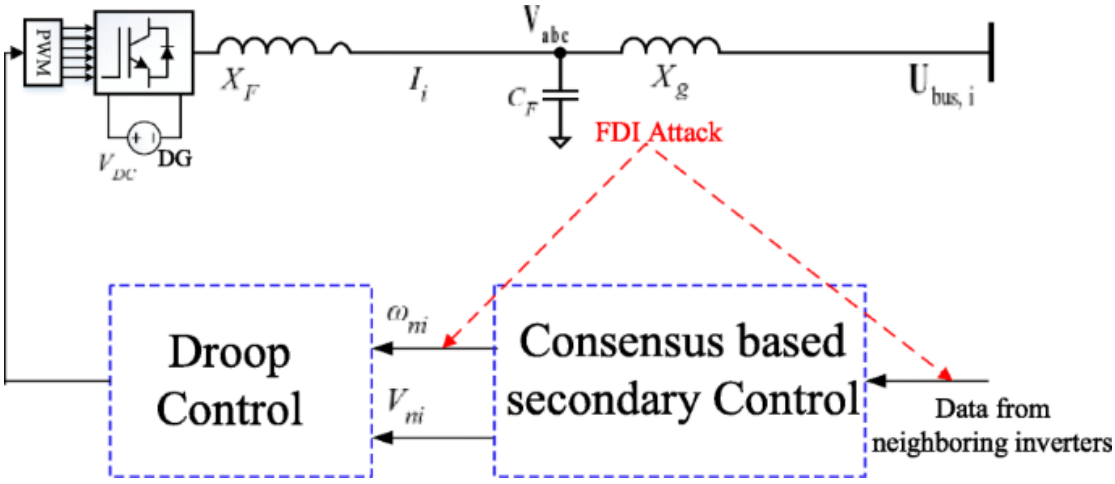
(53)

Από (50)–(53), η βοηθητική είσοδος u i χρησιμοποιεί τη συχνότητα του γείτονα για να μετριάσει την απόκλιση συχνότητας του συστήματος. Η ανταλλαγή πληροφοριών μεταξύ γειτονικών μετατροπέων είναι ευάλωτη σε κακόβουλες επιθέσεις, οι οποίες μπορεί να κάνουν την απόκλιση συχνότητας να μην επιστρέψει στο μηδέν. Δεδομένου ότι η παραδοσιακή ανίχνευση κακών δεδομένων αξιολογεί την εγκυρότητα των λαμβανόμενων δεδομένων με κεντρικό τρόπο, δεν ισχύει για τον κατανεμημένο έλεγχο των μικροδικτύων.

Δύο τύποι επιθέσεων, δηλαδή επιθέσεις ελεγκτών και επιθέσεις καναλιών επικοινωνίας, θεωρούνται όπως φαίνεται στο Σχ. 8 [51]. Οι επιθέσεις σε ελεγκτές εισάγουν ψευδή δεδομένα σε ενεργοποιητές/αισθητήρες για να επιτεθούν στον τοπικό ελεγκτή και οι επιθέσεις FDI σε ενεργοποιητές μπορούν να μοντελοποιηθούν ως [52 , 53]:

$$u_i^c = u_i + \mu_i u_i^a$$

(54)



Εικόνα 8. Ενδεικτικό διάγραμμα ελέγχου βάσει συναίνεσης του μετατροπέα i υπό επιθέσεις FDI

όπου uric=Ui+μl+μil είναι τα ψευδή δεδομένα που εισάγονται στον ενεργοποιητή i . Το sic=u+μeu είναι η κατεστραμμένη είσοδος ελέγχου και το u i είναι η αρχική βοηθητική είσοδος. Το μ i είναι το σήμα επίθεσης, και όταν συμβεί επίθεση, μ i = 1, διαφορετικά, μ i = 0. Σημειώστε ότι το σήμα επίθεσης μπορεί να είναι είτε μη σταθερό είτε σταθερό. Ένα μη σταθερό σήμα επίθεσης που θεωρείται ως θόρυβος μπορεί να αντιμετωπιστεί με τεχνικές φιλτραρίσματος θορύβου, ενώ το σήμα επίθεσης θεωρείται σταθερό εδώ [54].

Εάν παραβιαστεί ολόκληρος ο ελεγκτής, η καταστροφή συχνότητας του μετατροπέα i μπορεί να εκφραστεί ως

$$\omega_i^c = \omega_i + \eta_i \omega_i^a$$

(55)

Εάν το κανάλι επικοινωνίας μεταξύ δύο γειτονικών μετατροπέων προσβληθεί από FDI, ο τοπικός ελεγκτής λαμβάνει το κατεστραμμένο σήμα συχνότητας [7,11 ,5 ,56,57]. Η επίθεση FDI στο κανάλι επικοινωνίας μπορεί να μοντελοποιηθεί από:

$$\omega_i^j = \omega_i + \eta_i \omega_i^a$$

(56)

Το επόμενο βήμα είναι να αποκαλυφθεί η ευπάθεια του συνεργατικού ελέγχου ενός μικροδικτύου υπό επίθεση FDI. Λαμβάνοντας υπόψη ότι το πρωτόκολλο συνεργατικού ελέγχου (51) δέχεται επίθεση, το σφάλμα συγχρονισμού δεν θα επιστρέψει στο μηδέν για έναν άθικτο μετατροπέα, εάν είναι προσβάσιμο από έναν κατεστραμμένο μετατροπέα [17].

$$\dot{e}_\omega = -c_\omega (L + G) e_\omega$$

(57)

όπου L είναι ο Laplacian πίνακας που ορίζεται ως L = D − A , ενώ περισσότερες ιδιότητες του L μπορούν να βρεθούν στο [58,59,60]. D = diag{ N i } με το N i να είναι το σύνολο των μετατροπέων που στέλνουν δεδομένα στον μετατροπέα i (οι γείτονες του μετατροπέα i). A = [a ij] με το ij να είναι τα βάρη των ζεύξεων επικοινωνίας μεταξύ του μετατροπέα i και του j .

$$e_\omega(t) \text{ at } t = 0$$

(58)

Δεδομένου ότι το (L + G) είναι ένας θετικός καθορισμένος πίνακας, ο πρώτος όρος στο (58) πλησιάζει το μηδέν για c ω > 0. Χρησιμοποιώντας

$$e^{At} = \sum_{m=0}^{\infty} \frac{(At)^m}{m!}$$

(59)

Κεφάλαιο 2ο : «Σύγχρονες Προκλήσεις και Απειλές σε Δίκτυα Ηλεκτρικής Ενέργειας»

2.1 Εισαγωγή στις Σύγχρονες Προκλήσεις και Απειλές

Τα κίνητρα των εισβολέων στον κυβερνοχώρο εμπίπτουν κυρίως σε δύο κατηγορίες: οικονομικό κέρδος και όπλα πολέμου. Οι εγκληματίες του κυβερνοχώρου προσπαθούν να αποσπάσουν χρήματα από ευάλωτους στόχους χρησιμοποιώντας διαφορετικές τεχνικές, συμπεριλαμβανομένου του ransomware. Ζητούν λύτρα κλειδώνοντας τις επιχειρήσεις των θυμάτων. Πιο πρόσφατα, οι επιτιθέμενοι απειλούν να αποκαλύψουν τα κλεμμένα δεδομένα εάν δεν ικανοποιηθούν τα αιτήματά τους.

Ο κυβερνοπόλεμος είναι πιο περίπλοκος. Οι κυβερνοεγκληματίες που χρηματοδοτούνται από το κράτος έχουν ως αποστολή να κλέβουν, να διαταράσσουν και, το πιο σημαντικό, να προκαλέσουν ζημιά στις λειτουργίες των θυμάτων και στις κρίσιμες υποδομές.

Η πρόσφατη αποτυχία του Electric Reliability Council of Texas (ERCOT), η οποία προκλήθηκε από μια σφοδρή χειμερινή καταιγίδα τον Φεβρουάριο του 2021, αποτελεί πιθανό παράδειγμα της σφοδρότητας των συνεπειών. Αυτή η αποτυχία έγινε αισθητή σε όλη την πολιτεία, με 11 εκατομμύρια ανθρώπους να παγώνουν για τρεις ημέρες. Επίσης, το 2019, μια διακοπή ρεύματος στην Καλιφόρνια άφησε 248 νοσοκομεία χωρίς ρεύμα .

Ο αντίκτυπος των κυβερνοεπιθέσεων ενδέχεται να είναι ακόμη πιο σοβαρός. Η λίστα Σημαντικά Συμβάντα στον κυβερνοχώρο που παρέχεται από το Κέντρο Στρατηγικών και Διεθνών Μελετών σημειώνει την ανησυχητική τάση των κυβερνοεπιθέσεων να γίνονται πιο συχνές και καταστροφικές. Τα συστήματα ηλεκτρικής ενέργειας είναι ιδιαίτερα ευάλωτα και τα πιθανά σημεία εισόδου αυτών των επιθέσεων είναι παντού.

Σύμφωνα με τη δήλωση του Andreas Kuehlmann, διευθύνοντος συμβούλου της Tortuga Logic, οι κρίσιμες υποδομές της χώρας μας είναι εξαιρετικά ευάλωτες σε παραβιάσεις της ασφάλειας. Η διαδικασία μπορεί να παρομοιαστεί με μια διαδοχική εξέλιξη βημάτων, καθένα από τα οποία βασίζεται στο προηγούμενο. Σε περίπτωση που εντοπιστεί ευπάθεια σε έναν μετρητή ισχύος, είναι εύλογο ότι η λειτουργική ικανότητα μιας εγκατάστασης θα μπορούσε να τεθεί σε κίνδυνο μέσω της διακοπής της παροχής ρεύματος. Ωστόσο, υπάρχει η δυνατότητα να αχρηστευθούν όλες οι σχετικές

λειτουργίες. Δεν είναι απαραίτητο για την οντότητα να εξαπολύσει επίθεση στο δίκτυο καθαυτό. Ορισμένες επιθέσεις μπορεί να έχουν καταστροφικές συνέπειες. Πρόσφατα παρατηρήσαμε τη σφαίρα των δυνατοτήτων.

Το ζήτημα της ασφάλειας ενισχύεται σημαντικά από τη διασύνδεση. Σύμφωνα με τη δήλωση του Neeraj Paliwal, ο οποίος κατέχει τη θέση του αντιπροέδρου και γενικού διευθυντή της Rambus Security, αποτελούσε συμβατική πρακτική να θεωρούνται τα δίκτυα ηλεκτρικής ενέργειας ως κυρίως απομονωμένες υποδομές. Η έλευση της ψηφιοποίησης έχει επιφέρει σημαντικό μετασχηματισμό στο θέμα αυτό. Τα σύγχρονα διασυνδεδεμένα δίκτυα ηλεκτρικής ενέργειας προσφέρουν το πλεονέκτημα της απομακρυσμένης επιτήρησης, της κατανεμημένης ρύθμισης, της κατανομής φορτίων εναλλακτικής ενέργειας και της ανάλυσης δεδομένων. Η αξιοποίηση των απομακρυσμένων δυνατοτήτων του Διαδικτύου των Πραγμάτων (IoT) μπορεί να αξιοποιηθεί από τα ευφυή αστικά κέντρα για την ενίσχυση της επιχειρησιακής αποτελεσματικότητας και την παροχή πολύτιμων προοπτικών για την επικείμενη δημοτική χάραξη στρατηγικής.

Η διασυνδεσιμότητα των δικτυακών υποδομών δημιουργεί συχνά ανησυχίες σχετικά με την ασφάλεια. Η κρίσιμη υποδομή ενός σύγχρονου αστικού κέντρου αποτελεί στόχο κακόβουλων παραγόντων, γνωστών ως χάκερς, οι οποίοι στοχεύουν στην πρόκληση διαταραχών. Η εμφάνιση μιας διακοπής ρεύματος δεν έχει μόνο ως αποτέλεσμα την ταλαιπωρία των χρηστών, αλλά αποτελεί επίσης απειλή για τη συνέχεια των λειτουργιών σε περίπτωση έκτακτης ανάγκης. Τα νοσοκομεία οφείλουν να εξαρτώνται από εναλλακτικές πηγές ενέργειας, σε περίπτωση που αυτές είναι προσβάσιμες. Η συνήθης λειτουργία των κυβερνητικών φορέων θα υποστεί σημαντικές επιπτώσεις σε περίπτωση διακοπής της παροχής υπηρεσιών. Σε ορισμένες περιπτώσεις, αυτό μπορεί να αποτελέσει δυνητικό κίνδυνο για την ασφάλεια ενός έθνους. Ως εκ τούτου, η διασφάλιση αυτών των καίριων υποδομών παράλληλα με όλα τα τελικά σημεία είναι επιτακτική ανάγκη για την αποφυγή εκτεταμένων διαταραχών.

Σύμφωνα με το Γραφείο Λογοδοσίας της Κυβέρνησης των ΗΠΑ (Government Accountability Office – GAO), η κυβερνοασφάλεια περιλαμβάνεται στη λίστα υψηλού κινδύνου από το 1997. Το GAO είναι το τμήμα ελέγχου, αξιολόγησης και διερεύνησης του Κογκρέσου των ΗΠΑ. Υπάρχει για να υποστηρίξει το Κογκρέσο στην εκπλήρωση

των συνταγματικών του υποχρεώσεων και να συμβάλει στη βελτίωση της απόδοσης και της λογοδοσίας της ομοσπονδιακής κυβέρνησης έναντι του αμερικανικού λαού.

Στην έκθεσή του για την προστασία της υποδομής ζωτικής σημασίας, η οποία δημοσιεύθηκε τον Αύγουστο του 2019, ο GAO επεσήμανε ότι απαιτούνται ενέργειες για την αντιμετώπιση σημαντικών κινδύνων κυβερνοασφάλειας που αντιμετωπίζει το ηλεκτρικό δίκτυο. Συγκεκριμένα, οι κατασκευαστές και οι προγραμματιστές λογισμικού δημιουργούν τα προϊόντα τους σε πολλές διαφορετικές τοποθεσίες σε όλο τον κόσμο, καθιστώντας τα έτσι δυνητικά επιρρεπή σε απειλές που βασίζονται στο εξωτερικό.

Στην Έκθεση Electricity Grid Cybersecurity Report που δημοσιεύτηκε τον Μάρτιο του 2021, το GAO σημείωσε ότι το Υπουργείο Ενέργειας (DoE) και το Department of Homeland Security (DHS) έχουν την ευθύνη να χαράξουν μια εθνική στρατηγική για την ασφάλεια στον κυβερνοχώρο υποδομών ζωτικής σημασίας, συμπεριλαμβανομένων των δικτύων ηλεκτρικής ενέργειας.

Η έκθεση κατέληξε στο συμπέρασμα ότι τα συστήματα διανομής του δικτύου κινδύνευαν ολοένα και περισσότερο από κυβερνοεπιθέσεις. Το DoE, το DHS και άλλες ομοσπονδιακές υπηρεσίες έχουν συμβάλει στη βελτίωση της κυβερνοασφάλειας των συστημάτων διανομής. Ωστόσο, τα σχέδια του DoE για την εφαρμογή της εθνικής στρατηγικής κυβερνοασφάλειας για το δίκτυο δεν αντιμετωπίζουν πλήρως τους κινδύνους για αυτά τα συστήματα. Οι κυβερνοεπιθέσεις στα συστήματα διανομής ενδέχεται να οδηγήσουν σε διακοπές λειτουργίας σε εθνική κλίμακα.

Η έκθεση συνέστησε «ο Υπουργός Ενέργειας, σε συντονισμό με το DHS, τις πολιτείες και τη βιομηχανία, θα πρέπει να αντιμετωπίζει πληρέστερα τους κινδύνους για τα συστήματα διανομής του δικτύου από επιθέσεις στον κυβερνοχώρο — συμπεριλαμβανομένων των πιθανών επιπτώσεων τέτοιων επιθέσεων— στα σχέδια του DoE για την εφαρμογή της εθνικής στρατηγικής κυβερνοασφάλειας για το πλέγμα.»

Είναι επαρκείς αυτές οι προσπάθειες για την αντιμετώπιση του κινδύνου για τα ηλεκτρικά δίκτυα της χώρας; Επιπλέον, πώς θα δοθεί προτεραιότητα στις ενέργειες χρηματοδότησης και προγραμματισμού της ηλεκτρικής ενέργειας;

Τα ΣΗΕ εξελίσσονται. Θα γίνουν πιο συνδεδεμένα και πιο έξυπνα. Τα μελλοντικά δικτυακά δίκτυα θα χρησιμοποιούν δίκτυα ευρείας περιοχής χαμηλής κατανάλωσης

Low Power Wide Area Network (LPWAN) και 5G – 5ης γενιάς για τη βελτίωση της ενεργειακής απόδοσης μέσω κατανεμημένου και τηλεχειριστηρίου. Νέες καινοτομίες, όπως το νέο Wi-Fi CERTIFIED 6 Release 2, προστίθενται τακτικά για την προώθηση των δικτύων ισχύος.

«Είναι σίγουρα πιθανό ότι το Wi-Fi, συμπεριλαμβανομένου του νέου Wi-Fi CERTIFIED 6 Release 2, θα μπορούσε να χρησιμοποιηθεί από τους διαχειριστές συστημάτων μεταφοράς ως μέρος των δικτύων επικοινωνίας πληροφορικής τους», δήλωσε ο Νίκος Σαργολόγος, ανώτερος διευθυντής προϊόντων στη Wi-Fi Alliance. «Η πιο κοινή τοποθέτηση του Wi-Fi HaLow και του Wi-Fi CERTIFIED 6 Release 2 για εφαρμογές IoT (Internet of Things) είναι ότι το Wi-Fi HaLow είναι πιο κατάλληλο για χαμηλό ρυθμό δεδομένων, ευρέως διασκορπισμένες εφαρμογές IoT με τροφοδοσία μπαταρίας και Wi-Fi CERTIFIED 6 Release To 2 είναι πιο κατάλληλο για αισθητήρες IoT ή συσκευές αυτοματισμού κτιρίων που είναι συνδεδεμένες σε ένα πυκνό δίκτυο Wi-Fi υψηλής απόδοσης.»

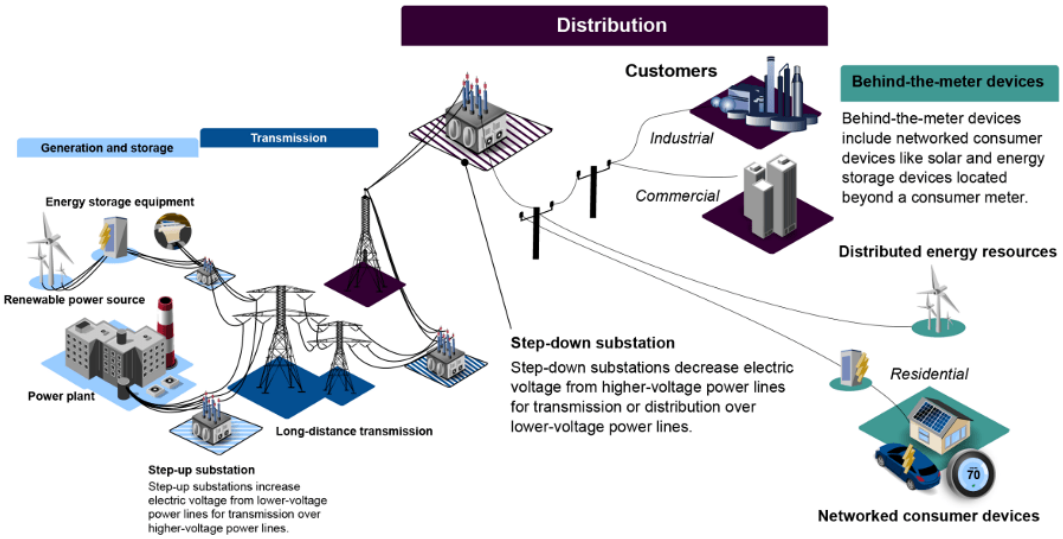
Τα δικτυωμένα δίκτυα παρέχουν πολλά οφέλη, αλλά παρουσιάζουν και προκλήσεις. Όσο πιο συνδεδεμένα είναι τα ΣΗΕ, τόσο περισσότερες ευκαιρίες αποκτούν οι εγκληματίες του κυβερνοχώρου για να χακάρουν τα συστήματα. Επιπλέον, όταν ενσωματωθούν οι ανανεώσιμες πηγές ενέργειας και το υπάρχον δίκτυο ηλεκτρικής ενέργειας, οι διεπαφές θα παρουσιάζουν πρόσθετα τρωτά σημεία.

«Όποτε συνδέονται πράγματα σε ένα δίκτυο, αυξάνετε τον κίνδυνο επιθέσεων στον κυβερνοχώρο», δήλωσε ο Steve Honda, διακεκριμένος μηχανικός, Honda Technologies. Με κρίσιμες υποδομές όπως το ηλεκτρικό δίκτυο, αυτός ο κίνδυνος ενισχύεται επειδή ο αντίκτυπος της αστοχίας είναι μεγάλος. Μία από τις μεγαλύτερες απειλές για την ασφάλεια στον κυβερνοχώρο για τα ΣΗΕ περιλαμβάνουν τα συστήματα ελέγχου όπως το άνοιγμα και το κλείσιμο των αυτόματων διακοπτών. Η δικτύωση αυτών των συστημάτων ελέγχου επιτρέπει την απομακρυσμένη παρακολούθηση και μπορεί να βελτιώσει το κόστος και την εξοικονόμηση ενέργειας. Ωστόσο, δημιουργεί επίσης περισσότερα σημεία πρόσβασης για τους χακέα. Οι επιθέσεις στο ουκρανικό δίκτυο ηλεκτρικής ενέργειας είναι ένα τυπικό παράδειγμα όπου οι εισβολείς μπόρεσαν να χρησιμοποιήσουν επιθέσεις μέσω Διαδικτύου για να κλείσουν το κύκλωμα».

2.2 Ετοιμότητα Απέναντι στις Σύγχρονες Απειλές του Κυβερνοχώρου

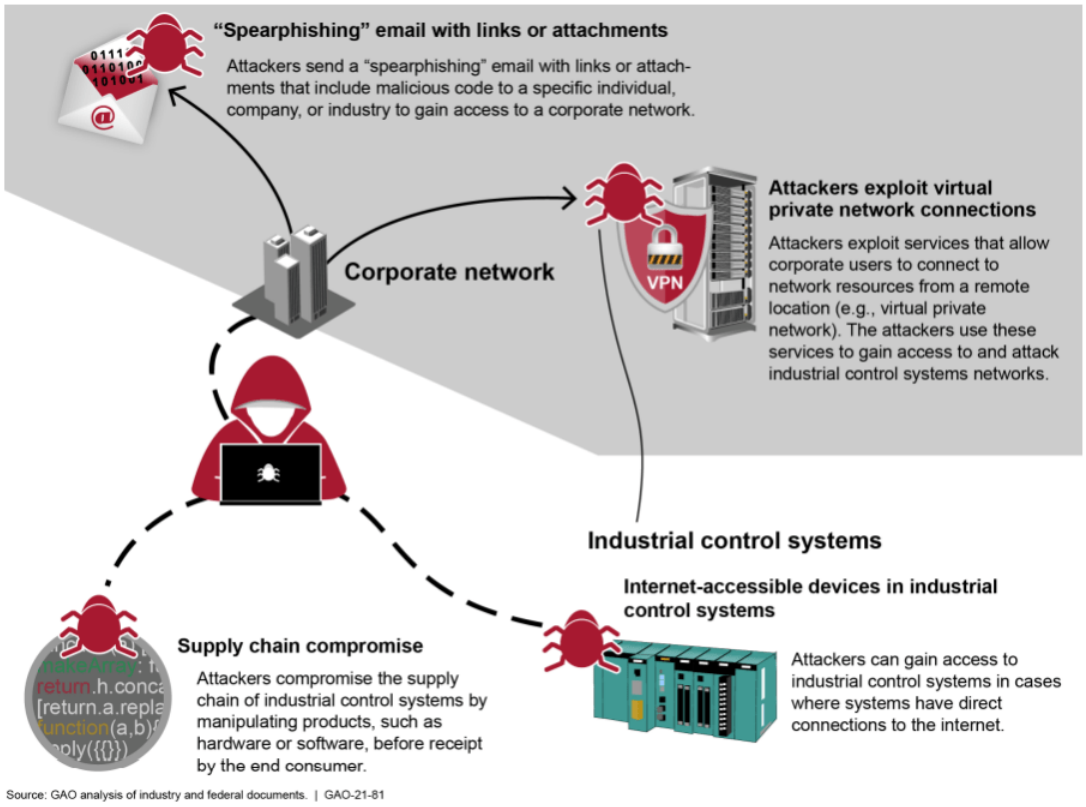
Στην Κάρτα Αναφοράς του 2021 για την Υποδομή της Αμερικής, η Αμερικανική Εταιρεία Πολιτικών Μηχανικών εξέδωσε βαθμό C– στον ενεργειακό τομέα (βαθμός για τον τομέα ενέργειας, μη ικανοποιητικός). Η έκθεση προειδοποίησε ότι «η πλειονότητα του εθνικού δικτύου γερνάει, με ορισμένα εξαρτήματα ηλικίας άνω του ενός αιώνα - πολύ μεγαλύτερη από το προσδόκιμο ζωής τους τα 50 χρόνια - και άλλα, συμπεριλαμβανομένου του 70% των γραμμών μεταφοράς και διανομής, βρίσκονται στο δεύτερο μισό του τη διάρκεια ζωής τους».

Στις ΗΠΑ, υπάρχουν τρεις περιοχές του συστήματος ηλεκτρικού δικτύου — ανατολικό, δυτικό και Τέξας (ERCOT). Υπάρχουν επίσης διασυνδέσεις μεταξύ των δικτύων ηλεκτρικής ενέργειας. Η ψηφιοποιήσει της διανομής ηλεκτρικής ενέργειας (έξυπνα δίκτυα) συζητήθηκε από το 2007, όταν ψηφίστηκε από το Κογκρέσο ο Τίτλος XIII του νόμου για την ενεργειακή ανεξαρτησία και ασφάλεια του 2007 (EISA - Energy ψηφιοποιήσει and Security Act).



Εικόνα 9. Εξαρτήματα του ηλεκτρικού δικτύου. Πηγή: GAO

Το 2019, η GAO προειδοποίησε για την ευπάθεια της αλυσίδας εφοδιασμού του ηλεκτρικού δικτύου των ΗΠΑ. Οποιοδήποτε από τα στοιχεία του ΣΗΕ μπορεί ενδεχομένως να παραβιαστεί και να διαταράξει την παροχή ηλεκτρικής ενέργειας στους χρήστες. Πιο ανησυχητικό είναι ότι εάν μια θεμελιώδη πηγή παραβιαστεί, μπορεί να σημαίνει μεγάλη καταστροφή.



Εικόνα 10. Τύποι επιθέσεων και πού συμβαίνουν. Πηγή: GAO

Υπάρχουν πολλά ζητήματα που αντιμετωπίζουν τα ΣΗΕ σήμερα και τα καθιστούν πιο ευάλωτα. Μεταξύ των τριών κορυφαίων είναι η ηλικία των συστημάτων, η έλλειψη συνεκτικού σχεδιασμού και δράσης και ο αριθμός των εμπλεκόμενων φορέων.

Στις ΗΠΑ, τα ενδιαφερόμενα μέρη περιλαμβάνουν φορείς εκμετάλλευσης, ιδιοκτήτες δικτύων ηλεκτρικής ενέργειας, τοπικές δημοτικές αρχές, το DoE και το DHS. Ο όρος «εθνικό δίκτυο ηλεκτρικής ενέργειας» περιλαμβάνει μια συλλογή ιδιόκτητων δικτύων και υποσταθμών. Επιπλέον, οι τρεις περιφέρειες των ΗΠΑ έχουν τις δικές τους πολιτικές και στρατηγικές για την ασφάλεια στον κυβερνοχώρο. Παρόλο που το DoE και το DHS έχουν τη συνολική ευθύνη για τον καθορισμό πολιτικών κυβερνοασφάλειας σε εθνικό επίπεδο, οι διάφοροι ενδιαφερόμενοι πρέπει να συνεργάζονται και να εφαρμόζουν τις πολιτικές έγκαιρα.

Ωστόσο, κάθε ενδιαφερόμενος έχει τις δικές του προτεραιότητες, συμφέροντα και προϋπολογισμούς, οι οποίοι μπορούν να μην ευθυγραμμίζονται με τις εθνικές πολιτικές. Σήμερα, είναι σχεδόν αδύνατο να υπάρχει ένα μεγάλο σχέδιο σε εθνικό επίπεδο για να ακολουθήσει κάθε ενδιαφερόμενος. Το πιο σημαντικό, τα μεμονωμένα δίκτυα ηλεκτρικής ενέργειας έχουν τον δικό τους εξοπλισμό, μηχανήματα και

μεθόδους παραγωγής ενέργειας. Δεν υπάρχει ομοιομορφία. Μπορεί να είναι ευκολότερο για μια νέα εγκατάσταση να εφαρμοστεί έξυπνα δίκτυα, ενώ θα ήταν πολύ δαπανηρό για ένα παλιό δίκτυο ηλεκτρικής ενέργειας να ψηφιοποιηθεί. Υπάρχει επίσης μια νοοτροπία: «Αν δεν είναι χαλασμένο, μην το διορθώσεις», που περιορίζει την ικανότητα να κάνεις οτιδήποτε για μια επίθεση. Μέχρι να γίνει αισθητός ο αντίκτυπος αυτής της επίθεσης, είναι πολύ αργά.

Το ουκρανικό δίκτυο ηλεκτρικής ενέργειας δέχθηκε αξιοσημείωτες επιθέσεις στον κυβερνοχώρο τον Δεκέμβριο του 2015 και του 2016. Οι επιθέσεις είχαν ως αποτέλεσμα διακοπές ρεύματος που επηρέασαν χιλιάδες πελάτες. Οι προαναφερθείσες επιθέσεις, οι οποίες αποδόθηκαν σε κυβερνητικές οντότητες, περιλάμβαναν τη χρήση κακόβουλου λογισμικού και συγχρονισμένες προσπάθειες για την παρεμπόδιση των συστημάτων, οι οποίες περιλάμβαναν τη χειραγώγηση των βιομηχανικών συστημάτων ελέγχου.

Το περιστατικό με το ransomware ψηφιοποιήσει τον Ιούνιο του 2017 είχε παγκόσμιο αντίκτυπο, καθώς επηρεάστηκαν πολλοί οργανισμοί, συμπεριλαμβανομένων ενεργειακών εταιρειών στην Ευρώπη. Παρόλο που αρχικά επικεντρώθηκε στην Ουκρανία, ο αντίκτυπός του διαδόθηκε γρήγορα σε όλο τον κόσμο. Το κακόβουλο λογισμικό ψηφιοποιήσει είχε αποδιοργανωτικό αντίκτυπο σε ζωτικής σημασίας υποδομές, ιδίως στον τομέα της ενέργειας, με αποτέλεσμα σημαντικές οικονομικές απώλειες και λειτουργικές διαταραχές.

Η εκστρατεία ψηφιοποιήσει ψηφιοποιήσει ή Energetic Bear παρατηρήθηκε μεταξύ 2011 και 2014 και συνεχίζεται ακόμη. Η κύρια εστίασή της ήταν στους ενεργειακούς τομείς διαφόρων ευρωπαϊκών κρατών, όπως η Γερμανία, η Ελβετία και η Τουρκία. Οι δράστες, οι οποίοι πιστεύεται ότι έλαβαν υποστήριξη από κυβερνητική οντότητα, κατάφεραν να διεισδύσουν σε συστήματα βιομηχανικού ελέγχου και πραγματοποίησαν προκαταρκτικές έρευνες, θέτοντας ενδεχομένως τις βάσεις για επερχόμενες επιθέσεις.

Η εισβολή του κακόβουλου λογισμικού Triton (ή Trisis) το 2017 είχε ως στόχο μια πετροχημική εγκατάσταση που βρισκόταν στη Σαουδική Αραβία, ωστόσο ο αντίκτυπός της επεκτάθηκε πέρα από τα όρια της Μέσης Ανατολής για να συμπεριλάβει τις ενεργειακές υποδομές της Ευρώπης. Το κακόβουλο λογισμικό παρουσίασε ιδιαίτερη εστίαση στα συστήματα με όργανα ασφαλείας (SIS), τα οποία είναι υψίστης σημασίας για τη διασφάλιση της ασφαλούς λειτουργίας των βιομηχανικών διεργασιών. Το προαναφερθέν περιστατικό έφερε στο προσκήνιο την πιθανότητα κυβερνοεπιθέσεων

που χρησιμοποιούνται για την αλλοίωση των μηχανισμών ασφαλείας σε υποδομές που σχετίζονται με την ενέργεια.

Το έτος 2018 σημειώθηκε ένα αξιοσημείωτο περιστατικό παραβίασης δεδομένων σε νορβηγική ενεργειακή εταιρεία, το οποίο φέρεται να εκτελέστηκε από χάκερς κινεζικής προέλευσης. Η παραβίαση της ασφάλειας είχε ως αποτέλεσμα την αποκάλυψη ευαίσθητων δεδομένων και έθεσε ενδεχομένως σε κίνδυνο πληροφορίες σχετικά με κρίσιμες υποδομές, προκαλώντας έτσι ανησυχίες σχετικά με το ενδεχόμενο μελλοντικών επιθέσεων σε ενεργειακά συστήματα.

Το ransomware Wannacry, το οποίο εμφανίστηκε το 2017, είχε σημαντικό αντίκτυπο σε διάφορους οργανισμούς σε παγκόσμια κλίμακα, ιδίως σε πολλά ευρωπαϊκά έθνη. Η προαναφερθείσα απειλή στον κυβερνοχώρο αξιοποίησε αποτελεσματικά μια ευπάθεια που ενυπάρχει στα λειτουργικά συστήματα Microsoft Windows, με αποτέλεσμα να εξαπλωθεί με επιταχυνόμενο ρυθμό και να χρησιμοποιήσει τεχνικές κρυπτογράφησης για να καταστήσει τα δεδομένα απρόσιτα. Στη συνέχεια, ο κακόβουλος δράστης που ήταν υπεύθυνος για την πράξη αυτή απαίτησε χρηματική αποζημίωση σε αντάλλαγμα για την αποκατάσταση των δεδομένων που είχαν παραβιαστεί. Η προαναφερθείσα επίθεση προκάλεσε σημαντικές διαταραχές σε ιδρύματα υγειονομικής περίθαλψης, εμπορικές επιχειρήσεις και κυβερνητικούς φορείς.

Η ομάδα Carbanak/Evilnum Group, η οποία διήρκεσε από το 2013 έως το 2018, αντιπροσωπεύει μια συλλογικότητα κυβερνοεγκληματιών που επικέντρωσε τις δραστηριότητές της σε χρηματοπιστωτικά ιδρύματα που βρίσκονται στην ευρωπαϊκή περιοχή. Εικάζεται ευρέως ότι η ομάδα αυτή προέρχεται από την Ανατολική Ευρώπη, τονίζοντας περαιτέρω τη γεωγραφική της συσχέτιση. Οι επιτιθέμενοι χρησιμοποίησαν περίπλοκες μεθοδολογίες στις επιθετικές τους προσπάθειες, οι οποίες περιλάμβαναν spear-phishing, τροϊκανά απομακρυσμένης πρόσβασης (RAT) και χειραγώγηση του δικτύου ATM, με τελική κατάληξη σημαντικές νομισματικές επιπτώσεις.

Η Επιχείρηση Aurora, είναι ένα σημαντικό γεγονός που συνέβη το έτος 2009. Η επιχείρηση αυτή περιελάμβανε μια σειρά από σχολαστικά ενορχηστρωμένες επιθέσεις στον κυβερνοχώρο, οι οποίες απευθύνονταν ειδικά σε ένα πλήθος ευρωπαϊκών εθνών, μαζί με άλλες οντότητες ενδιαφέροντος. Οι προαναφερθείσες επιθέσεις, οι οποίες αποδόθηκαν σε φορείς που χρηματοδοτούνταν από κράτη, εκτελέστηκαν με στόχο την αρπαγή πνευματικής ιδιοκτησίας και την παράνομη είσοδο στα δίκτυα πολυάριθμων

οργανισμών, οι οποίοι περιλάμβαναν οντότητες που δραστηριοποιούνται στους τομείς της τεχνολογίας και της άμυνας.

Η ληστεία της Τράπεζας του Μπανγκλαντές το 2016 αποτελεί αξιοσημείωτη περίπτωση εγκλήματος στον κυβερνοχώρο, που χαρακτηρίζεται από τη διείσδυση στα περίπλοκα συστήματα της αξιόλογης Τράπεζας του Μπανγκλαντές. Αυτή η τολμηρή παραβίαση επέτρεψε στους δράστες να παραβιάσουν με επιτυχία το ιδιαίτερα αξιόλογο δίκτυο πληρωμών SWIFT, εξασφαλίζοντας έτσι την παράνομη πρόσβασή τους σε ένα ευρύ φάσμα οικονομικών συναλλαγών. Η προσπάθεια μεταφοράς ενός ποσού περίπου 1 δισεκατομμυρίου δολαρίων αναλήφθηκε, αν και με μερική μόνο επιτυχία, προκαλώντας έτσι σημαντικές οικονομικές ζημίες και προκαλώντας ανησυχίες σχετικά με την ακεραιότητα της παγκόσμιας τραπεζικής υποδομής.

Η συνεχιζόμενη σειρά επιθέσεων, που συνήθως αναφέρεται ως APT 28 ή Fancy Bear, απαιτεί επιστημονική προσοχή. Η APT 28, μια ομάδα κυβερνοκατασκοπείας που φέρεται να συνδέεται με τον κυβερνητικό μηχανισμό της Ρωσικής Ομοσπονδίας, έχει κατευθύνει τις προσπάθειές της προς μια σειρά από έθνη που βρίσκονται τόσο στην ευρωπαϊκή όσο και στην ασιατική ήπειρο. Οι επιτιθέμενοι έχουν εμπλακεί σε διάφορες μορφές επιθετικών ελιγμών, όπως η εκτέλεση εκστρατειών phishing, η εκμετάλλευση ευπαθειών λογισμικού και η σκόπιμη εστίαση σε κυβερνητικούς φορείς, αμυντικούς οργανισμούς και τομείς που αφορούν κρίσιμες υποδομές.

Τέλος, η συνεχιζόμενη σειρά επιθέσεων που διαπράττει η ομάδα Lazarus Group, η οποία φέρεται να προέρχεται από τη Λαϊκή Δημοκρατία της Κορέας, αποτέλεσε αντικείμενο σημαντικής προσοχής. Αυτές οι επιθέσεις στον κυβερνοχώρο έχουν στραφεί εναντίον ποικίλων στόχων, που περιλαμβάνουν χρηματοπιστωτικά ιδρύματα καθώς και υποδομές ζωτικής σημασίας, και εκτείνονται στις περιοχές της Ασίας και της Ευρώπης. Ο τρόπος δράσης που χρησιμοποιούν οι δράστες περιλαμβάνει στρατηγικούς ελιγμούς όπως το spear-phishing, τη διάδοση κακόβουλου λογισμικού και την υπεξαίρεση κρυπτονομισμάτων ως μέσο χρηματοδότησης των παράνομων προσπαθειών τους.

2.3 Περιστατικά Κυβερνοεπιθέσεων

Περιστατικό Ουκρανίας

Το περιστατικό που αφορά την κυβερνοεπίθεση στην Ουκρανία, η οποία έλαβε χώρα τους μήνες Δεκέμβριο τόσο το 2015 όσο και το 2016, αναγνωρίζεται ευρέως ως μια επίθεση με μεγάλη συνέπεια και επιρροή σε ζωτικά συστήματα υποδομής. Το ηλεκτρικό δίκτυο της Ουκρανίας δέχθηκε σκόπιμες επιθέσεις, οι οποίες οδήγησαν σε εκτεταμένες διακοπές ρεύματος. Το περιστατικό αυτό έφερε στο προσκήνιο τις εγγενείς ευαισθησίες των βιομηχανικών συστημάτων ελέγχου (ICS) σε απειλές στον κυβερνοχώρο.

Οι επιτιθέμενοι χρησιμοποίησαν μια συρροή περίπλοκων μεθοδολογιών, που περιλαμβάνουν spear-phishing, ανάπτυξη κακόβουλου λογισμικού και συγχρονισμένες προσπάθειες με στόχο την αποσταθεροποίηση του δικτύου ηλεκτρικής ενέργειας. Οι επιτιθέμενοι χρησιμοποίησαν προσαρμοσμένες ηλεκτρονικές επικοινωνίες spear-phishing που περιείχαν κακόβουλα συνημμένα αρχεία ως μέσο για την αρχική διείσδυση στις καθορισμένες οντότητες. Στη συνέχεια, οι κακόβουλοι φορείς προχώρησαν στη χρήση επιβλαβούς λογισμικού, συγκεκριμένα των BlackEnergy και Industroyer/CrashOverride, με σκοπό να διεισδύσουν κρυφά και να ασκήσουν έλεγχο στο περίπλοκο σύνολο των συστατικών στοιχείων του Βιομηχανικού Συστήματος Ελέγχου (ICS). Ιδιαίτερο ενδιαφέρον για αυτούς τους κυβερνοεπιτιθέμενους είχαν τα συστήματα SCADA (Supervisory Control and Data Acquisition), τα οποία φέρουν την ευθύνη της εποπτείας και της διαχείρισης της διανομής ηλεκτρικής ενέργειας.

Η συγγραφή των επιθέσεων αποδόθηκε σε φορείς που χρηματοδοτήθηκαν από το κράτος, με αδιάσειστα στοιχεία που υποδεικνύουν τη συμμετοχή ομάδων που υποστηρίζονται από τη ρωσική κυβέρνηση. Πιστεύεται ότι οι επιθέσεις είχαν γεωπολιτικό χαρακτήρα, λόγω της τεταμένης δυναμικής που χαρακτήριζε τις σχέσεις μεταξύ Ουκρανίας και Ρωσίας κατά τη στιγμή των προαναφερθέντων περιστατικών. Οι διακοπές ρεύματος στην Ουκρανία είχαν βαθύτατες επιπτώσεις στις υποδομές της χώρας, με αποτέλεσμα σημαντικές διαταραχές στις καθημερινές συνήθειες του πληθυσμού της. Το ατυχές αυτό γεγονός επηρέασε σημαντικό αριθμό πελατών, που ανέρχονται σε εκατοντάδες χιλιάδες. Οι προαναφερθείσες επιθέσεις άσκησαν επιρροή τόσο σε αστικές όσο και σε αγροτικές περιοχές, τονίζοντας έτσι το εκτεταμένο πεδίο

εφαρμογής και τις επιπτώσεις των επιθέσεων στον κυβερνοχώρο σε ζωτικής σημασίας υποδομές.

Το περιστατικό λειτούργησε ως κομβική στιγμή συνειδητοποίησης για τις κυβερνήσεις, τους οργανισμούς και την παγκόσμια κοινότητα κυβερνοασφάλειας. Η προαναφερθείσα συζήτηση φώτισε τις εγγενείς ευαισθησίες των ζωτικών υποδομών, με ιδιαίτερη έμφαση στην επιτακτική απαίτηση για ενισχυμένα πρωτόκολλα ασφαλείας που αφορούν τα βιομηχανικά συστήματα ελέγχου. Το προαναφερθέν περιστατικό έφερε στο προσκήνιο τη σημασία της διάθεσης πόρων για την ενίσχυση των πρακτικών κυβερνοασφάλειας, της περιοδικής αξιολόγησης των μέτρων ασφαλείας και της θέσπισης ολοκληρωμένων πρωτοκόλλων αντιμετώπισης περιστατικών.

Το εν λόγω περιστατικό παρουσίασε επιπτώσεις που επεκτάθηκαν πέρα από τα όρια της Ουκρανίας, αναδεικνύοντας έτσι την ικανότητα των κυβερνοεπιθέσεων να παρεμποδίζουν κρίσιμες υποδομές σε παγκόσμια κλίμακα. Το προαναφερθέν περιστατικό προκάλεσε ανησυχίες σχετικά με τη διασφάλιση των βιομηχανικών συστημάτων ελέγχου σε διάφορους τομείς, όπως η ενέργεια, οι μεταφορές και η μεταποίηση.

Το περιστατικό λειτούργησε ως καταλύτης για την αύξηση της διεθνούς συνεργασίας στον τομέα της κυβερνοασφάλειας. Η Ουκρανία, σε συνεργασία με τις Ηνωμένες Πολιτείες και διάφορα ευρωπαϊκά έθνη, προχώρησε στην ανταλλαγή τεχνικών στοιχείων και δεικτών παραβίασης, προκειμένου να παράσχει βοήθεια στις οντότητες που επλήγησαν και να μετριάσει την εκδήλωση επακόλουθων επιθέσεων. Το προαναφερθέν περιστατικό προκάλεσε επίσης ενισχυμένη συνεργασία μεταξύ κυβερνητικών φορέων, φορέων ασφαλείας και βασικών παραγόντων του κλάδου, με στόχο τον αποτελεσματικό μετριασμό των κινδύνων στον κυβερνοχώρο που στοχεύουν σε ζωτικής σημασίας υποδομές.

Το περιστατικό ώθησε την κοινότητα της κυβερνοασφάλειας και τους υπεύθυνους χάραξης πολιτικής να υπογραμμίσουν τη σημασία της ενσωμάτωσης των αρχών της ασφάλειας κατά το σχεδιασμό στα συστήματα κρίσιμων υποδομών. Επιπλέον, τόνισαν την ανάγκη για ενισχυμένα προγράμματα κατάρτισης και ευαισθητοποίησης των φορέων εκμετάλλευσης, την εφαρμογή ολοκληρωμένων σχεδίων αντιμετώπισης περιστατικών και τη συνεχή επένδυση σε προσπάθειες έρευνας και ανάπτυξης που αφορούν την κυβερνοασφάλεια.

Στο σύνολό του, το περιστατικό αποτέλεσε μια σημαντική συγκυρία για την κατανόηση των μελλοντικών επιπτώσεων των κυβερνοεπιθέσεων σε ζωτικά συστήματα υποδομής. Το προαναφερθέν συμβάν προκάλεσε τη διάχυτη αναγνώριση της αναγκαιότητας ενισχυμένων πρακτικών στον τομέα της κυβερνοασφάλειας, λειτουργώντας έτσι ως καταλύτης για την προώθηση της διεθνούς συνεργασίας και της ανταλλαγής πληροφοριών στην προσπάθεια καταπολέμησης των κυβερνοαπειλών που στοχεύουν κρίσιμα συστήματα σε παγκόσμια κλίμακα.

ransomware NotPetya

Η επίθεση ransomware NotPetya, που σημειώθηκε τον Ιούνιο του 2017, άσκησε ευρεία επιρροή σε παγκόσμια κλίμακα, επηρεάζοντας έτσι πολυάριθμους οργανισμούς που βρίσκονται στην Ευρώπη, την Ασία και τη Βόρεια Αμερική. Η προαναφερθείσα επίθεση παρουσίασε υψηλό επίπεδο πολυπλοκότητας, καθώς χρησιμοποίησε μια προσαρμοσμένη επανάληψη του ransomware Petya και διαδόθηκε με διάφορα μέσα, κυρίως εκμεταλλευόμενη μια παραβιασμένη ενημέρωση λογισμικού ενός ευρέως χρησιμοποιούμενου λογιστικού λογισμικού, γνωστού ως MeDoc.

Η διάπραξη της επίθεσης αποδίδεται σε μια εθνική κρατική οντότητα, πιο συγκεκριμένα στον ρωσικό στρατό, με ρητό στόχο να στοχοποιήσει ουκρανικές εγκαταστάσεις. Ωστόσο, η ταχεία διάδοσή της ξεπέρασε τα γεωγραφικά όρια, επηρεάζοντας έτσι πολυεθνικές εταιρείες και οντότητες που είναι υπεύθυνες για τη διατήρηση κρίσιμων υποδομών.

Η κυβερνοεπίθεση NotPetya είχε ως αποτέλεσμα εκτεταμένες διαταραχές σε πολλαπλούς τομείς, περιλαμβάνοντας χρηματοπιστωτικά ιδρύματα, ναυτιλιακές επιχειρήσεις, παρόχους ενέργειας και οργανισμούς υγειονομικής περίθαλψης. Το αποτέλεσμα αυτού του συμβάντος οδήγησε σε σημαντικές οικονομικές επιπτώσεις και σημαντικές διαταραχές στις επιχειρησιακές δραστηριότητες.

Η κύρια ώθηση στην οποία στηρίχθηκε η επίθεση φαίνεται να προσανατολίζεται στους στόχους της διατάραξης και της εξόντωσης και όχι στην επιδίωξη χρηματικών οφελών. Οι δράστες χρησιμοποίησαν ransomware ως μέσο συγκάλυψης για να αποκρύψουν τα κίνητρά τους.

Η επίθεση αξιοποίησε αποτελεσματικά έναν αξιόπιστο μηχανισμό ενημέρωσης λογισμικού, θέτοντας έτσι σε κίνδυνο την αλυσίδα εφοδιασμού της MeDoc. Το προαναφερθέν περιστατικό επέστησε την προσοχή στους πιθανούς κινδύνους που συνδέονται με τα τρωτά σημεία στις αλυσίδες εφοδιασμού λογισμικού και τόνισε την αναγκαιότητα αυστηρών πρωτοκόλλων ασφαλείας καθ' όλη τη διάρκεια των διαδικασιών ανάπτυξης και διανομής.

Το NotPetya παρουσίαζε χαρακτηριστικά που έμοιαζαν με σκουλήκι, διευκολύνοντας έτσι την οριζόντια διάδοσή του σε διασυνδεδεμένα δίκτυα, διεισδύοντας έτσι σε πρόσθετα συστήματα και προκαλώντας διαταραχές στις επιχειρησιακές διαδικασίες. Το κακόβουλο λογισμικό, επιπλέον, ενσωμάτωσε καταστροφικούς μηχανισμούς που περιλάμβαναν την αντικατάσταση του κύριου αρχείου εκκίνησης (MBR), με αποτέλεσμα την αδρανοποίηση των μολυσμένων συστημάτων.

Το περιστατικό προκάλεσε αυξημένη επίγνωση όσον αφορά τις επιπτώσεις και τη σοβαρότητα των επιθέσεων στον κυβερνοχώρο, ειδικά στον τομέα των ζωτικών υποδομών και της διασφάλισης των αλυσίδων εφοδιασμού. Η προαναφερθείσα δήλωση υπογραμμίζει τη σημασία της επαρκούς προετοιμασίας για την αντιμετώπιση περιστατικών, της εφαρμογής αποτελεσματικών πρωτοκόλλων δημιουργίας αντιγράφων ασφαλείας και αποκατάστασης και της αναγνώρισης της επιτακτικής ανάγκης διεθνούς συνεργασίας για τον μετριασμό των παγκόσμιων κινδύνων στον κυβερνοχώρο.

SolarWinds

Η επίθεση στην αλυσίδα εφοδιασμού της SolarWinds, η οποία ήρθε στο φως της δημοσιότητας τον Δεκέμβριο του 2020, απευθυνόταν στη SolarWinds, έναν αξιόλογο πάροχο λογισμικού διαχείρισης ΤΠ. Οι κακόβουλοι παράγοντες διείσδυσαν με επιτυχία στον μηχανισμό ενημέρωσης λογισμικού της SolarWinds, διαδίδοντας έτσι μια ενημέρωση λογισμικού που ήταν μολυσμένη με μια κρυφή κερκόπορτα. Αυτή η επιβλαβής ενημέρωση έφτασε σε ένα πλήθος εγκαταστάσεων, που περιλάμβαναν κυβερνητικούς φορείς, τεχνολογικές επιχειρήσεις και οντότητες ζωτικής σημασίας υποδομών.

Οι δράστες διείσδυσαν με επιτυχία στο αναπτυξιακό οικοσύστημα της SolarWinds και εισήγαγαν κρυφά κακόβουλο κώδικα στις ενημερώσεις λογισμικού Orion, οι οποίες στη συνέχεια διαδόθηκαν στο πελατολόγιο της εταιρείας. Η διάπραξη αυτής της περίτεχνα ενορχηστρωμένης επίθεσης στην αλυσίδα εφοδιασμού διευκόλυνε την απόκτηση διαρκών προνομίων εισόδου στα ειδικά στοχευμένα δίκτυα.

Η επίθεση της SolarWinds είχε σημαντικό αντίκτυπο σε διάφορους διεθνείς οργανισμούς, μεταξύ των οποίων και κυβερνητικές υπηρεσίες των ΗΠΑ. Το λογισμικό Orion, το οποίο παραβιάστηκε, διευκόλυνε την αρχική εγκαθίδρυση μιας στρατηγικής θέσης για τους επιτιθέμενους, παρέχοντάς τους έτσι τη δυνατότητα να συμμετάσχουν σε μεταγενέστερες κακόβουλες προσπάθειες εντός των δικτύων που αποτέλεσαν ειδικό στόχο.

Ο κύριος στόχος της επίθεσης περιστράφηκε πιθανότατα γύρω από την κατασκοπεία και την υποκλοπή δεδομένων. Οι επιτιθέμενοι κατεύθυναν τις προσπάθειές τους στην απόσπαση ευαίσθητων πληροφοριών και στην εκτέλεση αναγνωριστικών προσπαθειών προκειμένου να αποκτήσουν γνώση των επιχειρησιακών διαδικασιών των υπό εξέταση οργανισμών.

Οι επιτιθέμενοι επέδειξαν υψηλό επίπεδο δεξιοτεχνίας στην τέχνη τους, χρησιμοποιώντας μεθοδολογίες που τους επέτρεπαν να αποφεύγουν τον εντοπισμό για παρατεταμένη διάρκεια. Οι χρησιμοποιούμενες στρατηγικές περιλάμβαναν διάφορες τεχνικές, συμπεριλαμβανομένης της πρακτικής της προσποίησης domain και της χειραγώγησης ψηφιακών πιστοποιητικών, τα οποία χρησιμοποιήθηκαν με σκοπό να διαφύγουν της ανίχνευσης.

Το προαναφερθέν περιστατικό χρησίμευσε για να τονίσει τον επιτακτικό χαρακτήρα της εφαρμογής και της διατήρησης ισχυρών πρακτικών που αφορούν την ασφάλεια της αλυσίδας εφοδιασμού. Το περιστατικό προκάλεσε έρευνες σχετικά με την ευρωστία των διαδικασιών ανάπτυξης λογισμικού, τον έλεγχο που εφαρμόζεται σε στοιχεία τρίτων και τον εντοπισμό περίπλοκων επιθέσεων με στόχο αξιόπιστους παρόχους.

Η επίθεση της SolarWinds λειτούργησε ως ηχηρό σύνθημα για τις οντότητες και τα διοικητικά όργανα σε όλο τον κόσμο, υπογραμμίζοντας αποτελεσματικά τις πιθανές επιπτώσεις των παραβιάσεων της αλυσίδας εφοδιασμού και τονίζοντας την επιτακτική φύση των ενισχυμένων πρωτοκόλλων κυβερνοασφάλειας.

2.4 Επίλυση Προβλημάτων

Η υπέρβαση αυτών των προβλημάτων απαιτούμενης χρήσης τεχνολογίας για την καταπολέμηση των εγκληματιών του κυβερνοχώρου, καλύτερη και πιο συγκεντρωτική ηγεσία και αλλαγή νοοτροπίας που αναγνωρίζει την αμεσότητα των απειλών στον κυβερνοχώρο.

Υπάρχουν πολλές τεχνολογίες και γνώσεις που βοηθούν στην καταπολέμηση των επιθέσεων στον κυβερνοχώρο. Όλα τα δίκτυα LPWAN και 5G διαθέτουν ενσωματωμένα πρωτόκολλα ασφαλείας. Οι προγραμματιστές τσιπ και το υλικό με την επίγνωση της ασφάλειας έχουν δημιουργήσει σταθερές και αξιόπιστες πλατφόρμες υλικού ασφαλείας, οι οποίες περιλαμβάνουν ασφαλή εκκίνηση, εξελιγμένη κρυπτογράφηση, έλεγχο ταυτότητας και πολλά άλλα.

Πιο δύσκολο είναι να πεισθεί κάθε χειριστή στο δίκτυο ηλεκτρικής ενέργειας να εξετάσει την τρέχουσα κατάσταση ασφάλειας και ετοιμότητας. Ευτυχώς, υπάρχουν πολλοί έμπειροι σύμβουλοι κυβερνοασφάλειας που είναι έτοιμοι να βοηθήσουν. Και με τον εγκεκριμένο προϋπολογισμό υποδομής σε ομοσπονδιακό επίπεδο, αυτή είναι μια καλή στιγμή για τις ομοσπονδιακές υπηρεσίες να συνεργαστούν με τον κλάδο, συμπεριλαμβανομένης της παροχής οικονομικής υποστήριξης και κινήτρων για τη βελτίωση και την αναβάθμιση μεμονωμένων δικτύων ενέργειας για την αντιμετώπιση μελλοντικών επιθέσεων.

«Το ΣΗΕ είναι επιρρεπές σε κακόβουλες επιθέσεις από διάφορα σημεία εισόδου, από την παραγωγή έως τη διανομή στον έξυπνο μετρητή», δήλωσε ο Andy Jaros, αντιπρόεδρος πωλήσεων και μάρκετινγκ IP (Intellectual Property) στη Flex Logix . «Όλα τα σημεία περιλαμβάνουν κάποια μορφή επικοινωνίας για την παρακολούθηση της δραστηριότητας, από την παρακολούθηση της κατανάλωσης ενέργειας έως τις διακυμάνσεις/ανωμαλίες τάσης έως παρακολούθηση του εξοπλισμού παραγωγής ηλεκτρικής ενέργειας. Κάθε σημείο αντιπροσωπεύει ευάλωτα σημεία πρόσβασης για να εισχωρήσετε στο δίκτυο ενός ΣΗΕ. Εκτός από τις τυπικές τεχνικές κρυπτογράφησης, η προσθήκη ευελιξίας FPGA (Field Programmable Gate Array) στις δικτυωμένες συσκευές μπορεί να γίνει ένα δεύτερο επίπεδο ασφάλειας μέσω συσκότισης κυκλώματος ή/και τη δυνατότητα προσθήκης ιδιόκτητων μέτρων ασφαλείας σε υλικό που μπορεί να ενημερωθεί μετά την ανάπτυξη της συσκευής.Το άλλο πλεονέκτημα των επαναδιαμορφωμένων κυκλωμάτων είναι ότι τα μοντέλα τεχνητής νοημοσύνης μπορούν να εφαρμοστούν (και να ενημερωθούν επιτόπου) για την παρακολούθηση ύποπτων, μη τυπικών επικοινωνιών, κινήσεων δεδομένων ή ανωμαλιών στη λειτουργία του εξοπλισμού».

Υπάρχουν νέα πρότυπα που αναπτύσσονται για να βοηθήσουν σε αυτό, συμπεριλαμβανομένου του IEEE Wi-SUN πεδίου δικτύου (FAN), το οποίο είναι ειδικά σχεδιασμένο για δίκτυα ισχύος.

«Το Wi-UN έχει ένα προφίλ ασφαλείας που πιστοποιητικά που έχουν επικυρωθεί από αξιόπιστες αρχές πιστοποίησης root για την αποτροπή μη εξουσιοδοτημένης πρόσβασης στο δίκτυο», δήλωσε ο Rogerio Almeida, μηχανικός μάρκετινγκ προϊόντων για μάρκετινγκ κάτω του 1 GHz στην Texas Instruments. «Χρησιμοποιεί επίσης αλγόριθμους κρυπτογράφησης, όπως η ελλειπτική καμπύλη Diffie-Hellman, οι αλγόριθμοι ψηφιακής υπογραφής ελλειπτικής καμπύλης και ο κώδικας ταυτότητας αλυσίδων κρυπτογράφησης Standard-128 Advanced Encryption Standard-128 για τη διατήρηση της εμπιστευτικότητας και των ακεραίων μηνών. Αυτό είναι σημαντικό όταν προσθέτετε νέες συσκευές στο δίκτυο και χρησιμοποιείτε την αναγνώριση και τον έλεγχο ταυτότητας τους. Οι κατασκευαστές εξοπλισμού Wi-SUN μπορούν ακόμη και να λάβουν πιστοποιητικό κυβερνοασφάλειας που υποδεικνύει τη συμμόρφωση με την Προδιαγραφή Τεχνικού Προφίλ FAN.

Τα πρότυπα ασφαλείας μπορούν να εφαρμοστούν κατά το σχεδιασμό των συστημάτων δικτύου και του εξοπλισμού ισχύος, κάτι που είναι ιδιαίτερα αποτελεσματικό. Η North American Electric Reliability Corporation (NERC) έχει συντάξει ένα σύνολο προτύπων αξιοπιστίας για τα ηλεκτρικά συστήματα της Βόρειας Αμερικής.

«Οι τεχνολογίες ασύρματης επικοινωνίας χρησιμοποιούνται εδώ και καιρό για τη σύνδεση δικτύων ηλεκτρικής ενέργειας, από το TETRA στο LoRaWAN και το Wi-Fi», δήλωσε η Kalina Barboutov, επικεφαλής ασύρματων προπωλήσεων και επιχειρηματικής ανάπτυξης της Hitachi Energy. «Μέχρι σήμερα, το 5G ως τεχνολογία παρέχει μερικά από τα πιο ισχυρά χαρακτηριστικά και αρχιτεκτονικές ασφάλειας στον κυβερνοχώρο. Όπως συμβαίνει με όλες τις τεχνολογίες 3GPP, η κίνηση 5G είναι κρυπτογραφημένη από άκρο σε άκρο. Η Hitachi Energy είναι ένας μακροχρόνιος προμηθευτής δικτύων ηλεκτρικής ενέργειας με πάνω από 100 χρόνια εμπειρίας και συνεισφοράς στον κλάδο. Ως εκ τούτου, εκτός από τα πρότυπα ασφάλειας στον κυβερνοχώρο 3GPP, συνεχίζουμε να εφαρμόζουμε ειδικά πρότυπα του κλάδου, όπως το IEC 62443 (και τα υποκείμενα πρότυπα), το οποίο επικεντρώνεται στην ασφάλεια στον κυβερνοχώρο των κρίσιμων λειτουργιών του δικτύου σε όλο τον κύκλο ζωής των στοιχείων.

Στις ΗΠΑ, το DoE και το DHS έχουν παράσχει πόρους και πληροφορίες για να αξιοποιήσει τη βιομηχανία, αλλά πρέπει να συνεχίσει να εργάζεται με τη βιομηχανία ηλεκτρικής ενέργειας για να παρέχει ηγεσία και κατευθυντήριες γραμμές για την αξιοποίηση εθνικών στόχων κυβερνοασφάλειας.

«Οι χειριστές πρέπει να συνεργαστούν με εμπειρογνώμονες στον κυβερνοχώρο και τις ομοσπονδιακές υπηρεσίες για να εντοπίσουν τα τρία σημεία στο δίκτυό τους, να μελετήσουν τις βιομηχανικές κατευθυντήριες γραμμές και τα πλαίσια ασφάλειας στον κυβερνοχώρο, να δημιουργήσουν ένα μοντέλο απειλής για να καθορίσουν το απαιτούμενο επίπεδο ασφάλειας για κάθε σύστημα και να το χαρτογραφήσουν στη διαθέσιμη ασφάλεια», είπε η Honda της Honda. «Για κενά, πρέπει να συνεργαστούν με προμηθευτές για να αντιμετωπίσουν τα κενά και να αναπτύξουν τη λύση σε μια σταδιακή προσέγγιση».

Αυτή η ηγεσία είναι απαραίτητη για την ανάπτυξη μιας συνολικής νοοτροπίας κυβερνοασφάλειας και πρέπει να συμβεί σε όλα τα επίπεδα.

«Η προηγμένη τεχνολογία, η ψηφιοποιήσει και η εξέλιξη προς την προσφορά και τη ζήτηση ηλεκτρικής ενέργειας σε πραγματικό χρόνο προκαλούν νέες διασυνδεδεμένες τεχνολογίες και συνεπώς την αυξημένη απειλή κακόβουλων γεωργοασφαλειών», δήλωσε ο Rich Springer, επικεφαλής της επιχειρηματικής στρατηγικής και ανάπτυξης βιομηχανικής κυβερνοασφάλειας στην Tripwire. Το ΣΗΕ είναι πάντα ένας στόχος και πρόσφατα έχουμε δει εκδηλώσεις λύτρων πολλών εκατομμυρίων δολαρίων σε άλλες κρίσιμες υποδομές. Επομένως, δεν είναι θέμα «αν», αλλά «πότε» θα συμβεί η επόμενη επίθεση. Συνεπώς, πρέπει να ενσωματωθεί η κυβερνοασφάλεια στα μελλοντικά σχέδια και να αξιολογηθεί η τρέχουσα υποδομή των ΣΗΕ. Ο κίνδυνος υφίσταται τόσο για απώλειες παραγωγής όσο και για απώλειες στον κυβερνοχώρο (πνευματική ιδιοκτησία, προσωπικές, απώλεια φήμης κ.λπ.), και τα δύο είναι ποσοτικοποιήσιμα. Επομένως, η ανάγκη για έναν ισχυρό προϋπολογισμό για την ασφάλεια στον κυβερνοχώρο δεν είναι αμφισβητήσιμη. Καθώς δικαίως βιαζόμαστε να χρησιμοποιήσουμε το Industry 4.0 και τις έξυπνες πόλεις, πρέπει επίσης να σκεφτούμε με όρους κυβερνοασφάλειας 4.0 και έξυπνων πόλεων με την ασφάλεια στον κυβερνοχώρο. Δυστυχώς, οι πτυχές κινδύνου για την ασφάλεια στον κυβερνοχώρο συχνά θεωρούνται πολύ χαμηλός κίνδυνος ή να προστεθούν αργότερα. Ομοίως, το NERC CIP καλύπτει μόνο τα πιο κρίσιμα τμήματα των λειτουργιών του δικτύου και αφήνει το υπόλοιπο πλέγμα σχετικά ανέγγιχτο. Ως εκ τούτου, πρέπει να αναπτύξουμε μια νοοτροπία για να έχουμε ενσωματωμένη την κυβερνοασφάλεια σε κάθε πτυχή των δικτύων ενέργειας». Καθώς δικαίως βιαζόμαστε να χρησιμοποιήσουμε το Industry 4.0 και τις έξυπνες πόλεις, πρέπει επίσης να σκεφτούμε με όρους κυβερνοασφάλειας 4.0 και έξυπνων πόλεων με την ασφάλεια στον κυβερνοχώρο.Δυστυχώς, οι πτυχές κινδύνου για την ασφάλεια στον κυβερνοχώρο συχνά θεωρούνται πολύ χαμηλός κίνδυνος ή να προστεθούν αργότερα. Ομοίως, το NERC CIP καλύπτει μόνο τα πιο κρίσιμα τμήματα των λειτουργιών του δικτύου και αφήνει το υπόλοιπο πλέγμα σχετικά ανέγγιχτο. Ως εκ τούτου, πρέπει να αναπτύξουμε μια νοοτροπία για να έχουμε ενσωματωμένη την κυβερνοασφάλεια σε κάθε πτυχή των δικτύων ενέργειας». Καθώς δικαίως βιαζόμαστε να χρησιμοποιήσουμε το Industry 4.0 και τις έξυπνες πόλεις, πρέπει επίσης να σκεφτούμε με όρους κυβερνοασφάλειας 4.0 και έξυπνων πόλεων με την ασφάλεια στον κυβερνοχώρο.Δυστυχώς, οι πτυχές κινδύνου για την ασφάλεια στον κυβερνοχώρο συχνά θεωρούνται πολύ χαμηλός κίνδυνος ή να προστεθούν αργότερα. Ομοίως, το NERC CIP καλύπτει μόνο τα πιο κρίσιμα τμήματα των λειτουργιών του δικτύου και αφήνει το υπόλοιπο πλέγμα σχετικά ανέγγιχτο. Ως εκ τούτου, πρέπει να αναπτύξουμε μια νοοτροπία για να έχουμε

ενσωματωμένη την κυβερνοασφάλεια σε κάθε πτυχή των δικτύων ενέργειας». Το NERC CIP καλύπτει μόνο τα πιο κρίσιμα τμήματα των λειτουργιών του δικτύου και αφήνει το υπόλοιπο πλέγμα σχετικά ανέγγιχτο. Ως εκ τούτου, πρέπει να αναπτύξουμε μια νοοτροπία για να έχουμε ενσωματωμένη την κυβερνοασφάλεια σε κάθε πτυχή των δικτύων ενέργειας».Το NERC CIP καλύπτει μόνο τα πιο κρίσιμα τμήματα των λειτουργιών του δικτύου και αφήνει το υπόλοιπο πλέγμα σχετικά ανέγγιχτο. Ως εκ τούτου, πρέπει να αναπτύξουμε μια νοοτροπία για να έχουμε ενσωματωμένη την κυβερνοασφάλεια σε κάθε πτυχή των δικτύων ενέργειας».

Από τη θετική πλευρά, η North American Electric Reliability Corporation (NERC), μια μη κερδοσκοπική διεθνής ρυθμιστική αρχή, με αποστολή να αυξήσει την αξιοπιστία και την ασφάλεια του δικτύου, πρωτοστατεί. Κάθε δύο χρόνια, η άσκηση ασφάλειας δικτύου του NERC, GridEx , θα φιλοξενεί 700 σχεδιαστές για να οδηγήσουν τον οργανισμό τους να συμμετάσχει σε μια προσομοίωση άσκησης για την καταπολέμηση των επιθέσεων στον κυβερνοχώρο. Είναι η μεγαλύτερη τέτοια άσκηση στη Βόρεια Αμερική. Το Κέντρο Διαμοιρασμού και Ανάλυσης Ηλεκτρικών Πληροφοριών του NERC (E-ISAC) θα δημοσιεύσει τα ευρήματά του στην έκθεση άσκησης ασφάλειας δικτύου για να βοηθήσει διάφορους οργανισμούς με παρόμοιο όραμα.

Ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Ασφάλεια στον Κυβερνοχώρο (ENISA) είναι μια κεντρική οντότητα για την προώθηση της ασφάλειας στον κυβερνοχώρο σε όλα τα κράτη μέλη της Ευρωπαϊκής Ένωσης (ΕΕ). Ο προαναφερόμενος φορέας παρέχει εξειδικευμένες γνώσεις, συμβουλές και προτάσεις για την ενίσχυση των ικανοτήτων κυβερνοασφάλειας, προωθεί τη συνεργασία μεταξύ των ενδιαφερομένων μερών και διευκολύνει τη διαμόρφωση στρατηγικών και πολιτικών κυβερνοασφάλειας.

Το Ευρωπαϊκό Κέντρο για το έγκλημα στον κυβερνοχώρο (EC3) είναι ένας θεσμός που δημιουργήθηκε από την Ευρωπόλ με στόχο την αντιμετώπιση του ζητήματος του εγκλήματος στον κυβερνοχώρο σε ολόκληρη την ευρωπαϊκή ήπειρο. Ο εν λόγω φορέας ασχολείται με τον συντονισμό και την παροχή υποστήριξης στις υπηρεσίες επιβολής του νόμου, πραγματοποιεί αξιολογήσεις των πιθανών απειλών, διευκολύνει την ανταλλαγή σχετικών πληροφοριών και οργανώνει συνεργατικές επιχειρήσεις με στόχο την αντιμετώπιση των δραστηριοτήτων του κυβερνοεγκλήματος.

Το Εθνικό Κέντρο Κυβερνοασφάλειας (NCSC) του Ηνωμένου Βασιλείου είναι ένας οργανισμός αφιερωμένος στη διαφύλαξη των ψηφιακών συστημάτων και δικτύων από κυβερνοαπειλές. Το Εθνικό Κέντρο Κυβερνοασφάλειας (NCSC) λειτουργεί ως η κατεξοχήν αρχή κυβερνοασφάλειας στο Ηνωμένο Βασίλειο. Ο εν λόγω φορέας παρέχει κατευθύνσεις και υλικό τόσο σε εταιρικές οντότητες όσο και σε ιδιώτες, προάγει τη γνώση της κυβερνοασφάλειας, εκτελεί αξιολογήσεις των ευπαθειών και συνεργάζεται με παγκόσμιους συνεργάτες για την αντιμετώπιση των κινδύνων στον κυβερνοχώρο.

Το Bundesamt für Sicherheit in der Informationstechnik (BSI), που εδρεύει στη Γερμανία, είναι ένας έγκυρος φορέας υπεύθυνος για τη διασφάλιση της ασφάλειας των πληροφοριών. Το Ομοσπονδιακό Γραφείο για την Ασφάλεια των Πληροφοριών (BSI) είναι η καθορισμένη αρχή που είναι υπεύθυνη για θέματα ασφάλειας στον κυβερνοχώρο σε ομοσπονδιακό επίπεδο στη Γερμανία. Ο οργανισμός παρέχει συστάσεις για την ασφάλεια στον κυβερνοχώρο, σημεία αναφοράς και διαπιστεύσεις για κυβερνητικούς φορείς, εμπορικές επιχειρήσεις και ιδιώτες. Η BSI ασχολείται επίσης με τη διεξαγωγή έρευνας, ανάλυσης και δραστηριοτήτων αντιμετώπισης περιστατικών με στόχο την ενίσχυση της ανθεκτικότητας της κυβερνοασφάλειας.

Το Κέντρο Συντονισμού της Ιαπωνικής Ομάδας Αντιμετώπισης Εκτάκτων Αναγκών Υπολογιστών (Japan Computer Emergency Response Team Coordination Center), που συνήθως αναφέρεται ως JPCERT/CC, είναι μια εξέχουσα οντότητα στον τομέα της ασφάλειας στον κυβερνοχώρο εντός του έθνους της Ιαπωνίας. Ο οργανισμός προσφέρει μια σειρά υπηρεσιών που αποσκοπούν στον μετριασμό των απειλών στον κυβερνοχώρο, συμπεριλαμβανομένης της αντιμετώπισης περιστατικών, του χειρισμού ευπαθειών και της ανταλλαγής πληροφοριών. Το JPCERT/CC ασχολείται επίσης με τη διεξαγωγή έρευνας, κατάρτισης και εκστρατειών ευαισθητοποίησης.

Ο Οργανισμός Κυβερνοασφάλειας (CSA) της Σιγκαπούρης είναι ένας οργανισμός αφιερωμένος στη διαφύλαξη της ασφάλειας και της ακεραιότητας των ψηφιακών συστημάτων και δικτύων εντός της χώρας. Ο Οργανισμός Κυβερνοασφάλειας της Σιγκαπούρης (CSA) είναι ο αρμόδιος φορέας που είναι υπεύθυνος για τη ρύθμιση και την εποπτεία των πρακτικών κυβερνοασφάλειας σε ολόκληρη τη χώρα. Ο οργανισμός συμμετέχει σε προσπάθειες συνεργασίας με κυβερνητικές οντότητες, εμπορικές επιχειρήσεις και τον γενικό πληθυσμό για την αύξηση των ικανοτήτων τους στον τομέα της κυβερνοασφάλειας. Ο Οργανισμός Κυβερνοασφάλειας και Ασφάλειας Υποδομών

(CSA) προσπαθεί να προωθήσει τις βέλτιστες μεθοδολογίες, να εκτελέσει ασκήσεις κυβερνοασφάλειας και να διαμορφώσει τακτικές για την οχύρωση κρίσιμων πληροφοριακών υποδομών.

Ο Οργανισμός Διαδικτύου και Ασφάλειας της Κορέας (KISA) είναι ο καθορισμένος φορέας στον οποίο έχει ανατεθεί η ευθύνη για τη διαφύλαξη του τοπίου της ασφάλειας στον κυβερνοχώρο στη Νότια Κορέα. Ο εν λόγω οργανισμός ασχολείται με τη λειτουργία ομάδων αντιμετώπισης έκτακτων περιστατικών σε υπολογιστές (CERT), την παροχή υπηρεσιών αντιμετώπισης περιστατικών και τη διεξαγωγή ερευνητικών προσπαθειών με στόχο τον μετριασμό των απειλών στον κυβερνοχώρο. Ο KISA παρέχει επιπλέον υποστήριξη σε πρωτοβουλίες που αποσκοπούν στην προώθηση της εκπαίδευσης και της ευαισθητοποίησης στον τομέα της ασφάλειας στον κυβερνοχώρο.

Το Εθνικό Κέντρο Αριστείας για την Κυβερνοασφάλεια (NCCoE) στην Ινδία είναι ένα εξέχον ίδρυμα αφιερωμένο στη μελέτη και την προώθηση της κυβερνοασφάλειας. Το Εθνικό Κέντρο Αριστείας για την Κυβερνοασφάλεια (NCCoE) στην Ινδία είναι αφιερωμένο κυρίως στην προώθηση της έρευνας, της ανάπτυξης και των πρωτοβουλιών δημιουργίας ικανοτήτων στον τομέα της κυβερνοασφάλειας. Ο εν λόγω φορέας συμμετέχει σε προσπάθειες συνεργασίας με ακαδημαϊκά ιδρύματα, βιομηχανικούς οργανισμούς και κυβερνητικές υπηρεσίες, προκειμένου να αντιμετωπίσει αποτελεσματικά τις προκλήσεις που θέτει η κυβερνοασφάλεια. Το Εθνικό Κέντρο Αριστείας για την Κυβερνοασφάλεια (NCCoE) συμμετέχει σε ερευνητικές πρωτοβουλίες, επιμελείται εκπαιδευτικά προγράμματα και υποστηρίζει τα βέλτιστα πρωτόκολλα κυβερνοασφάλειας.

Οι προαναφερθείσες προσπάθειες αποδεικνύουν την αφοσίωση των ευρωπαϊκών και ασιατικών εθνών στην αντιμετώπιση των δυσχερειών της κυβερνοασφάλειας μέσω συνεργατικών εγχειρημάτων, της διάδοσης πληροφοριών, της ενίσχυσης των δυνατοτήτων και της θέσπισης ανθεκτικών πλαισίων και πολιτικών. Μέσω των συνεργατικών προσπαθειών, τα προαναφερθέντα έθνη προσπαθούν να ενισχύσουν το σθένος τους στον τομέα της κυβερνοασφάλειας και να διασφαλίσουν τις ζωτικές υποδομές, τις εμπορικές επιχειρήσεις και τον πληθυσμό τους από κινδύνους στον κυβερνοχώρο.

Κεφάλαιο 3ο : Αποτελέσματα και συζήτηση

3.1 Συζήτηση

Στην τρέχουσα έρευνα σχετικά με τις επιπτώσεις των FDI στα συστήματα ισχύος, το υιοθετημένο μοντέλο FDI είναι συχνά στατικό σε ένα μόνο στιγμιότυπο, αγνοώντας την πολυπλοκότητα της συμπεριφοράς επίθεσης. Ο κίνδυνος των FDI δεν μπορεί να αποκαλυφθεί πλήρως, καθώς οι επιτιθέμενοι είναι σε θέση να κατασκευάσουν μια ανεπαίσθητα δυναμική επίθεση για να αποφύγουν τον εντοπισμό. Οι μελλοντικές προσπάθειες θα πρέπει να αφιερωθούν σε ένα πιο λεπτομερές μοντέλο FDI για να ληφθεί υπόψη η δυναμική συμπεριφορά των επιθέσεων.

Αν και υπάρχει πολλή βιβλιογραφία σχετικά με την επίδραση των FDI στην εκτίμηση της κατάστασης του συστήματος ηλεκτρικής ενέργειας, οι μελέτες για την επιρροή τους στην εκτίμηση της δυναμικής κατάστασης του συστήματος ηλεκτρικής ενέργειας είναι περιορισμένες. Οι εκτιμήσεις δυναμικής κατάστασης του συστήματος ισχύος μπορούν να χρησιμοποιηθούν ως είσοδοι ελεγκτή (π.χ. ελεγκτές απόσβεσης ευρείας περιοχής) για τη βελτίωση της απόδοσης του ελέγχου, ενώ οι εισβολείς μπορούν να μειώσουν την απόδοση του ελέγχου επιτιθέμενοι στην εκτίμηση δυναμικής κατάστασης. Για να προωθηθούν τα κατάλληλα αντίμετρα, είναι απαραίτητο να διερευνηθούν οι επιπτώσεις των FDI στην εκτίμηση της δυναμικής κατάστασης του συστήματος ηλεκτρικής ενέργειας.

Οι περισσότερες έρευνες σχετικά με τον αντίκτυπο των FDI στη σταθερότητα του συστήματος ηλεκτρικής ενέργειας επικεντρώνονται στο σπάσιμο της σταθερότητας της συχνότητας προκαλώντας μια ανισορροπία μεταξύ προσφοράς και ζήτησης. Πρέπει να διεξαχθεί μελλοντική έρευνα για τη μελέτη της αλληλεπίδρασης μεταξύ των FDI και της σταθερότητας μικρού σήματος/παροδικής. Στο σύγχρονο ηλεκτρικό δίκτυο, το σύστημα μέτρησης ευρείας περιοχής αξιοποιείται σε μεγάλο βαθμό για την ανίχνευση ανωμαλιών του συστήματος ισχύος. Τα δεδομένα από τις μονάδες μέτρησης φάσης (PMUs) κοινοποιούνται στο κέντρο ελέγχου για την παρακολούθηση και την απόσβεση των ταλαντώσεων μεταξύ των περιοχών [61]. Η επικοινωνία μεταξύ του PMU και του κέντρου ελέγχου μπορεί να καταστραφεί από επιθέσεις FDI. Αυτό μπορεί να υποβαθμίσει την απόσβεση των ταλαντώσεων μεταξύ των περιοχών και να προκαλέσει αστάθεια μικρού σήματος.

3.2 Συμπέρασμα

Με την ταχεία ανάπτυξη του έξυπνου δικτύου και την ευρεία χρήση της τεχνολογίας πληροφοριών και επικοινωνιών στα συμβατικά ΣΗΕ και μικροδίκτυα, η βιομηχανία ηλεκτρικής ενέργειας αντιμετωπίζει απειλές στον κυβερνοχώρο. Πρώτον, η οικονομική αποστολή μπορεί επίσης να επηρεαστεί αρνητικά από το σχεδιασμό βέλτιστων επιθέσεων FDI και την ενεργοποίηση ενός αρχικού έκτακτου κινδύνου που κατά συνέπεια προκαλεί διαδοχικές διακοπές λειτουργίας. Δεύτερον, Μια μη ανιχνεύσιμη επίθεση FDI μπορεί να ξεκινήσει χρησιμοποιώντας τις πληροφορίες πλήρους/τοπικού δικτύου. Τρίτον, η αστάθεια συχνότητας μπορεί να προκληθεί από την έγχυση ψευδών δεδομένων που εμποδίζουν την ενεργή έξοδο ισχύος ενός μετατροπέα ισχύος να παρακολουθεί την εντολή αποστολής του. Οι εισβολείς μπορούν επίσης να θέσουν σε κίνδυνο τον συνεργατικό έλεγχο ενός μικροδικτύου επιτιθέμενοι στους ελεγκτές. Η αστάθεια συχνότητας μπορεί να προκληθεί από την έγχυση ψευδών δεδομένων που εμποδίζουν την ενεργή έξοδο ισχύος ενός μετατροπέα ισχύος να παρακολουθεί την εντολή αποστολής του. Οι εισβολείς μπορούν επίσης να θέσουν σε κίνδυνο τον συνεργατικό έλεγχο ενός μικροδικτύου επιτιθέμενοι στους ελεγκτές.

Βιβλιογραφία

1. Liang, G., Zhao, J., Luo, F. J., Weller, S., & Dong, Z. (2017). A review of false data injection attacks against modern power systems. *IEEE Transactions on sensible Grid*, 8(4), 1630–1638.

2. Che, L., Liu, X., Shuai, Z., Li, Z., & Wen, Y. (2018). Cyber cascades screening considering the impacts of false information injection attacks. *IEEE Transactions on Power equipment and Systems*, 33(6), 6545–6556.

3. Che, L., Liu, X., Li, Z., & Wen, Y. (2019). False information injection attacks elicited serial outages in power systems. *IEEE Transactions on Power equipment and Systems*, 34(2), 1513–1522.

4. Yuan, Y., Li, Z., & Ren, K. (2011). Modeling load distribution attacks in power systems. *IEEE Transactions on sensible Grid*, 3(3), 382–390.

5. Liu, X., Li, Z., Shuai, Z., & Wen, Y. (2017). Cyber-attacks against the economic operation of power system: a quick resolution. *IEEE Transactions on sensible Grid*, 8(2), 1023–1025.

6. Xiang, Y., Ding, Z., Zhang, Y., & Wang, L. (2017). power grid responsibleness analysis considering load distribution attacks. *IEEE Transactions on sensible Grid*, 8(2), 889–901.

7. Liu, X., & Li, Z. (2014). native load distribution attacks in power systems with incomplete network info. *IEEE Transactions on sensible Grid*, 5(4), 1665–1676.

8. Zhang, Y., Wang, L., Xiang, Y., & Ten, C. (2015). power grid responsibleness analysis with SCADA cybersecurity issues. *IEEE Transactions on sensible Grid*, 6(4), 170–1721.

9. Zhang, Z., Gong, S., Dimitrovski, A., & Li, H. (2013). Time synchronization attack in sensible grid: Impact and analysis. *IEEE Transactions on sensible Grid*, 4(1), 87–98.

10. Kosut, O., Jia, L., Thomas, R., & Tong, L. (2011). Malicious information attacks

on the sensible grid. *IEEE Transactions on sensible Grid*, 2(4), 645–658
11. Liu, X., & Li, Z. (2017). False information attacks against ac state estimation with incomplete network info. *IEEE Transactions on sensible Grid*, 8(5), 2239–2248.

12. Zhao, J., Zhang, G., Dong, Z., & Wong, K. (2016). Foresting-aided imperfect false information injection attacks against power grid nonlinear state estimation. IEEE Transactions on sensible Grid, 7(1),

13. Zhao, J., Mili, L., & Wang, M. (2018). A generalized false information injection attacks against power grid nonlinear state computer and countermeasures. *IEEE Transactions on Power equipment and Systems*, 33(5), 4868–4877.

14. Deng, R. L., Zhuang, P., & Liang, H. (2019). False information injection attacks against state estimation in power distribution systems. *IEEE Transactions on sensible Grid, 10*I (3), 2871–2881.

15. Bi, S., & Zhang, Y. (2014). False information injection attacks with restricted susceptance info and new countermeasures in sensible grid. *IEEE Transactions on sensible Grid,* 15(3), 1619–1628.

16. Liu, Y., Xin, H., Qu, Z., & Gan, D. (2016). associate attack-resilient cooperative management strategy of multiple distributed generators in distribution networks. *IEEE Transactions on sensible Grid*, 7(6), 2923–2932.

17. Abhinav, S., Modares, H., Lewis, F., Ferrese, F., & Davoudi, A. (2018). synchronizing in networked microgrids underneath attacks. *IEEE Transactions on sensible Grid,* 9(6), 6731–6741.

18. Liu, S., Mashayekh, S., Kundur, D., Zourntos, T., & Bulter-Purry, K. (2012). *A*

sensible grid vulnerability analysis framework for coordinated variable structure change attacks, (pp. 1–6). San Diego: Proc. IEEE PES. Gen. Meeting.

19. Chen, B., Mashayekh, S., Butler-Purry, L., & Kundur, D. (2013). *Impact of cyber attacks on transient stability of sensible grids with voltage support devices,* (pp. 1–5). Vancouver: Proc. IEEE PES info. Meeting.

20. Brown, H., & DeMarco, C. (2018). Risk of cyber-physical attack via load with emulated inertia management. *IEEE Transactions on sensible Grid*, 9(6), 5854–5866.

21. Athari, M., & Wang, Z. (2018). Impacts of wind generation uncertainty on grid vulnerability to cascading overload failures. *IEEE Transactions on property Energy*, 9(1), 128–137.

22. Liang, G. Q., Weller, S. R., Luo, F. J., Zhao, J. H., & Dong, Z. Y. (2018). Generalized FDIA-based cyber topology attack with application to the Australian electricity market mercantilism mechanism. *IEEE Transactions on sensible Grid*, *9*(4), 3820–3829.

23. Final report on the August fourteen, 2003, blackout within the us and Canada: Causes and proposals. https://energy.gov/sites/prod/files/oeprod/documentsandmedia/blackoutfinal-web.pdf . Accessed 12 June 2022.

24. Vaiman, M. (2012). Risk assessment of cascading failures: Methodologies and challenges. *IEEE Transactions on Power equipment and Systems*, 27(2), 631–641.

25. Eppstein, M., & Hines, P. (2012). A random chemistry formula for characteristic collections of multiples contingencies that initiate cascading failure. *IEEE Transactions on Power equipment and Systems*, 27(3), 1698–1705.

26. Liang, J., Sankar, L., & Kosut, O. (2016). Vulnerability analysis and consequence of false information injection attack on power grid state estimation. *IEEE Transactions on Power equipment and Systems*, *31*(5), 3864–3872.

27. Wang, H. Z., Ruan, J. Q., Zhou, B., Li, C. B., Wu, Q. W., Raza, M. Q., & Cao, G. Z. (2019). Dynamic information injection attack detection of cyber physical power systems with uncertainties. *IEEE Transactions on Industrial science*, 15(10), 5505–5518.

28. Wood, A., & Wollenberg, B. (1996). *Power generation, operation and management*, (2nd ed.,). Hoboken: Wiley.

29. Qu, Z., & Simaan, M. (2014). Modularized style for cooperative management and plug-and-play operation of networked heterogeneous systems. *Automatica*, 50(9), 2405–2414.

30. Dorfler, F., Simpson-Porco, J., & Bullo, F. (2014). *Plug-and-play management and improvement in microgrids*, (pp. 211–216). Los Angeles: IEEE Conference on call and management.

31. Rocaber, J., Luna, A., Blaabjerg, F., & Rodriguez, P. (2012). management of power converters in AC microgrids. *IEEE Transactions on Power physical science*, 27(11), 4734–4749.

32. Simpson-Porco, J. (2015). Secondary frequency and voltage management of islanded microgrids via distributed averaging. *IEEE Transactions on Industrial physical science*, 62(11), 7025–7038.

33. Schiffer, J., Seel, T., Raisch, J., & Sezi, T. (2016). Voltage stability and reactive

power sharing in inverter-based microgrids with consensus-based distributed voltage management. *IEEE Transactions on management Systems Technology*, 24(1), 96–109.

34. Nasirian, V., Shafiee, Q., Guerrero, J., Lewis, F., & Davoudi, A. (2016). Droop-free distributed management for AC microgrids. *IEEE Transactions on Power physical science*, 31(2), 1600–1617.

35. Guo, M., Dimarogonas, D., & Johansson, K. (2012). *Distributed period of time fault detection and isolation for cooperative multi-agent systems*, (pp. 5270–5275). Montreal: Proc. Amer. management Conf.

36. Gusrialdi, A., Qu, Z., & Simaan, M. (2014). *Sturdy style of cooperative systems against attacks*, (pp. 1456–1462). Portland: Proc. Amer. Conf.

37. Horn, R., & Johnson, C. (1985). *Matrix analysis.* Cambridge: Cambridge Univ. Press.

38. Bidram, A., Lewis, F., & Davoudi, A. (2014). Distributed management systems for small-scale power networks: victimization multiagent cooperative management theory. *IEEE management Systems*, 34(6), 56–77.]

39. Vyver, J., De Kooning, J., Meersman, B., Vandevelde, L., & Vandoorn, T. (2016). Droop management as an alternate mechanical phenomenon response strategy for the artificial inertia on wind turbines. *IEEE Transactions on Power equipment and Systems*, 2(31), 1129–1138.

40. Ye, H., Pei, W., & Qi, Z. (2016). Analytical modeling of mechanical phenomenon and droop responses from a power plant for short-run frequency regulation in power systems. *IEEE Transactions on Power equipment and Systems*, 31(5), 3414–3423.

41. Ramtharan, G., Ekanayake, J., & Jenkins, N. (2007). Frequency support from doubly fed induction generator wind turbines. *IET Renewable Power Generation*, 1(1), 3–9.

42. Morren, J., Pierik, J., & DeHaan, S. (2006). Mechanical phenomenon response of variable speed wind turbines. *Electrical power Systems analysis*, 76(11), 980–987.

43. Liu, W., Gu, W., Sheng, W., Meng, X., Xue, S., & Chen, M. (2016). Pinning-based distributed cooperative management for autonomous microgrids underneath unsure communication topologies. *IEEE Transactions on Power equipment and Systems*, 2(31), 1320–1329.

44. Guo, F., Wen, C., Mao, J., Chen, J., & Song, Y. (2015). Distributed cooperative secondary management for voltage unbalance compensation in associate islanded microgrid. *IEEE Transactions on Industrial science*, 11(5), 1078–1088.

45. Manaffam, S., Talebi, M., Jain, A., & Behal, A. (2018). Intelligent promise primarily based cooperative secondary management of distributed generators for microgrid in islanding operation mode. *IEEE Transactions on Power equipment and Systems, 33(*2), 1364–1373.

46. Su, H., Rong, Z., Chen, Q., Wang, X., Chen, G., & Wang, H. (2013). redistributed accommodative promise management for cluster synchronization of advanced dynamic networks. *IEEE dealings on Cybernatics*, 43(1), 394–399.

47. Bidram, A., Davoudi, A., Lewis, F., & Guerrero, J. (2013). Distributed cooperative secondary management of microgrids victimization feedback linearization. *IEEE Transactions on Power equipment and Systems*, 28(3), 3462–3470.

48. DeLellis, P., Di Bernardo, M., & Garofalo, F. (2013). accommodative promise

management of networks of circuits and systems in Lur'e type. *IEEE dealings Circuits System I, RegPapers*, 60(11), 3033–3042.

49. Chen, T., Liu, X., & Lu, W. (2007). promise advanced networks by one controller. *IEEE dealings Circuits System I, RegPapers*, 54(6), 1317–1326.

50. Manaffam, S., Talebi, M., Jain, A., & Behal, A. (2017). Synchronization in networks of identical systems via pinning: Application to distributed secondary management of microgrids. *IEEE Transactions on management Systems Technology*, 25(6), 2227–2234.

51. Amin, S., Schwartz, G., & Sastry, S. (2013). Security of mutualist and identical networked management systems. *Automatica*, 49(1), 186–192.

52. Pasqualetti, F., Bicchi, A., & Bullo, F. (2012). accord computation in unreliable networks: A system suppositional approach. *IEEE Transactions on Automatic management*, 57(1), 90–104.

53. Pasqualetti, F., Dorfler, F., & Bullo, F. (2013). Attack detection and identification in cyber-physical systems. *IEEE Transactions on Automatic management*, 58(11), 2715–2729.

54. Abhinav, S., Schizas, I., Lewis, F., & Davoudi, A. (2018). Distributed noise-resilient networked synchronizing of active distribution systems. *IEEE Transactions on sensible Grid*, 9(2), 836–846.

55. Pan, K., Teixeira, A., Cvetkovic, M., & Palensky, P. (2019). Cyber risk analysis of combined information attacks against power grid state estimation. *IEEE Transactions on sensible Grid*, 10(3), 3044–3056.

56. Teixeira, A. (2010). *Cyber security analysis of state estimators in electrical power systems,* (pp. 5991–5998). Atlanta: Proc. forty ninth IEEE Conf., on selections and management.

57. Andersson, G. (2012). *Cyber-security of SCADA systems,* (pp. 1–2). Washington, DC: Proc. IEEE PES Innovative sensible Grid Technologies.

58. Olfati-Saber, R., & Murray, R. (2005). accord issues in networks of agents with change topology and time-delays. *IEEE Transactions on Automatic management*, 49(9), 1520–1533.

59. Fax, J., & Murray, R. (2004). info flow and cooperative management of car formations. *IEEE Transactions on Automatic management,* 49, 1465–1475.

60. Olfati-Saber, R., & Shamma, J. (2005). accord filters for detector networks and distributed detector fusion. *In Proc. forty fourth IEEE Conf. call and management /European management Conf,* (pp. 6698–6703).

61. Appasani, B., & Dusmanta, M. (2018). A review on synchrophasor communication system: Communication technologies, standards and applications. *In Protection and management of contemporary power systems.*