ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Με θέμα:

«**ΧΡΗΣΗ ΝΕΥΡΩΝΙΚΩΝ ΔΙΚΤΥΩΝ**

ΣΕ ΘΕΜΑΤΑ ΑΣΦΑΛΕΙΑΣ»

Της φοιτήτριας:

Μαγκίνα Αλεξίας, Α.Μ.:Ε/07098

Επιβλέπων καθηγητής:

Λαμπρινουδάκης Κωνσταντίνος, Επίκουρος Καθηγητής

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΕΦΑΛΑΙΟ 1^{ο} – ΝΕΥΡΩΝΙΚΑ ΔΙΚΤΥΑ

(Neural Network)

Στο κεφάλαιο αυτό θα αναλύσουμε τη σημασία του όρου «νευρωνικά δίκτυα», τι είναι πως ξεκίνησε η ιδέα καθώς και ποιες ομοιότητες μπορούμε να πούμε ότι έχει με τον ανθρώπινο οργανισμό. Επιπροσθέτως, θα αναλυθεί η δομή τους, τα είδη των αρχιτεκτονικών που τα συναντούμε, τους τομείς που έχουν ‘‘καταλάβει’’ με τις πρωτοποριακές λύσεις που προσφέρουν. Τέλος θα αναφερθούν τα βασικά πλεονεκτήματα τα οποία στην ουσία είναι οι πιο ενδιαφέρουσες και πρακτικές ιδιότητες που έχουν και εξυπηρετούν συγκεκριμένους σκοπούς.

1.1. ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ

Το πρώτο μοντέλο τεχνητού νευρωνικού δικτύου κατασκευάστηκε το 1943 από τους McCulloch και Pitts. Το μοντέλο αυτό παρουσιάζει τους νευρώνες ως μία βασική μονάδα (συστατικό) δικτύου. Οι ερευνητές αυτοί παρουσίασαν για πρώτη φορά την ιδέα ότι ένα νευρωνικό δίκτυο αποτελείται από μία συλλογή ενός μεγάλου αριθμού νευρώνων και έδειξαν πώς θα μπορούσαν να λειτουργούν οι νευρώνες με τις διασυνδέσεις τους.

Το 1949 ο Hebb δημοσίευσε την μελέτη του με τίτλο “The organization of behavior” η οποία προσέφερε στους ερευνητές μια θεμελιώδη αρχή, το μοντέλο μάθησης του Hebb το οποίο υποστήριζε πώς: κάθε φορά που ενεργοποιείται μια σύναψη, αυτή ενισχύεται, με αποτέλεσμα το δίκτυο να μαθαίνει ‘‘λίγο περισσότερο’’ το πρότυπο που παρουσιάζεται εκείνη τη στιγμή.

Το 1957 ο Rosenblatt παρουσίασε το μοντέλο απλού αισθητήρα-perceptron, ο οποίος αρχικά έφτιαξε το πρώτο δίκτυο με hardware που μπορούσε να κάνει διάφορες διεργασίες. Το απλό αυτό μοντέλο είχε μόνο δυο επίπεδα, αυτό της εισόδου και αυτό της εξόδου. Το σήμα προχωρά μονόδρομα από την είσοδο στην έξοδο.

Το 1969 οι Minsky και Papert απέδειξαν με μαθηματικό τρόπο ότι τα τεχνητά νευρωνικά δίκτυα ενός επιπέδου δεν μπορούν να λύσουν συγκεκριμένα προβλήματα. Στην έρευνά τους αυτή, λοιπόν, γίνεται μια συνολική εκτίμηση της χρησιμότητας του προτύπου του αισθητήρα και όλων των διεργασιών για τα οποία αυτό το πρότυπο είναι χρήσιμο. Η μαθηματική απόδειξη που αναφέρθηκε παραπάνω, στηρίζεται στο ότι υπάρχει μια πληθώρα περιορισμών στο πρότυπο αυτό που το καθιστούν ανίκανο να χρησιμοποιείται σε συγκεκριμένα προβλήματα.

Το 1982 ήρθε στο φώς από τον Hopfield η μαθηματική απόδειξη ότι ένα νευρωνικό δίκτυο πολλών επιπέδων μπορεί να αποθηκεύσει οποιαδήποτε πληροφορία καθώς και να επανακτήσει όλη την πληροφορία ενός συστήματος έστω και αν του δοθούν μόνο κάποια τμήματα του συστήματος και όχι όλο το σύστημα.

Το 1986 έγινε αποδεκτή από τους επιστήμονες η μέθοδος οπισθοδιάδοσης για την εκπαίδευση τεχνητών νευρωνικών δικτύων που παρουσιάστηκε από τους McClelland και Rumelhart. Παρουσιάζεται η ιδέα πώς ένα νευρωνικό δίκτυο μπορεί να θεωρηθεί και να χρησιμοποιηθεί ως παράλληλος επεξεργαστής. Το έργο αυτό κάνει ένα σημαντικό βήμα πέρα από το Perceptron, με το να επιτρέπει την ύπαρξη και άλλων επιπέδων νευρώνων, εκτός από την είσοδο και την έξοδο, που αποτελούν την εσωτερική δομή του δικτύου. Προτείνουν μία νέα διαδικασία εκπαίδευσης, την μέθοδο της οπισθοδιάδοσης (back–propagation. Η μέθοδος αυτή είχε προταθεί και πιο νωρίς αλλά η ολοκληρωμένη και αποδεδειγμένη παρουσίασή της έγινε το 1986.

Σήμερα, τα νευρωνικά δίκτυα καταλαμβάνουν ένα μεγάλο μέρος στην καθημερινότητά μας έστω και εν αγνοία μας, σε πολλούς τομείς που θα αναφερθούν στη συνέχεια. Η ανάπτυξή τους τα τελευταία χρόνια γίνεται με σταθερό ρυθμό και με σωστά βήματα. Καθώς ο κλάδος της τεχνητής νοημοσύνης εξελίσσεται με ραγδαίους ρυθμούς, έχοντας ως υπόβαθρο τα νευρωνικά δίκτυα, μπορεί κανείς να κατανοήσει πως οι μελέτες, εξελίξεις αλλά και ολοένα περισσότερες εκπλήξεις πάνω στο θέμα δεν παύουν ούτε θα πάψουν να συμβαίνουν.

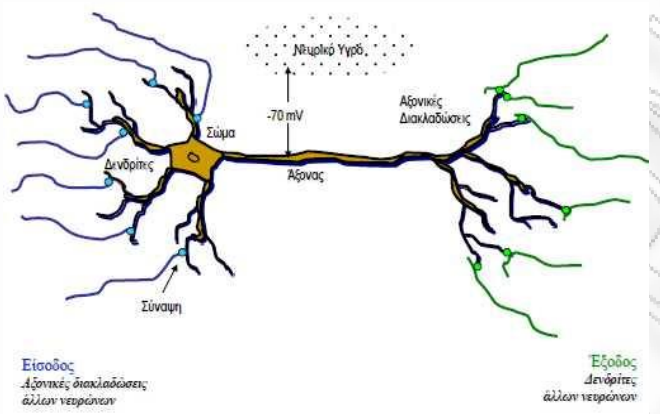
1.2. ΤΙ ΕΙΝΑΙ ΤΑ ΝΕΥΡΩΝΙΚΑ ΔΙΚΤΥΑ (Neural network)

Τα τεχνητά νευρωνικά δίκτυα δεν είναι παρά δίκτυα υπολογιστών και προγράμματα για υπολογιστές, ή και συστήματα εν γένει, που προσομοιώνουν την βιολογική οργάνωση και λειτουργία των νευρώνων. Στην ουσία υπάρχει ένας εγκέφαλος (όπως και στο ανθρώπινο σώμα) και απλουστέρα μέλη, οι νευρώνες.

Η λειτουργία τους προσπαθεί να συνδυάσει τον τρόπο σκέψης του ανθρώπινου εγκεφάλου με τον αφηρημένο μαθηματικό τρόπο σκέψης. Έτσι στα νευρωνικά δίκτυα χρησιμοποιούμε τέτοιες ιδέες όπως για παράδειγμα ένα δίκτυο μαθαίνει και εκπαιδεύεται, θυμάται ή ξεχνά μια αριθμητική τιμή κοκ., πράγματα που μέχρι τώρα τα αποδίδαμε μόνο στην ανθρώπινη σκέψη. Αλλά βέβαια μπορούν και χρησιμοποιούν επί πλέον και περίπλοκες μαθηματικές συναρτήσεις και κάθε είδους εργαλεία από την μαθηματική ανάλυση

1.2.1. ΒΙΟΛΟΓΙΚΑ ΝΕΥΡΩΝΙΚΑ ΔΙΚΤΥΑ

(Biological Neural Network)



Σχήμα 1.1

Στο σχήμα 1.1 φαίνεται η δομή ενός βιολογικού νευρωνικού δικτύου. Ο τρόπος λειτουργίας του πιο αναλυτικά:

Ο εγκέφαλος οργανώνει τους νευρώνες ώστε να μπορούν να πραγματοποιηθούν (εκτελεστούν) συγκεκριμένοι υπολογισμοί και λειτουργίες πιο γρήγορα από οποιοδήποτε ψηφιακό μέσο. Ουσιαστικά, σύμφωνα με τη δομή του, ο ανθρώπινος εγκέφαλος είναι ένα μη-γραμμικό σύστημα με μεγάλη πολυπλοκότητα.

Ο εγκέφαλος κατασκευάζει μόνος του και από το μηδέν τους δικούς του κανόνες οι οποίοι με τον καιρό και την εμπειρία αυξάνονται, διαφοροποιούνται ή αναπτύσσονται σημαντικά ανάλογα τα ερεθίσματα που έχει λάβει. Κατά τα δύο πρώτα χρόνια της ζωής μας έχουμε μέγιστη ανάπτυξη κατά την οποία δημιουργούνται ένα εκατομμύριο συνάψεις το δευτερόλεπτο.

Οι συνάψεις είναι οι βασικές δομικές και λειτουργικές μονάδες που μεσολαβούν στην ενδοεπικοινωνία των νευρώνων. Με άλλα λόγια είναι οι συνδέσεις των νευρώνων με τους άξονες και τους δενδρίτες.

1.2.2. ΤΕΧΝΗΤΑ ΝΕΥΡΩΝΙΚΑ ΔΙΚΤΥΑ (Artificial Neural Networks)

Τα τεχνητά νευρωνικά δίκτυα αποτελούν προσέγγιση της λειτουργίας του ανθρώπινου εγκεφάλου. Η αρχιτεκτονική τους βασίζεται στην αρχιτεκτονική

των βιολογικών νευρωνικών δικτύων. Έτσι, όπως στα βιολογικά εκπαιδεύεται ο εγκέφαλος με τον τρόπο που αναφέρθηκε παραπάνω, έτσι και στα τεχνητά η εκπαίδευση γίνεται με την βοήθεια παραδειγμάτων με τρόπο τέτοιο ώστε να «μαθαίνουν» το περιβάλλον τους και να «αντιλαμβάνονται» πως πρέπει ανάλογα με την κατάσταση να λειτουργήσουν κάθε φορά.

Σαφώς και τα Νευρωνικά Δίκτυα ανήκουν σε διάφορες κατηγορίες ανάλογα με την αρχιτεκτονική τους και τον τρόπο εκπαίδευσής τους.

1.2.3. ΚΟΙΝΑ ΣΗΜΕΙΑ ΒΙΟΛΟΓΙΚΩΝ ΚΑΙ ΤΕΧΝΗΤΩΝ ΝΕΥΡΩΝΙΚΩΝ ΔΙΚΤΥΩΝ

Και στις δύο περιπτώσεις η γνώση αποκτάται από το δίκτυο μέσα από διαδικασία μάθησης (διαφορετικού τύπου εκπαίδευση αλλά με κοινό άξονα και στόχο). Το επόμενο κοινό σημείο είναι ότι οι δυνάμεις των νευρώνων, γνωστές ως συναπτικά βάρη (synaptic), χρησιμοποιούνται για την αποθήκευση γνώσης.

1.3. ΔΟΜΗ ΕΝΟΣ ΤΕΧΝΙΚΟΥ ΝΕΥΡΩΝΙΚΟΥ ΔΙΚΤΥΟΥ

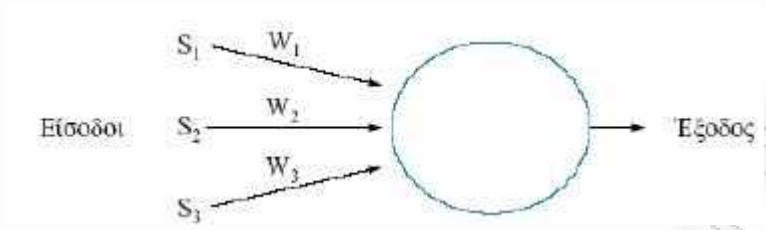
Σε αυτό το σημείο θα γίνει μια περιγραφή της δομής και του τρόπου λειτουργίας αυτού του ιδιόμορφου είδους δικτύων. Από αυτό το σημείο και έπειτα όπου συναντάμε τον όρο νευρωνικά δίκτυα αναφερόμαστε στα τεχνικά νευρωνικά δίκτυα ή χάριν συντομίας ΤΝΔ.

1.3.1. ΓΕΝΙΚΗ ΔΟΜΗ ΝΕΥΡΩΝΙΚΩΝ ΔΙΚΤΥΩΝ

Ένα τεχνητό νευρωνικό δίκτυο αποτελείται από πολλούς νευρώνες συνδεδεμένους μεταξύ τους, καθένας από τους οποίους έχει πολλές εισόδους αλλά μόνο μία έξοδο. Η μοναδική έξοδος του κάθε νευρώνα (μπορεί να) αποτελεί είσοδο για τον άλλο-ους νευρώνα-ες. Η σύνδεση του ενός νευρώνα με τον άλλο μπορεί να ποικίλει στην σημαντικότητα της, η οποία προσδιορίζει το βάρος (σύναψη) άρα και το κόστος της σύνδεσης.

Για να υποστεί κάποιος νευρώνας μεταποιήσεις στις ρυθμίσεις του πρέπει να τρέξει η συνάρτηση μεταφοράς. Αυτή είναι ο κύριος παράγοντας ο οποίος καθορίζει την κάθε έξοδο σε σχέση με τις εισόδους και τους συντελεστές βάρους.

1.3.2. ΔΟΜΗ ΝΕΥΡΩΝΑ



Σχήμα 1.2

Στο σχήμα αυτό ο κύκλος είναι ο νευρώνας ο οποίος έχει πολλές εισόδους (s_1 , s_2, s_3, …) οι οποίες έχουν αντίστοιχα βάρη (w_1, w_2, w_3, …) και μία έξοδο.

Είσοδος:

Όπως φαίνεται και στο σχήμα κάθε σήμα (S_1,S_2,S_3) χαρακτηρίζεται από μία πολύ συγκεκριμένη τιμή βάρους (W_1,W_2 ,W_3) που μαρτυρά την σημαντικότητα του κάθε σήματος. Στην ουσία είσοδος του νευρώνα είναι ο συνδυασμός των σημάτων ανάλογα με τον τύπο και τη λειτουργία που καλείται να κάνει το καθένα.

Έξοδος:

Η έξοδος από το νευρώνα είναι μοναδική και είναι συνάρτηση των σημάτων εισόδου. Η έξοδος ενός νευρώνα μπορεί να αποτελεί είσοδο για έναν άλλο νευρώνα του δικτύου.

Πιο ειδικά…..

Ένας νευρώνας πρακτικά είναι μια μονάδα επεξεργασίας πληροφορίας η οποία αποτελείται από τρία βασικά στοιχεία : α) ένα σύνολο από συνάψεις και συνδετικούς κρίκους, β) έναν αθροιστή και γ) μια συνάρτηση ενεργοποίησης.

Κάθε σύναψη χαρακτηρίζεται από ένα βάρος. Για παράδειγμα έστω ένα σήμα x_j στην είσοδο της σύναψης j το οποίο συνδέεται με το νευρώνα k πολλαπλασιάζεται με το συναπτικό βάρος $w_{kj,}$ το οποίο έχει θετικό πρόσημοο όταν σύναψη είναι διεγερτική και αρνητικό όταν είναι απαγορευτική.

Η συνάρτηση ενεργοποίησης χρησιμοποιείται για την μείωση του εύρους της εξόδου του νευρώνα. Η συνάρτηση ενεργοποίησης ορίζει την έξοδο του

νευρώνα συναρτήσει του επιπέδου ενεργοποίησης της εισόδου. Η συγκεκριμένη συνάρτηση κατατάσσεται σε τρεις τύπους :

- ✓ Τη συνάρτηση κατωφλίου, η οποία δίδεται από τον τύπο
  $\varphi(\upsilon) = \begin{cases} 1, \alpha\nu\ \tau o\ \upsilon \geq 0 \\ 0, \alpha\nu\ \tau o\ \upsilon < 0 \end{cases}$.

Στην πρώτη αυτή περίπτωση, ο νευρώνας εδώ δρα ως δυαδικό στοιχείο, γι' αυτό η έξοδός του, *f*(*x*), θα είναι 1 όταν είναι ενεργοποιημένος και 0 όταν είναι αδρανής

- ✓ Την τμηματικά γραμμική συνάρτηση, η οποία δίνεται από τον τύπο
  $$\varphi(\upsilon) = \begin{cases} 1, \acute{o}\tau\alpha\nu\ \upsilon \geq \frac{1}{2} \\ \upsilon, \acute{o}\tau\alpha\nu - \frac{1}{2} < \upsilon < \frac{1}{2} \\ 0, \acute{o}\tau\alpha\nu\ \upsilon \leq \frac{1}{2} \end{cases}$$

- ✓ Τη σιγμοειδή συνάρτηση, η οποία είναι η συνάρτηση που χρησιμοποιείται πιο συχνά στην κατασκευή τεχνητών νευρωνικών δικτύων. Ουσιαστικά πρόκειται για μια αυστηρά αύξουσα συνάρτηση που δίνεται από τον τύπο:
  $\varphi(\upsilon) = \frac{1}{1+e^{-\upsilon}}$

Η συνάρτηση κατωφλίου και η σιγμοειδής είναι αυτές που συναντάμε πιο συχνά ως συναρτήσεις ενεργοποίησης (activation function) ή συνάρτηση μεταφοράς (transfer function). Το κυριότερο κοινό τους χαρακτηριστικό είναι ότι πρέπει να είναι μη γραμμικές. Σε περίπτωση γραμμικής συνάρτησης η έξοδος θα είναι πάντα ανάλογη με την είσοδο, κάτι το οποίο δεν δύναται να συμβεί στα νευρωνικά δίκτυα.

1.4. ΝΕΥΡΩΝΙΚΑ ΔΙΚΤΥΑ ΚΑΙ ΥΠΟΛΟΓΙΣΤΕΣ

Τα νευρωνικά δίκτυα σχεδόν ποτέ δεν είναι τόσο απλά όπως αναφέραμε παραπάνω, δηλαδή να αποτελείται από έναν μόνο νευρώνα. Ως επί των πλείστων τα νευρωνικά δίκτυα είναι πιο περίπλοκα αποτελούμενα από πολλούς νευρώνες οι οποίοι συνδέονται μεταξύ τους με κάποια συγκεκριμένη αρχιτεκτονική-δομή. Η αρχιτεκτονική αυτή είναι τελείως διαφορετική από την γνωστή των παραδοσιακών υπολογιστών (ή και δικτύων) που περιέχουν έναν επεξεργαστή.

Οι κλασικοί υπολογιστές λειτουργούν σειριακά σε αντίθεση με τα ιδιόμορφα δίκτυα που μελετάμε τα οποία δεν λειτουργούν με σειριακό τρόπο αλλά με παράλληλο τρόπο λειτουργίας, εφόσον μια εργασία μοιράζεται σε επιμέρους νευρώνες που λειτουργούν παράλληλα. Έτσι τα δίκτυα αυτά θεωρούνται συστήματα ‘‘παράλληλων κατανεμημένων διεργασιών’’ (parallel distributed processing). Αυτό σαφώς και προσδίδει ταχύτητα στο σύστημα καθώς είναι σαν να λειτουργούν ταυτοχρόνως πολλοί επεξεργαστές. Παρόλα αυτά η αρχιτεκτονική των νευρωνικών δικτύων διαφέρει σημαντικά από αυτή των παράλληλων επεξεργαστών, για τον λόγω ότι οι απλοί επεξεργαστές των νευρωνικών δικτύων, με άλλα λόγια οι νευρώνες, έχουν μεγάλο αριθμό διασυνδέσεων, πολύ περισσότερες από τον συνολικό αριθμό νευρώνων εφόσον ένας νευρώνας μπορεί να έχει περισσότερες της μίας διασύνδεσης. Στους παράλληλους υπολογιστές απ’ την άλλη, οι επεξεργαστές δύναται να είναι περισσότεροι από τις διασυνδέσεις, κάτι που λαμβάνει χώρα στην πλειοψηφία των περιπτώσεων.

Σε ένα σύστημα παράλληλων υπολογιστών επιβάλλεται συγχρονισμός των επεξεργαστών (καθώς μιλάμε για κατανεμημένα συστήματα) για να μπορεί διεξαχθεί σωστά μια διεργασία. Στα νευρωνικά δίκτυα οι νευρώνες δεν χρειάζονται συγχρονισμό αφού λειτουργούν ανεξάρτητα ο ένας από τον άλλον. Σημαντικό πλεονέκτημα για τα νευρωνικά δίκτυα που τους προσδίδει ανοχή σε σφάλματα όπως θα αναλύσουμε και παρακάτω.

Μία εξίσου άξια αναφοράς διαφορά είναι ότι σε ένα στα νευρωνικά δίκτυα η πληροφορία που αποθηκεύεται διαμοιράζεται σε πολλούς νευρώνες. Αντιθέτως, σε έναν υπολογιστή η πληροφορία αποθηκεύεται σε δυαδική μορφή και τοποθετείται σε συγκεκριμένη τοποθεσία στη μνήμη.

Συνοπτικά, στον παρακάτω πίνακα αναφέρονται οι κυριότερες διαφορές :

ΝΕΥΡΩΝΙΚΑ ΔΙΚΤΥΑ	***ΥΠΟΛΟΓΙΣΤΗΣ***
Τρόπος λειτουργίας: Σύγχρονος	Τρόπος λειτουργίας: Ασύγχρονος
Παράλληλη επεξεργασία (παράλληλων κατανεμημένων διεργασιών)	Σειριακή επεξεργασία
Εκπαιδεύονται με παραδείγματα αλλάζοντας τα βάρη των συνδέσεών τους	Προγραμματίζονται με εντολές λογικού χαρακτήρα
Μνήμη, δίκτυα και μονάδες συνυπάρχουν	Μνήμη και επεξεργαστές χωρίζονται
Ανοχή σε σφάλματα και βλάβες	Καμία ανοχή σε σφάλματα και βλάβες
Η πληροφορία αποθηκεύεται στα βάρη των συνδέσεων	Η πληροφορία αποθηκεύεται σε συγκεκριμένες διευθύνσεις μνήμης
Αυτό-οργάνωση κατά τη διαδικασία εκπαίδευσης	Η οργάνωση του συστήματος εξαρτάται εξ ολοκλήρου από το λογισμικό που «φορά»

1.5. ΑΡΧΙΤΕΚΤΟΝΙΚΕΣ ΤΩΝ ΝΕΥΡΩΝΙΚΩΝ ΔΙΚΤΥΩΝ

Οι νευρώνες ενός νευρωνικού δικτύου δομούνται με βάση τον αλγόριθμο εκμάθησης για την εκπαίδευση του δικτύου. Σαν *εμπρός τροφοδότησης* αναφέρονται τα δίκτυα στα οποία τα σήματα κατευθύνονται από την είσοδο στην έξοδο. Στην περίπτωση που η έξοδος κάποιου νευρώνα αποτελεί σήμα εισόδου για άλλο νευρώνα τότε έχουμε το φαινόμενο της *ανάδρασης*.

Έχουμε 4 κλάσεις αρχιτεκτονικών δομών:

- Ενός επιπέδου Εμπρός τροφοδότησης δίκτυα. Σε αυτή την περίπτωση οι νευρώνες είναι οργανωμένοι σε μορφή επιπέδων.

- Πολλαπλών επιπέδων εμπρός τροφοδότησης δίκτυα. Στην προκειμένη περίπτωση έχουμε περισσότερα του ενός κρυφά επίπεδα των οποίων οι κόμβοι χαρακτηρίζονται ως *κρυφοί νευρώνες.* Σε κάθε επίπεδο οι νευρώνες έχουν εισόδους τις εξόδους του προηγούμενου επιπέδου. Ένα δίκτυο τέτοιας δομής συμβολίζεται και ως 10-4-2.

- Αναδρομικά δίκτυα. Υπάρχει τουλάχιστον ένας κόμβος ανάδρασης (κόμβος ο οποίος έχει είσοδο την έξοδο κάποιου άλλου). Εδώ βασικό

είναι να αναφερθεί το δίκτυο Hopfield, το οποίο είναι μια μη γραμμική μνήμη ή μνήμη διευθυνσιοδοτούμενη από τα περιεχόμενα. Η κύρια λειτουργία μιας τέτοιας μνήμης είναι η ανάκτηση ενός προτύπου που είχε αποθηκευτεί σε αυτή.

- Τέλος, δικτυωτές δομές. Πρόκειται για ένα πλέγμα αποτελούμενο από έναν πίνακα μίας, δύο ή μεγαλύτερης διάστασης με νευρώνες και από ένα αντίστοιχο σύνολο πηγαίων κόμβων που παρέχουν τα σήματα εισόδου στον πίνακα αυτόν.

1.6. ΒΑΣΙΚΑ ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΤΕΧΝΗΤΩΝ ΝΕΥΡΩΝΙΚΩΝ ΔΙΚΤΥΩΝ

Σαφώς ένας τέτοιος κλάδος ο οποίος είναι άμεσα συνδεδεμένος με τη ραγδαία ανάπτυξη της τεχνολογίας τα τελευταία χρόνια, έχει εφαρμογές σε πάρα πολλά επίπεδα τα οποία θα αναφερθούν παρακάτω. Τα βασικότερα πλεονεκτήματα τους που προσδίδουν το κύρος και την αναγνωρισημότητα στα νευρωνικά δίκτυα είναι τα εξής:

- Προσαρμοστικότητα. Η δυνατότητα των νευρωνικών δικτύων να προσαρμόζουν τα βάρη τους στις αλλαγές που μπορεί να υποστεί το περιβάλλον τους.
- Αποδεικτική Απόκριση. Η ικανότητα ένα δίκτυο τέτοιου είδους να παρέχει πληροφορίες όχι μόνο για το συγκεκριμένο υπόδειγμα που επιλέγεται αλλά και για την εμπιστοσύνη στην απόφαση που θα ληφθεί.
- Συναφής Πληροφορία. Η γνώση αναπαριστάνεται από την ενεργή κατάσταση του νευρωνικού δικτύου.
- Αντοχή σε σφάλματα. Αυτό συμβαίνει γιατί ένα δίκτυο το οποίο είναι υλοποιημένο σε hardware σαφώς και παρουσιάζει ανεκτικότητα σε σφάλματα αν ληφθούν υπόψη οι βασικές πολιτικές ασφάλειας ενός συστήματος. Η προστασία του δεν διαφοροποιείται, όσον αφορά το υλικό, λόγω των ιδιαιτεροτήτων που διακατέχουν ένα νευρωνικό δίκτυο.
- Υλοποιησιμότητα σε VLSI. Χάρη στην υλοποίηση του δικτύου σε τεχνολογία VLSI (Very Large Scale Integration) το νευρωνικό δίκτυο αποκτά τη δυνατότητα να χρησιμοποιεί εφαρμογές πραγματικού χρόνου.

- Ομοιομορφία ανάλυσης και σχεδιασμού. Σε όλα τα πεδία που περιέχεται εφαρμογή των νευρωνικών δικτύων χρησιμοποιείται ο ίδιος συμβολισμός για το κάθε τι.
- Αναλογία με νευροβιολογία. Ο σχεδιασμός νευρωνικών δικτύων γίνεται σε αναλογία με τον εγκέφαλο. Οι μηχανικοί βλέπουν στη νευροβιολογία για νέες ιδέες για την επίλυση πολύπλοκων προβλημάτων.

1.7. ΕΦΑΡΜΟΓΕΣ ΤΩΝ ΝΕΥΡΩΝΙΚΩΝ ΔΙΚΤΥΩΝ

Τα νευρωνικά δίκτυα λόγω της φύσης αλλά και των ιδιαίτερων ιδιοτήτων τους έχουν καταλάβει πρωταρχική θέση σε πολλούς τομείς. Παρακάτω θα αναφερθούν οι πιο σημαντικοί από αυτούς καθώς και τα πιο σημαντικά επιτεύγματα με τη χρήση των τεχνολογιών αυτών σε αυτούς.

- √ Αεροπορία: αυτόματοι πιλότοι υψηλής απόδοσης, προσομοιωτές πτήσης, συστήματα αυτόματου ελέγχου αεροπλάνων, συστήματα ανίχνευσης βλαβών.
- √ Άμυνα: τα πιο αξιοσημείωτα πεδία που αναπτύχθηκαν με τη χρήση νευρωνικών δικτύων είναι η ψηφιακή επεξεργασία σημάτων, η συμπίεση δεδομένων, τα ραντάρ, τα σόναρ, η πλοήγηση όπλων, η αναγνώριση σημάτων εικόνας, η ανίχνευση στόχων, νέα είδη αισθητήρων.
- √ Αυτοκίνηση: αυτοκινούμενα συστήματα αυτόματης πλοήγησης
- √ Βιομηχανία: δυναμικό μοντελάρισμα συστημάτων χημικών διεργασιών, διάγνωση βλαβών μηχανημάτων και διεργασιών, ανάλυση σχεδιασμού χημικών προϊόντων, βιομηχανικός έλεγχος διεργασιών, συστήματα ποιοτικού ελέγχου.
- √ Γεωλογία: γεωλογικές έρευνες με σκοπό τον εντοπισμό πετρελαίου και φυσικού αερίου
- √ Επεξεργασία φωνής: αναγνώριση φωνής, συμπίεση φωνής, σύνθεση φωνής από κείμενο.
- √ Ηλεκτρονική: πρόβλεψη ακολουθίας κωδίκων, μορφοποίηση και διάγνωση βλαβών ολοκληρωμένων κυκλωμάτων, έλεγχος διεργασιών, μηχανική όραση.
- √ Ιατρική: ανάλυση καρκινικών κυττάρων, ηλεκτροεγκεφαλογραφήματος και ηλεκτροκαρδιογραφήματος.
- √ Οικονομία: οικονομική ανάλυση, πρόβλεψη τιμών συναλλάγματος.
- √ Ρομποτική: έλεγχος τροχιάς και σύστημα όρασης ρομπότ

- √ Τηλεπικοινωνίες: συμπίεση εικόνας και δεδομένων, αυτοματοποιημένες υπηρεσίες πληροφοριών, μετάφραση πραγματικού χρόνου, συστήματα επεξεργασίας πληρωμών.
- √ Τραπεζικές εφαρμογές: αναγνώστες επιταγών και άλλων παραστατικών, συστήματα αξιολόγησης αιτήσεων δανειοδότησης.
- √ Χρηματιστηριακές εφαρμογές: Ανάλυση αγοράς, πρόβλεψη τιμών μετοχών.

ΚΕΦΑΛΑΙΟ 2^{Ο} – ΑΣΦΑΛΕΙΑ

ΤΕΧΝΟΛΟΓΙΕΣ ΚΑΙ ΣΗΜΑΝΤΙΚΟΤΗΤΑ

Στο κεφάλαιο αυτό θα μιλήσουμε για την ασφάλεια δικτύων και πληροφοριακών συστημάτων. Ποιά η αξία του να παρέχεται ασφάλεια, η ανάγκη καθώς και τεχνολογίες με τις οποίες αυτή παρέχεται. Στη συνέχεια θα γίνει κάποια αναφορά στο νομικό πλαίσιο και στις υπηρεσίες που προστατεύουν τον χρήστη κάποιου πληροφοριακού συστήματος οποιασδήποτε μορφής.

2.1. ΤΙ ΕΙΝΑΙ ΑΣΦΑΛΕΙΑ

Η ασφάλεια πληροφοριακών συστημάτων εντάσσεται στην επιστήμη της πληροφορικής και είναι ο κλάδος που ασχολείται με την προστασία των υπολογιστών, των δικτύων που τους συνδέουν και των δεδομένων που μεταφέρονται ή διατηρούνται στα συστήματα αυτά. Στόχος είναι η αποφυγή μη εξουσιοδοτημένης πρόσβασης ή (και) χρήσης της πληροφορίας που συντελούν τα δεδομένα αυτά. Η ασφάλεια στηρίζεται σε βασικές ιδέες (αρχές). Η παραβίασή της έχει επιχειρηθεί πάμπολλες φορές και με ποικίλους τρόπους και αποτελεί αστείρευτο θέμα μελέτης.

2.2. ΓΙΑ ΤΗΝ ΙΣΤΟΡΙΑ…

Η ασφάλεια ενός συστήματος μελετήθηκε πρώτη φορά στις αρχές της δεκαετίας του ’70 από την ομάδα Εργασίας του Συμβουλίου Αμυντικής Επιστήμης του υπουργείου Άμυνας των ΗΠΑ, όπως μαρτυρά σχετική δημοσίευση εκείνης της περιόδου. Η μελέτη αυτή εξέταζε την χρήση υπολογιστών εξ αποστάσεως μέσω τερματικών εφόσον μέχρι εκείνη την περίοδο η πρόσβαση σε σύστημα έθεται ως βασική προϋπόθεση την φυσική παρουσία του χρήστη ή διαχειριστή του *κεντρικού υπολογιστή*. Η ασφάλεια, με τα δεδομένα έως τότε, διασφαλιζόταν με την φυσική απομόνωση, προστασία του κεντρικού υπολογιστή αλλά και τον έλεγχο πρόσβασης σε αυτόν. Η μελέτη αυτής της ομάδας απέφερε ως αποτέλεσμα πολλές καινοτόμες για την εποχή ιδέες, όπως για παράδειγμα

η αναγνώριση από τους ερευνητές της αρχής της ισορροπίας μεταξύ της ευκολίας εργασίας του χρήστη και της προστασίας των πληροφοριών, όπου είχαν μεγάλη απήχηση και αποτελούν τα θεμέλια ερευνών σε θέματα ασφάλειας ακόμα και σήμερα.

Παρόλο που ο πρώτος υπολογιστής με το λειτουργικό σύστημα Multics εγκαταστάθηκε το 1967 με κωδικό πρόσβασης για χρήστες και με άλλα μέτρα ασφάλειας στο σχεδιασμό του, και δύο από τους δημιουργούς του, ο *Ken Thompson* και ο *Dennis Ritchie*, έπαιξαν κρίσιμο ρόλο στην ανάπτυξη του Unix, η πρώτη έκδοση του Unix δεν διέθετε κωδικούς. Η λειτουργία αυτή προστέθηκε αργότερα, το 1973. Σήμερα η χρήση αδύναμων κωδικών πρόσβασης παραμένει μία από τις κυριότερες δυσκολίες που αντιμετωπίζει ο επαγγελματίας στον τομέα. Χρησιμοποιούνται και άλλες μέθοδοι αυθεντικοποίησης, για παράδειγμα οι έξυπνες κάρτες, αλλά μόνο σε συγκεκριμένους τομείς.

2.3.ΒΑΣΙΚΕΣ ΑΡΧΕΣ ΑΣΦΑΛΕΙΑΣ

Οι τρεις βασικές αρχές στις οποίες στηρίζεται η ασφάλεια είναι οι εξής:

1) ***Ακεραιότητα.***

   Η έννοια της ακεραιότητας αφορά τη διατήρηση της πληροφορίας σε δεδομένη κατάσταση η οποία δεν πρέπει να τροποποιείται, αφαιρείται, προστίθεται από άτομα που δεν είναι εξουσιοδοτημένα. Επιπλέον αφορά στην αποτροπή χρήσης ή και πρόσβασης των υπολογιστών και δικτύων ενός συστήματος από μη εξουσιοδοτημένα άτομα.

2) ***Διαθεσιμότητα.***

   Είναι η εξασφάλιση ότι οι υπολογιστές, τα δίκτυα και τα δεδομένα του συστήματος θα είναι διαθέσιμα όταν απαιτείται η χρήση τους (πάντα από εξουσιοδοτημένους χρήστες όπως προαναφέρθηκε) .

3) ***Εμπιστευτικότητα.***

   Επιβεβαιώνει ότι ευαίσθητες πληροφορίες και δεδομένα δεν αποκαλύπτονται σε άτομα που δεν φέρουν άδεια χρήσης του συστήματος.

Σύμφωνα επομένως με αυτές τις 3 βασικές αρχές η ‘‘ασφάλεια πληροφορίας’’ ορίζεται ως αριθμός διαδικασιών, τεχνολογικές και διοικητικές, που εφαρμόζονται σε υπολογιστικά συστήματα έτσι ώστε να διασφαλιστεί η

ακεραιότητα, διαθεσιμότητα και εμπιστευτικότητα των πληροφοριών που διαχειρίζεται το σύστημα.

2.4. ΒΑΣΙΚΗ ΟΡΟΛΟΓΙΑ

Όταν μιλάμε για ασφάλεια ενός συστήματος χρησιμοποιούμε συγκεκριμένη ορολογία βασική για την κατανόηση της ανάλυσης που λαμβάνει χώρα ώστε να δηλωθεί και αν προστατευτεί ο πόρος που μας ενδιαφέρει(οτιδήποτε και να ναι αυτό). Η βασική ορολογία θα παραταχθεί παρακάτω.

Ξεκινώντας, το ***αγαθό(asset)*** είναι ο πόρος που χρήζει ασφάλειας και το φυσικό πρόσωπο, ή νομικό, που κατέχει ή χρησιμοποιεί νομίμως το αγαθό ονομάζεται ***ιδιοκτήτης ή χρήστης(owner/ user)***. Το συγκεκριμένο χαρακτηριστικό ενός αγαθού το οποίο πρέπει να προστατευθεί ορίζεται ως ***ιδιότητα(attribute).***

Όταν ορίζουμε ένα αγαθό ορίζουμε και περιορισμούς της αξίας ενός αγαθού. Αυτοί οι περιορισμοί αποτελούν τη ***ζημιά(harm)*** της οποίας το ενδεχόμενο να συμβεί ονομάζεται ***κίνδυνος(danger)*.**

Στόχος της ασφάλειας(infosec goal) είναι ο αντικειμενικός σκοπός του ιδιοκτήτη ή χρήστη ενός αγαθού που καθορίζει την επιθυμητή ισορροπία μεταξύ κόστους και ζημιάς που ενδέχεται να υποστεί το αγαθό σε περίπτωση κινδύνου.

Μέσο προστασίας(safeguard) ονομάζεται το σύνολο των ενεργειών τις οποίες μπορεί να κάνει ο ιδιοκτήτης ή χρήστης ενός αγαθού, ούτως ώστε να περιοριστεί ο κίνδυνος να υποστεί αυτό ζημιά.

Κόστος(cost),το οποίο αναφέραμε και παραπάνω αυθαίρετα, είναι η οικονομική ή άλλου είδους επιβάρυνση που προκύπτει από τη χρήση ενός μέσου προστασίας.

Και τέλος, ως ***εξασφάλιση(assurance)*** ορίζεται η βεβαιότητα ότι οι στόχοι της ασφάλειας επιτεύχθηκαν, ως αποτέλεσμα των μέσων προστασίας που υιοθετήθηκαν.

Να σημειώσουμε ότι όταν αναφερόμαστε σε ένα δίκτυο υπολογιστών η ασφάλεια έχει μεγάλη βαρύτητα καθώς δεν δύναται όλοι οι χρήστες να γνωρίζουν την «καλή πρόθεση» των υπολοίπων. Ας ξεκινήσουμε με βασικές αρχές που λίγο πολύ διαφοροποιούνται με τα προαναφερθέντα.

Δίκτυο υπολογιστών είναι μια συλλογή αυτόνομων υπολογιστών συνδεδεμένων μεταξύ τους με τρόπο τέτοιο ώστε να μπορεί να επιτευχθεί η ανταλλαγή δεδομένων.

Η ***ανθρώπινη*** οντότητα για τις δραστηριότητες και η ***διευθυνσιοδοτούμενη*** οντότητα σε ένα δίκτυο ή ένα κατανεμημένο σύστημα είναι ο ***Χρήστης (user)*** και ο ***Ξενιστής Υπολογιστής (host)*** αντίστοιχα.

Το στιγμιότυπο εκτελέσιμου προγράμματος σε συγκεκριμένο υπολογιστικό σύστημα ορίζεται ως ***Διεργασία(process)*** και χωρίζεται στις : CLIENT PROCESS που αιτείται και αποκτά υπηρεσία δικτύου και SERVER PROCESS που παρέχει την υπηρεσία δικτύου.

Η έγγραφη συμφωνία που περιλαμβάνει τεχνικές προδιαγραφές και κριτήρια ονομάζεται ***Πρότυπο(standard).*** Στην ασφάλεια δικτύων(όταν μιλάμε για προτυποποίηση) όμως εκτός από το πρότυπο απαιτείται και ***Μοντέλο Αναφοράς(reference model)*** το οποίο χρησιμοποιείται στην ανάλυση της συνεργασίας των συνιστωσών του συστήματος.

Η οντότητα που μπορεί να προκαλέσει ζημιά ή παραβίαση σε τμήμα ή και στο σύνολο του δικτύου είναι γνωστή και ως ***Απειλή(Threat)***. Όταν ένας εισβολέας που επιθυμεί να υλοποιήσει κάποια απειλή εκμεταλλευόμενος μια αδυναμία τότε μιλάμε για ***Επίθεση(Attack).*** Βέβαια υπάρχουν μηχανισμοί και διαδικασίες που προσπαθούν αν όχι να εξαφανίσουν, να περιορίσουν τις επιπτώσεις της απειλής και αποτελούν τα ***Αντίμετρα(Countermeasures).***

2.5. ΣΥΧΝΕΣ ΕΠΙΘΕΣΕΙΣ

Η ασφάλεια ενός συστήματος είναι βασικός παράγοντας για την υγιή λειτουργία αυτού εφόσον υπάρχουν πολλές περιπτώσεις επιθέσεων που μπορούν να λάβουν χώρα. Οι επιθέσεις έχουν διαφορετικό στόχο κάθε φορά αλλά σαφώς και προκαλούν σημαντικά προβλήματα σε κάθε περίπτωση. Οι «εισβολείς», αυτοί που είναι δυνατόν να επιχειρούν επιθέσεις στο σύστημα μπορεί να είναι είτε υπάλληλοι του οργανισμού για τον οποίο είναι «στημένο» το σύστημα, είτε ανταγωνιστές του οργανισμού είτε, το πιο αναμενόμενο, hackers. Μερικές από τις πιο συχνές επιθέσεις που συμβαίνουν είναι:

- Εισαγωγή, μετατροπή ή καταστροφή δεδομένων ή ακόμα και λογισμικού από άτομα που δεν έχουν άδεια για κάτι τέτοιο
- Αλλοίωση ή μείωση της αξιοπιστίας των δεδομένων (λόγω τυχούσας παρέμβασης χωρίς εξουσιοδότηση)
- Παρεμπόδιση ομαλής λειτουργίας του συστήματος εν γένει με ποικίλους τρόπους
- Εισβολή και αφαίρεση στοιχείων από το σύστημα χωρίς εξουσιοδότηση
- Παραβίαση των πνευματικών δικαιωμάτων

2.5.1. ΕΠΙΘΕΣΕΙΣ

2.5.1.1. ΤΥΠΟΙ ΕΠΙΘΕΣΕΩΝ

Οι βασικότεροι τύποι επιθέσεων σε ένα δίκτυο/σύστημα είναι οι εξής:

a. ***Μη εξουσιοδοτημένη χρήση (masquerade)***. Στην περίπτωση αυτή γίνεται προσπάθεια απόκτησης πρόσβασης σε διαθέσιμους πόρους από χρήστη που δεν φέρει άδεια.
b. ***Μη ενεργός ή παθητική παρακολούθηση (passive tapping)***. Εδώ γίνεται παρακολούθηση δεδομένων τα οποία διακινούνται μεταξύ χρηστών του δικτύου.
c. ***Ενεργός παρακολούθηση(active tapping).*** Γίνεται τροποποίηση των δεδομένων
d. ***Αποποίηση(repudiation)***. Στην περίπτωση αυτή υπάρχει κάποια οντότητα, ένα κομμάτι του δικτύου (όπως ένας υπολογιστής), η οποία αποποιείται τη συμμετοχή της σε κάποια επικοινωνία.
e. ***Άρνηση παροχής υπηρεσιών(denial of service)***. Παρεμποδίζεται η ομαλή λειτουργία του δικτύου.
f. ***Επανεκπομπή μηνυμάτων (replay)***. Καταγράφονται έγκυρα μηνύματα έτσι ώστε να μπορούν να σταλούν ξανά.
g. ***Ανάλυση επικοινωνίας(traffic analysis).*** Στοχεύοντας στην έμμεση εξαγωγή συμπερασμάτων γίνεται υποκλοπή πληροφορίας σχετικά με τη διακίνηση δεδομένων μεταξύ οντοτήτων.
h. ***Κακόβουλο λογισμικό.*** Τα γνωστά σε όλους μας (και μη εξαιρετέα από κανένα βιβλίο που αναφέρεται στην ασφάλεια) Trojan horses, Worms, Viruses.

2.5.1.2. ΚΙΝΔΥΝΟΙ ΒΑΣΕΙ ΤΕΧΝΙΚΩΝ ΕΠΙΘΕΣΕΩΝ

Για να μπορεί να γίνει μια επίθεση πρέπει ο επιτιθέμενος πρέπει να χρησιμοποιήσει κάποιες τεχνικές ώστε να μπορεί να πράξει την επίθεση. Οι βασικοί κίνδυνοι που δύναται να συμβούν βάσει συγκεκριμένων τεχνικών είναι:

i. **Επίθεση από Ωτακουστές(Eavesdropping).** Οι πληροφορίες που μεταδίδονται σε ένα δίκτυο ‘‘παρακολουθούνται’’ από τον επιτιθέμενο ωτακουστή ο οποίος έχει απώτερο σκοπό να ανιχνεύσει τον παραλήπτη ή τον αποστολέα.

ii. **Επίθεση Αντίστροφης Πορείας(Trace Back Attack).** Ξεκινώντας από γνωστό παραλήπτη ιχνηλατείται το μονοπάτι προς τον αποστολέα σύμφωνα με το μονοπάτι προώθησης ή και αντίστροφα.

iii. **Επίθεση Κωδικοποίησης Μηνυμάτων (Message Coding Attack).** Δίνεται η δυνατότητα στον επιτιθέμενο να ιχνηλατεί μηνύματα με την προϋπόθεση ότι η κωδικοποίηση τους δεν έχει υποστεί καμία τροποποίηση κατά τη μετάδοση.

iv. **Επίθεση Χρονοσήμανσης (Timing Attack).** Πακέτα μεταδίδονται και εντοπίζεται ο αποστολέας λόγω των συσχετισμένων χρόνων.

v. **Επίθεση από εχθρικούς συνεργάτες (Malicious Collaborators).** Χρήστες του δικτύου που στοχεύουν τον έλεγχο της μεταφοράς των δεδομένων που γίνεται στο δίκτυο, την διαστρέβλωση των δεδομένων αυτών και ου το καθεξής.

2.6. ΜΗΧΑΝΙΣΜΟΙ ΑΣΦΑΛΕΙΑΣ

Η ακατάπαυστη δίψα των επιστημόνων να βρίσκουν τρόπους που διασφαλίζουν την ασφάλεια σε ένα δίκτυο έδωσε στο κοινό μηχανισμούς που πλέον θεωρούνται απαραίτητοι. Ποτέ όμως δεν αποφεύγεται πλήρως ο κίνδυνος για επίθεση. Παρόλα αυτά, ελαχιστοποιούν τον κίνδυνο και σαφώς προσδίδουν μεγαλύτερη ασφάλεια στην χρήστη. Οι καθορισμένοι μηχανισμοί ασφάλειας είναι:

i. **Κρυπτογραφία**. Μεγάλο αντικείμενο μελέτης. Προσφέρει εμπιστευτικότητα (εγγύηση πως τα δεδομένα δεν αποκαλύπτονται σε οντότητες που δεν είναι εξουσιοδοτημένες)
ii. **Ψηφιακές Υπογραφές**. Όμοιες με την ιδιόχειρη υπογραφή αλλά δοσμένη «ψηφιακά»
iii. **Μηχανισμοί Ελέγχου Πρόσβασης**. Παρέχουν έλεγχο προσπέλασης σε πόρους συστημάτων-δικτύων χρησιμοποιώντας ***αυθεντικοποίηση*** (εξασφάλιση της γνησιότητας των μηνυμάτων καθώς αποδεικνύει την ταυτότητα της οντότητας)
iv. **Μηχανισμοί Ακεραιότητας Δεδομένων**. Συμβάλλουν στο να διαφυλάσσεται η ακεραιότητα των δεδομένων που μεταδίδονται στο δίκτυο
v. **Μηχανισμοί Ανταλλαγής Αυθεντικοποίησης**. Εξυπηρετούν στην αμοιβαία επιβεβαίωση της ταυτότητας των επικοινωνούντων οντοτήτων.
vi. **Μηχανισμοί Επιπρόσθετης Κίνησης**. Προστατεύουν από την Ανάλυση Επικοινωνίας, που αναφέραμε παραπάνω. Χωρίζονται στους:
    a) **Ισχυρούς**, χρησιμοποιείται στο μέγιστο βαθμό η κρυπτογραφία
    b) **Ασθενείς**, δεν γίνεται χρήση κρυπτογραφίας.

2.7. ΚΛΕΙΝΟΝΤΑΣ…

Κλείνοντας το κεφάλαιο πρέπει να σημειωθεί πως καθημερινά καινούριοι τρόποι επίθεσης αλλά και αντιμετώπισης επιθέσεων έρχονται στην επιφάνεια. Βέβαια δεν ζούμε σε ιδανικό κόσμο. Η παραβίαση και παρακολούθηση ενός συστήματος μπορεί να αποφέρει σε συγκεκριμένες περιπτώσεις τεράστιες επιπτώσεις, για παράδειγμα στο Σύστημα του Υπουργείου Εθνικής Αμύνης. Η μαγεία αυτού του κλάδου της ασφάλειας άλλωστε κρύβει τις ρίζες του στη συνεχή του εξέλιξη.

ΚΕΦΑΛΑΙΟ 3^{Ο}- ΧΡΗΣΗ ΝΕΥΡΩΝΙΚΩΝ ΔΙΚΤΥΩΝ ΓΙΑ ΑΝΙΧΝΕΥΣΗ ΚΑΤΑΧΡΗΣΗΣ

3.1. ΕΙΣΑΓΩΓΗ

Η ανίχνευση κατάχρησης σε ένα δίκτυο (ή σύστημα) είναι η διαδικασία που γίνεται με στόχο τον εντοπισμό τυχόν επιθέσεων στο δίκτυο (ή σύστημα). Η λογική της είναι να συγκρίνει την τρέχουσα δραστηριότητα στην οποία υποβάλλεται το δίκτυο εις βάρος των αναμενόμενων ενεργειών του εισβολέα. Για την ακρίβεια όταν μιλάμε για κατάχρηση εννοούμε το επόμενο στάδιο της επίθεσης (η οποία θα αναλυθεί στο επόμενο κεφάλαιο) κατά το οποίο η επίθεση μπορεί να γίνει αντιληπτή μέσω αλλαγών που ίσως να λαμβάνουν χώρα. Για να γίνει σαφές, μιλώντας για επίθεση μπορεί να εννοούμε κατάχρηση αλλά και παρακολούθηση του συστήματος(ή δικτύου) (βλ. Eavesdropping).

Στο κεφάλαιο αυτό θα δούμε την εφαρμογή και τα πλεονεκτήματα που έχει η χρήση νευρωνικών δικτύων έναντι των προαναφερθέντων μεθόδων στην ανίχνευση κατάχρησης ενός δικτύου καθώς και τα αποτελέσματα δοκιμών των νευρωνικών δικτύων σε μια έρευνα που στόχο είχε την απόδειξη της ευχρηστίας και διευκόλυνσης που μπορεί να προσφερθεί σε αυτόν τον τομέα.

Βάση της αρχιτεκτονικής και των ιδιαίτερων χαρακτηριστικό τους τα τεχνητά νευρωνικά δίκτυα προσφέρουν λύσεις σε προβλήματα που οι άλλες μέθοδοι είτε προκαλούν είτε δεν μπορούν να επιλύσουν. Έχουν προταθεί ως εναλλακτική λύση για την στατιστική ανάλυση των ανωμαλιών σε συστήματα ανίχνευσης. Η ***στατιστική ανάλυση*** απαρτίζεται από την στατιστική σύγκριση πρόσφατων γεγονότων σε προκαθορισμένο σύνολο κριτηρίων αναφοράς. Η πιο συχνή εφαρμογή της τεχνικής είναι στον εντοπισμό των αποκλίσεων από τυπική συμπεριφορά που έχει ένα δίκτυο. Πιο συγκεκριμένα τα νευρωνικά δίκτυα προτάθηκαν για να προσδιορίζονται τα τυπικά χαρακτηριστικά του συστήματος και οι σημαντικές αποκλίσεις από την πάγια συμπεριφορά του χρήστη.

Τα νευρωνικά δίκτυα έχουν επίσης μπει στη μάχη ανίχνευσης κακόβουλου λογισμικού στους υπολογιστές. Έχοντας το χαρακτηριστικό της αυτό-οργάνωσης χρησιμοποιούν ένα ενιαίο στρώμα νευρώνων γεωμετρικά οργανωμένο. Το προτεινόμενο δίκτυο, με αυτή την ειδική αρχιτεκτονική, σχεδιάστηκε για να γίνουν γνωστά τα χαρακτηριστικά της κανονικής δραστηριότητας του συστήματος και να προσδιοριστούν στατιστικά οι αποκλίσεις από τον κανόνα που είναι πιθανό να αποτελεί ένδειξη ενός κακόβουλου λογισμικού.

3.2.ΕΦΑΡΜΟΓΗ ΤΩΝ ΝΕΥΡΩΝΙΚΩΝ ΔΙΚΤΥΩΝ ΣΤΗΝ ΑΝΙΧΝΕΥΣΗ ΚΑΤΑΧΡΗΣΗΣ

Καθώς υπάρχει αυξανόμενη ανάγκη για συστήματα ικανά να αναγνωρίζουν τυχόν καταχρήσεις σε ένα δίκτυο, δεν έχει εφαρμοστεί τελευταία καμία εναλλακτική λύση βασισμένη στους κανόνες της ασφάλειας ώστε να γίνεται ανίχνευση εισβολής στο δίκτυο. Οι μέθοδοι που χρησιμοποιούνται έχουν αποδειχτεί σχετικά αποτελεσματικές εάν τα χαρακτηριστικά της επίθεσης είναι γνωστά. Ωστόσο αυτό είναι τις περισσότερες φορές αδύνατο καθώς οι εισβολές σε ένα δίκτυο συνεχώς αλλάζουν τρόπο δράσης λόγω μεμονωμένων προσεγγίσεων που λαμβάνονται από τους επιτιθέμενους αλλά και των συχνών αλλαγών σε υλικό και λογισμικό που γίνονται στα επιτιθέμενα συστήματα (ή δίκτυα). Λόγω, λοιπόν της τεράστιας ποικιλίας των επιτιθέμενων αλλά και των τρόπων επίθεσης ακόμα και μια προσπάθεια συνεχούς ενημέρωσης της βάσης ενός συστήματος, ώστε να προφυλάσσεται από του κινδύνους που έρχονται στο φως καθημερινά, δεν μπορεί να εγγυηθεί ακριβή και σίγουρο εντοπισμό κακόβουλης κίνησης, εισβολής ή κατάχρησης στο δίκτυο ή σύστημα.

Όπως είπαμε και παραπάνω η φύση των επιθέσεων , δηλαδή ο τρόπος και ο σκοπός που γίνεται η κάθε επίθεση, συνεχώς μεταβάλλεται. Αυτό σημαίνει ότι ένα δίκτυο για να θεωρείται ικανοποιητικά προστατευόμενο πρέπει να διαθέτει ένα ευέλικτο αμυντικό σύστημα που να είναι ικανό να αναλύσει την κίνηση του δικτύου, όσο μεγάλη και αν είναι, με τέτοιο τρόπο ώστε να λειτουργούν σαν «***έξυπνο σύστημα***» και όχι σε μια απλή καθορισμένη δομή. Ένα σύστημα ανίχνευσης κατάχρησης σε ένα δίκτυο με βάση τη χρήση νευρωνικών δικτύων θα μπορούσε να αντιμετωπίσει τα περισσότερα και πιο σημαντικά από τα προβλήματα που δεν μπορούν να αντιμετωπιστούν με άλλες μεθόδους.

3.2.1. ΠΛΕΟΝΕΚΤΗΜΑΤΑ

Για να υποστηρίξουμε τα προαναφερθέντα θα πρέπει να παραθέσουμε τα πλεονεκτήματα της χρήσης νευρωνικών δικτύων στην ανίχνευση κατάχρησης έναντι άλλων μεθόδων που χρησιμοποιούνται.

1. ***Η ευελιξία του δικτύου***. Ένα νευρωνικό δίκτυο έχει τη δυνατότητα να αναλύσει δεδομένα από το δίκτυο ακόμα και σε περίπτωση

αλλοιωμένων ή παραμορφωμένων δεδομένων. Ομοίως, το δίκτυο θα είναι ικανό να αναλύσει δεδομένα με μη- γραμμικό τρόπο. Αυτά είναι σημαντικά χαρακτηριστικά ειδικά όταν έχουμε να κάνουμε με ένα περιβάλλον δικτύου όπου τα δεδομένα διαμοιράζονται μεν αλλά μπορεί να έχουν γίνει και αποτυχίες αποστολής ή λήψης δεδομένων. Επιπλέον, έχοντας κατά νου και την περίπτωση συντονισμένης επίθεσης από πολλούς επιτιθέμενους εις βάρους του δικτύου, η δυνατότητα επεξεργασίας δεδομένων από ποικίλες πηγές και μη-γραμμικά είναι ιδιαίτερα σημαντική.

2. ***Η ταχύτητα***. Τα νευρωνικά δίκτυα είναι γνωστά για την έμφυτη ταχύτητά τους. Αυτό σίγουρα αποτελεί άλλο ένα πλεονέκτημα αυτής της προσέγγισης εφόσον η προστασία των υπολογιστικών πόρων απαιτεί έγκαιρη αναγνώριση των επιθέσεων που η ταχύτητα των νευρωνικών δικτύων θα μπορούσε να αντιμετωπίσει (απαντήσει στις προκλήσεις) τις επιθέσεις πριν η καταστροφή του συστήματος αποβεί ανεπανόρθωτη.
3. ***Δυνατότητα πρόβλεψης επίθεσης***. Επειδή το αποτέλεσμα που δίνει το νευρωνικό δίκτυο εκφράζεται με μορφή πιθανότητας, μπορεί να παρέχει τη δυνατότητα πρόβλεψης κατάχρησης ή γενικότερα, πρόβλεψη οποιουδήποτε τύπου επίθεσης στο δίκτυο. Η ανίχνευση κατάχρησης με χρήση νευρωνικού δικτύου μπορεί να προσδιορίσει την πιθανότητα ενός συγκεκριμένου γεγονότος, ή πολλών γεγονότων, να αποτελεί προκείμενη επίθεση στο σύστημα. Δεδομένου ότι ένα νευρωνικό δίκτυο δεν παύει ποτέ να εκπαιδεύεται αλλά αντιθέτως μαθαίνει από τις εμπειρίες του, η ικανότητά του να καταλάβει αν επίκειται κάποια επίθεση βελτιώνεται συνεχώς. Αυτό μπορεί να εξυπηρετήσει στην ανάπτυξη της άμυνας του δικτύου αν πραγματικά γίνει επίθεση σε αυτό. Τότε δεν θα επιτραπεί να βλάψει το δίκτυο, τουλάχιστον όχι σε μεγάλο βαθμό, η προκείμενη επίθεση.
4. ***Εκπαίδευση***. Ίσως το κύριο πλεονέκτημα των νευρωνικών δικτύων και αυτό που τα καθιστά πιο κατάλληλα στην ασφάλεια. Ένα νευρωνικό δίκτυο μπορεί να μάθει τα χαρακτηριστικά των επιθέσεων με στόχο την κατάχρηση, αλλά και γενικότερα, και να αναγνωρίσει σε κάθε περίπτωση αν έχει ξανασυμβεί παρόμοιο περιστατικό ή όχι. Έτσι, ένα νευρωνικό δίκτυο μπορεί να εκπαιδευτεί να αναγνωρίζει με μεγάλη ακρίβεια γνωστές περιπτώσεις που ίσως αποτελούν κίνδυνο για το σύστημα. Ακριβώς λοιπόν επειδή οι επιτιθέμενοι μιμούνται τους τρόπους επίθεσης άλλων που έχουν διεξαχθεί με επιτυχία, το δίκτυο θα αναγνωρίσει και αυτές τις επιθέσεις καθώς «ξαναβλέπει» βασικά χαρακτηριστικά που έχουν αποτελέσει επίθεση στο παρελθόν.

3.2.2.ΜΕΙΟΝΕΚΤΗΜΑΤΑ

Όπως σε κάθε περίπτωση έτσι και εδώ υπάρχει και κάποιος αριθμός μειονεκτημάτων. Τα δύο βασικά, τα οποία είναι μεγίστης σημασίας και αυτό αποδεικνύεται από το γεγονός ότι η μέθοδος δεν χρησιμοποιείται ευρέως, είναι τα εξής:

1. ***Ανάγκη εκπαίδευσης***. Καθώς η δυνατότητα των τεχνητών νευρωνικών δικτύων να αναγνωρίζουν περιπτώσεις επικείμενης επίθεσης/διείσδυσης στο δίκτυο/σύστημα εξαρτάται απόλυτα από την ακριβή εκπαίδευσή του, τα δεδομένα αλλά και η μέθοδος εκμάθησης που θα χρησιμοποιηθούν είναι κρίσιμοι παράγοντες. Η σωστή εκπαίδευση απαιτεί μεγάλο πλήθος δεδομένων ώστε να διασφαλίζεται ότι τα αποτελέσματα θα είναι ακριβή. Μπορεί για την εκπαίδευση να απαιτούνται άπειρες ατομικές επιθέσεις στη σειρά κάτι το οποίο είναι δύσκολο να συμβεί καθώς τέτοια ποσότητα αυτών των ευαίσθητων πληροφοριών είναι δύσκολο να αποκτηθεί.
2. ***Το πρόβλημα του «Μαύρου Κουτιού»***. Σε αντίθεση με τα έμπειρα συστήματα που έχουν προγραμματιστεί με πολύ σαφείς και ακριβείς κανόνες για την ανάλυση γεγονότων, τα νευρωνικά δίκτυα προσαρμόζουν την ανάλυση των δεδομένων τους σύμφωνα με το πώς εκπαιδεύεται κάθε φορά το δίκτυο. Τα βάρη των συνδέσεων και των λειτουργιών μετάδοσης σε διάφορους κόμβους του δικτύου συχνά ‘‘παγώνουν’’ όταν το δίκτυο φτάνει σε ένα επίπεδο επιτυχίας για τον προσδιορισμό γεγονότων. Παρόλο που η ανάλυση του δικτύου καταφέρνει να έχει μεγάλη πιθανότητα επιτυχίας, η βάση για αυτό το επίπεδο ακρίβειας συχνά δεν είναι γνωστή. Αυτό είναι το γνωστό πρόβλημα του «Μαύρου Κουτιού» και το βασικό μειονέκτημα των νευρωνικών δικτύων, οποιοσδήποτε και αν είναι ο σκοπός χρήσης τους. Η λύση για αυτό το πρόβλημα είναι ακόμα σε ερευνητικό στάδιο.

3.3.ΠΙΘΑΝΕΣ ΕΦΑΡΜΟΓΕΣ

Υπάρχουν δύο γενικά αποδεκτές εφαρμογές των νευρωνικών δικτύων σε συστήματα ανίχνευσης κατάχρησης. Λόγω των μειονεκτημάτων που αναφέραμε, γενικότερα κάποιος διστάζει να μπει σε μια διαδικασία που μπορεί ή να του κάνει τεράστιο καλό ή ακόμα μεγαλύτερο κακό. Ωστόσο, δύο ασφαλείς και σίγουρες εφαρμογές ευρέως γνωστές παρατίθενται στη συνέχεια.

3.3.1. Πρώτη Εφαρμογή-

Νευρωνικά Δίκτυα και Έμπειρα Συστήματα

Η πρώτη αφορά ***την ενσωμάτωση των νευρωνικών δικτύων σε υπάρχοντα ή τροποποιημένα έμπειρα συστήματα***. Σε αντίθεση με άλλες απόπειρες χρήσης νευρωνικών δικτύων για τον εντοπισμό ανωμαλιών χρησιμοποιώντας τα στην αντικατάσταση ήδη υπάρχουσας ανάλυσης, εδώ μας ενδιαφέρει να φιλτράρεται η εισερχόμενη στο σύστημα πληροφορία για ύποπτα στοιχεία που μπορεί να υποδεικνύουν προκείμενη κατάχρηση και να παραπέμπονται αυτά τα στοιχεία στο έμπειρο σύστημα. Με αυτή την προσέγγιση θα βελτιωθεί η αποτελεσματικότητα της ανίχνευσης μειώνοντας ταυτόχρονα το ποσοστό των λανθασμένων «συναγερμών» του έμπειρου συστήματος. Επειδή το νευρωνικό δίκτυο θα καθορίσει την πιθανότητα ένα συγκεκριμένο στοιχείο να γεννά επίθεση, ένα όριο που μπορεί να τεθεί (καταρρίπτοντας έτσι το δεύτερο μειονέκτημα) είναι όταν τα στοιχεία ή το στοιχείο προωθείται στο εμπειρικό σύστημα.

Εφόσον ένα έμπειρο σύστημα μόνο θα λαμβάνει τα ύποπτα στοιχεία της πληροφορίας η ευαισθησία τους μπορεί να παρουσιάσει αύξηση, κάτι το οποίο δεν θέλουμε καθώς έμπειρα συστήματα πρέπει να κρατούν χαμηλά τα επίπεδα ευαισθησίας τους ώστε να μην παρουσιάζονται συχνά λανθασμένοι συναγερμοί. Αυτή η ρύθμιση θα εξυπηρετούσε οργανισμούς που έχουν επενδύσει σε τεχνολογίες έμπειρων συστημάτων βελτιώνοντας την αποτελεσματικότητα του συστήματος αλλά διατηρώντας και τις κινήσεις που έχουν γίνει στα συστήματα ανίχνευσης εισβολής.

Το ***μειονέκτημα*** αυτής της εφαρμογής είναι ότι αφού το νευρωνικό δίκτυο βελτίωσε την ικανότητά του να προσδιορίζει νέες επιθέσεις, το έμπειρο σύστημα θα πρέπει να ενημερώνεται (update) ώστε να αναγνωρίζει και αυτό τέτοιες απειλές. Αν το έμπειρο σύστημα δεν ενημερώνεται τότε οι νέες επιθέσεις που έχουν προσδιοριστεί και καταγραφεί από τα νευρωνικά δίκτυα θα αγνοούνται από το έμπειρο σύστημα καθώς η βάση του δεν θα είναι σε θέση να αναγνωρίσει τη νέα απειλή.

3.3.2. Δεύτερη Εφαρμογή-

Νευρωνικά Δίκτυα ως Αυτόνομα Συστήματα

Η δεύτερη εφαρμογή δέχεται το ***νευρωνικό δίκτυο ως αυτόνομο σύστημα ανίχνευσης κατάχρησης***. Εδώ, το νευρωνικό δίκτυο θα παίρνει όλα τα δεδομένα της ροής πληροφορίας στο δίκτυο και αναλύει την πληροφορία σε περιπτώσεις κατάχρησης. Οι περιπτώσεις που εντοπίζονται ως ένδειξη επίθεσης προωθείται στον διαχειριστή ασφάλειας(security administrator) ή θα χρησιμοποιούνται από ένα αυτοματοποιημένο σύστημα απάντησης εισβολής. Η προσέγγιση αυτή διαθέτει το πλεονέκτημα της ταχύτητας έναντι τις προηγούμενης εφαρμογής, εφόσον υπάρχει μόνο ένα ενιαίο επίπεδο, το επίπεδο της ανάλυσης. Επιπροσθέτως, αυτή η ρύθμιση μπορεί να βελτιώσει την αποτελεσματικότητα του συστήματος συγκριτικά με το χρόνο, αφού το δίκτυο ‘‘μαθαίνει’’ τα χαρακτηριστικά των επιθέσεων.

Σε αντίθεση με την πρώτη εφαρμογή, σε αυτή την περίπτωση και διατηρώντας αυτή τη λογική η εφαρμογή δεν θα περιορίζεται από την ικανότητα του έμπειρου συστήματος να αναλύει και ως εκ τούτου θα μπορεί να επεκταθεί πέρα από τα όρια ενός έμπειρου συστήματος.

3.3.3. Πιθανοί Τρόποι Εφαρμογής

Όπως ειπώθηκε και παραπάνω υπάρχουν δύο τρόποι που χρησιμοποιούνται κυρίως και αφορούν το «πάντρεμα» των νευρωνικών δικτύων με την ανίχνευση κατάχρησης σε ένα δίκτυο ή σύστημα.

1. Ο πρώτος εξυπηρετείται με την ενσωμάτωσή των νευρωνικών δικτύων σε ήδη υπάρχοντα ή διαμορφωμένα (επεξεργασμένα με κάποιον τρόπο και για κάποιο λόγο) έμπειρα συστήματα. Αντίθετα με τις προηγούμενες προσπάθειες χρήσης νευρωνικών δικτύων στην ανίχνευση χρησιμοποιώντας τα για την αντικατάσταση των συνιστωσών της υπάρχουσας στατιστικής ανάλυσης, η πρόταση αυτή ισχυρίζεται την *χρήση των νευρωνικών δικτύων στο φιλτράρισμα των δεδομένων που εισέρχονται στο σύστημα ψάχνοντας για ύποπτα γεγονότα που να υποδεικνύουν την κατάχρηση και προώθηση τέτοιων στοιχείων στο έμπειρο σύστημα*. Αυτή η εφαρμογή αποσκοπεί στη βελτίωση της αποτελεσματικότητας του συστήματος ανίχνευσης μειώνοντας τους συχνούς λανθασμένους συναγερμούς των έμπειρων συστημάτων. Επειδή μέσω των νευρωνικών δικτύων καθορίζεται η πιθανότητα συγκεκριμένης επίθεσης (η οποία καθορίζεται από τα ύποπτα γεγονότα που ανιχνεύονται), μία λειτουργία ενεργοποιείται όπου τα γεγονότα αυτά προωθούνται στο έμπειρο σύστημα για περαιτέρω ανάλυση. Από τη στιγμή που μόνο το έμπειρο σύστημα λαμβάνει τα γεγονότα ή τα δεδομένα τα οποία θεωρούνται ύποπτα ή επικίνδυνα,

η ευαισθησία του έμπειρου συστήματος αυξάνεται (θεωρητικά, ένα έμπειρο σύστημα πρέπει να έχει χαμηλά επίπεδα ευαισθησίας ώστε να αποφεύγονται οι πολύ συχνοί λανθασμένοι συναγερμοί).
Αυτή η εφαρμογή είναι ωφέλιμη σε οργανισμούς που επενδύουν σε τεχνολογίες rule-base έμπειρων συστημάτων βελτιώνοντας την αποτελεσματικότητα του συστήματος διατηρώντας όμως και την επένδυση που έχει γίνει στα ήδη υπάρχοντα συστήματα ανίχνευσης εισβολής και επίθεσης.
Το ***μειονέκτημα*** της προσέγγισης αυτής είναι ότι χρησιμοποιώντας τα νευρωνικά δίκτυα για την βελτιστοποίηση της δυνατότητας ανίχνευσης νέας επίθεσης σε έμπειρο σύστημα πρέπει να ενημερωθεί ώστε να μπορεί να αναγνωρίσει τα γεγονότα ως απειλές. Αν το έμπειρο σύστημα δεν ενημερωθεί τότε ολοένα και περισσότερες επιθέσεις που τα νευρωνικά δίκτυα θα έχουν ανιχνεύσει, θα αγνοούνται από το έμπειρο σύστημα καθώς το rule-base του δεν θα είναι σε θέση να τις αναγνωρίσει.

2. Η δεύτερη πρόταση προτείνει την αυτοδυναμία του νευρωνικού δικτύου ως σύστημα ανίχνευσης. Εδώ, το νευρωνικό δίκτυο λαμβάνει τα δεδομένα από τη ροή του δικτύου και τα αναλύει αναζητώντας τυχόν περιπτώσεις κατάχρησης. Όποια τέτοια περίπτωση που έχει ανιχνευτεί ως ενδεχόμενος κίνδυνος -επίθεση προωθείται στον security administrator ασφάλειας ή εξουδετερώνεται από σύστημα αυτόματης αντιμετώπισης επίθεσης.
Βασικό πλεονέκτημα αυτής της μεθόδου είναι η ταχύτητα αφού στην προκειμένη περίπτωση έχουμε μόνο ένα στρώμα ανάλυσης. Επιπλέον, εδώ βελτιώνεται και η αποτελεσματικότητα έναντι του χρόνου καθώς το δίκτυο μαθαίνει (εκπαιδεύεται) τα χαρακτηριστικά των επιθέσεων.
Αντίθετα με την πρώτη εφαρμογή, δεν υπάρχει η δυνατότητα οριοθέτησης που επιβάλλει το έμπειρο σύστημα, με αποτέλεσμα να μπορεί να επεκταθεί το «σχέδιο δράσης» του συστήματος πέρα των ορίων του rule-base του έμπειρου συστήματος.
Το ***μειονέκτημα*** αυτής της προσέγγισης έγκειται στο γεγονός ότι για να αναγνωριστεί μια απειλή ή επίθεση πρέπει να έχει γίνει εκπαίδευση του νευρωνικού συστήματος που να αφορά τη συγκεκριμένη επίθεση.

3.4. ΑΝΑΛΥΣΗ ΠΕΙΡΑΜΑΤΙΚΗΣ ΠΡΟΣΕΓΓΙΣΗΣ

Πολλές έρευνες έχουν λάβει χώρα ώστε να ξεκαθαρίσει και να προσδιοριστεί η δυνατότητα εφαρμογής των νευρωνικών δικτύων στην ανίχνευση κατάχρησης δικτύου ή πληροφοριακού συστήματος εν γένει. Σε μια έρευνα για να μπορέσουν οι μελετητές να βγάλουν κάποιο αποτέλεσμα, αποφάσισαν να χρησιμοποιήσουν *προσομοιωτή κίνησης του δικτύου*. Η έρευνα δηλαδή είχε στόχο να δείξει αν περιπτώσεις επίθεσης και δε κατάχρησης μπορούν να εντοπισθούν και να διαφοροποιηθούν από τα «άκακα» δεδομένα που μεταφέρονται εντός του δικτύου. Βέβαια, το αρνητικό στοιχείο της έρευνας είναι ότι έχει αφήσει ένα μεγάλο κομμάτι εκτός θέματος : δεν αποσκοπούσε να επιλύσει πλήρως το ζήτημα που μελετάμε εδώ αλλά ένα τμήμα του, επομένως ούτε και το ενδεχόμενο όφελος προσδιορισμού προηγούμενων επιθέσεων σε περίπτωση ανίχνευσης με χρήση νευρωνικών δικτύων. Ωστόσο, η θεωρία πως ένα νευρωνικό δίκτυο είναι δυνατό να ανιχνεύσει περιστατικά κατάχρησης σε επιθυμητό βαθμό ακρίβειας λαμβάνεται υπόψη έπειτα.

3.4.1. Περιγραφή Νευρωνικού Δικτύου

Το πρώτο πρότυπο νευρωνικού δικτύου σχεδιάστηκε για να αποδειχθεί αν ένα τέτοιο δίκτυο είναι ικανό να ανιχνεύει εισβολές σε αυτό που να προμηνύουν κατάχρηση ή επίθεση. Το πρότυπο αυτό ακολουθεί MLP (Master Limited Partnership) αρχιτεκτονική αποτελούμενη από τέσσερα βασικά επίπεδα πλήρως συνδεδεμένα με εννέα κόμβους εισόδου και δύο εξόδου. Έτσι γίνεται ροή των δεδομένων προς τα εμπρός προσφέροντας ευελιξία και δυνατότητα καλύτερης προσέγγισης ποικίλων προβλημάτων

Ο αριθμός των κρυφών επιπέδων, αλλά και των κρυφών κόμβων στα επίπεδα αυτά, μπορούσε να προσδιοριστεί με τη διαδικασία «δοκιμής και λάθους». Καθένας από τους κρυμμένους κόμβους και τους κόμβους εξόδου εφαρμόζει τη Σιγμοειδή συνάρτηση μεταφοράς (η οποία έχε αναφερθεί στο κεφάλαιο 1) στα διάφορα βάρη των συνδέσεων. Το νευρωνικό δίκτυο πρέπει να παράγει μία τιμή εξόδου 0.0 και 1.0 στους δύο κόμβους εξόδου όταν δεν υπάρχει υπόνοια επίθεσης στο δίκτυο και 1.0 και 0.0 όταν υπάρχει σχετική υπόνοια.

Τα στοιχεία για την εκπαίδευση και δοκιμή του προτύπου δημιουργήθηκε με τη χρήση RealSecure™ και καταγράφηκε από την Internet Security Systems, Inc. Το RealSecure έχει σχεδιαστεί για να χρησιμοποιείται από τους administrators ασφάλειας του δικτύου για να συλλέγουν με παθητικό τρόπο δεδομένα από το δίκτυο και να εντοπίζουν επιθέσεις. Χρησιμοποιεί ένα έμπειρο σύστημα το οποίο περιλαμβάνει πάνω από 360 υπογραφές επιθέσεων και τις συγκρίνει με την τρέχουσα κίνηση στο δίκτυο ώστε να εντοπιστούν αν τυχόν υπάρχουν. Έχει ρυθμιστεί έτσι ώστε να συγκεντρώνει στοιχεία για κάθε περιστατικό που είναι συμβατό ή σύμφωνο με ένα πλαίσιο του δικτύου, όπως για παράδειγμα διεύθυνση πηγής ή προορισμού, και να επιστρέφει ως αποτέλεσμα την ανάλυση καθενός από αυτά τα περιστατικά.

Τα τρία επίπεδα προεπεξεργασίας των δεδομένων διεξάγονται για να ετοιμαστούν σωστά τα δεδομένα που χρησιμοποιούνται για την εκπαίδευση και εξέταση των νευρωνικών δικτύων.

1. Εννέα από τα καταγεγραμμένα στοιχεία-δεδομένα των συμβάντων επιλέγονται. Η επιλογή γίνεται βάση των στοιχείων των συνηθών πακέτων δεδομένων του δικτύου αλλά και αυτών που παρέχουν πλήρη περιγραφή της πληροφορίας που προωθείται με τα πακέτα.
   - **ID Πρωτοκόλλου**: με τι πρωτόκολλο συνδέεται το συμβάν (έχουμε TCP=0, UDP=1, ICMP=2 και για άγνωστο 3).
   - **Port πηγής** : ο αριθμός της θύρας που χρησιμοποιεί η πηγή
   - **Port Προορισμού**: ο αριθμός θύρας που χρησιμοποιεί ο προορισμός.
   - **Διεύθυνση Πηγής**: η IP διεύθυνση της πηγής
   - **Διεύθυνση προορισμού**: η IP διεύθυνση του προορισμού
   - **Τύπος ICMP**: Echo Request ή Null
   - **Κωδικός ICMP**: το πεδίο κωδικού από το πακέτο ICMP
   - **Μήκος ακατέργαστων δεδομένων**: το μήκος δεδομένων στο πακέτο
   - **Ακατέργαστα δεδομένα**: το τμήμα των δεδομένων του πακέτου
2. Τρία από τα εννέα στοιχεία-δεδομένα (*τύπος ICMP, κωδικός ICMP και Ακατέργαστα δεδομένα*) που επιλέχθηκαν στο προηγούμενο επίπεδο μετατρέπονται σε τυποποιημένη αριθμητική μορφή. Η διαδικασία αφορά στην δημιουργία σχεσιακών πινάκων για κάθε έναν από τους τύπους δεδομένων και στην ανάθεση διαδοχικών αριθμών για κάθε μοναδικό τύπο στοιχείου. Με τον τρόπο αυτό δημιουργούνται **DISTINCT SELECT** ερωτήσεις για καθένα από τους τύπους και τα αποτελέσματα φορτώνονται σε πίνακες στους οποίους αποδίδεται ένας μοναδικός ακέραιος για κάθε καταχώρηση. Έπειτα, οι τρεις αυτοί πίνακες συνδέονται και δίνουν έναν τελικό που περιέχει το καταγεγραμμένο συμβάν. Μία ερώτηση (**DISTINCT SELECT**) χρησιμοποιείται μετά για να επιλεχθούν έξι από τα εννέα στοιχεία (όσα έχουν μείνει δηλαδή) και τα μοναδικά αναγνωριστικά στοιχεία που αφορούν τα τρία στοιχεία που επιλέχθηκαν πρώτα. Όμως υπάρχει και ένα δέκατο στοιχείο (**Attack**) που εκχωρείται σε κάθε εγγραφή, που βασίζεται στην διαπίστωση του κατά πόσο το συμβάν αυτό αποτελεί επίθεση ή μέρος αυτής σε ένα δίκτυο. Το στοιχείο αυτό χρησιμοποιείται στην εκπαίδευση ως *ζητούμενος στόχος των νευρωνικών δικτύων για κάθε εγγραφή.*
3. Τα αποτελέσματα των ερωτήσεων μετατρέπονται σε ASCII οριοθετημένη με κόμματα ώστε να μπορεί να χρησιμοποιηθεί από το νευρωνικό δίκτυο. Τα προεπεξεργασμένα δεδομένα τελικά φορτώνονται στη DataPro υπηρεσία που παρέχεται από την QNet. Το QNet χρησιμοποιεί την εφαρμογή αυτή για να φορτώσει

τα δεδομένα στο νευρωνικό δίκτυο κατά τη διάρκεια της εκπαίδευσης αυτού.

3.4.2. Αποτελέσματα Πειράματος

Η εκπαίδευση των νευρωνικών δικτύων στο πείραμα αυτό έγινε με χρήση ενός backpropagation αλγορίθμου για 10000 αναφορές-δοκιμές των επιλεγμένων στοιχείων κατάρτισης(δηλαδή των στοιχείων που χρησιμοποιήθηκαν στην εκπαίδευση). Όπως και στην αρχιτεκτονική του νευρωνικού δικτύου(που χρησιμοποιούμε) που επιτρέπει τη ροή δεδομένων προς τα εμπρός, η χρήση του backpropagation αλγορίθμου στην εκπαίδευση βασίζεται στις μέχρι τώρα αποδεδειγμένη προσέγγιση στην ανάπτυξη των νευρωνικών δικτύων σε διάφορες περιπτώσεις. Από τις 9463 αναφορές που ήταν προεπεξεργασμένα ώστε να μπορούν να χρησιμοποιήσουν το πρότυπο, 100 επιλέχθηκαν τυχαία και τα υπόλοιπα χρησιμοποιήθηκαν στην εκπαίδευση του συστήματος.

Η εκπαίδευση του νευρωνικού δικτύου με δοκιμές χρειάζεται 27 περίπου ώρες ώστε να ολοκληρωθεί.

Μετά την ολοκλήρωση της εκπαίδευσης και δοκιμής του MLP νευρωνικού δικτύου τα διαφορετικά βάρη των συνδέσεων παγώνουν και το δίκτυο εξετάζεται. Τρία πρότυπα δείγματα περιέχουν τα «κανονικά» συμβάντα του δικτύου και μια μοναδική αναπαράσταση (προσομοίωση) επίθεσης λαμβανόμενη ως συμβάν που χρησιμοποιείται για τις δοκιμές που υπόκειται το νευρωνικό δίκτυο. Το MLP είναι σε θέση να αναγνωρίσει σωστά καθεμία από τις ενσωματωμένες επιθέσεις στα δεδομένα δοκιμών. Αν και το πρότυπο δεν είναι σχεδιασμένο για να ανιχνεύσει την εισβολή σε δίκτυο ή σύστημα γενικά τα αποτελέσματα δείχνουν καθαρά τις δυνατότητες ενός νευρωνικού δικτύου στην ανίχνευση μεμονωμένων περιπτώσεων πιθανής κατάχρησης από μια αντιπροσωπευτική ροή δεδομένων στο δίκτυο ή σύστημα.

3.5. Κλείνοντας….

Η έρευνα και ανάπτυξη συστημάτων ανίχνευσης εισβολής έχει ξεκινήσει από τις αρχές της δεκαετίας του ’80. Οι μεγάλες προκλήσεις που αντιμετώπισαν οι ερευνητές λόγω της ραγδαίας εξέλιξης των κακόβουλων λογισμικών και των τρόπων επίθεσης σε συστήματα, τους ανάγκασαν να ψάχνουν καλύτερες και πιο αποτελεσματικές μεθόδους ανίχνευσης κατάχρησης.

Η ανίχνευση κατάχρησης σε δίκτυο καθίσταται πολύ δύσκολη ως επιχείρηση λόγω του μεγάλου ποσοστού ευαισθησίας σε πολλά σημεία των πληροφοριακών συστημάτων αλλά και της εξέλιξης των τρόπων επίθεσης που χρησιμοποιούνται.

ΚΕΦΑΛΑΙΟ 4^{Ο}: ΧΡΗΣΗ ΝΕΥΡΩΝΙΚΩΝ ΔΙΚΤΥΩΝ ΣΤΗΝ ΑΝΙΧΝΕΥΣΗ ΕΙΣΒΟΛΗΣ

4.1. Εισαγωγή στα Συστήματα Ανίχνευσης Εισβολής(Intrusion Detection Systems- IDS)

Στις μέρες μας τα Συστήματα Ανίχνευσης Εισβολής (τα οποία θα αποκαλούμε IDS από εδώ και έπειτα) χρησιμοποιούνται κυρίως για την ασφάλεια δικτύων εταιρειών και εκπαιδευτικών παραγόντων (Σχολεία, Πανεπιστήμια κτλ). Ιδανικά, ένα IDS παρέχει την δυνατότητα ανίχνευσης επιθέσεων σε πραγματικό χρόνο (είτε που έχουν ήδη λάβει χώρα, είτε λαμβάνουν χώρα την επικείμενη στιγμή είτε πρόκειται να συμβούν και κάτι μπορεί να προδιαθέσει τέτοιου είδους κίνηση) και εξυπηρετεί στην παύση της επίθεσης (για παράδειγμα τροποποιώντας τους περιορισμούς στο firewall).

Με τη χρήση νευρωνικών δικτύων σε IDS, εκτός όλων των άλλων που θα αναλυθούν παρακάτω, αποφεύγονται οι πολλαπλοί και λανθασμένοι συναγερμοί ανίχνευσης επίθεσης ή εισβολής. Σε αυτό το σημείο πρέπει να αναφερθεί ότι παρόλο που η μέθοδος είναι ακόμα σε ερευνητικό στάδιο διαθέτει μακράν περισσότερα υπέρ από τα κατά της και δείχνει να κερδίζει καθημερινά έδαφος στον ερευνητικό τομέα.

Οι πιο πρόσφατες προσεγγίσεις για αυτή τη διαδικασία χρησιμοποιούν βασικούς κανόνες της ασφάλειας σε συστήματα που αποσκοπούν στον εντοπισμό και γνώση πιθανόν γνωστών επιθέσεων. Ωστόσο, τέτοιου είδους τεχνικές δεν διαθέτουν δυνατότητα εντοπισμού επιθέσεων που δεν έχουν την αναμενόμενη μορφή, οπότε παραμένουν άγνωστες έως ότου συμβούν. Τα τεχνητά νευρωνικά δίκτυα παρέχουν τη δυνατότητα ταυτοποίησης και διαβάθμισης δραστηριοτήτων βασιζόμενων σε περιορισμένες, ελλιπείς και μη-γραμμικές πηγές δεδομένων. Η προσφορά και άλλα πολλά πλεονεκτήματα των νευρωνικών δικτύων, που αναφέραμε στο 1^{ο} κεφάλαιο, είναι η βάση για μια διαδικασία εντοπισμού κατάχρησης η οποία θα αναλυθεί περαιτέρω.

Λόγω της αυξανόμενης εξάρτησης που έχουν οι εταιρείες και οι κρατικές υπηρεσίες στα δίκτυά τους η σημασία και κρισιμότητα προστασίας των δικτύων αυτών από επιθέσεις είναι μεγάλη. Μία και μόνο διείσδυση σε ένα δίκτυο υπολογιστών μπορεί να προκαλέσει απώλεια η μη εξουσιοδοτημένη χρήση ή τροποποίηση μεγάλης ποσότητας δεδομένων και τελικά αναξιοπιστία, για όλη την πληροφορία που διαρρέεται στο δίκτυο, στους χρήστες. Η πληθώρα μεθόδων αντιμετώπισης εισβολών σε δίκτυο έδωσαν ελπίδα στους χρήστες αλλά έχουν ένα βασικό μειονέκτημα: απαιτούν ακριβή και έγκαιρο προσδιορισμό της επίθεσης, κάτι που συνήθως δεν είναι εφικτό.

Στο κεφάλαιο αυτό θα αναφέρεται αρχικά τι είναι ένα IDS,η αρχιτεκτονική του αλλά και εργαλεία του και έπειτα αναλύονται οι διαφορές που έχουν απασχολήσει τους ερευνητικούς κύκλους για την βελτίωση των IDS και ειδικότερα με τη χρήση Νευρωνικών Δικτύων.

4.2. Ταξινόμηση IDS

4.2.1. Κατηγορίες IDS

Τα συστήματα ανίχνευσης εισβολής μπορούν να ταξινομηθούν σε 3 (τρεις) κατηγορίες:

i. ***host-based IDS***, δηλαδή βασίζεται στην αξιολόγηση πληροφοριών που έχουν βρεθεί σε ένα ή και περισσότερα συστήματα (host συστήματα), συμπεριλαμβανομένου του περιεχόμενου των λειτουργικών συστημάτων, αρχείων του συστήματος αλλά και αρχείων εφαρμογών.
ii. ***network-based IDS***, δηλαδή βασίζεται στο δίκτυο, στην αξιολόγηση πληροφοριών που έχουν συλλεχθεί από δικτυακές εφαρμογές και επικοινωνίες κάνοντας ανάλυση της ροής των πακέτων (τα οποία συλλαμβάνονται με μια σειρά αισθητήρων) που ταξιδεύουν σε όλο το δίκτυο.
iii. ***vulnerability-assessment IDS***, δηλαδή ανάλογα με την ευπάθεια του συστήματος. Γίνεται ανίχνευση της ευπάθειας σε εσωτερικά δίκτυα και firewalls

4.2.2. Μοντέλα IDS

Υπάρχουν 2 (δύο) βασικά μοντέλα ανάλυσης γεγονότων για την ανίχνευση επίθεσης:

a. ***Το μοντέλο ανίχνευσης κατάχρησης*** (το οποίο έχει αναλυθεί διεξοδικά σο κεφάλαιο 3), και
b. ***Το μοντέλο ανίχνευσης ανωμαλίας***.

Στην πρώτη περίπτωση το IDS ανιχνεύει κατάχρηση του συστήματος ψάχνοντας για δραστηριότητες που συνάδουν με γνωστές υπογραφές

εισβολών ή ευπάθειας ενώ αντίθετα στην δεύτερη περίπτωση γίνεται ανίχνευση ψάχνοντας μη φυσιολογική κίνηση δικτύου.

Βέβαια υπάρχουν και τα εργαλεία. Τα περισσότερα IDS εργαλεία που υπάρχουν στο εμπόριο αφορούν το πρώτο μοντέλο, πρέπει βέβαια οι υπογραφές να ενημερώνονται(να γίνεται συνεχές update ώστε να μπορεί να είναι εφικτή η βελτιστοποίηση του στόχου).

Τα IDS που είναι βασισμένα στο μοντέλο ανίχνευσης ανωμαλιών έχουν τη δυνατότητα να ανιχνεύουν κάποια στοιχεία της εκάστοτε επίθεσης(και να μπορούν να αναγνωρίσουν την απόπειρα επίθεσης) χωρίς να έχουν εκπαιδευτεί για συγκεκριμένο μοντέλο επίθεσης. Βέβαια το μεγάλο τους μειονέκτημα έγκειται στο γεγονός ότι τα IDS είναι επιρρεπή σε λανθασμένους (ψευδείς) συναγερμούς λόγω της μεγάλης τους ευαισθησίας.

4.3. Εργαλεία IDS

4.3.1. Η Έρευνα του Jackson

Η μελέτη του Jackson αφορά την πλήρη καταγραφή των εργαλείων–προϊόντων IDS. Συγκεκριμένα μελέτησε δεκαεπτά(17) προϊόντα και σύμφωνα με τα βασικά χαρακτηριστικά τους τα κατέταξε σε ομάδες και ασχολήθηκε περεταίρω μαζί τους. Οι ομάδες των προϊόντων είναι οκτώ(8), όσα και τα χαρακτηριστικά τους, και είναι οι εξής:

* *Καταλληλότητα του IDS* στην αρχιτεκτονική που ακολουθεί και στο σύστημα διαχείρισης
* *Ευελιξία προσαρμογής* τους σε συγκεκριμένο δίκτυο ώστε να παρακολουθείται
* *Προστασία* απέναντι σε κακόβουλα λογισμικά άγνωστα ή παραποιημένα (ώστε να περνούν χωρίς να αναγνωρίζονται)
* *Διαλειτουργικότητα* με άλλα εργαλεία-προϊόντα IDS ή διαχείριση δικτύου ή γενικά άλλους μηχανισμούς ασφάλειας
* *Πληρότητα*, δηλαδή να υπάρχει η δυνατότητα να επεκτείνεται (αν κρίνεται αναγκαίο) το σενάριο εντοπισμού εισβολή, πχ κλείδωμα συγκεκριμένων urls ή παρακολούθηση του περιεχόμενου e-mails κτλ.
* *Διαχείριση γεγονότων*, δηλαδή διαχείριση και αναφορά ανίχνευσης ίχνους και ενημέρωση της βάσης δεδομένων του IDS
* *Ενεργή αντίδραση* όταν λαμβάνει χώρα μια επίθεση όπως αναδιαμόρφωση αναχώματος ασφαλείας ή δρομολογητή
* *Τεχνική Υποστήριξη* προϊόντος.

4.3.2. ***Αποτελέσματα Άλλων Ερευνών***

Μια άλλη πρόσφατη έρευνα πάνω στα εργαλεία ανίχνευσης εισβολής (IS-Intrusion Detection) πραγματοποιεί την κατάταξη βάσει των τριών μοντέλων (όπως τα έχουμε αναλύσει και παραπάνω) :

- ***Host-based***, αυτά τα συστήματα IDS ανιχνεύουν επιθέσεις σε μεμονωμένο σύστημα, με τη χρήση συστημάτων καταγραφής και ελέγχων του λειτουργικού συστήματος. Γνωστά εργαλεία αυτού του τύπου είναι τα: *Cybercop from Network Associates* (NAI) (http://www.pgp.com), *KaneSecurity Monitor (KSM) from RSA Security* (http://www.rsasecuriy.com) καθώς επίσης και το *Tripwire* (http://www.tripwire.org) το οποίο είναι ένα πολύ ενδιαφέρον εργαλείο καθώς ανιχνεύει αλλαγές σε administrator αρχεία ή αρχεία χρήστη σε έναν Server.
- ***Network-based***, αυτά τα IDS συστήματα ανιχνεύουν επιθέσεις λαμβάνοντας και αναλύοντας τα πακέτα του δικτύου από *αισθητήρες* τοποθετημένους σε διάφορα σημεία του δικτύου. Παραδείγματα από γνωστά εργαλεία IDSαυτής της ομάδας είναι τα : *RealSecure* της *Internet Security Scanner* (ISS) (http://www.iss.net), *Cisco Secure IDS και NetRanger* της Cisco Systems, *Centrax* της CyberSafe corporation και *Network Flight Recorder NFR.* Επίσης ένα ανοιχτό και ελεύθερα διαθέσιμο IDS αυτής της κατηγορίας είναι το *Snort* (www.snort.org) το οποίο είναι ιδιαίτερα ελαφρύ συν τοις άλλοις.

  Το βασικότερο μειονέκτημα των Network-Based IDS είναι η δυσκολία στην επεξεργασία σε πραγματικό χρόνο όλων των πακέτων ενός πολύ μεγάλου δικτύου. Βέβαια προσφέρονται παροδικές λύσεις. Ένα εξίσου σημαντικό πρόβλημα είναι ο κατακερματισμός των δικτύων από switches, κάτι που συνεπάγεται δυσκολία στην ομαλή καταγραφή πληροφορίας σε ένα παγκόσμιο δίκτυο(global network) .

- ***Vulnerability-based***, δηλαδή εργαλεία αξιολόγησης ευπάθειας τα οποία είναι σαρωτές ασφάλειας που ανιχνεύουν αν υπάρχει στο σύστημα κάποια ευπάθεια (γνωστού τύπου) σε συγκεκριμένες περιοχές του λειτουργικού συστήματος. Παραδείγματα εργαλείων αυτής της κατηγορίας είναι τα : *CyberCop Scanner* της PGP Security και *SecureScan NX* της Networks Vigilance (γνωστή και ως NV e-secure).

  Ένα ελεύθερα διαθέσιμο στην αγορά εργαλείο αυτού του τύπου είναι το *Nessus,* το οποίο τρέχει σε περιβάλλον linux(www.nessus.org).

4.3.3. Επιδόσεις Εμπορικών Εργαλείων IDS

Η πλειοψηφία των διαθέσιμων εργαλείων σήμερα αφορά την ανίχνευση κατάχρησης που σημαίνει πως οι διαχειριστές πρέπει να κάνουν συνέχεια *update* στην βάση δεδομένων όπου υπάρχουν οι γνωστές περιπτώσεις ευπάθειας. Έπειτα, όλα αυτά τα εργαλεία είναι ευάλωτα σε νέες υπογραφές επιθέσεων για τις οποίες δεν έχουν ενημερωθεί(άρα και δεν μπορούν να αντιμετωπίσουν).

Επιπλέον, τα εργαλεία αυτά είναι συχνά ιδιαίτερα ευαίσθητα σε ψευδής συναγερμούς επίθεσης συνεπώς δεν γίνεται ομαλά η διακίνηση πληροφορίας σε δίκτυο.

Σημαντικά IDS που διατίθενται στην αγορά δεν μπορούν να διαχειριστούν περιπτώσεις κατακερματισμού και επανασυναρμολόγησης πακέτων IP (κάτι που πιθανώς να πρέπει να γίνει).

4.4. Εφαρμογή Νευρωνικών Δικτύων στην Ανίχνευση Εισβολής

Πάνω σε αυτό το θέμα, καθώς έχει γίνει κάποια αναφορά και στο κεφάλαιο 3, έχουν γίνει τέσσερις(4) βασικές προσεγγίσεις. Αυτές αφορούν *1)την ανίχνευση κατάχρησης, 2)την ανίχνευση Ανωμαλίας, 3)την ανίχνευση εισβολής σε βάση δεδομένων και 4) την Χρήση Νευρωνικών Δικτύων για ανίχνευση εισβολής*. Παρακάτω γίνεται ανάλυση της κάθε προσέγγισης με λεπτομέρειες.

4.4.1. Προσέγγιση για την Ανίχνευση Κατάχρησης

Διάφορες προσεγγίσεις που έχουν χρησιμοποιηθεί και γίνει αποδεκτά(μετά τη χρήση τους σε πειράματα και πειραματικές μεθόδους) είναι:

- *Τα έμπειρα συστήματα*, συμπεριλαμβανομένου ενός συνόλου κανόνων που περιγράφουν και βοηθούν στο να εντοπιστούν οι επιθέσεις
- *Η επιβεβαίωσης υπογραφής*, όπου τα σενάρια επίθεσης μεταφράζονται σε ακολουθίες ελέγχου γεγονότων
- *Τα δίκτυα PETRI*, όπου οι γνωστού τύπου επιθέσεις παρουσιάζονται με γραφικά δίκτυα petri

- *Διαγράμματα καταστάσεων*(state transition diagrams), τα οποία εντοπίζουν τις επιθέσεις με ένα σύνολο στόχων και μεταβατικών καταστάσεων

Η προσέγγιση από τις προαναφερθέντες που είναι κοινώς διαδεδομένη (περισσότερο από οποιαδήποτε άλλη), είναι η επιβεβαίωση υπογραφής. Εδώ το σύστημα ανιχνεύει επιθέσεις που έχει ξαναδεί και του είναι γνωστές αναζητώντας υπογραφές αναλλοίωτες από τις επιθέσεις αυτές. Οι υπογραφές εντοπίζονται σε αρχεία ελέγχου ή σε εφαρμογές που ψάχνουν πακέτα μέσα και έξω από την επιτιθέμενη συσκευή.

Ο περιορισμός της προσέγγισης οφείλεται:

- Στη μεγάλη συχνότητα λανθασμένων συναγερμών του συστήματος
- Στην ανάγκη καθορισμού της υπογραφής της επίθεσης και έπειτα της ενημέρωσης των υπογραφών των επιθέσεων στο εργαλείο IDS. Η υπογραφή μιας επίθεσης μπορεί αν είναι δύσκολο να εντοπιστεί.
- Στο γεγονός ότι οι υπογραφές νέων επιθέσεων δεν εντοπίζονται αυτόματα χωρίς να έχει ενημερωθεί το IDS.

4.4.2. Προσέγγιση για την Ανίχνευση Ανωμαλιών

Η ανίχνευση ανωμαλιών σε Network ή Host-based IDS περιλαμβάνει :

- *Ανίχνευση threshold*, όπου ανιχνεύεται η ανώμαλη λειτουργία του Server ή του δικτύου, για παράδειγμα μη φυσιολογική κατανάλωση CPU για έναν server ή αδικαιολόγητος κορεσμός στο δίκτυο
- *Στατιστικές μετρήσεις*
- Σε κανόνες που απορρέουν από τα *έμπειρα συστήματα* (και με τη χρήση έμπειρων συστημάτων σε αυτό)
- *Μη γραμμικούς αλγόριθμους* όπως τα **Νευρωνικά Δίκτυα**

Η πιο διαδεδομένη προσέγγιση από τις παραπάνω είναι η *στατιστική ανάλυση*, όπου ο χρήστης ή η συμπεριφορά του συστήματος μετριέται βάσει του αριθμού των μεταβλητών ανά το χρόνο. Οι μεταβλητές αυτές μπορεί να αφορούν το όνομα του χρήστη ή ο χρόνος του logout του κάθε session ή οι πόροι που χρησιμοποιούνται σε κάθε session ή ακόμα και η διάρκεια χρήσης των πόρων.

Ο κυριότερος περιορισμός αυτής της προσέγγισης είναι να βρεθεί το σωστό threshold και παράλληλα να αποφεύγονται οι συχνοί ψευδείς συναγερμοί.

4.4.3. Προσέγγιση χρήσης Νευρωνικών Δικτύων Για την Ανίχνευση Εισβολής

Μια πολλά υποσχόμενη έρευνα για την ανίχνευση εισβολής αφορά τεχνικές βασισμένες στα Νευρωνικά Δίκτυα.

Προσέγγιση

Γνωρίζοντας πως ένα νευρωνικό δίκτυο αλλάζει ανάλογα με τα δεδομένα που έχει λάβει κατά την εκπαίδευσή του είναι κατανοητό πως μπορούν να μετατρέπονται τα εισερχόμενα και τα εξερχόμενα δεδομένα στο σύνολό τους μέσω ενός συνόλου απλών μονάδων επεξεργασίας ή κόμβων και συνδέσεων μεταξύ τους. Τα υποσύνολα των μονάδων είναι βασικά κόμβοι εισόδου, εξόδου και κόμβοι μεταξύ αυτών σε κρυμμένα (ή όχι) επίπεδα. Η σημαντικότητα της σύνδεσης μεταξύ των κόμβων είναι μεγάλη καθώς καθορίζει κατά πόσο η μία μονάδα μπορεί να επηρεάσει την άλλη.

Υπάρχουν δύο αρχιτεκτονικές των νευρωνικών δικτύων :

* ***Supervised αλγορίθμων εκπαίδευσης*** (κατάρτισης) των Νευρωνικών Δικτύων. Σε αυτό το στάδιο εκπαίδευσης, το δίκτυο γνωρίζοντας την είσοδο γνωρίζει την επιθυμητή έξοδο. Η αρχιτεκτονική αυτή είναι Multi-Level Perceptron (MLP).
* ***Unsupervised αλγορίθμων*** κατάρτισης (εκπαίδευσης). Εδώ το δίκτυο μαθαίνει χωρίς όμως να γνωρίζει την έξοδο δεδομένης εισόδου όπως παραπάνω. Γνωστοί Unsupervised αλγόριθμοι κατάρτισης είναι οι SOM(Self-Organizing Maps) οι οποίοι προσπαθούν να μάθουν μια χαρτογράφηση από το χώρο εισόδου στα clusters. Τέτοιοι αλγόριθμοι χρησιμοποιούνται σε προβλήματα ταξινόμησης παντός τύπου.

Η πιο σημαντική ιδιότητα των Νευρωνικών Δικτύων είναι ότι μπορούν αυτόματα να μαθαίνουν/ διαμορφώνουν τον τρόπο αντίδρασής τους ανάλογα με τα δεδομένα εισόδου που δέχονται(ουσιαστικά μιλάμε για το γεγονός ότι εκπαιδεύονται με τρόπο τέτοιο ώστε να θυμούνται σε περίπτωση εισόδου δεδομένων που έχουν ξαναχρησιμοποιηθεί και να γνωρίζουν την αντίδραση στο δίκτυο καθώς και τα αποτελέσματα εξόδου που πρέπει να δοθούν). Για να εφαρμοστούν τα Νευρωνικά Δίκτυα στην Ανίχνευση Εισβολής πρέπει πρώτα να τα εκπαιδεύσουμε. Τα εκθέτουμε σε «άκακα» δεδομένα αρχικά αλλά και σε επιθέσεις στις οποίες αμύνονται αυτόματα στην φάση της εκπαίδευσης. Εν συνεχεία λαμβάνουν χώρα τεστ επίδοσης του δικτύου με την κανονική κίνηση του δικτύου και κανονικές επιθέσεις σε αυτό.

4.4.4. Πρόσφατες Μελέτες

Τα νευρωνικά δίκτυα έχουν χρησιμοποιηθεί σημειώνοντας μεγάλες επιτυχίες σε σύνθετα προβλήματα. Παρακάτω παρατίθενται τέσσερις(4) μελέτες που αφορούν την εφαρμογή των νευρωνικών δικτύων στην ανίχνευση εισβολής, είτε αυτό αφορά την ανίχνευση κατάχρησης, με την οποία ασχοληθήκαμε στο προηγούμενο κεφάλαιο, είτε την ανίχνευση ανωμαλίας στο δίκτυο.

4.4.4.1. ΠΑΝΕΠΙΣΤΗΜΙΟ ΓΕΩΡΓΙΑΣ: Εφαρμογή Νευρωνικών Δικτύων σε IDS

Οι J. Cannady και J. Mahaffey της ερευνητικής μονάδας του Ινστιτούτου Τεχνικής Έρευνας (GTRI) έκαναν μια έρευνα θέλοντας να εφαρμόσουν το μοντέλο Multi-Level Perceprton (MLP) και Self-Organizing Maps(MLP/SOM) στην ανίχνευση κατάχρησης.

Το πρωτότυπο MLP έχοντας συγκεκριμένα χαρακτηριστικά μπορούσε να γίνει δυνατή η προσομοίωση συγκεκριμένων τύπων επιθέσεων όπως ISS, SYNFlood και SATAN Scans αλλά και κάθε επίθεση που μπορεί να είναι αναγνωρίσιμη εντός της φυσιολογικής κίνησης του δικτύου. Τα χαρακτηριστικά του πρωτοτύπου είναι τα εξής: **α.** τέσσερα επίπεδα άκρως συνδεδεμένα μεταξύ τους, **β.** 9 κόμβους εισόδου και 2 κόμβους εξόδου.

Εν συνεχεία ένα MLP/SOM πρωτότυπο σχεδιάζεται στοχεύοντας στην ανίχνευση (ίσως) κρυφών και πιθανών επιθέσεων. Το νευρωνικό δίκτυο στη φάση εκπαίδευσης συγκλίνει σε εξαιρετικά γρήγορους ρυθμούς. Αποτελέσματα της εφαρμογής αυτής με ανεπιτυχείς FTP προσπάθειες σύνδεσης έχουν ανιχνευτεί σωστά ως επιθέσεις όπως έπρεπε.

4.4.4.2. MIT: Έρευνα για IDS Νευρωνικά Δίκτυα

Και οι R. Lippmann και R. Cunningham του MIT Lincoln Laboratory διερεύνησαν κατά πόσο μπορεί να εφαρμοστεί για επιτυχή ανίχνευση κατάχρησης το μοντέλο των Νευρωνικών Δικτύων, ψάχνοντας για λέξεις κλειδιά που να υποδηλώνουν επίθεση που μπορεί να λαμβάνει χώρα στην κίνηση του δικτύου. Χρησιμοποίησαν και εδώ MLP για να ανιχνεύσουν Unix-Host επιθέσεις αλλά και επιθέσεις που «χτυπούν» απευθείας στον server. Ομόρριζες λέξεις κλειδιά χρησιμοποιήθηκαν για να ανιχνεύουν παρασκευασμένες επιθέσεις και ενέργειες που εκτελούνται μετά την επίθεση.

Ένας αισθητήρας (perceptron) δύο επιπέδων σχεδιάστηκε φέροντας k κόμβους εισόδου, 2k κρυφούς κόμβους και 2 εξόδους(φυσιολογικής κίνησης και επιθέσεων). Το backpropagation στη φάση της εκπαίδευσης ανιχνεύει τα βάρη του νευρωνικού δικτύου(ανατρέχουμε στο κεφάλαιο 1 όπου έχει αναφερθεί η σημαντικότητα του βάρους στο Νευρωνικό Δίκτυο). Καλή επίδοση της ανίχνευσης επιτεύχθηκε με τη χρήση 30 λέξεων-κλειδιά που χρησιμοποιήθηκαν στην ανίχνευση όπως «cat», «uudecode».

Εφαρμόζοντας στον Shell πηγαίο κώδικα 7 βασικές εντολές που αντιπροσωπεύουν μια επίθεση οι 17 στις 20 επιθέσεις ήταν ανιχνεύσιμες και μόνο μία φορά υπήρξε ψευδής συναγερμός. Όταν όμως εφαρμόστηκε σε C πηγαίο κώδικα με 2 χαρακτηριστικά οι 68 από τις 73 επιθέσεις ανιχνεύθηκαν και υπήρξαν μόλις 4 ψευδείς συναγερμοί.

Με την εφαρμογή των νευρωνικών δικτύων στη μελέτη, οι ψευδείς συναγερμοί μειώθηκαν στο (το πολύ) έναν την ημέρα και αυξήθηκε το ποσοστό επιτυχής ανίχνευσης στο 80% σύμφωνα με την βάση δεδομένων DARPA. Το σύστημα μπορούσε πλέον να ανιχνεύσει όσο παλιές τόσο και καινούργιες επιθέσεις που δεν έχουν σχέση με τα δεδομένα που χρησιμοποιήθηκαν στην φάση εκπαίδευσης και σε μικρότερη κλίμακα κατανεμημένες επιθέσεις σε πολλαπλά Sessions.

4.4.4.3. Έρευνα UBILAB Laboratory

Ο Luc Girardin του εργαστηρίου του UBILAB, ασχολήθηκε με SOM για να διαμορφώσει την ομαδοποίηση της κίνησης του δικτύου και τον εντοπισμό επιθέσεων βασιζόμενος στα Νευρωνικά Δίκτυα, συσχετίζοντάς τα με μια οπτική προσέγγιση του κίνησης του δικτύου. Οι SOM τρέχουν το project των συμβάντων του δικτύου σε κατάλληλο δισδιάστατο χώρο για την απεικόνιση. Έπειτα παρατίθενται στον Admin του δικτύου δίνοντας του μια ολοκληρωμένη εικόνα της κίνησης. Έτσι οι εισβολές μπορούν εύκολα να απομακρυνθούν από το «μοτίβο» αυτό.

Ο Girardin, λοιπόν, δοκίμασε αυτή την προσέγγιση για τις εξής επιθέσεις:

- Network Scanning
- Network Hopping
- Πλαστογράφηση IP
- «Σπάσιμο» του κωδικού του FTP

Τα συστήματα καταγραφής των αρχείων σκανάρωνται από τα Firewalls. Ωστόσο, η συγκεκριμένη μέθοδος που χρησιμοποιήθηκε χρήζει οπτικής ερμηνείας κίνησης του δικτύου από τον administrator ώστε να ανιχνεύονται οι επιθέσεις.

4.4.4.4. Έρευνα του RST

Οι A. Ghosh και A. Schwartzbard του Reliable Software Technologies Corporations χρησιμοποίησαν τα Νευρωνικά Δίκτυα για την ανίχνευση ανωμαλιών, αναλύοντας τη τα προφίλ της συμπεριφοράς του προγράμματος για την Ανίχνευση Εισβολής. Το προφίλ της συμπεριφοράς του προγράμματος δημιουργείται από τη σύλληψη κλήσεων του συστήματος που γίνονται από το πρόγραμμα, ώστε να παρακολουθείται η συμπεριφορά των προγραμμάτων σημειώνοντας τις παρατυπίες στη συμπεριφορά τους.

Το IDS τους ήταν ένα κρυφό επίπεδο MLP. Επίσης χρησιμοποιούσαν τον λεγόμενο Lucky Bucket αλγόριθμο για να κρατούν χρονική απομνημόνευση των πρόσφατων ανωμαλιών στο σύστημα. Αυτό γίνεται με τη βοήθεια ενός μετρητή: για μια φυσιολογική έξοδο ο μετρητής είναι μηδέν(0), και για ανωμαλία ο μετρητής είναι ένα(1).

Η επίδοση του συστήματος δοκιμάστηκε με DARPA βάση δεδομένων Συμπεριλαμβανομένων και συμβατικών αλλά και όχι sessions. Εφαρμόζοντας στην ανίχνευση ανωμαλιών, το σύστημα παρουσιάζει καλή επίδοση στο θέμα της ανίχνευσης και σε παλιές και σε καινούργιες επιθέσεις. Με άλλα λόγια, εντοπίστηκε το 77% των επιθέσεων και υπήρξε ένα ποσοστό 3% ψευδών συναγερμών. Παρόλα ταύτα, η εφαρμογή για την ανίχνευση κατάχρησης παρουσίασε μεγάλο ποσοστό ψευδών συναγερμών.

Θέλοντας να βελτιώσουν το μοντέλο ανίχνευσης ανωμαλιών, δοκίμασαν μια άλλη τοπολογία του Νευρωνικού Δικτύου για την ανίχνευση εισβολής, το Elman δίκτυο για την αναγνώριση επαναλαμβανόμενων χαρακτηριστικών στα ίχνη εκτέλεσης του προγράμματος.

Εφαρμόζοντας την DARPA, τα Elman Δίκτυα μπόρεσαν να εντοπίσουν το 77% των επιθέσεων, μην έχοντας παρουσιάσει ούτε έναν ψευδή συναγερμό, βελτιώνοντας έτσι τα αποτελέσματα που δόθηκαν όταν χρησιμοποιήθηκε η MLP τοπολογία.

4.5. Κλείνοντας…

Όπως είδαμε, έχουν γίνει πολλές έρευνες πάνω στα IDS σε συνδυασμό με τα νευρωνικά δίκτυα. Σε πολλά πανεπιστήμια έγινε αναλυτική μελέτη του θέματος, χωρίς όμως να έχει βρεθεί μια καθολικά αποδεκτή λύση.

ΚΕΦΑΛΑΙΟ 5^{Ο}- ΧΡΗΣΗ ΝΕΥΡΩΝΙΚΩΝ ΔΙΚΤΥΩΝ ΣΤΗΝ ΑΣΦΑΛΕΙΑ ΣΥΣΤΗΜΑΤΩΝ ΗΛΕΚΤΡΙΚΗΣ ΕΝΕΡΓΕΙΑΣ

(Power Systems)

5.1. Εισαγωγή

Τα τελευταία χρόνια, τα συστήματα παραγωγής ηλεκτρικής ενέργειας, λόγω της μεγάλης ανάγκης, λειτουργούν υπό ακραίες συνθήκες οι οποίες πλησιάζουν ιδιαίτερα τα όρια ασφάλειας τους. Κάτω από αυτές τις συνθήκες η οποιαδήποτε διατάραξη του συστήματος(έστω και πολύ μικρή), θα μπορούσε να αποβεί μοιραία καθώς θα μπορούσε να οδηγήσει ακόμα και στην απόλυτη κατάρρευσή του συστήματος. Έτσι, ο γρήγορος και ακριβής έλεγχος είναι ιδιαίτερα σημαντικός παράγοντας για την ομαλή λειτουργία του συστήματος. Ασφάλεια Συστημάτων Ηλεκτρικής Ενέργειας, ορίζεται η ικανότητα του συστήματος να αντιστέκεται σε απρόβλεπτες καταστάσεις χωρίς όμως να παραβιάζονται τα όρια του συστήματος(αυτά που προδιαθέτουν σε ποιο βαθμό θεωρείται η λειτουργία του συστήματος φυσιολογική ή όχι).

Η ανάλυση της ασφάλειας συνήθως ορίζεται είτε ως ***Στατική(Μόνιμη)*** είτε ως ***Παροδική Ασφάλεια***. Με την εκτίμηση της *στατικής ασφάλειας* μπορεί να ανιχνευθεί περίπτωση υπερφόρτωσης τμήματος του συστήματος ή/και εκτός ορίου τάση, ακολουθώντας μια λίστα με απρόοπτα. Στην περίπτωση της *παροδικής ασφάλειας* αναφερόμαστε στην δυναμική της συμπεριφοράς του συστήματος υπό όρους όταν αυτό υποβάλλεται σε απρόοπτα. Η αξιολόγηση του επιπέδου ασφάλειας με παραδοσιακές μεθόδους περιλαμβάνει την επίλυση μη-γραμμικών εξισώσεων ροής φορτίου και ανάλυση της σταθερότητας και αξιοπιστίας σε απρόοπτες περιπτώσεις. Με τον τελευταίο τρόπο όμως απαιτείται μεγάλη διάρκεια χρόνου υπολογισμού, έτσι έχει θεωρηθεί ανίκανο να δώσει αποτελέσματα σε πραγματικό χρόνο σε συστήματα μεγάλων απαιτήσεων.

Για την πρόβλεψη της ασφάλειας τέτοιων συστημάτων μεγάλης κλίμακας έχουν χρησιμοποιηθεί τεχνικές *Αναγνώρισης Προτύπων* (Pattern Recognition-PR) καταρρίπτοντας έτσι τα όποια μειονεκτήματα προέκυπταν μέχρι τώρα με τις παραδοσιακές μεθόδους. Στο πρωταρχικό στάδιο της εφαρμογής Αναγνώρισης Προτύπων στην αξιολόγηση της ασφάλειας των συστημάτων, δημιουργήθηκε μια λίστα με δείγματα(τα οποία αποτελούν τα Πρότυπα) τα οποία δημιουργούνται από προσομοιώσεις off-line είτε λαμβάνονται από γεγονότα πραγματικού χρόνου. Το επόμενο στάδιο εξίσου μεγάλης βαρύτητας για την καλή απόδοση του συστήματος, είναι η επιλογή των στοιχείων

εισόδου, κάτι για τη διευκόλυνση του οποίου υπάρχει πληθώρα αλγορίθμων όπως Principal Component Analysis, Μεγιστοποίηση της εντροπίας και άλλοι.

Σε αυτό το κεφάλαιο θα δούμε ένα συνονθύλευμα των αλγορίθμων αυτών έτσι ώστε να επιλεχθούν τα στοιχεία εισόδου στο σύστημα σε έρευνα που έγινε από τους ***S. KALYANI and K. SHANTI SWARUP*** στο Department of Electrical Engineering, Indian Institute of Technology Madras, Chennai, India. Το θέμα της έρευνας που έκαναν αφορούσε τη χρήση των Νευρωνικών Δικτύων ώστε να αποδεικνύεται με αξιόπιστο τρόπο αν το ένα συγκεκριμένο Σύστημα Παραγωγής Ηλεκτρικής Ενέργειας είναι ασφαλές ή όχι. Αυτό γίνεται καθώς κατά την ***είσοδο στοιχείων στο σύστημα ενεργοποιείται μια συνάρτηση ταξινόμησης που έχει τη δυνατότητα να ορίζει τη κατάσταση ασφάλειας του συστήματος.***

Στην προσέγγιση αυτή θα δούμε πως χρησιμοποιούνται διάφορες δομές των Νευρωνικών Δικτύων, όπως MLP που έχουμε δει και σε προηγούμενο κεφάλαιο, Learning Quantization Vector(LQV) κατά το οποίο χρησιμοποιούνται εξισώσεις που εξυπηρετούν στην κβαντοποίηση παραμέτρων-διανυσμάτων, Probabilistic Νευρωνικά Δίκτυα τα οποία λειτουργούν βάση συναρτήσεων πιθανοτήτων(PNN) και Adaptive Resonance Theory Mapping(ARTMAP) τα οποία ουσιαστικά εξυπηρετούν στην χαρτογράφηση και σύγκριση των στοιχείων που παράγονται ανάλογα με τα δεδομένα εισόδου από το σύστημα. Τα Νευρωνικά δίκτυα(κάθε δομής) δημιουργούνται και εκπαιδεύονται βάσει συγκεκριμένων στοιχείων ανάλογα τις εκάστοτε ανάγκες. Μετά την εκπαίδευση των δικτύων γίνεται αξιολόγηση της απόδοσής τους ανάλογα με το ποσοστό ακρίβειάς και εσφαλμένης κατάταξης των στοιχείων.

5.2. Αξιολόγηση Ασφάλειας (Security Assesment)

Αξιολόγηση ασφάλειας σε τέτοιου είδους συστήματα ορίζουμε την διαδικασία η οποία καθορίζει αν και σε ποιο βαθμό ένα σύστημα είναι λογικά ασφαλές από σημαντικούς κινδύνους που μπορούν να συμβούν κατά την λειτουργία του. Υπολογίζει την ανθεκτικότητα του συστήματος σε επίπεδο ασφάλειας έναντι μιας λίστας απρόοπτων ενδεχόμενων που μπορεί να υπάρχουν στην παρούσα φάση είτε σε μελλοντική.
Στην έρευνα αυτή, παρουσιάστηκαν τα δύο είδη ασφάλειας που είδαμε και στην εισαγωγή (στατική και παροδική) όσον αφορά την αξιολόγηση ασφάλειας τέτοιων συστημάτων.

5.2.1 Αξιολόγηση Στατικής Ασφάλειας

(Static Security Assessment-SSA)

Η στατική ασφάλεια σε ένα σύστημα παραγωγής ενέργειας, συν τοις άλλοις, καθοδηγεί είτε (έπειτα από κάποια διακοπή) το σύστημα ώστε να φτάσει σε ένα συγκεκριμένο σημείο λειτουργίας χωρίς να αναγκάζεται το σύστημα να λειτουργήσει βάση ορίων συγκεκριμένων περιορισμών (Περιορισμοί Ασφάλειας)- ιδανικό είναι το σύστημα να λειτουργεί φυσιολογικά χωρίς να χρειάζεται να λαμβάνονται υπόψη οι περιορισμοί ασφαλείας. Οι περιορισμοί αυτοί ορίζουν τα όρια της τιμής της ενέργειας στο δίκτυο ώστε αυτό να ισορροπεί (μέσω της συνάρτησης 1), τη διαφορά δυναμικού και το όριο της θερμότητας των συνδέσεων στο δίκτυο (συνάρτηση 2). Σε περίπτωση παραβίασης των ορίων που προκύπτουν από τους περιορισμούς το σύστημα πιθανόν θα καταρρεύσει(το αποτέλεσμα θα είναι γενικό black–out).

Οι συναρτήσεις

$$\sum_{i=1}^{N_g} P_{Gi} = P_D + P_{Loss} \qquad P_{Gi}^{\min} \le P_{Gi} \le P_{Gi}^{\max} \quad i = 1,2 \ldots N_g \tag{1}$$

$$|V|_k^{\min} \le |V|_k \le |V|_k^{\max} \quad k = 1,2 \ldots N_b \qquad S_{km} \le S_{km}^{\max} \quad \forall \ branches\ k-m \tag{2}$$

Όπου P_{Gi} η πραγματική παραγωγή ενέργειας στο σταθμό, P_{Loss} η συνολική απώλεια ενέργειας μέσα στο δίκτυο, $|V|_k$ η διαφορά δυναμικού στο σταθμό, S_{ks} η ροή μεταξύ των k και m, N_g και N_b ο αριθμός των γεννητριών και σταθμών αντίστοιχα.

Στη διαδικασία αξιολόγησης στατικής ασφάλειας, η κατάσταση του συστήματος υπολογίζεται για πολλά ενδεχόμενα (με τη βοήθεια μη-γραμμικών συναρτήσεων ροής). Το σύστημα θα οριστεί ***στατικά ασφαλές*** αν και μόνον αν δεν παραβιάζονται οι περιορισμοί. Αν έστω και ένας περιορισμός παραβιάζεται τότε το σύστημα θεωρείται ***στατικά ανασφαλές***.

5.2.2. Αξιολόγηση Παροδικής Ασφάλειας (Transient Security Assessment-TSA)

Η παροδική ασφάλεια ενός συστήματος παραγωγής ηλεκτρικής ενέργειας καθοδηγεί (μετά από κάποια διαταραχή της ομαλής λειτουργίας) το σύστημα ώστε να επανέλθει στις φυσιολογικές του τιμές βασιζόμενο πάνω σε συγκεκριμένα φαινόμενα(συγκεκριμένες καταστάσεις) του συστήματος. Μια πρωταρχική ανάγκη ώστε να είναι αξιόπιστο ένα τέτοια σύστημα είναι η δυνατότητα να διατηρεί τις μηχανές που είναι κατανεμημένες και συγχρονισμένες να τρέχουν παράλληλα με αρκετή χωρητικότητα ώστε να μεταφέρουν το φορτίο. Η αξιολόγηση παροδικής ασφάλειας αποτελείται από την οριοθέτηση στις ταλαντώσεις του συστήματος, αν αυτές υπάρχουν, ακολουθώντας την πιθανότητα ύπαρξης λάθους ή μεγάλη πιθανότητα απροόπτου, που θα μπορούσαν να προκαλέσουν απώλεια του συγχρονισμού των κατανεμημένων μηχανών- γεννητριών.

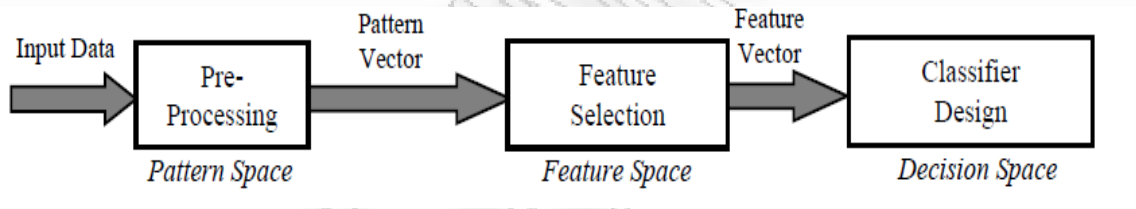
Στην ουσία η αξιολόγηση παροδικής ασφάλειας είναι ένα σύνολο σταθερών όρων που συνάδουν με την καλή κατάσταση συγχρονισμένου συστήματος. Ένα σύστημα θεωρείται ***παροδικά ασφαλές*** όταν διατηρεί

σταθερά τις τιμές που ορίζονται από το TSA αλλιώς το σύστημα είναι ***παροδικά ανασφαλές.***

5.3. Αναγνώριση Προτύπων (Pattern Recognition-PR)

Ως αναγνώριση προτύπων (PR) ορίζεται «το να παίρνεις με τη σειρά δεδομένα και να παίρνεις ως αποτέλεσμα μια πράξη βασισμένη στην κατηγορία που ανήκουν τα δεδομένα που χρησιμοποιήθηκαν». Η ταξινόμηση συγκεκριμένων δεδομένων-που αποτελεί τα πρότυπα- δίνει έναν αριθμό κατηγοριών ή κλάσεων. Τα βασικά συστατικά των PR είναι η προεπεξεργασία, επιλογή χαρακτηριστικού και κατηγοριοποίηση δομής. Ο ρόλος της προεπεξεργασίας είναι η διασαφήνιση ενός πολύπλοκου προτύπου. Ο αντίστοιχος ρόλος της επιλογής χαρακτηριστικού είναι η επιλογή συγκεκριμένου χαρακτηριστικού μέσω της αριθμητικής πληροφορίας που προκύπτει από την παρατήρηση των μελετητών του συστήματος. Με το βασικό χαρακτηριστικό να έχει επιλεγεί, το τρίτο εργαλείο κατηγοριοποιεί τα αποτελέσματα των παρατηρήσεων, βασιζόμενο πάνω στα επιλεγμένα-ή στο επιλεγμένο- χαρακτηριστικό.

ΔΙΑΓΡΑΜΜΑ ΣΥΣΤΗΜΑΤΟΣ ΑΝΑΓΝΩΡΙΣΗΣ ΠΡΩΤΟΤΥΠΩΝ



5.4. Νευρωνικά Δίκτυα και Αναγνώριση Προτύπων (NN-PR) στην Αξιολόγηση της Ασφάλειας

Βασική ιδέα της προσέγγισης Αναγνώρισης Προτύπων

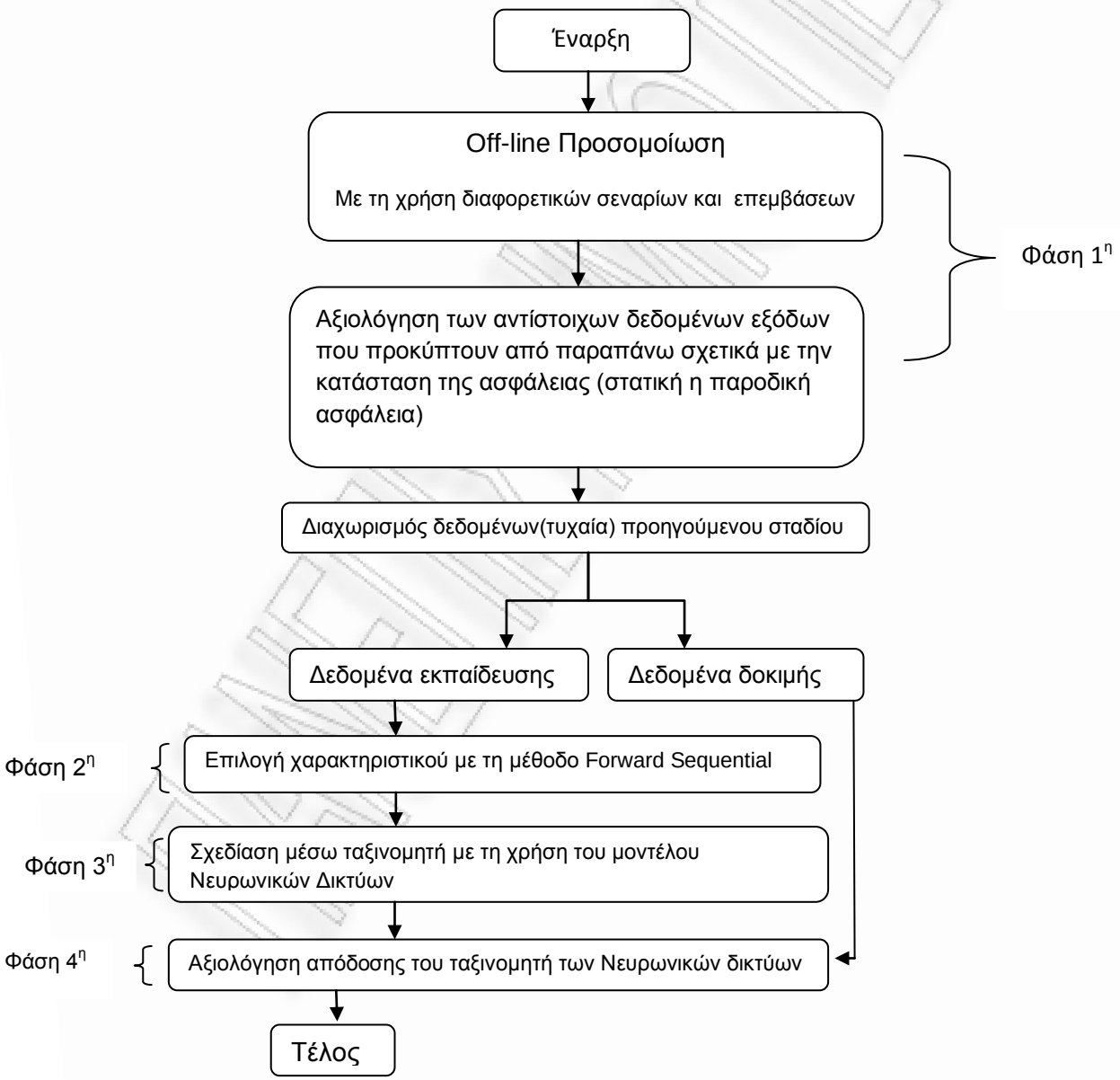
Η βασικότερη αντίληψη για το πώς μπορεί να υλοποιηθεί η προσέγγιση Αναγνώρισης Προτύπων σε θέματα αξιολόγησης ασφάλειας ενός συστήματος είναι να μειωθούν οι απαιτήσεις υπολογιστικού τύπου σε on-line τρόπους αξιολόγησης που χρησιμοποιούνταν. Αυτό μπορεί να συμβεί δίνοντας μεγαλύτερη βαρύτητα σε off-line υπολογισμούς στο σύστημα, οι οποίοι γίνονται με την δημιουργία δεδομένων «σημαδεμένων»(συγκεκριμένα δεδομένα για τα οποία θα μελετηθεί η συμπεριφορά του συστήματος και ανάλογα με αυτή θα μπορεί να γίνεται σαφές κατά πόσο το σύστημα είναι ασφαλές ή όχι) στα δεδομένα που χρησιμοποιούνται για την εκπαίδευση του συστήματος. Αν η διαχωριστική επιφάνεια μεταξύ των ξεχωριστών κλάσεων

θεωρείται λειτουργία ασφαλείας , στην ασφάλεια του συστήματος μπορεί να γίνει πρόσβαση οποιαδήποτε χρονική στιγμή.

Σχηματικά τα βήματα που ακολουθούνται στην off-line προσομοίωση παρατίθονται στο παρακάτω σχήμα, όπου χρησιμοποιούνται διαφορετικά μοντέλα Νευρωνικών Δικτύων τα οποία υποβάλλονται σε μια σειρά βημάτων(όπως είπαμε και παραπάνω). Οι φάσεις που αναφέροναι στο σχήμα είναι:

Φάση 1η: Δημιουργία δεδομένων(μεταβλητές των Προτύπων)
Φάση 2η: Επιλογή χαρακτηριστικών (μεταβλητές χαρακτηριστικών)
Φάση 3η: Σχεδίαση με Ταξινομητή (λειτουργία του ταξινομητή)
Φάση 4η: Αξιολόγηση απόδοσης ταξινομητή

Στο σχήμα παρουσιάζεται μια μικρή ανάλυση των φάσεων αυτών και οι διαφορετικές αρχιτεκτονικές των Νευρωνικών Δικτύων που χρησιμοποιούνται στις φάσεις του σχεδιασμού μέσω ταξινομητή στο σύστημα.



5.4.1. Δημιουργία δεδομένων

Η επιτυχία αυτής της προσέγγισης στηρίζεται κατά κανόνα στη χρήση των σωστών δεδομένων εκπαίδευσης του συστήματος. Τα δεδομένα πρέπει να καλύπτουν όλο το φάσμα των λειτουργιών του συστήματος. Ένας σημαντικός αριθμός χαρακτηριστικών σημείων λειτουργίας(τα λεγόμενα και πρότυπα) χρησιμοποιούνται μέσω της off-line προσομοίωσης ώστε να αξιολογηθεί η κατάσταση ασφάλειας του συστήματος σε κάθε πιθανό κίνδυνο στα πλαίσια της μελέτης. Κάθε πρότυπο σχετίζεται με κάποια συγκεκριμένα χαρακτηριστικά, πχ επίπεδο φόρτισης, τάση συστήματος, γεννήτρια ισχύος κτλ. Τα χαρακτηριστικά αυτά διαμορφώνουν τα στοιχεία ενός κλάσματος ,του κλάσματος Χ του προτύπου. Αξιολογώντας την ασφάλεια του συστήματος κάθε πρότυπο χαρακτηρίζεται ασφαλές ή όχι. Τα δεδομένα που παράγονται στην πρώτη φάση κατατάσσονται σε δεδομένα εκπαίδευσης και δοκιμής.

5.4.2. Επιλογή Χαρακτηριστικών

Η επιλογή χαρακτηριστικού μειώνει τη διάσταση των αποτελεσμάτων του πειράματος επιλέγοντας ένα υποσύνολο συγκεκριμένων στοιχείων για τη δημιουργία ενός μοντέλου. Ένα θεωρητικά «καλό» σύνολο χαρακτηριστικών καθορίζεται από την αύξηση της αποτελεσματικότητας και τη βέλτιστη ακρίβειας του ταξινομητή. Η φάση αυτή αφορά την επιλογή του βέλτιστου υποσυνόλου μεταβλητών, που αποτελεί το χαρακτηριστικό, από ένα μεγάλο σύνολο μεταβλητών προτύπου. Τα επιλεγμένα χαρακτηριστικά πρέπει να είναι ικανά να παρέχουν περισσότερες πληροφορίες για την κατασκευή του ταξινομητή σχεδίασης. Τα χαρακτηριστικά αυτά στη φάση αυτή διαμορφώνουν ένα κλάσμα, γνωστό και ως κλάσμα χαρακτηριστικών Z.

Τα χαρακτηριστικά είναι δυνατόν να επιλέγονται και από τεχνικής απόψεως. Όμως, σε τέτοιες περιπτώσεις υποκειμενικής κρίσης υπάρχει πιθανότητα απόρριψης σημαντικών μεταβλητών. Η μέθοδος που χρησιμοποιείται περισσότερο είναι η διαδοχική επιλογή χαρακτηριστικών η οποία αποτελείται από δύο στοιχεία: μια αντικειμενική συνάρτηση που ονομάζεται κριτήριο και έναν αλγόριθμο αναζήτησης. Στη μελέτη αυτή που παρατίθεται, χρησιμοποιείται η επιλογή με Sequential Forward SFS). Η μέθοδος αυτή ξεκινά με μια κενή σειρά και προσθέτει διαδοχικά μεταβλητές-χαρακτηριστικά μέχρι η προσθήκη περαιτέρω μεταβλητών να μην επηρεάζει το κριτήριο(ελαχιστοποίηση του ρυθμού ταξινόμησης).

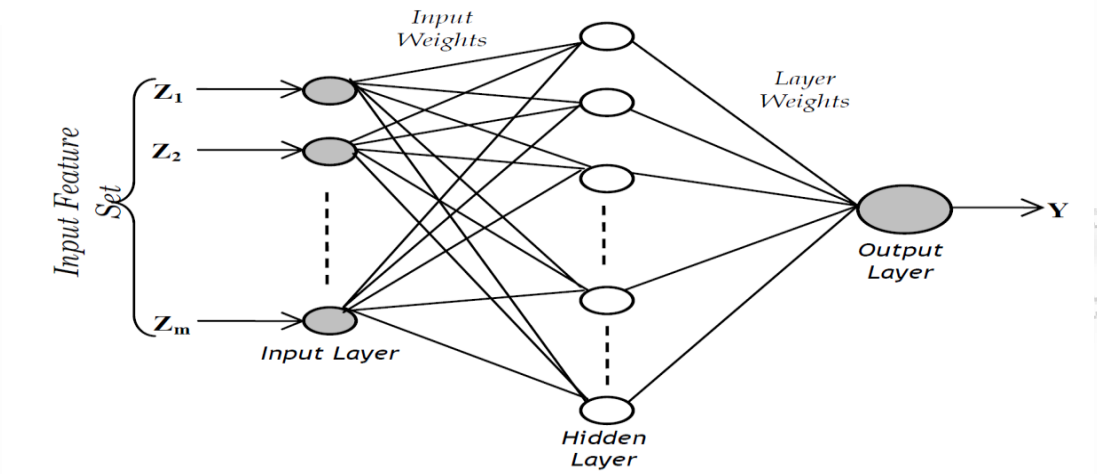
5.4.3. Σχεδίαση Ταξινομητή (Classifier Design)

Αφού έχει επιτευχθεί το στάδιο της επιλογής χαρακτηριστικού προχωράμε στο στάδιο του σχεδιασμού του κατάλληλου ταξινομητή ώστε να μπορεί να αξιολογηθεί το ζήτημα ασφάλειας που μας απασχολεί. Στη βιβλιογραφία υπάρχει πληθώρα αλγορίθμων που χρησιμοποιούνται στην σχεδίαση ταξινομητή κάποιοι από τους οποίους ανήκουν σε αλγόριθμους γραμμικού προγραμματισμού, δυναμικού προγραμματισμού κ.ά. Οι αλγόριθμοι αυτοί, παρόλο που απαιτούν λιγότερο χρόνο, δεν παρέχουν μεγάλη ακρίβεια ταξινόμησης. Όμως, από τις σημαντικότερες απαιτήσεις ύπαρξης ενός καλού ταξινομητή είναι το υψηλό επίπεδο ακρίβειας. Αυτό οδήγησε στη δημιουργία αλγορίθμων πιο αποτελεσματικών από τους προαναφερθέντες όσον αφορά τη σχεδίαση ταξινομητή. Στην καινούργια ομάδα τεχνολογιών που χρησιμοποιήθηκαν ήταν και τα Νευρωνικά Δίκτυα στο θέμα της εκπαίδευσης για την αξιολόγηση στατικής και παροδικής ασφάλειας. Τα μοντέλα νευρωνικών δικτύων που χρησιμοποιούνται περισσότερο είναι MLP(Multilayer Perceptron), LVQ(Learning Vector Quantization), PNN (Probabilistic Neural Network), ARTMAP (Adaptive Resonance Theory Mapping).

5.4.3.1. MLP (Multilayer Perceptron)

Μιλώντας για γραμμικό ταξινομητή, το perceptron είναι το πιο απλό δίκτυο το οποίο έχει ένα (ενιαίο) επίπεδο. Η μεγαλύτερη αδυναμία του είναι ότι μπορεί να λύσει αποκλειστικά προβλήματα γραμμικού τύπου. Όμως, τα μεγαλύτερα προβλήματα που προκύπτουν αφορούν μη γραμμικά συστήματα. Το MLP είναι ένα feedforward μοντέλο όπου σύνολα χαρτών δεδομένων εισόδου είναι «ταιριασμένα» με αντίστοιχα σύνολα δεδομένων εξόδου. Πρόκειται για μια τροποποίηση του γραμμικού μοντέλου perceptron που χρησιμοποιεί τρία ή και περισσότερα επίπεδα-νευρώνες(κόμβους του δικτύου) με μη-γραμμικές συναρτήσεις ενεργοποίησης. Έτσι, είναι πιο ελπιδοφόρο από το αρχικό μοντέλο perceptron αφού μπορεί να διαχωρίζει δεδομένα που είναι μη-γραμμικά διαχωρίσιμα.

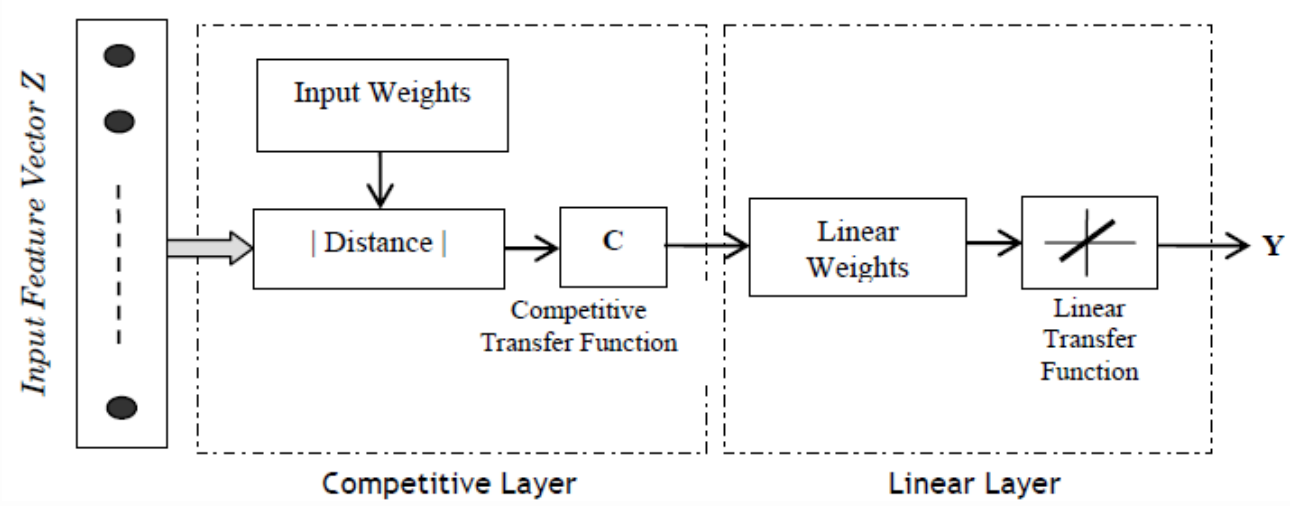
Η δομή ενός MLP φαίνεται στο παρακάτω σχήμα:



Το δίκτυο αποτελείται από ένα επίπεδο εισόδου(input layer) και ένα εξόδου(output layer) με ένα κρυφό επίπεδο(hidden layer) μη-γραμμικών κόμβους ενεργοποίησης. Κάθε κόμβος κάθε επιπέδου συνδέεται με ορισμένο βάρος σε κάθε άλλο κόμβο ή επίπεδο. Ο αριθμός των νευρώνων (κόμβων) στο επίπεδο εισόδου είναι ίδιος με τον αριθμό των χαρακτηριστικών εισόδου και ο αριθμός των νευρώνων στο κρυφό επίπεδο επιλέγεται ως 30 με την «υπερβολική εφαπτομένη σιγμοειδή». Το δίκτυο είναι εκπαιδευμένο με τον αλγόριθμο ‘Levenberg- Marquardt”.

5.4.3.2. LVQ (Learning Vector Quantization)

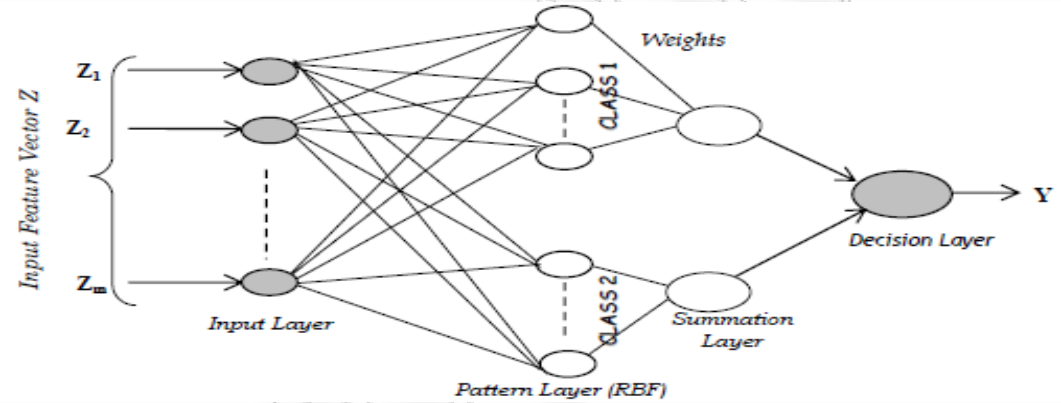
Πολλές δομές Νευρωνικών Δικτύων εμπεριέχουν ένα επίπεδο ανταγωνισμού ώστε να αναγνωρίζουν τις ομάδες παρόμοιων διανυσμάτων εισόδου. Το LVQ είναι μια μέθοδος εκπαίδευσης των νευρώνων του επιπέδου ανταγωνισμού. Η εκπαίδευση αυτή στηρίζεται σε έναν supervised αλγόριθμο ταξινόμησης. Η δομή του LVQ που χρησιμοποιείται στην περίπτωση που μελετάμε φαίνεται στο σχήμα:



Αποτελείται από ένα επίπεδο ανταγωνισμού(Competitive Layer) ακολουθούμενο από ένα γραμμικό επίπεδο(Lineal Layer). Το πρώτο μαθαίνει πώς να κατατάσσει τα διανύσματα εισόδου και το δεύτερο μεταμορφώνει τις προηγούμενες κατατάξεις σε ταξινομήσεις-στόχους καθοριζόμενους από το χρήστη.

5.4.3.3. PNN (Probabilistic Neural Network)

Το PNN είναι ένα είδος MLP που χρησιμοποιείται στον τομέα της ταξινόμησης ως πρότυπο. Είναι ένα μη-γραμμικό, χωρίς παραμέτρους πρότυπο αναγνώρισης αλγορίθμων που λειτουργεί όταν οριστεί η συνάρτηση πυκνότητας πιθανότητας για κάθε μία από τις ομάδες δεδομένων που βασίζονται στις παραμέτρους κατάρτισης και βελτιστοποίησης βάρους του πυρήνα του δικτύου. Σχηματικά η δομή του μοιάζει πολύ με αυτή του MLP όπως φαίνεται παρακάτω:



Η RBF (Radial Basis Function) χρησιμοποιείται ως συνάρτηση ενεργοποίησης του κρυφού επιπέδου.

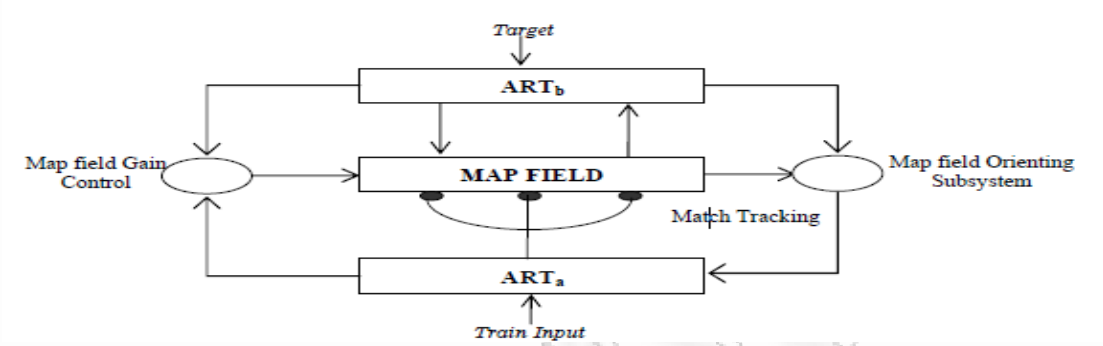
Το επίπεδο εισόδου έχει ένα νευρώνα για κάθε μεταβαλλόμενο χαρακτηριστικό. Το κρυφό επίπεδο αποτελείται από ένα νευρώνα για κάθε σύνολο δεδομένων κατάρτισης. Οι κρυφοί νευρώνες αποθηκεύουν τις τιμές των μεταβλητών και των ταξινομήσεων-στόχων. Το επίπεδο σύνοψης (summation) έχει ένα νευρώνα για κάθε κατηγορία μεταβλητών-στόχων. Οι νευρώνες υπολογίζουν το βάρος της κάθε κατηγορίας. Το επίπεδο απόφασης (decision) υπολογίζει το βάρος του επιπέδου σύνοψης και χρησιμοποιεί την μεγαλύτερη τιμή για να προβλέψει την κατηγορία- στόχο (Y).

5.4.3.4. ARTMAP (Adaptive Resonance Theory Mapping)

Το ART είναι ένα μοντέλο νευρωνικού δικτύου που χρησιμοποιεί μέθοδο επιβλεπόμενης κατάρτισης και αντιμετωπίζει θέματα όπως η αναγνώριση προτύπων και προβλέψεων. Το ARTMAP είναι «προφητικό» ART ικανό να

εκπαιδεύεται αναγνωρίζοντας τα on-line δεδομένα που λαμβάνει. Τα συστήματα ARTMAP αποτελούνται από δύο ART μοντέλα(ARTa, ARTb) συνδεδεμένα μεταξύ τους με μία μνήμη. Η μονάδα ARTa λαμβάνει τα δεδομένα εισόδου και η ARTb τα διορθωμένα δεδομένα- στόχους και πραγματοποιεί τη μικρότερη δυνατή προσαρμογή της παραμέτρου επαγρύπνησης στην πρώτη μονάδα έτσι ώστε να γίνει σωστή ταξινόμηση.

Σχηματικά η δομή ενός ARTMAP:



5.4.4. Αποτελέσματα έρευνας

Για να ελεγχθεί η απόδοση των διαφορετικών μοντέλων Νευρωνικών Δικτύων στην Αξιολόγηση Ασφάλειας έγινε προσομοίωση ανάλογη κανονικής λειτουργίας συστήματος παραγωγής ενέργειας. Τα δεδομένα που απαιτούνταν για τις φάσεις εκπαίδευσης και δοκιμής δημιουργούνται από Off-line προσομοιώσεις με προγράμματα που αναπτύσσονται με τη χρήση του Matlab. Έχουν θεωρηθεί διαφορετικά σενάρια ώστε να γίνει κατανοητή και εμφανής η βέλτιστη λειτουργία.

5.4.4.1. Αποτελέσματα αξιολόγησης στατικής ασφάλειας

Στην αξιολόγηση στατικής ασφάλειας(Static Security Assessment-SSA), γίνονται ανεξάρτητες προσομοιώσεις για κάθε ενδεχόμενο. Για μια δεδομένη κατάσταση και υπό συγκεκριμένο τύπο σφάλματος χρησιμοποιείται η μέθοδος Fast Decoupled Load Flow όταν υπάρχει κρίσιμο θέμα στην ροή φορτίου. Έτσι επιτυγχάνεται αποσύνδεση, εφόσον αυτό απαιτείται. Η κατάσταση της στατικής ασφάλειας(αν δηλαδή, είναι το σύστημα ασφαλές ή όχι) ορίζεται από την αξιολόγηση των περιορισμών ασφαλείας που γίνονται στο σύστημα οι οποίοι δίνονται από τις εξισώσεις που έχουμε αναφέρει και παραπάνω. Ένα βέλτιστο υποσύνολο πρωτοτύπων είναι το «διάνυσμα χαρακτηριστικών» το οποίο αναγνωρίζεται από τη μέθοδο επιλογής χαρακτηριστικού SFS.

Τα αποτελέσματα της κατάταξης διάφορων ταξινομητών μέσω Νευρωνικών Δικτύων δείχνουν ότι η PNN και η ARTMAP παρέχουν μεγάλη ακρίβεια στην ταξινόμηση και μικρότερο ποσοστό εσφαλμένης ταξινόμησης

συγκριτικά με τα άλλα μοντέλα νευρωνικών δικτύων. Ο ταξινομητής PNN μπορεί να ταξινομεί δείγματα τα οποία δεν έχει ξανασυναντήσει με μεγάλη ακρίβεια. Από την πλευρά τους ένας ARTMAP ταξινομητής (όπως και ένας PNN) δίνει πολύ μικρό ποσοστό εσφαλμένης απόρριψης(τείνει στο μηδέν). Επομένως και οι 2 δομές είναι άκρως ικανές έως και κατάλληλες για την εφαρμογή τους σε On-line συστήματα. Αυτό δίνει το προβάδισμα στις δομές αυτές των Νευρωνικών δικτύων όσον αφορά την ταξινόμηση και την στατική ασφάλεια ενός συστήματος παραγωγής ηλεκτρικής ενέργειας.

5.4.4.2. Αποτελέσματα αξιολόγησης παροδικής ασφάλειας

Η διαδικασία της αξιολόγησης της παροδικής ασφάλειας, λαμβάνεται υπόψιν όλα τα σενάρια που έχουν χρησιμοποιηθεί και στην αξιολόγηση της στατικής ασφάλειας γιατί το πρώτο πράγμα που ορίζεται με την έναρξη του προγράμματος ροής φορτίου είναι η κατάσταση της στατικής ασφάλειας. Τα σενάρια στα οποία το σύστημα κρίθηκε ανασφαλές απορρίπτονται άμεσα ενώ για κάθε περίπτωση που έχει κριθεί το σύστημα ασφαλές γίνεται ανάλυση της παροδικής του ασφάλειας πραγματοποιώντας προσομοίωση πιθανών αδυναμιών της παροδικής ασφάλειας. Τα σφάλματα(για τη δοκιμή) τοποθετούνται τη χρονική στιγμή 0 και αποσύρονται όταν θεωρείται ότι έχουν ληφθεί τα απαραίτητα αποτελέσματα.

Η συνάρτηση ταξινόμησης είναι σχεδιασμένη με βάση τα δεδομένα κατάρτισης του διανύσματος χαρακτηριστικών. Οι ταξινομητές PNN και ARTMAP φέρουν καλύτερα αποτελέσματα(όπως είδαμε και στην στατική ασφάλεια). Επιπλέον, ο χρόνος που απαιτείται για την ταξινόμηση με τη χρήση των δύο αυτών δομών, είναι απόλυτα αποδεκτός από το σύστημα καθώς επιτρέπει την on-line καταγραφή της ασφάλειας του συστήματος.

5.5. Συνοψίζοντας…

Το σύστημα ασφαλείας που αναπτύχθηκε βασισμένο στα Νευρωνικά Δίκτυα αποτελείται από ταξινομητές (οι οποίοι βασίζονται σε δομές των Νευρωνικών Δικτύων) και επιτρέπουν την On-line εφαρμογή τους. Αυτό δίνει τη δυνατότητα στο διαχειριστή του συστήματος να κάνει καταγραφή της κατάστασης ασφάλειας προειδοποιώντας όταν το σύστημα βρίσκεται σε δυσμενή και σοβαρή κατάσταση.

Η εφαρμογή της αναγνώρισης προτύπων στην ταξινόμηση του διανύσματος χαρακτηριστικών παίζει βασικό παράγοντα όπως είδαμε στο κεφάλαιο αυτό, στη διατήρηση της ασφάλειας ενός συστήματος παραγωγής ηλεκτρικής ενέργειας. Ο ταξινομητής στο σύστημα αναγνώρισης προτύπων βασίζεται σε διαφορετικές δομές Νευρωνικών Δικτύων. Τα αποτελέσματα των προσομοιώσεων δείχνουν ότι είναι καλύτερα τα αποτελέσματα όταν χρησιμοποιούνται οι PNN και ARTMAP ταξινομητές. Η χρήση των ταξινομητών αυτών επιτρέπει την real time παρακολούθηση του συστήματος, άρα μπορούν να χρησιμοποιηθούν και σε πρακτικό επίπεδο πέραν του θεωρητικού.

Κεφάλαιο 6^{ο}: Καθορισμός Βέλτιστης Εφαρμογής

6.1. Εισαγωγή

Στο παρόν κεφάλαιο θα γίνει μια μικρή σύνοψη του τι είδαμε μέχρι στιγμής στις έρευνες που μελετήθηκαν. Έπειτα θα κριθεί ποια θα είναι και η βέλτιστη εφαρμογή των Νευρωνικών Δικτύων όσον αφορά την εξασφάλιση της ασφάλειας ενός συστήματος, ανάλογα πάντα με την περίπτωση.

Σημαντικό ρόλο έχει το σύστημα που μελετάται. Έχει μεγάλη απόκλιση η επιλογή της εφαρμογής σε ένα σύστημα παραγωγής εργοστασίου για παράδειγμα και ενός δικτύου κατοχύρωσης δεδομένων και ενδοεπικοινωνίας μιας εταιρείας. Αυτό βέβαια θα αναλυθεί περαιτέρω στη συνέχεια.

6.2. Νευρωνικά Δίκτυα vs Έμπειρα Συστήματα

Τα έμπειρα συστήματα σε περιπτώσεις που έχουν χρησιμοποιηθεί για την ασφάλεια κάποιου συστήματος δεν ήταν όσο αποδοτικά περίμεναν οι μελετητές. Αφενός η διαχείρισή του ήταν ιδιαίτερα περίπλοκη και αφετέρου (και θεωρητικά το μεγαλύτερο μειονέκτημά τους) υπήρχε μεγάλο ποσοστό λανθασμένων συναγερμών. Αυτό σαφώς και ήταν σημαντικός παράγοντας καθώς δεν δύναται το σύστημα να «παγώνει» χωρίς να υπάρχει σοβαρός λόγος. Μην ξεχνάμε ότι σε περιπτώσεις επιχειρήσεων το κόστος ήταν μεγάλο όσο προέκυπταν λανθασμένοι συναγερμοί.

Από την άλλη τα Νευρωνικά Δίκτυα υπερτερούσαν λόγω της ευελιξίας τους (διότι ένα νευρωνικό δίκτυο έχει την ικανότητα να αναλύσει ακόμα και παραμορφωμένη ή και κατεστραμμένη πληροφορία αλλά και με μη-γραμμικό τρόπο-σημαντικός παράγοντας για πολλαπλές επιθέσεις), λόγω της ταχύτητάς τους, λόγω της δυνατότητας πρόβλεψης επίθεσης (δεδομένου ότι ένα νευρωνικό δίκτυο δεν παύει ποτέ να εκπαιδεύεται αλλά αντιθέτως μαθαίνει από τις εμπειρίες του, η ικανότητά του να καταλάβει αν επίκειται κάποια επίθεση βελτιώνεται συνεχώς) και τέλος λόγω της εκπαίδευσής τους (ένα νευρωνικό δίκτυο μπορεί να εκπαιδευτεί να αναγνωρίζει με μεγάλη ακρίβεια γνωστές περιπτώσεις που ίσως αποτελούν κίνδυνο για το σύστημα. Ακριβώς λοιπόν επειδή οι επιτιθέμενοι μιμούνται τους τρόπους επίθεσης

άλλων που έχουν διεξαχθεί με επιτυχία, το δίκτυο θα αναγνωρίσει και αυτές τις επιθέσεις καθώς «ξαναβλέπει» βασικά χαρακτηριστικά που έχουν αποτελέσει επίθεση στο παρελθόν).

Βέβαια υπάρχουν και μειονεκτήματα στη μέθοδο. Το βασικότερο μειονέκτημά του είναι το ίδιο με το πιο σημαντικό, ίσως, πλεονέκτημά του : την εκπαίδευση του. Η ανάγκη για σωστή και ακριβή εκπαίδευση γεννά και προβλήματα σε περιπτώσεις που η κατάρτιση του νευρωνικού δικτύου δεν έχει γίνει υπό την καταλληλότερη μέθοδο για την εκάστοτε περίπτωση. Μπορεί για την εκπαίδευση να απαιτούνται άπειρες ατομικές επιθέσεις στη σειρά κάτι το οποίο είναι δύσκολο να συμβεί καθώς τέτοια ποσότητα αυτών των ευαίσθητων πληροφοριών είναι δύσκολο να αποκτηθεί.

Το επόμενο μειονέκτημα είναι το πρόβλημα του Μαύρου Κουτιού. Κάθε νευρωνικό δίκτυο έχει διαφορετική συμπεριφορά ανάλογα με την εκπαίδευση που γίνεται σε κάθε περίπτωση. Όταν το ποσοστό επιτυχίας για τον προσδιορισμό συμβάντων στο δίκτυο φτάσει σε κάποιο επιθυμητό επίπεδο τα βάρη των συνδέσεων κάποιων κόμβων «παγώνουν». Βέβαια με την ανάλυση που έχει γίνει μέχρι αυτό τη στιγμή καλύπτει κάποια πιθανότητα επιτυχίας δεν μπορεί κανείς να γνωρίζει με απόλυτη ακρίβεια. Αυτό είναι το πρόβλημα του «Μαύρου Κουτιού» και αφορά οποιαδήποτε χρήση των νευρωνικών δικτύων.

6.3. Συνύπαρξη Έμπειρων Συστημάτων και Νευρωνικών Δικτύων

Όπως, λοιπόν, είναι φανερό ούτε τα Έμπειρα Συστήματα αλλά ούτε και τα Νευρωνικά Δίκτυα από μόνα τους θα μπορούσαν να προσφέρουν ασφάλεια σε ένα σύστημα ή/και δίκτυο με μεγάλη ακρίβεια. Σε κάθε περίπτωση θα πρέπει να καταπολεμηθούν κατά βάσει τα εξής δύο:

- η μεγάλη συχνότητα των λανθασμένων συναγερμών των Έμπειρων Συστημάτων και
- το πρόβλημα του «Μαύρου Κουτιού» των Νευρωνικών Δικτύων.

Η βέλτιστη λύση που θα μπορούσαμε να προτείνουμε είναι η ενσωμάτωση Νευρωνικών Δικτύων και Έμπειρων Συστημάτων. Σε αυτή την περίπτωση και τα δύο προβλήματα που προαναφέρθηκαν θα καταπολεμηθούν. Αφενός η ανίχνευση επίθεσης θα είναι πιο αποτελεσματική και οι λανθασμένοι συναγερμοί θα είναι σαφώς λιγότεροι εφόσον το νευρωνικό δίκτυο θα είναι αυτό που θα καθορίζει την πιθανότητα επίθεσης. Αφετέρου το πρόβλημα του

«Μαύρου Κουτιού» παύει να απασχολεί καθώς το έμπειρο σύστημα δεν επιτρέπει να μην γίνει έλεγχος σε όλα τα δεδομένα. Επομένως, με την προσέγγιση αυτή έχουμε τη βέλτιστη δυνατή ασφάλεια και χωρίς να μεταλαμπαδεύονται τα μειονεκτήματα του κάθε συστήματος στο συνονθύλευμα και των δύο.

Βέβαια υπάρχει και σε αυτή την προσέγγιση κάποιο μειονέκτημα στην πράξη (όπως γίνεται και σε κάθε περίπτωση). Το θέμα είναι ότι από τη στιγμή που έχει γίνει η εκπαίδευση του Νευρωνικού δικτύου με τρόπο τέτοιο ώστε να μπορεί να αναγνωρίσει νέες επιθέσεις, το έμπειρο σύστημα πρέπει να ενημερώνεται με αντίστοιχο update συνεχώς ώστε να είναι και αυτό σε θέση να αναγνωρίσει τις ίδιες απειλές. Αν αυτό δεν γίνεται, οι απειλές που έχουν αναγνωριστεί από το Νευρωνικό Δίκτυο του συστήματος όταν θα περνούν από φιλτράρισμα στο Έμπειρο Σύστημα αυτό πιθανότατα να τις παρακάμπτει και να μην τις αναγνωρίζει.

Όσον αφορά συστήματα εταιρειών προτεινόμενη λύση είναι το «πάντρεμα» των Νευρωνικών Δικτύων μα τα Έμπειρα Συστήματα. Προσφέρουν την μεγαλύτερη ασφάλεια από άλλες μεθόδους που χρησιμοποιούνται και οι συγκεκριμένες του ιδιαιτερότητες τους δίνουν το πλεονέκτημα ότι μπορούν να προσφέρουν ασφάλεια παρόλο που οι απαιτήσεις και οι κίνδυνοι μεγαλώνουν με τα χρόνια.

6.4. Νευρωνικά Δίκτυα σε Γραμμές Παραγωγής Εργοστασίων

Στο κεφάλαιο 5 αναλύθηκαν κάποια πράγματα που ίσως να είναι φαινομενικά άσχετα με αυτό που μελετάμε. Όμως, η ευρύτερη ανάπτυξη των δομών των Νευρωνικών Δικτύων και το πώς χρησιμοποιούνται στη διασφάλιση της ασφάλειας μας δίνει μια μεγαλύτερη ιδέα για το φάσμα που καταλαμβάνουν τα Νευρωνικά Δίκτυα στο θέμα μας. Σε περιπτώσεις λοιπόν παραγωγής προϊόντων(οποιουδήποτε είδους) μας ενδιαφέρει αν το σύστημα είναι ασφαλές ή όχι ώστε να συνεχίζει η παραγωγή και μην υπάρχει κόστος στο εργοστάσιο. Η προσέγγιση λοιπόν που αναφέραμε είναι η πλέον κατάλληλη σε αυτές τις περιπτώσεις. υπενθυμίζουμε πως οι δομές που χρησιμοποιούνται είναι η PNN και η ARTMAP.

6.5. Συνοψη

Στο κεφάλαιο αυτό αναφέρονται οι βέλτιστες λύσεις από τις μελέτες και τις προσεγγίσεις που έχουμε δει μέχρι στιγμής και αιτιολογείται η επιλογή τους. Στα αντίστοιχα κεφάλαια που αναφέρονται γίνεται εκτενέστερη περιγραφή τους. Για το λόγο αυτό στο σημείο αυτό οι προσεγγίσεις αναφέρονται, καθώς και σημεία εφαρμογών αυτών αλλά δεν επαναλαμβανόμαστε με εμβάθυνση στην προσέγγιση. Άλλες προσεγγίσεις και μελέτες που δεν έχουν αναφερθεί ίσως να έχουν πιο σημαντικά μειονεκτήματα ή μεγαλύτερο κόστος ή να μην είναι καθολικά αποδεκτές, όπως οι προτεινόμενες.

ΠΑΡΑΡΤΗΜΑ

ΕΜΠΕΙΡΟ ΣΥΣΤΗΜΑ(expert system) : σύστημα που συντελεί στην επίλυση προβλημάτων σε συγκεκριμένο τομέα ή περιοχή εφαρμογής με συναγωγές από μια βάση γνώσεων αναπτυγμένη από την ανθρώπινη εμπειρογνωσία. Εφαρμόζουν προγραμματισμένες ρουτίνες λογικής, σχεδιασμένες αποκλειστικά για μία συγκεκριμένη εργασία, προκειμένου να εξαχθεί κάποιο συμπέρασμα. Για το σκοπό αυτό, διεξάγεται επεξεργασία μεγάλων ποσοτήτων γνωστών πληροφοριών. Εντάσσεται στα συστήματα Τεχνητής Νοημοσύνης και το εύρος ων εφαρμογών του είναι ιδιαίτερα μεγάλο.

ΑΥΤΟΝΟΜΑ ΣΥΣΤΗΜΑΤΑ(autonomous system): σύστημα, δίκτυο ή σύνολα δικτύων υπό έναν ενιαίο έλεγχο συγκεκριμένου admin. Θα μπορούσε να είναι το σύνολο των υπολογιστών ενός πανεπιστημίου ή μιας εταιρείας. Στη βιβλιογραφία αναφέρεται συχνά χάριν συντομίας ως AS.

ΣΥΣΤΗΜΑΤΑ ΠΑΡΑΓΩΓΗΣ ΗΛΕΚΤΡΙΚΗΣ ΕΝΕΡΓΕΙΑΣ (electric power system: δίκτυο συστημάτων-εξαρτημάτων που χρησιμοποιούνται στην παροχή, μετάδοση και χρήση την παραγόμενης από το σύστημα ηλεκτρικής ενέργειας. Τα απλούστερα αυτών είναι τα αυτόνομα συστήματα φωτοβολταϊκών.

ΠΗΓΕΣ

[1] ΝΕΥΡΩΝΙΚΟ ΔΙΚΤΥΟ-ΒΙΚΙΠΑΙΔΕΙΑ (http://el.wikipedia.org/wiki/%CE%9D%CE%B5%CF%85%CF%81%CF%89%CE%BD%CE%B9%CE%BA%CF%8C_%CE%B4%CE%AF%CE%BA%CF%84%CF%85%CE%BF)

[2] ΓΕΝΙΚΑ ΠΕΡΙ ΝΕΥΡΩΝΙΚΩΝ ΔΙΚΤΥΩΝ (http://egnatia.ee.auth.gr/~imatz/ann_chapter1.html)

[3] Σ. Κάτσικας, Δ. Γκρίτζαλης, Σ. Γκρίτζαλης- Ασφάλεια Πληροφοριακών Συστημάτων

[4] James Cannady – Artificial Neural Networks for Misuse Detection (http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.39.5179&rep=rep1&type=pdf)

[5] Jean- Philippe Planquart – Application of Neural Networks in Intrusion Detection

[6] Anil Naik – Artificial Neural Network for Home Security System (http://www.yuvaengineers.com/?p=681)

[7] N. Kussul, A. Shelestov, A. Sidorenko, V. Pasechnik,S. Skakun, Y.Veremeyenko, N. Levchenko – Multi-Agent Security System Based on Neural Network Models of User's Behavior

[8] S. KALYANI, K. SHANTI SWARUP – Neural Network Models for Security Assessment in Electric Power Systems