Πανεπιστήμιο Δυτικής Μακεδονίας
Πολυτεχνική Σχολή
Τμήμα Μηχανικών Πληροφορικής και Τηλεπικοινωνιών

Υλοποίηση Συστήματος Ανίχνευσης Εισβολών σε Περιβάλλον Android για Ασύρματα Δίκτυα Πρόσβασης

Ράδογλου Γραμματίκης Παναγιώτης

Επιβλέπων Καθηγητής: Δρ. Παναγιώτης Σαρηγιαννίδης

Κοζάνη, Νοέμβριος 2016

Σύνοψη Παρουσίασης

- Εισαγωγή
- Συστήματα Ανίχνευσης Εισβολών
- Αρχιτεκτονική
- Μοντέλα Εισβολών
- Επιβλεπόμενη Μηχανική Μάθηση
- Τεχνητά Νευρωνικά Δίκτυα
- Διαδικασία Εκπαίδευσης ΤΝΔ
- Λειτουργίες Εφαρμογής
- Ανάλυση Δικτυακής Κίνησης
- Στιγμιότυπα Ανάλυσης Δικτυακής Κίνησης
- Αμφίδρομες Δικτυακές Ροές
- Ανίχνευση Εισβολών
- Εξαγωγή Δικτυακών Ροών
- Επεξεργασία Δικτυακών Ροών
- Εκπαίδευση ΤΝΔ
- Αξιολόγηση ΤΝΔ
- Στιγμιότυπα Ανίχνευσης Εισβολών
- Συμπεράσματα – Μελλοντικές Επεκτάσεις

Εισαγωγή

- Η εξέλιξη της τεχνολογίας έχει ως αρνητικό παράγοντα την ταυτόχρονη ανάπτυξη κακόβουλων λογισμικών.
- Ανάγκη ανάπτυξης νέων τεχνικών προστασίας, ικανών να προβλέπουν άγνωστες πιθανές απειλές.
- Τα συστήματα ανίχνευσης εισβολών αποτελούν μηχανισμούς, οι οποίοι ενισχύουν σημαντικά την ασφάλεια ενός συστήματος, ωστόσο η έρευνα για την προσαρμογή τους στις κινητές συσκευές είναι περιορισμένη.

Συστήματα Ανίχνευσης Εισβολών

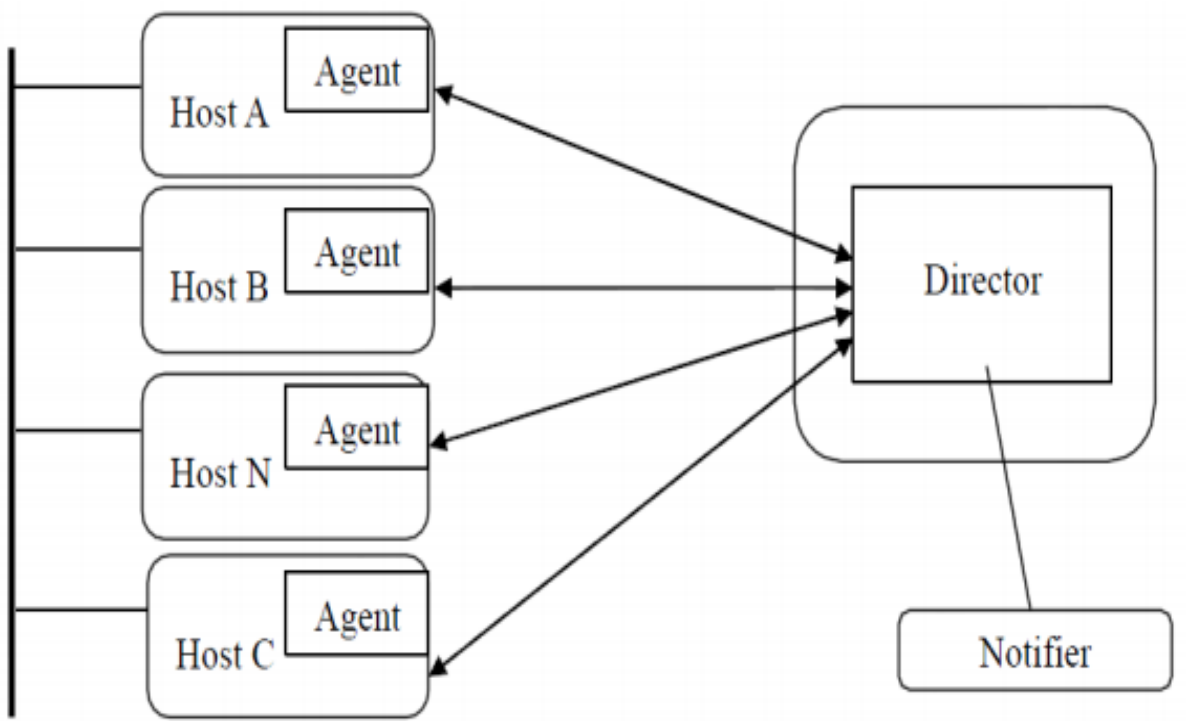
Σκοπός: Παρακολούθηση της συνολικής κατάστασης ενός ή πολλαπλών συστημάτων με στόχο την ανίχνευση απειλητικών ενεργειών.

Κύρια χαρακτηριστικά:

- Αναγνώριση μεγάλου εύρους εισβολών.
- Έγκαιρη ανίχνευση εισβολών.
- Υψηλή ακρίβεια.
- Εύχρηστη διεπαφή χρήστη.

Αρχιτεκτονική

- **Αντιπρόσωπος** (Agent)
- **Διευθυντής** (Director)
- **Αγγελιοφόρος** (Notifier)



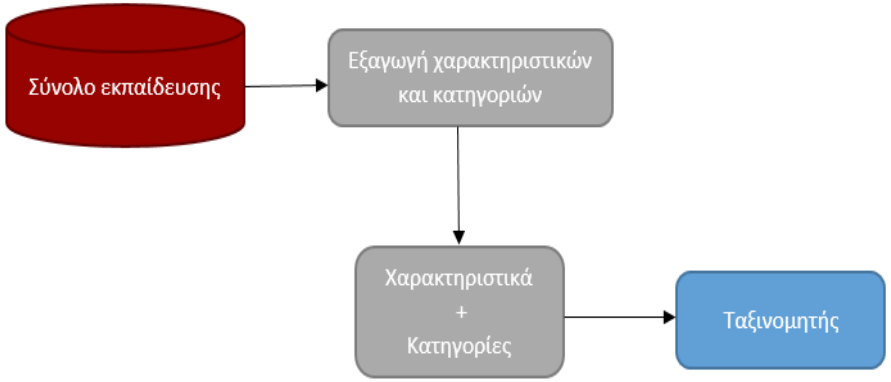
Δομή συστήματος ανίχνευσης εισβολών.

Μοντέλα Εισβολών

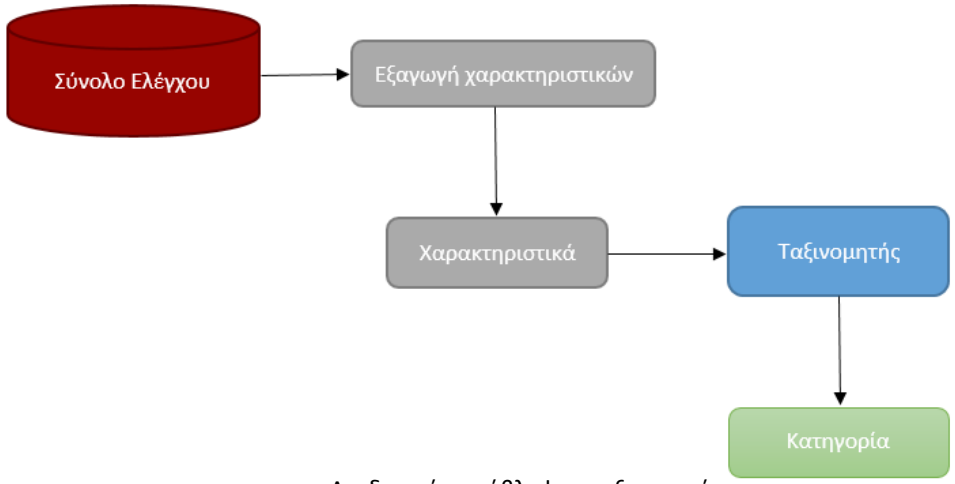
- Μοντέλα κακής συμπεριφοράς
- Μοντέλα ανίχνευσης διαταραχών
- Μοντέλα ανίχνευσης διαταραχών πρωτοκόλλων

Επιβλεπόμενη Μηχανική Μάθηση

Ταξινόμηση: Εκπαίδευση ενός αλγορίθμου με ένα προκαθορισμένο σύνολο δεδομένων, στόχος του οποίου αποτελεί η πρόβλεψη των κατηγοριών ενός άγνωστου συνόλου αντικειμένων.

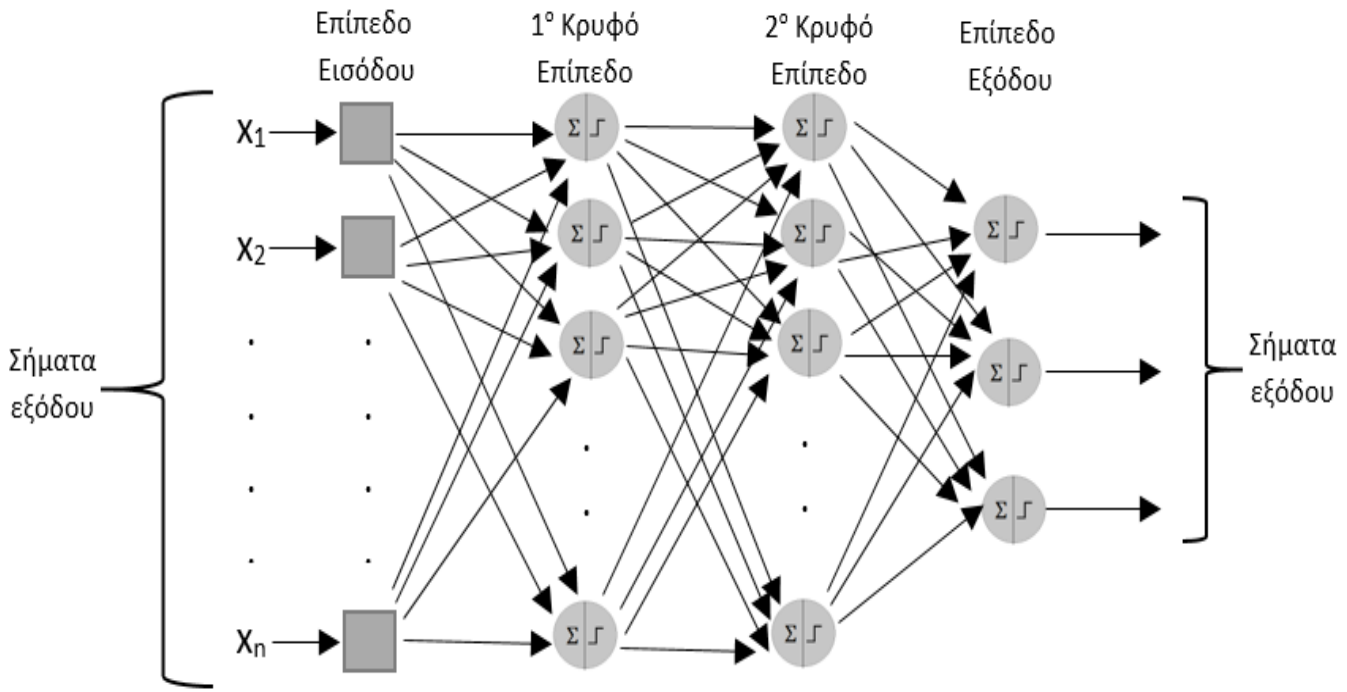


Διαδικασία εκπαίδευσης ταξινομητή.



Διαδικασία πρόβλεψης ταξινομητή.

Τεχνητά Νευρωνικά Δίκτυα (ΤΝΔ)



ΤΝΔ πολλαπλών επιπέδων.

Διαδικασία Εκπαίδευσης ΤΝΔ

- Καθορισμός των βαρών, όλων των νευρώνων, όλων των κρυφών επιπέδων και του επιπέδου εξόδου, ώστε τα υπό εξέταση αντικείμενα να ταξινομούνται με υψηλό ποσοστό ακρίβειας.
- Στόχος των περισσότερων αλγορίθμων εκπαίδευσης είναι η ελαχιστοποίηση της συνάρτησης τετραγωνικού σφάλματος:

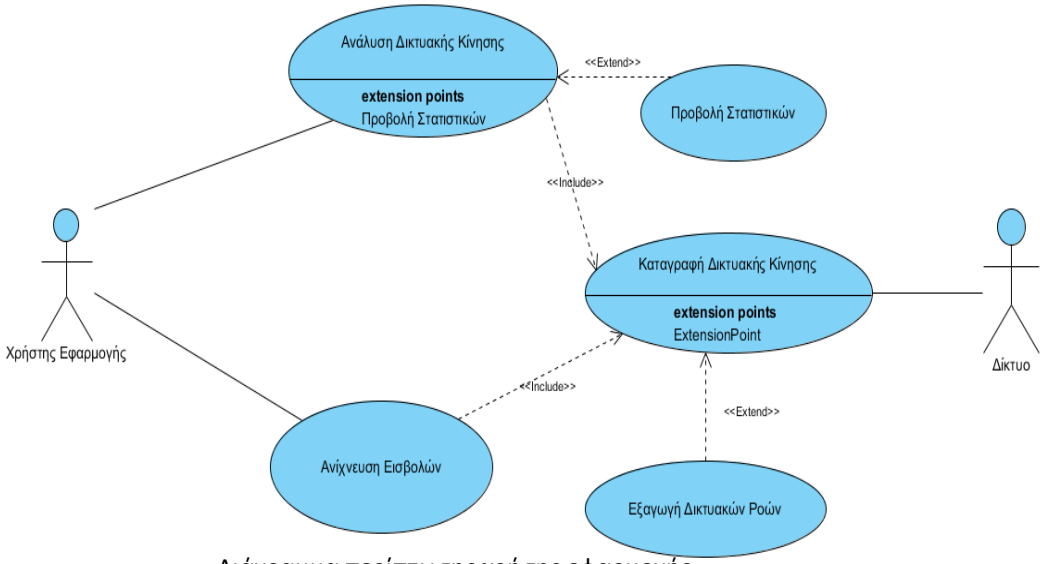
$$\mathrm{E(w)} = \frac{1}{2}\sum_{i=1}^{N}(t_i - y_i)^2$$

Όπου:

t: Η έξοδος του συνόλου εκπαίδευσης.
y: Η έξοδος που υπολόγισε το μοντέλο.

Λειτουργίες Εφαρμογής

- Ανάλυση της δικτυακής κίνησης
- Ανίχνευση εισβολών



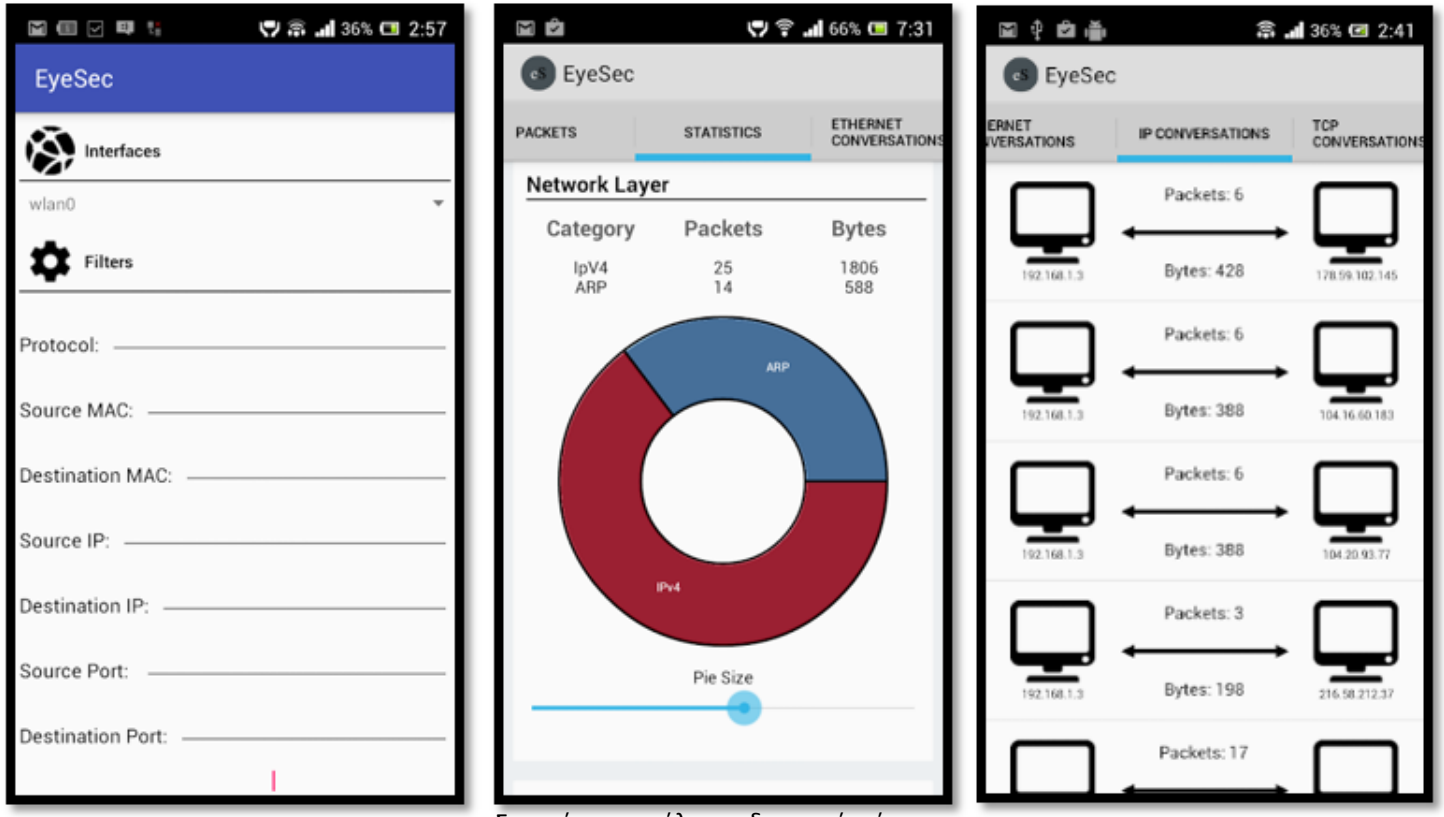
Διάγραμμα περίπτωσης χρήσης εφαρμογής.

Βασικές λειτουργίες εφαρμογής.

Ανάλυση Δικτυακής Κίνησης

- Καταγραφή της δικτυακής κίνησης (Scapy).
- Ανάλυση της δικτυακής κίνησης (Scapy).
- Εμφάνιση των πακέτων που καταγράφηκαν.
- Εμφάνιση πληροφοριών ανά επίπεδο της στοίβας TCP/IP.
- Δεκαεξαδική αναπαράσταση των πακέτων.
- Παρουσίαση στατιστικών στοιχείων ανά επίπεδο της στοίβας TCP/IP.
- Εμφάνιση των Ethernet, IP, TCP και UDP επικοινωνιών.

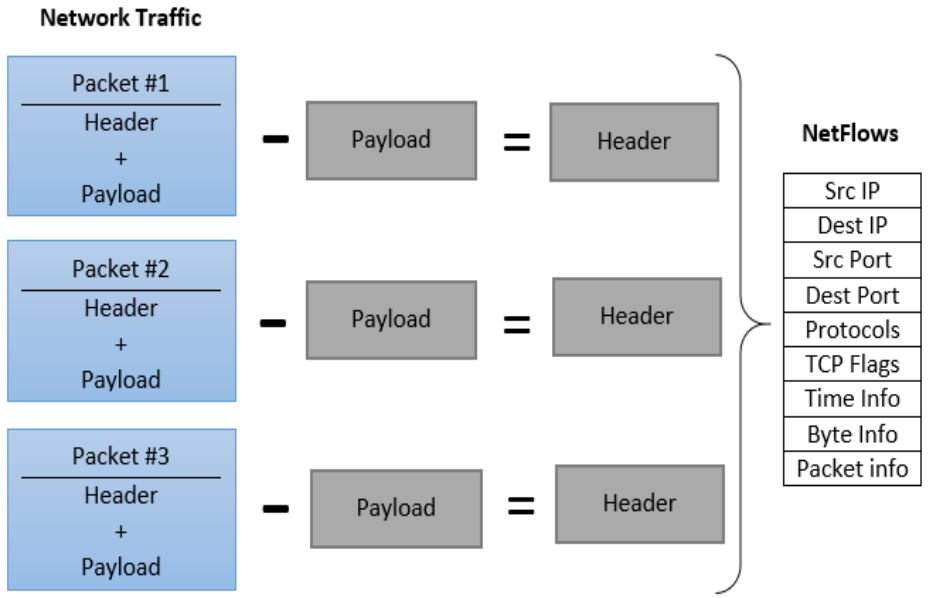
Στιγμιότυπα Ανάλυσης Δικτυακής Κίνησης



Στιγμιότυπα ανάλυσης δικτυακής κίνησης.

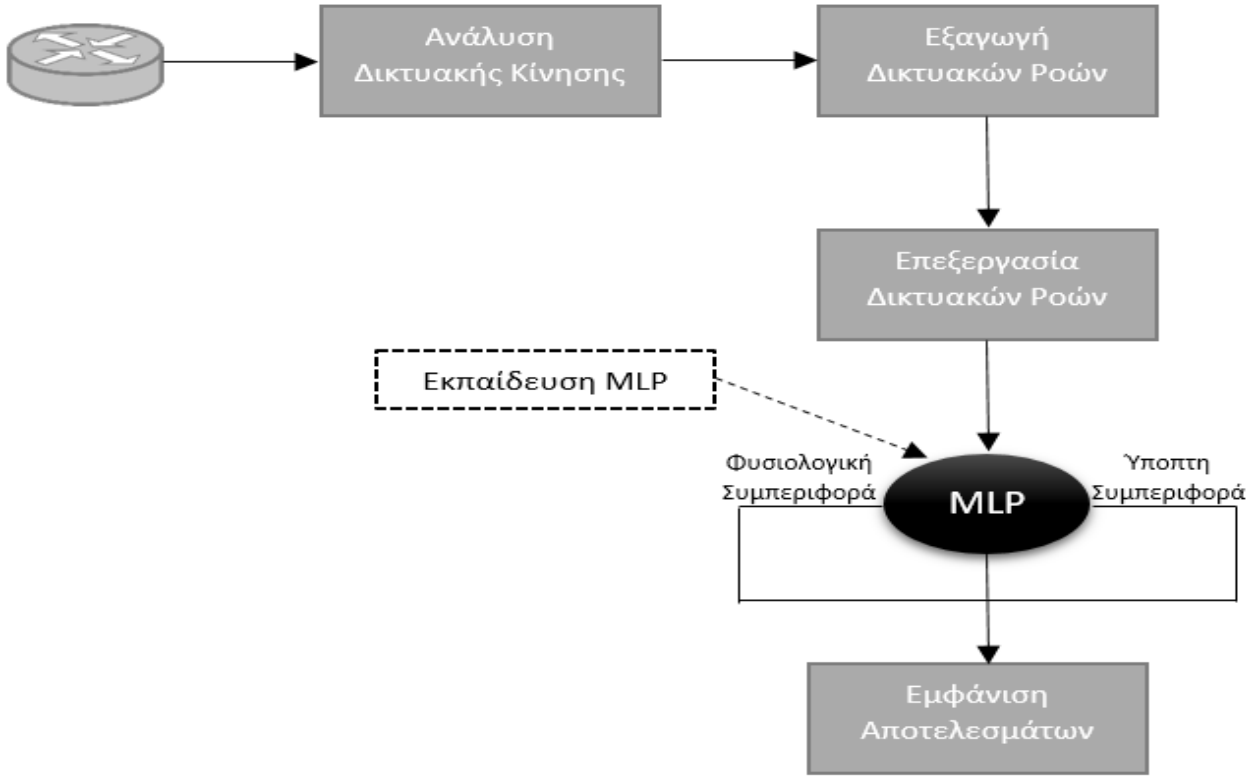
Αμφίδρομες Δικτυακές Ροές

Αμφίδρομη δικτυακή ροή: Συγκεκριμένες πληροφορίες από το σύνολο των IP πακέτων που ανταλλάσσεται μεταξύ δύο TCP ή UDP σημείων τερματισμού.



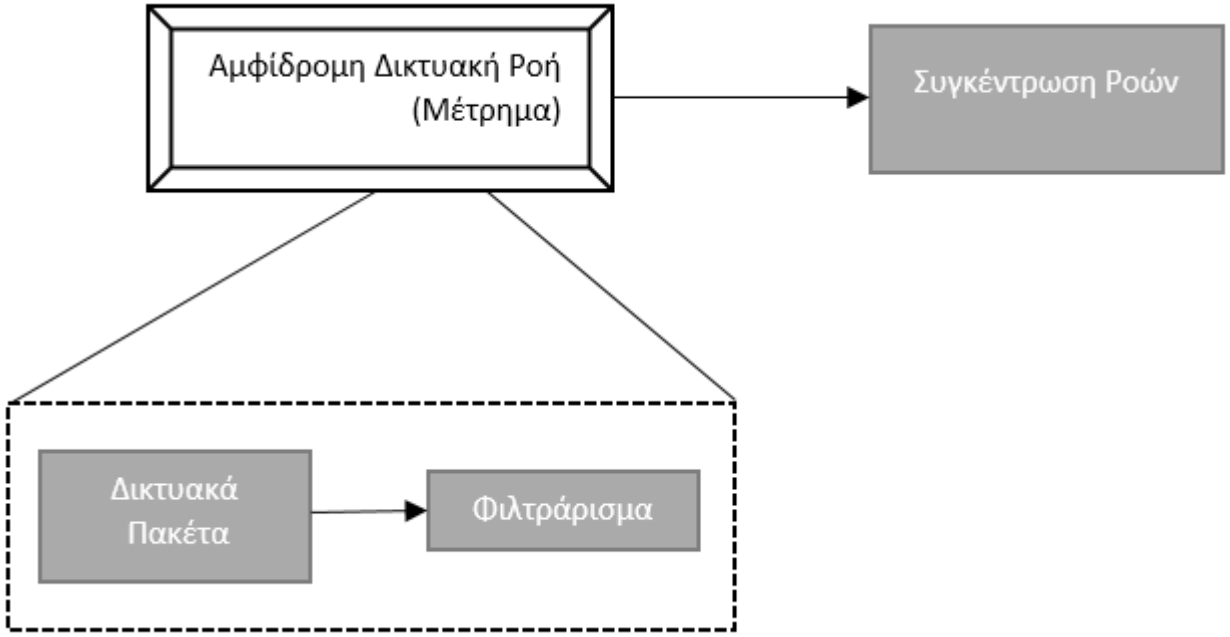
Σύγκριση δικτυακής κίνησης και δικτυακών ροών.

Ανίχνευση Εισβολών



Δομή λειτουργίας ανίχνευσης εισβολών.

Εξαγωγή Δικτυακών Ροών

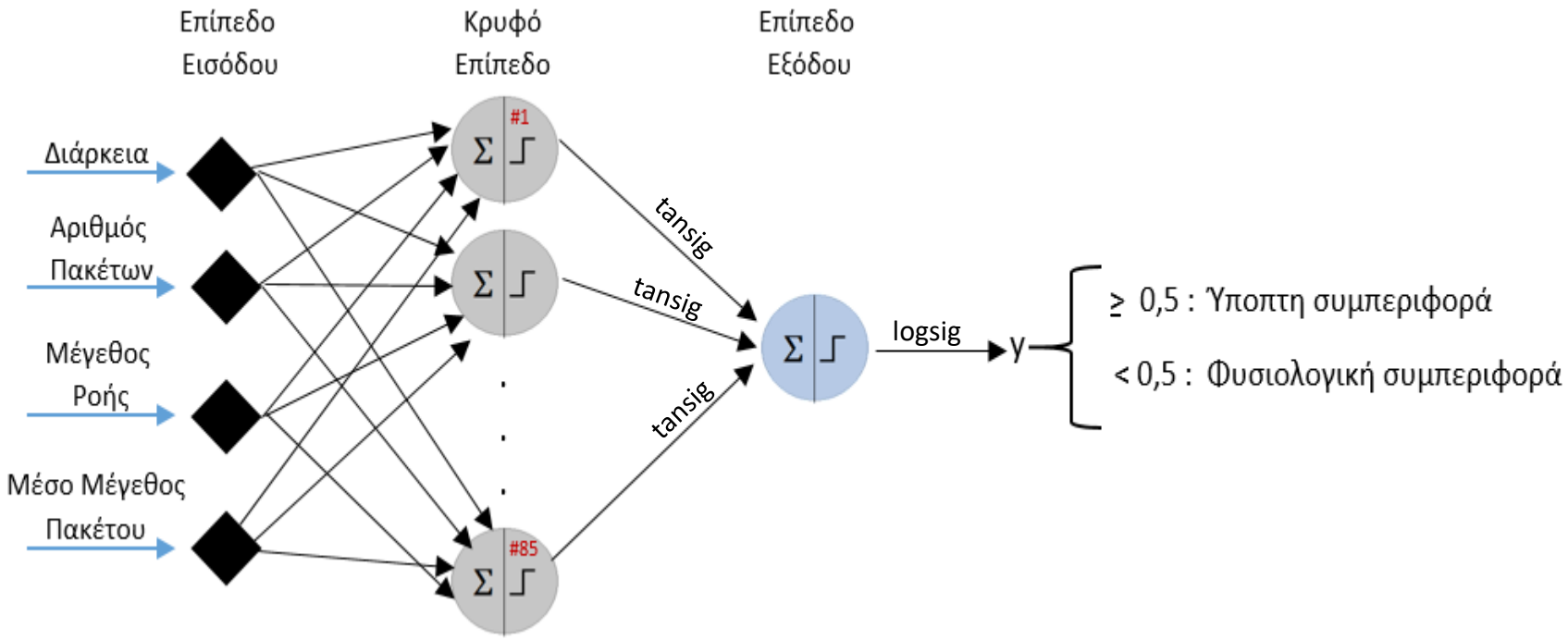


Διαδικασία εξαγωγής δικτυακών ροών.

Επεξεργασία Δικτυακών Ροών

- Διάρκεια δικτυακής ροής
- Αριθμός πακέτων
- Μέγεθος δικτυακής ροής
- Μέσο μέγεθος πακέτων

Δομή ΤΝΔ

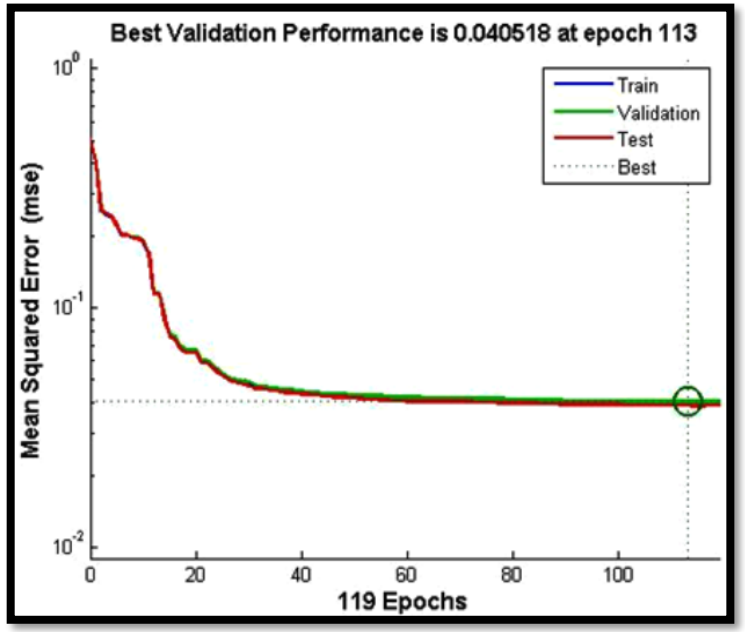


Δομή τεχνικού νευρωνικού δικτύου εφαρμογής.

Εκπαίδευση ΤΝΔ

Σύνολο Δικτυακών Ροών	Φυσιολογική Συμπεριφορά	Ύποπτη Συμπεριφορά
806132	361433	444699

- Levenberg-Marquardt
- Συνάρτηση τετραγωνικού σφάλματος
- Υποσύνολο εκπαίδευσης CTU-13
- MATLAB Neural Network Toolbox

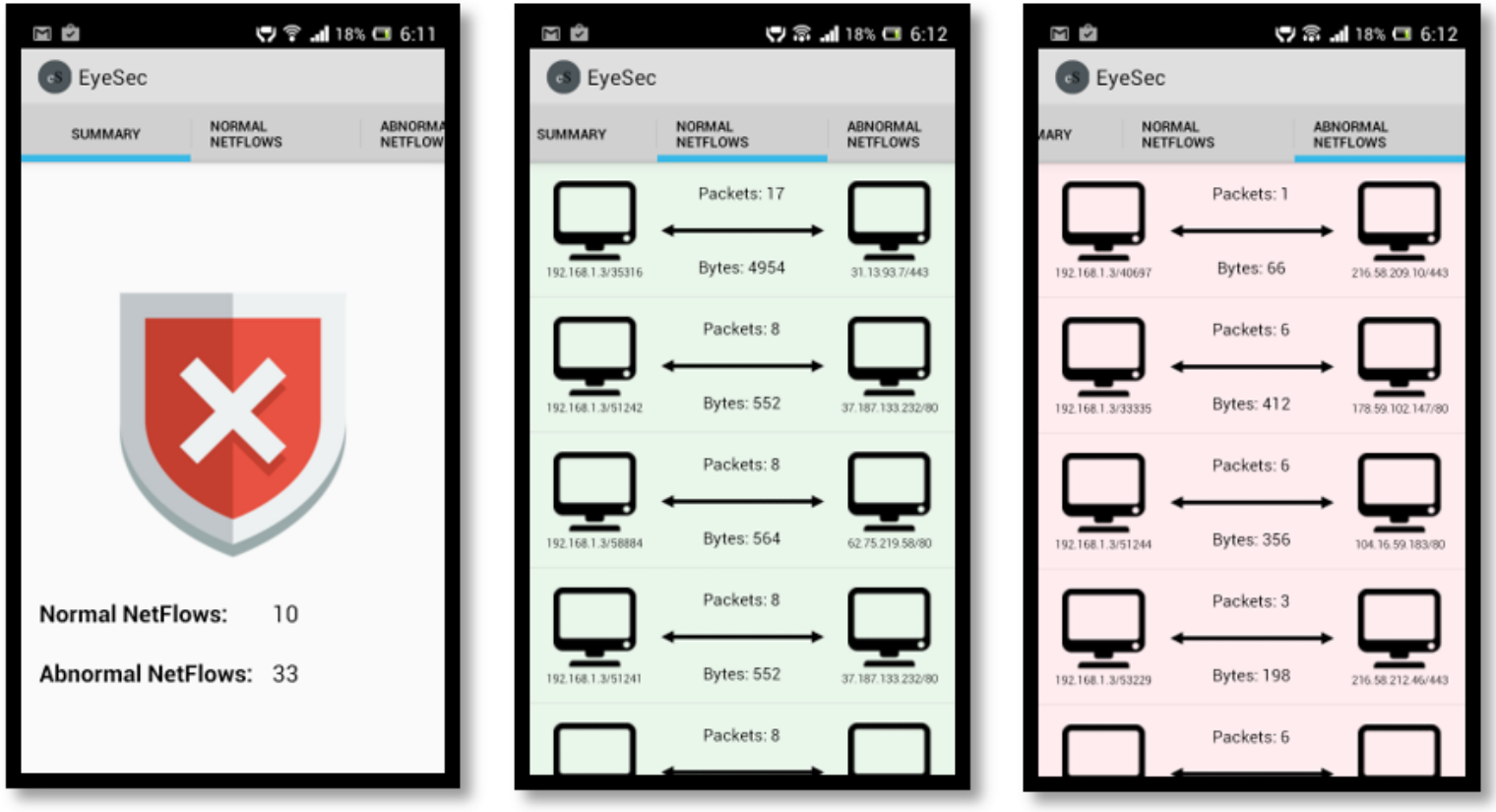


Ρυθμός μείωσης της συνάρτηση τετραγωνικού σφάλματος.

Αξιολόγηση ΤΝΔ

- Υποσύνολα ελέγχου του συνόλου CTU-13.
- Υποσύνολα ελέγχου του συνόλου της Sperotto.
- $\text{Ακρίβεια} = \frac{\text{Σύνολο ορθών προβλέψεων}}{\text{Σύνολο προβλέψεων}} = \frac{\text{TP+TN}}{\text{TP+TN+FP+FN}} = 85{,}55\%$
- $\text{Βαθμός ανίχνευσης} = \frac{\text{Ορθές προβέψεις εισβολών}}{\text{Σύνολο εισβολών}} = \frac{\text{TP}}{\text{TP+FN}} = 81{,}56\%$

Στιγμιότυπά Ανίχνευσης Εισβολών



Συμπέρασμα - Μελλοντικές Επεκτάσεις

Συμπέρασμα: Δημιουργία μίας εφαρμογής η οποία μπορεί να αποτελέσει αφετηρία για την περαιτέρω ανάπτυξη των IDS στις κινητές συσκευές.

Μελλοντικές Επεκτάσεις:

- Περαιτέρω βελτίωση των τιμών της ακρίβειας και του βαθμού ανίχνευσης.
- Δημιουργία δεύτερου ΤΝΔ σκοπός τους οποίου θα αποτελεί της ύποπτης δικτυακής ροής σε συγκεκριμένους τύπους επιθέσεων.
- Ανίχνευση περισσότερων εισβολών χρησιμοποιώντας πληροφορίες από τα χαρακτηριστικά της κινητής συσκευής.
- Ανίχνευση περισσότερων εισβολών χρησιμοποιώντας πληροφορίες από το προφίλ του χρήστη.

Σας ευχαριστώ πολύ !

Ακολουθεί επίδειξη της εφαρμογής