2021

þÿ ‘ » ³ Ì Á ¹ ¸ ¼ ¿ ¹ ‘ ½ ¯ Ç ½ µ Å Ã · Â • ¹ Ã ² ¿ »

þÿ ” ¯ º Ä Å ± » · Á ¿ Æ ¿ Á ¹ Î ½ ’ ¬ Ã µ ¹ ¤ µ

þÿ ‘ ½ ¿ Ã ¿ À ¿ ¹ · Ä ¹ º ¿ Í £ Å Ã Ä ® ¼ ± Ä ¿ Â

þÿ ¤ Ã ¹ Á Î ½ · Â , ‘ ¸ ± ½ ¬ Ã ¹ ¿ Â

þÿ œ µ Ä ± À Ä Å Ç ¹ ± º Ì Á Ì ³ Á ± ¼ ¼ ± Ã Ä ± » · Á ¿ Æ ¿ Á ¹ ± º ¬ £ Å Ã Ä ® ¼ ± Ä ± º ± ¹ Ä · ½ ¨ · Æ ¹ ± º

þÿ £ Ç ¿ » ® ” ¹ ¿ ¯ º · Ã · Â º ± ¹ • À ¹ Ã Ä ® ¼ · Â ¥ À ¿ » ¿ ³ ¹ Ã Ä Î ½ , ± ½ µ À ¹ Ã Ä ® ¼ ¹ ¿ • µ ¬ À ¿ » ¹ Â

ΜΑΙΟΣ 2021

ΣΧΟΛΗ ΟΙΚΟΝΟΜΙΚΩΝ,ΔΙΟΙΚΗΣΗ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΑΛΓΟΡΙΘΜΟΙ ΑΝΙΧΝΕΥΣΗΣ ΕΙΣΒΟΛΗΣ ΣΕ ΔΙΚΤΥΑ ΠΛΗΡΟΦΟΡΙΩΝ ΒΑΣΕΙ ΤΕΧΝΗΤΟΥ ΑΝΟΣΟΠΟΙΗΤΙΚΟΥ ΣΥΣΤΗΜΑΤΟΣ

ΑΘΑΝΑΣΙΟΣ ΤΣΙΡΩΝΗΣ

ΜΑΙΟΣ 2021

ΣΧΟΛΗ ΟΙΚΟΝΟΜΙΚΩΝ,ΔΙΟΙΚΗΣΗ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΑΛΓΟΡΙΘΜΟΙ ΑΝΙΧΝΕΥΣΗΣ ΕΙΣΒΟΛΗΣ ΣΕ ΔΙΚΤΥΑ ΠΛΗΡΟΦΟΡΙΩΝ ΒΑΣΕΙ ΤΕΧΝΗΤΟΥ ΑΝΟΣΟΠΟΙΗΤΙΚΟΥ ΣΥΣΤΗΜΑΤΟΣ

Διατριβή η οποία υποβλήθηκε προς απόκτηση εξ αποστάσεως μεταπτυχιακού τίτλου σπουδών στα Πληροφοριακά Συστήματα και Ψηφιακή Καινοτομία στο Πανεπιστήμιο Νεάπολις

ΑΘΑΝΑΣΙΟΣ ΤΣΙΡΩΝΗΣ

ΣΕΛΙΔΑ ΕΓΚΥΡΟΤΗΤΑΣ

Ονοματεπώνυμο Φοιτητή/Φοιτήτριας: Τσιρώνης Αθανάσιος

Τίτλος Μεταπτυχιακής Διατριβής: Αλγόριθμοι Ανίχνευσης Εισβολής Σε Δίκτυα Πληροφοριών Βάσει Τεχνητού Ανοσοποιητικού Συστήματος

Η παρούσα Μεταπτυχιακή Διατριβή εκπονήθηκε στο πλαίσιο των σπουδών για την απόκτηση εξ αποστάσεως μεταπτυχιακού τίτλου στο Πανεπιστήμιο Νεάπολις και εγκρίθηκε στις …..…… [ημερομηνία έγκρισης] από τα μέλη της Εξεταστικής Επιτροπής.

Εξεταστική Επιτροπή:

Πρώτος επιβλέπων (Πανεπιστήμιο Νεάπολις Πάφος)……[ονοματεπώνυμο, βαθμίδα, υπογραφή]

Μέλος Εξεταστικής Επιτροπής: ……[ονοματεπώνυμο, βαθμίδα, υπογραφή]

Μέλος Εξεταστικής Επιτροπής: ……[ονοματεπώνυμο, βαθμίδα, υπογραφή]

ΥΠΕΥΘΥΝΗ ΔΗΛΩΣΗ

Ο Τσιρώνης Αθανάσιος γνωρίζοντας τις συνέπειες της λογοκλοπής, δηλώνω υπεύθυνα ότι η παρούσα εργασία με τίτλο «Αλγόριθμοι Ανίχνευσης Εισβολής Σε Δίκτυα Πληροφοριών Βάσει Τεχνητού Ανοσοποιητικού Συστήματος», αποτελεί προϊόν αυστηρά προσωπικής εργασίας και όλες οι πηγές που έχω χρησιμοποιήσει, έχουν δηλωθεί κατάλληλα στις βιβλιογραφικές παραπομπές και αναφορές. Τα σημεία όπου έχω χρησιμοποιήσει ιδέες, κείμενο ή/και πηγές άλλων συγγραφέων, αναφέρονται ευδιάκριτα στο κείμενο με την κατάλληλη παραπομπή και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη περιγραφή.

Ο Δηλών

ΕΥΧΑΡΙΣΤΙΕΣ

Ξεκινώντας θα ήθελα να ευχαριστήσω θερμά όλους εκείνους που συνέβαλαν στη δημιουργία, ολοκλήρωση και τελειοποίηση της πτυχιακής μου εργασίας. Ευχαριστώ θερμά τον καθηγητή μου κ. Λευτέρη Ζαχαριουδάκη για την ουσιαστική καθοδήγησή του πάνω στο σκελετό που θα έπρεπε να στηριχτεί η διπλωματική μου εργασία. Επίσης θα ήθελα να ευχαριστήσω και όλους τους καθηγητές και συμφοιτητές μου που με υποστήριξαν και με βοήθησαν όλα αυτά τα χρόνια της φοίτησής μου.

Αθανάσιος Τσιρώνης

ΑΦΙΕΡΩΜΕΝΗ

Στην οικογένειά μου, για την υπομονή και την πίστη που υπέδειξαν όλα αυτά τα έτη των σπουδών μου, και για την στήριξή τους καθ' όλη τη διάρκεια της προετοιμασίας και ολοκλήρωσης αυτής της εργασίας.

ΠΕΡΙΕΧΟΜΕΝΑ

ΕΥΧΑΡΙΣΤΙΕΣ **3**

ΠΙΝΑΚΑΣ ΠΙΝΑΚΩΝ **6**

ΠΙΝΑΚΑΣ ΕΙΚΟΝΩΝ **6**

ΠΙΝΑΚΑΣ ΔΙΑΓΡΑΜΜΑΤΩΝ ..... ERROR! BOOKMARK NOT DEFINED.

ΠΙΝΑΚΑΣ ΣΥΝΤΜΗΣΕΩΝ **7**

ΠΕΡΙΛΗΨΗ **8**

ABSTRACT **9**

ΕΙΣΑΓΩΓΗ **10**

ΚΕΦΑΛΑΙΟ 1. ΦΥΣΙΚΟ ΑΝΟΣΟΠΟΙΗΤΙΚΟ ΣΥΣΤΗΜΑ **11**

1.1 Εισαγωγη 11
1.2 Όργανα του ανοσοποιητικου συστηματος 12
1.2.1 Έμφυτη και επικτητη ανοσοποιηση 12
1.2.2 Πως το ανοσοποιητικο συστημα προστατευει τον οργανισμο μας 13
1.2.3 Σωματικη υπερ-μεταλλαξη και τροποποιηση υποδοχεων 15
1.2.4 Αντιγονα και αντισωματα 16
1.2.5 Λευκα κυτταρα 17
1.2.6 Λεμφοκυτταρα 18
1.2.7 Τα Β-κυτταρα 19
1.2.8 Μνημη του ανοσοποιητικου συστηματος 20

ΚΕΦΑΛΑΙΟ 2. ΣΥΣΤΗΜΑΤΑ ΑΝΙΧΝΕΥΣΗΣ ΕΠΙΘΕΣΕΩΝ (IDS) **22**

2.1 Ασφαλεια Πληροφοριων 22
2.2 Συστηματα Ανιχνευσης Εισβολων 23
2.2.1. Ευπαθη Συστηματα 23
2.2.2. Ιστορικη αναδρομη - Ορισμος IDS 23
2.2.3. Ταξινομηση των IDS 24
2.2.1.1. Ταξινόμηση βάσει της μεθόδου ανίχνευσης *24*
2.2.1.2. Συστήματα ανίχνευσης ανωμαλιών *25*
2.2.1.3. Συστήματα ανίχνευσης με υπογραφές *26*
2.2.1.4. Ταξινόμηση με βάση τα χαρακτηριστικά του συστήματος *26*
2.2.1.4.1. Χρόνος ανίχνευσης 26
2.2.1.4.2. Απόκριση σε ανιχνευμένες επιθέσεις 27
2.2.1.4.3. Προέλευση των δεδομένων ανάλυσης 27
2.3. Εξελιξη της τεχνολογιας IDS 29

ΚΕΦΑΛΑΙΟ 3. ΤΟ ΤΕΧΝΗΤΟ ΑΝΟΣΟΠΟΙΗΤΙΚΟ ΣΥΣΤΗΜΑ **31**

3.1. Εισαγωγη 31
3.2 Μοντελα του τεχνητου ανοσοποιητικου συστηματος 32
3.2.1. Αλγοριθμος για το τεχνητο ανοσοποιητικο συστημα 32
3.2.2. Κλασικη αποψη για τα μοντελα των AIS 34
3.2.3. Αρνητικη επιλογη 35
3.2.4. Εξελικτικες προσεγγισεις 36
3.2.5. Αλγοριθμος επεκτασης κλωνων και επιλογης 37
3.2.6. Η θεωρια δικτυου 40
3.3. Μοντελα βασισμενα στην επιλογη κλωνων 40
3.3.1. CLONALG 41
3.3.2. Δυναμικη επιλογη κλωνων 43

3.3.3. Πολυ-επιπεδο AIS 45

ΚΕΦΑΛΑΙΟ 4. ΑΝΙΧΝΕΥΣΗ ΕΙΣΒΟΛΗΣ (ID) ΒΑΣΕΙ ΤΕΧΝΗΤΟΥ ΑΝΟΣΟΠΟΙΗΤΙΚΟΥ ΣΥΣΤΗΜΑΤΟΣ (AIS) 50

4.1. Το πλαισιο για τον σχεδιασμο Συστηματων Ανιχνευσης Εισβολης (IDS) που βασιζονται σε Τεχνητο Ανοσοποιητικο Συστημα (AIS) 50
4.2. Κωδικοποιηση Αντισωματος / Αντιγονου 51
4.3. Αλγοριθμος Παραγωγης 57
4.4. Τροπος Εξελιξης 61

ΚΕΦΑΛΑΙΟ 5. ΣΥΜΠΕΡΑΣΜΑΤΑ 65

ΒΙΒΛΙΟΓΡΑΦΙΑ 67

ΠΙΝΑΚΑΣ ΠΙΝΑΚΩΝ

Πίνακας 2 Αντιστοιχία μεταξύ της επιλογής κλώνων και της βελτιστοποίησης [8] 39
Πίνακας 3 Σύγκριση των αλγορίθμων επιλογής κλώνων με τους εξελικτικούς αλγορίθμους [8] 40
Πίνακας 4. Χρονικές και διαστημικές πολυπλοκότητες όλων των αλγορίθμων παραγωγής ανιχνευτών [88]. 58

ΠΙΝΑΚΑΣ ΕΙΚΟΝΩΝ

Εικόνα 1. Ανοσοποιητικό σύστημα [5] 13
Εικόνα 2Πως το ανοσοποιητικό σύστημα προστατεύει τον οργανισμό [1] 14
Εικόνα 3Σύμπλεγμα αντιγόνου-αντισώματος [39] 17
Εικόνα 4 Τύποι των λευκών κυττάρων [12] 18
Εικόνα 5Κύκλος ζωής των λεμφοκυττάρων [12] 19
Εικόνα 6Τα Β-κύτταρα μετατρέπονται σε κύτταρα πλάσματος παράγοντας αντισώματα [8] .. 20
Εικόνα 10. Σύστημα ανίχνευσης ανωμαλιών 25
Εικόνα 11. Σύστημα ανίχνευσης με υπογραφές 26
Εικόνα 12. Ταξινόμηση του IDS 28
Εικόνα 7. Ταξινόμηση των AIS αλγορίθμων 31
Εικόνα 8. R-συνεχής κανόνας 35
Εικόνα 9Επέκταση κλώνων (και επιλογή) των Β-κυττάρων κατά την παρουσία ενός αντιγόνου [1] 38

ΠΙΝΑΚΑΣ ΣΥΝΤΜΗΣΕΩΝ

ΑΠ - Ασφάλεια Πληροφοριών	ID - Intrusion Detection
ΠΣ - Πληροφοριακά Συστήματα	IDS - Intrusion Detection Systems
ΤΑΣ - Τεχνητά Ανοσοποιητικά Συστήματα	IDPS - Intrusion Detection and Prevention System
AIS - ArtificialImmuneSystems	IDWG - Intrusion Detection Working Group
ALC - Artificial Lymphocytes	IODEF - Incident Object Description Exchange Format
ANN - Artificial Neural Network	Ip - Internet Protocol
APC - Antigen Presenting Cell	IPS - Intrusion Prevention System
CIA - Confidentiality, Integrity, Availability	IS - Immune System
CIDF - Common Intrusion Detection Framework	IT - immunoassay techniques
CIDSS - Common Intrusion Detection Signatures Standard	ITO - Information Technology Office
CISL - Common Intrusion Specification Language	MHC - Major Histocompatibility Complex
CPU – Central Processing Unit	ML machine learning
DOS - Disk Operating System	NASA - National Aeronautics and Space Administration
GIDOs - Generalized Intrusion Detection Objects	NC - Negative Control
HIDS - Host-based IDS	NIDS - Network-based IDS
HIS - Human Immune System	NIS - natural immune system
HMM - hidden Markov model	NSP - Network Security Platform
HTTP – Hypertext Transfer Protocol	PC - Positive Control
IBM - International Business Machines	SIDs - Semantic Identifiers
IC - Immune Calculation	XML - Extensible Markup Language
IDMEF - Intrusion Detection Message Exchange Format	
IETF - Internet Engineering Task Force	

ΠΕΡΙΛΗΨΗ

Η παρούσα διπλωματική εργασία επιδιώκει να προσεγγίσει τα Τεχνητά Ανοσοποιητικά Συστήματα (ΤΑΣ) και τους αλγόριθμους ανίχνευσης εισβολής σε δίκτυα πληροφοριών.

Τα συστήματα υπολογιστών, καθώς εξελίσσονται είναι όλο και περισσότεροεκτεθειμένα σε επιθέσεις.Αυτός είναι ο λόγος που η ασφάλεια του υπολογιστήέχει αποκτήσει ζωτική σημασία για το δίκτυο. Οι εισβολές προκαλούν καταστροφήμέσα στα δίκτυα. Τα συστήματα ανίχνευσης εισβολής (IDS) χρησιμοποιούνται για την παρακολούθηση πληροφοριών σχετικά με αυτά και την αναφορά τους στους διαχειριστές ασφαλείας. Ένας σημαντικός και φυσικός τομέας εφαρμογών για προσαρμοστικά συστήματα που βασίζονται σε σμήνη, είναι αυτός του υπολογιστήασφαλείας.Ένα σύστημα ασφαλείας υπολογιστή πρέπει να προστατεύει ένα μηχάνημα ή ένα σύνολο μηχανημάτων από μη εξουσιοδοτημένους εισβολείς. Ο Εντοπισμός Εισβολής (ID) είναι ένας μηχανισμός που προσπαθεί να ανακαλύψει την μη φυσιολογική πρόσβαση σε υπολογιστές αναλύοντας διάφορες αλληλεπιδράσεις. Η**ερευνητικήπρόταση** της παρούσας μελέτης, είναι οι προσεγγίσεις του ID που βασίζονται στο Τεχνητό Ανοσοποιητικό Σύστημα (AIS). Η χρήση του AIS στον ID είναι μια «ελκυστική» έννοια στις τρέχουσες τεχνικές. Σε αυτή την μελέτη γίνεται μια προσπάθεια για τη συνοψίζει των ID μεθόδων που βασίζονται σε AIS από μια νέα οπτική γωνία. Επιπλέον, **προτείνεται ένα πλαίσιο για τον σχεδιασμό ID συστημάτων που βασίζονται στο AIS (IDSs)**. Η ανάλυση αυτή βασίστηκε σε τρεις βασικές πτυχές: κωδικοποίηση αντισωμάτων/αντιγόνων, αλγόριθμος παραγωγής και λειτουργία εξέλιξης. Επίσης γίνεται μία σύνοψη των αλγορίθμων που χρησιμοποιούνται συνήθως, τα χαρακτηριστικά εφαρμογής τους και την ανάπτυξη των IDSs μέσα σε αυτό το πλαίσιο. Τέλος, επισημαίνονται ορισμένες από τις μελλοντικές προκλήσεις σε αυτόν τον τομέα.

<u>Λέξεις-κλειδιά</u>: *Σύστημα ανίχνευσης εισβολής-IDS, Εντοπισμός Εισβολής-ID, Τεχνητό ανοσοποιητικό σύστημα-AIS, Ανθρώπινο ανοσοποιητικό σύστημα*

ABSTRACT

This dissertation seeks to approach Artificial Immune Systems (AIS) and intrusion detection algorithms into information networks.

Computer systems as they evolve are increasingly exposed to attacks. This is why computer security has become vital for the network. Intrusions cause destruction within the networks. Intrusion detection systems (IDS) are used to track information about it and report it to security administrators. An important and natural application area for swarm-based adaptive systems is computer security. A computer security system must protect a machine or set of machines from unauthorized intruders.Intrusion Detection (ID) is a mechanism that attempts to detect abnormal access to computers by analyzing various interactions. The research purpose of the present study is the approaches of ID based on the Artificial Immune System (AIS). The use of AIS in ID is an "attractive" concept in current techniques. In this study, an attempt is made to summarize AIS-based ID methods from a new perspective. In addition, a framework for designing AIS-based systems IDs (IDSs) is proposed. This analysis was based on three key aspects: antibody / antigen coding, production algorithm, and evolution function. It also summarizes the commonly used algorithms, their application features and the development of IDSs within this framework. Finally, some of the future challenges in this area are also highlighted.

Keywords:*Invasion Detection System-IDS, Invasion Detection – ID, Artificial Immune System-AIS, Human Immune System*

ΕΙΣΑΓΩΓΗ

Το τεχνητό ανοσοποιητικό σύστημα ή οι τεχνικές ανοσοποιητικού υπολογισμού (IC) χρησιμοποιούνται για να αντιμετωπιστούν προβλήματα διαφόρων κατηγοριών. Για παράδειγμα, εφαρμόζονται στους τομείς της βελτιστοποίησης, της ταξινόμησης, της μηχανικής μάθησης, του προσαρμοστικού ελέγχου, της ανίχνευσης διαταραχών. Εφαρμόζονται ακόμα και συνδυαστικά με τη χρήση άλλων μεθόδων, όπως με γενετικούς αλγόριθμους, με νευρωνικά δίκτυα, με τη νοημοσύνη σμήνους [1].

Από πολλές απόψεις, η ασφάλεια των υπολογιστών ομοιάζει με την βιολογική άμυνα. Το μεγαλύτερο μέρος των εργασιώνμε εφαρμογή των ArtificialImmuneSystems (AIS)σχετίζονται με την ανάπτυξη ψηφιακών συστημάτων υπεράσπισης. Για την αύξηση των υπαρχόντων συστημάτων ασφαλείας, τα AIS παράγουν ένα σύστημα προστασίας γενικού σκοπού, με τη χρήση ποικίλων εννοιών της προστασίας δεδομένων και της διαταραχής. Δραστηριότητες όπως να αναγνωρίζεται η μη εξουσιοδοτημένη χρήση, να διατηρείται η ακεραιότητα των δεδομένων και να αποτρέπεται η εξάπλωση ενός ιού, είναι καθοριστικές για τη διασφάλιση της ασφάλειας των υπολογιστικών συστημάτων.

Η αρνητική επιλογή στην προστασία των υπολογιστικών συστημάτων προτάθηκε αρχικά το 1994, από τον Forrest [2]. Στην συγκεκριμένη μελέτη, προκειμένου να προστατευθούν τα υπολογιστικά συστήματα, αξιοποιήθηκε η ικανότητα διάκρισης του ανοσοποιητικού συστήματος ανάμεσα στα ξένα κύτταρα (μη εξουσιοδοτημένοι χρήστες, ιοί) και τα φυσιολογικά (νόμιμοι χρήστες, ασφαλή αρχεία). Η μέθοδος αυτή συμπληρώνει τις άλλες μεθόδους που χρησιμοποιούνται για να αναγνωρίζονται οι ιοί, την κλασική μέθοδο κρυπτογραφίας και αυτή της ντετερμινιστικής πιστοποίησης αρχείων. Η υλοποίηση των πειραμάτων έγινε σε περιβάλλον DOS με διαφορετικούς ιούς. Βάσει των αποτελεσμάτων, αποδείχθηκε η ικανότητα της μεθόδου αναγνώρισης αλλοιώσεων των αρχείων εξαιτίας ιών. Ο αλγόριθμος αυτός πλεονεκτεί σε αρκετά σημεία σε σύγκριση με άλλες μεθόδους, όπως στον εντοπισμό καινοφανών ιών ή στο ότι είναι πιθανοτικός και κατανεμημένος. Ωστόσο, λόγω της αστάθειας της πληροφορίας που αποθηκεύεται στο υπολογιστικό σύστημα, χρειάζεται το φυσιολογικό στα υπολογιστικά συστήματα να οριστεί πιο δυναμικά από ότι στα φυσικά συστήματα.

ΚΕΦΑΛΑΙΟ 1. ΦΥΣΙΚΟ ΑΝΟΣΟΠΟΙΗΤΙΚΟ ΣΥΣΤΗΜΑ

1.1 Εισαγωγή

Το ανοσοποιητικό σύστημα του ανθρώπου αποτελείται από ένα πολύπλοκο δίκτυο εξειδικευμένων μελών όπως οι ιστοί, τα όργανα, τα κύτταρα και τα χημικά μόρια. Το φυσικό ανοσοποιητικό σύστημα μπορεί να αναγνωρίζει, να καταστρέφει και να διατηρεί ιστορικό ενός πλήθους από ξένα σωματίδια, όπως και να προστατεύει τον οργανισμό από εισβολείς.Για να είναι δυνατή η προστασία του οργανισμού από το ανοσοποιητικό σύστημα χρειάζεται να έχει αναπτυχθεί η ικανότητα διάκρισης των ξένων σωματιδίων.

Από τη μελέτη του ανοσοποιητικού συστήματος (IS)υπό την προοπτική της μοντελοποίησης, έχει προκύψει διαφορά απόψεων αναφορικά με τον τρόπο ανάπτυξης των ικανοτήτων και των λειτουργιών του ανοσοποιητικού συστήματος. Οι απόψεις αυτές, συνοψίζονται στα εξής:

- στη κλασική άποψη, σύμφωνα με την οποία η διάκριση ανάμεσα στα φυσιολογικά και στα ξένα κύτταρα γίνεται με τη χρήση των λεμφοκυττάρων
- στη θεωρία της επιλογής κλώνων, που ισχυρίζεται ότι πραγματοποιείται παραγωγή μεταλλαγμένων κλώνων από τα ενεργοποιημένα Β-κύτταρα
- στην θεωρία κινδύνου, που εστιάζει στη δυνατότητα διάκρισης του ανοσοποιητικού συστήματος των επικίνδυνων και των μη επικίνδυνων ξένων κυττάρων
- στην θεωρία του δικτύου, που υποστηρίζει τη δημιουργία δικτύου ανιχνευτών από τα Β-κύτταρα [3].

Οι παραπάνω θεωρίες αποτέλεσαν τη βάση για την ανάπτυξη αντίστοιχων μοντέλων με επιτυχή εφαρμογή σε πραγματικά προβλήματα. Στην επόμενη ενότητα, παρουσιάζονται παραδείγματα τέτοιων εφαρμογών.

1.2 Όργανα του ανοσοποιητικού συστήματος

Το ανοσοποιητικό σύστημα αποτελείται από όργανα, τα οποία κατηγοριοποιούνται σε δύο ομάδες, τα κεντρικά λεμφοειδή όργανα και τα περιφερειακά. Στα κεντρικά λεμφοειδή όργανα, τα οποία έχουν ως στόχο τη δημιουργία ώριμων κυττάρων ανοσοποίησης (λεμφοκύτταρα), κατατάσσονται ο μυελός των οστών και ο θύμος αδένας. Ο μυελός των οστών παράγει αιμοσφαίρια και αιμοπετάλια, Β-κύτταρα και κύτταραεξολοθρευτών, κοκκωδών κυττάρων και ανώριμων κύτταρων θύμου αδένα. Ο θύμος αδένας παράγει ώριμα Β-κύτταρα.

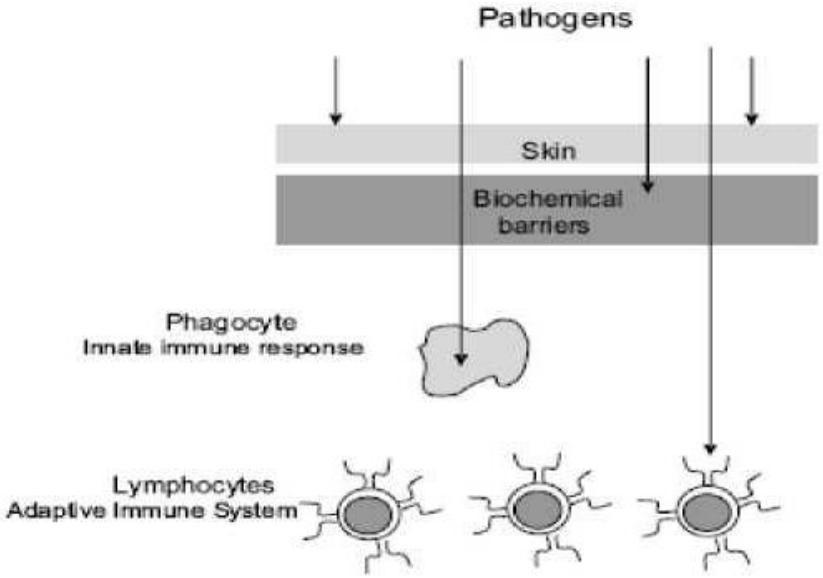
Στα περιφερειακά λεμφοειδή όργανα ανήκουν η σπλήνα, οι λεμφαδένες, και οι ιστοί του αναπνευστικού συστήματος. Σκοπός των οργάνων αυτών είναι η διευκόλυνση της αλληλεπίδρασης ανάμεσα στα λεμφοκύτταρα και τα αντιγόνα, τα οποία συγκεντρώνονται σε μεγάλο βαθμό στα όργανα αυτά. Η σπλήναποτελείται από Β-κύτταρα, Τ- κύτταρα, μεγάλα φαγοκύτταρα και αιμοσφαίρια. Στο όργανο αυτό συντελείται η ενεργοποίηση των Β-κυττάρων και η παραγωγή μεγάλων ποσοτήτων αντισωμάτων, καθώς και η καταστροφή των παλιών αιμοσφαιρίων.Οι λεμφαδένες συνίστανται κυρίως από Τ και Β-κύτταρα, μέσω των οποίων γίνεται αντιληπτή η ύπαρξη αντιγόνων, καθώς και από μεγάλα φαγοκύτταρα, ενεργοποιώντας και αυτοί το ανοσοποιητικό σύστημα [3], [4].

1.2.1 Έμφυτη και επίκτητη ανοσοποίηση

Στο φυσικό ανοσοποιητικό σύστημα υπάρχουν πολλαπλά επίπεδα υπεράσπισης. Στο πρώτο επίπεδο υπεράσπισης (δέρμα, ρινικές τρίχες) μπλοκάρεται η απορρόφηση παθογόνων. Η απομάκρυνση των παθογόνων ενισχύεται από την φυσιολογική άμυνα μέσω υγρών του σώματος (σάλιο, ιδρώτας και δάκρυα). Επιπρόσθετα, οι άνθρωποι διαθέτουν έμφυτη και προσαρμόσιμη ανοσοποίηση. Για την αναγνώριση των παθογόνων, το έμφυτο ανοσοποιητικό σύστημα χρησιμοποιεί πλήθος απόμοριακάπρότυπα.

Το έμφυτο ανοσοποιητικό σύστημα υφίσταται από τη γέννηση χωρίς δυνατότητα προσαρμογής κατά τη διάρκεια της ζωής ενός ατόμου. Εάν δεν είναι δυνατή η απομάκρυνση ενός παθογόνου από το έμφυτο ανοσοποιητικό σύστημα, τότε λαμβάνει

δράσητο επίκτητο ανοσοποιητικό σύστημα. Το επίκτητο ανοσοποιητικό σύστημα δραενάντια σε συγκεκριμένα παθογόνα και τροποποιείται από την έκθεση σε αυτά. Έτσι, συντελείται από το ανοσοποιητικό σύστημα η δημιουργία και η διατήρηση ενός ιστορικού των εισβολέων και των τρόπων αντιμετώπισής τους [5].



Εικόνα 1. Ανοσοποιητικό σύστημα [5]

1.2.2 Πως το ανοσοποιητικό σύστημα προστατεύει τον οργανισμό μας

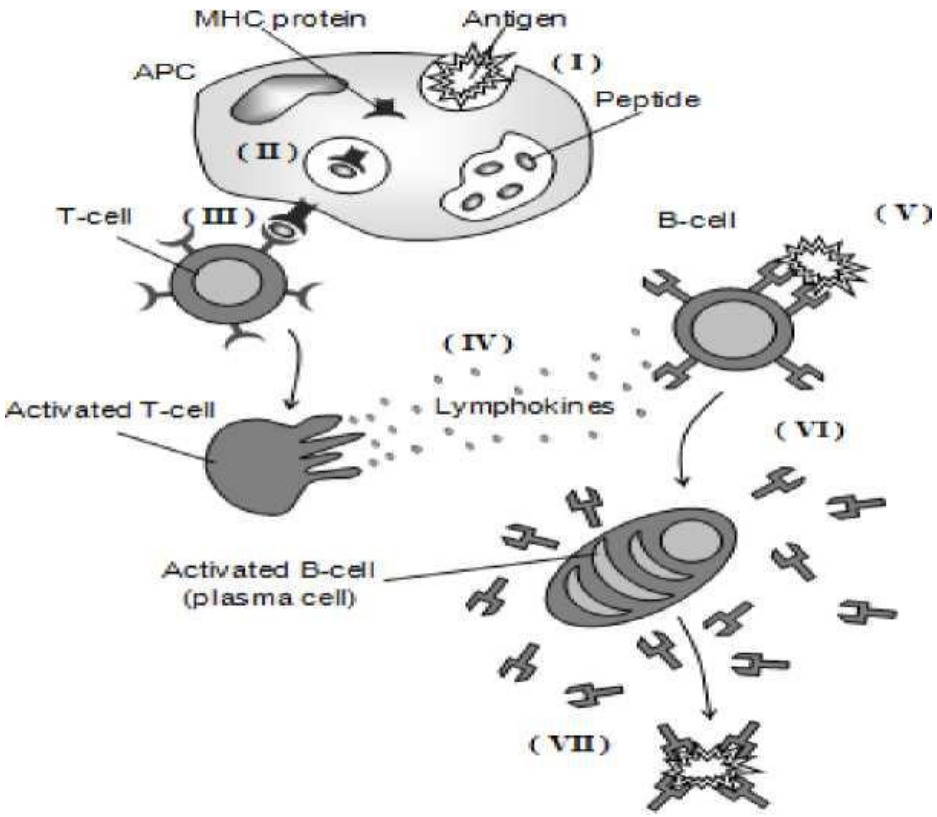
Η προστασία του οργανισμού συντελείται από κύτταρα και μόρια που συνεργάζονται για την επίτευξη ενός κοινού στόχου, το αντιγόνο, το οποίο συνήθως είναι ένα ξένο μόριο ενός βακτηρίου ή κάποιου άλλου εισβολέα.

Η διαρκής κυκλοφορία στον οργανισμό ειδικών αντιγόνο-παρουσιαστικών(APC) κυττάρων, όπως τα μεγάλα φαγοκύτταρα, έχει ως αποτέλεσμα την απορρόφηση των αντιγόνων που εντοπίζονται και τον θρυμματισμό τους σε αντιγονικά πεπτίδια (Εικ.2-I). Ορισμένα μέρη από τα πεπτίδια αυτά σχετίζονται με τα μόρια του συμπλέγματος ιστοσυμαβοτότητας (MHC). Η δράση των συγκεκριμένων μορίων συνίσταται στη μεταφορά των πεπτιδίων από το εσωτερικό του κυττάρου στην επιφάνεια του. Οι ειδικοί μοριακοί υποδοχείς των Τ-κυττάρων ή λεμφοκυττάρων καθιστούν δυνατή την αναγνώριση των συνδυασμών των πεπτιδίων-MHCμορίων (Εικ.2-II). Με την έκκρισηλεμφοκίνων ή χημικών σημάτων από τα ενεργοποιημένα Τ-κύτταρα

επιτυγχάνεται η ενεργοποίηση άλλων συστατικών μερών του ανοσοποιητικού συστήματος (Εικ.2-III).

Στα παραπάνω σήματααποκρίνονται τα Β-λεμφοκύτταρα, τα οποία επίσης διαθέτουν μοριακούς υποδοχείς μοναδικής ειδικότητας στην επιφάνεια τους. Αντίθετα με τα Τ-κύτταρα,στα Β-λεμφοκύτταρα είναι δυνατή η αναγνώριση μερών των αντιγόνων χωρίς την ύπαρξη του MHCμορίου (Εικ.2-IV).

Μετά την ενεργοποίηση των Β-λεμφοκυττάρων ακολουθεί η διαίρεση και διαφοροποίησή τους σε κύτταρα πλάσματος, τα οποία εκκρίνουν αντισώματα, που είναι διαλυτές μορφές των υποδοχέων τους (Εικ.2-V). Το ταίριασμα των αντισωμάτων και των αντιγόνων μπορεί να επιφέρει την αδρανοποίησή τους (Εικ.2-VI) ή την επιτάχυνση της καταστροφή τους με συμπληρωματικά ένζυμα ή με κύτταρα 'καθαριστές'. Η μετατροπή ορισμένων Τ και Β- κυττάρων σε κύτταρα μνήμης, ενισχύει την άμεση αντίδραση του ανοσοποιητικού σε περίπτωση αντιμετώπισης του ίδιου αντιγόνου μελλοντικά. Η συχνή μετάλλαξη των γονιδίων των Β-κυττάρων βελτιώνει την απόκριση των αντισωμάτων με τις επαναλαμβανόμενες ανοσοποιήσεις, το φαινόμενο αυτό ονομάζεται μετάλλαξη της συγγένειας.



Εικόνα 2Πως το ανοσοποιητικό σύστημα προστατεύει τον οργανισμό [1]

1.2.3 Σωματική υπέρ-μετάλλαξη και τροποποίηση υποδοχέων

Κατά τη διάρκεια της ανοσοποιητικής αντίδρασης που εξαρτάται από τα Τ-κύτταρα, δύο μηχανισμοί ευθύνονται για τη ποικιλομορφία των ενεργοποιημένων Β-κυττάρων: η*υπέρ-μετάλλαξη* και η*διόρθωση των υποδοχέων.*Στο σύνολο των κυττάρων μνήμης προστίθενται μόνο οι εκδοχές των κυττάρων που εμφανίζουν την μεγαλύτερη συγγένεια. Πρόκειται για μια διαδικασία ωρίμανσης του ανοσοποιητικού που πραγματοποιείται σε ένα ειδικό περιβάλλον, το βλαστικό κέντρο (GerminalCenter).

Σε μια αντίδραση μνήμηςσυμμετέχουναντισώματαμε μεγαλύτερη συγγένεια από τα αντίστοιχα της πρωταρχικής αντίδρασης. Αυτό οφείλεται στην ωρίμανση τωνλεμφοκυττάρων.Υπάρχουν τρία διαφορετικά είδη μετάλλαξης της Υ-περιοχής του αντισώματος:

- μεταλλάξεις σημείων
- σύντομες διαγραφές
- μεταλλαγή μετατόπισης

Η πραγματοποίηση τυχαίων αλλαγών σε ορισμένες περιπτώσεις αυξάνουν τη συγγένεια του αντισώματος.Τα αντισώματα αυτά επιλέγονται σαν κύτταρα μνήμης. Εξαιτίας της τυχαίας φύσης της διαδικασίας της σωματικής μετάλλαξης, είναι πιθανή η μετατροπή ορισμένων μεταλλαγμένων γονιδίων σε μη λειτουργικά ή η ανάπτυξη βλαβερώνιδιοτήτων για τον οργανισμό. Στην περίπτωση αυτή, είναι αναγκαία η εξάλειψη των κυττάρων αυτών για να αποφευχθεί η συμπερίληψή τους στα κύτταρα μνήμης. Η διαδικασία εξάλειψης των Β-κυττάρων δεν είναι πλήρως κατανοητή. Πιθανόν να ευθύνεται για την εξάλειψή τους η διαδικασία της ‘διάλυσης’ στο βλαστικό κέντρο.

Το γεγονός ότι η συγγένεια των αντισωμάτων αυξάνεται κατά τη δευτερογενή αντίδραση συγκριτικά με την αρχική υποδεικνύει ότι η ωρίμανση του ανοσοποιητικού συστήματος είναι μια συνεχής διαδικασία. Τα τρία βασικά χαρακτηριστικά των αποκρίσεων του προσαρμοζόμενου ανοσοποιητικού συστήματος είναι:

α) *η επαρκής ποικιλία* ώστε να μπορέσουν να αντιμετωπίσουν τα διαφορετικά αντιγόνα

β) *η διάκριση μεταξύ των φυσιολογικών και μη φυσιολογικών κυττάρων*

γ) *η μεγάλης διάρκειας ανοσολογική μνήμη.*

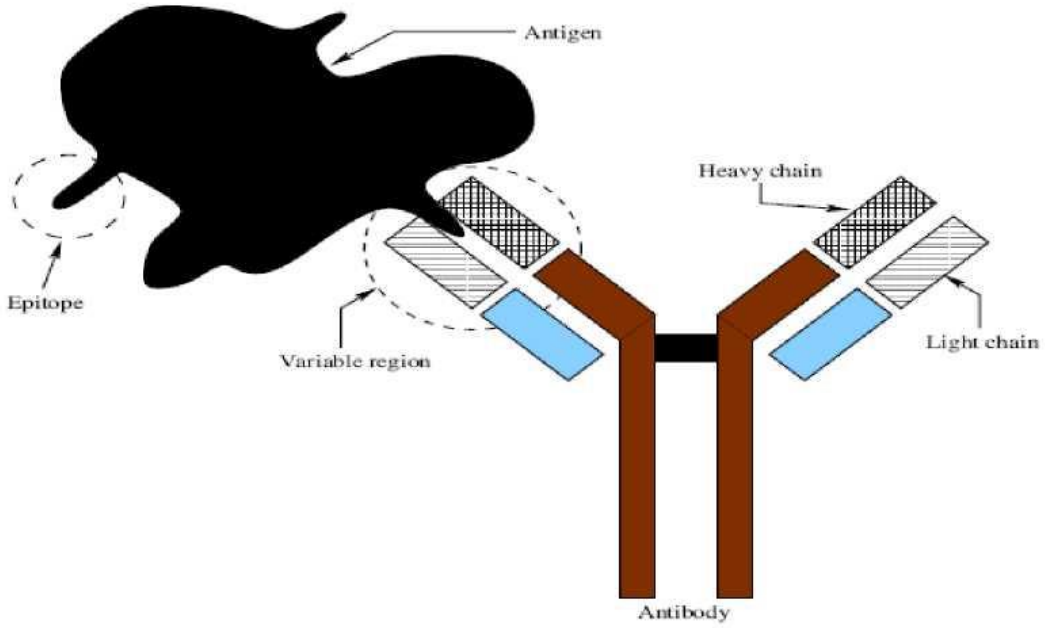
Πέρα από την κλασική άποψη που προτάθηκε από τον Burnet(1959) για την επιλογή των κλώνων, υποδεικνύεται από πρόσφατες έρευνες η εφαρμογή από το ανοσοποιητικό σύστημα μοριακής επιλογής των υποδοχέων σε συνδυασμό με την επιλογή κλώνων.

Η τροποποίηση των υποδοχέων των Β-κυττάρων προσφέρει τη δυνατότητα διαφυγής από ένα τοπικό ελάχιστο συγγένειας. Συνεπώς, οι μετατροπές των υποδοχέων και οι μεταλλάξεις σημείων αποτελούν συμπληρωματικές διαδικασίες κατά την ωρίμανση του ανοσοποιητικού. Επιπλέον, καινούριακύτταρα εισάγονται από τον μυελό των οστών, τα οποία προστίθενται στα λεμφοκύτταρα για τη διατήρηση της ποικιλομορφίας του πληθυσμού [1].

1.2.4 Αντιγόνα και αντισώματα

Στο φυσικό ανοσοποιητικό σύστημα, όταν εμφανίζεται ένα αντιγόνο προκαλεί αντίδραση για την αποφυγή της βλάβης που πιθανόν να προκαλέσει.Τα αντιγόνα είναι σύνθετα μόρια, συνήθως πρωτεΐνες ή υδρογονάνθρακες, η εισαγωγή των οποίων σε οργανικό σώμαπροκαλεί μια ανοσοαπόκριση, στην οποία περιλαμβάνεται ηπαραγωγή συγκεκριμένων αντισωμάτων. Τα αντιγόνα μπορεί να είναι τοξίνες ή και μόρια στην κυτταρική επιφάνεια και η αναγνώρισή τους γίνεται με τη δημιουργία ενός μοριακού δεσμού ανάμεσα σε ένα αντιγόνο και τους υποδοχείς στην επιφάνεια των Β-κυττάρων. Επειδή τα περισσότερα αντιγόνα είναι ιδιαίτερα πολύπλοκα, είναι δυνατή η σύνδεση με τους υποδοχείς των Β- κυττάρων μόνο ορισμένων μερών τους, των επιτομών,όπως φαίνεται στην εικόνα 5. Οι επιτομές προκαλούν στοανοσοποιητικό σύστημα μια ειδική αντίδραση και η σύνδεση των επιτομών με τους υποδοχείς των αντισωμάτων γίνεται μέσω μιας ειδικής δύναμης ταιριάσματος, η οποία ονομάζεται ‘συγγένεια’, ‘συνάφεια’.

Στην επιφάνεια ενός λεμφοκυττάρου υπάρχουν περίπου 10^5 υποδοχείς, καθώς λόγω της ίδιας δομής τους είναι δυνατό το ταίριασμα μόνο ενός λεμφοκυττάρου με τις σχετικές επιτομές. Οι υποδοχείς που δεσμεύονται από τα παθογόνα καθορίζουν την συγγένεια του λεμφοκυττάρου με ένα δεδομένο παθογόνο. Στην περίπτωση που η προκύπτουσα συγγένεια βρίσκεται εντός του κατώτατου αποδεκτού ορίου, το λεμφοκύτταρο στέλνει ένα σήμα στα κύτταρα και το ανοσοποιητικό σύστημα αποκρίνεται [12].

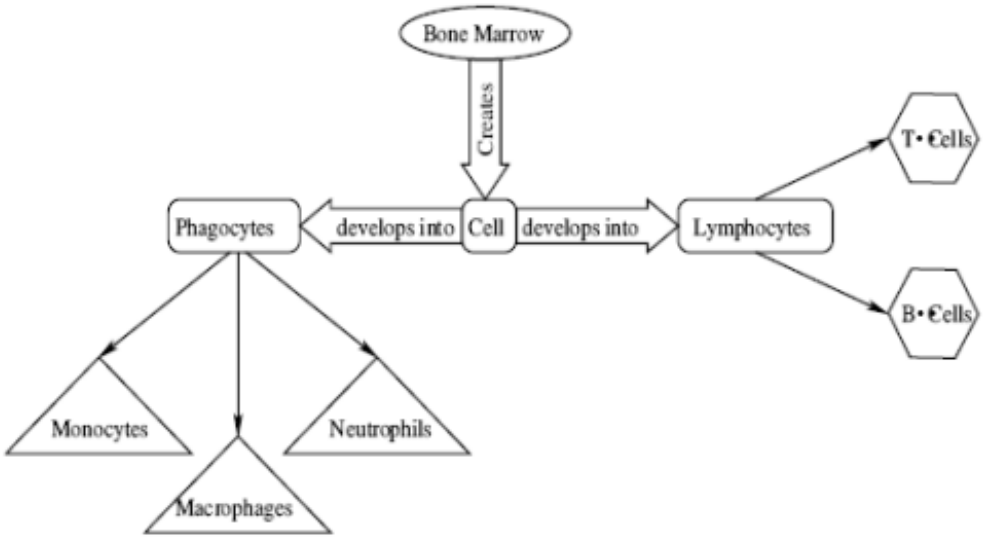


Εικόνα 3Σύμπλεγμα αντιγόνου-αντισώματος [39]

Τα αντισώματα είναι χημικές πρωτεΐνες και αποτελούν μέρος των φυσιολογικών σωματιδίων *(self).* Παράγονται με την επαφή των λεμφοκυττάρων και των αντιγόνων *(nonself).*Ο σχηματισμός του αντισώματος είναιΥ (εικόνα 3) και αποτελείται από μια ελαφριά και μια βαριά πολυπεπτιδική αλυσίδα αντισωμάτων. Οι δύο αλυσίδες διακρίνονται διότι τα αμινοξέα που αποτελούν την βαριά αλυσίδα είναι σε διπλάσιο αριθμό από ότι στην ελαφριά. Το ταίριασμα και η ένωση του αντισώματος με τις επιτομές του αντιγόνου είναι εφικτό σε ποικίλες περιοχές. Μετά την πραγματοποίηση την ένωσης αυτής, ακολουθεί η δημιουργία ενός συμπλόκου αντιγόνου-αντισώματος,που αδρανοποιεί του αντιγόνο. Τα αντισώματα κατηγοριοποιούνται σε 5 ομάδες: IgM, IgG, IgA, IgE, IgD [12].

1.2.5 Λευκά κύτταρα

Η δημιουργία των κυττάρων συντελείται στο μυελό των οστών (εικόνα 4). Ορισμένα κύτταρα εξελίσσονται σε λευκά κύτταρα, τα φαγοκύτταρα. Στα φαγοκύτταρα περιέχονται μονοκύτταρα, μεγάλα φαγοκύτταρα και φαγοκυτταρικά κύτταρα αίματος. Τα μεγάλα φαγοκύτταρα είναι ευμετάβλητα κύτταρα από τα οποία εκκρίνονται ισχυρά χημικά διαδραματίζοντας σημαντικό ρόλο στην ενεργοποίηση των Τ κυττάρων.Άλλα κύτταρα εξελίσσονται σε μικρά λευκά κύτταρα που είναι γνωστά ως λεμφοκύτταρα.

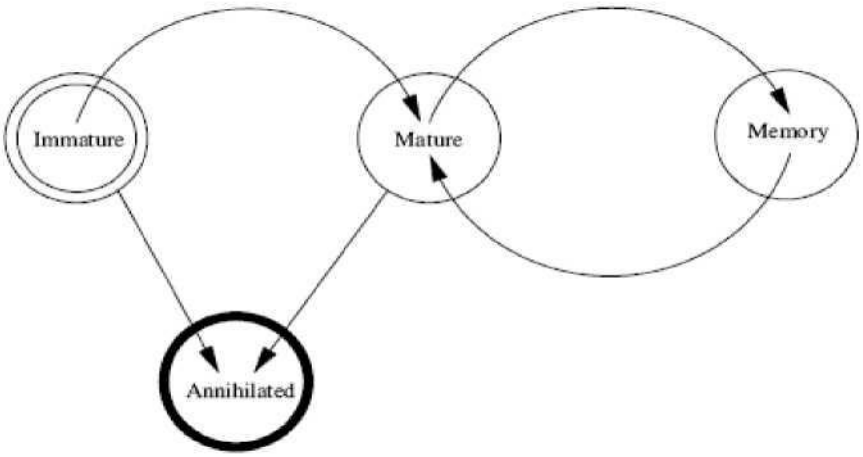


Εικόνα 4Τύποι των λευκών κυττάρων [12]

1.2.6 Λεμφοκύτταρα

Τα λεμφοκύτταρα είναι δύο ειδών: τα Τ-κύτταρα και τα Β-κύτταρα.Μέσω των υποδοχέων που βρίσκονται στην επιφάνειά τους ενώνονται με άλλα κύτταρα. Τα Τ-κύτταρα,αφού ωριμάσουν στον θύμο αδένα, ενώνονται με σωματίδια που βρίσκονται στην επιφάνεια άλλων κυττάρων. Τα Β-κύτταρα είναι έτοιμα αφού δημιουργηθούν στον μυελό των οστών. Για την ωρίμανση ενός Τ-κυττάρου είναι απαραίτητοι οι υποδοχείς για την ένωσή τους με μόρια τα οποία αναπαριστούν φυσιολογικά κύτταρα *(self).*Τα λεμφοκύτταρα εμφανίζονται σε διαφορετικές φάσεις: ώριμα, ανώριμα, λεμφοκύτταρα μνήμης (στην εικόνα 5 φαίνεται ο κύκλος ζωής των λεμφοκυττάρων).

Τα Τ και Β κύτταρα εκκρίνουν λεμφοκίνες, ενώ τα μεγάλα φαγοκύτταρα εκκρίνουν μονοκίνες. Οι πρωτεΐνες αυτές είναι γνωστές και ως κυτταροκίνες, οι οποίες συμβάλλουν στο να αναπτυχθούνκαι να ενεργοποιηθούν τακύτταρα ή να καταστρέφουν ορισμένα κύτταρα-στόχοι [12].

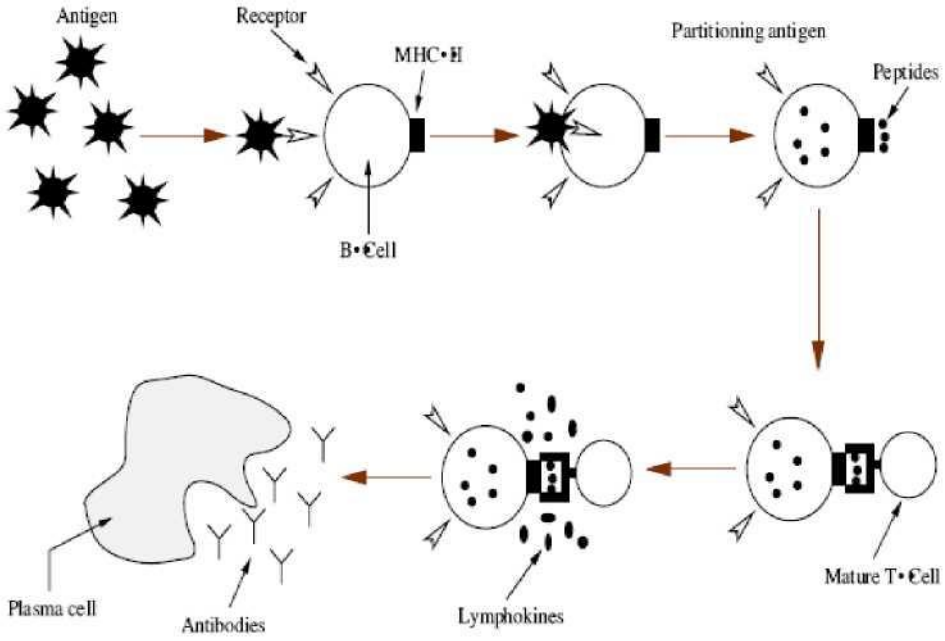


Εικόνα 5Κύκλος ζωής των λεμφοκυττάρων [12]

1.2.7 Τα Β-κύτταρα

Τα Β-κύτταρα δημιουργούνται στο μυελό των οστών με μονομερείς IgMυποδοχείς στην επιφάνεια τους. Ένας μονομερής υποδοχέας είναι ένα χημικό συστατικό το οποίο υφίσταται μια χημική αντίδραση με άλλα μόρια προκειμένου να δημιουργηθούν μεγαλύτερα μόρια. Τα Β-κύτταρα υπάρχουν κυρίως σε σημεία όπου είναι εφικτή η μετατροπή τους σε κύτταρα πλάσματος, εφόσον έχει προηγηθεί η επαφή τους με τα αντιγόνα. Τα σημεία αυτά είναι η σπλήνα και οι αμυγδαλές. Στη συνέχεια, από τα κύτταρα πλάσματος παράγονται αντισώματα που δρουν αποτελεσματικά ενάντια στα αντιγόνα.

Οι υποδοχείς των Β-κυττάρων είναι ειδικοί στην αναγνώρισητων αντιγόνων. Κατά την επαφή των αντιγόνων με τα Β-κύτταρα, τα Β-κύτταρα αρχίζουν να κλωνοποιούνται. Την διαδικασία αυτή ενισχύουν και τα βοηθητικά Τ-κύτταρα. Κατά τη διάρκεια της κλωνοποίησης προκύπτουν δυο τύποι κυττάρων: τα κύτταρα πλάσματος και τα κύτταρα μνήμης. Τα κύτταρα μνήμης εξαπλώνονται στα κύτταρα πλάσματος για τη διασφάλιση της γρήγορης αντίδρασηςαπέναντιστα αντιγόνα και παράγουναντισώματα για τα αντιγόνα [12].



Εικόνα 6Τα Β-κύτταρα μετατρέπονται σε κύτταρα πλάσματος παράγοντας αντισώματα [8]

1.2.8 Μνήμη του ανοσοποιητικού συστήματος

Κατά την αντιμετώπιση ενός αντιγόνου από το ανοσοποιητικό σύστημα για πρώτη φορά, προκαλείται μια πρωταρχική απόκριση στο προσαρμοστικό ανοσοποιητικό σύστημα, δοκιμάζοντας ο οργανισμός μια μόλυνση και μαθαίνοντας το ανοσοποιητικό σύστημανα αναγνωρίζει το αντιγόνο. Αντιδρώντας ο οργανισμός στην εισβολή, παράγει ένα πλήθος από αντισώματα, που θα βοηθήσουν να απομακρυνθεί το παθογόνο από το σώμα. Μετά την εξάλειψη της μόλυνσης,διατηρείταιμια μνήμη των επιτυχών υποδοχέων ώστε να αποκριθούν πιο γρήγορα σε περίπτωση εισβολής των ίδιων ή άλλων παρόμοιων παθογόνων στο σώμα.

Κατά την δευτερογενή απόκριση, τα σχετικά αντισώματα παράγονται πιο γρήγορα και σε πιο μεγάλο αριθμό σε σχέση με την αρχική απόκριση. Σε περίπτωση αντιμετώπισης παρόμοιας παραλλαγής του παθογόνου αργότερα, τη δευτερογενής απόκριση μπορεί να προκαλέσει ένα αντίσωμα στο αρχικό αντιγόνο, το οποίο ταιριάζει αρκετά με τα διαφοροποιημένα αντιγόνα του νέου παθογόνου. Επομένως,η αντιμετώπιση μιας μεταλλαγμένης έκδοσης του αρχικού παθογόνου σημαίνει πως βάσει της προηγούμενης γνώσης του το ανοσοποιητικό σύστημα έχει ήδη προσαρμοστείσε ένα βαθμό ώστε να το αντιμετωπίσει. Αυτή είναι η έννοια που κρύβεται πίσω από τη διαδικασία της

ανοσοποίησης ενάντια σε μια ασθένεια που χρησιμοποιεί μια μη-επιβλαβή παραλλαγή της ίδιας της ασθένειας.

Σχετικά με τον ακριβή τρόπο διατήρησης της μνήμης του ανοσοποιητικού συστήματος υπάρχει διαμάχη. Σε γενικές γραμμές όμως, μπορούμε να πούμε ότι διατηρείται στο ανοσοποιητικό σύστημα ένα πλήθος μακρόβιων λεμφοκυττάρων ή κυττάρων μνήμης. Οι εκδοχές μνήμης των Τ και Β κυττάρωνείναι διαφορετικές. Ο λόγος της δημιουργίας των κυττάρων μνήμης είναι η εξασφάλιση της κωδικοποίησης των αποτελεσμάτωντης εκμάθησης του παρελθόντοςστον τρέχοντα πληθυσμό των λεμφοκυττάρων [8].

Κεφάλαιο 2. Συστήματα Ανίχνευσης Επιθέσεων (IDS)

2.1 Ασφάλεια Πληροφοριών

Στη σύγχρονη εποχή, εποχή της τεχνολογίας και της πληροφορίας, οι ηλεκτρονικοί υπολογιστές αποτελούν πλέον αναπόσπαστο μέρος της καθημερινότητας των ανθρώπων, είτε σε επίπεδο εργασίας είτε σε επικοινωνιακό ή ψυχαγωγικό επίπεδο. Είναι λοιπόν, απαραίτητο τα σύγχρονα Πληροφοριακά Συστήματα (ΠΣ), όπως οι βάσεις δεδομένων, τα δίκτυα υπολογιστών κ.α., να παρέχουν τη μεγαλύτερη δυνατή ασφάλεια ώστε να λειτουργούν και να αξιοποιούνται σωστά. Στο σημείο αυτό, σκόπιμος κρίνεται ο ορισμός της έννοια της Ασφάλειας Πληροφοριών (ΑΠ).

Η Ασφάλεια Πληροφοριών (ΑΠ) αφορά την προστασία της πληροφορίας και των Πληροφοριακών Συστημάτων από το να αλλοιωθεί, να καταστραφεί ή να μετατραπεί λόγω μη-εξουσιοδοτημένης πρόσβασης-χρήσης [13]. Έτσι, λαμβάνονται μέτρα προκειμένου να προληφθούν, να ανιχνευθούν και να αντιμετωπιστούν ενδεχόμενες φθορές. Σύμφωνα με την Denning (1982), η ΑΠ αποτελεί μια προσπάθεια διασφάλισης των δεδομένων μέσω της μυστικότητας-προστασίας τους και της διατήρησης της αυθεντικότητας-ακεραιότητάς τους [14]. Λίγο αργότερα, το 1995, ο Neumann αναφέρεται στην ΑΠ με την έννοια ότι απουσιάζουν οι κίνδυνοι και τα ανεπιθύμητα γεγονότα που μπορεί να προκύψουν από κακόβουλη χρήση. Η προσέγγιση της Denning συμπληρώνεται από τους Pfleeger και Pfleeger [15], προσθέτοντας ότι διατηρείται η εμπιστευτικότητα και η διαθεσιμότητα των δεδομένων. Ένας ορισμός ακόμα προτείνεται από τον Anderson, αναφερόμενος στην ΑΠ ως «*την επαρκώς ενημερωμένη αίσθηση ότι διασφαλίζουμε το ρίσκο της μετάδοσης πληροφοριών και ο έλεγχος αυτής να βρίσκονται σε ισορροπία*»,αντιλαμβανόμαστε από τον παραπάνω ορισμό ότι ποτέ δεν είναι δυνατή η πλήρης ασφάλεια των Πληροφοριακών Συστημάτων [16].

2.2 Συστήματα Ανίχνευσης Εισβολών

2.2.1. Ευπαθή Συστήματα

Τα Πληροφοριακά Συστήματα είναι ευπαθή από τη φύση τους. Προκειμένου να διασφαλιστούν, απαιτείται μια διαδικασία δύσκολη και δαπανηρή. Ο σχεδιασμός συστημάτων τα οποία δύσκολα προσβάλλονται από επιθέσεις, δεν είναι εύκολος στα σημερινά δίκτυα όπως και στο διαδίκτυο. Για την υποστήριξη των ολοένα αυξανόμενων απαιτήσεων του κοινού, παρατηρείται διαρκής εμφάνιση νέων τεχνολογιών, νέων συστημάτων υλικού και λογισμικού. Δεν είναι δυνατή η πρόβλεψη των αδυναμιών τους εξ αρχής, παρά μόνο αφού κυκλοφορήσουν στο εμπόριο. Επιπλέον, για την αύξηση του κέρδους, παρατηρείται από πολλούς οργανισμούς η ελλιπής διάθεση επαρκών πόρων για την ασφάλεια των συστημάτων, δίνοντας προτεραιότητα στην λειτουργικότητά τους. Τέλος,λόγω των λαθών των προγραμματιστών και των μηχανικών ανάπτυξης λογισμικού [18], ο ανθρώπινος παράγοντας αποτελεί έναν σημαντικό παράγοντα των αδυναμιών των ΠΣ.
Το σύνολο των παραγόντων των σχετικών με την ασφάλεια των ΠΣ και των δικτύων, καθιστά σαφές πως δεν είναι η απόλυτη διασφάλισή τους. Η συνεχής ανακάλυψη νέων επιθέσεων μπορεί να προκαλέσει ευπάθειες ακόμη και στα συστήματα που έχουν σχεδιαστεί με μεγάλη προσοχή. Χαρακτηριστικά αναφέρεται ότι ο μοναδικός τρόπος διασφάλισης ενός συστήματος είναι τα τεθεί εκτός λειτουργίας [18]! Επομένως, είναι απαραίτητος ένας τρόπος ώστε να είναι δυνατή η ανίχνευση και ταυτοποίηση των όποιων αδυναμιών και ενδεχόμενων επιθέσεων των ΠΣ.

2.2.2. Ιστορική αναδρομή - Ορισμός IDS

Υπάρχουν αποτελεσματικοί τρόποι αντιμετώπισης όλης της μη εξουσιοδοτημένης χρήσης, της κακής χρήσης και κατάχρησης του συστήματος υπολογιστών. Πολλοί ερευνητές έχουν καταβάλει προσπάθειες. Ο Anderson [19] επεσήμανε για πρώτη φορά το πρόβλημα Ανίχνευσης Εισβολής υπολογιστών (ID) το 1972. Στη συνέχεια, πρότεινε την έννοια του IDS το 1980 [20] η οποία ήταν ένα από τα πρώτα έργα στην ID. Μεταξύ 1984 και 1987, ο Denning πρότεινε για πρώτη φορά ένα μοντέλο IDS [21]. Αυτό το πρωτότυπο ονομάστηκε Ειδικό Σύστημα Ανίχνευσης Εισβολής (IDES). Το 1990 είναι

ένα σημείο καμπής στην ιστορία ανάπτυξης του IDS. Αυτή τη χρονιά ο Heberlein ανέπτυξε την παρακολούθηση της ασφαλείας του δικτύου - Network Security Monitor (NSM) [22]. Τότε, το IDS χωρίστηκε σε δύο ομάδες: IDS με βάση το δίκτυο (NIDS) και host based IDS με βάση τον κεντρικό υπολογιστή (HIDS).

Κύριος στόχος του IDS είναι η παρακολούθηση των δραστηριοτήτων του ΠΣ ή της κίνησης του δικτύου, για την αναφορά πιθανών προσπαθειών επίθεσης, καθώς και η προσπάθεια ταυτοποίησής τους και προσπάθεια ανάλογης αντίδρασης.

Σύμφωνα με τον Heady,η έννοια της *επίθεσης* αφορά τις ενέργειες εκείνες που έχουν ως στόχο την καταπάτηση κάποιου μέλους της τριάδας CIA (εμπιστευτικότητα, ακεραιότητα ή διαθεσιμότητα ενός πόρου συστήματος), που αναφέρθηκε πιο πάνω [23]. Πιο παλιά, με την ίδια έννοια χρησιμοποιούνταν ο όρος *απειλή* από τον Anderson, που την όριζε ως την πιθανότητα μη-εξουσιοδοτημένης προσπάθειας για την απόκτηση πρόσβασης σε πληροφορίες, τη μεταχείριση πληροφοριών ή την καταστροφή της αξιοπιστίας ενός συστήματος [24].

Με τον όρο α*νίχνευση επιθέσεων,* περιγράφεται η διαδικασία με την οποία παρακολουθούνται γεγονότα - συμβάντα σε ένα ΠΣ ή δίκτυο και αναλύονται για πιθανές απειλές [8]. Η διαδικασία αυτή πραγματοποιείται από ένα λογισμικό που ονομάζεται *Σύστημα Ανίχνευσης Εισβολών* (IDS) [25].

Πλέον, η Ανίχνευση Εισβολής (ID) είναι ένα φλέγον θέμα στον τομέα της ασφάλειας των υπολογιστών και πολλά πρότυπα έχουναναπτυχθεί χρησιμοποιώντας διαφορετικές προσεγγίσεις. Βέβαια η παρούσα εργασία ειδικεύεται στις ID μεθόδους χρησιμοποιώντας Τεχνητό Ανοσοποιητικό Σύστημα (AIS).

2.2.3. Ταξινόμηση των IDS

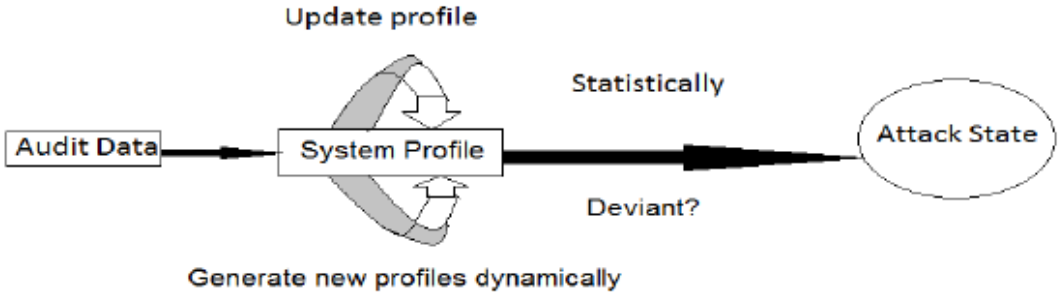
Η ταξινόμηση των IDS, για την καλύτερη περιγραφή και εξήγηση των ιδιαιτεροτήτων των ΠΣ, γίνεται αναλόγως του τρόπου που λειτουργούν. Η αρχική κατηγοριοποίηση γίνεται βάσει των μεθόδων ανίχνευσης και έπειτα βάσει των χαρακτηριστικών του συστήματος [26].

2.2.3.1.Ταξινόμηση βάσει της μεθόδου ανίχνευσης

Με βάση των τρόπο ανίχνευσης μιας επίθεσης, η ταξινόμηση των IDS γίνεται σε συστήματα ανίχνευσης ανωμαλιών (anomaly detection) και σε συστήματα υπογραφής (signature-based). [51]

2.2.3.2.Συστήματα ανίχνευσης ανωμαλιών

Τα *συστήματα ανίχνευσης ανωμαλιών* (anomaly detection)χαρακτηρίζουν ως ανωμαλίες τις δραστηριότητες που διαφοροποιούνται σημαντικά από κάποια κανονικώς αποδεκτά προφίλ χρήσης του συστήματος ή του δικτυακού πόρου (π.χ. μεγάλες αποκλίσεις στον αριθμό των εντολών που εκτελούνται από κάποια συνεδρία χρήστη σε σχέση με αυτόν που συνήθως παρατηρείται) [51]. Δεδομένου ότι δεν απαιτείται εκ των προτέρων γνώση σχετικά με τα είδη των πιθανών εισβολών, είναι δυνατή η ανίχνευση νέων εισβολών. Η μέθοδος αυτή, χρησιμοποιεί κυρίως τεχνικές βασισμένες σε τεχνικές μηχανών εκμάθησης (machine learning, ML) και ορισμένες φορές σε στατιστικές διαδικασίες. Η παρατήρηση των δραστηριοτήτων του συστήματος με τα συστήματα ανίχνευσης ανωμαλιών, οδηγεί στον προσδιορισμό του τι είναι φυσιολογικό χτίζοντας ένα μοντέλο βασισμένο στις παρατηρούμενες, φυσιολογικές συμπεριφορές.Η εκμάθηση μπορεί να γίνει με τεχνικές όπως τα νευρωνικά δίκτυα (artificial neural network, ANN) [27] ή τα μοντέλα Markov (hidden Markov model, HMM) [28].



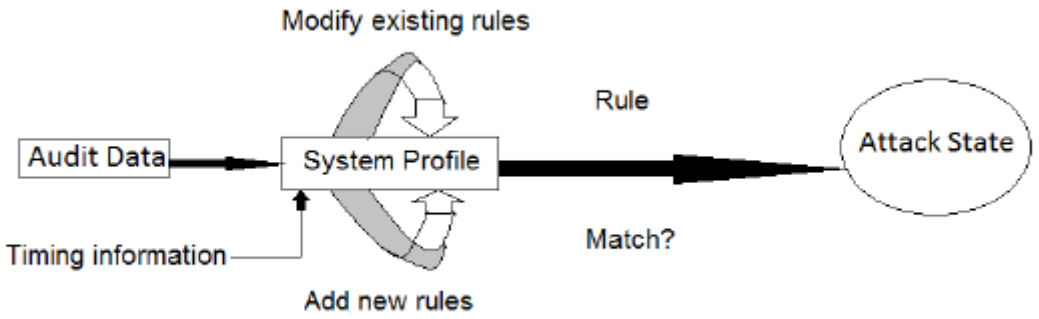
Εικόνα 7. Σύστημα ανίχνευσης ανωμαλιών

Στην εικόνα 10, φαίνεται η συνεχής ανανέωση των προφίλ συμπεριφορών του συστήματος και μετά τη συλλογή των δεδομένων, λαμβάνεται η στατιστική απόφασηγια το αν ακολουθείται η φυσιολογική συμπεριφορά. [51]

2.2.3.3.Συστήματα ανίχνευσης με υπογραφές

Τα *συστήματα ανίχνευσης με υπογραφές* (signature-based) (Εικόνα 11), κάνουν χρήση των πρότυπων γνωστών επιθέσεων (κανόνες) για το ταίριασμα και την αναγνώριση ενδεχόμενης απόπειρας επίθεσης. Παραδείγματος χάριν, ένα κανόνας θα μπορούσε να είναι ο εξής: «*δεν μπορούμε να έχουμε πάνω από 4 λάθος προσπάθειες εισόδου (login) σε χρονικό διάστημα 2 λεπτών*».

Με τον κανόνα υποδεικνύεται είτε μια συγκεκριμένη σειρά καταστάσεων που πρέπει να ακολουθείται (state-transition) είτε περιλαμβάνεται μια συμβολοσειρά που πρέπει να υπάρχει στο μήνυμα που ανταλλάσσεται (string matching) [51]. Στα συστήματα αυτά, η πιο σημαντική κατηγορία είναι τα συστήματα εμπειρογνώμονες (experts-system) [29], τα οποία έχουν κανόνες περιγραφής συμπεριφορών επίθεσης, διακρίνονται από ευελιξία και ισχυρή απόδοση αλλά υστερούν στην ταχύτητα.



Εικόνα 8. Σύστημα ανίχνευσης με υπογραφές

2.2.3.4.Ταξινόμηση με βάση τα χαρακτηριστικά του συστήματος

2.2.3.4.1. Χρόνος ανίχνευσης

Οι αναγνωρισμένοι τύποι των IDS είναι δύο: εκείνα που εστιάζουν στην ανίχνευση των επιθέσεων σε πραγματικό χρόνο (real-time) και εκείνα που επικεντρώνονται στην ανάλυση των δεδομένων με κάποια καθυστέρηση και όχι σε πραγματικό χρόνο (non-real-time), αναβάλλοντας την ανίχνευση για κάποιο χρονικό διάστημα [51]. Στην περίπτωση των συστημάτων πραγματικού χρόνου, είναι δυνατή η λειτουργία τους και offline, καθώς έχουν τη δυνατότητα να αποθηκεύουν τα ιστορικά δεδομένα.

2.2.3.4.2. Απόκριση σε ανιχνευμένες επιθέσεις

Στην περίπτωση αυτή, τα IDS διακρίνονται στα *ενεργά IDS* (active IDS) και στα *παθητικά IDS* (passive IDS). Με τα παθητικά IDS επιτυγχάνεται ανίχνευση της επίθεσης και ειδοποίηση για την ύπαρξή της, δίχως τη λήψη κάποιων μέτρων αντιμετώπισης. Αντιθέτως, τα ενεργά IDS ελέγχουν το σύστημα που δέχεται επίθεση προσπαθώντας για την αλλαγή της κατάστασης αυτής, για το μετριασμό των επιπτώσεων της επίθεσης. Έτσι, μπορεί να τερματιστούν διεργασίες, η επικοινωνία σε ένα δίκτυο κλπ.

Καθώς τα παθητικά IDS εξελίχθηκαν στα ενεργά IDS, εισήχθη η έννοια του *Συστήματος Πρόληψης Εισβολών* (Intrusion Prevention System, IPS). Πρόκειται για ένα λογισμικό με τις ικανότητες ενός Συστήματος Ανίχνευσης Εισβολών, προσπαθώντας επιπλέον να σταματήσει πιθανές απειλές [30]. Σήμερα, στην πλειοψηφία των συστημάτωνοι δύο λειτουργίες είναι συνδεδεμένες και γίνεται πλέον λόγος για *IntrusionDetectionandPreventionSystem*(IDPS).

2.2.3.4.3. Προέλευση των δεδομένων ανάλυσης

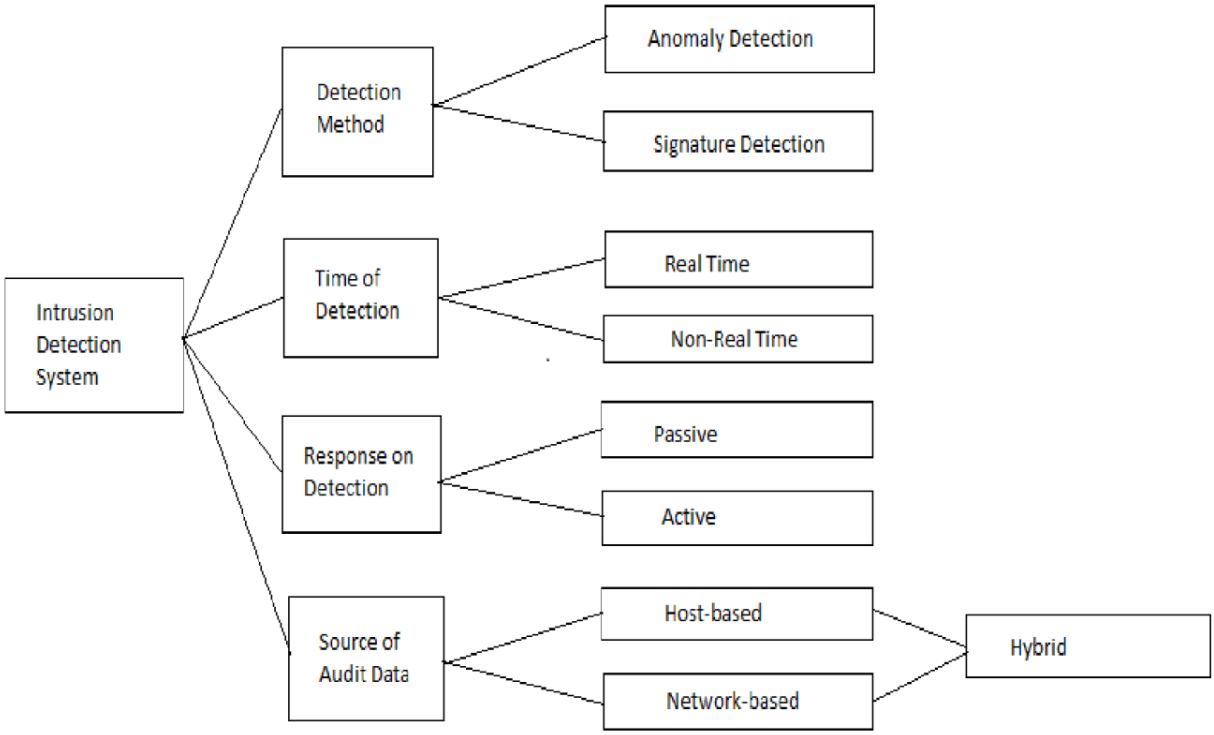
Η βασικότερη κατηγοριοποίηση των IDSαφορά την προέλευση των δεδομένων. Με τα *Host-based IDS* (HIDS) γίνεται παρακολούθηση αρχείων και καταχωρήσεων σε αυτόνομους υπολογιστές, ενώ με τα *Network-based IDS* (NIDS) καταγραφή της κίνησης ενός δικτύου. [51]

Τα HIDS είναι τα πρώτα συστήματα ανίχνευσης που ερευνήθηκαν. Πιο παλιά, πριν από την ύπαρξη των δικτύων υπολογιστών, στόχος των εργαλείων ανίχνευσης ήταν απλοί υπολογιστές με συγκεκριμένους χρήστες. Επομένως, η διαδικασία ήταν αρκετά απλή λόγω των μειωμένων κινδύνων. Η συλλογή των πληροφοριών από ένα HIDS περιλαμβάνει το σύνολο των δεδομένων του εγκατεστημένου Λειτουργικού Συστήματος και των δεδομένωντων δραστηριοτήτων των χρηστών του. Η προέλευση των εντολών αυτών μπορεί να είναι είτε οι εντολές του συστήματος είτε οι πόροι του (μνήμη, χρόνος επεξεργαστή, χρήση δίσκων, χρησιμοποιούμενες εφαρμογές) [30].

Καθώς τα δίκτυα υπολογιστών αναπτύχθηκαν και χρησιμοποιούνταν ολοένα και περισσότερο το Ίντερνετ, προτεραιότητα των IDS αποτέλεσαν οι επιθέσεις στο δίκτυο. Έτσι, εισήχθη η έννοια του NIDS. Το γεγονός πως δεν ήταν δυνατή η ανίχνευση ορισμένων επιθέσεων με την εξέταση αποκλειστικά των δεδομένων του υπολογιστή,

οδήγησε στη δημιουργία εργαλείων (sniffers) για την παρατήρηση των πακέτων του δικτύου σε πραγματικό χρόνο και την ανίχνευση πιθανών εισβολών. Με τα NIDSo διαχειριστής του συστήματος/δικτύου έχει τη δυνατότητα επιλογής στρατηγικών θέσεων για να τα εγκαταστήσει. Επιπλέον, με τη χρήση λίγων κόμβων NIDS είναι δυνατή η κάλυψη των περισσότερων επιθέσεων στο δίκτυο. Στην περίπτωση αυτή, οι πληροφορίες που θα αναλυθούν είναι διευθύνσεις δικτύου (IP addresses), πίνακες δρομολόγησης (routing tables), μετρήσεις από την κίνηση του δικτύου, διάφορα δεδομένα από τα πακέτα δικτύου κλπ. [30].

Τέλος, υπάρχει και η κατηγορία των *υβριδικών IDS* (Hybrid-IDS). Πρόκειται για συνδυασμό της λειτουργικότητας του HIDS με του NIDS. Τα υβριδικά IDS αναλύουν την κίνηση και τις εισερχόμενες ή εξερχόμενες πληροφορίες του δικτύου σε κάθε αυτόνομο υπολογιστή που έχει εγκατασταθεί στο δίκτυο [30].



Εικόνα 9. Ταξινόμηση του IDS [51]

2.3. Εξέλιξη της τεχνολογίας IDS

Οι πιο μεγάλοι προμηθευτές IDS/IPS, σύμφωνα με έρευνα του 2009 [36], είναι οι Cisco, McAfee, Juniper, IBM, Sourcefire και TippingPoint, σύμφωνα με διάφορα κριτήρια (σχέση τιμής-απόδοσης, μελλοντικό πλάνο, κ.α.) που τέθηκαν από μεγάλους οργανισμούς. Από άποψη αποδοτικότητας, στην κορυφή βρίσκονται οι Cisco και IBM. Το πιο σημαντικό στοιχείο που εξελίχθηκε στην τεχνολογία ανίχνευσης επιθέσεων είναι η μετάβαση από τα παθητικά IDS (απλή παρακολούθηση και ανάλυση των επιθέσεων που δεχόταν το σύστημα) στα ενεργά, προληπτικά IPS. Πλέον, υπάρχει στην περίμετρο του δικτύου μια ασπίδα και στο εσωτερικό του προστατεύεται ξεχωριστά κάθε κόμβος. Ακόμη, στα σημερινά IPS είναι δυνατή η λειτουργία σε πιο μεγάλες ταχύτητες και η συμπερίληψη επιπλέον μηχανισμών για να αναγνωρίζονται οι επιθέσεις, εκτός από τους απλούς κανόνες υπογραφής, δίχως να απαιτείται διακοπή συνδέσεων για την αντιμετώπισή τους.

Η **Cisco,**μέσω του *IPS Sensor Software,*δίνει αρκετές επιλογές από IPS. Ένα μέλος του Cisco Self-Defending Network, η σειρά αισθητήρων (καταγραφείς/γεννήτριες γεγονότων) *IPS 4200 Series Sensors* προσφέρειπροστασία εναντία σε σκουλήκια, δούρειους ίππους και άλλες επιθέσεις εφαρμογών και λειτουργικών συστημάτων. Διαθέτει φίλτρα με πάνω από 300 υπογραφές και 30 μηχανές ανίχνευσης, προστατεύοντας πάνω από 30.000 γνωστές απειλές. Βρίσκεται στην κορυφή της ανίχνευσης με υπογραφές.

Το *IBM Protocol Analysis Module* της **IBM,**αποτελεί το κλειδί στην απόδοση του Proventia IPS,υποστηρίζοντας ανάλυση πακέτων δικτύου σε βάθος. Προσφέρει προστασία από απειλές, όπως επιθέσεις Ιστού, επιθέσεις εντός του συστήματος (insider threats) και από κακόβουλο λογισμικό (malware). Κύριο πλεονέκτημα είναι ότι ανανεώνεται συνεχώς για νέες απειλές από την ομάδα ανάπτυξης X-Force.

Σε υψηλό επίπεδο βρίσκεται και η **Juniper Networks,**με το σχεδιασμό ενός IPS που μπορεί να προσφέρει ασφάλεια είτε σε αυτόνομα συστήματα είτε σε ολόκληρα δίκτυα, συνδυάζοντας τη λειτουργικότητα των HIDS με αυτή των NIDS. Το συγκεκριμένο IPS μπορεί να συνυπάρξει και με άλλα λογισμικά ασφαλείας. Μπορεί ακόμη, να επικυρώσει πρωτόκολλα επικοινωνίας και να παρακολουθεί επιλεκτικά την κίνηση του δικτύου, ενώ πολύ σημαντική είναι η δυνατότητα υψηλού ελέγχου. Εξελίσσοντας τα συστήματα που αγόρασε από την Netscreen Technologies στην ανάπτυξη της πλατφόρμας *JUNOS,*της επέτρεψε να παραμείνει σε υψηλό επίπεδο στην αγορά των IDS/IPS.

Η αγορά του *IntruShield IDS* από την **McAfee,**της έδωσε άλλη ώθηση στις αγορές με το *McAfee Network Security Platform* (NSP). Όλοι οι IPS κόμβοι διαχειρίζονται κεντρικά και μπορούν ταυτόχρονα να εγκατασταθούν μέχρι και 1000 αισθητήρες.

Η **Sourcefire** είναι γνωστή κυρίως για το *Snort IDS* [37]. Είναι ένα ελαφρύ εργαλείο για TCP/IP δίκτυα, που δεν απαιτεί να εγκατασταθούν επιπρόσθετοι εμπορικοί αισθητήρες (μείωση κόστους). Το Snort είναι μια μηχανή ανίχνευσης και πρόληψης ανοιχτού κώδικα και για αυτό το λόγο έγινε ευρέως αποδεκτό από την φοιτητική και την επιστημονική κοινότητα. Είναι ιδιαίτερα προσαρμόσιμο, και οι κανόνες του μπορούν να προσαρμοστούν στο εκάστοτε είδος δικτύου που προστατεύει. Σημαντικό πλεονέκτημα του Snort είναι η συνεισφορά που δέχεται από τις κοινότητες ανοικτού κώδικα, οι οποίες το προμηθεύουν συνεχώς με ενημερώσεις. Το Snort είναι από τα πλέον επεκτάσιμα IDS/IPS με βιβλιοθήκη 14.000 κανόνων και αποτελεί το IDS με το ασχολείται η παρούσα εργασία. Σε επόμενο Κεφάλαιο (μετά την παρουσίαση της γενικότερης λειτουργίας του Snort), θα αναλυθεί η δυνατότητα επέκτασής του, προσφέροντας έτσι τη δυνατότητα δημιουργίας ενός υποπρογράμματος για το Snort, το οποίο αναγνωρίζει επιθέσεις τύπου Slow HTTP DoS. [38]

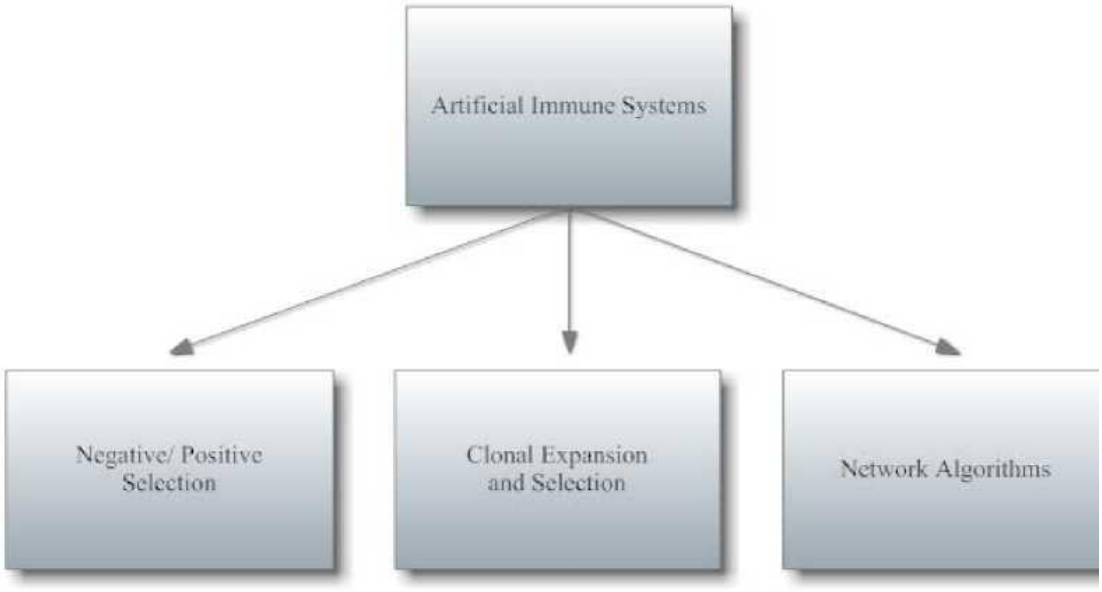
Τέλος,υπάρχει και το IPS της TippingPoint (ανήκει στην 3Com από το 2005) [36]. Βασικό χαρακτηριστικό του είναι ότι μπορεί να προστατεύει από άγνωστες επιθέσεις (zero-day attacks) χάρη στο μεγάλο πλήθος από ανεξάρτητους ερευνητές. Ακόμη, διαθέτει φίλτρα που μπλοκάρουν επιθέσεις πολλαπλών-συνδυασμένων ειδών (συνήθως πρόκειται για νέα είδη απειλών). [38]

Κεφάλαιο 3. Το τεχνητό ανοσοποιητικό σύστημα

Στο παρόν κεφάλαιο γίνεται μία γενική αναφορά στα τεχνητά ανοσοποιητικά συστήματα (AIS) αναλύοντας τα βασικά μοντέλα και τους βασικούς αλγορίθμους των AIS.

3.1. Εισαγωγή

ΤαAIS σχεδιάζονται με στόχο όχι να αναπαραγάγουν πιστά τα μοντέλα του φυσικού ανοσοποιητικού συστήματος, αλλά να εξάγουν ιδέες από τον τρόπο που λειτουργεί το φυσικό ανοσοποιητικό σύστημα, οι οποίες ιδέες μπορούν να συμβάλουν στην επίλυση πραγματικών προβλημάτων. Υπάρχουν τρεις κατηγορίες AIS, όπως φαίνεται στο σχήμα που ακολουθεί (Εικ.7), αναλόγωστων διακριτών χαρακτηριστικών του τεχνητού ανοσοποιητικού συστήματος [8].



Εικόνα 10. Ταξινόμηση των AIS αλγορίθμων

3.2 Μοντέλα του τεχνητού ανοσοποιητικού συστήματος

Οι θεωρίες που αναλύθηκαν στο κεφάλαιο1 σχετικά με τη λειτουργική και οργανωτική συμπεριφορά του φυσικού ανοσοποιητικού συστήματος (NIS), ενέπνευσαν τη μοντελοποίηση του φυσικού ανοσοποιητικού συστήματος στο τεχνητό ανοσοποιητικό σύστημα και την εφαρμογή του σε μη βιολογικά περιβάλλοντα [52]. Παρακάτω αναφέρονται περιληπτικά οι ικανότητες του φυσικού ανοσοποιητικού συστήματος τις οποίες εκμεταλλεύεται το τεχνητό ανοσοποιητικό σύστημα [39]:

- Το NISχρειάζεται να γνωρίζει μόνο τα φυσιολογικά κύτταρα (self)
- Η ικανότητα τουNISδιαχωρισμού των φυσιολογικών(self) από τα ξένα κύτταρα (nonself)
- Ο χαρακτηρισμός ενόςξένουκυττάρουως επιβλαβές ή μη επιβλαβές
- Η ικανότητα κλωνοποίησης και μετάλλαξης των λεμφοκυττάρων για την προσαρμογή τους με τα ξένα κύτταρα που αντιμετωπίζει ο οργανισμός
- Η συμβολή των κυττάρων μνήμης στο να αντιδράσει γρήγορα ο οργανισμός απέναντι σε αντιγόνα έχει ήδη αντιμετωπίσει
- Η συνεργασία ανάμεσα στα λεμφοκύτταρα δημιουργεί ένα δίκτυο λεμφοκυττάρων

Ακολουθεί η ανάλυση ορισμένων υπαρχόντων τεχνητών ανοσοποιητικώνσυστημάτων. Βασιζόμενα στοφυσικό ανοσοποιητικό σύστημα, τα μοντέλα αυτά καταφέρνουν την υλοποίηση ορισμένων ή όλων των βασικών εννοιών του τεχνητού ανοσοποιητικού συστήματος.

3.2.1. Αλγόριθμος για το τεχνητό ανοσοποιητικό σύστημα

Οι κύριες ικανότητες του φυσικού ανοσοποιητικού συστήματος είναι η εσωτερική λειτουργία και η συνεργασία των ώριμων Β και Τκυττάρων, που ευθύνονται για την έκκριση αντισωμάτων ως αντίδραση του συστήματος στα αντιγόνα [52]. Η ικανότητα διάκρισης, που έχουν τα ώριμα Τ- κύτταρα, ανάμεσα στα φυσιολογικά και τα ξένα κύτταρα προσδίδει στο φυσικό ανοσοποιητικό σύστημα την ικανότητα εντοπισμού των ξένων κυττάρων.

Μετά τη δέσμευση ενός αντιγόνου από τον υποδοχέα του Β-κυττάρου, ακολουθεί ο διαχωρισμός και η μεταφορά του στην επιφάνεια με ένα ΜΗΣμόριο.Η δέσμευση του ΜΗΣμορίουστην επιφάνεια του Β- κυττάρου γίνεται με κάποια συγκεκριμένη έλξη από τονυποδοχέα του Τ-κυττάρου. Η έλξη μπορεί να θεωρηθεί σαν ένα μέτρο του πλήθους των λεμφοκίνων, που εκκρίνονται από το Τ-κύτταρο για την κλωνοποίηση του Β-κυττάρου σε ένα κύτταρο πλάσματος, το οποίο θα μπορεί να παράγει αντισώματα [52].

Η συχνή μετατροπή των Β-κυττάρων σε κύτταρα πλάσματος δημιουργεί τημνήμη του φυσικού ανοσοποιητικού συστήματος για τα αντιγόνα που αντιμετωπίζει πιο συχνά. Έτσι, για τη μοντελοποίηση ενός τεχνητού ανοσοποιητικού συστήματος χρειάζεται να ληφθούν υπόψη οι ακόλουθες βασικές έννοιες:

- Εκπαιδευμένοι ανιχνευτές (τεχνητά λεμφοκύτταρα) είναι ικανοί στον εντοπισμό των ξένων προτύπων με κάποια συνάφεια.
- Για την εκπαίδευση των τεχνητών λεμφοκυττάρων (ALCs) ώστενα αποκτήσουν ανοχή, είναι ίσως απαραίτητη η ύπαρξη στο τεχνητό ανοσοποιητικό σύστημα ενός καλού αποθέματος φυσιολογικών και ξένων προτύπων.
- Η μέτρηση της συνάφειας ανάμεσα σε ALCκαι ένα πρότυπο είναι απαραίτητη ώστε να εντοπιστεί ο βαθμός αναγνώρισης ενός προτύπου από έναALC.
- Για να μπορέσει να μετρηθεί η συνάφεια θα πρέπει η δομή τωνπροτύπων και των ALCs να είναι ίδια.
- Είναι απαραίτητη και η μέτρηση της συνάφειασμεταξύ δυο ALCs, ώστε να εντοπιστεί ο βαθμός σύνδεσηςενός ALCμε κάποιο άλλο για τον σχηματισμό ενός δικτύου.
- Τα τεχνητά λεμφοκύτταρα δημιουργούν τη μνήμη του τεχνητού ανοσοποιητικού συστήματος για την αναγνώριση των μη φυσιολογικών προτύπων.
- Μετά τον εντοπισμό μη φυσιολογικών προτύπων από ένα ALC, ακολουθεί η κλωνοποίησή τους και η μετάλλαξη των κλώνων ώστε να αποκτηθούν περισσότερες λύσεις.

Με οδηγό τις παραπάνω έννοιες, επιχειρείται να μοντελοποιηθεί ένα βασικό τεχνητό ανοσοποιητικόσύστημα. Ακολούθως αναλύονται συνοπτικά τα μέρη του αλγορίθμου [39].

Αλγόριθμος 1. Βασικό τεχνητό ανοσοποιητικό σύστημα

Αρχικοποίησε ένα σύνολο από ALCs σαν τον πληθυσμό C

Καθόρισε το πρότυπο του αντιγόνου σαν το δείγμα εκμάθησης D_T

Ενώ κάποια συνθήκη δεν είναι αληθής **επανάλαβε**

Για κάθε πρότυπο αντιγόνου $z_p \in D_T$ **επανάλαβε**

Επίλεξε ένα υποσύνολο των ALCs για έκθεση στο σύνολο των z_p, σαν τον πληθυσμό $S \subseteq C$

Για κάθε ALC $x_i \in S$ **επανάλαβε**

Υπολόγισε την συνάφεια μεταξύ των z_p και x_i

τέλος

Επίλεξε ένα υποσύνολο των ALCs με την υψηλότερη συνάφεια σαν τον πληθυσμό $H \subseteq C$

Προσάρμοσε τα ALCs στο σύνολο H με κάποια μέθοδο επιλογής, η οποία θα βασίζεται στην συνάφεια των αντιγόνων είτε στην συνάφεια του δικτύου που έχει υπολογιστεί μεταξύ των ALCs στο σύνολο H

Ενημέρωσε το επίπεδο υποκίνησης (stimulation) για κάθε ALC στο σύνολο H

Τέλος

Τέλος

3.2.2. Κλασική άποψη για τα μοντέλα των AIS

Σύμφωνα με κλασσική άποψη του φυσικού ανοσοποιητικού συστήματος, ένα βασικό χαρακτηριστικό γνώρισμα είναι η ικανότητα των ώριμων T-κύτταρων διάκρισης ανάμεσαστα φυσιολογικάκαι τα ξένα κύτταρα. Ακολουθεί η ανάλυση μοντέλωνAIS, των οποίων βάση ή έμπνευση αποτελεί ηκλασική άποψη γύρω από το φυσικό ανοσοποιητικό σύστημα. Επομένως, τα πρότυπα AISεκπαιδεύουν τα τεχνητά λεμφοκύτταρα (ALCs) για την απόκτηση της ικανότηταςδιάκρισης μεταξύ των

φυσιολογικών και μη φυσιολογικών προτύπων. Αναλύεται η τεχνική της αρνητικής επιλογής, καθώς και διάφορες άλλες τεχνικές μέτρησης οι οποίες καθορίζουν το βαθμό ταιριάσματος μεταξύ ενός ALCκαι ενός φυσιολογικού/ μη φυσιολογικού προτύπου [52].

3.2.3. Αρνητική επιλογή

Στην κλασσική άποψη του φυσικού ανοσοποιητικού συστήματοςβασίστηκε το μοντέλοAISπου εισήχθη από τον Forrest[2]. Σε αυτό το κλασσικό AIS, εισάγεται ως τεχνική εκπαίδευσης η αρνητική επιλογή. Στο συγκεκριμένο μοντέλο, η αναπαράσταση όλων των προτύπων και των ALCs γίνεται ως γνωρίσματα με ονομαστική τιμή ή ως δυαδικές αλληλουχίες. Ο υπολογισμός της συνάφειαςανάμεσα σε έναALCκαι έναπρότυπογίνεται με τη χρήση του κανόνα αντιστοιχίας r-συνεχής, ο οποίος απεικονίζεται στην εικόνα 9. Ο r-συνεχής κανόνας είναι ένας εν μέρει κανόνας ταιριάσματος. Δηλαδή, η ύπαρξη rσυνέχων ή περισσότερων ταιριασμάτων στις αντίστοιχες θέσεις καθορίζει τον εντοπισμό ενός προτύπου από ένα ALC. Ως R ορίζεται ο βαθμός συνάφειας για ένα ALCνα ανιχνεύσει ένα πρότυπο. Στην εικόνα 10, υπάρχουν επτά συνεχείς αντιστοιχίες μεταξύ του ALCκαι του προτύπου. Κατά συνέπεια, εάν r= 4, το ALCταιριάζει με το πρότυπο, εφόσον 7 >r. Εάν r> 7, το ALCδεν ταιριάζει με το πρότυπο. Μια υψηλή τιμή του rυποδεικνύει ισχυρότερη συγγένεια μεταξύ ενός ALCκαι ενός προτύπου [52].

Εικόνα 11. R-συνεχής κανόνας [52]

Μερικά από τα ALCs του μοντέλου αναπαριστούν τα ώριμα T-κύτταρα στο φυσικό ανοσοποιητικό σύστημα. Ένα δείγμα εκπαίδευσης των φυσιολογικών προτύπων χρησιμοποιείται για την εκπαίδευση τουσυνόλου των ALCs με τη χρήση της τεχνικής της αρνητικής επιλογής. Ο αλγόριθμος που ακολουθεί συνοψίζει τη μέθοδο της αρνητικής επιλογής [52].

Αλγόριθμος 2 Εκπαίδευση των ALCs μέσω της αρνητικής επιλογής

Θέσε τον μετρητή n_a σαν το πλήθος των ALCs τα οποία πρόκειται να εκπαιδευτούν

Δημιούργησε ένα κενό σύνολο ALCs, σαν το σύνολο C

Όρισε το δείγμα εκπαίδευσης των φυσιολογικών προτύπων, σαν D_T

ενώ *το μέγεθος του C δεν ισούται με* n_a **επανάλαβε**

Τυχαία δημιούργησε ένα ALC, **x***i*;

Ταίριασμα=ψευδές;

για κάθε φυσιολογικό πρότυπο $z_p \in D_T$

αν η *συνάφεια μεταξύ των* $\mathbf{x}_i$ *και* $\mathbf{z}_p$ *είναι υψηλότερη από το κατώφλι r* **τότε**

Ταίριασμα =αληθές;

διακοπή;

τέλος

τέλος

αν *δεν ταιριάζει* **τότε**

πρόσθεσε το **x***i* στο σύνολο *C*;

τέλος

Τέλος

3.2.4. Εξελικτικές προσεγγίσεις

Η μέθοδος της αρνητικής επιλογής προσεγγίζεται με διαφορετικό τρόπο από τους Kimκαι Bentley[40]. Σύμφωνα με αυτή την προσέγγιση, η δημιουργία και ο έλεγχος των ALCs δεν γίνεται με τυχαίο τρόπο, όπως συμβαίνει στην αρνητική επιλογή, αλλά με τη χρήση μιας εξελικτικής διαδικασίας, με την οποία επιτυγχάνεται η εξέλιξη των ALCs σε μη φυσιολογικά και η διατήρηση της ποικιλίας και της γενικότηταςμεταξύ τωνALCs. Σε ένα άλλο μοντέλο, των Potterκαι DeJong,[41] γίνεταιεφαρμογήενός συν-εξελικτικού γενετικού αλγόριθμου για την εξέλιξη τωνALCsσε μη φυσιολογικάπρότυπα στο δείγμα εκπαίδευσης.

Όταν η εξέλιξη τηςκαταλληλότητας του ALCσυνόλου φτάσει σε σημείο εντοπισμού όλων των μη φυσιολογικώνπροτύπων και όχι τωνφυσιολογικώνπροτύπων, τα

ALCsαναπαριστούν μια περιγραφή της ιδέας. Αν το δείγμα εκπαίδευσης των φυσιολογικών και μη φυσιολογικών προτύπων είναι ‘θορυβώδες’, η εξέλιξη του συνόλου τωνALCθα συμβεί όταν εντοπιστούν τα περισσότερα από τα μη φυσιολογικά πρότυπα και λίγα από το πλήθος των φυσιολογικώνπροτύπων [52].

Η παρουσίαση της μεθόδου της αρνητικής επιλογής για την εκπαίδευση των ALCsεκτιμώντας συνεχώς τα φυσιολογικά πρότυπα, πραγματοποιήθηκε από τον Gonzalez και τους συνεργάτες του [42].Για τη μεγιστοποίηση της κάλυψης των μη φυσιολογικών προτύπων, μιας και είναι επιθυμητή η μικρότερη δυνατή επικάλυψη μεταξύ των ALCs, η εξέλιξη των ALCsξεπερνά το δείγμα εκπαίδευσης των φυσιολογικών προτύπων και διασκορπίζονται αρκετά μεταξύ τους.

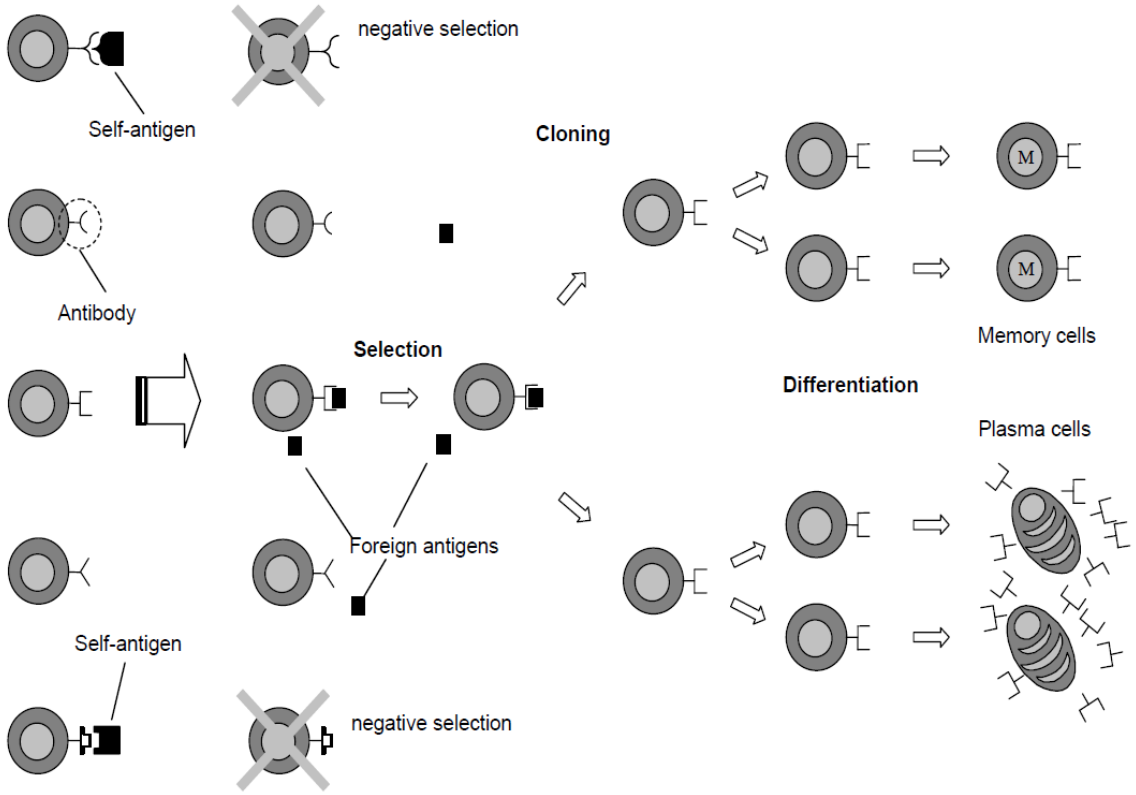
3.2.5. Αλγόριθμος επέκτασης κλώνων και επιλογής

Η θεωρία της επιλογής κλώνων προτάθηκε από τον Burnet(1959), προκειμένου να δοθεί μια εξήγηση για την διαδικασία που τα ανοσοποιητικάκύτταρα πολλαπλασιάζονται όταν εμφανίζεται ένα αντιγόνο. Σύμφωνα με αυτή τη θεωρία, με υπόδειξη ενός αντιγόνου επιλέγεται από το πλήθος των λεμφοκυττάρων ένα συγκεκριμένο λεμφοκύτταρο, για κλωνοποίηση.

Δεδομένου ότι οι υποδοχείς λεμφοκυττάρων βρίσκονται σε μεγάλη ποικιλία, μπορεί να θεωρηθεί πως το αντιγόνο αναγνωρίζεται από τους υποδοχείς τυχαία. Ωστόσο, αφού ενεργοποιηθεί τοσυγκεκριμένο λεμφοκύτταρο, κλωνοποιείται και ακολουθεί η εξάπλωσή του. Η διαδικασία αυτή, κατά την οποία τα Β-λεμφοκυττάρα επιλέγονται από ένα αντιγόνο και κατόπιν εξαπλώνονται με τους κλώνους τους, απεικονίζεται στην εικόνα 9. Οι βασικές ιδιότητες της επιλογής κλώνων είναι οι εξής [43]:

- Οι κλώνοι που αντιδρούν σε φυσιολογικά κύτταρα εξαλείφονται.
- Τα ώριμαλεμφοκύτταρα πολλαπλασιάζονται και διαφοροποιούνται μέσω της αντί-γονικής προσομοίωσης.
- Έναπρότυπο περιορίζεται σε ένα διαφοροποιημένο κύτταρο και διατηρείται από τους απογόνους-κλώνους.
- Νέες γενετικές αλλαγές παράγονται που στη συνεχεία εκφράζονται σαν διαφορετικά πρότυπα αντισωμάτων με την μορφή μιας επισπευσμένης σωματικής μετάλλαξης.

Η επιλογή των κλώνων μελετήθηκε και από άλλους ερευνητές, προκειμένου να γίνει κατανοητός ο τρόπος επιλογής ορισμένων τύπων Β και Τ λεμφοκυττάρων για την εξολόθρευση συγκεκριμένων αντιγόνων που εισβάλλουν στο σώμα.



Εικόνα 12Επέκταση κλώνων (και επιλογή) των Β-κυττάρων κατά την παρουσία ενός αντιγόνου [1, 52]

Ο αλγόριθμος με τον οποίο επιλέγονται και επεκτείνονται οι κλώνοι εμπνέεται από την αντίστοιχη διαδικασία μετάλλαξης των Β-κυττάρων, όταν εντοπίζεται ένα παθογόνο από το ανοσοποιητικό σύστημα. Η διαδικασία επιλογής κλώνων στοχεύει στο να δημιουργηθεί ένα πλήθος από αντισώματα που θα είναι σε μεγάλο βαθμό ταιριαστά με συγκεκριμένα αντιγόνα.

Με την προσαρμογή της παραπάνω έννοιας για τη δημιουργία ενός αλγόριθμου,οι πιθανές λύσεις μπορεί να θεωρηθεί πως είναι τα αντισώματα, τα δεδομένα δοκιμής είναι τα αντιγόνα και η ποιότητα ή καταλληλότητα της λύσης καθορίζεται από τον βαθμό που ταιριάζουν τα αντισώματα και τα αντιγόνα. Σκοπός είναι, ξεκινώντας από έναν αρχικό πληθυσμό, να εφαρμοστεί ο αλγόριθμος με το σύνολο των δεδομένων και να χρησιμοποιηθεί επαναληπτικάγια τη βελτίωση της ποιότητας των λύσεων στον

πληθυσμό. Η μετατροπή της έννοιας της επιλογής κλώνων σε έναν αλγόριθμο βελτιστοποίησης μπορεί να γίνει με πολλούς τρόπους.[44, 52]

Πίνακας 1Αντιστοιχία μεταξύ της επιλογής κλώνων και της βελτιστοποίησης [8]

Ανοσοποιητικό σύστημα	
Συστατικό	**Αντιστοιχία**
Αντίσωμα	Κανόνας, εξίσωση ή πρόγραμμα.
Αντιγόνα	Δεδομένα δοκιμής .
Ταίριασμα αντιγόνου-αντισώματος	Ποιότητα του κανόνα ή του προγράμματος.
Κλωνοποίηση, μετάλλαξη	Δημιουργία ποικιλίας προκειμένου να προκύψουν καλύτερες λύσεις.

Ο ακόλουθος πίνακας 3, παρουσιάζει τις βασικές διαφορές ανάμεσα σε έναν εξελικτικόαλγόριθμο και έναναλγόριθμο επιλογής κλώνων. Όπως φαίνεται, διαφοροποιούνται κυρίως ως προς την χρησιμοποιούμενη τεχνολογία. Στην περίπτωση του αλγόριθμου επιλογής κλώνων, ο μηχανισμός με τον οποίο επιλέγονται τα καταλληλότερααντισώματα βασίζεται στην συνάφεια τους με τα αντιγόνα. Στους εξελικτικούς αλγόριθμους, οι παραδοσιακοί μηχανισμοί επιλογής που χρησιμοποιούνται έχουν την ικανότητα προσαρμογής για την εφαρμογή τους και στους αλγορίθμους επιλογής κλώνων. Η επιλογή ενός ατόμου στους εξελικτικούς αλγορίθμους καθορίζεται από την καταλληλότητα του. Το παραπάνω μοιάζει με την καταλληλόλητα του αντισώματος ή του αντιγόνου.

Υπάρχουν διάφορες εκδοχές του αλγορίθμου επιλογής κλώνων.Ο DeCastro(2002) έχει προτείνει τον αλγόριθμο clonAlg, για την αναγνώριση προτύπων και οποίος παρουσιάζεται παρακάτω. Η εκδοχή αυτή του αλγορίθμου επιλογής κλώνων, δέχεται σαν είσοδο ένα σύνολο προτύπων τα οποία πρόκειται να αναγνωριστούν, ενώ η εκδοχή βελτιστοποίησης θεωρεί μια αντικειμενική συνάρτηση η οποία πρόκειται να βελτιστοποιηθεί [44, 45].

Πίνακας 2Σύγκριση των αλγορίθμων επιλογής κλώνων με τους εξελικτικούς αλγορίθμους [8]

Χαρακτηριστικά	Εξελικτικοί αλγόριθμοι	Αλγόριθμος επιλογής κλώνων
Χώρος λύσεων	Σύνολο χρωμοσωμάτων	Σύνολο αντισωμάτων
Υποψήφια λύση	Χρωμόσωμα	Αντίσωμα
Αναπαράσταση ατόμου	Οποιαδήποτε(αλληλουχία, Πραγματικά διανύσματα κτλ.)	Οποιαδήποτε
Μέγεθος πληθυσμού	Σταθερό	Σταθερό
Συνάρτηση καταλληλότητας	Βασίζεται στην συνάρτηση	Συνάφεια
Τελεστές	Επιλογή χρωμοσωμάτων Μετάλλαξη Διασταύρωση	Επιλογή κλώνων Υπέρ-μετάλλαξη

3.2.6. Η θεωρία δικτύου

Η θεωρία δικτύου υποστηρίζει ότι η σύνδεση των Β-κυττάρων στοχεύει στον σχηματισμό ενός δικτύου κυττάρων. Η αντίδραση ενός Β-κυττάρου κατά τον εντοπισμό ενός αντιγόνου, προκαλεί την ενεργοποίηση όλων των Β-κυττάρων του δικτύου. Έτσι, η ενεργοποίηση των λεμφοκυττάρων πραγματοποιείται όχι μόνο από τα αντιγόνα αλλά και από κάποιο γειτονικό λεμφοκύτταρο [52]. Η αντίδραση ενός λεμφοκυττάρου σε ένα αντιγόνο παράγοντας Β-κύτταρα και κλώνους, προκαλεί την ενεργοποίηση των ενδιάμεσωνλεμφοκυττάρων. Επομένως, η απόκριση ενός γειτονικού λεμφοκυττάρου παράγοντας κλώνους, μπορεί να ενεργοποιήσειστη συνέχεια τους γείτονες του κτλ. [8]

3.3. Μοντέλα βασισμένα στην επιλογή κλώνων

Στο τεχνητό ανοσοποιητικό σύστημα, οι κλώνοι που επιλέγονται αποτελούν επιλογή ενός συνόλου ALCs που είναι περισσότερο συναφή με ένα μη φυσιολογικό πρότυπο. Ακολουθεί η κλωνοποίηση και μετάλλαξη των επιλεγμένων ALCs, ώστε να είναι ακόμα πιο πολύ συναφή με το μη φυσιολογικό πρότυπο. Παρακάτω, πραγματοποιείται ανάλυση ορισμένων μοντέλων τεχνητού ανοσοποιητικού συστήματος που βασίζονται στην επιλογή κλώνων και παρουσίαση ενός ψευδό-αλγόριθμου για κάθε ένα από αυτά τα μοντέλα [40].

3.3.1. CLONALG

Η μοντελοποίηση του CLONALG είναι βασισμένη στην επιλογή ενός λεμφοκυττάρου από ένα ανιχνευμένο αντιγόνο για κλωνοποίηση. Η παρουσίαση του CLONALG ως αλγόριθμου που υλοποιεί μηχανική μάθηση και αναγνώριση προτύπων, πραγματοποιήθηκε από τους De Castro και Von Zuben [44, 45]. Όλα τα πρότυπα παρουσιάζονται σαν δυαδικές ακολουθίες.

Ο υπολογισμός της συνάφειας ανάμεσα σε ένα ALC και ένα μη φυσιολογικό πρότυπο γίνεται με την μεταξύ τους απόσταση Hamming. Όσο πιο μικρή είναι η απόσταση τόσο πιο μεγάλη είναι η συνάφειά τους. Στο δείγμα εκπαίδευσης, το σύνολο των προτύπων αντιμετωπίζεται ως μη φυσιολογικά πρότυπα. Ο αλγόριθμος 3 συνοψίζει το CLONALG για εφαρμογή σε αναγνώριση προτύπων. Τα μέρη του αλγορίθμου αναλύονται παρακάτω [52].

Το σύνολο Cτων ALCs, αρχικοποιείται με n_aτυχαία ALCs. Το σύνολο ALCδιαιρείται σε ένα σύνολο μνήμης, M, και ένα σύνολο *R*με τα υπόλοιπα ALCs.
Συνεπώς:

$$C = M \cup R \text{ και } \mathrm{n_{ci}} = \mathrm{round}\left(\frac{\beta \times n_h}{i}\right).$$

Η αρχική υπόθεση στον αλγόριθμοCLONALGείναι ότι υπάρχει ένα ALCμνήμης για κάθε πρότυπο προς αναγνώριση στο σύνολο D_T. [52]

Αλγόριθμος 3 CLONALG αλγόριθμος για αναγνώριση προτύπων

$t = t_{max}$;

Καθόρισε τα πρότυπα αντιγόνου σας το δείγμα εκπαίδευσης D_T ;

Αρχικοποίησε ένα σύνολο n_a τυχαία ALCs σαν τον πληθυσμό C;

Επίλεξε ένα υποσύνολο $n_m = |DT|$ ALCs, σαν τον πληθυσμό $M \subseteq C$;

Επίλεξε ένα υποσύνολο $n_a - n_m$ των ALCs, σαν τον πληθυσμό $R \subseteq C$;

Όσο t>0 επανάλαβε

Για κάθε *πρότυπο αντιγόνου* $\mathbf{z}_p \in D_T$ **επανάλαβε**

Υπολόγισε την συνάφεια μεταξύ του $\mathbf{z}_p$ και κάθε ALC στο C;

Επίλεξε n_h ALCs με την υψηλότερη συνάφεια με το $\mathbf{z}_p$ από το C σαν το υποσύνολο H;

Ταξινόμησε τα ALCs του συνόλου H με αύξουσα σειρά, με βάση τη συνάφεια των ALCs ;

Δημιούργησε το W σαν το σύνολο κλώνων ALC του H;

Δημιούργησε το W' σαν το σύνολο των μεταλλαγμένων κλώνων για κάθε ALC στο W;

Υπολόγισε τη συνάφεια μεταξύ των $\mathbf{z}_p$ και κάθε ALC στο σύνολο W' ;

Επίλεξε το ALC με την υψηλότερη συνάφεια στο W' *σαν* $\hat{x}$;

Εισήγαγε το $\hat{x}$ στο M στη θέση p;

Αντικατέστησε τα n_l ALCs με τη χαμηλότερη συνάφεια στο R με τυχαία ALCs;

τέλος

$t = t - 1$;

Τέλος

Κάθε πρότυπο $\mathbf{z}_p$, σε τυχαία θέση, ρ, στο *DT*,εμφανίζεται στο C. Η συνάφεια μεταξύ των $\mathbf{z}_p$και κάθε ALCστο *C*υπολογίζεται. Ένα υποσύνολο n_hτων ALCsμε την υψηλότερη συνάφεια επιλέγεται από το *C*σαν το υποσύνολο Η. Ακολουθεί η ταξινόμηση του συνόλου n_hτων ALCsσε αύξουσα σειρά σε σχέση με τη συνάφεια με το $\mathbf{z}_p$. Κάθε ALCστο ταξινομημένο σύνολο *H*κλωνοποιείται ανάλογα με την υπολογισμένη

συνάφεια με το $\mathbf{z}_p$και προστίθεται στο σύνολο W. Το πλήθος των κλωνοποιημένων, n_{ci},για κάθε ALC, x_i,στην θέση *ιστο* ταξινομημένο σύνολο *H,* προσδιορίζεται ως εξής [52]:

$$n_{ci} = \text{round}\left(\frac{\beta \times n_h}{i}\right),$$

όπου β είναι ένας συντελεστής και η συνάρτηση round*i* επιστρέφει τον πλησιέστερο ακέραιο αριθμό.

Τα ALCsστο κλωνοποιημένο σύνολο, W, μεταλλάσσονται με ένα ποσοστό μεταλλαγής που είναι αντιστρόφως ανάλογο της υπολογισμένης συνάφειας. Όσο δηλαδή, πιο υψηλή είναι η συνάφεια τόσο πιο χαμηλό είναι το ποσοστό μεταλλαγής. Οι μεταλλαγμένοι κλώνοι στο Wπροστίθενται σε ένα σύνολο μεταλλαγμένων κλώνων, W'. Η συνάφεια μεταξύ των μεταλλαγμένων κλώνων στο σύνολο W' και του επιλεγμένου συνόλου εκπαίδευσης, z_p, υπολογίζεται [52].

Το ALCμε την υψηλότερη υπολογισμένη συνάφεια στο σύνολο W', X, αντικαθιστά το ALCστη θέση, ρ, στο σύνολο M, εάν η συνάφεια X είναι υψηλότερη από τη συνάφεια του ALCστο σύνολο M. Τα τυχαία παραγμένα ALCsαντικαθιστούν τα niALCsμε τη χαμηλότερη συνάφεια στο σύνολο R. Η διαδικασία εκμάθησης επαναλαμβάνεται, μέχρι να επιτευχθεί ο μέγιστος αριθμός γενεών, tmax. Μια τροποποιημένη έκδοση του αλγορίθμου CLONALGέχει εφαρμοστεί στην βελτιστοποίηση της πολύμορφης λειτουργίας (multi-modalfunctionoptimization) [52].

3.3.2. Δυναμική επιλογή κλώνων

Σε ορισμένα προβλήματα που χρειάζονται βελτιστοποίηση, τα πρότυπά τους είναι φυσιολογικά και τροποποιούνται με το πέρασμα του χρόνου. Για την εξέταση τέτοιων προβλημάτων, οι Kimκαι Bentley [40] εισήγαγαν τον δυναμικό κλωνικό αλγόριθμο επιλογής (DCS), ο οποίος βασίζεται στο AISπου πρότεινε ο Hofmeyr[46]. Το ζητούμενο είναι να υπάρχουν τρεις διαφορετικοί πληθυσμοί ALCs, ανώριμα, ώριμα και πληθυσμοί μνήμης.

Η μελέτη των Kimκαι Bentley[40] εστίασε στον τρόπο που επιδρούν στην προσαρμοστικότητα του μοντέλου όταν αλλάζουν τα πρότυπα τρεις παράμετροι, α) η

περίοδος ανεκτικότητας, β) το κατώτατο όριο ενεργοποίησης και γ) ο κύκλος ζωής. Η περίοδος ανεκτικότητας είναι ένα κατώτατο όριο του αριθμού των γενεών που το ALCsμπορεί να γίνει αυτό-ανεκτικό (self-tolerant). Το κατώτατο όριο ενεργοποίησης χρησιμοποιείται ως μέτρο για να καθοριστεί εάν ένα ώριμο ALCαντιμετώπισε τον ελάχιστο αριθμό αντιστοιχιών αντιγόνων για να είναι σε θέση να γίνει ένα ALCμνήμης. Τέλος, ο κύκλος ζωής δείχνει το μέγιστο αριθμό γενεών για τον οποίο ένα ώριμο ALCεπιτρέπεται να είναι στο σύστημα [52].

Η ταύτιση του κύκλου ζωής του ώριμου ALC με την προκαθορισμένη τιμή της παραμέτρου του κύκλου ζωής, συνεπάγεται διαγραφή του ώριμου ALC από το σύστημα. Βάσει πειραματικών αποτελεσμάτων με διαφορετικές τιμές για τις παραμέτρους, υποδεικνύεται ότι εάν αυξηθεί ο κύκλος ζωής και μειωθεί στο κατώτατο όριο ενεργοποίησης αυξάνεται η πιθανότητα το μοντέλο να ανιχνεύσει σωστά τα πραγματικά μη φυσιολογικά πρότυπα. Εάν αυξηθεί η περίοδος ανεκτικότητας, μειώνεται η λανθασμένη ανίχνευση των φυσιολογικών προτύπων, εφόσον τα φυσιολογικά πρότυπα είναι σταθερά.

Αν και θα ήταν δυνατή η σταδιακή εκμάθηση της δομής των φυσιολογικών και μη φυσιολογικών προτύπων από το DCS, δεν θα ήταν δυνατή η εκμάθηση οποιονδήποτε αλλαγών στα απαρατήρητα φυσιολογικά πρότυπα. Τα ALCsμνήμης διαρκούν επ’ άπειρον στον αλγόριθμο DCS. Η παράλειψη του γνωρίσματος αυτού στο εκτεταμένο DCS έγινε αφαιρώντας τα ALCsμνήμης που δεν ήταν μόνο-ανεκτικά (selftollerant) στα πρόσφατα εισαχθέντα φυσιολογικά πρότυπα [40].

Το DCS επεκτάθηκε επιπλέον εισάγοντας την υπέρ-μετάλλαξη στα διαγραμμένα ALCsμνήμης [40]. Η μετάλλαξη των διαγραμμένων ALCsμνήμης έχει σκοπό την τροφοδότηση του ανώριμου πληθυσμού ανιχνευτών. Λόγω της περιεχόμενης πληροφορίας των διαγραμμένων ALCsμνήμης, όταν μεταλλάσσονται το σύστημα διατηρείται και τελειοποιείται, ενισχύοντας τον αλγόριθμο με ήδη εκπαιδευμένα ALCs.

3.3.3. Πολύ-επίπεδο AIS

Ένα νέο μοντέλο, που έχει βασιστεί στην επιλογή κλώνων, έχουν προτείνει οι Knight και Timmis [47]. Πρόκειται για ένα πολυεπίπεδο μοντέλο για την εξομάλυνση των ανεπαρκειών του μοντέλου AINE. Η αλληλεπίδραση των καθορισμένων επιπέδων οδηγεί στην προσαρμογή τους και στην εκμάθηση της δομής των παρουσιαζόμενων προτύπων αντιγόνων. Η δομή που ακολουθείται από το συγκεκριμένο μοντέλο είναι αυτή του AIS. Για ένα AIS απαιτείται να αναπαρίστανται τα συστατικά του (B-κύτταρα), να αξιολογούνται οι αλληλεπιδράσεις μεταξύ τους ή με το περιβάλλον τους (συνάφεια) και να μπορεί το μοντέλο να προσαρμοστεί σε ένα δυναμικό περιβάλλον.

Το πολύ-επίπεδο AIS που προτείνεται, περιλαμβάνει τα εξής επίπεδα: το επίπεδο των ελεύθερων-αντισωμάτων (F), το επίπεδο των B-κυττάρων (B) και το επίπεδο μνήμης (M). Το σύνολο των προτύπων εκπαίδευσης, DT, θεωρείται ότι είναι το αντιγόνο [52]. Σε κάθε επίπεδο υπάρχει ένα κατώτατο όριο συνάφειας (α_F, α_B, α_M) και ένα κατώτατο όριο επιβίωσης ($\varepsilon_F, \varepsilon_B, \varepsilon_M$). Ο υπολογισμός του κατώτατου ορίου επιβίωσης γίνεται σε σχέση με το χρονικό διάστημα, καθώς η διέγερση ενός κυττάρου συμβαίνει σε ένα συγκεκριμένο επίπεδο. Εάν το χρονικό διάστημα που έχει υπολογιστεί δεν ξεπεραστεί από το κατώτατο όριο επιβίωσης, τότε ακολουθεί ο θάνατος του κυττάρου και η αφαίρεσή του από τον πληθυσμό του συγκεκριμένου επιπέδου. Ο καθορισμός της ενότητας ενός αντιγόνου με μια οντότητα σε ένα συγκεκριμένο επίπεδο ή μη, γίνεται από το κατώτατο όριο συνάφειας. Ο υπολογισμός της συνάφειας, f_A, ανάμεσα σε ένα πρότυπο αντιγόνων και σε μια οντότητα σε ένα επίπεδο, γίνεται με την ευκλείδεια απόσταση. Το πολύ-επίπεδο AIS συνοψίζεται με τον αλγόριθμο 4. Ακολουθεί η ανάλυση των διαφορετικών μερών του αλγορίθμου.

Αρχικά, στο στρώμα των ελεύθερων αντισωμάτων, F, εισβάλλει ένα αντιγόνο, zp, και έπειτα το πρότυπο αντιγόνων παρουσιάζεται στα n_fελεύθερα- αντισώματα. Τα ταιριάσματα που δημιουργούν τα ελεύθερα-αντισώματα αποθηκεύονται στη μεταβλητή n_b. Στη συνέχεια, το αντιγόνο, z_p, εισέρχεται στο επίπεδο των B-κυττάρων, B, και παραμένει μέχρι την δέσμευσή του από ένα από τα B-κύτταρα. Μετά από τη σύνδεση, το υποκινημένο B-κύτταρο, u_k, παράγει έναν κλώνο, u_kεάν το επίπεδο υποκίνησης υπερβαίνει ένα προκαθορισμένο κατώτατο όριο υποκίνησης, γ_B. Το επίπεδο υποκίνησης βασίζεται στο πλήθος των συνδέσεων των ελεύθερων-αντισωμάτων, n_b, όπως

υπολογίζεται στο επίπεδο των ελεύθερων αντισωμάτων. Ο κλώνος έπειτα μεταλλάσσεται, u_k', και προστίθεται στο στρώμα των Β-κυττάρων. Το υποκινημένο Β κύτταρο, u_k, παράγει τα ελεύθερα αντισώματα που είναι μεταλλαγμένες εκδόσεις του αρχικού Β-κυττάρου. Ο αριθμός των ελεύθερων αντισωμάτων που παράγονται από ένα Β-κύτταρο καθορίζεται ως εξής [52]:

$$f_F(z_p, u_k) = (a_{\max} - f_a(z_p, u_k)) \times a$$

Όπου f_Fείναι το πλήθος των αντισωμάτων,που προστίθενται στο επίπεδο των ελεύθερων αντισωμάτων, a_{max}είναι η μέγιστη δυνατή απόσταση μεταξύ ενός Β-κυττάρου και ενός προτύπου αντιγόνου στο χώρο δεδομένων, $f_a(z_p, u_k)$ είναι ησυνάφεια μεταξύ ενός αντιγόνου, $\mathbf{z}_p$, και ενός Β-κυττάρου,^, και a είναι μια θετική μεταβλητή.
Εάν ένα αντιγόνο δεν ταιριάξει με κανένα από τα Β-κύτταρα ένα καινούριο Β- κύτταρο, δημιουργείται με την ίδια αναπαράσταση με το αντιγόνο $\mathbf{z}_p$. Το καινούριο Β-κύτταρο προστίθεται στο επίπεδο των Β-κυττάρων με αποτέλεσμα την αύξηση της ποικιλίας των αντιγόνων. Το καινούριο Β-κύτταρο u_{new},επίσης παράγει μεταλλαγμένα ελεύθερα αντισώματα, τα οποία προστίθενται στο επίπεδο των ελεύθερων αντισωμάτων [52].

Το τελικό επίπεδο Μ, αποτελείται μόνο από τα κύτταρα μνήμης και αποκρίνεται μόνο σε καινούρια κύτταρα μνήμης. Ο κλώνος U_kεμφανίζεται σαν ένα καινούριο κύτταρο μνήμης στο επίπεδο μνήμης, Μ. Το κύτταρο μνήμης με την μικρότερη συγγένεια στο U_kεπιλέγεται σαν v_{min}. Αν η συνάφεια μεταξύ των U_kκαι v_{min}είναι μικρότερη απότο προκαθορισμένο κατώφλι μνήμης, a_M, και η συνάφεια του U_kείναι μικρότερη από τη συνάφεια του v_{min}με το αντιγόνο z(αυτή ήταν η αιτία της δημιουργίας του νέου Β-κυττάρου, U_k), τότε το v_{min}αντικαθίσταται από το καινούριο κύτταρο μνήμης U_k [52]. Αν η συνάφεια μεταξύ των U_kκαι v_{min}είναι υψηλότερη από το προκαθορισμένο κατώφλι μνήμης, a_Mτο καινούριο κύτταρο μνήμης U_kπροστίθεται στο επίπεδο μνήμης.

Αλγόριθμος 4 Ένας πολύ – επίπεδος AIS αλγόριθμος

Καθόρισε τα πρότυπα αντιγόνων σαν το δείγμα εκπαίδευσης D_T

Για κάθε πρότυπο αντιγόνου $z_p \in D_T$ **επανάλαβε**

n_b=0;

bcell_bind=false;

Επίλεξε τυχαία n'_f ελεύθερα αντισώματα από το σύνολο F ,υποσύνολο E

Για κάθε ελεύθερο αντίσωμα $y_j \in E$ **επανάλαβε**

Υπολόγισε την συνάφεια $f_a(z_p, y_j)$

Αν $f_a(z_p, y_j) < a_F$ **τότε**

n_b++;

Αφαίρεσε το ελεύθερο αντίσωμα y_j από το σύνολο F;

Τέλος

Τέλος

Για κάθε τυχαία επιλεγμένο B-κύτταρο u_k στην θέση k στο σύνολο των B-κύτταρων, B **επανάλαβε**

Υπολόγισε την συνάφεια $f_a(z_p, u_k)$

Αν $f_a(z_p, u_k) < a_B$ **τότε**

B_cell_bind=true;

Break;

Τέλος

Τέλος

Αν δεν υπάρχει ταίριασμα **τότε**

Αρχικοποίησε το καινούριο B-κύτταρο, u_{new} ,με το z_p και πρόσθεσε το B-κύτταρο στο B

Δημιούργησε $f_F(z_p, u_{new})$ ελεύθερα αντισώματα και πρόσθεσε τα στο F

Τέλος

Αλλιώς

Δημιούργησε $f_F(z_p, u_k)$ ελεύθερα αντισώματα και πρόσθεσε τα στο F

Ενημέρωσε το επίπεδο παρακίνησης του u_k προσθέτοντας το n_b

Αν το επίπεδο παρακίνησης του $u_k \geq \gamma_B$ **τότε**

Κλωνοποίησε το Β-κύτταρο u_k, σαν $\tilde{u}_k$

Μετάλλαξε το $\tilde{u}_k$, σαν u_k'

Πρόσθεσε το u_k' στο σύνολο των Β-κυττάρων, Β

Επίλεξε το κύτταρο μνήμης $v_{\min}$ από το σύνολο Μ, σαν το κύτταρο μνήμης με την μικρότερη συνάφεια f_a σε σχέση με το $\tilde{u}_k$

Αν $f_a(\tilde{u}_k, v_{\min}) < a_M$ **τότε**

Πρόσθεσε το $\tilde{u}_k$ στο σύνολο μνήμης Μ

Τέλος

Αλλιώς

Αν $f_a(z_p, \tilde{u}_k) < f_a(z_p, v_{\min})$ **τότε**

Αντικατέστησε το κύτταρο μνήμης $v_{\min}$ με τον κλώνο $\tilde{u}_k$ στο σύνολο μνήμης Μ

Τέλος

Τέλος

Τέλος

Τέλος

Τέλος

Για κάθε κύτταρο x_i, στο σύνολο $F \cup B \cup M$ **επανάλαβε**

Αν ο χρόνος επιβίωσης του $x_i > \varepsilon_{F,B,M}$ **τότε**

Αφαίρεσε το x_i από το αντίστοιχο σύνολο

Τέλος

Τέλος

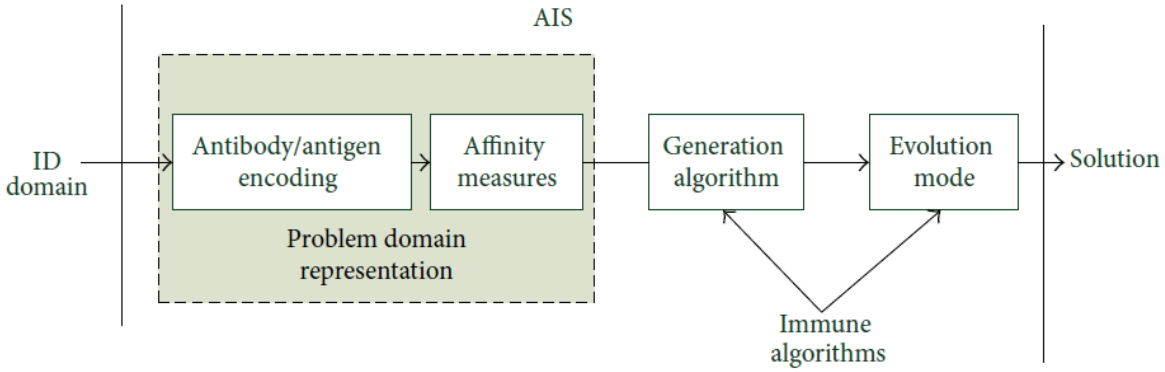
Κεφάλαιο 4. ΑΝΙΧΝΕΥΣΗ ΕΙΣΒΟΛΗΣ (ID) ΒΑΣΕΙ ΤΕΧΝΗΤΟΥ ΑΝΟΣΟΠΟΙΗΤΙΚΟΥ ΣΥΣΤΗΜΑΤΟΣ (AIS)

Το παρόν κεφάλαιο ειδικεύεται στον σχεδιασμό των IDSπου βασίζονται σε AIS. Λόγο του ότι υπάρχουν πολλές μέθοδοι AIS και πολλές φορές είναι δύσκολη η επιλογή για το ποιες θα πρέπει να χρησιμοποιηθούν ή αν υπάρχει κάποιος νόμος που πρέπει να ακολουθηθεί, στο παρόν κεφάλαιο παρέχεται ένα γενικό πλαίσιο στην περιοχή του IDS που βασίζεται στο AIS και ανάλυση γύρω από τρεις πτυχές: κωδικοποίηση αντισωμάτων / αντιγόνων, αλγόριθμο παραγωγής και λειτουργία εξέλιξης.

4.1. Το πλαίσιο για τον σχεδιασμό Συστημάτων Ανίχνευσης Εισβολής (IDS) που βασίζονται σε Τεχνητό Ανοσοποιητικό Σύστημα (AIS)

Ο σκοπός του IDS δεν είναι μόνο να αποτρέψει την επίθεση, αλλά και να αναφέρει όλες τις ασυνήθιστες συμπεριφορές του συστήματος. Για το σχεδιασμό ενός επιτυχημένου IDS που βασίζεται σε AIS, το πρώτο πράγμα που πρέπει να ληφθεί υπόψη είναι η προβληματική παρουσίαση του συστήματος στον τομέα ID και στη συνέχεια ο συνδυασμός μεθόδων AIS με IDS.

Παρόλο που υπάρχουν πολλά άρθρα που έχουν συνοψίσει τις έρευνες για αυτό το θέμα, αυτές οι κριτικές απλά χώρισαν τις τρέχουσες μεθόδους σε διαφορετικές ομάδες και δεν μπορούν να παρέχουν αρκετές πληροφορίες καθοδήγησης για το σχεδιασμό των ID μεθόδων που βασίζονται στο AIS. Στην παρούσα εργασία, θα γίνει μια ανάλυση για αυτές τις μεθόδους, από βασικά στοιχεία, που απαιτεί ένα πλαίσιο για IDS που βασίζεται στο AIS, και παρουσιάζονται στο Σχήμα 1.



Σχήμα 1.Πλαίσιο σχεδιασμού IDSβασισμένο σε AIS

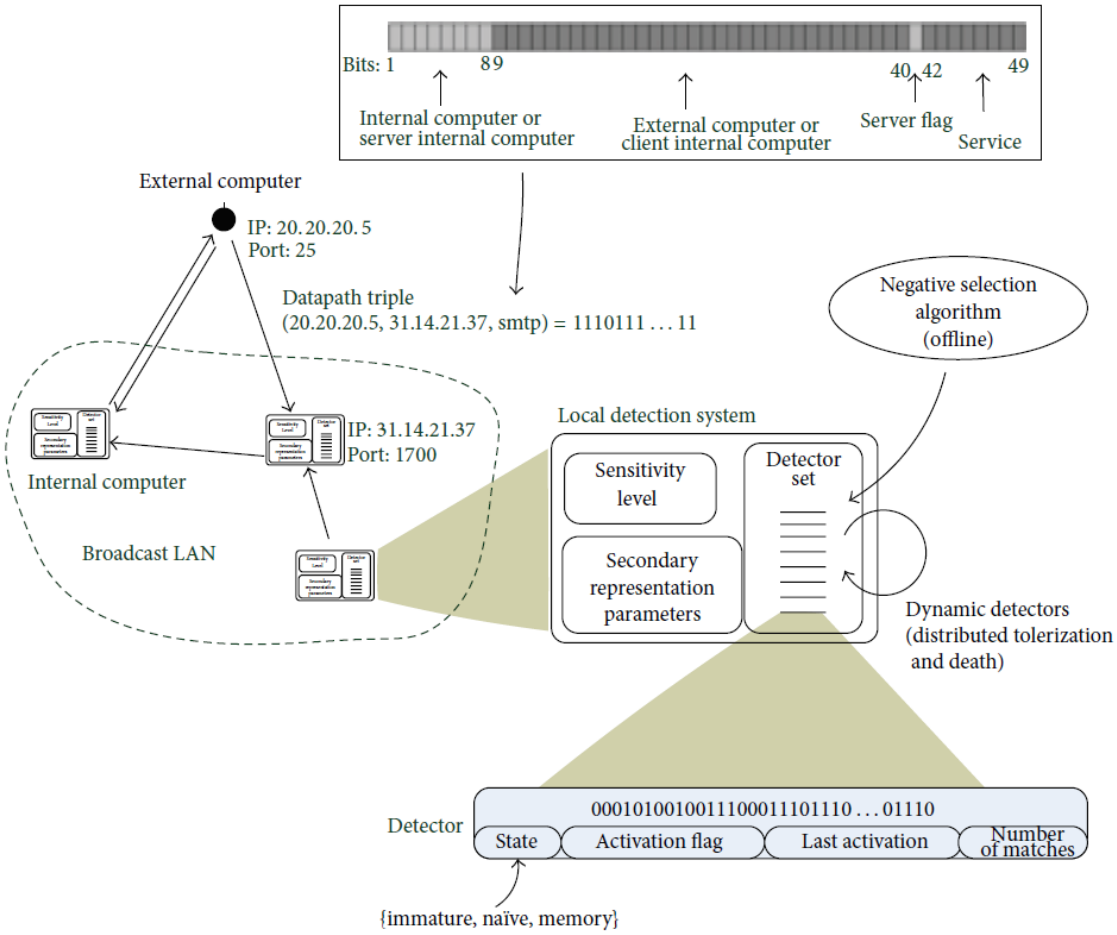
Για την εφαρμογή του AIS στο IDS, ακολουθούνται τρία βήματα σε αυτό το πλαίσιο. Το πρώτο βήμα (το αριστερό γκρι πλαίσιο στο Σχήμα 1) είναι να αντιπροσωπεύσει τα στοιχεία του συστήματος και την αλληλεπίδραση των ατόμων σε μια ανοσολογική μορφή. Ο στόχος αυτού του βήματος είναι να αντιπροσωπεύσει τα στοιχεία Ανίχνευσης Εισβολής (ID) με τρόπο ανοσολογικό (π.χ. δημιουργώντας αφηρημένα μοντέλα ανοσοκυττάρων, μορίων κ.λπ.) και να ποσοτικοποιήσει την αλληλεπίδραση αυτών των στοιχείων με μέτρα συγγένειας. Για παράδειγμα, η μη φυσιολογική συμπεριφορά στο IDS παρουσιάζεται ως το αντιγόνο (μη-εαυτός) στο AIS. Στον τομέα ID, συγγένεια σημαίνει η ομοιότητα μεταξύ ανιχνευτών και δεδομένων. Οι διαφορετικές αναπαραστάσεις μπορούν να υιοθετήσουν διαφορετικά μέτρα συγγένειας. Το δεύτερο βήμα είναι η δημιουργία των αρχικών ρεπερτορίων (αλγόριθμος παραγωγής) και το τρίτο βήμα είναι η βελτιστοποίηση του αλγορίθμου (λειτουργία εξέλιξης). Μπορούν να επιλεγούν περισσότεροι αλγόριθμοι ανοσοποιητικού για αυτά τα δύο βήματα. Αυτό το πλαίσιο μπορεί να θεωρηθεί ως μια διαδικασία σχεδιασμού για το μηχανικό AIS εμπνευσμένο IDS. Πάνω σε αυτό θα αναλυθούν στη συνέχεια τρία θέματα: κωδικοποίηση αντισωμάτων/αντιγόνων, αλγόριθμος παραγωγής και λειτουργία εξέλιξης.

4.2. Κωδικοποίηση Αντισώματος / Αντιγόνου

Ο πυρήνας του HIS είναι η διάκριση εαυτού και μη-εαυτού που γίνεται από τα λεμφοκύτταρα, η οποία είναι παρόμοια με το IDS που διακρίνει τη φυσιολογική και μη φυσιολογική συμπεριφορά. Το κλειδί της μοντελοποίησης αυτού του μηχανισμού στο IDS που βασίζεται στο AIS είναι ο τρόπος αναπαράστασης των στοιχείων στον

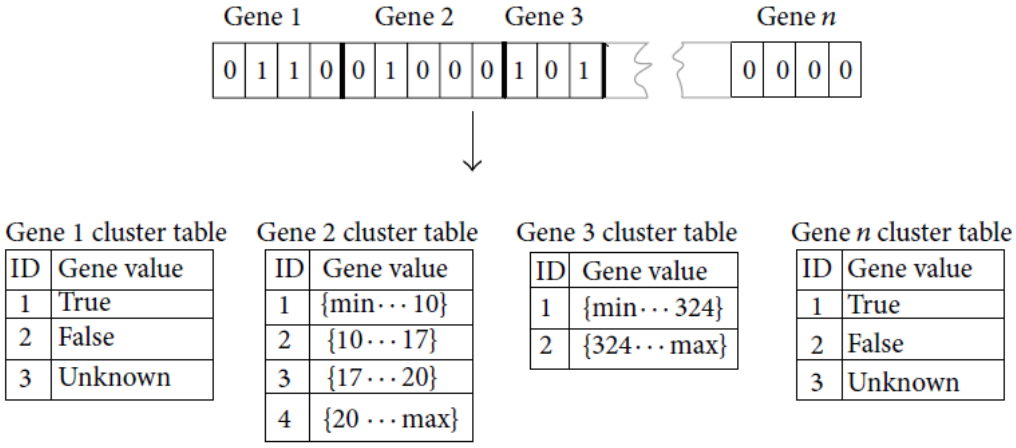
προβληματικό τομέα και η λήψη απόφασης σχετικά με τους κανόνες αντιστοίχισης. Τα αντισώματα δημιουργούνται από τυχαίους συνδυασμούς ενός συνόλου τμημάτων γονιδίων. Ως εκ τούτου, η αναπαράσταση των ανιχνευτών είναι να τους κωδικοποιούν ως γονιδιακές ακολουθίες. Στο IDS που βασίζεται στο AIS, ακολουθούμε [53] υποθέτοντας τη γενική περίπτωση ότι κάθε αντίσωμα Ab είναι ανιχνευτής που αντιπροσωπεύεται από ένα *L*- dimensional vector Ab = (Ab1, Ab2, . . . , Ab$_L$⟩ και κάθε αντιγόνο Ag είναι ένα δεδομένο που πρέπει να ταξινομηθεί και το οποίο αντιπροσωπεύεται από ένα *L*- dimensional vectorAg = (Ag1, Ag2, . . . , Ag$_L$), όπου το *L* είναι το μήκος του διανύσματος. Κάθε αντίσωμα στη συνέχεια ταυτίζεται με κάθε ένα από τα αντιγόνα και τα αναγνωρίζει. Η συγγένεια, όταν αντιστοιχιστεί στον τομέα ID, σημαίνει την ομοιότητα μεταξύ Ag και Ab.

Επειδή οποιαδήποτε δεδομένα τελικά εφαρμόζονται ως δυαδικά bit σε υπολογιστές, οι έρευνες επικεντρώνονται στη δυαδική αναπαράσταση ως κύρια. Αυτός είναι ο λόγος για τον οποίο η δυαδική συμβολοσειρά είναι ο πιο συχνά υιοθετημένος συνδυασμός κωδικοποίησης στο AIS. Το πρώτο μοντέλο AIS υιοθέτησε δυαδική κωδικοποίηση, η οποία προτείνεται από τον Forrest, προσομοιώνοντας την αρχή του εαυτού / μη-εαυτού του HIS [55]. Η NSA είναι ο πυρήνας αυτού του μοντέλου, με το οποίο οι μη έγκυροι ανιχνευτές εξαλείφονται όταν ταιριάζουν με τα δεδομένα του εαυτού τους. Η NSA είναι ο πυρήνας αυτού του μοντέλου, με το οποίο οι μη έγκυροι ανιχνευτές εξαλείφονται όταν ταιριάζουν με τα δεδομένα του εαυτού τους. Η NSA υιοθετεί δυαδική κωδικοποίηση για την προσομοίωση αντισωμάτων/ αντιγόνων. Σπάει τη συμβολοσειρά 32-bit σε οκτώ υποστρώσεις ως αντιγόνο και αντίσωμα. Αν και δεν χρησιμοποιήθηκαν πολλά ανοσοποιητικά χαρακτηριστικά, δείχνει τη σκοπιμότητα αυτού του αλγορίθμου. Το LISYS (Lightweight Immune SYStem - Ελαφρύ Ανοσοποιητικό Σύστημα) είναι ένα σχετικά πρώιμο μοντέλο συστήματος που χρησιμοποιείται για την προστασία του LAN από επιθέσεις που βασίζονται στο δίκτυο [61]. Σε αυτό το σύστημα, κάθε ανιχνευτής είναι μια δυαδική συμβολοσειρά 49-bit, κυρίως για το πακέτο TCP SYN. (βλέπε Σχήμα 2).



Σχήμα 2. Κωδικοποίηση LISYS ενός πακέτου TCPSYN [61]

Αργότερα, το CDIS προσανατολισμένο στον ιό [62] επέκτεινε περαιτέρω τη LISYS και χρησιμοποίησε δυαδική συμβολοσειρά 320-bit για κάθε υπογραφή αντισωμάτων, αποτελούμενη από 29 από τα πιθανά πεδία δεδομένων σε ένα πακέτο πρωτοκόλλου δικτύου, για τον εντοπισμό TCP, UDP και ICMP. Ο Kim και ο Bentley χρησιμοποίησαν ένα στατικό CSA με τον χειριστή NS ως ένα στοιχείο του AIS για αναγνωριστικό δικτύου (NID). Το στοιχείο αυτό αναπτύχθηκε ειδικά με σκοπό την κατασκευή ανιχνευτή κατάχρησης με αποτελεσματικότερο τρόπο [63]. Χρησιμοποιούν δυαδικούς γονότυπους για να κωδικοποιήσουν τους συνδετικούς κανόνες των ανιχνευτών, όπως φαίνεται στο Σχήμα 3.



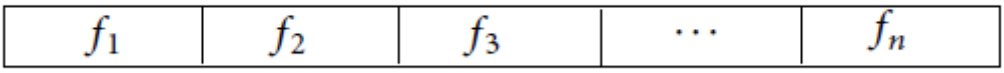
Σχήμα 3. Αναπαράστασητων DynamiCS γονιδίων [63]

Μετά ερεύνησαν τη δυναμική επιλογή κλώνων και διαπίστωσαν ότι μπορεί να προσαρμοστεί σε νέα δεδομένα στο NID [64]. Μια συνεργατική ανοσολογική προσέγγιση για την ανίχνευση της ανωμαλίας δικτύου παρουσίασε το σύνολο του εαυτού ως δυαδικού διανύσματος για την τριπλή επικοινωνία (πηγή, προορισμός IP και Θύρα, και πρωτόκολλο) [65].

Αλλάζοντας την κωδικοποίηση από δυαδικό σε Gray κώδικα, η απόδοση μπορεί να βελτιωθεί [66]. Ο λόγος είναι ότι οι κωδικοποιήσεις δύο διαδοχικών αριθμών έχουν μικρή απόσταση Hamming. Και αυτή η μέθοδος εξακολουθεί να ανήκει στη δυαδική κωδικοποίηση.

Τα περισσότερα έργα έχουν περιοριστεί στη δυαδική αναπαράσταση δεδομένων και ανιχνευτών, αλλά χρησιμοποιούν διαφορετικά μέτρα συγγένειας, για παράδειγμα, r-contiguous bits matching [55], r-chunks matching [67], landscape-affinity matching [62], Hamming distance [68], και Rogers and Tanimoto (R&T) matching [69], και ούτω καθεξής. Ωστόσο, αυτή η κωδικοποίηση αντισωμάτων/αντιγόνων δείχνει πολλά μειονεκτήματα. Το πιο σημαντικό πρόβλημα είναι ότι η σχέση συγγένειας μεταξύ δύο δυαδικών συμβολοσειρών που αντιπροσωπεύονται από τους κανόνες αντιστοίχισης έχει ως αποτέλεσμα την κακή κάλυψη του προβληματικού χώρου [70]. Επιπλέον, η εκθετική αύξηση του υπολογιστικού χρόνου που προκαλείται από τον αριθμό των παραγόμενων ανιχνευτών είναι αρκετά μεγάλη. Προκειμένου να επιλυθούν αυτά τα προβλήματα, ένας άλλος διαφορετικός NSA προτάθηκε από τον Gonzalez και τους συνεργάτες [71]. Στη μέθοδό αυτή, τα αντισώματα δεν παρουσιάζονταν ως bit-strings αντίθετα, αντιπροσωπεύονται ως hyperspheres (υπερσφαίρες). Οι Gonzalez et al.,

ονόμασαν αυτή την προσέγγιση, real-valued NS. Κάθε χαρακτηριστικό ανήκει στην περιοχή [0.0, 1.0] όπως φαίνεται στο Σχήμα 4. Επικεντρώθηκαν σε πραγματικά προβλήματα ανίχνευσης ανωμαλιών και όχι σε ID προβλήματα. Αυτός ο αλγόριθμος δημιουργεί hyperspheres με ίσα μήκη ακτίνας. Ο Kim χρησιμοποίησε την NSA για να κατασκευάσει έναν ανιχνευτή ανωμαλιών για NID [72]. Στην κωδικοποίηση των ανιχνευτών, κάθε γονίδιο ενός ανιχνευτή χρησιμοποιεί δεκαδικά σύμβολα. Το αυτο-προφίλ έχει 33 διαφορετικά πεδία και αυτός ο αριθμός καθορίζει τον συνολικό αριθμό των αντίστοιχων γονιδίων στους ανιχνευτές.

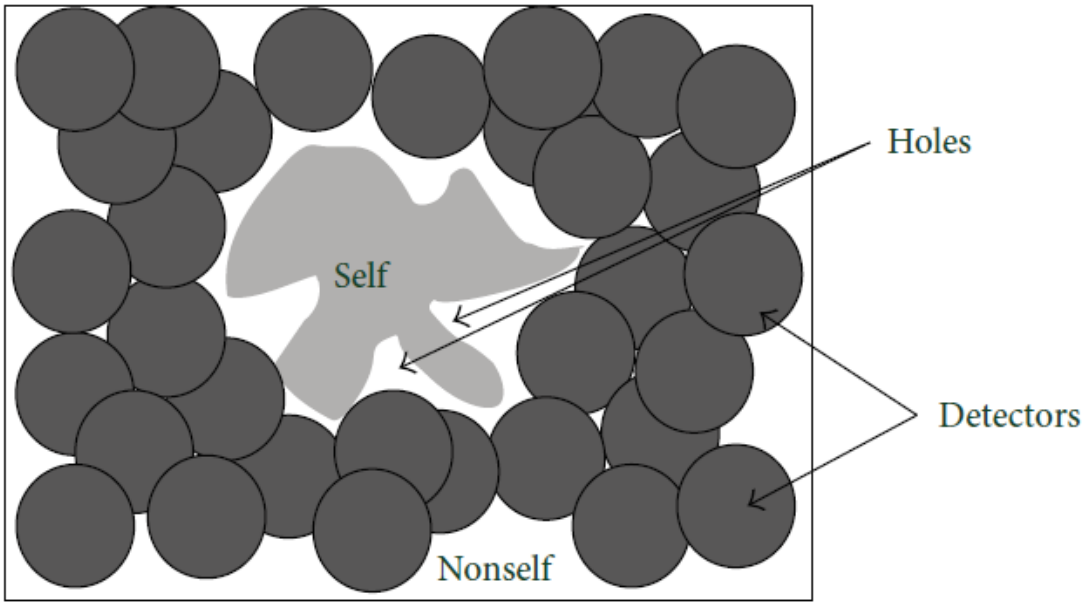


Σχήμα 4. Αναπαράσταση Real - value

Στους real – valued NS αλγορίθμους, ένας μεγάλος αριθμός ανιχνευτών σταθερού μεγέθους είναι απαραίτητος για την κάλυψη μεγάλης περιοχής μη-εαυτού διαστήματος, ενώ κανένας ανιχνευτής δεν μπορεί να χωρέσει στη μικρή περιοχή του μη-εαυτού διαστήματος, ειδικά κοντά στα όρια μεταξύ του εαυτού και του μη εαυτού [73, 74]. Ως εκ τούτου, προτάθηκε μια μεταβλητή ακτίνα στους ανιχνευτές μεταβλητού μεγέθους που ονομάζεται V-detector [75]. Ο V-detector αλγόριθμος παράγει υποψήφιους ανιχνευτές τυχαία, στους οποίους η ακτίνα ενός ανιχνευτή αλλάζει δυναμικά το μέγεθος της έως ότου το όριο της περιοχής να έρθει σε επαφή με την πλησιέστερη υπερσφαίρα ενός αυτο-στοιχείου. Ο αλγόριθμος τερματίζεται εάν δημιουργηθεί ο προκαθορισμένος αριθμός ανιχνευτών ή εάν καλυφθεί το προκαθορισμένο ποσοστό του μη εαυτού. Η ευελιξία που παρέχεται από τη μεταβλητή ακτίνα είναι ευκολονόητη. Ο Ostaszewski υπολόγισε επίσης μεταβλητές παραμέτρους ανιχνευτών για την κάλυψη του μη εαυτού διαστήματος [76]. Εκτός αυτού, προτάθηκε ένας feedback NSA για να λύσει την ανίχνευση ανωμαλιών, ο οποίος ρυθμίζει προσαρμοστικά την ακτίνα εαυτού και την ακτίνα ανίχνευσης αλλά και τον αριθμό των ανιχνευτών σύμφωνα με το αποτέλεσμα ανίχνευσης [77].

Το ζήτημα των κενών (η περιοχή μη-εαυτού που δεν μπορεί να καλυφθεί από έγκυρους ανιχνευτές, βλέπε Σχήμα 5) προκάλεσε τους γεωμετρικούς ανιχνευτές, πράγμα που σημαίνει ότι όχι μόνο η ακτίνα του ανιχνευτή αλλά και το σχήμα του ανιχνευτή μπορούν να αλλάξουν. Ο Zhou Ji ανέφερε ότι η μεταβλητότητα του ανιχνευτή μπορεί επίσης να επιτευχθεί με σχήματα ανιχνευτών ή κανόνες αντιστοίχισης και ούτω

καθεξής. Το NS με Κανόνες Ανίχνευσης (NSDR) χρησιμοποιεί έναν γενετικό αλγόριθμο για την ανάπτυξη ανιχνευτών με ένα hyperrectangle (υπέρ ορθογώνιο) σχήμα που μπορεί να καλύψει το διάστημα του μη-εαυτού . Χρησιμοποίησαν μια διαδοχική τεχνική εξειδίκευσης για να αναπτύξουν πολλαπλούς ανιχνευτές στην αρχική έκδοση [78] και στη συνέχεια χρησιμοποίησαν προσδιοριστική συσσώρευση ως την τεχνική εξειδίκευσης στη βελτιωμένη έκδοση [79]. Επιπλέον, ο Shapiro και οι συνεργάτες χρησιμοποίησαν υπερελλιψοειδή αντί για υπερσφαίρες για να εκφράσουν τους ανιχνευτές [80]. Το υπερελλιψοειδές είναι μια ειδική υπερσφαίρα που μπορεί να τεντωθεί και να επαναπροσανατολιστεί για να ταιριάζει στα όρια του εαυτού και του μη εαυτού. Οι Balachandran κ.α. ενσωμάτωσαν μαζί αυτούς τους πολλαπλούς ανιχνευτές υπερσφαιρών για να καλύψουν την περιοχή του μη-εαυτού [81]. Τα πειραματικά αποτελέσματά τους, δείχνουν ότι οι ανιχνευτές πολλαπλών σχημάτων παρέχουν καλύτερη κάλυψη του χώρου του μη-εαυτού από άλλες προσεγγίσεις χρησιμοποιώντας μόνο έναν τύπο ανιχνευτών και λιγότερο χρόνο.



Σχήμα 5. NSA. Τυχαία δημιουργία υποψήφιων ανιχνευτών (εμφανίζονται μεσκούρο κύκλο) οι οποίοι εάν ταιριάζουν με οποιονδήποτε εαυτό (δηλαδή, εάν κάποιο από τα σημεία που καλύπτονται από τον ανιχνευτή βρίσκεται στο σετ των εαυτών), εξαλείφονται και αναγεννούνται μέχρι να λάβουν αρκετούς έγκυρους ανιχνευτές [61].

Όταν ασχολούνται με δεδομένα πραγματικής αξίας, η πλειονότητα των ερευνών AIS χρησιμοποιεί τις αποστάσεις του Ευκλείδη και του Manhattan στο σχήμα του διαστήματος [82]. Επιπλέον, η διαφορά μεταξύ των αποστάσεων του Ευκλείδη και του Manhattan έχει συζητηθεί από τους Freitas και Timmis [83].

Τέλος, οι υβριδικές αναπαραστάσεις είναι πιθανές και διαισθητικά επιθυμητές κατά την αντιμετώπιση συνόλων δεδομένων που έχουν χαρακτηριστικά διαφορετικών τύπων δεδομένων [84]. Τα αριθμητικά χαρακτηριστικά κωδικοποιούνται σε μορφή πραγματικής αξίας και τα χαρακτηριστικά κατηγοριών κωδικοποιούνται σε συμβολοσειρές. Στη μελέτη των Kotov & Vasilyev [85], επέλεξαν διανύσματα παραμέτρων για να αντιπροσωπεύσουν το μοτίβο δικτύου, συμπεριλαμβανομένου του αριθμού των byte και των flag τιμών . Ωστόσο, ορισμένοι αλγόριθμοι δεν μπορούν να χειριστούν αυτά τα δεδομένα. Για παράδειγμα, [66] εφαρμόζουν τον NSA σε πολυδιάστατα δεδομένα προσωπικού που περιέχουν τόσο κατηγοριακά όσο και αριθμητικά δεδομένα. Ωστόσο, αντί να χρησιμοποιούν μια υβριδική κατηγοριακή/αριθμητική αναπαράσταση και να λαμβάνουν υπόψη όλα τα χαρακτηριστικά, απλά αγνοούν τα κατηγοριακά χαρακτηριστικά και λειτουργούν μόνο με τα αριθμητικά χαρακτηριστικά.

4.3. Αλγόριθμος Παραγωγής

Η δημιουργία ακριβών και αποτελεσματικών ανιχνευτών είναι σημαντική όταν εφαρμόζεται το AIS σε ένα πρόβλημα ανίχνευσης. Ένας καλός ανιχνευτής δεν πρέπει να καλύπτει το δικό του διάστημα και θα πρέπει να έχει ελάχιστη επικάλυψη με τους υπόλοιπους ανιχνευτές. Οι περισσότερες μέθοδοι που βασίζονται στο NSA παράγουν τυχαία ανιχνευτές όπως περιγράφεται στο αρχικό NSA του Forrest. Η τυχαία παραγωγή κατανέμεται ομοιόμορφα μεταξύ του διαστήματος του μη-εαυτού και επιλύει το πρόβλημα του άγνωστου διαστήματος του μη-εαυτού. Στη φάση εκπαίδευσης, ο αλγόριθμος δημιουργεί τυχαία ένα σύνολο ανιχνευτών. Το κάθε σύνολο αποτυγχάνει να ταιριάξει με οποιοδήποτε στοιχείο στον εαυτό του. Στη συνέχεια, στη φάση δοκιμής, αυτοί οι ανιχνευτές εφαρμόζονται για να ταξινομήσουν τα νέα δεδομένα ως εαυτός ή μη-εαυτός, όπως το Σχήμα 5.

Παρόλο που η μέθοδος αυτή υιοθετείται συχνά σε άλλα ερευνητικά έργα, όπως επισημαίνεται από τον Stibor [86], αυξάνει τις δυνατότητες δημιουργίας άκυρων ανιχνευτών. Με την αύξηση του μεγέθους της αυτορύθμισης, η πολυπλοκότητα του χρόνου εκτέλεσης της παραγωγής ανιχνευτών έχει εξαιρετική ανάπτυξη.

Ο D'haeseleer εισήγαγε δύο αλγόριθμους παραγωγής ανιχνευτών: τον αλγόριθμο δημιουργίας ανιχνευτών γραμμικού χρόνου και τον άπληστο αλγόριθμο δημιουργίας ανιχνευτών [87]. Συγκρίθηκαν με τη μέθοδο του Forrest που ονομάζεται "εξαντλητικός

αλγόριθμος παραγωγής ανιχνευτών". Ο γραμμικός αλγόριθμος επιλύει μια επανάληψη μέτρησης για τον αριθμό των συμβολοσειρών που δεν ταιριάζουν με τις συμβολοσειρές στους υποψήφιους ανιχνευτές και στη συνέχεια χρησιμοποιεί τον αριθμό που επιβάλλεται από την επανάληψη της μέτρησης για να επιλέγει ανιχνευτές τυχαία από αυτό το σύνολο υποψήφιων ανιχνευτών. Σε σύγκριση με τον εξαντλητικό αλγόριθμο, το πλεονέκτημα του γραμμικού αλγορίθμου είναι προφανές, επειδή αφαιρεί τις συμβολοσειρές μοτίβου που δεν θα γίνουν έγκυρες συμβολοσειρές ανιχνευτών. Ο άπληστος αλγόριθμος βελτιώνει τον γραμμικό αλγόριθμο μέσω της εξάλειψης των περιττών ανιχνευτών. Διαδίδει τους ανιχνευτές και παρέχει τη μέγιστη κάλυψη για έναν δεδομένο αριθμό ανιχνευτών. Ωστόσο, θυσιάζει την ταχύτητα της παραγωγής ανιχνευτών. Ο χρόνος θα αυξηθεί γραμμικά με το μέγεθος της αυτορύθμισης. Ο Castro και ο Timmis πρότειναν το NS με αλγόριθμο μετάλλαξης (NSMutation) ο οποίος έχει καλύτερη απόδοση όσον αφορά την πολυπλοκότητα του χρόνου. Το NSMutation έχει μια μικρή τροποποίηση του εξαντλητικού σταδίου του NS εισάγοντας σωματική υπερμετάλλαξη [55]. Ο στόχος του αλγόριθμου NSMutation είναι να καθοδηγήσει τον υποψήφιο ανιχνευτή μακριά από την αυτορύθμιση κατά τη διαδικασία μετάλλαξης ενός υποψήφιου ανιχνευτή. Στο [88], οι συντάκτες κατέληξαν στο συμπέρασμα ότι το NSMutation είναι παρόμοιο με τον εξαντλητικό αλγόριθμο με τη διαφορά της εξάλειψης του πλεονασμού και της κατοχής παραμέτρων που μπορούν να βελτιστοποιηθούν για καλύτερη απόδοση. Όλοι αυτοί οι αλγόριθμοι δημιουργίας ανιχνευτών χρονικής και διαστημικής πολυπλοκότητας παρουσιάζονται στον πίνακα 4, όπου το m είναι ο αλφαβητικός πληθυσμός, το l είναι το μήκος της συμβολοσειράς, το r είναι το όριο αντιστοίχισης, το Ns είναι ο αριθμός του εαυτού, και το NR είναι ο αριθμός των ανιχνευτών.

Πίνακας 3. Χρονικές και διαστημικές πολυπλοκότητες όλων των αλγορίθμων παραγωγής ανιχνευτών [88].

Algorithm	Time	Space
Exhaustive	$O(m^l \cdot N_S)$	$O(l \cdot N_S)$
Linear	$O((l-r+1)\cdot N_S \cdot m^r) + O((l-r+1)\cdot m^r) + O(l \cdot N_R)$	$O((l-r+1)^2 \cdot m^r)$
Greedy	$O((l-r+1)\cdot N_S \cdot m^r) + O((l-r+1)\cdot m^r \cdot N_R)$	$O((l-r+1)^2 \cdot m^r)$
NSMutation	$O(m^l \cdot N_S) + O(N_R \cdot m^r) + O(N_R)$	$O(l \cdot (N_S + N_R))$

Στο HIS, η κλωνική επιλογή χρησιμοποιείται για τον πολλαπλασιασμό και τη διαφοροποίηση της διέγερσης των κυττάρων με αντιγόνα. Ο Burne όπως προαναφέρθηκε στο κεφάλαιαο 3, πρότεινε το 1959 [89] ότι μπορούμε να βελτιώσουμε

την παραγωγή τυχαίων ανιχνευτών με την αρχή της κλωνικής επιλογής. Η τεχνητή μορφή της κλωνικής επιλογής διαδόθηκε από τους de Castro και Von Zuben. Έδωσαν έναν αλγόριθμο που ονομάζεται CSA [90], ο οποίος στη συνέχεια τροποποιήθηκε και μετονομάστηκε σε CLONALG [50]. Ο Garrett εισήγαγε ένα προσαρμοστικό CSA ως τροποποίηση του CLONALG [91]. Το CSA χρησιμοποιείται πάντα ως στρατηγική για τη βελτιστοποίηση και την αναγνώριση προτύπων [92]. Είναι ένας μηχανισμός αναζήτησης αποικιών στη φύση, ο οποίος επιτρέπει στους ανιχνευτές να κλωνοποιούν τους γονείς τους σύμφωνα με έναν μηχανισμό μετάλλαξης με υψηλά ποσοστά. Αυτή η στρατηγική εξελίσσει το ανοσοποιητικό σύστημα έτσι ώστε να μπορεί να αντιμετωπίσει τα αντιγόνα που έχει συναντήσει στο παρελθόν. Από αυτό, οι ερευνητές συνδυάζουν την κλωνική επιλογή με άλλες μεθόδους για την επίλυση προβλημάτων του ID. Ο Kim και ο Bentley υιοθέτησαν την κλωνική επιλογή ως ένα στοιχείο του AIS για το NID [65, 66, 92]. Ο Liu εφάρμοσε το CSA στη διαδικασία μοντελοποίησης της φυσιολογικής συμπεριφοράς στο ID και τα πειραματικά αποτελέσματα έδειξαν ότι ο αλγόριθμος έχει υψηλότερο ρυθμό ανίχνευσης (DR) και χαμηλότερο ρυθμό ψευδούς συναγερμού (FA) [93], σε σύγκριση με τους αλγορίθμους που εφαρμόζουν τον γενετικό αλγόριθμο σε ID ή εφαρμόζουν το NSA του AIS σε ID. Ο Tang παρουσίασε ένα CSA βασισμένο σε ένα άπληστο μοντέλο για το NID, το οποίο έχει επίσης υψηλότερο DR και χαμηλότερο FA σε σύγκριση με άλλες προσεγγίσεις [94]. Εκτόςαυτού, πολλέςάλλεςπροσεγγίσειςαναφέρθηκανστο“Recent advances in artificial immune systems: models and applications” των Dasgupta, Yu, & Nino [95]. Επιπλέον, το διάσημο μοντέλο ανοσοποιητικού δικτύου aiNet [96] χρησιμοποιεί επίσης CLONALG με πρόσθετες αλληλεπιδράσεις δικτύου. Ο μηχανισμός που χρησιμοποιείται από το μοντέλο aiNet βασίζεται στις ιδέες της κλωνικής επιλογής και συνδυάζεται κυρίως με τη θεωρία του ανοσοποιητικού δικτύου. Υπάρχει ένα δίκτυο διεγερτικών και κατασταλτικών αλληλεπιδράσεων μεταξύ αντισωμάτων που επηρεάζουν τις συγκεντρώσεις κάθε τύπου αντισώματος και στη συνέχεια φθάνουν σε κατάσταση ισορροπίας. [97].

Σύμφωνα με τα χαρακτηριστικά του AIS, πολλές μέθοδοι και τεχνικές έχουν συνδυαστεί με το AIS για την καλύτερη ανίχνευση της ανώμαλης συμπεριφοράς, όπως τεχνητά νευρικά δίκτυα, ασαφή συστήματα και γενετικοί αλγόριθμοι. Για παράδειγμα, [71] ο συνδυασμός NSA και ενόςσυμβατικού αλγόριθμου ταξινόμησης για την ανίχνευση ανωμαλιών·[98] παρουσιάζει μια ανοσολειτουργική προσέγγιση στην ανίχνευση ανωμαλιών, επειδή η ασαφής λογική μπορεί να παρέχει έναν καλύτερο

ορισμό του ορίου μεταξύ φυσιολογικής και μη φυσιολογικής συμπεριφοράς. Ο Dasgupta πρότεινε ένα Πολυεπίπεδο Αλγόριθμο Ανοσολογικής Μάθησης (MILA) για την ανίχνευση εισβολών και την έκδοση συναγερμών [99]. Ο ανιχνευτής MILA χρησιμοποίησε πολλαπλές στρατηγικές για τη δημιουργία ανιχνευτών, όπου οι ανιχνευτές Τ εκτελούσαν συνεχή αμφίσημη αντιστοιχία χαμηλού επιπέδου, ενώ οι ανιχνευτές Β εκτελούσαν αντιστοιχία υψηλού επιπέδου σε μη συνεχόμενες θέσεις συμβολοσειρών. Οι ενεργοί ανιχνευτές Τ θα παρέχουν περαιτέρω ένα σήμα για να βοηθήσουν στην ενεργοποίηση των ανιχνευτών Β. Αυτό το μοντέλο προσομοιώνει περαιτέρω το NSA, το CSA, και την σωματική υπέρ-μετάλλαξη των ώριμων Τ κυττάρων και των Β κυττάρων.

Ένα υβριδικό σύστημα που αποτελείται από AIS και ένα αυτοοργανωτικό χάρτη παρουσιάζεται στο "A hybrid artificial immune system and Self Organising Map for network intrusion detection" των Powers&He[100]. Τα πειραματικά αποτελέσματά τους έδειξαν υψηλότερο ποσοστό ανίχνευσης και ταξινόμησης για επιθέσεις Denial-of-Service και User-to-Root.

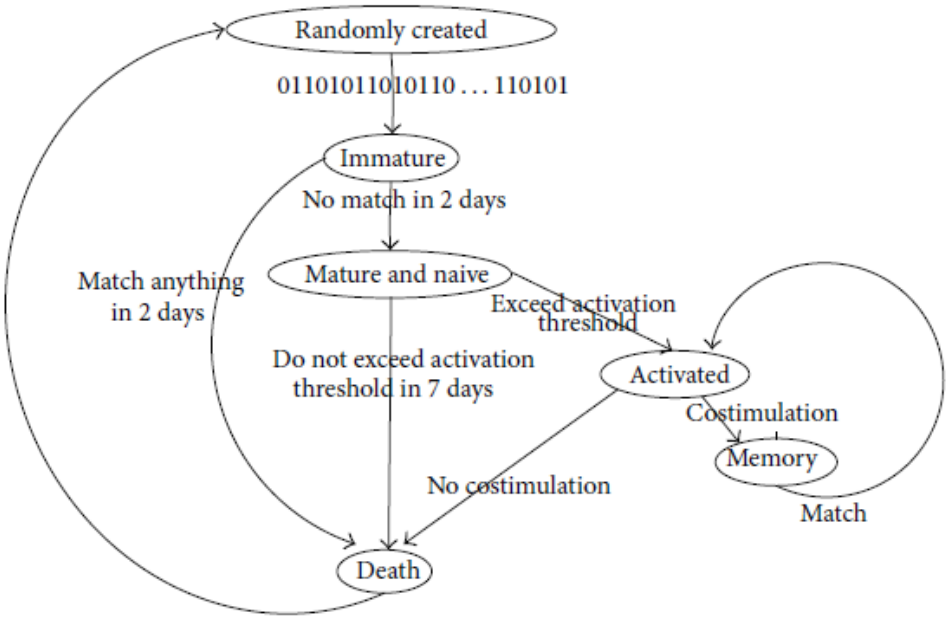
Η διάκριση του εαυτού και του μη-εαυτού είναι η θεμελιώδης αρχή που καθοδηγεί την ανάπτυξη του AIS. Ως εκ τούτου, το NS ενεργεί ως σημαντικός ρόλος στο AIS. Ωστόσο, ο Matzinger πρότεινε τη θεωρία κινδύνου (DT) και υποστήριξε ότι οι ανοσολογικές αποκρίσεις ενεργοποιούνται από τα σήματα κινδύνου που αποστέλλονται όταν τα κύτταρα πεθαίνουν με έναν αφύσικο θάνατο, όχι από τα αντιγόνα του μη-εαυτού [101, 102]. Αυτό παρέχει μια νέα ιδέα για το AIS. Με βάση αυτή την ιδέα, ο Aickelin και η ερευνητική του ομάδα εφάρμοσαν την DT σε IDS [58, 103]. Στην έρευνά τους, τα σήματα κινδύνου αντιπροσωπεύονται ως αριθμοί. Στη συνέχεια, οι Twycross και Aickelin παρουσίασαν ένα πλαίσιο libtissue1(implementing innate immunity) που ενσωματώνει ιδέες από έμφυτη ανοσία στους AIS. Το libtissue έχει αρχιτεκτονική πελάτη/διακομιστή. Οι πελάτες στο libtissue συλλέγουν αντιγόνα και εξωτερικά σήματα και τα μεταδίδουν στο διακομιστή libtissue. Οι διακομιστές εφάρμοσαν τον αλγόριθμο AIS. Χρησιμοποίησαν libtissue για τη δυναμική ανίχνευση ανωμαλιών. Από τα δενδριτικά κύτταρα και την αλληλεπίδρασή τους με τα Τ κύτταρα της DT, ο αλγόριθμος Dendritic Cell Algorithm (DCA) και ο αλγόριθμος Toll-Like Receptor Algorithm (TLRA) προτάθηκαν από τους Greensmith και Aickelin, Twycross και Aickelin, αντίστοιχα. [104, 105] Το TLRA αναπτύχθηκε στο πλαίσιο libtissue για

[1]Το σύστημα libtissue είναι ένα έμφυτο ανοσοποιητικό πλαίσιο που εφαρμόζεται ως API

την ανίχνευση μη φυσιολογικής διεργασίας [106, 107]. Ωστόσο, το DCA βασίζεται στην πτυχή της επεξεργασίας σήματος χρησιμοποιώντας πολλαπλά σήματα εισόδου και εξόδου, ενώ το TLRA χρησιμοποιεί μόνο σήματα κινδύνου. Ωστόσο το DTA εξακολουθεί να είναι αμφιλεγόμενο μεταξύ των ανοσολόγων σχετικά με τον τρόπο του σαφούς προσδιορισμού των σημάτων κινδύνου.

4.4. Τρόπος Εξέλιξης

Με την ανάπτυξη του συστήματος, οι ανιχνευτές θα αυξηθούν. Ωστόσο, το σύστημα είναι πεπερασμένο, όπως το σώμα, δεν μπορούμε να παράγουμε ανιχνευτές για πάντα. Οι παλιοί και μη έγκυροι ανιχνευτές πρέπει να εξαλειφθούν. Ενώ οι συμπεριφορές εισβολής εμφανίζονται καθημερινά, οι νέοι ανιχνευτές πρέπει να δημιουργούν και να εξελίσσονται για να τους ανιχνεύουν. Αντί να πετάει αναποτελεσματικά ανιχνευτές που ταιριάζουν με δείγματα εαυτού, ο Hofmeyer πρότεινε την αλλαγή των ανιχνευτών με την πάροδο του χρόνου, δηλαδή να γίνουν δυναμικοί. [61]. Έδωσε σε κάθε ανιχνευτή μια πεπερασμένη διάρκεια ζωής. Στο τέλος της ζωής του, ο ανιχνευτής θα εξαλειφθεί και θα αντικατασταθεί από έναν νέο τυχαία παραγόμενο ανιχνευτή. Η εικόνα του κύκλου ζωής ενός ανιχνευτή, όπως φαίνεται στο Σχήμα 6.



Σχήμα 6. Ο κύκλος ζωής του ανιχνευτή [108]

Ο Ayara [88], ο Gonzalez και ο Dasgupta [109] προσπάθησαν να δώσουν στους ανιχνευτές ένα χρονικό διάστημα πριν τους εξαλείψουν.

Ο Κιμ και ο Μπέντλεϊ διερεύνησαν περαιτέρω επέκταση του DynamiCS [110]· όταν οι ανιχνευτές μνήμης δείχνουν χαμηλό βαθμό αυτο-ανοχής σε νέα αντιγόνα, θα εξαλειφθούν. Ο Li πρότεινε μια επεξεργασία υποδοχέων που ενέπνευσε το πραγματικό NSA [111]. Για τον ανιχνευτή που ταιριάζει με τον εαυτό του, ο αλγόριθμος χρησιμοποιεί επεξεργασία κατευθυντικών υποδοχέων για να κάνει μια νέα ζωή και, για τον ανιχνευτή που δεν ταιριάζει με τον εαυτό του, ο αλγόριθμος χρησιμοποιεί επεξεργασία υποδοχέων κατεύθυνσης για τον προσδιορισμό του ίδιου πλησιέστερου εαυτού για να επεκτείνει την κάλυψη του διαστήματος του μη-εαυτού.

Εάν δημιουργηθούν νέοι ανιχνευτές λαμβάνοντας ανατροφοδότηση από προηγούμενους ανιχνευτές αντί για τυχαίους, τότε ο νέος ανιχνευτής μπορεί να είναι πιο κατάλληλος για τα αντιγόνα του μη-εαυτού. Οι Hightower [112], Perelson [113], και Oprea & Forrest [114] χρησιμοποίησαν έναν γενετικό αλγόριθμο (GA) για να μελετήσουν τις επιπτώσεις της εξέλιξης στη γενετική κωδικοποίηση των μορίων αντισωμάτων, η οποία μπορεί να φανεί ως στρατηγική ανατροφοδότησης. Επιπλέον, [115] ενσωμάτωσαν το στάδιο της βιβλιοθήκης γονιδίων των Kim και Bentley στο τεχνητό ανοσοποιητικό μοντέλο τους για το NID. Η βιβλιοθήκη γονιδίων είναι μια δυναμική εξελικτική βιβλιοθήκη που αποθηκεύει τα πιθανά γονίδια των ανιχνευτών και οι ποικίλοι γενετικοί μηχανισμοί παράγουν νέους ανιχνευτές. Τα πιθανά γονίδια είναι τα επιλεγμένα πεδία προφίλ για να περιγράψουν ανώμαλα μοτίβα κυκλοφορίας δικτύου. Μετά από αυτό, χρησιμοποιούν τους διαγραμμένους ανιχνευτές μνήμης ως εικονική βιβλιοθήκη γονιδίων [116]. Στην πραγματικότητα, η μέθοδός τους συνάδει με τη θεωρία HIS, επειδή οι διαγραμμένοι ανιχνευτές προέρχονται επίσης από γονιδιακές βιβλιοθήκες.

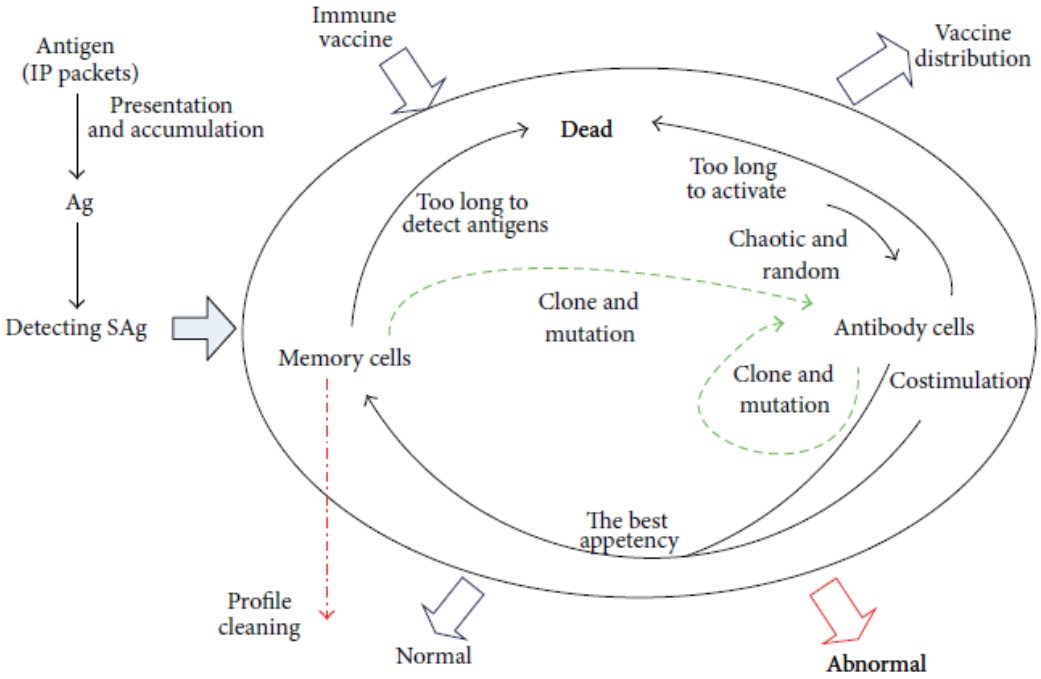
Ο Zeng χρησιμοποιεί επίσης τη βιβλιοθήκη γονιδίων για να δημιουργήσει τους νέους ανιχνευτές στο αρχικό IDS [117]. Έτσι, οι βιβλιοθήκες γονιδίων παρέχουν έναν τρόπο να θυμόμαστε προηγούμενες συναντήσεις, έτσι ώστε η δημιουργία αντισωμάτων να είναι πιο πιθανό να ταιριάζει με νέες συστάδες που είναι ωστόσο παρόμοιες με αυτές που παρατηρήθηκαν πριν από λίγο καιρό. [118].

Η γονιδιακή βιβλιοθήκη είναι μια προσέγγιση που καθοδηγεί τη διαδικασία παραγωγής αντισωμάτων με καλή πιθανότητα επιτυχίας. Ωστόσο, οι προσεγγίσεις της γονιδιακής βιβλιοθήκης είναι σχετικά περίπλοκες. Εκτός από την αλλαγή της ακτίνας και του σχήματος του ανιχνευτή, μια άλλη προσέγγιση για τη βελτίωση της αποτελεσματικότητας είναι απλά η μετακίνηση της θέσης του ανιχνευτή. Οι Gonzalez και Dasgupta υπολόγισαν τους k-γείτονες του ανιχνευτή στο σύνολο εαυτού, και στη

συνέχεια υπολόγισαν τη διάμεση απόσταση αυτών των k-γειτόνων. Εάν αυτή η διάμεση απόσταση είναι μικρότερη από ένα όριο, ο ανιχνευτής θεωρείται ότι ταιριάζει με τον εαυτό του και μετακινείται προς την αντίθετη κατεύθυνση. Αυτή η στρατηγική είναι καλή για να είναι ισχυρή στο θόρυβο και τις ακραίες τιμές [109]. Ο Laurentys διανέμισε τους ανιχνευτές σε μικτούς κινούμενους ανιχνευτές του διαστήματος των μη-εαυτών και των ανιχνευτών που δημιουργούνται με σταθερή ακτίνα και V-ανιχνευτή μαζί [119].

Ένα IDS αξιολογεί μια εικαζόμενη εισβολή μόλις λάβει θέση και σηματοδοτεί συναγερμό. Στην πραγματικότητα, οι περισσότερες τρέχουσες ID μέθοδοι δεν μπορούν να επεξεργαστούν μεγάλες ποσότητες δεδομένων ελέγχου για λειτουργίες σε πραγματικό χρόνο. Οι ρόλοι του εαυτού και του μη-εαυτού τους μπορούν να ανταλλάσσονται δυναμικά. Δηλαδή, οι τωρινές νομικές συμπεριφορές μπορεί να είναι επικίνδυνες την επόμενη φορά, και αντίστροφα.. Τα τελευταία χρόνια, οι επιστήμονες υπολογιστών έχουν σχεδιάσει αλγορίθμους εμπνευσμένους από το ανοσοποιητικό που θα μπορούσαν να ανιχνεύσουν αποτελεσματικά την ανώμαλη συμπεριφορά.. Το DynamiCS έχει κάνει μια δοκιμή για αυτή την περίπτωση [64]. Μπορεί να είναι σε θέση να αντιμετωπίσει ένα πραγματικό περιβάλλον όπου οι συμπεριφορές του εαυτού αλλάζουν μετά από μια συγκεκριμένη περίοδο. Το DynamiCS εισήγαγε τρεις σημαντικές παραμέτρους: την περίοδο ανοχής ενός ανώριμου ανιχνευτή, το κατώτατο όριο ενεργοποίησης ενός ώριμου ανιχνευτή και τη διάρκεια ζωής ενός ώριμου ανιχνευτή, αλλά μόνο μία περίοδος ανίχνευσης για την αυτοενημέρωση· είναι πολύ σύντομο για να συλλέξει αρκετά στοιχεία του εαυτού του. Ο Li πρότεινε ένα νέο μοντέλο ID δυναμικής που βασίζεται στο ανοσοποιητικό (Idid) [120]. Στο Idid, χτίζονται τα δυναμικά μοντέλα και οι αντίστοιχες αναδρομικές εξισώσεις του κύκλου ζωής των ώριμων λεμφοκυττάρων και της ανοσολογικής μνήμης. η δυναμική περιγραφή του εαυτού και του μη-εαυτού του επιλύεται. Ο Yang παρουσίασε ένα μοντέλο ασφάλειας δικτύου με βάση το AIS, το οποίο χρησιμοποίησε κατανεμημένους παράγοντες για να καταγράψει την κυκλοφορία του δικτύου σε πραγματικό χρόνο [121]. Το μοντέλο απεικόνιζε τις δυναμικές εξελίξεις του εαυτού, αντιγόνα, ανοσολογική ανοχή, κύκλο ζωής ώριμου παράγοντα και ανοσολογική μνήμη. Τα πειραματικά αποτελέσματά τους δείχνουν ότι έχει τα χαρακτηριστικά της επεξεργασίας σε πραγματικό χρόνο και της αυτοπροσαρμογής. Ο Peng πρότεινε έναν αλγόριθμο ανίχνευσης δυναμικών ανωμαλιών με ανοσοποιητικό NS (DADAI) [108], συνδυάζοντας τη θεωρία κλώνων του αντισώματος και τον εμβολιασμό. Καθιέρωσε

δυναμικές διατυπώσεις εξέλιξης προφίλ ανίχνευσης που μπορούν να συγχρονίσουν δυναμικά τα προφίλ ανίχνευσης με το πραγματικό περιβάλλον δικτύου. Ο αλγόριθμος περιέχεται στο Σχήμα 7. Θεωρητική ανάλυση και πειραματικά αποτελέσματα έδειξαν ότι το DADAI μπορεί να αναπτυχθεί αποτελεσματικά στο NID σε πραγματικό χρόνο σε περιβάλλον δικτύου υψηλής ταχύτητας.



Σχήμα 7. Δυναμική ανίχνευση ανωμαλιών σε πραγματικό χρόνο με ανοσοποιητικό NS [108]

Κεφάλαιο 5. ΣΥΜΠΕΡΑΣΜΑΤΑ

Αυτή η ανασκόπηση επικεντρώθηκε στο IDS που βασίζεται στο AIS. Παρουσίασε για μια σύντομη εισαγωγή στο AIS προκειμένου να παρέχει στους αναγνώστες το υπόβαθρο για να το κατανοήσουν. Η κύρια συμβολή αυτής της εργασίας είναι το πλαίσιο για το σχεδιασμό του IDS που βασίζεται στο AIS. Με βάση αυτό το πλαίσιο, περιεγράφηκαν τρεις πτυχές, ακολουθούμενες από εξερευνήσεις των βιβλιογραφιών σχετικά με τα IDS. Αυτές οι θεωρίες και προσεγγίσεις που βασίζονται στο AIS είναι σε θέση να συνδυαστούν για να χρησιμεύσουν ως βάση για αποτελεσματική ID μέσω της ανάλυσης που αναπτύχθηκε. Από την ανάλυση του πλαισίου που αναπτύχθηκε στην παρούσα εργασία, διαπιστώνουμε ότι το σύστημα με πραγματική αντιπροσώπευση είναι καταλληλότερο για IDS, στο οποίο οι ανιχνευτές δημιουργούνται αποτελεσματικά και εξελίσσονται δυναμικά.

Τα τελευταία χρόνια, η έρευνα AIS έχει απομακρυνθεί από τα βιολογικά ελκυστικά μοντέλα, και ακολουθεί τις βιολογικές λεπτομέρειες, όπως το DCA, το οποίο είναι εμπνευσμένο από το ρόλο των δενδριτικών κυττάρων (ένα εξειδικευμένο αντιγόνο που παρουσιάζει κύτταρα που παρέχουν μια ζωτική σύνδεση μεταξύ του έμφυτου και του προσαρμοστικού ανοσοποιητικού συστήματος) [122]. Είναι πιο χρήσιμο στην ασφάλεια του υπολογιστή, καθώς δεν αντιπροσωπεύουν όλα τα ανώμαλα συμβάντα επιθέσεις [105, 123]. Η υπόθεση του Κατώτατου Ορίου Ενεργοποίησης (TAT) του Grossman [124] είναι μια άλλη προοπτική. Το TAT υποστηρίζει ότι κάθε μεμονωμένο ανοσοποιητικό κύτταρο έχει το δικό του κατώτατο όριο ενεργοποίησης τόνου, η αξία του οποίου αντικατοπτρίζει το πρόσφατο ιστορικό αλληλεπιδράσεων με το περιβάλλον. Οι Antunes και Correia [125] περιέγραψαν το AIS που βασίζεται στο TAT για το NID. Η μελέτη«Ρυθμιζόμενοι ανιχνευτές για τεχνητό ανοσοποιητικό σύστημα: από μοντέλο σε αλγόριθμο» των Andrews&Timmis[126] δίνει την ανάλυση του προτύπου TAT. Υπάρχουν πολλοί χρήσιμοι και ισχυροί αλγόριθμοι που έχουν ήδη προκύψει και μπορεί να προκύψουν όταν περισσότερες από δύο από τις διαφορετικές προσεγγίσεις είναι υβριδικές ή προτείνεται νέα θεωρία HIS.

Όπως στην μελέτη των Andrews&Timmis[126] και άλλων επιστημών [123–125], πολλές περιλήψεις της έρευνας αναφέρθηκαν στο AIS. Το HIS ενσωματώνει τα

χαρακτηριστικά της ευρωστίας, της διανομής, του ελαφριού, της αυτό-οργάνωσης και της αυτό-προσαρμογής. Τα AIS είναι εξαιρετικά αφηρημένα μοντέλα των βιολογικών ομολόγων τους που εφαρμόζονται για την επίλυση προβλημάτων σε διαφορετικούς τομείς. Η αναλογία μεταξύ του HIS και του IDS προσελκύει φυσικά επιστήμονες των υπολογιστών για να κάνουν έρευνα σχετικά με τις προσεγγίσεις του ανοσοποιητικού συστήματος στο ID. Τα AIS έχουν επίσης χρησιμοποιηθεί σε συνδυασμό με άλλες προσεγγίσεις, προκειμένου να δημιουργηθούν πιο ισχυρά μοντέλα και να βελτιωθούν οι ατομικές επιδόσεις.

Παρά τα υπάρχοντα πλεονεκτήματα του AIS, τα IDS εξακολουθούν να έχουν πολλά προβλήματα, για παράδειγμα, έλλειψη υποστήριξης του συστήματος αντιμετώπισης IPv6, υψηλά επίπεδα ψευδώς θετικών και ψευδώς αρνητικών ποσοστών συναγερμού, έλλειψη γρήγορης απόκρισης για τις άγνωστες επιθέσεις. Και το AIS είναι ένας σχετικά νέος τομέας. Το IDS που βασίζεται στο AIS αντιμετωπίζει πολλές δυσκολίες: τα περιβάλλοντα του πραγματικού κόσμου είναι πολύ πιο περίπλοκα, οι αυτό-συλλογές αλλάζουν συνεχώς και η ανίχνευση είναι σε πραγματικό χρόνο. Προκειμένου να επιλυθούν όλα αυτά τα ζητήματα και να σημειωθεί πρόοδος σε αυτήν την έρευνα, τα μελλοντικά IDS μας θα πρέπει να επικεντρωθούν στα ζητήματα της γρήγορης απάντησης και λιγότερο στους ψευδούς συναγερμούς και του ψευδώς αρνητικού. Στο μέλλον, ανάλογα με τον βιολογικό ανοσοποιητικό μηχανισμό, θα είναι σε θέση να προτείνει αποτελεσματικά ID μοντέλα και αλγορίθμους, αν και θα υπάρχει ένας δύσκολος και τραχύς δρόμος.

Μελλοντικές έρευνες σχετικές με το παρόν αντικείμενο θα μπορούσαν να είναι η διερεύνησητου μηχανισμού εντοπισμού εισβολήςτου σταδίου επιλογής κλώνων.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] L.N. de Castro and F.J. Von Zuben, Artificial Immune Systems. Part I - Basic Theory and Applications. Technical Report DCA-RT 01/99, Department of Computer Engineering and Industrial Automation, School of Electrical and Computer Engineering, State University of Campinas, Brazil, 1999.

[2] Engelbrecht Andries P., Forrest S., Perelson A.S., Allen L., and Cherukuri R., Self-Nonself Discrimination in a Computer, In Proceedings of the IEEE Symposium on Research in Security and Privacy, pp. 202-212, 1994.

[3] Abbas, A. K. and A. H. Lichtman, Basic Immunology: Functions and Disorders of the Immune System, Saunders, 2004.

[4] Abbas, A. K. and A. H. Lichtman, Cellular and Molecular Immunology, 5th edition, Saunders, 2005.

[5] Bellanta, J. and Kadlec, J., Introduction to immunology, Chapter in the book entitled: Immunology: Basic Processes, edition, Saunders, pp. 1-15, 1985.

[8] Michael O' Neil, Antony Brabazon, Artificial Immune Systems, Chapter 7, In the book entitled: Biologically Inspired Algorithms for Financial Modelling, Publisher: Springer-Verlag, pp.115-127, 2004.-ΝΑΓΙΝΕΙ 39

[12] Schindler L., Kerrigan D. and Kelly J., Understanding the Immune System, Science Behind the News- National Cancer Institute , 2002.

[13] P.Bond, 2004, Standards for Security Categorization of Federal Information and Information Systems
http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.153.2832&rank=1

[14] D.E.Denning, 1982, Cryptography and Data Security
http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.81.5750

[15] Charles P. Pfleeger, Shari L. Pfleeger, 2003, Security in Computing

[16] J.M.Anderson, 2003, Why we need a new definition of information security, Computers & Security, Elsevier
http://www.sciencedirect.com/science/article/pii/S0167404803004073

[18] Dorothy E.Denning, 1996, Protection and Defence of Intrusion
http://faculty.nps.edu/dedennin/publications/Protection%20and%20Defense%20of%20I

ntrusion.htm

[19] J. P. Anderson, *Computer Security Technology Planning Study*, vol. 2, James P. Anderson Company, Fort Washington, Pa, USA, 1972

[20] J. P. Anderson, "Computer security threat monitoring and surveillance," Tech. Rep., James P. Anderson Company, Fort Washington, Pa, USA, 1980

[21] D. E. Denning, "An intrusion-detection model," *IEEE Transactions on Software Engineering*, vol. 13, no. 2, pp. 222–232, 1987.

[22] L. T. Heberlein, G. V. Dias, K. N. Levitt, B. Mukherjee, J. Wood, and D. D. Wolber, "A network security monitor," in *Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy*, pp. 296–304, Oakland, Calif, USA, May 1990.

[23] R. Heady, G.Luger, A.Maccabe, M.Servilla, 1990, The Architecture of a Network Level Intrusion Detection System

[24] J.P.Anderson, 1980, Computer Security Threat Monitoring and Surveillance http://www.mendeley.com/research/computer-security-threat-monitoring-and-surveillance-4/

[25] K.Scarfone, P.Mell, 2007, Guide to Intrusion Detection and Prevention Systems (IDPS), National Institute of Standards and Technology

[26] S.Axelsson, 2000, Intrusion Detection Systems: A Survey and Taxonomy

[27] H. Debar, M. Becker, D. Siboni, 1992, A neural network component for an intrusion detection system, Security and Privacy IEEE Symposium 1999, Conference Publications

[28] C. Warrender, S. Forrest, B. Pearlmutter, 1999, Detecting intrusion using system calls: alternative data models, Security and Privacy IEEE Symposium 1999, Conference Publications

[29] D. Anderson, T. Frivold, A. Valdes, 1995, Next-generation Intrusion Detection Expert System (NIDES) A summary, Computer Science Laboratory

[30] H.Debar, M.Dacier, A.Wespi, 1999, Towards a taxonomy of intrusion-detection systems, Elsevier

[36] A.Kibirkstis, 2009, Intrusion Detection FAQ: What Are The Top Selling IDS/IPS and What Differentiates Them from Each Other? http://www.sans.org/security-

resources/idfaq/top-selling-ids-ips.php

[37] M.Roesch, 1999, Snort-Lightweight Intrusion Detection for Networks http://www.usenix.org/event/lisa99/full_papers/roesch/roesch.pdf

[38] D. Dagupta and F. Gonz´alez "*An Immunity-Based Technique to Characterize Intrusions in Computer Networks*".IEEE Transactions on Evolutionary Computation, 6(3), pages 1081-1088 June 2002.

[40] Kim J. and Bentley P.J., Negative Selection and Niching by an Artificial Immune System for Network Intrusion Detection. Chapter 19 in the book entitled: Computational Intelligence. An introduction, Publisher John Wiley & Sons, pp. 458483, 2007.

[41] Potter M.A. and Jong K.A., The Coevolution of Antibodies for Concept Learning, In Proceedings of the Fifth International Conference on Parallel Problem Solving from Nature, pp. 530-539, 1998.

[42] Gonzalez F., Dasgupta D., and Kozma R., Combining Negative Selection and Classification Techniques for Anomaly Detection, In Proceedings of the Congress on Evolutionary Computation, volume 1, pp. 705-710, 2002.

[43] Stewart J. and Carneiro J., The Central and Peripheral Immune Systems: Modeling and Simulation, Chapter 3 in the book entitled Artificial Immune Systems and their applications, Publisher: Springer-Verlag, pp. 47-61, 1999.

[44] De Castro, L. and Von Zuben, F., Learning and optimization using the clonal selection principle, IEEE Transactions on Evolutionary Computation, Volume 3, pp.239-251, 2002.

[45] L.N. de Castro and F.J. Von Zuben, The Clonal Selection Algorithm with Engineering Applications, In Proceedings of the Genetic and Evolutionary Computational Conference, pages 36-37, 2000.

[46] Hofmeyr S., An Immunological Model of Distributed Detection and Its Application to Computer Security, PhD thesis, University of New Mexico, 1999.

[47] Knight T. and Timmis J., A Multi-Layered Immune Inspired Approach to Data Mining, In Proceedings of the Fourth International Conference on Recent Advances in Soft Computing, pp. 266–271, 2002.

[50] L. N. de Castro and F. J. von Zuben, “Learning and optimization using the clonal selection principle,” IEEE Transactions on Evolutionary Computation, vol. 6, no. 3, pp. 239–251, 2002.

[55] Αδάμου, Α. «Σχεδίαση και ανάπτυξη μηχανισμού για τη δυναμική ανίχνευση αργών επιθέσεων σε Συστήματα Ανίχνευσης Εισβολής (IDS)». Μεταπτυχιακή εργασία, ΑΠΘ Πολυτεχνική σχολή, Θεσσαλονίκη, 2013

[56] Γεωργίου Ε. «Ανάπτυξη αλγορίθμου τεχνητού ανοσοποιητικού συστήματος για τηνεπίλυσητου προβλήματος Δρομολόγησης Οχημάτων». Διατριβή, Πολυτεχνείο Κρήτης, 2010

[57] S. Forrest, L. Allen, A. S. Perelson, and R. Cherukuri, “Selfnonself discrimination in a computer,” in Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy, pp. 202–212, Oakland, Calif, USA, May 1994.

[61] S. A. Hofmeyr and S. Forrest, An Immunological Model of Distributed Detection and Its Application to Computer Security, The University of New Mexico, Albuquerque, NM, USA, 1999.

[62] P. K. Harmer, P. D. Williams, G. H. Gunsch, and G. B. Lamont, “An artificial immune system architecture for computer security applications,” IEEE Transactions on Evolutionary Computation, vol. 6, no. 3, pp. 252–280, 2002.

[63] J. Kim and P. J. Bentley, “Towards an artificial immune system for network intrusion detection: an investigation of clonal selection with a negative selection operator,” in Proceedings of the Congress on Evolutionary Computation (CEC ’01), pp. 1244– 1252, Seoul, Korea, May 2001.

[64] J. Kim and P. J. Bentley, “Towards an artificial immune system for network intrusion detection: an investigation of clonal selection,” in Proceedings of the Congress on Evolutionary Computation (CEC ’02), vol. 2, pp. 1015–1020, Honolulu, Hawaii, USA, May 2002.

[65] T. S. Sobh and W. M. Mostafa, “A cooperative immunological approach for detecting network anomaly,” Applied Soft Computing Journal, vol. 11, no. 1, pp. 1275–1283, 2011.

[66] D. Dasgupta and N. S. Majumdar, “Anomaly detection in multidimensional data using negative selection algorithm,” in Proceedings of the Congress on Evolutionary

Computation (CEC ’02), vol. 2, pp. 1039–1044, Honolulu, Hawaii, USA, May 2002.

[67] J. Balthrop, F. Esponda, S. Forrest, and M. Glickman, “Coverage and generalization in an artificial immune system,” in Proceedings of the Genetic and Evolutionary Computation Conference (GECCO ’02), pp. 3–10, July 2002.

[68] S. Forrest and S. Hofmeyr, “Immunity by design: an artificial immune system,” in Proceedings of the Genetic and Evolutionary Computation Conference (GECCO ’99), pp. 1289–1296, MorganKaufmann, San Francisco, Calif, USA, 1999.

[69] P. K. Harmer, “A distributed agent architecture for a computer virus immune system,” DTIC Document, 2000.

[70] F. Gonzalez, D. Dasgupta, and J. G´ omez, “The effect of binary´ matching rules in negative selection,” in Genetic and Evolutionary Computation-GECCO 2003, vol. 2723 of Lecture Notes in Computer Science, pp. 195–206, Springer, Berlin, Germany, 2003.

[71] F. Gonzalez, D. Dasgupta, and R. Kozma, “Combining negative selection and classification techniques for anomaly detection,” in Proceedings of the Congress on Evolutionary Computation (CEC ’02), vol. 1, pp. 705–710, Honolulu, Hawaii, USA, May 2002.

[72] J. Kim and P. J. Bentley, “An evaluation of negative selection in an artificial immune system for network intrusion detection,” in Proceedings of the Genetic and Evolutionary Computation Conference (GECCO ’01), pp. 1330–1337, 2001.

[73] Z. Ji, “A boundary-aware negative selection algorithm,” in Proceedings of the 9th IASTED International Conference on Artificial Intelligence and Soft Computing (ASC ’05), Acta Press, Benidorm, Spain, 2005.

[74] D. Wang, F. Zhang, and L. Xi, “Evolving boundary detector for anomaly detection,” Expert Systems with Applications, vol. 38, no. 3, pp. 2412–2420, 2011.

[75] Z.JiandD.Dasgupta,“Real-valuednegativeselectionalgorithm with variable-sized detectors,” in Genetic and Evolutionary Computation-GECCO 2004, vol. 3102 of Lecture Notes in Computer Science, pp. 287–298, Springer, Berlin, Germany, 2004.

[76] M. Ostaszewski, F. Seredynski, and P. Bouvry, “Coevolutionarybased mechanisms for network anomaly detection,” Journal of Mathematical Modelling and Algorithms, vol. 6, no. 3, pp. 411– 431, 2007.

[77] J. Zeng, T. Li, X. Liu, C. Liu, L. Peng, and F. Sun, “A feedback negative selection algorithm to anomaly detection,” in Proceedings of the 3rd International Conference on Natural Computation (ICNC ’07), pp. 604–608, Haikou, China, August 2007.

[78] D. Dasgupta and F. Gonzalez, “An immunity-based technique´ to characterize intrusions in computer networks,” IEEE Transactions on Evolutionary Computation, vol. 6, no. 3, pp. 281–291, 2002.

[79] F. A. Gonzalez and D. Dasgupta, “An imunogenetic technique to detect anomalies in network traffic,” in Proceedings of the Genetic and Evolutionary Computation Conference (GECCO ’02), pp. 1081–1088, Morgan Kaufmann, 2002.

[80] J. M. Shapiro, G. B. Lament, and G. L. Peterson, “An evolutionary algorithm to generate hyper-ellipsoid detectors for negative selection,” in Proceedings of the Genetic and Evolutionary Computation Conference (GECCO ’05), pp. 337–344, Atlanta, Ga, USA, June 2005.

[81] S. Balachandran, D. Dasgupta, F. Nino, and D. Garrett, “A framework for evolving multi-shaped detectors in negative selection,” in Proceedings of the IEEE Symposium on Foundations of Computational Intelligence (FOCI ’07), pp. 401–408, Honolulu, Hawaii, USA, April 2007.

[82] Z. Ji and D. Dasgupta, “Revisiting negative selection algorithms,” Evolutionary Computation, vol. 15, no. 2, pp. 223–251, 2007.

[83] A. A. Freitas and J. Timmis, “Revisiting the foundations of artificial immune systems: a problem-oriented perspective,” in Artificial Immune Systems, vol. 2787 of Lecture Notes in Computer Science, pp. 229–241, Springer, Berlin, Germany, 2003.

[84] X. Hang and H. Dai, “An extended negative selection algorithm for anomaly detection,” in Advances in Knowledge Discovery and Data Mining, vol. 3056 of Lecture Notes in Computer Science, pp. 245–254, Springer, Berlin, Germany, 2004.

[85] V. D. Kotov and V. I. Vasilyev, “Immune model based approach for network intrusion detection,” in Proceedings of the 3rd International Conference on Security of Information and Networks (SIN ’10), pp. 233–237, Taganrog, Russia, September 2010.

[86] T. Stibor, P. Mohr, and J. Timmis, “Is negative selection appropriate for anomaly detection?” in Proceedings of the Genetic and Evolutionary Computation Conference (GECCO ’05), pp. 321– 328, Washington, DC, USA, June 2005.

[87] P. D'haeseleer, S. Forrest, and P. Helman, "Immunological approach to change detection: algorithms, analysis and implications," in Proceedings of the 17th IEEE Symposium on Security and Privacy, pp. 110–119, May 1996.

[88] M. Ayara, J. Timmis, R. de Lemos, L. N. de Castro, and R. Duncan, "Negative selection: how to generate detectors," in Proceedings of the 1st International Conference on Artificial Immune Systems (ICARIS '02), pp. 89–98, 2002.

[89] S. F. M. Burnet, The Clonal Selection Theory of Acquired Immunity, vol. 3, Vanderbilt University Press, Nashville, Tenn, USA, 1959.

[90] L. N. de Castro and F. J. Von Zuben, "Artificial immune systems: part I-basic theory and applications," Tech. Rep., Universidade Estadual de Campinas, Campinas, Brazil, 1999.

[91] S. M. Garrett, "Parameter-free, adaptive clonal selection," in Proceedings of the Congress on Evolutionary Computation (CEC '04), pp. 1052–1058, June 2004.

[92] S. M. Garrett, "How do we evaluate artificial immune systems?" Evolutionary Computation, vol. 13, no. 2, pp. 145–177, 2005.

[93] F. Liu, B. Qu, and R. Chen, "Intrusion detection based on immune clonal selection algorithms," in AI 2004: Advances in Artificial Intelligence, vol. 3339 of Lecture Notes in Computer Science, pp. 1226–1232, Springer, Berlin, Germany, 2004.

[94] W. Tang, X.-M. Yang, X. Xie, L.-M. Peng, C.-H. Youn, and Y. Cao, "Avidity-model based clonal selection algorithm for network intrusion detection," in Proceedings of the IEEE 18th International Workshop on Quality of Service (IWQoS '10), pp. 1–5, Beijing, China, June 2010.

[95] D. Dasgupta, S. Yu, and F. Nino, "Recent advances in artificial immune systems: models and applications," Applied Soft Computing Journal, vol. 11, no. 2, pp. 1574–1587, 2011.

[96] L. Nunes de Casto and F. J. Von Zuben, "An evolutionary immune network for data clustering," in Proceedings of the 6th Brazilian Symposium on Neural Networks, pp. 84–89, Rio de Janeiro, Barzil, 2000.

[97] J. C. Galeano, A. Veloza-Suan, and F. A. Gonzalez, "A comparative analysis of artificial immune network models," in Proceedings of the Genetic and Evolutionary Computation Conference (GECCO '05), pp. 361–368, Washington, DC, USA, June

2005.

[98] J. Gomez, F. Gonz´ alez, and D. Dasgupta, “An immuno-fuzzy´ approach to anomaly detection,” in Proceedings of the 12th IEEE International Conference on Fuzzy Systems (FUZZ ’03), pp. 1219– 1224, Baton Rouge, La, USA, May 2003.

[99] D. Dasgupta, S. Yu, and N. S. Majumdar, “MILA-multilevel immune learning algorithm and its application to anomaly detection,” Soft Computing, vol. 9, no. 3, pp. 172–184, 2005.

[100]S. T. Powers and J. He, “A hybrid artificial immune system and Self Organising Map for network intrusion detection,” Information Sciences, vol. 178, no. 15, pp. 3024–3042, 2008.

[101]P. Matzinger, “Tolerance, danger, and the extended family,” Annual Review of Immunology, vol. 12, pp. 991–1045, 1994.

[102]P. Matzinger, “Essay 1: the danger model in its historical context,” Scandinavian Journal of Immunology, vol. 54, no. 1-2, pp. 4–9, 2001.

[103]U. Aickelin and S. Cayzer, “The danger theory and its application to artificial immune systems,” in Proceedings of the 1st Internat Conference on ARtif icial Immune Systems (ICARIS ’02), pp. 141–148, Canterbury, UK, 2002.

[104]J. Greensmith and U. Aickelin, “Dendritic cells for real-time anomaly detection,” in Proceedings of the Workshop on Artificial Immune Systems and Immune System Modelling (AISB ’06), pp. 7–8, Bristol, UK, April 2006.

[105]J. Greensmith and U. Aickelin, “Dendritic cells for SYN scan detection,” in Proceedings of the 9th Annual Genetic and Evolutionary Computation Conference (GECCO ’07), pp. 49–56, London, UK, July 2007.

[106]J. Twycross and U. Aickelin, “An immune inspired approach to anomaly detection,” in Handbook of Research on Information Assurance and Security, charpter 10, pp. 109–121, Information Science Reference, New York, NY, USA, 2007.

[107]J. P. Twycross and U. Aickelin, Integrated innate and adaptive artificial immune systems applied to process anomaly detection [Ph.D. thesis], University of Nottingham, Nottingham, UK, 2007.

[108]L. Peng, W. Chen, D. Xie, Y. Gao, and C. Liang, “Dynamically real-time anomaly

detection algorithm with immune negative selection," Applied Mathematics & Information Sciences, vol. 7, no. 3, pp. 1157–1163, 2013.

[109] F. A. Gonzalez and D. Dasgupta, "Anomaly detection using real-´ valued negative selection," Genetic Programming and Evolvable Machines, vol. 4, no. 4, pp. 383–403, 2003.

[110]J.KimandP.J.Bentley,"Immunememoryinthedynamicclonal selection algorithm," in Proceedings of the 1st International Conference on Artificial Immune Systems (ICARIS '02), pp. 59– 67, 2002.

[111]G. Y. Li and T. Guo, "Receptor editing-inspired real negative selection algorithm," Computer Science, vol. 39, pp. 246–251, 2012.

[112]R. Hightower, S. Forrest, and A. S. Perelson, "The evolution of secondary organization in immune system gene libraries," in Proceedings of the 2nd European Conference on Artificial Life, pp. 458–470, Brussels, Belgium, 1994.

[113]A. S. Perelson, R. Hightower, and S. Forrest, "Evolution and somatic learning in V-region genes," Research in Immunology, vol. 147, no. 4, pp. 202–208, 1996.

[114]M. Oprea and S. Forrest, "How the immune system generates diversity: Pathogen space coverage with random and evolved antibody libraries," Tech. Rep. 99-02-014, 1999.

[115]J. Kim and P. Bentley, "The artificial immune model for network intrusion detection," in Proceedings of the 7th European Conference on Intelligent Techniques and Soft Computing (EUFIT '99), Aachen, Germany, 1999.

[116]J. Kim and P. J. Bentley, "A model of gene library evolution in the dynamic clonal selection algorithm," in Proceedings of the 1st International Conference on Artificial Immune Systems (ICARIS '02), Canterbury, UK, 2002.

[117]J. Zeng, X. Liu, T. Li, G. Li, H. Li, and J. Zeng, "A novel intrusion detection approach learned from the change of antibody concentration in biological immune response," Applied Intelligence, vol. 35, no. 1, pp. 41–62, 2011.

[118]S. Cayzer, J. Smith, J. A. R. Marshall, and T. Kovacs, "What have gene libraries done for AIS?" in Artificial Immune Systems, vol. 3627 of Lecture Notes in Computer Science, pp. 86–99, Springer, Berlin, Germany, 2005.

[119]C. A. Laurentys, G. Ronacher, R. M. Palhares, and W. M. Caminhas, “Design of an artificial immune system for fault detection: a negative selection approach,” Expert Systems with Applications, vol. 37, no. 7, pp. 5507–5513, 2010

[120]T. Li, “An immune based dynamic intrusion detection model,” Chinese Science Bulletin, vol. 50, no. 22, pp. 2650–2657, 2005.

[121]J. Yang, X. Liu, T. Li, G. Liang, and S. Liu, “Distributed agents model for intrusion detection based on AIS,” Knowledge-Based Systems, vol. 22, no. 2, pp. 115–119, 2009.

[122]J. Greensmith, U. Aickelin, and S. Cayzer, “Introducing dendritic cells as a novel immune-inspired algorithm for anomaly detection,” in Artificial Immune Systems, vol. 3627 of Lecture Notes in Computer Science, pp. 153–167, Springer, Berlin, Germany, 2005.

[123]J. Kim, P. Bentley, C. Wallenta, M. Ahmed, and S. Hailes, “Danger is ubiquitous: detecting malicious activities in sensor networks using the dendritic cell algorithm,” in Artificial Immune Systems, vol. 3627 of Lecture Notes in Computer Science, pp. 153–167, Springer, Berlin, Germany, 2005.

[124]Z. Grossman and A. Singer, “Tuning of activation thresholds explains flexibility in the selection and development of T cells in the thymus,” Proceedings of the National Academy of Sciences of the United States of America, vol. 93, no. 25, pp. 14747–14752, 1996.

[125]M. Antunes and M. Correia, “TAT-NIDS: an immune-based anomaly detection architecture for network intrusion detection,” in Proceedings of the 2nd International Workshop on Practical Applications of Computational Biology and Bioinformatics (IWPACBB ’08), pp. 60–67, Salamanca, Spain, 2009.

[126]P. S. Andrews and J. Timmis, “Tunable detectors for artificial immune systems: from model to algorithm,” in Bioinformatics for Immunomics, vol. 3, pp. 103–127, Springer, New York, NY, USA, 2010