Abstract

As telecommunication networks become a critical component of our society a key challenge is to maintain network availability and reliability. Today, one of the biggest risks to network survivability is growing number of attacks by malicious intruders. Not only are these attacks becoming more numerous, they are also becoming more sophisticated. One fact that contributes to this increasing threat is network heterogeneous and contributed character. The main features to be addressed in the development of Intrusion Detection Systems (IDS), able to correspond to such numerous and sophisticated attacks, are flexibility, adaptability, autonomy and distribution. The current project presents an overview of a new approach in Detection Systems (IDS) that is based upon use of intelligent agents. The introduction of multi-agents system (MAS) in a network allows network entities to perform adaptive behavior and "intelligence" which means autonomy, interaction, communication and co-operation. Therefore, this new approach seems promising to enable Intrusion Detection Systems exhibit characteristics as flexibility and adaptability.

Section A contains some general terms that concern issues of network security and technology of intelligent agents, meanwhile, section B presents some of the proposed architectures and implementations of intrusion detection systems that rely on intelligent agent technology.

Περίληψη

Καθώς τα δίκτυα τηλεπικοινωνιών έχουν γίνει αναπόσπαστο και κρίσιμο κομμάτι της σημερινής κοινωνίας της πληροφορίας η μεγάλη πρόκληση που πλέον αντιμετωπίζει η τεχνολογία των επικοινωνιών είναι η διατήρηση της διαθεσιμότητας και της αξιοπιστίας τους. Ο μεγαλύτερος κίνδυνος για την βιωσιμότητα των δικτύων σήμερα είναι ο ολοένα αυξανόμενος αριθμός των επιθέσεων από κακόβουλους εισβολείς που υπονομεύουν την ασφάλεια ενός δικτύου. Επιπλέον, οι επιθέσεις αυτές γίνονται συνεχώς πιο πολύπλοκες και επιτηδευμένες. Στο γεγονός αυτό συμβάλλουν πολύ και η ετερογένεια των σημερινών δικτύων αλλά και ο κατανεμημένος χαρακτήρας τους. Για την αντιμετώπιση αυτών των συνεχώς μεταβαλλόμενων τύπων επιθέσεων εναντίον των δικτύων απαιτείται η ανάπτυξη νέων τύπων Συστημάτων Ανίχνευσης και Απάντησης σε Εισβολές (IDS) τα οποία θα ενσωματώνουν χαρακτηριστικά όπως ευελιξία, προσαρμοστικότητα, αυτονομία και κατανεμημένος χαρακτήρας. Το παρόν έργο εξετάζει μία νέα προσέγγιση στα Συστήματα Ανίχνευσης και Απάντησης σε Εισβολές (IDS) η οποία βασίζεται στην χρήση ευφυών πρακτόρων. Η εισαγωγή Πολυπρακτορικών Συστημάτων (MAS) σε ένα δίκτυο επιτρέπει στις οντότητες του δικτύου να επιδεικνύουν προσαρμοστικότητα και «ευφυή» συμπεριφορά δηλαδή αυτονομία, αλληλεπίδραση, επικοινωνία και συνεργατικότητα. Αυτή η νέα λοιπόν προσέγγιση είναι πολλά υποσχόμενη ως προς την υιοθέτηση ευελιξίας και προσαρμοστικότητας στα Συστήματα Ανίχνευσης και Απάντησης σε Εισβολές.
Στο Α΄μέρος παρατίθενται περιληπτικά κάποιοι χρήσιμοι όροι και έννοιες της ασφάλειας δικτύων και της τεχνολογίας ευφυών πρακτόρων ενώ στο Β΄μέρος παρουσιάζονται μερικές προτεινόμενες αρχιτεκτονικές και υλοποιήσεις Συστημάτων Ανίχνευσης και Απάντησης σε Εισβολές που βασίζονται σε τεχνολογία ευφυών πρακτόρων.

Περιεχόμενα

1. Εισαγωγή

Το κύριο χαρακτηριστικό του περιβάλλοντος μέσα στο οποίο αναπτύσσεται σήμερα ένα δίκτυο τηλεπικοινωνιών είναι η ετερογένεια. Το υλικό ενός δικτύου παρουσιάζει σημαντικό βαθμό ασυμβατότητας λόγω διαφορετικής πλατφόρμας τεχνολογίας,διαφορετικού λειτουργικού συστήματος κάτω από το οποίο λειτουργεί ή ακόμα και διαφορετικού κατασκευαστή,γεγονός που εισάγει στην διαδικασία ανάπτυξης και διαχείρισης ενός δικτύου μεγάλο βαθμό πολυλοκότητας. Λόγω της μεγάλης ποικιλίας υλικού από το οποίο μπορεί να αποτελείται ένα δίκτυο οι εφαρμογές διαχείρισης του δικτύου ενσωματώνουν πλήθος εργαλείων και διασυνδέσεων (interfaces) με αποτέλεσμα να αυξάνουν σε μέγεθος εις βάρος πάντα της ευκολίας διατήρησής τους.

Επιπλέον, ο αποκεντρωτικός χαρακτήρας των σύγχρονων δικτύων με κατανεμημένα κέντρα επεξεργασίας οδηγεί σε μία επίσης 'κατανεμημένη' προσέγγιση στην διαχείρισή τους αφού πλέον, αντί ενός μεγάλου συστήματος κεντρικού ελέγχου, είναι πιο αποτελεσματική η ύπαρξη πολλών μικρότερων συστημάτων τα οποία με συνεργατικό τρόπο αναλαμβάνουν την επίλυση προβλημάτων που αφορούν την διαχείριση ενός δικτύου.

Σήμερα η άμεση,έγκαιρη και έγκυρη ανταλλαγή πληροφοριών είναι ζωτικής σημασίας για την βιωσιμότητα και την ανάπτυξη οργανισμών και επιχειρήσεων γεγονός που έχει επιφέρει σημαντική αύξηση στην ζήτηση αλλά και στην προσφορά πληροφοριών μέσω δικτύων και εισήγαγε πρόσθετη δυσκολία στην διαδικασία διαχείρισης ενός δικτύου. Είναι πολύ κρίσιμο ζήτημα πλέον η ταχύτητα επανάκαμψης του δικτύου σε περίπτωση δυσλειτουργίας γεγονός το οποίο επιβάλλει αναγνώριση του σφάλματος και την άμεση ανάληψη δράσης είτε αυτόματα από το σύστημα είτε από τον διαχειριστή μετά από ενημέρωσή του από το σύστημα.

Τέλος, παρατηρείται αύξηση των προσδοκιών των χρηστών για αξιοπιστία και ποιότητα υπηρεσιών των δικτύων.

Όλα τα παραπάνω ώθησαν προς την κατεύθυνση μελέτης της χρήσης τεχνολογίας ευφυών πρακτόρων στην διαχείριση ενός δικτύου η οποία, όπως αναφέρθηκε παραπάνω, αποτελεί μία όλο και πιο πολύπλοκη και δύσκολη διαδικασία. Τι ακριβώς αφορά όμως η διαχείριση ενός δικτύου;

Η διαχείριση ενός δικτύου περιλαμβάνει:

- Την διασφάλιση της αποτελεσματικής και επαρκούς λειτουργίας των συστημάτων του δικτύου
- Την διαδικασία δημιουργίας μίας πολιτικής διαχείρισης (management policy) με συγκεκριμένους στόχους

- Την παρακολούθηση (monitoring) και έλεγχο του δικτύου
- Τον σχεδιασμό της εξέλιξης του δικτύου

Πιο συγκεκριμένα, η διαχείριση ενός δικτύου διακρίνεται στις εξής υποπεριοχές:

- Διαχείριση σφαλμάτων (Fault manageme*nt)*, δηλαδή την ανίχνευση ανωμαλιών και επανάκαμψη του δικτύου ή και την πρόβλεψη αυτών.
- Διαχείριση διάταξης (Configuration management) δηλαδή την διατήρηση της διαμόρφωσης (configuration) του δικτύου και των αναβαθμίσεων (updates) ώστε να διασφαλίζεται η κανονική του λειτουργία
- Διαχείριση λογαριασμών (Accounting management) δηλαδή την διαχείριση των χρηστών
- Διαχείριση απόδοσης (Performance management) δηλαδή διασφάλιση της αξιοπιστίας και και της ποιότητας υπηρεσιών του δικτύου.
- Διαχείριση ασφάλειας (Security management) δηλαδή την προστασία εναντίον κάθε είδους απειλής κατά των δεδομένων, των πόρων και των υπηρεσιών του δικτύου αλλά και των προσωπικών δεδομένων (privacy) των χρηστών του.

Η βιβλιογραφική αυτή μελέτη επικεντρώνεται στην χρήση ευφυών πρακτόρων στον τομέα της διαχείρισης της ασφάλειας ενός δικτύου.

2. Υπόβαθρο

2.1 Ασφάλεια δικτύου

Η ασφάλεια των δικτύων αποτελεί σήμερα ένα από τα πιο σημαντικά ζητήματα προς απάντηση λόγω των συνεχώς αυξανόμενων σε πλήθος αλλά και σε πολυπλοκότητα επιθέσεων εναντίον της ιδιωτικότητας των δικτύων και των πόρων τους.

Με τον όρο *ασφάλεια δικτύου* εννούμε την προστασία του από μη εξουσιοδοτημένη μετατροπή, καταστροφή ή αποκάλυψη των δεδομένων και από μη εξουσιοδοτημένη χρήση των πόρων του.Επιπλέον, η ασφάλεια ενός δικτύου αφορά και την αξιόπιστη παροχή πληροφοριών που είναι πάντα διαθέσιμες για τους χρήστες του. Ουσιαστικά αποτελεί την διαβεβαίωση οτι το δίκτυο εκτελεί σωστά όλες τις κρίσιμες λειτουργίες του.

Οι απειλές εναντίον ενός δικτύου είναι δύο ειδών γενικά : επιθέσεις εναντίον των δεδομένων του που απειλούν την εμπιστευτικότητα, την ακεραιότητα των τελευταίων και επιθέσεις άρνησης παροχής υπηρεσιών (denial of service attack) οι οποίες αποσκοπούν στην

παρακώλυση της πρόσβασης των νόμιμων χρηστών στο δίκτυο ή πρόκληση καθυστέρησης λειτουργιών που είναι κρίσιμες ως προς τον χρόνο. Ένα τέτοιο παράδειγμα είναι οι επιθέσεις 'πλημμύρας' όπου ο επιτιθέμενος κατακλύζει ένα εξυπηρετητή του δικτύου με μεγάλο πλήθος αιτήσεων σύνδεσης με αποτέλεσμα ο εξυπηρετητής να μη μπορεί κάποια στιγμή να ανταποκριθεί στις πραγματικές αιτήσεις των χρηστών. Ως εισβολή λοιπόν μπορούμε να ορίσουμε κάθε ενέργεια που υπονομεύει την εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα ενός πόρου του δικτύου.

2.2 Ανίχνευση εισβολών σε δίκτυα

Η πρώτη γραμμή άμυνας ενός δικτύου είναι τεχνικές όπως η αυθεντικοποίηση των χρηστών, η κρυπτογράφηση αλλά και τα φράγματα ασφαλείας (firewalls). Η δεύτερη γραμμή άμυνας είναι τα λεγόμενα συστήματα ανίχνευσης εισβολών που ως στόχο τους έχουν όχι μόνο την ανίχνευση μίας επίθεσης εναντίον του δικτύου αλλά και την λήψη έγκαιρων μέτρων. Ένα σύστημα ανίχνευσης εισβολών (intrusion detection system-IDS) είναι ένα σύνολο μηχανισμών, υλικού και λογισμικού που αυτοματοποιούν την διαδικασία παρακολούθησης όλων των γεγονότων που συμβαίνουν σε ένα δίκτυο ενημερώνοντας παράλληλα τον διαχειριστή του για οποιοδήποτε συμβάν ή κακόβουλη ενέργεια επιτρέποντας έτσι την ανίχνευση εισβολών στο δίκτυο.

Γενικά, οι τεχνικές που χρησιμοποιούνται για την ανίχνευση εισβολών στα δίκτυα είναι τρείς:

- Στατιστική ανίχνευση ανωμαλιών (Statistical Anomaly Detection): χρησιμοποιεί δεδομένα από αρχεία που καταγράφουν τις ενέργειες των χρηστών τα οποία αναλύει και επεξεργάζεται έτσι ώστε να βρεθούν στατιστικοί τύποι συμβάντων για συγκεκριμένες ενέργειες για τις οποίες στην συνέχεια εξάγονται τύποι χρήσης (usage patterns). Επιπλόν, υπάρχει ένα προκαθορισμένο προφίλ της συμπεριφοράς ενός φυσιολογικού χρήστη το οποίο συνήθως προέρχεται από την εμπειρία του διαχειριστή του συστήματος. Οι τύποι χρήσης που προέκυψαν παραπάνω συγκρίνονται με το προφίλ και έτσι προκύπτει το αναμενόμενο προφίλ του χρήστη δηλαδή το πώς αναμένεται αυτός να συμπεριφερθεί.
- Ανίχνευση βασισμένη σε κανόνες (Rule Based Detection): χρησιμοποιεί ένα σύνολο κανόνων που καθορίζουν την τυπική μή νόμιμη συμπεριφορά ενός χρήστη και οι οποίοι προκύπτουν από την ανάλυση προηγούμενων εισβολών στο δίκτυο. Το κύριο μειονέκτημα της μεθόδου είναι οτι οι κανόνες προκαθορίζονται από τους διαχειριστές του συστήματος και επομένως δεν είναι δυνατό να ανιχνευτούν νέες τεχνικές επίθεσης που δεν έχουν ξαναχρησιμοποιηθεί.

- Υβριδική ανίχνευση (Hybrid Detection): αποτελεί συνδυασμό των δύο προηγούμενων δηλαδή χρησιμοποιεί κανόνες για να ανιχνεύσει γνωστές μεθόδους επίθεσης και στατιστικές μεθόδους για να ανιχνεύσει νέες τεχνικές.

2.3 Ευφυείς πράκτορες

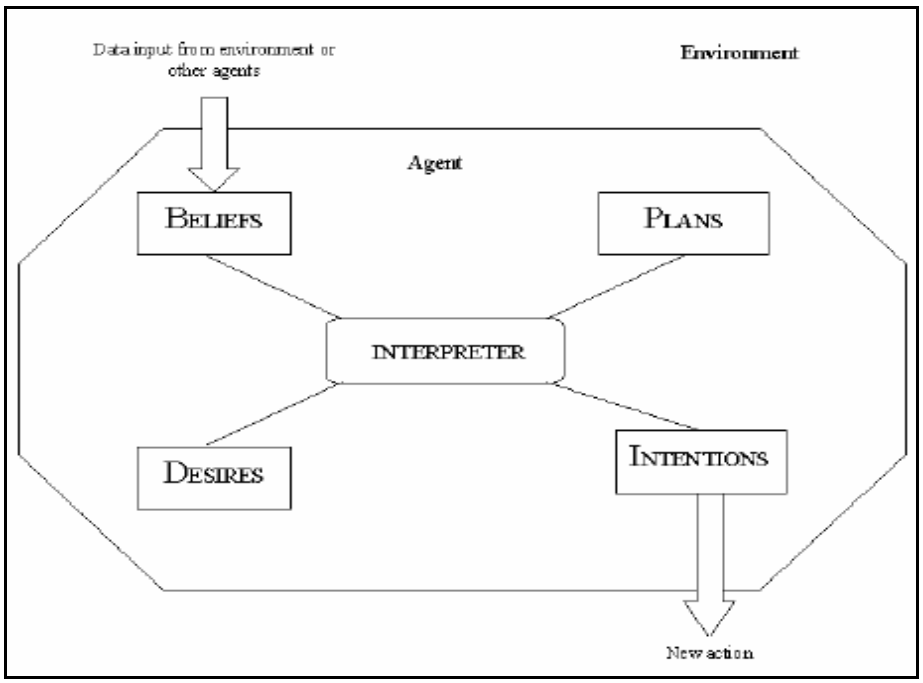
Ένας ευφυής πράκτορας λογισμικού (intelligent software agent) μπορεί να οριστεί ως «*μια υπολογιστική οντότητα η οποία δρα εκ μέρους ενός χρήστη ή προγράμματος, είναι αυτόνομη, προδραστική και αντιδραστική και διαθέτει ικανότητα μάθησης, συνεργασίας και κίνησης*» [9].
Η δράση ενός πράκτορα βασίζεται στις πεποιθήσεις, τις επιθυμίες και τις προσδοκίες του (BDI - Beliefs, Desires and Intensions).
Ένας κινούμενος πράκτορας (mobile agent) είναι ένας πράκτορας λογισμικού που έχει την δυνατότητα να κινείται μεταξύ διαφορετικών περιβαλλόντων εκτέλεσης.
Ένα πολυπρακτορικό σύστημα (Multi-Agent systems- MAS) είναι *«ένα δίκτυο από οντότητες επίλυσης προβλημάτων οι οποίες συνεργάζονται για την επίλυση προβλημάτων που είναι πέρα από τις δυνατότητες της κάθε μίας χωριστά.»* (Durfee et al).

3. Συστήματα που βασίζονται στην αρχιτεκτονική BDI πρακτόρων

3.1 Γενικά

Η αρχιτεκτονική BDI (Belief-Desire-Intension) αναπτύχθηκε από τους Rao και Georgeff [5] και σύμφωνα με αυτή ένας πράκτορας είναι ικανός να λαμβάνει αποφάσεις με λογικό τρόπο με βάση τις πεποιθήσεις, τους στόχους και τις προθέσεις του και να δρα ανάλογα. Οι κύριες έννοιες της αρχιτεκτονικής αυτής είναι:

- Οι πεποιθήσεις (beliefs) ενός πράκτορα είναι πληροφορίες για το περιβάλλον του.
- Οι επιθυμίες (desires) είναι στόχοι που ανατίθενται στον πράκτορα
- Οι προθέσεις (intensions) είναι οι δεσμεύσεις ενός πράκτορα για την επίτευξη κάποιων στόχων. Δηλαδή, μπορούμε να πούμε οτι είναι τα σχέδια που εκτελούνται.
- Τα σχέδια (plans) είναι οι επιλογές που έχει κάθε στιγμή ο πράκτορας στη διάθεσή του για να χρησιμοποιήσει για την επίτευξη των σκοπών του.

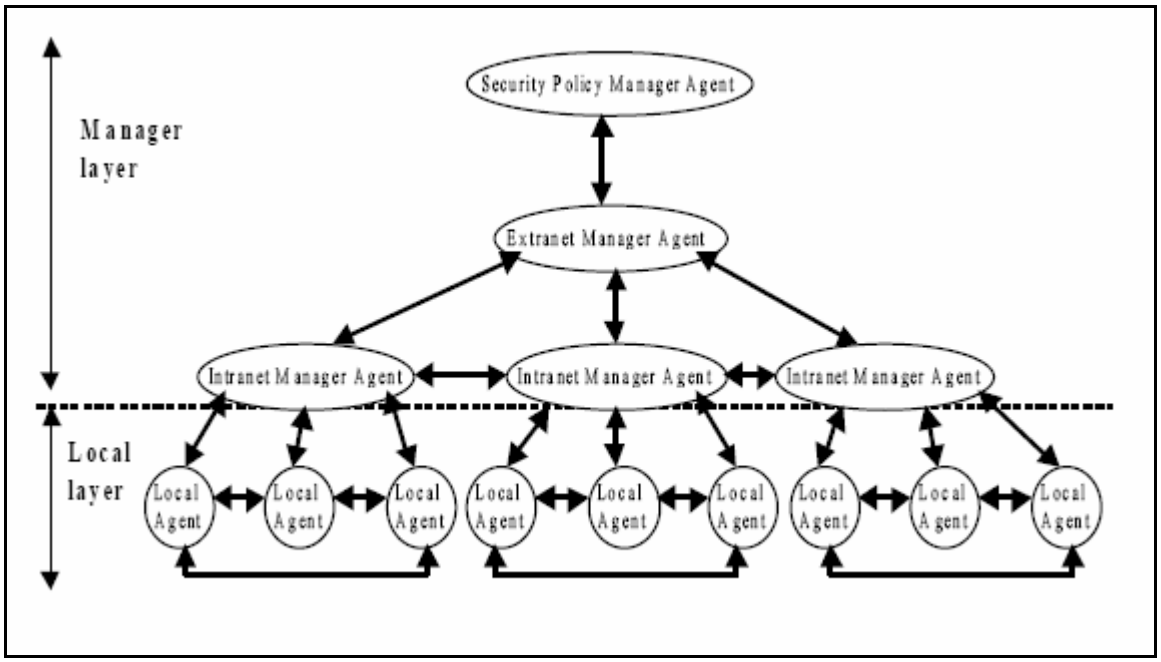


Σχήμα 3.1: Η αρχιτεκτονική BDI πρακτόρων

Η αρχιτεκτονική BDI χρησιμοποιείται πλέον ευρέως σε διάφορους τομείς της διαχείρισης των δικτύων. Παρακάτω, παρουσιάζονται μερικές περιπτώσεις αρχιτεκτονικών και συγκεκριμένες υλοποιήσεις τους που βασίζονται στην αρχιτεκτονική πρακτόρων BDI.

3.2 Αρχιτεκτονική MANSMA (The Multi-agents System-based Network Security Management Architecture)

Μία προσέγγιση για την χρήση πολυπρακτορικών συστημάτων για την διαχείριση δικτύων είναι η αρχιτεκτονική MANSMA η οποία βασίζεται σε ένα πλήθος ευφυών πρακτόρων που βρίσκονται σε συγκεκριμένες οντότητες του δικτύου και είναι οργανωμένοι ιεραρχικά όπως φαίνεται και στο παρακάτω σχήμα:



Σχήμα 3.2 : Η αρχιτεκτονική των λειτουργιών στο πρότυπο MANSMA

Όπως φαίνεται στο παραπάνω σχήμα, η αρχιτεκτονική MANSMA αποτελείται από δύο επίπεδα: το επίπεδο διαχείρισης (Manager layer) και το τοπικό επίπεδο (Local layer).
Το τοπικό επίπεδο διαχειρίζεται την ασφάλεια σε ένα υποσύνολο υπολογιστών ενός τοπικού δικτύου. Αποτελείται από ένα σύνολο από τοπικούς πράκτορες (Local agents – LA) οι διακρίνονται σε τρείς κατηγορίες: τοπικοί πράκτορες εξωδικτύου (Extranet LA), τοπικοί πράκτορες ενδοδικτύου (Intranet LA) και εσωτερικοί τοπικοί πράκτορες (Internal LA). Ο κάθε ένας από αυτούς τους πράκτορες αναλαμβάνει την παρακολούθηση μίας συγκεκριμένης λειτουργίας.
Το επίπεδο διαχείρισης είναι υπεύθυνο για την συνολική ασφάλεια του δικτύου. Οι πράκτορες που συναντούμε σε αυτό το επίπεδο είναι τριών ειδών:

- Ένας πράκτορας διαχείρισης της πολιτικής ασφαλείας (Security Policy Manager Agent – SPMA) ο οποίος διαχειρίζεται τις πολιτικές της ασφάλειας του δικτύου που καθορίζονται από τον διαχειριστή του.
- Ένας πράκτορας διαχείρισης εξωδικτύου (Extranet Manager Agent) ο οποίος διαχειρίζεται την ασφάλεια του κατανεμημένου δικτύου. Ειδικότερα, ελέγχει τους IMA πράκτορες και εκτελεί επιπλέον ανάλυση στα αποτελέσματα που αυτοί του παρέχουν για να επιβεβαιώσει την ύπαρξη εισβολής στο δίκτυο. Επιπλέον, μπορεί να ζητήσει την περαιτέρω επεξεργασία των δεδομένων ή και να αναθέσει νέα

καθήκοντα παρακολούθησης στους πράκτορες IMA. Τέλος, είναι υπεύθυνος να αναθέτει ένα σύνολο τοπικών πρακτόρων LA σε ένα πράκτορα IMA.

- Πράκτορες διαχείρισης ενδοδικτύου (Intranet Manager Agents – IMA) καθένας από τους οποίους αναλαμβάνει την ασφάλεια ενός τοπικού δικτύου ελέγχοντας τους τοπικούς πράκτορες που του ανατέθηκαν και αναλύοντας τα συμβάντα που που καταγράφονται από αυτούς.

Όπως φαίνεται και από το σχήμα 3.2, σε κάθε επίπεδο οι πράκτορες επικοινωνούν μεταξύ τους ανταλλάσοντας την γνώση και τις αναλύσεις που πραγματοποίησαν ώστε συνεργαζόμενοι να ανιχνεύσουν μία εισβολή στο δικτύου και να αντιδρούν άμεσα σε πιθανές αλλαγές του περιβάλλοντός τους.

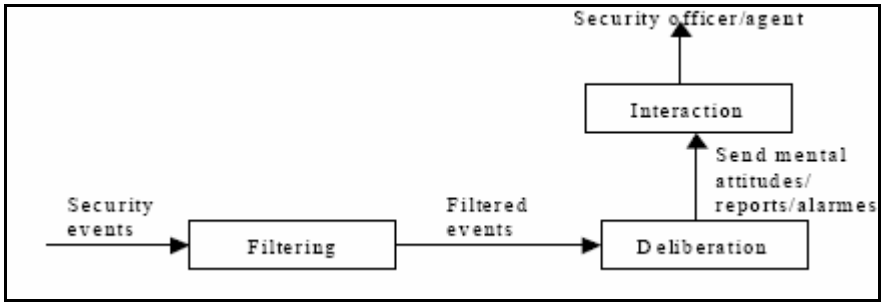
Για την αρχιτεκτονική αυτή χρησιμοποιείται ένα μοντέλο ευφυούς πράκτορα σύμφωνα με το οποίο κάθε πράκτορας σε ένα σύστημα ανίχνευσης εισβολών θα πρέπει να διαθέτει αφ' ενός γνωστικές ικανότητες τις οποίες θα χρησιμοποιεί για να αναγνωρίζει τις επιθέσεις στο δίκτυο και αφ'ετέρου ικανότητα αντίδρασης ώστε να ανταποκρίνεται άμεσα στις αλλαγές του δικτυακού περιβάλλοντος. Πιο συγκεκριμένα, το μοντέλο πράκτορα που χρησιμοποιείται διαθέτει τρείς λειτουργίες:

i. Λειτουργία φιλτραρίσματος (filtering): κάθε συμβάν που καταγράφεται στο δίκτυο αντιστοιχίζεται με βάση τον τύπο του σε μία από τις προκαθορισμένες κλάσεις συμβάντων. Στην πραγματικότητα δεν συλλέγονται όλα τα συμβάντα παρά μόνο αυτά που ταιριάζουν με κάποια από αυτές τις κλάσεις, τα οποία στην συνέχεια αποθηκεύονται μέχρι να τα χειριστεί η λειτουργία της μελέτης.
ii. Λειτουργία αλληλεπίδρασης (interaction) : με αυτή οι πράκτορες μπορούν να ανταλλάσουν γνώσεις και αναλύσεις ώστε να συνεργάζονται. Πιο συγκεκριμένα, οι πράκτορες διαχείρισης αλληλεπιδρούν με τους τοπικούς πράκτορες στέλνοντάς τους τους σκοπούς που απορρέουν από την πολιτική ασφαλείας του δικτύου, κατανέμοντάς τους τις λειτουργίες του δικτύου που πρέπει να παρακολουθεί ο κάθε ένας, ζητώντας συγκεκριμένες πληροφορίες για κάποια συμβάντα και λαμβάνοντας τις σχετικές αναφορές, αναλύσεις, προειδοποιήσεις κ.α. Επιπλέον, η λειτουργία αφορά και την επικοινωνία μεταξύ του υπεύθυνου ασφαλείας και των πρακτόρων SPMA και EMA ώστε να τους γίνεται γνωστή η πολιτική ασφαλείας που θα ακολουθηθεί αλλά και για να στέλνονται στον υπεύθυνο ασφαλείας αναφορές και προειδοποιήσεις σε περιπτώσεις ανίχνευσης εισβολής.
iii. Λειτουργία διαπραγμάτευσης (deliberation): το βασικό χαρακτηριστικό ενός δικτύου είναι η συνεχής διαφοροποίηση χρηστών, υπηρεσιών αλλά και

εμφανιζόμενων προβλημάτων ασφάλειας. Για να μπορεί να προσαρμόζεται και να αντιδρά άμεσα σε αυτές τις αλλαγές του περιβάλλοντός του ένας πράκτορας θα πρέπει να μπορεί να συνδυάζει τις γνώσεις και εμπειρίες του με λογικό τρόπο ώστε κάθε φορά να φτάνει στον προσδοκώμενο στόχο και στην εκτέλεση των ανάλογων ενεργειών. Η αρχιτεκτονική MANSMA υιοθετεί το πρότυπο BDI για τους πράκτορες οι οποίοι χρησιμοποιώντας τις πεποιθήσεις που απορρέουν από το φιλτράρισμα των συμβάντων αλλά και από την ανταλλαγή γνώσεων και εμπειριών με άλλους πράκτορες φτάνουν στον στόχο τους δηλαδή την ανίχνευση της επίθεσης και την εκτέλεση των αντίστοιχων ενεργειών.

Η υλοποίηση αυτής της αρχιτεκτονικής έγινε με την πλατφόρμα DIMA η οποία έχει ως βασικό χαρακτηριστικό της την αρθρωτή αρχιτεκτονική (modular) και παρουσιάζεται αναλυτικότερα παρακάτω.

Κάθε μία από τις τρείς λειτουργίες που εκτελεί ένας πράκτορας στο πρότυπο MANSMA ανατίθεται σε ένα από τα τμήματα της εφαρμογής (modules). Όταν ένας πράκτορας αντιληφθεί ένα συμβάν, το φιλτράρει μέσα στο τμήμα (module) που είναι υπεύθυνο για την λειτουργία του φιλτραρίσματος και κατόπιν στέλνεται στο τμήμα που εκτελεί την λειτουργία της μελέτης (deliberation). Αυτό με τη σειρά του ενημερώνει πρώτα το σύνολο των πεποιθήσεων (beliefs) του πράκτορα και στην συνέχεια ελέγχει αν το συμβάν ταιριάζει με μία επίθεση. Άν ναι, τότε έχει λάβει χώρα η επίτευξη ενός στόχου ασφάλειας και μία λίστα από ενέργειες προς εκτέλεση στέλνονται στο τμήμα που είναι υπεύθυνο για την αλληλεπίδραση του πράκτορα (σχήμα 3.3).



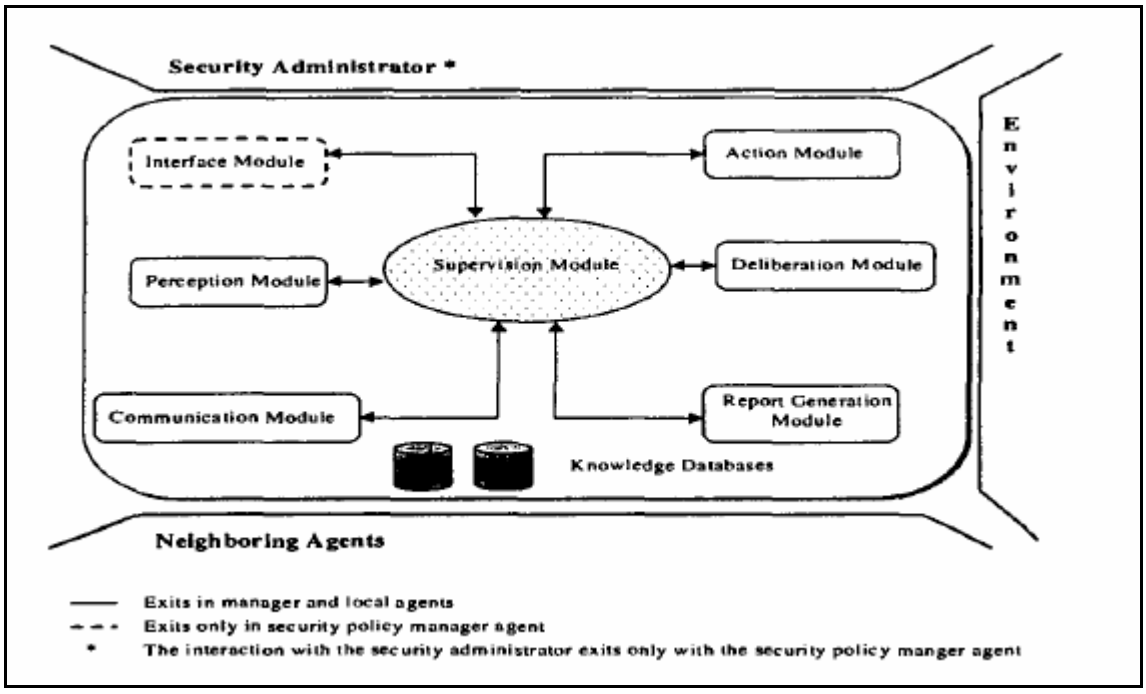
Σχήμα 3.3: Λειτουργία του μοντέλου του πράκτορα στην αρχιτεκτονική MANSMA

Το βασικό πλεονέκτημα αυτής της προτεινόμενης αρχιτεκτονικής είναι οτι με την χρήση του μοντέλου BDI δίνει την δυνατότητα στους πράκτορες να προσαρμόζονται στις συνεχείς εξελίξεις και διαφοροποιήσεις τόσο του δικτυακού περιβάλλοντος στο οποίο βρίσκονται όσο και των διαφορετικών τύπων επιθέσεων εναντίον του δικτύου. Το γεγονός αυτό είναι πολύ

σημαντικό καθώς, όπως επισημάνθηκε και στην εισαγωγή, το βασικό χαρακτηριστικό των δικτύων σήμερα είναι η ετερογένεια (υλικού, λογισμικού, υπηρεσιών κλπ) αλλά και η ποικιλομορφία απειλών που κάνουν ακόμα δυσκολότερη την διαχείρισή του.
Ένα μικρό μειονέκτημα που εντοπίζεται είναι στον τρόπο που αναγνωρίζονται τα συμβάντα (με χρήση κλάσεων) ο οποίος δεν επιτρέπει πάντα την αναγνώριση όλων των συμβάντων. Παρόλα αυτά, κατά την υλοποίηση της αρχιτεκτονικής αυτής, μπορεί να αντιμετωπιστεί αυτό το μειονέκτημα με συχνές ανανεώσεις των κλάσεων που χρησιμοποιούνται στο φιλτράρισμα.
Μία κατεύθυνση προς την οποία θα μπορούσε να γίνει βελτίωση της προτεινόμενης αρχιτεκτονικής είναι η εισαγωγή κινητών αντί στατικών πρακτόρων ώστε να ενσωματωθούν όλα τα πλεονεκτήματα αυτών όπως η μείωση του φόρτου και των καθυστερήσεων σε ένα δίκτυο, η δυνατότητα ασύγχρονης εκτελεσής τους καθώς και η δυνατότητα δυναμικής προσαρμογής τους στο υπολογιστικό περιβάλλον στο οποίο εκτελεούνται. Αναλυτικότερα τα πλεονεκτήματα των κινούμενων πρακτόρων παρουσιάζονται παρακάτω.

3.3 Αρχιτεκτονική IA-NSM (Intelligent-agent Network Security Management)

Μία άλλη προσέγγιση που βασίζεται στην ίδια αρχιτεκτονική των δύο επιπέδων (Manager και Local layer) του MANSMA είναι και το πρότυπο IA-NSM. Εδώ χρησιμοποιείται ένα μοντέλο υβριδικού πράκτορα, που συνδυάζει γνωστικές και αντιδραστικές ικανότητες, και με βάση το οποίο κάθε πράκτορας του συστήματος αποτελείται από 7 τμήματα (modules), όπως φαίνεται και στο παρακάτω σχήμα.



Σχήμα 3.4: Δομή μοντέλου του πράκτορα της αρχιτεκτονικής IA-NSM

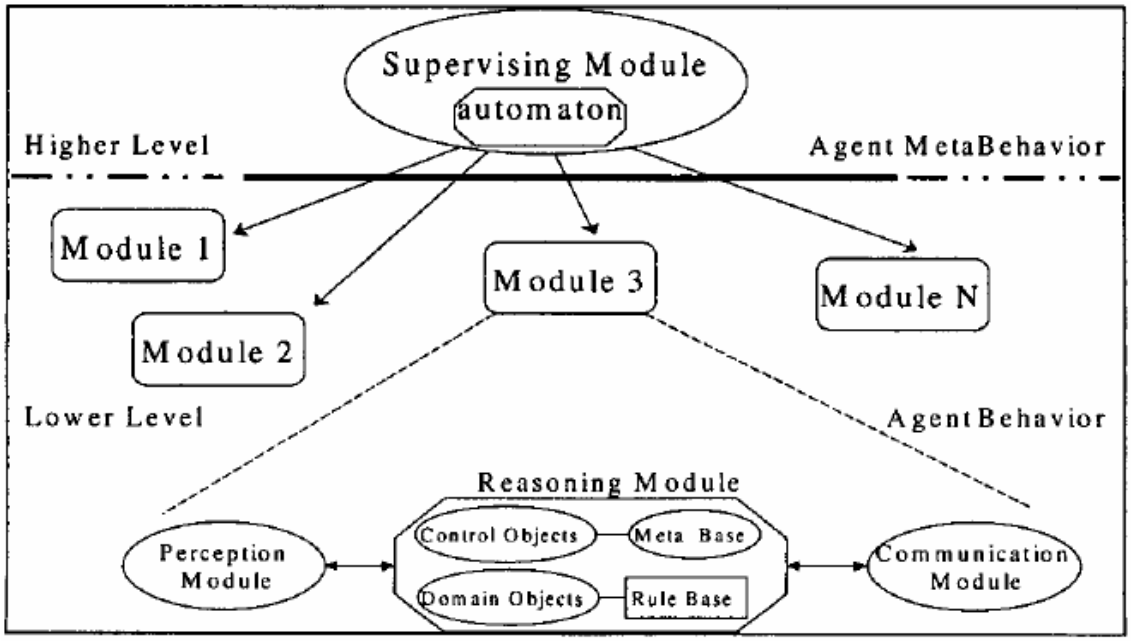
Κάθε ένα από τα τμήματα αυτά, που περιγράφονται παρακάτω, εκτελεί μία διαφορετική εργασία και ο συντονισμός τους πραγματοποιείται από την επιβλέπουσα οντότητα (supervision module).

- Τμήμα αντίληψης (Perception module): είναι υπεύθυνο για την συλλογή όλων των συμβάντων που σχετίζονται με την ασφάλεια του δικτύου.
- Τμήμα επικοινωνίας (Communication module): επιτρέπει στους πράκτορες να ανταλλάσσουν τις αναλύσεις, τις αποφάσεις και την γνώση τους.
- Τμήμα δράσης (Action module): επιτρέπει την ανάληψη κατάλληλης δράσης όταν ανιχνευτεί κάποιος εισβολέας.
- Τμήμα παραγωγής αναφορών (Report generation module): αναλαμβάνει την δημιουργία αναφορών των ανιχνευθέντων εισβολών οι οποίες στέλνονται στον διαχειριστή του δικτύου.
- Τμήμα μελέτης (Deliberation module): είναι αυτό το οποίο εξασφαλίζει την ευφυία και αυτονομία του πράκτορα. Με αυτό ο πράκτορας είναι σε θέση να λαμβάνει αποφάσεις με λογικό τρόπο βασιζόμενος στην υπάρχουσα γνώση και εμπειρία.
- Τμήμα διασύνδεσης (Interface module): υπάρχει μόνο στον πράκτορα διαχείρισης της πολιτικής ασφαλείας (SPMA) και είναι υπεύθυνο για την αλληλεπίδραση του με τον διαχειριστή ασφαλείας του δικτύου. Μέσω αυτού ο πράκτορας λαμβάνει

από τον διαχειριστή διάφορες αιτήσεις ή διευκρινίσεις σχετικές με την πολιτική ασφαλείας, παραδίδονται οι αναφορές στον διαχειριστή και στέλνονται σήματα συναγερμού όταν ανιχνευτεί κάποιος εισβολέας.

- Τμήμα επίβλεψης (Supervision module): συντονίζει την αλληλεπίδραση μεταξύ των διαφόρων άλλων τμημάτων.

Η υλοποίηση αυτής της αρχιτεκτονικής βασίζεται στην πλατφόρμα DIMA, η οποία έχει ως βασικό χαρακτηριστικό της την αρθρωτή αρχιτεκτονική (modular) και ουσιαστικά προτείνει την επέκταση μίας μοναδικής συμπεριφοράς ενός ενεργού αντικειμένου σε ένα σύνολο από συμπεριφορές. Η αρχιτεκτονική της DIMA βασίζεται σε δύο επίπεδα, όπως φαίνεται και στο σχήμα 3.5.



Σχήμα 3.5: Αρχιτεκτονική της πλατφόρμας DIMA

Το πρώτο επίπεδο αποτελείται από αλληλεπιδραστικά τμήματα που αντιπροσωπεύουν συμπεριφορές του πράκτορα όπως επικοινωνία, λογικός συλλογισμός και αντίληψη συμβάντων και τα οποία παρέχουν στον πράκτορα ιδιότητες όπως αυτονομία και συνεργατικότητα. Το δεύτερο επίπεδο αποτελείται από το τμήμα επίβλεψης που αντιπροσωπεύει την μετα-συμπεριφορά του πράκτορα δηλαδή την δυνατότητα να θεμελιώνει λογικά τις συμπεριφορές του.

Η DIMA προτείνει τρία παραδείγματα των τμημάτων ενός πράκτορα:

- Τμήμα αντίληψης (Perception module): διαχειρίζεται την αλληλεπίδραση του πράκτορα με το περιβάλλον του, για παράδειγμα καθορίζει ποιά συμβάντα ασφάλειας γίνονται αντιληπτά από τον πράκτορα.
- Τμήμα διαπραγμάτευσης (Deliberation module): αντιπροσωπεύει τις πεποιθήσεις, τις γνώσεις και τους τους στόχους του πράκτορα και είναι υπεύθυνο για την ανταπόκριση στα μηνύματα που προέρχονται από το τμήμα επικοινωνίας, για την αντίδραση στις αλλαγές που ανιχνεύονται από το τμήμα αντίληψης και για την επίτευξη τον αντικειμενικών σκοπών του πράκτορα, για παράδειγμα την ανίχνευση μίας συγκεκριμένης επίθεσης.
- Τμήμα επικοινωνίας (Communication module): χειρίζεται την επικοινωνία του πράκτορα με τους υπόλοιπους. Πιο συγκεκριμένα, καθορίζει τον τρόπο με τον οποίο δέχεται τα μηνύματά του ο πράκτορας και τα αποθηκεύει για μετέπειτα διερμηνεία καθώς και τον τρόπο με τον οποίο επικοινωνεί για να ζητήσει επιπλέον πληροφορίες που χρειάζεται.

Τα τρία αυτά τμήματα είναι κατάλληλα για να υλοποιήσουν τα αντίστοιχα τμήματα ενός πράκτορα της αρχιτεκτονικής IA-NSM ενώ πρέπει να υλοποιηθούν και να ενσωματωθούν επιπλέον και τμήματα διασύνδεσης, δράσης και παραγωγής αναφορών.
Η αρχιτεκτονική IA-NSM τελικά υλοποιείται με εγκατάσταση υβριδικών πρακτόρων, με βάση το παραπάνω μοντέλο, στις οντότητες SPMA, EMA, IMA, LA.

3.4 Αρχιτεκτονική FASA (Fuzzy Adaptive Survivability Architecture)

Η αρχιτεκτονική FASA προσπαθεί σε γενικές γραμμές να μιμηθεί την κοινή λογική και τον τρόπο λήψης αποφάσεων του διαχειριστή του συστήματος για την ανίχνευση εισβολών εναντίον του δικτύου και την παραγωγή αντίδρασης στην επίθεση. Το μοντέλο στο οποίο βασίζεται (Fuzzy Adaptive Survivability Model – FASM) περιλαμβάνει παρακολούθηση της δραστηριότητας του δικτύου, ανίχνευση ύποπτης κυκλοφορίας και μετριασμό των εισβολών ώστε να πληρούνται οι προϋποθέσεις βιωσιμότητας του δικτύου σύμφωνα με κάποια ορισμένη πολιτική . Τρείς είναι οι λειτουργίες που καθορίζονται από το μοντέλο:

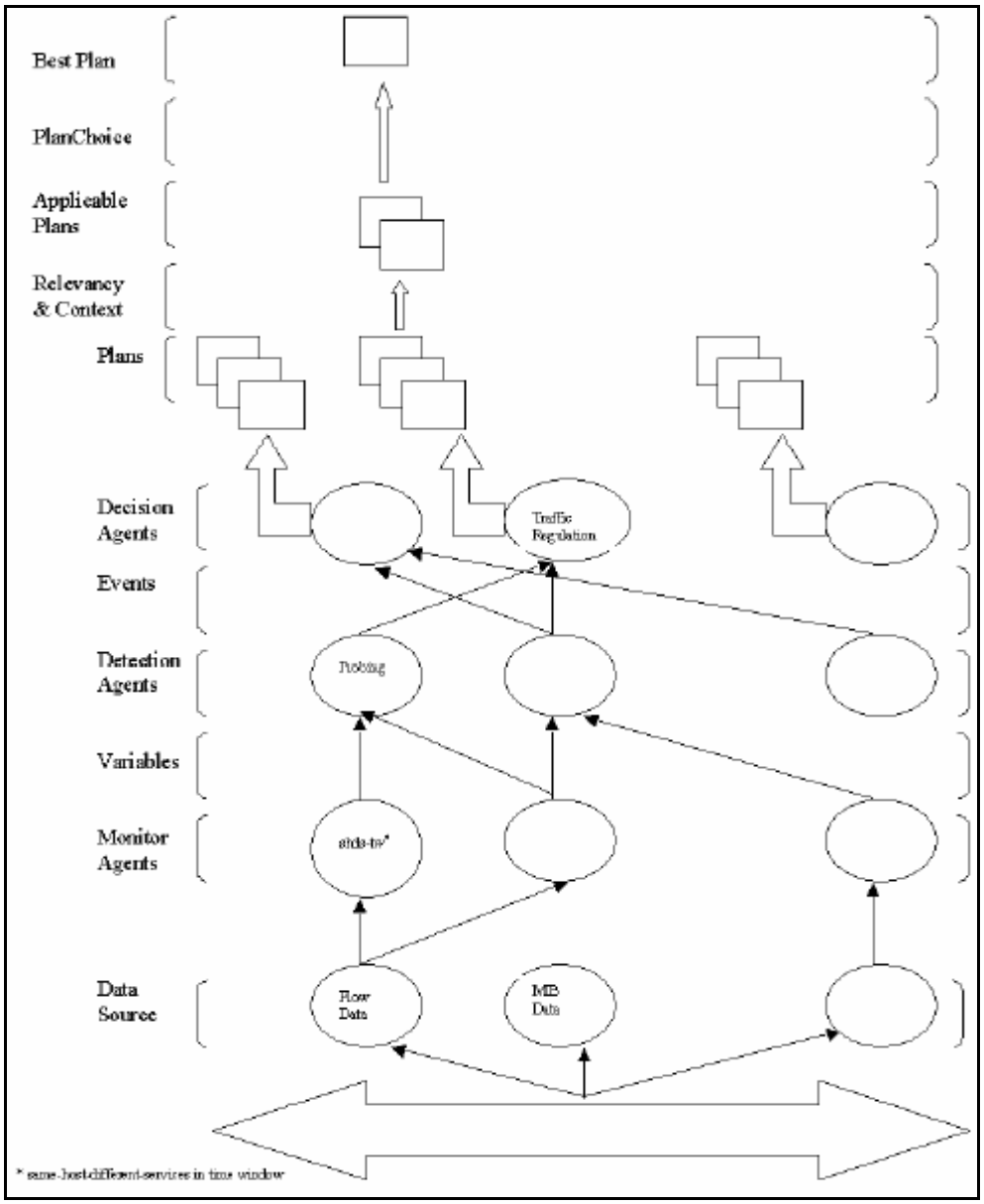
- Παρακολούθηση και συλλογή δεδομένων (monitoring): παρακολουθούνται οι μεταβλητές οι οποίες αντιπροσωπεύουν σημαντικές απόψεις της λειτουργίας του δικτύου και ελέγχεται η τυχούσα απόκλισή τους από τις φυσιολογικές τιμές τους.
- Ανίχνευση συμβάντων (event detection): παρακολουθείται η ροή δεδομένων στο δίκτυο ώστε να εντοπιστούν σημάδια εισβολής.

- Σχεδιασμός αντίδρασης και εκτέλεση (Response planning and execution): η λειτουργία αυτή λαμβάνει τις παραπάνω πληροφορίες και παράγει σχέδια αντίδρασης, με βάση τον τύπο της επίθεσης και την κατάσταση του δικτύου, τα οποία στην συνέχεια αξιολογεί με βάση τις συνέπειες του καθενός και τις τοπικές πολιτικές που εφαρμόζει το δίκτυο.

Στην αρχιτεκτονική FASA η κάθε μία λειτουργία ανατίθεται σε ένα λειτουργικό «κουτί», οπότε έχουμε τα : κουτί παρακολούθησης (monitor-box ή M-box), κουτί ανίχνευσης (detection-box ή D-box) και κουτί απόφασης (decision box ή X-box).

- Κάθε κουτί παρακολούθησης αναλαμβάνει την παρακολούθηση μίας από τις μεταβλητές του δικτύου και διατηρεί και ένα προφίλ της φυσιολογικής συμπεριφοράς της.
- Κάθε κουτί ανίχνευσης αποφαίνεται αν η έξοδος ενός κουτιού παρακολούθησης είναι ένδειξη επίθεσης και σε ποιο βαθμό.
- Το κάθε κουτί απόφασης αποφασίζει για το σχέδιο απάντησης που θα ακολουθηθεί. Η απόφαση λαμβάνεται σε τρία στάδια. Αρχικά, με βάση την σοβαρότητα της επίθεσης επιλέγεται ένα υποσύνολο των αντιδράσεων που είναι σχετικές με την ανιχνευθείσα επίθεση. Ο βαθμός σοβαρότητας υπολογίζεται με βάση τις συνέπειες που θα υπάρξουν αν ολοκληρωθεί η επίθεση με επιτυχία. Στην συνέχεια το υποσύνολο αυτών των επιλεχθέντων ενεργειών αξιολογείται στα πλαίσια των συγκεκριμένων περιστάσεων και με βάση την παρούσα κατάσταση του δικτύου. Αυτό που προκύπτει είναι ένα σύνολο από εφαρμόσιμα σχέδια τα οποία αξιολογούνται ανάλογα με το βαθμό ικανοποίησης προκαθορισμένων κριτηρίων και έτσι τέλος επιλέγεται ένα απο αυτά προς εκτέλεση.

Μία υλοποίηση της αρχιτεκτονικής FASA που βασίζεται σε πράκτορες είναι το FAST (Fuzzy Adaptive Survivability Tool), όπου κάθε κουτί λειτουργιών υλοποιείται με ένα ευφυή πράκτορα, όπως φαίνεται και παρακάτω.



Σχήμα 3.6: Πράκτορες που χρησιμοποιούνται στην υλοποίηση του FAST

Όπως φαίνεται και στο σχήμα 3.6, η υλοποίηση αυτή αποτελείται από τέσσερις τύπους πρακτόρων οι οποίοι είναι οι παρακάτω:

- HCI πράκτορας (HCI agent), ο οποίος παρέχει την κατάλληλη διασύνδεση στον χρήστη για την δημιουργία νέων πρακτόρων αλλά και για ανάμειξη σε περιπτώσεις όπου αυτό απαιτείται. Διαθέτει τέσσερις δυνατότητες: α) δημιουργεί νέους πράκτορες μετρά από αίτηση του χρήστη, β) ζητά την αλλαγή της διάταξης (configuration) των άλλων πρακτόρων μετά από αίτηση που λαμβάνει από τον χρήστη, γ) «διαβάζει» την ροή δεδομένων που συλλέχθηκε από το δίκτυο και δ)

προσομοιώνει ένα φίλτρο ώστε να μπλοκάρει την κάποιο συγκεκριμένο τύπο κυκλοφορίας δεδομένων από την εισερχόμενη ροή.

- Πράκτορες παρακολούθησης (Monitor agents), κάθε ένας από τους οποίους υλοποιεί ένα M-box παρακολουθώντας μία από τις μεταβλητές του δικτύου. Οι δυνατότητες που έχει είναι οι εξής: α) αρχικοποιείται μετά από εντολή του HCI πράκτορα και δέχεται μία λίστα από πράκτορες ανίχνευσης με τους οποίους θα επικοινωνεί, β)δέχεται μία ροή εισόδου δεδομένων από τον HCI πράκτορα και υπολογίζει την νέα τιμή της μεταβλητής που παρακολουθεί και γ) στέλνει την τελευταία τιμή της μεταβλητής αυτής στους πράκτορες ανίχνευσης.
- Πράκτορες ανίχνευσης (Detection agents), κάθε ένας από τους οποίους χρησιμοποιείται για την ανίχνευση μίας από τις γνωστές επιθέσεις και λαμβάνει πληροφορίες από πολλούς πράκτορες παρακολούθησης.
- Πράκτορας απόφασης (Decision agent), ο οποίος αποφασίζει για την παραγωγή μίας προειδοποίησης και επιλέγει ένα σχέδιο αντίδρασης με βάση κάποια προκαθορισμένα κριτήρια και την πολιτική βιωσιμότητας που ακολουθεί το δίκτυο. Η πολιτική αυτή είναι ουσιαστικά μία λίστα από υπηρεσίες του δικτύου οι οποίες αξιολογούνται ανάλογα με την σημαντικότητά τους με βάση ένα βαθμό σημαντικότητας που βρίσκεται αποθηκευμένος σε μία βάση δεδομένων. Επιπλέον, ο πράκτορας απόφασης λαμβάνει υπόψιν του το γενικό πλαίσιο συνθηκών που αφορά την κατάσταση του δικτύου την δεδομένη χρονική στιγμή. Ο διαχειριστής του δικτύου είναι αυτός που παρέχει μία πολιτική η οποία καθορίζει το πώς μεταβάλλονται οι προτιμήσεις του ανάλογα με την διαφορετική κατάσταση του δικτύου. Έτσι λοιπόν, με βάση την πολιτική βιωσιμότητας και τις δεδομένες συνθήκες στο δίκτυο ο πράκτορας απόφασης αποφασίζει να άν θα ληφθούν μέτρα ή όχι όταν μία επίθεση ανιχνευτεί. Επίσης, έχει την δυνατότητα να μετριάζει τις επιπτώσεις μίας επίθεσης μπλοκάροντας συγκεκριμένη κυκλοφορία στο δίκτυο χωρίς να παρεμποδίζονται οι βασικές λειτουργίες.

Για κάθε τύπο πράκτορα υπάρχουν καθορισμένα συμβάντα (events) τα οποία αναγνωρίζει και σχέδια (plans) τα οποία ακολουθεί. Μία λεπτομερέστερη περιγραφή της υλοποίησης αυτής βρίσκεται στο [4].

Το βασικό πλεονέκτημα του μοντέλου αυτού είναι στον τρόπο με τον οποίο επιλέγεται η απάντηση του δικτύου σε μία επίθεση, γεγονός που έχει κρίσιμο ρόλο στην συνολική λειτουργικότητα του δικτύου. Ο τρόπος αυτός μιμείται την λήψη απόφασης από τον άνθρωπο κάτω από συνθήκες αβεβαιότητας, μόνο που το FAST εκτελεί πιο ακριβή παρατήρηση και

ανάλυση, με αποτέλεσμα να μπορεί να λάβει αποφάσεις που ικανοποιούν με ακρίβεια τα κριτήρια και να εκκινήσει τις αντίστοιχες ενέργειες πιο γρήγορα σε σύγκριση με τον ανθρώπινο παράγοντα.
Το μέλλον της έρευνας της συγκεκριμένης αρχιτεκτονικής αφορά τον σχεδιασμό προ-δραστικής συμπεριφοράς (goal-driven), πέρα από την αντιδραστική συμπεριφορά (event-driven) του συστήματος.

3.5 Bayesian Intrusion Detection System

Το προτεινόμενο σύστημα χρησιμοποιεί μία υβριδική μέθοδο ανίχνευσης εισβολών στο δίκτυο σύμφωνα με την οποία η μη φυσιολογική συμπεριφορά προσδιορίζεται μετά από σύγκριση της τρέχουσας συμπεριφοράς του χρήστη με την τυπική του συμπεριφορά, η οποία περιέχεται στο προφίλ του χρήστη, αλλά καθώς και με γενικούς κανόνες που έχει θέσει ο διαχειριστής του συστήματος. Για τις προβλέψεις χρησιμοποιείται ένα στατιστικό μοντέλο πολλών μεταβλητών (Bayesian multivariate statistical model).
Σε κάθε σταθμό εργασίας χρήστη βρίσκεται ο πράκτορας του χρήστη και υπάρχει και ένας πράκτορας πυρήνα (core agent) ο οποίος βρίσκεται στον κεντρικό εξυπηρετητή του δικτύου. Όταν ένας χρήστης συνδέεται στο σύστημα ο πράκτορας χρήστη ανακτά το προφίλ του χρήστη από τον πράκτορα πυρήνα και αρχίζει την παρακολούθηση του χρήστη. Το προφίλ περιλαμβάνει αφ'ενός κανόνες που περιγράφουν την προηγούμενη φυσιολογική συμπεριφορά του χρήστη και αφ'ετέρου μία στατιστική πρόβλεψη αυτών των κανόνων. Ο πράκτορας του χρήστη παρακολουθεί τον χρήστη και συγκρίνει το δείγμα που έχει με το ιστορικό προφίλ του χρήστη. Άν υπάρχουν διαφορές στέλνονται προειδοποιήσεις προς τον διαχειριστή του συστήματος. Άν ο διαχειριστής δεχτεί τις αλλαγές τότε αυτές προστίθενται στο προφίλ του χρήστη. Όταν τελικά ο χρήστης αποσυνδεθεί από το σύστημα ο πράκτορας του χρήστη στέλνει μήνυμα στον πράκτορα πυρήνα να ενημερώσει το προφίλ του με τα δεδομένα των στατιστικών προβλέψεων και να αποθηκεύσει τις νέες προβλέψεις.
Το σύστημα υλοποιήθηκε ως εξής: ο πράκτορας πυρήνα βρίσκεται σε ένα εξυπηρετητή σε περιβάλλον WINDOWS NT και οι πράκτορες χρήστη βρίσκονται σε κάθε σταθμό εργασίας. Το λογισμικό όλων των πρακτόρων γράφτηκε σε SUN Java JDK Version 1.2.
Κάθε πράκτορας χρήστη υλοποιείται με τέσσερα μέρη:

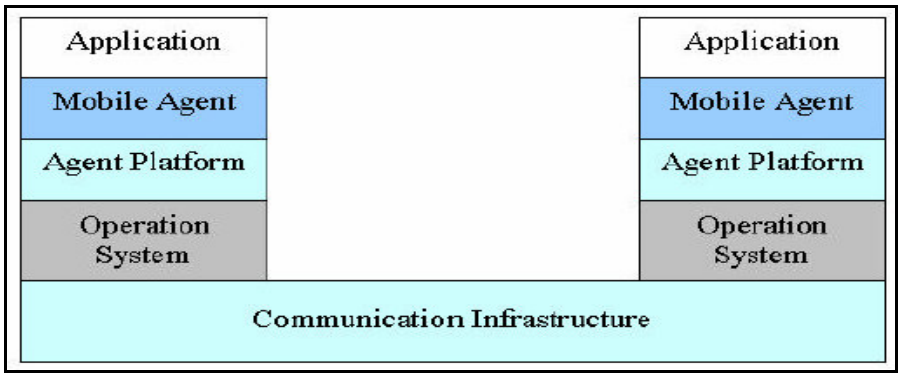
- Αισθητήρας (sensor) : ο αισθητήρας παρακολουθεί την δραστηριότητα του χρήστη καταγράφοντας τις εφαρμογές που αυτός χρησιμοποιεί.

- Πομπός (transmitter): οι πληροφορίες που καταγράφει ο αισθητήρας στέλνονται στον πράκτορα πυρήνα ο οποίος απαντάει στέλνοντας το ιστορικό προφίλ του χρήστη.
- Τμήμα ανάγνωσης προφίλ (profile reader): διαβάζει το ιστορικό προφίλ που έστειλε ο πράκτορας πυρήνα.
- Συγκριτής (comparator): ο συγκριτής συγκρίνει το ιστορικό προφίλ του χρήστη με τις πληροφορίες που καταγράφει ο αισθητήρας. Άν αυτό διαφέρει στέλνει, μέσω του πομπού, στον πράκτορα πυρήνα το ανγνωριστικό το χρήστη, τον τύπο της παράνομης ενέργειας που επιχείρησε και τα δεδομένα που αφορούσε. Στην συνέχεια μπορούν να ληφθούν πολλά διαφορετικά μέτρα όπως για παράδειγμα ενημέρωση του διαχειριστή, ή τερματισμό της εφαρμογής που προκάλεσε την παράνομη ενέργεια κ.α.

4. Συστήματα ανίχνευσης εισβολών με χρήση κινούμενων πρακτόρων

4.1 Γενικά

Όπως αναφέρθηκε και παραπάνω κινούμενος πράκτορας είναι ένας πράκτορας λογισμικού που έχει την δυνατότητα κίνησης μεταξύ διαφορετικών περιβαλλόντων εκτέλεσης. Οι κινούμενοι πράκτορες αποτελούν αντικείμενο μελέτης εδώ και αρκετά χρόνια, παρόλα αυτά η σχετική έρευνα περιοριζόταν κατά κύριο λόγο στα εργαστήρια αφού δεν τύχαινε ευρείας αποδοχής και υιοθέτησης από την βιομηχανία. Ο σημαντικότερος λόγος ήταν τα προβλήματα ασφάλειας που συνοδεύουν την χρήση κινούμενων πρακτόρων σε ένα ανοιχτό σύστημα. Τελευταία έχουν πραγματοποιηθεί μελέτες που αφορούν την ανάπτυξη μίας ασφαλούς αρχιτεκτονικής κινούμενων πρακτόρων και ειδικότερα προς την κατεύθυνση ανάπτυξης πολυπρακτορικών συστημάτων ανίχνευσης εισβολών εναντίον δικτύων.
Γενικά, όλοι οι κινούμενοι πράκτορες διαθέτουν την παρακάτω δομή.



Σχήμα 4.1: Γενική δομή ενός κινούμενου πράκτορα

Σε γενικές γραμμές, ένας κινούμενος πράκτορας δημιουργείται από μία εφαρμογή και εκτελείται πάνω σε μία πλατφόρμα, που λέγεται πλατφόρμα πράκτορα (agent platform), και η οποία χρησιμοποιεί τους πόρους και τα κανάλια επικοινωνίας που παρέχονται από το λειτουργικό σύστημα (operation system) και από το δίκτυο ώστε να υποστηρίζει την εκτέλεση των λειτουργιών του πράκτορα.

Τα πλεονεκτήματα που απορρέουν από την χρήση κινητού κώδικα μέσω κινούμενων πρακτόρων στα συστήματα ανίχνευσης εισβολών (intrusion detection systems) είναι πολλά και μπορούν να συνοψιστούν στα παρακάτω:

- Αποφυγή καθυστερήσεων στο δίκτυο: οι κινούμενοι πράκτορες είναι ιδιαίτερα χρήσιμοι σε εφαρμογές στις οποίες απαιτείται αντίδραση πραγματικού χρόνου στις μεταβολές του περιβάλλοντος λόγω της δυνατότητάς τους να αποσπώνται από τον κεντρικό διαχειριστή και να εκτελούνται απομακρυσμένα. Αυτή η ιδιότητά τους είναι ιδιαίτερα χρήσιμη στα συστήματα ανίχνευσης εισβολών στο δίκτυο τα οποία εκτός από την ανίχνευση μίας πιθανής επίθεσης πρέπει να λαμβάνουν και μέτρα για την προστασία του δικτύου. Η υλοποίηση αυτή είναι σαφώς πιο γρήγορη από την ύπαρξη ενός κεντρικού διαχειριστή ο οποίος θα πρέπει να διανέμει πληροφορίες και οδηγίες αντιμετώπισης των εισβολών στους απομακρυσμένους κόμβους μέσω αργών και πιθανώς μη αξιόπιστων συνδέσεων.
- Μείωση του φόρτου σε ένα δίκτυο: ένα από τα βασικότερα προβλήματα που αντιμετωπίζουν τα συστήματα ανίχνευσης εισβολών είναι η διαχείριση του τεράστιου όγκου δεδομένων που παράγουν τα εργαλεία παρακολούθησης της κίνησης στο δίκτυο και τα οποία επιβαρύνουν σημαντικά τον φόρτο στο δίκτυο κατά την μεταφορά τους. Η χρήση κινούμενων πρακτόρων μπορεί να μειώσει σημαντικά αυτή την επιβάρυνση καθώς έχουν την δυνατότητα να μετακινούνται

στον κόμβο που συλλέχθηκαν τα δεδομένα και να εκτελούν τοπικά την επεξεργασία. Μεταφέροντας λοιπόν τους πράκτορες και όχι τα δεδομένα μειώνεται και η κίνηση στο δίκτυο καθώς οι πράκτορες είναι πολύ μικρότεροι σε μέγεθος.

- Ασύγχρονη εκτέλεση και αυτονομία: σε συστήματα ανίχνευσης εισβολών τα οποία λειτουργούν με βάση ένα κεντρικό κόμβο διαχείρισης και ελέγχου υπάρχει πάντα ο κίνδυνος για βλάβη ή καταστροφή του κόμβου αυτού, γεγονός που θα προκαλέσει την αδράνεια όλου του συστήματος. Αντίθετα, ένας κινούμενος πράκτορας που έχει εισαχθεί στο σύστημα από ένα κόμβο του δικτύου μπορεί να συνεχίσει την λειτουργία του αυτόνομα ακόμα και αν ο κόμβος αυτός καταρρεύσει.
- Δυναμική προσαρμογή: είναι προφανές οτι καθώς η τοπολογία, η κίνηση και άλλα χαρακτηριστικά του δικτύου αλλάζουν με την πάροδο του χρόνου αλλάζουν και οι απαιτούμενοι έλεγχοι που πρέπει να διενεργούνται σε κάθε κόμβο του. Οι δυνατότητες των κινούμενων πρακτόρων όπως να ανακατευθύνονται, να αντιγράφονται, να τίθενται σε αναμονή και να τερματίζονται είναι πολύ σημαντικές γιατί προσφέρουν μεγάλη ευελιξία στην διαχείριση.
- Κλιμάκωση (scalability): η διεύρυνση του δικτύου με την προσθήκη νέων κόμβων αυξάνει συνεχώς τον φόρτο και τις απαιτήσεις ελέγχου σε ένα δίκτυο. Οι κινούμενοι πράκτορες σε κατανεμένα συστήματα μπορούν να υποστηρίξουν με επιτυχία την αύξηση των στοιχείων ενός δικτύου λόγω των δυνατοτήτων αντιγραφής τους και μεταφοράς τους σε κάθε νέο κόμβο που προστίθεται στο δίκτυο.
- Ανίχνευση πολλαπλών σημείων (multi-point detection): η ανίχνευση πολλαπλών σημείων αφορά την ανάλυση συμβάντων σε πολλά σημεία ταυτόχρονα ώστε να εντοπιστούν πιθανές επιθέσεις που έχουν ως στόχο το δίκτυο και τους πόρους του και όχι μεμονωμένους κόμβους. Οι κινούμενοι πράκτορες μπορούν να συσχετίσουν επιθέσεις σε διάφορους κόμβους του δικτύου, δρομολογητές κ.α. ώστε να ανιχνεύσουν μία τέτοια επίθεση ενώ στατικά συστήματα που είναι εγκατεστημένα σε ένα συγκεκριμένο κόμβο θα ανιχνεύουν μόνο μεμονωνμένες επιθέσεις.

4.2 Ελαφρείς πράκτορες για την ανίχνευση εισβολών (Light-weight agents for intrusion detection)

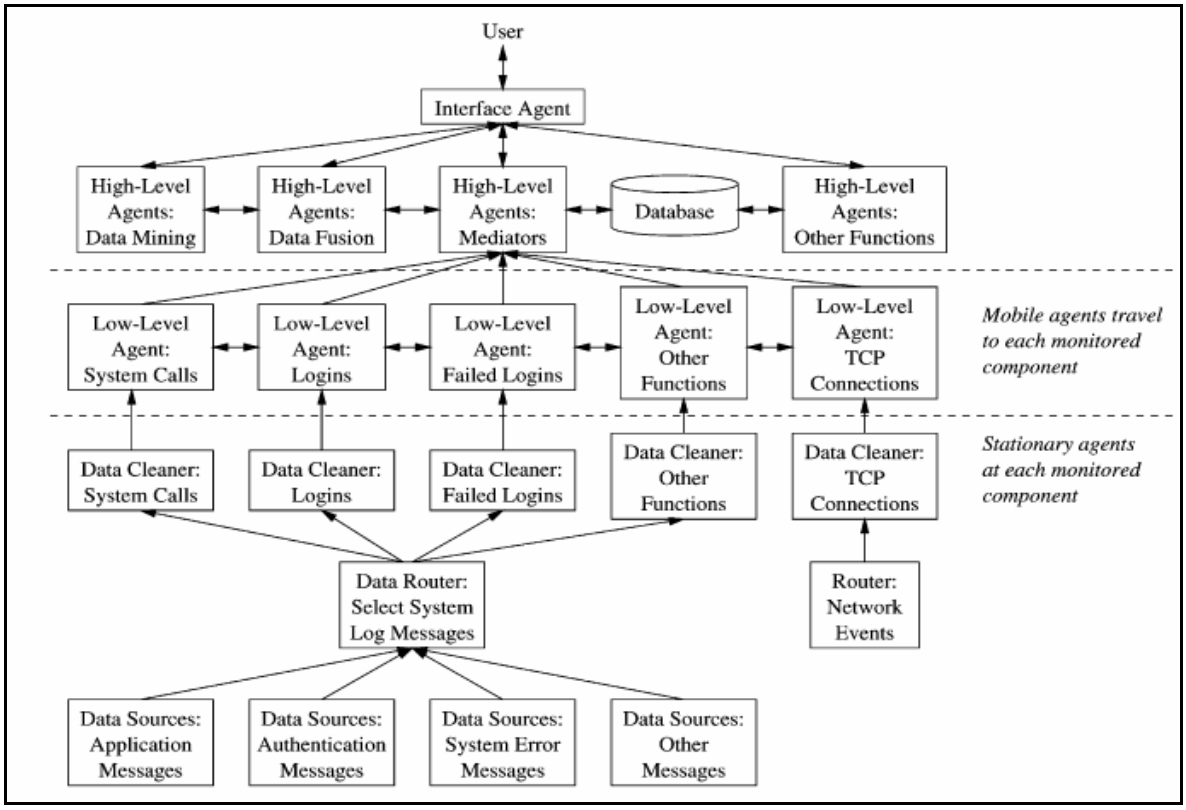
Μία πολύ ενδιαφέρουσα προσέγιση της χρήσης ευφυών πρακτόρων στην διαχείριση ασφάλειας του δικτύου και συγκεκριμένα στην ανίχνευση εισβολών είναι και το σύστημα που προτάθηκε

και υλοποιήθηκε από τους Guy Helmer, Johnny S.K. Wong, Vasant Honavar, Les Miller και Yanxin Wang του πανεπιστημίου της Iowa των Ηνωμένων Πολιτειών. Πιο συγκεκριμένα, η ομάδα αυτή ανέπτυξε ένα πρωτότυπο σύστημα ανίχνευσης εισβολών (IDS – Intrusion Detection System) που βασίζεται σε «ελαφρείς» πράκτορες οι οποίοι έδωσαν επιπλέον δυνατότητες επικοινωνίας και συνεργασίας.

Οι ελαφρείς πράκτορες είναι πράκτορες που μπορούν να εκτελούν τα βασικά τους καθήκοντα με τον ελάχιστο κώδικα δηλαδή κουβαλούν μόνο τους κανόνες που τους προσδίδουν τα πρωταρχικά τους χαρακτηριστικά και όταν φτάνουν στον προορισμό τους αναβαθμίζονται και ενημερώνονται ανάλογα με τις εκάστοτε απαιτήσεις. Επιπλέον, εκτός από δυναμικά ανανεώσιμοι και αναβαθμίσιμοι, είναι και πιο γρήγοροι στην μεταφορά τους εξαιτίας του μικρού τους μεγέθους.

Στο σύστημα, όπως φαίνεται και στο σχήμα 4.2, η επικοινωνία γίνεται σε δύο άξονες:

Η κατακόρυφη επικοινωνία αφορά την μεταφορά πληροφοριών από τους πράκτορες που συλλέγουν τις πληροφορίες προς τους αντίστοιχους κινούμενους πράκτορες και από εκεί στον τελικό προορισμό που είναι η διασύνδεση του χρήστη. Η οριζόντια επικοινωνία επιτυγχάνεται με την εισαγωγή της έννοιας της ευαισθησίας ενός πράκτορα. Ο βαθμός ευαισθησίας ενός πράκτορα καθορίζει πόσο ευαίσθητος είναι αυτός απέναντι σε συμβάντα που υπό φυσιολογικές συνθήκες δεν θεωρούνται απειλητικά αλλά μπορεί να αποτελούν εισβολή υπό την παρουσία συσχετιζόμενων εισβολών. Η υλοποίηση του βαθμού ευαισθησίας πραγματοποιήθηκε με την λεγόμενη δυναμική άθροιση (dynamic aggregation) που θα περιγραφεί παρακάτω.



Σχήμα 4.2: Αρχιτεκτονική και διάρθρωση της επικοινωνίας του συστήματος ελαφρών πρακτόρων

Η αρχιτεκτονική του συστήματος αποτελείται από τα ακόλουθα επίπεδα:

- Διασύνδεση χρήστη: εξασφαλίζει τον έλεγχο των πρακτόρων και παράγει αναφορές σε περιπτώσεις ανίχνευσης εισβολής.
- Συγχώνευση και εξόρυξη δεδομένων (data fusion and data mining): σε αυτό το επίπεδο οι πράκτορες συνδυάζουν τα δεδομένα που έλαβαν από τους πράκτορες χαμηλότερων επιπέδων και εξάγουν γνώση από την βάση δεδομένων που περιέχει στοιχεία ανιχνεύσιμων εισβολών κ.α. ώστε να δημιουργήσουν κανόνες πρόβλεψης εισβολών.
- Διαμεσολαβητές: διαχειρίζονται τους πράκτορες χαμηλού επιπέδου λαμβάνοντας τα δεδομένα από αυτούς, ελέγχοντας τα συστήματα που παρακολουθούνται και δρομολογώντας δεδομένα προς την διασύνδεση χρήστη και την βάση δεδομένων του συτήματος.
- Συλλογή δεδομένων και κατηγοριοποίηση: σε αυτό το επίπεδο βρίσκονται οι πράκτορες χαμηλού επιπέδου οι οποίοι περιοδικά επισκέπτονται τους στατικούς πράκτορες συλλογής δεδομένων με τους οποίους συνδέονται , παραλαμβάνουν από

αυτούς τα δεδομένα που συλλέχθηκαν και τα κατηγοριοποιούν ώστε να προσδιορίσουν αν συνέβησαν μεμονωνμένες εισβολές στο σύστημα.

- Πρωτογενής συλλογή στοιχείων: στο τελευταίο επίπεδο βρίσκονται οι στατικοί πράκτορες που συλλέγουν δεδομένα από παρακολούθηση αρχείων του συστήματος, των δρομολογητών κ.α. και παραδίδουν τα δεδομένα αυτά σε απλή μορφή στο ανώτερο επίπεδο.

Η υλοποίηση των πρακτόρων του συστήματος έγινε με την πλατφόρμα Voyager, η οποία είναι γραμμένη σε Java, άρα πλήρως μεταφέρσιμη και συμβατή με διάφορα λειτουργικά συστήματα και πλατφόρμες υλικού, αλλά είναι και η μόνη που υποστηρίζει την δυνατότητα της δυναμικής άθροισης που αποτελεί το κύριο χαρακτηριστικό της υλοποίησης αυτής.

Η δυναμική άθροιση είναι η δυνατότητα προσθήκης νέων χαρακτηριστικών στους πράκτορες κατά την διάρκεια εκτέλεσής τους. Στο συγκεκριμένο σύστημα οι ευφυείς πράκτορες είναι οι ονομαζόμενοι χαμηλού επιπέδου και είναι «ελαφρείς» με την έννοια του οτι είναι προσανατολισμένοι στην συλλογή πληροφοριών και δεν επικοινωνούν άμεσα μεταξύ τους παρά μόνο με τους στατικούς πράκτορες από τους οποίους αποκτούν δεδομένα. Η δυναμική άθροιση χρησιμοποιείται για την προσθήκη δυνατότητας συνεργασίας ανάμεσα σε αυτούς τους «ελαφρείς» πράκτορες του συστήματός ώστε αυτοί να αλληλοενημερώνονται για την ύπαρξη σχετιζόμενων επιθέσεων και να μεταβάλλουν το επίπεδο ευαισθησίας τους ώστε να επηρεάζουν ανάλογα την λήψη αποφάσεων.

Η υλοποίηση αυτού του συστήματος παρουσιάζει πολλά πλεονεκτήματα, πέρα από την ακρίβεια και μικρό χρόνο απόκρισης, το κύριο χαρακτηριστικό είναι οτι παρουσιάζει μειωμένο αριθμό λανθασμένων συναγερμών και αυτό οφείλεται στο επίπεδο ευασιθησίας που χρησιμοποιείται και επηρεάζει τον πράκτορα κατά την λήψη απόφασης σχετικά με το άν έχει συμβεί πραγματικά ή όχι επίθεση.

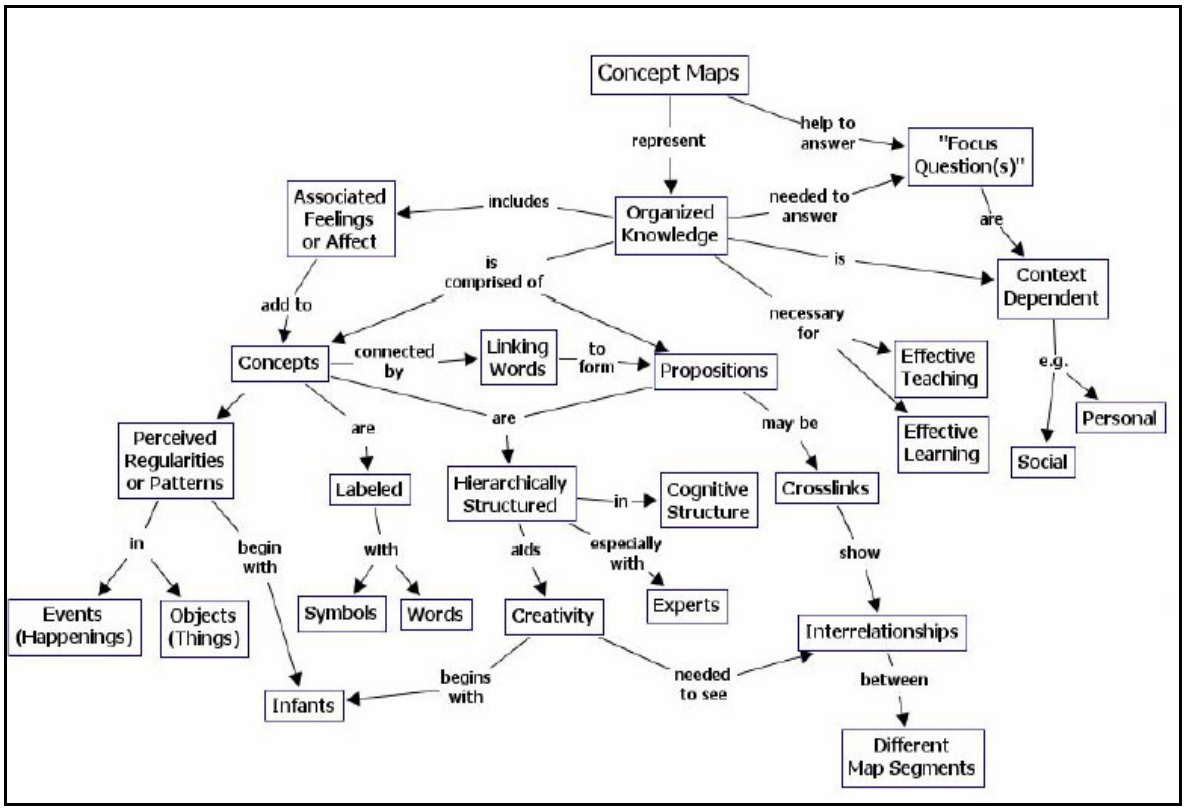
Μία ενδιαφέρουσα επέκταση του συστήματος αυτού θα περιλάμβανε την λήψη μέτρων για την αντιμετώπιση μίας εισβολής. Ο κώδικας που θα ήταν υπεύθυνος για την εκτέλεση των μέτρων δράσης θα μπορούσε να προστίθεται μόνο στους αντίστοιχους πράκτορες που θα εκτελέσουν τις ενέργειες αυτές όταν αυτό χρειάζεται μέσω της δυναμικής άθροισης και να μην υπάρχει εκ των προτέρων σε όλους τους πράκτορες που υλοποιεί το σύστημα.

4.3 Η προσέγγιση MAST (Mobile Agent-based Security Tool)

Το MAST αποτελεί μία πρόταση των Marco Carvalho, Thomas Cowin και Niranjan Suri του Institute for Human and Machine Cognition του Πανεπιστημίου της Δ. Φλόριντα και

αφορά ένα εργαλείο διαχείρισης ασφάλειας βασιζόμενο σε τεχνολογία κινούμενων πρακτόρων και γνωστικούς χάρτες (concept maps).

Οι γνωστικοί χάρτες είναι μία σύλληψη του Novak κατά την δεκαετία του ΄70 και ουσιαστικά αποτελούν εργαλείο οργάνωσης και αναπαράστασης της γνώσης. Ένας γνωστικός χάρτης αφορά ένα γνωστικό πεδίο και αποτελείται από μία γραφική αναπαράσταση διαφόρων εννοιών του συγκεκριμένου γνωστικού πεδίου και των μεταξύ τους σχέσεων. Κάθε χάρτης είναι ιεραρχικά οργανωμένος με βάση συγκεκριμένες δηλώσεις οι οποίες αναφέρονται και ως σημασιολογικές μονάδες (semantic units). Ουσιαστικά, οι σημασιολογικές μονάδες περιγράφουν την σχέση μεταξύ δύο εννοιών που περιέχονται στον χάρτη. Η οργάνωση των εννοιών γίνεται από πάνω προς τα κάτω (top down) με αποτέλεσμα οι πιο γενικές έννοιες να βρίσκονται στην κορυφή και οι πιο ειδικές στην βάση του χάρτη. Ένα παράδειγμα γνωστικού χάρτη παρουσιάζεται στο σχήμα 4.3.



Σχήμα 4.3: Δομή γνωστικού χάρτη

Οι γνωστικοί χάρτες μπορούν να χρησιμοποιηθούν ως εργαλείο εκμαίευσης και αναπαράστασης της γνώσης ενός ειδικού σε μία γνωστική περιοχή καθώς και για εύκολη πλοήγηση ακόμα και από ένα αρχάριο μέσα στις πληροφορίες του γνωστικού μοντέλου που

προκύπτει. Ένα πολύ βασικό χαρακτηριστικό των γνωστικών χαρτών, που βρίσκει μεγάλη εφαρμογή στο εργαλείο MAST, είναι η έννοια της οριζόντιας σύνδεσης (cross-link) η οποία αποτελεί συσχέτιση μεταξύ εννοιών που βρίσκονται σε διαφορετικά κλαδιά (διαφορετικές γνωστικές υπο-περιοχές) του γνωστικού χάρτη.
Οι κινούμενοι πράκτορες χρησιμοποιούνται κατά κάποιο τρόπο ως φρουροί ασφαλείας που περιφέρονται μέσα στο δίκτυο και αξιολογούν τα πιθανώς ευάλωτα σημεία του. Το MAST χρησιμοποιεί πράκτορες ειδικού-σκοπού οι οποίοι εισάγονται στο σύστημα αυτόματα είτε από το ίδιο το εργαλείο είτε από τον διαχειριστή και εκτελούνται τοπικά εκτελώντας ενέργειες παρακολούθησης και συντήρησης του δικτύου όπως αναβαθμίσεις κ.α. Εδώ χρησιμοποιείται εκτενώς το χαρακτηριστικό του «κινητού κώδικα» των κινούμενων πρακτόρων οι οποίοι «κουβαλούν» μαζί τους κώδικα για αναβαθμίσεις σε χαρακτηριστικά ασφάλειας και αλλαγές στην διάταξη (configuration) του δικτύου προκειμένου να αντιμετωπίζονται οι νέες απειλές επιθέσεων.

Τα κύρια συστατικά του MAST είναι τα παρακάτω:

- Η κονσόλα του διαχειριστή (administrator's console) η οποία είναι μία εφαρμογή που παρέχει το κύριο τμήμα της γραφικής διασύνδεσης με τον χρήστη. Μέσω αυτής γίνεται η πιστοποίηση της ταυτότητας των χρηστών πριν αποκτήσουν πρόσβαση στο σύστημα. Μετά την πιστοποίηση ο πυρήνας ασφαλείας του συγκεκριμένου κόμβου καθώς και οι πράκτορες που φορτώνονται από αυτή την κονσόλα είναι επίσης πιστοποιημένοι. Αυτό το μοντέλο διασφαλίζει οτι κάθε πράκτορας που εισάγεται από την συγκεκριμένη κονσόλα και τον συγκεκριμένο χρήστη θα συνεχίζει να θεωρείται αξιόπιστος από το σύστημα ακόμα και όταν κλείσει η κονσόλα ή αποσυνδεθεί ο χρήστης.
- Ο πυρήνας ασφαλείας (security kernel) ο οποίος είναι εγκατεστημένος στους κόμβους του δικτύου και είναι υπεύθυνος για την εκτέλεση εξ' αποστάσεως (remote execution) των πρακτόρων. Επιπλέον, ο πυρήνας παρέχει υπηρεσίες κρυπτογράφησης και πιστοποίησης κατά την επικοινωνία μεταξύ πρακτόρων και κονσόλας διαχειριστή ώστε κάθε φορά που επικοινωνεί ένας πράκτορας με την κονσόλα ή μεταφέρεται ένας πράκτορας σε ένα κόμβο να διασφαλίζεται η ακεραιότητα του κώδικα που εισάγεται στην συνέχεια στον πυρήνα ασφαλείας κάθε κόμβου. Πιο συγκεκριμένα, πυρήνας ασφαλείας εγκαθίσταται σε όλα τα συστήματα από τον διαχειριστή ο οποίος παρέχει κατά την εγκατάσταση το δημόσιο κλειδί του MAST server το οποίο διασφαλίζει την πιστοποίησή του.

Επίσης, κάθε πυρήνας δημιουργεί το δικό του ζεύγος κλειδιών που θα χρησιμοποιεί για την αυθεντικοποίησή του (authentication) κατά την επικοινωνία του με άλλους πυρήνες. Όλα τα υπόλοιπα αντικείμενα του MAST βρίσκονται πάνω από τον πυρήνα συνεπώς κάθε επικοινωνία μεταξύ των πρακτόρων ή άλλων συστατικών του MAST γίνεται μέσω των πυρήνων που έτσι διασφαλίζουν την αυθεντικότητα των μερών που επικοινωνούν. Επιπλέον, ο πυρήνας εξασφαλίζει την τήρηση κάποιας πολιτικής σχετικά με τον έλεγχο των πόρων του κόμβου στον οποίο εκτελείται ένας πράκτορας ώστε η εκτέλεση των πρακτόρων να μην επηρεάζει την κανονική λειτουργία των κόμβων του δικτύου.

- Ένα γνωστικό μοντέλο (knowledge model) της ασφάλειας του δικτύου,που βασίζεται στους γνωστικούς χάρτες που περιγράφηκαν παραπάνω, και το οποίο είναι συνεχώς αναβαθμιζόμενο. Στο πλαίσιο του MAST οι γνωστικοί χάρτες χρησιμοποιούνται για την οργάνωση και παροχή πρόσβασης σε πληροφορίες που αφορούν διάφορα θέματα ασφάλειας του δικτύου. Για τον χειρισμό των χαρτών που αποτελούν το γνωστικό μοντέλο του συστήματος χρησιμοποιείται το CmapTools, το οποίο είναι λογισμικό διαχείρισης γνωστικών χαρτών, με κάποιες μετατροπές. Το σημαντικό είναι οτι η λειτουργία του MAST δεν βασίζεται στο γνωστικό μοντέλο αποκλειστικά αλλά κάθε διαδικασία μπορεί κάλλιστα να εκτελεστεί απευθείας από τον διαχειριστή ή εναλλακτικά μέσω αλληλεπίδρασης με τους πράκτορες που σχετίζονται μετο γνωστικό μοντέλο του θέματος προς αντιμετώπιση.
- Ένα σύνολο πρακτόρων ασφάλειας (security agents) οι οποίοι αποτελούν μέρος του γνωστικού μοντέλου και περιηγούνται στους κόμβους του δικτύου για να εκτελούν τα καθήκοντά τους. Ανάλογα με το επίπεδο πρόσβασης του κάθε χρήστη οι πράκτορες μπορεί να είναι ή απλά διερευνητικοί για ενημερωτικούς σκοπούς είτε πράκτορες παρακολούθησης ή διόρθωσης οι οποίοι θα ελέγχουν την ύπαρξη ευάλωτων σημείων και θα τα διορθώνουν.
- Ο διακομιστής MAST (MAST Server) ο οποίος υλοποιείται ως ένα σύνολο τμημάτων (modules) τα οποία συλλογικά διατηρούν την βάση δεδομένων και υλοποιούν τις λειτουργίες του συστήματος. Ο διαχειριστής του συστήματος είναι υπεύθυνος να ορίσει πόσα τμήματα μπορούν να εκτελούνται ταυτόχρονα σε ένα κόμβο. Τα τμήματα αυτά είναι στην ουσία κινητοί πράκτορες και επομένως έχουν την δυνατότητα αντιγραφής του εαυτού τους και κίνησης ακολουθώντας την καθορισμένη πολιτική ασφάλειας του δικτύου. Όταν ένα σύστημα του δικτύου

επιθυμεί πρόσβαση σε ένα τμήμα (module) που παρέχει μία συγκεκριμένη υπηρεσία πρέπει πρώτα να προσδιορίσει την τοποθεσία του τμήματος που υλοποιεί την υπηρεσία αυτή και μετά είναι σε θέση για επικοινωνία με χρήση ενός συγκεκριμένου πρωτοκόλλου, του SLP πρωτοκόλλου (Service Location Protocol). Το μόνο τμήμα που θα βρίσκεται σταθερά σε μία συγκεκριμένη θέση είναι το SKBS (Security Kernel Bootstrap Service) το οποίο χρησιμοποιείται κατά την διαδικασία εκκίνησης του συστήματος.

Τα τμήματα του διακομιστή είναι:

- Το τμήμα που υλοποιεί την υπηρεσία διαχείρισης των πρακτόρων (Agent Management Service module). Η υπηρεσία διαχείρισης πρακτόρων (Agent Management Service) ασχολείται με την φόρτωση και τον εντοπισμό των πρακτόρων στο σύστημα καθώς και με τον τερματισμό τους. Η εισαγωγή των πρακτόρων είναι δυνατό να γίνει μόνο μέσω της υπηρεσίας αυτής οπότε επιτρέπεται στον διαχειριστή πριν την εισαγωγή να πιστοποιεί αν ο κώδικας ενός πράκτορα διατηρεί την ακεραιότητά του γεγονός το οποίο παρέχει ένα ακόμα επίπεδο ασφάλειας πέρα από τις υπηρεσίες του πυρήνα ασφαλείας ενάντια σε επιθέσεις κακόβουλων πρακτόρων.
- Το τμήμα που υλοποιεί την υπηρεσία καταγραφής (Logging Service module). Πέρα από τα αρχεία log που διατηρεί ο κάθε πυρήνας ασφαλείας, διατηρείται και μία κεντρική βάση δεδομένων στην οποία οι πράκτορες αναφέρουν συμβάντα κια σφάλματα που παρουσιάστηκαν.
- Το τμήμα που υλοποιεί την υπηρεσία πιστοποίησης (Authentication Service module), η οποία είναι υπεύθυνη για την πιστοποίηση των πυρήνων ασφαλείας, των πρακτόρων αλλά και των χειριστών του συστήματος.
- Το τμήμα διαχείρισης ευπαθειών (Vulnerability/Advisory Management Service module). Το τμήμα αυτό διατηρεί μία βάση δεδομένων με αναφορές ασφαλείας από πηγές στο διαδίκτυο.

Πολύ σημαντικό είναι και το θέμα της ασφάλειας του ίδιου του πράκτορα αφού το κύριο μειονέκτημα των κινούμενων πρακτόρων είναι το ότι μπορούν να γίνουν φορείς επιθέσεων για το δίκτυο. Το MAST χειρίζεται το θέμα αυτό πολύ αποτελεσματικά καθώς η πολιτική ασφαλείας του ορίζει οτι η κίνηση των πρακτόρων θα γίνεται πάντα μεταξύ της κονσόλας και του πυρήνα ασφαλείας ενός κόμβου και ποτέ μεταξύ πυρήνων (single hop mobility). Με αυτόν τον τρόπο αποφεύγεται ο κίδυνος κάποιος εχθρικός κόμβος να μεταβάλλει τον πυρήνα του ώστε επιτεθεί στον πράκτορα και να μεταβάλλει τον κώδικά του ώστε να μεταδοθεί σε όλο το

δίκτυο. Τέλος, κάθε πράκτορας ελέγχεται για την ακεραιότητά του κάθε φορά που επιστρέφει στην κονσόλα του διαχειριστή. Η διασφάλιση της ασφάλειας των ίδιων των πρακτόρων του συστήματος είναι ένα από τα μεγαλύτερα πλεονεκτήματα του MAST και αναπτύσσεται λεπτομερώς στο [8]. Μία πρόταση για μελλοντική έρευνα θα αφορούσε την επέκταση του εργαλείου MAST έτσι ώστε κάθε πράκτορας να ελέγχει αν το περιβάλλον στο οποίο πρόκειται να εκτελεστεί έχει υποστεί μεταβολή, γεγονός το οποίο θα μπορούσε να επηρεάσει την ακεραιότητά του, και επομένως να μην υφίσταται η απαίτηση για αποδοχή της υπόθεσης οτι η κινήσεις των πρακτόρων είναι πάντα μοναδικού άλματος (single hop). Επιπλέον, οι ίδιοι οι σχεδιαστές του εργαλείου MAST βρίσκονται ήδη προς την κατεύθυνση εισαγωγής αυτοματισμού στις διαδικασίες διατήρησης των γνωστικών μοντέλων και των βάσεων δεδομένων που διατηρεί το σύστημα και οι οποίες σήμερα απαιτούν μεγάλο βαθμό ανθρώπινης ανάμιξης κυρίως όσο αφορά διορθώσεις και αναβαθμίσεις. Επίσης, ένας από τους επόμενους στόχους θα είναι η δημιουργία ενός μηχανισμού παραγωγής ειδοποιήσεων προς τον διαχειριστή του δικτύου όταν συμβαίνουν αλλαγές στο γνωστικό μοντέλο του συστήματος γεγονός το οποίο όταν υλοποιηθεί θα αποτελεί σημαντικό πλεονέκτημα στην χρήση του MAST αφού θα παρέχει δυνατότητα στον διαχειριστή να παρακολουθεί απο κοντά τις όποιες αλλαγές επηρεάζουν την συμπεριφορά όλου του συστήματος.

5. Βιβλιογραφία

[1] K. Boudaoud, H. Labiod, R. Boutaba, Z. Guessoum, *"Network Security Management with Intelligent Agents"*

[2] K. Boudaoud, Noria Foukia, Z. Guessoum, *"An Intelligent Agent Approach for Security Management"*

[3] Γ.Πάγκαλου Ι. Μαυρίδη, *"Ασφάλεια πληροφοριακών συστημάτων και δικτύων"*

[4] Mehdi Shajari and Ali A. Ghorbani, *"Application of Belief-Desire-Intention Agents in Intrusion Detection & Response",* Institute for Information Technology - e-Business, National Research Council of Canada.

[5] A. Rao and M. Georgeff, *"Modeling rational agents within a BDIarchitecture,"* Proceedings of the Second International Conference on Principles of Knowledge Representation and Reasoning, J. Allen, R. Fikes, and E. Sandewall, eds., pp. 473–484. Morgan Kaufmann Publishers, San Mateo, CA, 1991.

[6] Guy Helmer, Johnny S.K. Wong, Vasant Honavar, Les Miller και Yanxin Wang, *"Ligthweight agents for intrusion detection" ,* Iowa State University USA, The Journal of Systems and Software 67 (2003) 109–122

[7] Marco Carvalho, Thomas Cowin and Niranjan Suri, *"MAST – A Mobile Agent-based Security Tool ,* Institute for Human and Machine Cognition – University of West Florida

[8] Marco Carvalho, Thomas Cowin, Niranjan Suri, Maggie Breedy, Kenneth Ford, *"Using Mobile Agents as Roaming Security Guards to Test and Improve Security of Hosts and Networks"* , Institute for Human and Machine Cognition

[9] Green, S. et al. *"Software Agents: A review"*, Technical Report, Department of Computer Science, Trinity College, Dublin, Ireland.

[10] Jack Intelligent Agent User Guide, *http://www.agent-software.com*

[11] T. Karygiannis, *"Network Security Testing Using Mobile Agents",* National Institute of Standards and Technology, Practical Application of Intelligent Agents and Multi-Agents - March 1998.

[12] Jansen, W, Mell, P, Karygiannis, T and Marks*, "D Mobile Agents in Intrusion Detection and Response",* Proc. of the 12th Annual Canadian Information Technology Security Symposium, Ottawa, Canada (2000).