Μοντελοποίηση και Επαλήθευση Κινητών Συστημάτων με Τεχνικές Αλγεβρικών Προδιαγραφών

Διδακτορική Διατριβή

Ιάκωβος Χ. Ουρανός
Ηλεκτρολόγος Μηχ. & Μηχ. Υπολογιστών Ε.Μ.Π.
E-mail: iouranos@central.ntua.gr

1. Εισαγωγή – Βασικές έννοιες

Τυπικές μέθοδοι

Η πολυπλοκότητα και οι χρήστες των συστημάτων λογισμικού και υλικού αυξάνονται συνεχώς.

Σημαντικό πρόβλημα: Πιθανά ΣΦΑΛΜΑΤΑ μπορούν να έχουν αρνητικές συνέπειες.

Σκοπός: Ανάπτυξη αξιόπιστων συστημάτων ανεξαρτήτως πολυπλοκότητας

Τυπικές μέθοδοι

- Τεχνικές, γλώσσες και εργαλεία

- βασίζονται στα μαθηματικά

- ισχυρή βάση για σχεδίαση, προδιαγραφή και επαλήθευση συστημάτων υλικού και λογισμικού.

Τυπικές μέθοδοι

- Abstract State Machines
- B method
- RAISE
- UNITY
- SDL
- Petri Nets
- Process algebras
- Z
- TLA
- LOTOS
- Αλγεβρικές Γλώσσες Προδιαγραφών

Αλγεβρικές Γλώσσες Προδιαγραφών

-Maude (USA)

- CASL (Common Algebraic Specification Language, Ευρώπη)

- CafeOBJ (Ιαπωνία)

Κινητά Συστήματα

Συστήματα επικοινωνιών ή/και υπολογισμού όπου η μεταβολή της θέσης επηρεάζει τη συμπεριφορά τους.

Κινητά Συστήματα

Ιδιαίτερα χαρακτηριστικά που τα διακρίνουν από τα στατικά κατανεμημένα συστήματα:

1. περιορισμοί ασύρματης επικοινωνίας,
2. χαρακτηριστικά κινητών συσκευών,
3. περιορισμοί λόγω κινητικότητας.

Κινητά Συστήματα

περιορισμοί ασύρματης επικοινωνίας

α) μικρό εύρος ζώνης,
β) μεταβλητό εύρος ζώνης,
γ) αποσύνδεση,
δ) άλλοι (καθυστέρηση δικτύου, απώλειες πακέτων, κ.α.)

Κινητά Συστήματα

χαρακτηριστικά κινητών συσκευών

α) περιορισμένοι πόροι,
β) συχνές αποσυνδέσεις από το δίκτυο,
γ) ασφάλεια

Κινητά Συστήματα

περιορισμοί λόγω κινητικότητας

α) ετερογένεια,
β) δυναμικό περιβάλλον,
γ) μεταβολές διαθεσιμότητας πόρων

Κινητά Συστήματα

Είδη κινητικότητας:

α) φυσική κινητικότητα,

β) λογική κινητικότητα

Τυπικές Μέθοδοι & Κινητά Συστήματα

Για τη σχεδίαση και ανάπτυξη αξιόπιστων κινητών συστημάτων, υπηρεσιών και πρωτοκόλλων έχουν παρουσιασθεί αντίστοιχες τυπικές μέθοδοι.

Δύο τρόποι ανάπτυξης:

1) Με επέκταση μιας υπάρχουσας μεθόδου.
2) Με υλοποίηση νέας, αποκλειστικά για κινητά συστήματα.

Τυπικές Μέθοδοι & Κινητά Συστήματα

- Mobile UNITY
- Mobile TLA
- Mobile Z
- Mobile Maude

- π-calculus

CafeOBJ

Τυπικά μοντέλα που υποστηρίζει

1. **Αφηρημένους Τύπους Δεδομένων**
2. **Αφηρημένες Μηχανές Καταστάσεων**

“Η CafeOBJ παρέχει ενοποιημένο τρόπο προδιαγραφής τόσο για στατικά όσο και δυναμικά συστήματα”

CafeOBJ

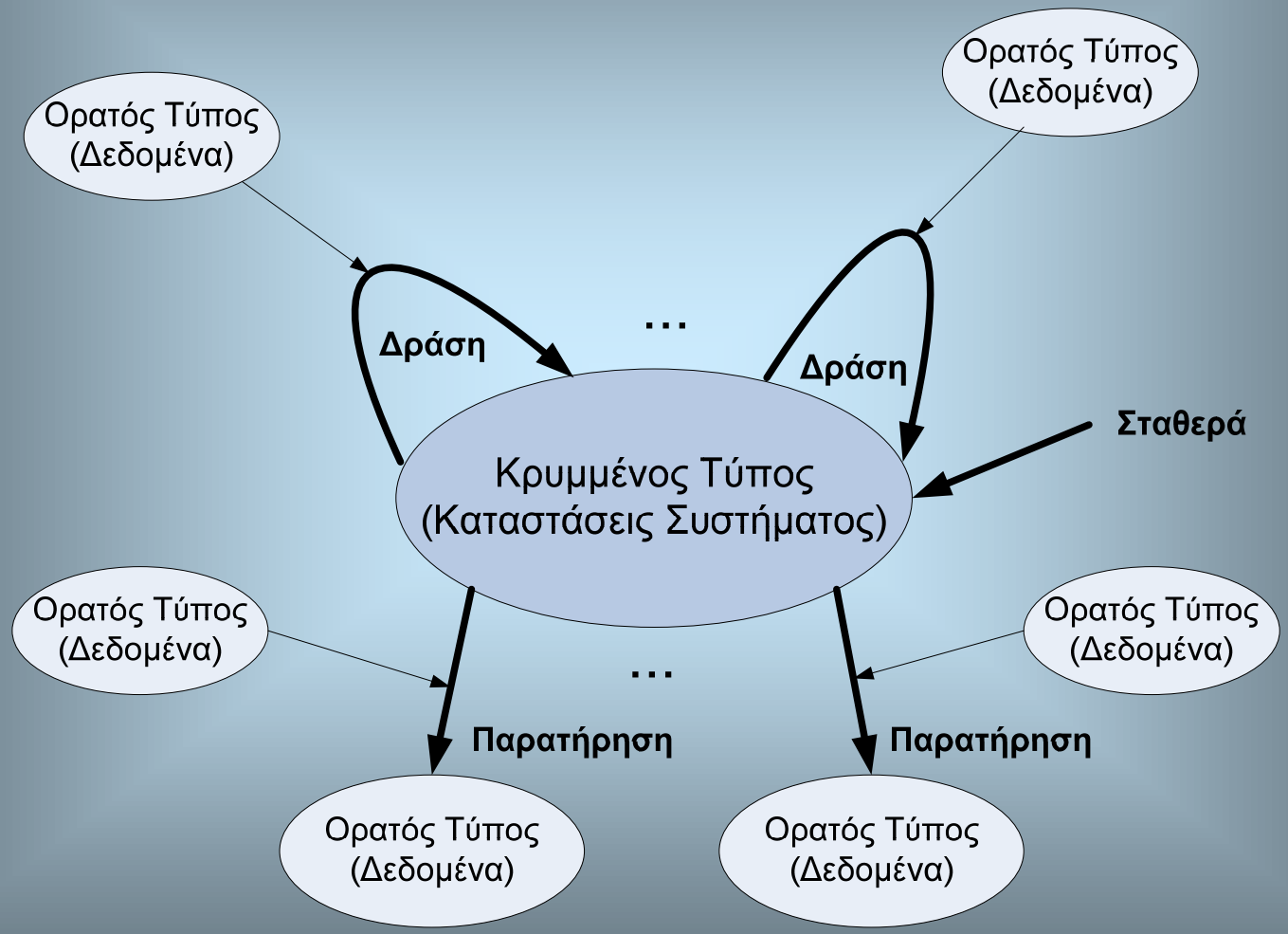
Στοιχεία Συντακτικού της Γλώσσας

Δύο είδη **τύπων**:

- **Ορατοί (Visible)**

- **Κρυμμένοι (Hidden)**

CafeOBJ


Ορατός Τύπος
(Δεδομένα)
Ορατός Τύπος
(Δεδομένα)
Δράση
...
Δράση
Σταθερά
Κρυμμένος Τύπος
(Καταστάσεις Συστήματος)
Ορατός Τύπος
(Δεδομένα)
Ορατός Τύπος
(Δεδομένα)
...
Παρατήρηση
Παρατήρηση
Ορατός Τύπος
(Δεδομένα)
Ορατός Τύπος
(Δεδομένα)

CafeOBJ

Δηλώσεις τελεστών στην CafeOBJ

(δράση)
bop *όνομα_δράσης* **:** *ορατός1 ορατός2 ... ορατόςn κρυμμένος* $\rightarrow$ *κρυμμένος*

(παρατήρηση)
op *όνομα_παρατ* **:** *ορατός1 ορατός2 ... ορατόςn κρυμμένος* $\rightarrow$ *ορατός*

(σταθερά)
op *όνομα_σταθεράς* **:** $\rightarrow$ *κρυμμένος*

CafeOBJ

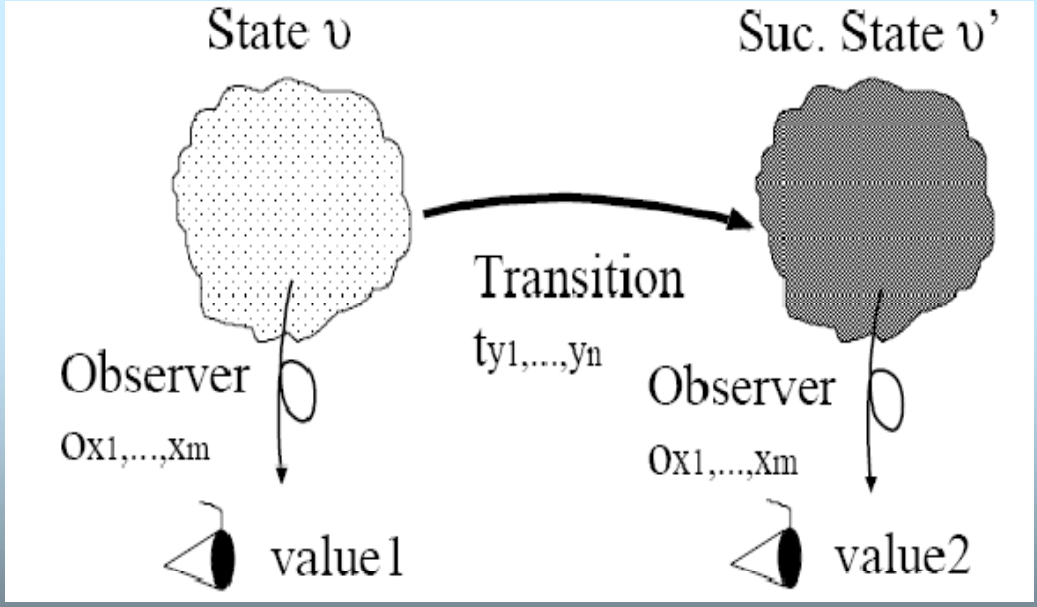
Ορισμός τελεστών με εξισώσεις (κανόνες αναγραφής)

eq *term1 = term2* .

Για εξίσωση με συνθήκη:
ceq *term1 = term2* **if** *cond1* .

CafeOBJ και ΠΣΜ

<u>Παρατηρήσιμα Συστήματα Μεταβάσεων (ΠΣΜ)</u>:
Συστήματα μετάβασης που μπορούν να γραφούν άμεσα ως αλγεβρικές προδιαγραφές.



CafeOBJ και ΠΣΜ

Παρατηρήσιμα Συστήματα Μεταβάσεων (Observational Transition Systems):

Ένα ΠΣΜ $S = <O, I, T>$ αποτελείτε από:

• O: Ένα πεπερασμένο σύνολο από παρατηρητές. Κάθε $o \in O$ είναι μια δεικτοδοτημένη συνάρτηση $o_{x1:Do1,...,xm:Dom} : Y \rightarrow D$, όπου Y ο χώρος καταστάσεων και D ο τύπος δεδομένων που επιστρέφει ο παρατηρητής. Η σχέση ισοδυναμίας $(v1 =_S v2)$ ανάμεσα σε δύο καταστάσεις $v_1, v_2 \in Y$ ορίζεται ως $\forall o \in O. o(v_1) = o(v_2)$.

CafeOBJ και ΠΣΜ

Παρατηρήσιμα Συστήματα Μεταβάσεων (Observational Transition Systems):

Ένα ΠΣΜ $S = <O, I, T>$ αποτελείται από:

- *I:* Το σύνολο αρχικών καταστάσεων ώστε $I \subseteq Y$.
- *T*: Ένα πεπερασμένο σύνολο από μεταβάσεις. Κάθε $t \in T$ είναι μια δεικτοδοτημένη συνάρτηση $t_{y1:Dt1,...,yn:Dtn} : Y \rightarrow Y$. Σε κάθε *t* αντιστοιχεί μια συνθήκη *c-t* που καλείται αποτελεσματική συνθήκη της μετάβασης. Εάν η συνθήκη της μετάβασης δεν ικανοποιείται σε μία κατάσταση, τότε η εφαρμογή της δεν επηρεάζει το σύστημα.

CafeOBJ και ΠΣΜ

Επιτεύξιμες καταστάσεις και αμετάβλητα κατηγορήματα

Οι επιτεύξιμες καταστάσεις ενός ΠΣΜ S ορίζονται επαγωγικά:

- Κάθε αρχική κατάσταση $u_{init} \in I$ είναι επιτεύξιμη
- Για κάθε $t_{y1,...,yn} \in T$ και κάθε $y_k : D_{tk}$ για $k = 1,... ,n$, η $t_{y1,...,yn}(\upsilon)$ είναι επιτεύξιμη στο S εάν η $\upsilon \in Y$ είναι επιτεύξιμη στο S.

Έστω R_s το σύνολο όλων των επιτεύξιμων καταστάσεων στο S ή επιτεύξιμος χώρος καταστάσεων στο S.

CafeOBJ και ΠΣΜ

Επιτεύξιμες καταστάσεις και αμετάβλητα κατηγορήματα κατάστασης

Ένα κατηγόρημα κατάστασης $p : Y \rightarrow \text{Bool}$ είναι *αμετάβλητο* στο S εάν η τιμή του είναι true για όλες τις επιτεύξιμες καταστάσεις του S, δηλαδή $\forall\, v : R_s.\ p(v)$.

Όλες οι ιδιότητες που αποδεικνύονται στη διατριβή είναι αμετάβλητα κατηγορήματα καταστάσεων (invariants).

CafeOBJ και ΠΣΜ

Γράφοντας ΠΣΜ στην CafeOBJ

Ένα ΠΣΜ γράφεται στην CafeOBJ και μοντελοποιεί κατανεμημένα συστήματα:

- Ο χώρος καταστάσεων *Y* μοντελοποιείται από ένα κρυμμένο τύπο *H*.
- Οι παρατηρητές $o_{i1 \ldots im}$ συμβολίζονται από τους τελεστές παρατήρησης της CafeOBJ και δηλώνονται ως εξής

bop o : H V_{i1} … V_{im} -> V

CafeOBJ και ΠΣΜ

Γράφοντας ΠΣΜ στην CafeOBJ

• Οι μεταβάσεις $t_{j1\ldots jn}$ συμβολίζονται από τους τελεστές δράσης της CafeOBJ και δηλώνονται ως εξής

bop a : H V_{j1} … V_{jn} -> H

ενώ ο ορισμός τους γίνεται μέσω εξισώσεων που περιγράφουν την αλλαγή της τιμής των παρατηρητών μετά την εφαρμογή τους

ceq o(X_{i1},…,X_{im}, a(X_{j1},…,X_{jn}, S)) =

e-a(X_{j1},…,X_{jn}, X_{i1},…,X_{im}, S) **if** c-a(X_{j1},…,X_{jn}, S) .

CafeOBJ και ΠΣΜ

Γράφοντας ΠΣΜ στην CafeOBJ

- Η αρχική κατάσταση συμβολίζεται με μια σταθερά έστω init

  op init : -> H

Επαλήθευση ΠΣΜ

Σημαντικότερη συνεισφορά: Δυνατότητα επαλήθευσης ιδιοτήτων της προδιαγραφής - σχεδίασης του συστήματος.

ΤΕΧΝΙΚΗ ΑΠΟΔΕΙΞΗΣ: Επαγωγική

Συνήθως απαιτούνται: Διάκριση υπό-περιπτώσεων και εύρεση βοηθητικών λημμάτων.

Επαλήθευση ΠΣΜ

Τι μας προσφέρει: Σωστότερο και αξιόπιστο σχεδιασμό – καλύτερη κατανόηση συστήματος – λιγότερα λάθη στην υλοποίηση

Πλεονεκτήματα: Ευκολότερα κατανοητή μέθοδος (εξισώσεις), αποδείξεις για συστήματα με άπειρο χώρο καταστάσεων, κατανόηση συστήματος μέσα από την δια-δραστική μεθοδολογία αποδείξεων.

Επαλήθευση ΠΣΜ

Μειονεκτήματα: Δυσκολία στην εύρεση λημμάτων – λιγότερο αυτοματοποιημένη σε σχέση με τεχνικές ελέγχου μοντέλου.

Επαλήθευση ΠΣΜ

Μεθοδολογία

1. Έκφραση της ιδιότητας προς απόδειξη ως κατηγόρημα κατάστασης *pred (p, x)*.

2. Δήλωση της ιδιότητας ως όρο της CafeOBJ σε ένα module που συνήθως καλείται INV

```
op inv : H V -> Bool

eq inv (P, X) = pred (P, X) .
```

Επαλήθευση ΠΣΜ

Μεθοδολογία

3. Δείχνουμε ότι η ιδιότητα διατηρείται σε κάθε αρχική κατάσταση, έστω init

```
open INV
    red inv (init, X) .
close
```

Επαλήθευση ΠΣΜ

Μεθοδολογία

4. Γράφουμε ένα module ISTEP στο οποίο δηλώνονται μια κατάσταση και η διαδοχή της (μετά την εφαρμογή της μετάβασης) ως σταθερές p και p' και το επαγωγικό βήμα της απόδειξης της ιδιότητας

```
op istep : V -> Bool

eq istep (X) = inv(p, X)

                    implies inv(p', X) .
```

Επαλήθευση ΠΣΜ

Μεθοδολογία

5. Γράφουμε το αποδεικτικό κομμάτι για κάθε περίπτωση μετάβασης

```
  open ISTEP
Δήλωση σταθερών που συμβολίζουν αντικείμενα
Δήλωση εξισώσεων που δηλώνουν την περίπτωση
  eq p' = a(p, y) .
  red istep(x) .
    close
```

2. Το πλαίσιο αλγεβρικών προδιαγραφών MobileOBJ

Κινητά ΠΣΜ

Επέκταση των ΠΣΜ για την προδιαγραφή κινητών συστημάτων

Μοντελοποίηση κινητικότητας:

- παρατηρητές θέσης (spatial observers) για κάθε αντικείμενο,
- δράση κινητικότητας (mobility action) για μεταβολή θέσης (όταν το αντικείμενο μπορεί να ελέγχει τη θέση του – mobile robots)

Κινητά ΠΣΜ

Επέκταση των ΠΣΜ για την προδιαγραφή κινητών συστημάτων

Μοντελοποίηση επικοινωνίας:

- μέσω ασύγχρονης μεταφοράς μηνυμάτων (asynchronous message passing)
- δράσεις επικοινωνίας (communication actions) με παραμέτρους μηνύματα
- χρήση ουρών ή/και συνόλων μηνυμάτων

Κινητά ΠΣΜ

Επέκταση των ΠΣΜ για την προδιαγραφή κινητών συστημάτων

Μοντελοποίηση αλληλεπίδρασης:

- για σύνδεση – αποσύνδεση στο σύστημα
- μέθοδοι αλληλεπίδρασης (interaction methods)

Κινητά ΠΣΜ

Επέκταση των ΠΣΜ για την προδιαγραφή κινητών συστημάτων

Για κινητό κώδικα:

- μέθοδοι κλωνοποίησης (cloning methods)

Για διαχείριση πόρων:

- δράσεις και παρατηρητές διαχείρισης πόρων των αντικειμένων

Κινητά ΠΣΜ

Τυπικός Ορισμός

Έστω L σύνολο από περιοχές. Ένα Κινητό ΠΣΜ S ορίζεται ως $< O, I, T \cup \{move_\lambda \mid \lambda \in L\} > \tau.\omega$:

- O το σύνολο των παρατηρητών το οποίο διαχωρίζεται στο σύνολο των D των διακριτών παρατηρητών και το σύνολο SP των χωρικών δηλ. $O = D \cup SP$. Ο τύπος της περιοχής $\lambda \in L$ μπορεί να είναι διακριτός ή συνεχής, μονοδιάστατος ή πολυδιάστατος.
- I το σύνολο των αρχικών καταστάσεων. Ο χωρικός παρατηρητής για κάθε αντικείμενο είναι ο *home location*.

Κινητά ΠΣΜ

Τυπικός Ορισμός

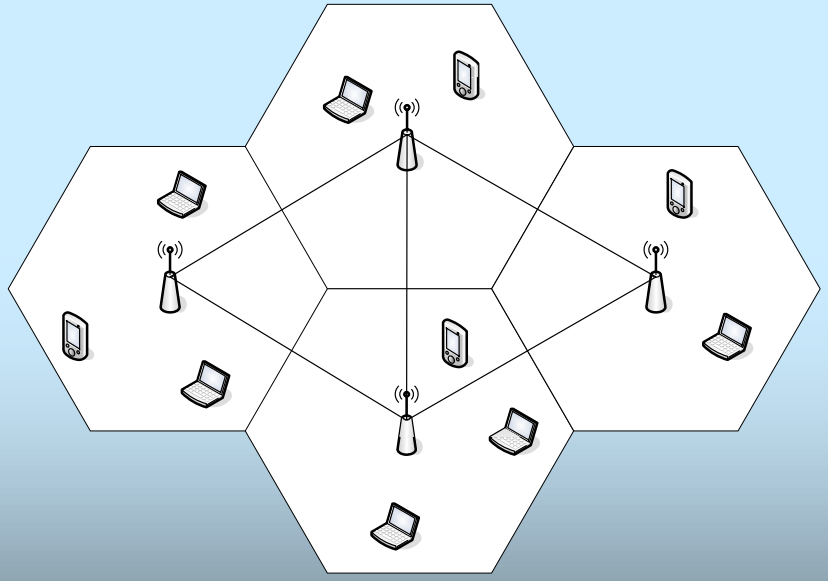
• $T \cup \{move_\lambda \mid \lambda \in L\}$ το σύνολο των υπό συνθήκη μεταβάσεων. Η μετάβαση $move_\lambda$ μεταβάλλει τον παρατηρητή της *τρέχουσας περιοχής (current location)* σε λ.

Κινητά ΠΣΜ

MobileOBJ	
Αλγεβρική Γλώσσα Προδιαγραφών CafeOBJ	
Μαθηματικό υπόβαθρο	Τεχνικές προδιαγραφών και επαλήθευσης
Συμπεριφοριακή Προδιαγραφή Άλγεβρα με κρυμμένους τύπους Συστήματα μετάβασης	Επέκταση των ΠΜΣ στα Κινητά ΠΜΣ Μέθοδος OTS/CafeOBJ Ταυτόχρονη επαγωγή Ιεραρχική σύνθεση αντικειμένων Coinduction

Παράδειγμα εφαρμογής

Περιβάλλον Κινητού Υπολογισμού



Παράδειγμα εφαρμογής

Αλγεβρική Προδιαγραφή

Σχετική Πληροφορία	**Τεμάχια Προδιαγραφών CafeOBJ**
IDs	MHOST-ID, LOC-ID, MSS-ID, MO-ID, RES-ID
Locations	R-LOC, MO-LOC, MH-LOC, MSS-LOC
Queues	QUEUE(MESSAGE) for incoming and outgoing queues of messages
Sets	SET(MHOST-ID), SET(MO-ID), SET(MSS-ID)
Lists	ASSIGN-LIST, REQ-LIST, HOARD-LIST as SET(RESOURCE)
Resources	RES-KIND, RES-VAL, RESOURCE
Messages	MESSAGE

Παράδειγμα εφαρμογής

Αλγεβρική Προδιαγραφή

- Μηνύματα: Τύπος **`Message`**,

Κατασκευαστής: `m : Mhid Mhid Data -> Message`

- Πόροι: Τύπος **`Resource`**

Κατασκευαστής: `r : Rid Rval Rloc Rkind MOid -> Resource`

Παρατηρητές: `op sharable? : Rkind -> Bool`

`op hoardable? : Rkind -> Bool`

Π.χ. `sharable?(printer) = false, sharable(file) = true,`
`hoardable?(memory) = false, hoardable?(file) = true.`

Παράδειγμα εφαρμογής

Αλγεβρική Προδιαγραφή

Δράσεις: `addResHost : Resource Host -> Host` (προσθήκη πόρου σε host)

`addResHL : Resource Mobile -> Mobile` (προσθήκη πόρου στη λίστα αποθηκευμένων πόρων αντικειμένου)

Ορισμός με εξίσωση υπό συνθήκη:

```
ceq hoardedRes(addResHL(R, M)) = R , hoardedRes(M)   if
                                   c-addResHL(R, M) .
```

Παράδειγμα εφαρμογής

Αλγεβρική Προδιαγραφή

• Επικοινωνία: Ασύγχρονη με χρήση θυρίδων επικοινωνίας (στον MSS της home location) για την διάρκεια αποσύνδεσης.

Παράδειγμα εφαρμογής

Αλγεβρική Προδιαγραφή

- Σύστημα: Κινητό ΠΣΜ **SYSTEM**
- Χώρος καταστάσεων: Κρυμμένος τύπος **Sys**
- Ουρές εισερχομένων και εξερχόμενων μηνυμάτων: Παραμετροποιημένη προδιαγραφή **QUEUE (MESSAGE)**
- Σύνολα MH και MSS συστήματος: Παραμετροποιημένη προδιαγραφή **SET (MSS)**, **SET (MH)**
- Αρχική κατάσταση: Κρυμμένη σταθερά **init**
- Χωρικοί παρατηρητές: **loc-mh : Mhid Sys -> Lid, loc-mss : MSSid Sys -> Lid**
- Μέθοδοι αλληλεπίδρασης: **connect : Mhid MSSid Sys -> Sys**

  disconnect : Mhid MSSid Sys -> Sys

Παράδειγμα εφαρμογής

Αλγεβρική Προδιαγραφή

- Δράσεις επικοινωνίας: **send-ss : MSSid MSSid Message Sys -> Sys**
  send-sm : MSSid Mhid Message Sys -> Sys
  post-in-mailbox : Mhid Message Sys -> Sys

Για κάθε δράση δηλώνεται η αποτελεσματική συνθήκη

bop c-action_name : <Parameters> Sys -> Bool

Παράδειγμα εφαρμογής

Αλγεβρική Προδιαγραφή

Αξιώματα (εξισώσεις) προδιαγραφής:

Αριθμός: *(o + 1) * a,* όπου *o*: αριθμός παρατηρήσεων, *a*: αριθμός δράσεων

Δράση disconnect

Αποτελεσματική συνθήκη: `op c-disconnect : Mhid SSid Sys -> Bool`

```
eq c-disconnect(M1, SS1, S) = (M1 \in mobiles-sys(S)) and
                              (M1 \in mobiles-ss(SS1, S)) and
                 connected?(M1, S) and connected-to?(M1, SS1, S) .
```

Παρατήρηση: `ceq mobiles-ss(SS1, disconnect(M2, SS2, S)) =`

```
                        M2 - mobiles-ss(SS1, S) if (SS1 = SS2)
                                        and c-disconnect(M1,SS1,
S) .
```

Παράδειγμα εφαρμογής

Επαλήθευση Ιδιοτήτων Προδιαγραφής

α/α	Ορισμός
1	Σε κάθε πιθανή κατάσταση του συστήματος, εάν ένα κινητό είναι συνδεδεμένο, η θυρίδα μηνυμάτων του είναι άδεια.
2	Σε κάθε πιθανή κατάσταση του συστήματος, ένα κινητό μπορεί να έχει μια και μόνη περιοχή-γονέα.
3	Σε κάθε πιθανή κατάσταση του συστήματος, ένα κινητό μπορεί να βρίσκεται σε μια και μόνη περιοχή
4	Σε κάθε πιθανή κατάσταση του συστήματος, ένα κινητό μπορεί να έχει μια και μόνη εγκατεστημένη θυρίδα σε ένα σταθμό υποστήριξης.
5	Σε κάθε πιθανή κατάσταση του συστήματος, ένα κινητό μπορεί να έχει μια και μόνη ουρά εισερχόμενων μηνυμάτων.
6	Σε κάθε πιθανή κατάσταση του συστήματος, ένα κινητό μπορεί να έχει μια και μόνη ουρά εξερχόμενων μηνυμάτων.
7	Σε κάθε πιθανή κατάσταση του συστήματος, ένας σταθμός υποστήριξης μπορεί να έχει μια και μόνη ουρά εισερχόμενων μηνυμάτων.

Παράδειγμα εφαρμογής

Ιδιότητα 1

```
op inv1 : Sys Mhid SSid -> Bool
eq inv1(S, M1, SS1) = (connected-to?(M1, SS1, S)implies
                        mailbox(M1, SS1, S) = empty) .
```

Επαγωγικό βήμα:

```
op istep1 : Mhid SSid -> Bool
eq istep1(M1, SS1) = inv1(s, M1, SS1) implies
                                  inv1(s',  M1, SS1) .
```

Αρχική κατάσταση:

```
open INV
red inv1(init, m1, ss1) .
close
```

Παράδειγμα εφαρμογής

Απόδειξη με ταυτόχρονη επαγωγή για κάθε δράση

Για την περίπτωση της **connect** διακρίνονται μόνο οι δύο βασικές περιπτώσεις

c-connect και **not c-connect**

```
-- 1) connect(m, ss, s)
-- 1.1) c-connect(m, ss, s)
open ISTEP
-- arbitrary objects
op m : -> Mhid .
op ss : -> SSid .
-- assumptions
-- c-connect(m, ss, s) = true
eq m \in mobiles-sys(s) = true .
eq connected?(m, s) = true .
-- successor state
eq s' =  connect(m, ss, s) .
-- check if the predicate is true.
  red istep1(m1, ss1) .
close
```

```
-- 1.2) not c-connect(m, ss, s)
open ISTEP
-- arbitrary objects
op m : -> Mhid .
op ss : -> SSid .
-- assumptions
eq c-connect(m, ss, s) = false .
-- successor state
eq s' =  connect(m, ss, s) .
-- check if the predicate is true.
  red istep1(m1, ss1) .
close
```

Παράδειγμα εφαρμογής

Απόδειξη με ταυτόχρονη επαγωγή για κάθε δράση

Για την περίπτωση της **send-ss** απαιτείται επιπλέον διάκριση περιπτώσεων αφού η CafeOBJ δεν επιστρέφει true ή false όταν **c- send-ss = true**

```
-- subcase 4.1.1
open ISTEP
-- arbitrary objects
ops ss ss' : -> SSid .
op ms : -> Message .
-- assumptions
-- c-send-ss = true
 eq not(ss = ss') = true .
 eq ss \in sstations(s) = true .
 eq ss' \in sstations(s) = true .
-- subcase1
eq connected-to?(m1,ss1,s) = true .
-- successor state
eq s' =  send-ss(ss, ss', ms, s) .
-- check if the predicate is true.
  red istep1(m1, ss1) .
close
```

```
-- subcase 4.1.2
open ISTEP
-- arbitrary objects
ops ss ss' : -> SSid .
op ms : -> Message .
-- assumptions
-- c-send-ss = true
 eq not(ss = ss') = true .
 eq ss \in sstations(s) = true .
 eq ss' \in sstations(s) = true .
-- subcase2
eq connected-to?(m1,ss1,s) =
false .
-- successor state
eq s' = send-ss(ss, ss', ms, s) .
-- check if the predicate is
true.
  red istep1(m1, ss1) .
close
```

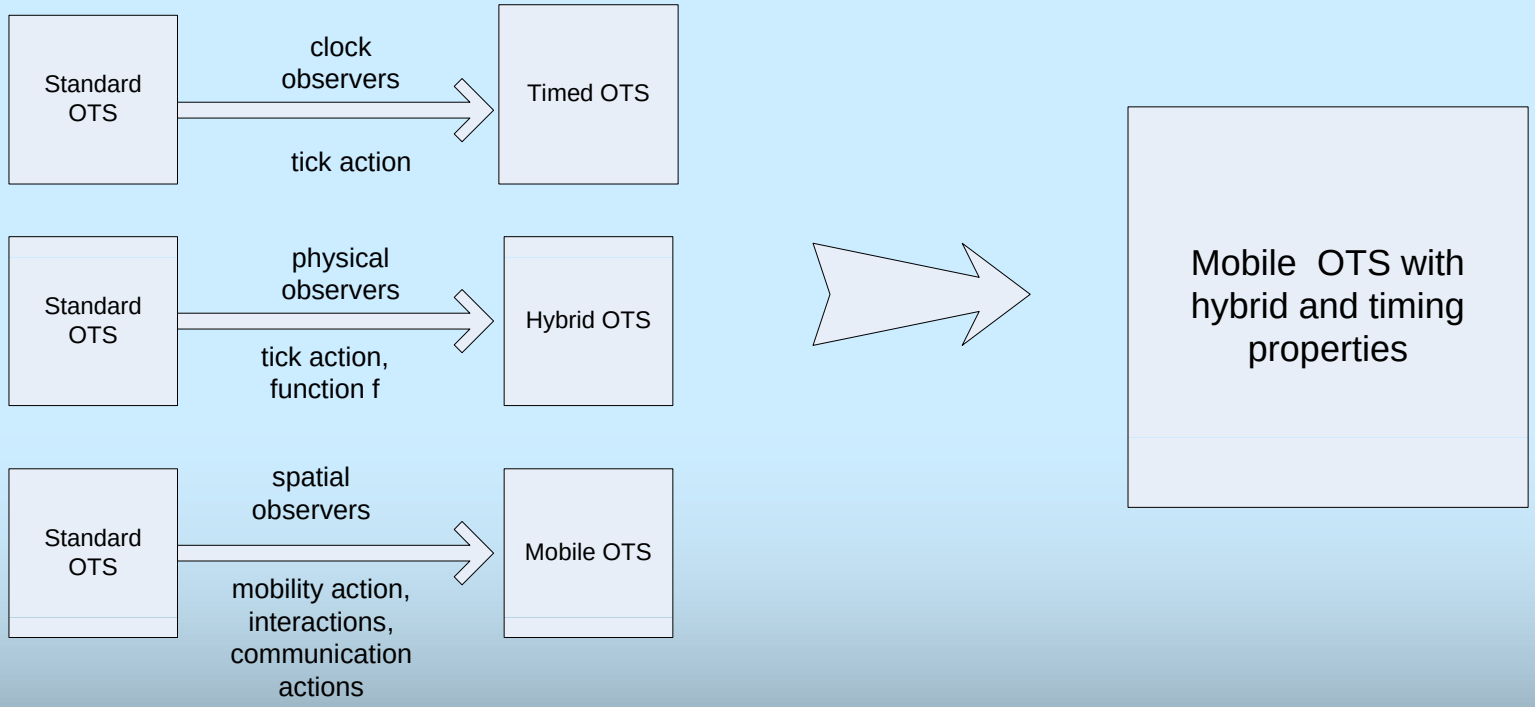
Επέκταση για Χρονικά-Υβριδικά Μοντέλα

Κινητά ΠΣΜ => Διακριτά Χαρακτηριστικά Κινητών Συστημάτων

Για μεγέθη και με συνεχή χαρακτηριστικά (υβριδικά) => Ανάγκη για επέκταση τους

Έχουν προταθεί: Χρονικά ΠΣΜ (για συστήματα πραγματικού χρόνου) και τα Υβριδικά ΠΣΜ (γενικά για υβριδικά συστήματα).

Επέκταση για Χρονικά-Υβριδικά Μοντέλα



Παραδείγματα εφαρμογής

1. Διαδικασία καταχώρησης Κινητού Host στο Mobile IP (για χρονικούς περιορισμούς)

2. Διαπομπή σε σύστημα GSM (για υβριδικά χαρακτηριστικά)

Διαδικασία καταχώρησης του Mobile IP

- Πρωτόκολλο Mobile IP

- Διάρθρωση: Το συνολικό δίκτυο αποτελείται από υποδίκτυα στα οποία υπάρχει ένας δρομολογητής. Ο δρομολογητής είναι ταυτόχρονα και η πύλη επικοινωνίας του υποδικτύου με το διαδίκτυο και έχει το ρόλο του *Home Agent* ή του *Foreign Agent* για τους MHs.

Διαδικασία καταχώρησης του Mobile IP

Σενάριο: Ο MH εισέρχεται σε ένα *foreign network* (διαφορετικό του *home network*). Λαμβάνει μήνυμα advertisement (το οποίο είναι broadcast) από τον Agent του υποδικτύου και στέλνει ένα μήνυμα Registration Request στο HA μέσω του FA με την προσωρινή του διεύθυνση (Care of Address). Ο HA απαντάει με μήνυμα Registration Reply για επικύρωση ή μη της καταχώρησης η οποία είναι έγκυρη για συγκεκριμένο χρονικό διάστημα (απαιτούνται re-registrations).

Διαδικασία καταχώρησης του Mobile IP

Αλγεβρική Προδιαγραφή

Κινητό ΠΣΜ με Χρονικά χαρακτηριστικά

Προδιαγραφή: Σύνολο από modules που προδιαγράφουν τους τύπους δεδομένων και το σύστημα.

Διαδικασία καταχώρησης του Mobile IP

Module Name	Informal Description
SUBNET, NODE	Απλά τεμάχια που ορίζουν τα subnet ids και node ids
ADDRESS	Ορίζει τη διεύθυνση ως ζεύγος των subnet και node. Η διεύθυνση Broadcasting ορίζεται επίσης ως σταθερά. Εισάγει τα SUBNET και NODE σε κατάσταση protecting.
STATUS	Ορίζει την κατάσταση της απάντησης σε μήνυμα καταχώρησης. Λαμβάνει τις τιμές OK εάν έχει επικυρωθεί από τον HA και DENY εάν όχι.
STATE	Η κατάσταση μιας παράκλησης καταχώρησης. Λαμβάνει τις τιμές Confirmed εάν έχει απαντηθεί ή Pending.
TIMEVAL	Τεμάχιο που ορίζει χρονικές τιμές ως μη αρνητικούς θετικούς αριθμούς.
MSG	Ορίζει τα μηνύματα που ανταλλάσσονται από τους agents του συστήματος.
NETWORK	Μοντελοποίηση του internet (backbone of network) ως multiset μηνυμάτων.
SUBNETWORK	Μοντελοποίηση υποδικτύων ως multiset μηνυμάτων.

Διαδικασία καταχώρησης του Mobile IP

Module MSG: Μοντελοποίηση μηνυμάτων διαδικασίας

3 είδη μηνυμάτων – 3 τελεστές CafeOBJ

- `op FaAdv : Address Address -> Msg -- μήνυμα advertisement`

`FaAdv (διεύθυνση αποστολέα, διεύθυνση broadcast υποδικτύου)`

- `op ReqMsg : Address Address Address Address Id -> Msg`

`ReqMsg (διεύθυνση αποστολέα-MH, διεύθυνση παραλήπτη-HA, διεύθυνση home, διεύθυνση CoA, Message Id)`

- `op RepMsg : Address Address Address Status Id  -> Msg`

`RepMsg(διεύθυνση αποστολέα-HA, διεύθυνση παραλήπτη-MH, διεύθυνση home, OK Reply or DENY, Message ID)`

Τελεστές που επιστρέφουν τα ορίσματα των μηνυμάτων και άλλα χρήσιμα χαρακτηριστικά.

Διαδικασία καταχώρησης του Mobile IP

Μοντελοποίηση Δικτύου και Υποδικτύων: Modules NETWORK, SUBNETWORK

ΩΣ ΠΟΛΥΣΥΝΟΛΑ (Multisets) ΜΗΝΥΜΑΤΩΝ

ΑΠΟΣΤΟΛΗ ΜΗΝΥΜΑΤΟΣ – ΠΡΟΣΘΗΚΗ ΣΤΟ ΔΙΚΤΥΟ

ΛΗΨΗ ΜΗΝΥΜΑΤΟΣ – ΑΦΑΙΡΕΣΗ ΑΠΟ ΤΟ ΔΙΚΤΥΟ

ΕΞΑΙΡΕΣΗ: Μηνύματα Broadcast (FaAdv) που αφαιρούνται μόνο μετά την πάροδο προκαθορισμένου χρονικού διαστήματος από τον αποστολέα.

Διαδικασία καταχώρησης του Mobile IP

Κινητό ΠΣΜ **`mip`** με χώρο καταστάσεων του πρωτοκόλλου τον κρυμμένο τύπο **`Sys`**.

3 αντικείμενα: Mobile Host, Home Agent και Foreign Agent

Για κάθε αντικείμενο: Παρατηρητές και Δράσεις που μοντελοποιούν τη συμπεριφορά τους

Διαδικασία καταχώρησης του Mobile IP

Mobile Host

Παρατηρητές: *home-addr*, *care-addr*, *gotflag*?, *confirmed*?

Δράσεις: *RcvFaAdv, SndReq, ReSndReq, ReRegister, RcvRep*

Foreign Agent

Παρατηρητές: *visitors*, *state*
Δράσεις: *SndFaAdv, RmvFaAdv, RecRegReq, FwdRegReq, RcvRegRep, FwdRegRep*

Home Agent

Παρατηρητές: *ha-mobiles, fwd-addr*
Δράσεις: *HaRcvReq*, *HaSndRep*

Διαδικασία καταχώρησης του Mobile IP

Άλλοι διακριτοί παρατηρητές

nw, *subnw*, *uids*

Χρονικοί τελεστές

Δράση: $tick_r$

Παρατηρητές: *now (master clock) + χρονικά όρια + καθυστερήσεις*

Για κάθε δράση: Άνω + Κάτω χρονικό όριο, Άνω + Κάτω καθυστέρηση

Όταν κάτω όριο = 0 ή άνω όριο = οο μπορεί να παραληφθεί

Διαδικασία καταχώρησης του Mobile IP

Θεωρείται:

• Δράση *ReSndReq* (επαν-αποστολή αίτησης καταχώρησης) ενεργοποιείται *d1* χρονικές μονάδες το λιγότερο μετά την τελευταία αποστολή.

• Δράση *ReRegister* (επανεκκίνηση διαδικασίας καταχώρησης) ενεργοποιείται *d2* χρονικές μονάδες το λιγότερο μετά την τελευταία καταχώρηση.

• Δράση *RmvFaAdv* (απόσυρση μηνύματος advertisement) πραγματοποιείται κάθε *d3* χρονικές μονάδες.

Διαδικασία καταχώρησης του Mobile IP

Για κάθε δράση: Ορισμός Αποτελεσματικής συνθήκης + εξισώσεις μεταβολής παρατηρητών όταν εφαρμόζεται η δράση.

Π.χ. Για τη δράση **RmvFaAdv**

- Ορισμός αποτελεσματικής συνθήκης

```
op c-RmvFaAdv : Sys Msg -> Bool
eq c-RmvFaAdv(S, M1) = fa-adv?(M1) and M1 \in subnw(S,
subnet(src-addr(M1))) and l3(S) <= now(s) and now(S) <=
u3(S) .
```

- Παρατηρητές που αλλάζουν τιμή όταν εφαρμόζεται η δράση

```
-- παρατηρητής του υποδικτύου
ceq subnw(RmvFaAdv(S, M1), subnet(src-addr(M1))) = subnw(S,
subnet(src-addr(M1))) - M1 if c-RmvFaAdv(S, M1) .
```

Διαδικασία καταχώρησης του Mobile IP

```
-- χρονικοί παρατηρητές
ceq l3(RmvFaAdv(S, M1)) = now(S) + d3 if c-RmvFaAdv(S,M1) .
ceq u3(RmvFaAdv(S, M1)) = now(S) + d3 if c-RmvFaAdv(S, M1) .
```

Οι υπόλοιποι παρατηρητές παραμένουν αμετάβλητοι

Για τη δράση **RcvRegReq**

• Ορισμός αποτελεσματικής συνθήκης

```
op c-RcvRegReq : Sys Address Msg -> Bool
eq c-RcvRegReq(S, A1, M1) = M1 \in subnw(S, subnet(A1)) and
req-m?(M1) .
```

• Παρατηρητές που αλλάζουν τιμή όταν εφαρμόζεται η δράση

```
-- παρατηρητής του υποδικτύου
ceq subnw(RcvRegReq(S, A1, M1) , subnet(A1)) = subnw(S,
      subnet(A1)) - M1 if c-RcvRegReq(S, A1, M1) .
```

Διαδικασία καταχώρησης του Mobile IP

```
-- παρατηρητές για τον κινητό κόμβο
ceq care-addr(RcvRegReq(S, A1, M1), A2) = req-coa(M1) if c-
RcvRegReq(S, A1, M1) .

-- παρατηρητές για τον FA
ceq visitors(RcvRegReq(S, A1, M1), subnet(A1)) = req-ha(M1)
, visitors(S, subnet(A1)) if c-RcvRegReq(S, A1, M1) .

ceq state(RcvRegReq(S, A1, M1), A2) = Pending if c-
RcvRegReq(S, A1, M1) and src-addr(M1) = A2 .
```

Οι υπόλοιποι παρατηρητές παραμένουν αμετάβλητοι

Διαδικασία καταχώρησης του Mobile IP

Τυπική επαλήθευση ιδιοτήτων

Απόδειξη ιδιοτήτων ασφαλείας ως αμετάβλητα κατηγορήματα κατάστασης (invariants)

α/α	Ορισμός
1	Σε κάθε πιθανή κατάσταση του συστήματος της διαδικασίας καταχώρησης, εάν ένα μήνυμα advertisement υπάρχει σε ένα υποδίκτυο, τότε ένα κινητό που βρίσκεται σε αυτό θα το έχει παραλάβει.
2	Σε κάθε πιθανή κατάσταση του συστήματος της διαδικασίας καταχώρησης, εάν ένα μήνυμα που εστάλη σε απάντηση ενός μηνύματος μιας αίτησης καταχώρησης υπάρχει στο δίκτυο και η κατάσταση του είναι OK, τότε η διεύθυνση του κινητού που έκανε την αίτηση έχει προστεθεί στο σύνολο των κινητών μακριά από το home network και η διεύθυνση προώθησης των μηνυμάτων του στον home agent έχει τεθεί στη διεύθυνση COA που ζητήθηκε.

Διαδικασία καταχώρησης του Mobile IP

Απόδειξη ιδιότητας 1

1. Ορισμός στην CafeOBJ στο module INV

```
op inv1 : Sys Address Msg -> Bool
   eq inv1(S, A1, M1) = M1 \in subnw(S, subnet(src-
   addr(M1))) and fa-adv?(M1) implies gotflag?(S, A1, M1) .
```

Όταν ένα μήνυμα τύπου advertisement (**`fa-adv?(M1) = true`**) υπάρχει στο υποδίκτυο (**`M1 \in subnw(S, subnet(src-addr(M1))) and fa-adv?(M1)`**) τότε η μεταβλητή **`gotflag`** του κινητού host με διεύθυνση **`A1`** για το μήνυμα αυτό είναι true, δηλαδή έχει παραληφθεί.

2. Επαγωγικό βήμα στο module ISTEP

```
op istep1 : Address Msg -> Bool
   eq istep1(A1, M1) = inv1(s, A1, M1) implies
                                        inv1(s', A1, M1) .
```

Διαδικασία καταχώρησης του Mobile IP

Απόδειξη ιδιότητας 1

3. Απόδειξη για κάθε αρχική κατάσταση, έστω **`init`**

```
-- for the first invariant
   open INV
   red inv1(init, a1, m1) .
   close
```

4. Proof scores για κάθε δράση και ανάλογα με την επιστροφή του συστήματος της CafeOBJ επιπλέον διάκριση περιπτώσεων ή/και χρήση λημμάτων

Διαδικασία καταχώρησης του Mobile IP

Για την δράση **RcvRep**

```
open ISTEP
-- arbitrary objects
ops m10 m100 : -> Msg .
op a10 : -> Address .
op subnw10 : -> SubNetwork .
-- assumptions
   --  c-RcvRep(s, a10, m10, m100) = true .
eq subnw(s, subnet(a10)) = m10, subnw10 .
eq rep-m?(m10) = true .
eq req-m?(m100) = true .
eq rep-id(m10) = req-id(m100) .
-- further case splitting
eq gotflag?(RcvRep(s,a10,m10,m100),a1,m1) =
true .
-- successor state
eq s' = RcvRep(s, a10, m10, m100) .
-- check if the predicate holds
red istep1(a1, m1) .
close
```

Διαδικασία καταχώρησης του Mobile IP

Για την δράση **ReSndReq**

```
open ISTEP
-- arbitrary objects
ops m10 m100 : -> Msg .
ops a10 a100 : -> Address .
op subnw10 : -> SubNetwork .
op i10 : -> Id .
-- assumptions
   --  c-ReSndReq(s, a10, a100, i10, m10, m100) .
eq subnw(s, subnet(src-addr(m10))) = m10, subnw10 .
eq fa-adv?(m10) = true .
eq (gotflag?(s, a10 , m10)) = false .
eq a100 = src-addr(m10) .
eq i10 \in uids(s) = false .
eq c-RcvRep(s, a10, m10, m100) = false .
eq (l1(s) <= now(s)) = true .
--
-- successor state
eq s' = ReSndReq(s, a10, a100, i10, m10, m100) .
-- check if the predicate holds
red inv1(s, a10, m10) implies istep1(a1, m1) .
close
```

Διαπομπή σε σύστημα GSM

Περιγραφή συστήματος

Το σύστημα αποτελείται από δύο κυψέλες η καθεμία από τις οποίες ελέγχεται από ένα σταθμό βάσης BS1 και BS2 αντίστοιχα. Το σύστημα ελέγχεται από το Κέντρο Ελέγχου CC που μπορεί να γνωρίζει τη θέση των κινητών. Η κάθε κυψέλη θεωρείται κυκλική, το κινητό μετακινείται κατά μήκος της ακτίνας της με σταθερή ταχύτητα, και ο χώρος θεωρείται δύο διαστάσεων. Η BS1 βρίσκεται στην αρχή των αξόνων (0,0) και το κινητό έχει συντεταγμένες (x,y). Οπότε η απόσταση του κινητού σε συνάρτηση με το χρόνο είναι μια συνεχής συνάρτηση $d = c * t$.

Διαπομπή σε σύστημα GSM

Απλή διαπομπή

Όταν ο CC αντιληφθεί ότι ένα κινητό πλησιάζει μια νέα κυψέλη που ελέγχεται από τον BS2 ξεκινάει τη διαδικασία μεταγωγής των συνδέσεων:

1. Ο CC στέλνει ένα μήνυμα *release* στον παλιό σταθμό βάσης (BS1) και ένα μήνυμα *alert* στο νέο (BS2).

2. Ο BS1 μόλις λάβει το μήνυμα release στέλνει ένα μήνυμα *switch* στο κινητό με το id του νέου σταθμού βάσης.

3. Ο BS2 μόλις λάβει το μήνυμα alert αποθηκεύει το αναγνωριστικό του νέου κινητού.

Διαπομπή σε σύστημα GSM

Μοντελοποίηση

Κινητό ΠΣΜ με συνεχές μέγεθος την απόσταση ανάμεσα στο κινητό και το BS1.

Διαπομπή: Πρέπει να έχει ολοκληρωθεί όταν το κινητό φθάσει στα όρια της κυψέλης => δράσεις λαμβάνουν άνω και κάτω όρια απόστασης.

Διαπομπή σε σύστημα GSM

Αλγεβρική Προδιαγραφή

Βασικοί τύποι δεδομένων:

• Μηνύματα (τύπος **Msg**)

```
op release : Control Point Mid -> Msg
op alert : Control Point Mid -> Msg
op switch : Point Mid Point -> Msg
```

• Δίκτυο (τύπος **Network**) ως πολυσύνολο μηνυμάτων

• Συντεταγμένες - σημείο - απόσταση σημείων (τύπος **Point**)

Κινητό ΠΣΜ: module **SYSTEM**, χώρος καταστάσεων τύπος **Sys**

Διαπομπή σε σύστημα GSM

Δράσεις

Αν **C** -> τύπος συντεταγμένων CC, **P** -> τύπος συντεταγμένων BS, **M** -> τύπος συντεταγμένων κινητού, **MS** -> τύπος μηνύματος, και **S** -> τύπος **Sys**:

- **SndRel : S C P M -> S** δηλώνει ότι το κέντρο ελέγχου **C** τοποθετεί ένα μήνυμα **release** στο δίκτυο για το σταθμό βάσης **BS1** με συντεταγμένες **P** για το κινητό **M**.

- **RcvRel : S P MS -> S** δηλώνει ότι ο σταθμός βάσης **BS1** με συντεταγμένες **P** λαμβάνει ένα μήνυμα **release MS** από το δίκτυο.

- **SndAlert : S C P M -> S** δηλώνει ότι το κέντρο ελέγχου **C** τοποθετεί ένα μήνυμα **alert** στο δίκτυο για το σταθμό βάσης **BS2** με συντεταγμένες **P** για το κινητό **M**.

Διαπομπή σε σύστημα GSM

Δράσεις

-**RcvAlert : S P MS -> S** δηλώνει ότι ο σταθμός βάσης **BS2** με συντεταγμένες **P** λαμβάνει το μήνυμα **alert**.

-**SndSwitch : S M P MS -> S** δηλώνει ότι ο σταθμός βάσης **BS1** με συντεταγμένες **P,** μετά τη λήψη του μηνύματος **release** τοποθετεί ένα μήνυμα **switch** στο δίκτυο για το κινητό **M**.

- **RcvSwitch : S M MS -> S** δηλώνει ότι το κινητό **M** αποσύρει από το δίκτυο

ένα μήνυμα **switch** .

- **tick : S R -> S** αυξάνει το master clock κατά **R**

Διαπομπή σε σύστημα GSM

Περιορισμοί απόστασης

Απόσταση: Θετικός πραγματικός αριθμός

Rmax : Ακτίνα κυψέλης BS1 – η διαπομπή θα πρέπει να έχει ολοκληρωθεί

SndRel [d1 d2]

RcvRel [d1′ d2′]

SndAlert [d3 d4]

RcvAlert [d3′ d4′]

SndSwitch [d5 d6]

RcvSwitch [d5′ Rmax]

Διαπομπή σε σύστημα GSM

Παρατηρητές

Διακριτοί:

$time_s$: επιστρέφει την τελευταία χρονική στιγμή στην οποία εφαρμόσθηκε μια δράση στην κατάσταση s. Αρχικά επιστρέφει 0.

$value_s$: επιστρέφει την απόσταση τη χρονική στιγμή που επιστρέφεται από τον παρατηρητή $time_s$. Αρχικά επιστρέφει 0.

nw_s: επιστρέφει το δίκτυο στην κατάσταση s. Αρχικά επιστρέφει το κενό σύνολο, δηλαδή στο δίκτυο δεν υπάρχουν μηνύματα.

$base_{s,m}$: επιστρέφει το σταθμό βάσης με τον οποίο το κινητό m είναι συνδεδεμένο στην κατάσταση s.

Διαπομπή σε σύστημα GSM

Παρατηρητές

Φυσικοί:

$distance_{s,m,p}$: επιστρέφει την απόσταση ανάμεσα σε ένα κινητό m και το σταθμό βάσης με συντεταγμένες p.

now_s: επιστρέφει την ώρα του συστήματος. Αρχικά επιστρέφει 0.

$f\text{-}dist_\tau$: συνάρτηση που επιστρέφει την απόσταση ανάμεσα στο σταθμό βάσης BS1 και ένα κινητό τη χρονική στιγμή τ.

Διαπομπή σε σύστημα GSM

Σύνολο οκτώ εξισώσεων για κάθε δράση

-Για την **RcvRel**

```
  op c-RcvRel : Sys Point Msg -> Bool
  eq c-RcvRel(S, P, MS) = MS \in nw(S) and release?(MS) and
dst(MS) = P and   d1' <= distance(S, data(MS), BS1) and
distance(S, data(MS), BS1) <= d2' .
  --
  ceq time(RcvRel(S, P, MS)) = now(S) if c-RcvRel(S, P, MS) .
  ceq value(RcvRel(S, P, MS)) = distance(S, data(MS), P) if
  c-RcvRel(S, P, MS) .
  ceq nw(RcvRel(S, P, MS)) = nw(S) - MS if c-RcvRel(S, P, MS) .
  eq base(RcvRel(S, P, MS), M') = base(S, M') .
  eq distance(RcvRel(S, P, MS), M, P') = distance(S, M, P') .
  eq now(RcvRel(S, P, MS)) = now(S) .
  ceq RcvRel(S, P, MS) = S if not c-RcvRel(S, P, MS) .
```

Διαπομπή σε σύστημα GSM

Σύνολο οκτώ εξισώσεων για κάθε δράση

- Για την **tick**

```
op c-tick : Sys Real+ -> Bool
eq c-tick(S, D) = (( value(S) + f-dist((now(S) + D) -
time(S)) ) <= Rmax) .
eq time(tick(S, D)) = time(S) .
eq value(tick(S, D)) = value(S) .
eq nw(tick(S, D)) = nw(S) .
eq base(tick(S, D), M) = base(S, M) .
ceq distance(tick(S, D), M, P) = value(S) + f-
dist((now(S) + D) - time(S)) if c-tick(S, D) .
ceq now(tick(S, D)) = now(S) + D if c-tick(S, D) .
ceq tick(S, D) = S if not c-tick(S, D) .
```

Διαπομπή σε σύστημα GSM

Επαλήθευση

Οι ιδιότητες της προδιαγραφής που επαληθεύθηκαν είναι:

α/α	**Ορισμός**
1	Σε κάθε πιθανή κατάσταση του συστήματος η διαδικασία διαπομπής θα έχει ολοκληρωθεί πριν το κινητό φθάσει στο όριο της κυψέλης.
2	Σε κάθε πιθανή κατάσταση του συστήματος, εάν η απόσταση ανάμεσα στο σταθμό βάσης BS1 και το κινητό είναι μικρότερη ή ίση με D μονάδες απόστασης, τότε το ρολόι του συστήματος θα δείχνει D ή μικρότερες χρονικές μονάδες.

Διαπομπή σε σύστημα GSM

Επαλήθευση

Οι ιδιότητες εκφράσθηκαν ως εξής:

invariant*(S, M, MS):* Για κάθε κατάσταση S, κινητό M and μήνυμα MS, εάν το MS είναι ένα μήνυμα *switch* και υπάρχει στο δίκτυο, και ο προορισμός του είναι το κινητό M, τότε η απόσταση ανάμεσα στο σταθμό βάσης BS1 και το M είναι μικρότερη από την ακτίνα της κυψέλης.

```
eq inv(S, M, MS) = MS \in nw(S) and switch?(MS) and dst-
sw(MS) = M implies distance(S, M, BS1) <= Rmax .
```

Διαπομπή σε σύστημα GSM

Επαλήθευση

invariant*(S, M, D):* Για κάθε κατάσταση S, κινητό M και θετικό πραγματικό αριθμό D, εάν η απόσταση ανάμεσα στο σταθμό βάσης BS1 και το κινητό M είναι μικρότερη από D, τότε το ρολόι του συστήματος δείχνει ότι έχει περάσει χρόνος μικρότερος από D χρονικές μονάδες .

```
eq inv (S, M, D) =  (distance(S, M, BS1) <= D implies
now(S) <= D) .
```

3. Τυπική ανάλυση πρωτοκόλλων ασφαλείας

Πρωτόκολλα Ασφαλείας και CafeOBJ

Πρωτόκολλα ασφαλείας: Αξιοπιστία και σωστή σχεδίαση

Εφαρμογή της μεθόδου σε πρωτόκολλα ασφαλείας για επαλήθευση ιδιοτήτων ασφαλείας.

SPINS protocol suite, TESLA protocol

Πρωτόκολλα Ασφαλείας και CafeOBJ

Βασικές παραδοχές

- το σύστημα κρυπτογράφησης είναι ασφαλές (δηλ. για να αποκρυπτογραφήσει κάποιος κρυπτοκείμενα πρέπει να έχει το αντίστοιχο κλειδί).
- στο σύστημα υπάρχουν και κακόβουλοι χρήστες που δεν ακολουθούν το πρωτόκολλο. Ακολουθείται το μοντέλο του γενικού εισβολέας των Dolev – Yao, όπου ο εισβολέας μπορεί:
  1. Να συλλέξει μηνύματα που έχουν τοποθετηθεί στο δίκτυο και να ανακτήσει πληροφορία από αυτά,
  2. Να τοποθετήσει μηνύματα στο δίκτυο με βάση την πληροφορία που έχει υποκλέψει.

1. SPINS Protocol Suite

SPINS Protocols

- Πρωτόκολλα SPINS
- Αρχές συμμετρικής κρυπτογραφίας
- SNEP (Secure Network Encryption Protocol) και πρωτόκολλο συμφωνίας κλειδιού δύο πλευρών
- Για πρώτη φορά επαληθεύονται με τυπικές μεθόδους

SPINS Protocols

SNEP

Μήνυμα 1. $A \rightarrow B : \mathrm{N_A}$

Μήνυμα 2. $B \rightarrow A : \{ B \}_{<Kenc,\ C>}, MAC(K_{mac}, N_A \mid C \mid \{ B \}_{<Kenc,\ C>})$

SPINS Protocols

SNEP: Αλγεβρική Μοντελοποίηση

• Παραδοχές: Εκτός από τις βασικές, υποθέτουμε επίσης ότι τα κλειδιά K_{mac} και K_{enc} είναι ίδια και ότι υπάρχει ένας αυθαίρετος αριθμός αξιόπιστων κόμβων

• Μοντελοποίηση μηνυμάτων

Μήνυμα 2. $A \rightarrow B : \{ B \}_{<Kenc,\ C>}, MAC(K_{mac}, N_A \mid C \mid \{ B \}_{<Kenc,\ C>})$

```
op m2 : Node Node Node Cipher Mac -> Msg
```

Υποθέτουμε ότι το μήνυμα **`m2 (n1, n2, n3, ci, mc)`** βρίσκεται στο δίκτυο:

- ο **`n1`** έχει αποστείλει το μήνυμα στον **`n3`**

- Εάν το **`n2`** είναι διαφορετικό από το **`n1`**, ο **`n1`** είναι κακόβουλος κόμβος και το μήνυμα είναι πλαστό

  - Εάν ο **`n3`** λάβει το μήνυμα, απλά πιστεύει ότι το μήνυμα έχει σταλεί από τον **`n2`**, χωρίς να μπορεί να είναι σίγουρος ότι αυτό αληθεύει.

SPINS Protocols

SNEP: Αλγεβρική Μοντελοποίηση

- Μοντελοποίηση δικτύου

- Το δίκτυο μοντελοποιείται ως πολυσύνολο μηνυμάτων

- Δεδομένου του δικτύου μπορούν να βρεθούν τα δεδομένα που είναι διαθέσιμα στον κακόβουλο κόμβο

Υποθέτουμε ότι το μήνυμα τύπου 2 βρίσκεται στο δίκτυο:

$$\{ B \}_{<Kenc,\ C>},\ MAC(K_{mac},\ N_A \mid C \mid \{ B \}_{<Kenc,\ C>})$$

Τα δεδομένα που είναι διαθέσιμα στον εισβολέα είναι:

- τα δύο κρυπτοκείμενα

- το αναγνωριστικό του B εάν τα K_{enc} και C είναι διαθέσιμα

- το $N_A \mid C \mid \{B\}_{<Kenc,C>}$ εάν το K_{mac} είναι διαθέσιμο

SPINS Protocols

SNEP: Αλγεβρική Μοντελοποίηση

- Μοντελοποίηση αξιόπιστων κόμβων

Η συμπεριφορά τους μοντελοποιείται από δύο κανόνες μετάβασης:

Δράση sdm2 (αποστολή μηνύματος τύπου 2)

```
bop sdm2 : Snep Node Msg -> Snep
```

Αποτελεσματική συνθήκη: Ένα μήνυμα τύπου **m1** υπάρχει στο δίκτυο

Μετάβαση: Το μήνυμα

```
(m2(P1, P1, src(M1), enc(k(P1), c(P1), P1), mac(kmac(P1),
      n(M1), c(P1), enc(k(P1), c(P1),P1))), nw(S))
```

εισάγεται στο δίκτυο

SPINS Protocols

SNEP: Αλγεβρική Μοντελοποίηση

- Μοντελοποίηση εισβολέα

Η συμπεριφορά τους μοντελοποιείται από τέσσερις κανόνες μετάβασης:

Π.χ. : Η δημιουργία και αποστολή ενός πλαστού μηνύματος τύπου m2 με χρήση ενός κρυπτογραφημένου node ID και ενός MAC ορίζεται ως εξής:

```
bop fkm21 : Snep Node Node Cipher Mac -> Snep
```

Αποτελεσματική συνθήκη: Τα κρυπτοκείμενα είναι διαθέσιμα στον εισβολέα (ως μέρος παλαιότερου μηνύματος)

Μετάβαση: Το μήνυμα `(m2(enemy, P1, P2, CI, M),nw(S))` τοποθετείται στο δίκτυο. Η σταθερή `enemy` δηλώνει τον κακόβουλο κόμβο-εισβολέα.

SPINS Protocols

SNEP: Αλγεβρική Μοντελοποίηση

- Μοντελοποίηση εισβολέα

Εξισώσεις που ορίζουν την **fkm21**

```
-- for action fkm21

op c-fkm21 : Snep Node Node Cipher Mac -> Bool
eq c-fkm21(S, P1, P2, CI, M) = (CI \in ciphers(nw(S)) and
M \in macs(nw(S))) .

ceq nw(fkm21(S, P1, P2, CI, M)) = (m2(enemy, P1, P2, CI,
M),nw(S)) if c-fkm21(S, P1, P2, CI, M) .
eq ur(fkm21(S, P1, P2, CI, M)) = ur(S) .
ceq fkm21(S, P1, P2, CI, M) = S if not
                                  c-fkm21(S,P1,P2,CI,M) .
```

SPINS Protocols

SNEP: Επαλήθευση Ιδιότητας

Authentication property (Ιδιότητα ασφάλειας): Οποτεδήποτε ο κόμβος Α παραλάβει ένα έγκυρο μήνυμα *m2* από τον κόμβο Β, ο Β θα είναι ένας αξιόπιστος κόμβος.

Η ιδιότητα ορίζεται με όρους της προδιαγραφής ως εξής:

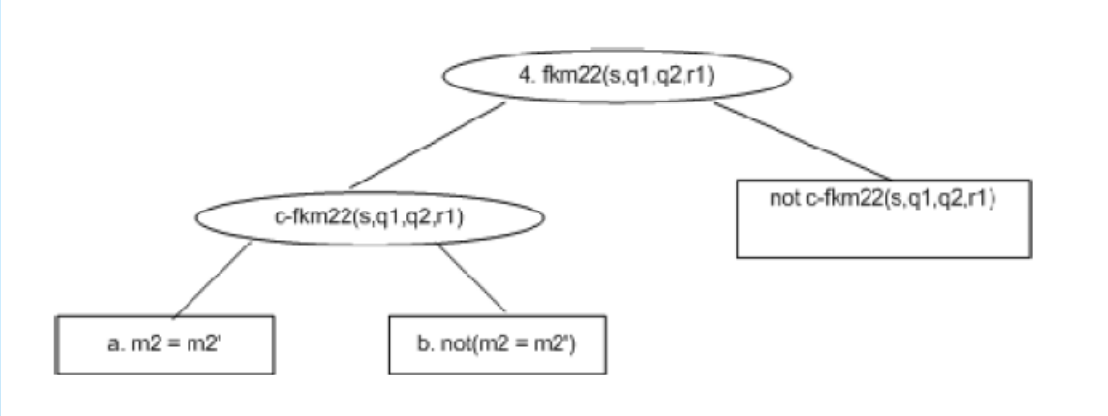
Για κάθε δυνατή κατάσταση s, κόμβους αισθητήρων n1, n2, n3, κλειδί k, κλειδί mac k', nonce n και μετρητή c,

***invariant*((not(k = k(enemy)) and not(k'=kmac(enemy)) and not(c=c(enemy)) and not(creator(n) = enemy) and (m2(p1,p2,p3,enc(k,c,p2), mac(k',n,c,enc(k,c,p2))) \in nw(s))) implies not(p2 = enemy)).**

SPINS Protocols

SNEP: Επαλήθευση Ιδιότητας

Πλάνο απόδειξης για την δράση **`fkm22`**



Για κάθε τετράγωνο γράφεται το αντίστοιχο proof score.

SPINS Protocols

SNEP: Επαλήθευση Ιδιότητας

Για την υπό-περίπτωση *m2 = m2'* το proof score είναι:

```
open ISTEP
-- arbitrary objects
ops q1 q2 : -> Node .
op r1 : -> Rand .
-- assumptions
-- c-fkm22(s, p1, p2, r1) = true .
eq r1 \in ur(s) = true .
eq (m2(p1,p2,p3,enc(k,c,p2),mac(k',n,c,enc(k,c,p2))) =
m2(enemy,q1,q2,enc(k(q1),c(q1),q1),mac(kmac(q1),n(q1,q2,r1),c(q
1),enc(k(q1),c(q1),q1)))) = false .
-- successor state
eq s' = fkm22(s, q1, q2, r1) .
-- check if the predicate is true.
red istep1(p1,p2,p3,k,k',n,c) .
close
```

SPINS Protocols

Πρωτόκολλο συμφωνίας κλειδιών

Έναρξη ασφαλούς σύνδεσης μεταξύ δύο κόμβων– εγκατάσταση συμμετρικών κλειδιών

Έμπιστος agent: Σταθμός βάσης

Μήνυμα 1. $A \rightarrow B : N_A, A$
Μήνυμα 2. $B \rightarrow S : N_A, N_B, A, B, MAC(K_{BS}, N_A \mid N_B \mid A \mid B)$
Μήνυμα 3. $S \rightarrow A : \{SK_{AB}\}K_{AS}, MAC(K_{AS}, N_A \mid B \mid \{SK_{AB}\}K_{AS})$
Μήνυμα 4. $S \rightarrow B : \{SK_{AB}\}K_{BS}, MAC(K_{BS}, N_B \mid A \mid \{SK_{AB}\}K_{BS})$

SPINS Protocols

Αλγεβρική Προδιαγραφή

Ακολουθήθηκε η ίδια μεθοδολογία μοντελοποίησης

- 4 είδη μηνυμάτων (**`m1, m2, m3, m4`**)
- Agents συστήματος: Κόμβοι αισθητήρων (**`Node`**) + σταθμός βάσης (**`Base`**), 4 δράσεις που τους μοντελοποιούν
- Υπάρχουν επίσης κακόβουλοι κόμβοι (**`enemy`**) + σταθμός βάσης (**`ibase`**), 12 δράσεις

SPINS Protocols

Επαλήθευση

Ιδιότητα Συμφωνίας Κλειδιών: Οποτεδήποτε ένας κόμβος *A (B)* λάβει από το σταθμό βάσης ένα έγκυρο μήνυμα *m3 (m4)*, τότε το κλειδί της συνόδου που περιέχεται σε αυτό θα είναι πάντα έγκυρο.

Η ιδιότητα γράφεται ως invariant:

Σε κάθε δυνατή κατάσταση του συστήματος s, σταθμούς βάσης b1, b2, κόμβους αισθητήρων n1, n2, κλειδιά bk, nk και τυχαίο αριθμό r,

invariant (not(n(bk) = enemy)) and (not(b(bk) = ibase)) and (m3(b1,b2,n1,enc(bk, nk), mac2(bk, n(n1, r), n2, enc(bk, nk))) \in nw(S)) implies not (b2 = ibase) .

Και αποδεικνύεται με ταυτόχρονη επαγωγή για κάθε τελεστή δράσης.

2. TESLA Protocol

TESLA Protocol

- Πρωτόκολλο εξακρίβωσης ταυτότητας (authentication) για συστήματα multicast ή/και broadcast.
- Χρήση αρχών συμμετρικής κρυπτογραφίας – εξοικονόμηση πόρων
- Χρονικά χαρακτηριστικά
- Χρήση MAC, Ψευδοτυχαίων συναρτήσεων για την παροχή δεσμεύσεων (commitments) κλειδιών.

TESLA Protocol

- Λόγω χρήσης χρόνου: Το πρωτόκολλο μοντελοποιείται ως Χρονικό ΠΣΜ.
- Ο χώρος καταστάσεων: Κρυμμένος τύπος `Tesla`
- 2 διακριτοί παρατηρητές, 5 χρονικοί παρατηρητές, 12 δράσεις

TESLA Protocol

$\mathcal{O}_{TESLA} \triangleq \{\text{nw} : Y \rightarrow \text{Network}, \text{ur} : Y \rightarrow \text{URands}, \text{now} : Y \rightarrow \text{Timeval},$

$\text{fkl} : Y \rightarrow \text{Timeval}, \text{fku} : Y \rightarrow \text{Timeval}, \text{sdl} : Y \rightarrow \text{Timeval}, \text{sdu} : Y \rightarrow \text{Timeval} \}$

$\mathcal{I}_{TESLA} \triangleq \{v_{\text{init}} \in Y \mid \text{nw}(v_{\text{init}}) = \text{void}, \text{ur}(v_{\text{init}}) = \text{empty}, \text{now}(v_{\text{init}}) = 0, \text{sdl}(v_{\text{init}}) = 0,$

$\text{sdu}(v_{\text{init}}) = 0, \text{fkl}(v_{\text{init}}) = 0, \text{fku}(v_{\text{init}}) = \text{oo}\}$

$\mathcal{T}_{TESLA} \triangleq \{\text{sdim}_{\text{a:Agent, b:Agent, r:Rand}} : Y \rightarrow Y, \text{sdrm}_{\text{a:Agent, r:Rand,m:Msg}} : Y \rightarrow Y,$

$\text{sdm1}_{\text{a:Agent, n:Nat}} : Y \rightarrow Y, \text{sdmn}_{\text{a:Agent, n:Nat}} : Y \rightarrow Y,$

$\text{fkim}_{\text{a:Agent, b:Agent, r:Rand}} : Y \rightarrow Y, \text{fkrm1}_{\text{a:Agent, b:Agent, c:Cipher}} : Y \rightarrow Y,$

$\text{fkrm2}_{\text{a:Agent, b:Agent, r:Rand}} : Y \rightarrow Y, \text{fkrm3}_{\text{a:Agent, b:Agent, n:Nonce}} : Y \rightarrow Y,$

$\text{fkm11}_{\text{a:Agent, b:Agent, p:Prf,mc1:Mac1}} : Y \rightarrow Y, \text{fkm12}_{\text{a:Agent, b:Agent,n:Nat}} : Y \rightarrow Y,$

$\text{fkmn1}_{\text{a:Agent, b:Agent, p:Prf,mc2:Mac2,k:Key,i:Nat}} : Y \rightarrow Y,$

$\text{fkmn2}_{\text{a:Agent, b:Agent, i:Nat}} : Y \rightarrow Y, \text{tick}_{\text{n:Nat}} : Y \rightarrow Y \}$

TESLA Protocol

- Επαλήθευση ιδιότητας πρωτοκόλλου

Ιδιότητα ορθότητας TESLA. *Σε κάθε κατάσταση του πρωτοκόλλου, εάν ένα κλειδί μπορεί να αποκτηθεί από ένα κακόβουλο χρήστη, τότε το κλειδί είτε ανήκει σε αυτόν, είτε έχει αποκαλυφθεί ως μέρος ενός μηνύματος.*

```
inv1(T, K) = K \in keys(nw(T)) implies p(K) = enemy or (s s
i(K))*d1 <= now(T) .
```

Για την απόδειξη απαιτήθηκε και η χρήση της ως λήμμα (χαρακτηριστικό μεθόδου)

4. Άλγεβρα – Σύνθεση Πρωτοκόλλων

Άλγεβρα - Σύνθεση Πρωτοκόλλων

Χρήση τυπικών μεθόδων (συμπεριφοριακής αλγεβρικής προδιαγραφής) για ανάπτυξη πρωτοκόλλων

- Αντικειμενοστραφής προσέγγιση
- Ανα-χρησιμοποίηση προδιαγραφών και αποδείξεων

Βάσεις της προσέγγισης:

1. Ιεραρχική σύνθεση συμπεριφοριακών αντικειμένων
2. Module Algebra

Άλγεβρα – Σύνθεση Πρωτοκόλλων

Πλεονεκτήματα-Δυνατότητες

- Εξισωτική αλγεβρική προδιαγραφή => ευκολότερα κατανοητή
- Εκτελέσιμες προδιαγραφές
- Συμβατή με ημιαυτόματες τεχνικές απόδειξης θεωρήματος - Επαλήθευση στο επίπεδο σχεδίασης

Άλγεβρα - Σύνθεση Πρωτοκόλλων

Συμπεριφοριακή Προδιαγραφή

- Λογική βάση: Άλγεβρα με κρυμμένους τύπους
- Χαρακτηρίζει την συμπεριφορά συστημάτων μετά από πειράματα ανεξάρτητα του τρόπου υλοποίησης

Άλγεβρα - Σύνθεση Πρωτοκόλλων

Προδιαγραφή πρωτοκόλλου: Συμπεριφοριακό αντικείμενο P, όπου:

- Ο κρυμμένος τύπος $h_P \in H_P$ συμβολίζει το χώρο καταστάσεων S του πρωτοκόλλου
- Οι P-δράσεις συμβολίζουν το σύνολο των μεταβάσεων οι οποίες αλλάζουν υπό συνθήκες την κατάσταση του πρωτοκόλλου
- Η αρχική κατάσταση ορίζεται ως μια σταθερή $s_0 \in S$
- Οι τελικές καταστάσεις $F \subseteq S$ είναι όλες οι επιτεύξιμες καταστάσεις του συμπεριφοριακού αντικειμένου

Άλγεβρα - Σύνθεση Πρωτοκόλλων

- Οι P-παρατηρήσεις επιστρέφουν τις τιμές των ποσοτήτων του πρωτοκόλλου σε πιθανές καταστάσεις του
- Οι συμμετέχοντες agents στο πρωτόκολλο προδιαγράφονται είτε ως συμπεριφοριακά αντικείμενα, είτε ως τύποι δεδομένων

Ισοδυναμία καταστάσεων πρωτοκόλλων: Ταυτίζεται με την συμπεριφοριακή ισοδυναμία των αντικειμένων

Εκτέλεση πρωτοκόλλου: Μια άπειρη ή πεπερασμένη ακολουθία καταστάσεων

Άλγεβρα – Σύνθεση Πρωτοκόλλων

Τεχνική Ιεραρχικής Σύνθεσης Συμπεριφοριακών Αντικειμένων

- Ιεραρχική
- Τελεστές προβολής

Είδη σύνθεσης: Παράλληλη (ταυτόχρονη) - δυναμική ή Συγχρονισμένη παράλληλη

Άλγεβρα - Σύνθεση Πρωτοκόλλων

Υπο-πρωτόκολλα: Τα συστατικά πρωτόκολλα ενός σύνθετου πρωτοκόλλου

Πρωτόκολλο βασικού επιπέδου: Ένα πρωτόκολλο χωρίς συστατικά

Άλγεβρα - Σύνθεση Πρωτοκόλλων

Βιβλιογραφία: Τρεις προσεγγίσεις σύνθεσης πρωτοκόλλων

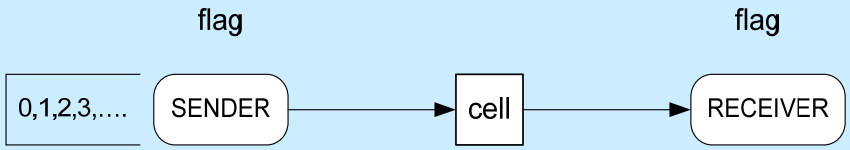
1. Πρωτόκολλα ως συστήματα – σύνθεση συστημάτων
2. Πρωτόκολλα ως ακολουθία – διαδοχή μηνυμάτων ανάμεσα στους agents (interaction protocols)
3. Στοίβα πρωτοκόλλων

Πως μπορούν να διαχειρισθούν ενοποιημένα από την προσέγγιση μας

Άλγεβρα - Σύνθεση Πρωτοκόλλων

Πρωτόκολλα ως συστήματα

Σενάριο 1 (*Απλό πρωτόκολλο μεταφοράς δεδομένων*).



Ο πομπός τοποθετεί ένα αριθμό από μια λίστα στην κυψέλη και ο δέκτης τον λαμβάνει από αυτή. Για να τοποθετήσει στην κυψέλη τον επόμενο αριθμό ο πομπός, πρέπει η κοινή μεταβλητή flag να είναι false. Αρχικά flag = false, ενώ κάθε φορά που λαμβάνει ένα αριθμό ο δέκτης η flag τίθεται true. Όταν flag=true, ο πομπός παίρνει τον επόμενο αριθμό από τη λίστα και θέτει flag = false.

Άλγεβρα - Σύνθεση Πρωτοκόλλων

Αλγεβρική προδιαγραφή

Modules τύπων δεδομένων: **`CELL`**, **`NAT`**, **`LIST`**

Συμπεριφοριακό αντικείμενο: **`DTP`** με τύπο **`Protocol`**

Παρατηρητές: **`flag`**, **`next`**, **`list`**

Δράσεις: **`send`**, **`receive`**, **`update`**

Εξισώσεις π.χ. για τη δράση **`send`**

```
ceq cell(send(P)) = c(next(P)) if not flag(P) .
eq flag(send(P)) = flag(P) .
eq next(send(P)) = next(P) .
eq list(send(P)) = list(P) .
ceq send(P)       = P          if flag(P) .
```

Άλγεβρα – Σύνθεση Πρωτοκόλλων

Παράλληλη σύνθεση

• Μετονομασία συμπεριφοριακού αντικειμένου για δύο ίδια πρωτόκολλα

```
mod* DTP1 {
pr(DTP *{hsort Protocol -> Protocol1,
op init -> init1})}

mod* DTP2 {
pr(DTP *{hsort Protocol -> Protocol2,
op init -> init2})}
```

• Σύνθετο πρωτόκολλο: Ο πομπός στέλνει ανεξάρτητα τα δεδομένα σε δύο δέκτες.

• Τελεστές προβολής για κάθε πρωτόκολλο:

```
bop pr1 : 2Protocol -> Protocol1
bop pr2 : 2Protocol -> Protocol2
```

Άλγεβρα - Σύνθεση Πρωτοκόλλων

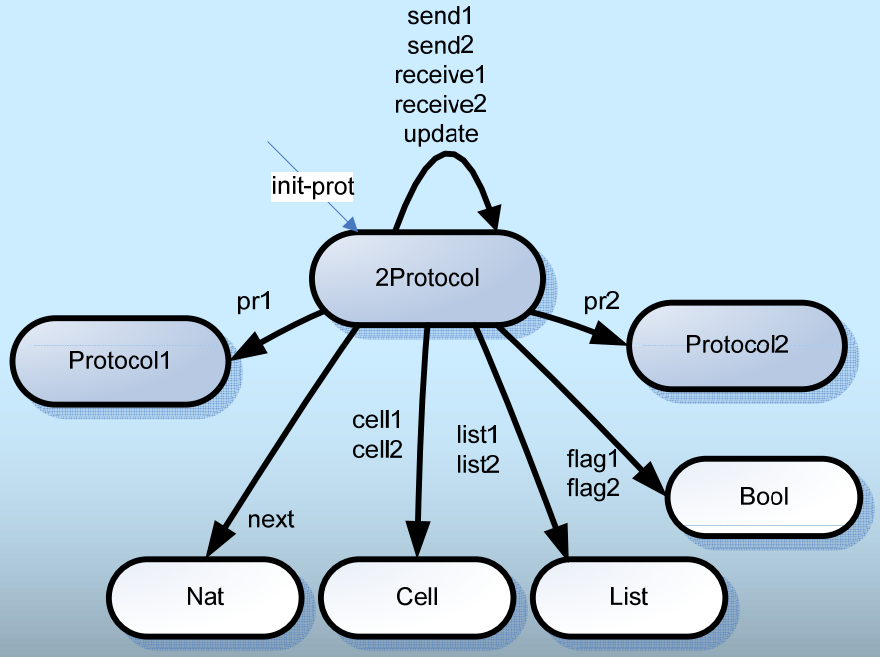
- Εξισώσεις ορισμού τελεστών προβολής (π.χ. για **pr1**)

```
eq pr1(init-prot) = init1 .
          eq pr1(send1(P)) = send(pr1(P)) .
                        eq pr1(receive1(P)) =
receive(pr1(P)) .                       eq
pr1(update1(P)) = update(pr1(P)) .
eq pr1(send2(P)) = pr1(P) .
eq pr1(receive2(P)) = pr1(P) .
eq pr1(update2(P)) = pr1(P) .
```

Άλγεβρα - Σύνθεση Πρωτοκόλλων

Συγχρονισμένη Παράλληλη σύνθεση

• Για να στείλει τον επόμενο αριθμό ο πομπός θα πρέπει να έχουν λάβει και οι δύο δέκτες



Άλγεβρα - Σύνθεση Πρωτοκόλλων

Συγχρονισμένη Παράλληλη σύνθεση

- Για τη δράση **update**

```
eq cell1(update(P)) = cell1(P) .
ceq flag1(update(P)) = false if (flag1(P) and flag2(P)) .
ceq next(update(P)) = s(next(P)) if (flag1(P) and
                                     flag2(P)) .
eq list1(update(P)) = list1(P) .
eq cell2(update(P)) = cell2(P) .
ceq flag2(update(P)) = false if (flag1(P) and flag2(P)) .
eq list2(update(P)) = list2(P) .
ceq update(P)       = P if not (flag1(P) and flag2(P)) .
```

Στην τρίτη εξίσωση φαίνεται ο συγχρονισμός

Άλγεβρα - Σύνθεση Πρωτοκόλλων

Πρωτόκολλα αλληλεπίδρασης

Σενάριο 2

Ένας πελάτης ζητάει από το βιβλιοπωλείο την τιμή ενός βιβλίου μέσω του μηνύματος *reqQuote*, και μόλις λάβει την απάντηση από το βιβλιοπωλείο (μήνυμα *sendQuote*), δέχεται την προσφορά του (μήνυμα *sendAccept*). Το βιβλιοπωλείο στη συνέχεια αποστέλλει το βιβλίο (μήνυμα *sendGoods*) και ο πελάτης πληρώνει (μήνυμα *sendMoney*).

Άλγεβρα – Σύνθεση Πρωτοκόλλων

Προδιαγραφή πρωτοκόλλου

- Συμπεριφοριακό αντικείμενο **`PURCHASE1`** με κρυμμένο τύπο **`Prot1`**
- Τύποι δεδομένων: **`BANK`**, **`BOOK`**, **`PRICE`**, **`CUSTOMER`**, **`BOOKSTORE`**, **`MESSAGE`** και **`NETWORK`**
- Σειρά αποστολής μηνυμάτων (δράσεις): μέσω συνθηκών

Άλγεβρα – Σύνθεση Πρωτοκόλλων

Κληρονομικότητα πρωτοκόλλου

Στην περίπτωση που το βιβλιοπωλείο είναι πρόθυμο να επιστρέψει τα χρήματα ενός επιστρεφόμενου βιβλίου, το σενάριο είναι όμοιο με το προηγούμενο μέχρι το σημείο της μεταφοράς του βιβλίου στον πελάτη, ενώ στη συνέχεια επεκτείνεται με τα μηνύματα επιστροφής του βιβλίου (*returnGoods*) και επιστροφής των χρημάτων (*sendRefund*).

Το νέο πρωτόκολλο PURCHASE2 κληρονομεί τις δράσεις του PURCHASE1 και το επεκτείνει με τις δύο νέες δράσεις αποστολής μηνυμάτων

Άλγεβρα - Σύνθεση Πρωτοκόλλων

Στοίβες πρωτοκόλλων

Συνδυασμός πρωτοκόλλων – Χρήση υπηρεσιών από πρωτόκολλα υψηλότερου επιπέδου

ΤΕΛΕΣΤΕΣ: εισαγωγή (import) + άθροισης/συνδυασμού (sum/combination)

Άλγεβρα - Σύνθεση Πρωτοκόλλων

Τελεστές άλγεβρας

- **Άθροισμα** πρωτοκόλλων (+) - ως άθροισμα προδιαγραφών συμπεριφοριακών αντικειμένων.
  Χρήση: Εισαγωγή ή χρήση πάνω από μιας προδιαγραφής για τον ορισμό του νέου πρωτοκόλλου.
  Ιδιότητες: P1 + P2 = P2 + P1, P1 + (P2 + P3) = (P1 + P2) + P3, P1 + P1 = P1.
  Απόδειξη: Εφόσον κάθε πρωτόκολλο ορίζεται ως συμπεριφοριακό αντικείμενο, το άθροισμα ορίζεται ως η ένωση των αντίστοιχων συνόλων, οπότε ισχύουν οι παραπάνω ιδιότητες.

- **Εισαγωγή** πρωτοκόλλου ($\lhd_{\text{mode}}$), mode = protecting, extending ή using.
  Χρήση: Όταν το πρωτόκολλο P1 χρησιμοποιεί τις προδιαγραφές των P2, P3 ως έχουν (mode = protecting), γράφουμε: $(P1 + P2) \lhd_{pr} P1$.
  Ιδιότητα: Για P1, P2, P3 προδιαγραφές πρωτοκόλλων, εάν $P2 \lhd_{\text{mode}} P1$ και $P3 \lhd_{\text{mode}} P2$, τότε $P3 \lhd_{\text{mode}} P1$

Άλγεβρα – Σύνθεση Πρωτοκόλλων

Τελεστές άλγεβρας

- **Σύνθεση** πρωτοκόλλων

  1. Παράλληλη σύνθεση (χωρίς συγχρονισμό $\|$)
  Χρήση: Για την παράλληλη σύνθεση πρωτοκόλλων ως συμπεριφοριακών αντικειμένων, $P = P1 \| P2$

  2. Συγχρονισμένη Παράλληλη σύνθεση ($\otimes$)
  Χρήση: Για την παράλληλη σύνθεση πρωτοκόλλων ως συμπεριφοριακών αντικειμένων, $P = P1 \otimes P2$

Άλγεβρα – Σύνθεση Πρωτοκόλλων

Τελεστές άλγεβρας

- **Υπο-εκτέλεση** πρωτοκόλλων ([ ). Αν r_i, r_j εκτελέσεις πρωτοκόλλων, r_j [r_i συμβολίζει ότι η r_i είναι υπό-εκτέλεση της r_j. Επίσης:

  r_j [$r_i \Leftrightarrow \forall s_i \in r_i, \exists s_j \in r_j : s_j \sim s_i$ και $\forall s_i' \in r_i, \exists s_j' \in r_j : s_j' \sim s_i' \Leftrightarrow (s_i <_{ri} s_i' \Leftrightarrow s_j <_{ri} s_j')$.

  Ιδιότητες: Ανακλαστικότητα (κάθε εκτέλεση είναι υποεκτέλεση του εαυτού της), Μεταβατικότητα (Εάν r_j [r_1 και r_k [r_j, τότε r_k [r_i).

- **Υπο-Πρωτόκολλο** ([|). Αν τα το Q είναι σύνθετο πρωτόκολλο και το P συστατικό του, τότε P [| Q. Εάν P = P1 || P2 ή P = P1 ⊗P2, τότε P1 [| P και P2 [| P

- Άλλοι τελεστές: Μετονομασία *, Περιεκτικότητα.

Συνεισφορά Διατριβής

Προδιαγραφή, σχεδίαση και **επαλήθευση** κινητών συστημάτων με χρήση τεχνικών συμπεριφοριακής αλγεβρικής προδιαγραφής.

- Προτάθηκαν τα Κινητά ΠΣΜ
- Ενοποιήθηκαν με τα Χρονικά και Υβριδικά ΠΣΜ
- Παρουσιάσθηκαν παραδείγματα εφαρμογής και αποδείχθηκαν ιδιότητες ασφαλείας των προδιαγραφών.
- Προδιαγράφηκαν και επαληθεύθηκαν ιδιότητες πρωτοκόλλων ασφαλείας με την προτεινόμενη μέθοδο.
- Προτάθηκε άλγεβρα πρωτοκόλλων για τη σύνθεση πρωτοκόλλων και ανάπτυξη πολυπλοκότερων από απλούστερα.

Εφαρμογές

Οι τεχνικές της διατριβής έχουν ήδη χρησιμοποιηθεί στο πλαίσιο **διπλωματικών** εργασιών σε:

- μοντελοποίηση συστημάτων διαχείρισης ψηφιακών δικαιωμάτων για κινητές συσκευές,
- ανάλυση απαιτήσεων υπηρεσιών όπως m-learning και m-commerce,
- εφαρμογή άλγεβρας πρωτοκόλλων στη σύνθεση του πρωτοκόλλου αυθεντικοποίησης NSLPK και διερεύνηση συνδυασμού της με τη Θεωρία Strand Space
- μελέτη περιπτώσεων πρωτοκόλλων ασφαλείας κινητών επικοινωνιών και διαδικασίας από τη στοίβα του Bluetooth.

Μελλοντική Έρευνα

Στο μέλλον:

- να ενσωματωθούν τεχνικές απόδειξης ιδιοτήτων ζωντάνιας (liveness) των κινητών συστημάτων στο πλαίσιο MobileOBJ,
- να συνδυασθεί με τη Mobile Maude για την αυτοματοποιημένη απόδειξη μέσω ελέγχου μοντέλου και της μεθόδου Bounded OTS/Maude,
- να διερευνηθεί περαιτέρω η περισσότερο αυτοματοποιημένη τεχνική απόδειξης συμπεριφοριακών προδιαγραφών (coinduction) στην επαλήθευση κινητών συστημάτων.

Μελλοντική Έρευνα

Για την άλγεβρα πρωτοκόλλων:

- ανάπτυξη βιβλιοθηκών προδιαγραφών πρωτογενών πρωτοκόλλων που έχουν επαληθευμένες ιδιότητες για χρήση τους στη δημιουργία σύνθετων πρωτοκόλλων,
- σύνθεση πρωτοκόλλων ασφαλείας σε συνδυασμό με τη θεωρία Strand Space,
- ανάπτυξη προδιαγραφών νέων πρωτοκόλλων με χρήση της άλγεβρας και υλοποίηση με μια γλώσσα χαμηλότερου επιπέδου (C++, Java).

Λίστα Δημοσιεύσεων

1. Για τα Κινητά ΠΣΜ

Journal

J1) **Iakovos Ouranos,** Petros Stefaneas, Panayiotis Frangos, An algebraic framework for modeling of mobile systems, IEICE Trans. on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E90-A, No. 9, pp. 1986-1999, September 2007.

J2) **Iakovos Ouranos,** Petros Stefaneas, Panayiotis Frangos, Formal analysis of real-time and hybrid models of mobile systems in MobileOBJ framework, Science of Computer Programming, Elsevier, **submitted** for publication, January 2008.

Conference

C1) **Iakovos Ouranos,** Petros Stefaneas, and Panayiotis Frangos, A formal specification framework for ad hoc mobile communication networks, In: Proc: SOFSEM 2007, pp. 91-102, Harrachov, Czech, 2007.

Λίστα Δημοσιεύσεων

1. Για τα Κινητά ΠΣΜ

Conference

C2) **Iakovos Ouranos**, Petros Stefaneas and Panayiotis Frangos, MobileOBJ: A mobility approach using CafeOBJ algebraic specification language, International Conference on Numerical Analysis and Applied Mathematics (ICNAAM 2004), Chalkis, Greece, September 2004.

C3) **Iakovos Ouranos**, Petros Stefaneas and Panayiotis Frangos, An algebraic specification of mobile IPv6 protocol, 1st International Conference PRISE 2004 (Principles of Software Engineering), Buenos Aires, Argentina, November 22 - 27, 2004.

Λίστα Δημοσιεύσεων

1. Για πρωτόκολλα ασφαλείας

Conference

C4) **Iakovos Ouranos,** Petros Stefaneas, Kostas Barlas, Stefanos Demertzis, George Koletsos, Panayiotis Frangos, Modelling real time authentication protocols using algebraic specification techniques-the case of TESLA protocol, In: Proc. IFIP TC7 Conference, pp. 388-389, Krakow, July 2007.

C5) **Iakovos Ouranos,** and Petros Stefaneas, Verifying security protocols for sensor networks using algebraic specification techniques, In: Proc. CAI 2007, Thessalonica, Greece, May 2007, Lecture Notes in Computer Science, vol. 4728, pp. 247-259, 2007, Springer.

Ημερίδες

ΗΜ1) Ι. Ουρανός, Π. Στεφανέας, Π. Φράγκος, Προδιαγραφή και επαλήθευση πρωτοκόλλων ασφαλείας συστημάτων κινητών επικοινωνιών με χρήση τυπικών μεθόδων, Σύγχρονες τάσεις στις τηλεπικοινωνίες και τεχνολογίες αιχμής, Ημερίδα Τ.Ε.Ε., Ιανουάριος 2006

Λίστα Δημοσιεύσεων

1. Για άλγεβρα πρωτοκόλλων

Journal

J3) **Iakovos Ouranos,** Petros Stefaneas, Panayiotis Frangos, Applying behavioural specification techniques to protocol composition, IEICE Trans. on Fundamentals of Electronics, Communications and Computer Sciences, submitted for publication, September 2007.

Conference

C6) **I. Ouranos**, P. Stefaneas, P. Frangos, A behavioural specification approach to protocol algebra, Formal Methods 2008, submitted for publication, November 2007.

Λίστα Δημοσιεύσεων

1. Άλλες δημοσιεύσεις

Journal

J4) E. Papkelis, I. Psarros, **I. Ouranos,** H. Moshovitis, K. Karakatselos, E. Vagenas, H. Anastassiu, P. Frangos, A radio coverage prediction model in wireless communication systems based on physical optics and the physical theory of diffraction, IEEE Antennas and Propagation Magazine, Vol. 49-2, pp. 156-165, April 2007.

Conference

C7) Ch. G. Moschovitis, E. G. Papkelis, H. T. Anastassiu, K. T. Karakatselos, **I. Ch. Ouranos**, and P. V. Frangos, Asymptotic calculation of the scattered electric field from a finite rectangular plate using an enhanced stationary phase method (SPM) approximation, European Conference on Antennas & Propagation (EuCAP 2006), November 6 - 10, 2006, Nice, France.

Λίστα Δημοσιεύσεων

1. Άλλες δημοσιεύσεις

Conference

C8) Ch. G. Moschovitis, E. G. Papkelis, H. T. Anastassiu, K. T. Karakatselos, **I. Ch. Ouranos**, P. V. Frangos, An application of an enhanced stationary phase method (SPM) approximation for the asymptotic calculation of the scattered electric field from a finite rectangular plate, International Conference on Communications, Electromagnetics and Medical Applications (CEMA 2006), October 19 - 21, 2006, Sofia, Bulgaria.

C9) E. Papkelis, **I. Ouranos**, H. Moshovitis, K. Karakatselos, P. Frangos, Radio coverage simulation tool in urban environments using physical optics and physical theory of diffraction, International Conference Mediterranean Microwaves Symposium 2005, September 6 - 8, 2005, Athens, Greece.

Λίστα Δημοσιεύσεων

1. Άλλες δημοσιεύσεις

Conference

C10) E. Papkelis, **I. Ouranos**, H. Moshovitis, K. Karakatselos, P. Frangos, A radio coverage prediction method in urban microcellular environments using electromagnetic Techniques, International Conference 'Days on Diffraction 2005, June 28 - July 1, 2005, St. Petersburg, Russia.

C11) **I. Ouranos**, E. Papkelis and P. Frangos, An electromagnetic method for calculating radiocoverage in urban microcellular environments, Conference Days on Diffraction 2004, June 29 - July 2, 2004, St. Petersburg, Russia.

ΕΥΧΑΡΙΣΤΩ ΓΙΑ ΤΗΝ

ΠΡΟΣΟΧΗ ΣΑΣ !

Ερωτήσεις;