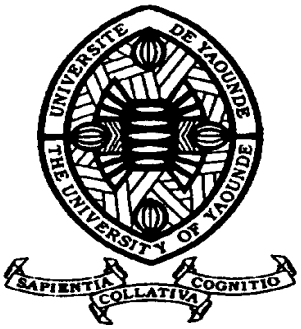
REPUBLIQUE DU CAMEROUN
Paix – Travail – Patrie
****
UNIVERSITE DE YAOUNDE I
FACULTE DES SCIENCES
DEPARTEMENT DE INFORMATIQUE
****
CENTRE DE RECHERCHE ET DE FORMATION DOCTORALE EN SCIENCES, TECHNOLOGIE& GEOSCIENCES



REPUBLIC OF CAMEROUN
Peace – Work – Fatherland
****
UNIVERSITY OF YAOUNDE I
FACULTY OF SCIENCE
DEPARTMENT OF COMPUTER SCIENCE
****
POSTGRADUATE SHOOL OF SCIENCE, TECHNOLOGY& GEOSCIENCE

Proposition d'une approche opportuniste de gestion de la Mobilité dans les réseaux communautaires sans fil Basée sur le modèle de Markov

THÈSE
Pour obtenir le grade de
Docteur de l'Université de Yaoundé I

Par : **ABDOU ASKIDI**

Sous la direction de
Maurice TCHUENTÉ
Professeur, Université de Yaoundé I
Thomas DJOTIO NDIÉ
Maitre de Conférences, Université de Yaoundé I

Année Académique : 2019 - 2020

RÉPUBLIQUE DU CAMEROUN
PAIX-TRAVAIL-PATRIE
****
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR
****
UNIVERSITÉ DE YAOUNDÉ I
****
CENTRE DE RECHERCHE ET DE FORMATION DOCTORALE EN SCIENCES, TE*CHNOLOGIES* ET *GEOSCIENCES*
****

REPUBLIC OF CAMEROON
PEACE-WORK-FATHERLAND
****
MINISTRY OF HIGHER EDUCATION
****
THE UNIVERSITY OF YAOUNDE I
****
POSTGRADUATE SCHOOL OF SCIENCE, TECHNOLOGY AND GEO-SCIENCES
****

DÉPARTEMENT D'INFORMATIQUE
DEPARTMENT OF COMPUTER SCIENCE

ATTESTATION DE CORRECTION DE LA THÈSE DE DOCTORAT/PhD

Nous soussignés, Professeur **AWONO ONANA Charles**, Maître de Conférences **NDOUNDAM René**, membres du jury de la thèse de Doctorat/PhD présentée par Monsieur **ABDOU ASKIDI**, Matricule **10U0612**, intitulée: **«Proposition d'une approche opportuniste de gestion de la Mobilité dans les réseaux communautaires sans fil Basée sur le modèle de Markov »** et soutenue le **15/04/2020** en vue de l'obtention du diplôme de **Doctorat/PhD en Informatique**, attestons que toutes les corrections demandées par le jury de soutenance en vue de l'amélioration de ce travail, ont été effectuées.

En foi de quoi la présente attestation lui est délivrée pour servir et valoir ce que de droit.

Président

AWONO ONANA Charles
Professeur

Examinateur

NDOUNDAM René
Maître de Conférences

LISTE PROTOCOLAIRE

UNIVERSITÉ DE YAOUNDÉ I **Faculté des Sciences** Division de la Programmation et du Suivi des Activités Académiques		THE UNIVERSITY OF YAOUNDE I **Faculty of Science** Division of Programming and Follow-up of Academic Affaires
LISTE DES ENSEIGNANTS PERMANENTS		**LIST OF PERMANENT TEACHING STAFF**

ANNÉE ACADEMIQUE 2017/2018

(Par Département et par Grade)

DATE D'ACTUALISATION : 10 Mars 2018

ADMINISTRATION

DOYEN : AWONO ONANA Charles, *Professeur*
VICE-DOYEN / DPSAA : DONGO Etienne, *Professeur*
VICE-DOYEN / DSSE : AJEAGAH Gidéon AGHAINDUM
VICE-DOYEN / DRC : ABOSSOLO Monique, *Maitre de Conférences*
Chef Division Administrative et Financière : NDOYE FOE Marie C. F., *Maitre de Conférences*
Chef Division des Affaires Académiques, de la Scolarité et de la Recherche MBAZE MEVA'A Luc Léonard, Maitre de Conférences

1- DÉPARTEMENT DE BIOCHIMIE (BC) (41)			
N°	**NOMS ET PRÉNOMS**	**GRADE**	**OBSERVATIONS**
1	FEKAM BOYOM Fabrice	Professeur	En poste
2	MBACHAM FON Wilfried	Professeur	En poste
3	MOUNDIPA FEWOU Paul	Professeur	Chef de Département
4	NINTCHOM PENLAP V. épse BENG	Professeur	En poste
5	OBEN Julius ENYONG	Professeur	En poste
6	ATOGHO Barbara Mma	Maître de Conférences	En poste
7	BELINGA née NDOYE FOE M. C. F.	Maître de Conférences	Chef DAF / FS
8	BIGOGA DIAGA Jude	Maître de Conférences	En poste
9	BOUDJEKO Thaddée	Maître de Conférences	En poste
10	EFFA NNOMO Pierre	Maître de Conférences	En poste
11	FOKOU Elie	Maître de Conférences	En poste
12	KANSCI Germain	Maître de Conférences	En poste

13	NANA Louise épouse WAKAM	Maître de Conférences	En poste
14	NGONDI Judith Laure	Maître de Conférences	En poste
15	NGUEFACK Julienne	Maître de Conférences	En poste
16	NJAYOU Frédéric Nico	Maître de Conférences	En poste
17	ACHU Merci BIH	Chargée de Cours	En poste
18	DJOKAM TAMO Rosine	Chargée de Cours	En poste
19	DJUIDJE NGOUNOUE Marcelline	Chargée de Cours	En poste
20	DJUIKWO NKONGA Ruth Viviane	Chargée de Cours	En poste
21	EVEHE BEBANDOUE Marie-Solange	Chargée de Cours	En poste
22	EWANE Cécile Anne	Chargée de Cours	En poste
23	KOTUE KAPTUE Charles	Chargé de Cours	En poste
24	LUNGA Paul KEILAH	Chargé de Cours	En poste
25	MBONG ANGIE M. Mary Anne	Chargée de Cours	En poste
26	MOFOR née TEUGWA Clotilde	Chargée de Cours	Inspecteur de Service MINESUP
27	NJAYOU Frédéric Nico	Chargé de Cours	En poste
28	Palmer MASUMBE NETONGO	Chargé de Cours	En poste
29	TCHANA KOUATCHOUA Angèle	Chargée de Cours	En poste
30	PACHANGOU NSANGOU Sylvain	Chargé de Cours	En poste
31	DONGMO LEKAGNE Joseph Blaise	Chargé de Cours	En poste
32	FONKOUA Martin	Chargé de Cours	En poste
33	BEBOY EDZENGUELE Sara Nathalie	Chargée de Cours	En poste
34	DAKOLE DABOY Charles	Chargée de Cours	En poste
35	MANANGA Marlyse Joséphine	Chargée de Cours	En poste
36	MBOUCHE FANMOE Marceline Joëlle	Assistante	En poste
37	BEBEE Fadimatou	Assistante	En poste
38	TIENTCHEU DJOKAM Leopold	Assistant	En poste

2- DÉPARTEMENT DE BIOLOGIE ET PHYSIOLOGIE ANIMALES (BPA) (44)			
1	BILONG BILONG Charles-Félix	Professeur	**Chef de Département**
2	DIMO Théophile	Professeur	En Poste
3	DJIETO LORDON Champlain	Professeur	En poste
4	ESSOMBA née NTSAMA MBALA	Professeur	*VDoyen/FMSB/UYI*
5	FOMENA Abraham	Professeur	En Poste
6	KAMTCHOUING Pierre	Professeur	EN POSTE
7	NJAMEN Dieudonné	Professeur	En poste
8	NJIOKOU Flobert	Professeur	En Poste
9	NOLA Moïse	Professeur	En poste
10	TAN Paul VERNYUY	Professeur	En poste
11	TCHUEM TCHUENTE Louis Albert	Professeur	*Coord. Progr. MINSANTE*
12	AJEAGAH Gidéon AGHAINDUM	Maître de Conférences	**Chef Service DPER**
13	DZEUFIET DJOMENI Paul Désiré	Maître de Conférences	En poste
14	FOTO MENBOHAN Samuel	Maître de Conférences	En poste
15	KAMGANG René	Maître de Conférences	*C.S. MINRESI*
16	KEKEUNOU Sévilor	Maître de Conférences	En poste
17	MEGNEKOU Rosette	Maître de Conférences	En poste
18	MONY Ruth épse NTONE	Maître de Conférences	En Poste
19	TOMBI Jeannette	Maître de Conférences	En poste
20	ZEBAZE TOGOUET Serge Hubert	Maître de Conférences	En poste
21	ALENE Désirée Chantal	Chargée de Cours	En poste
22	ATSAMO Albert Donatien	Chargée de Cours	En poste
23	BELLET EDIMO Oscar Roger	Chargé de Cours	En poste
24	BILANDA Danielle Claude	Chargée de Cours	En poste
25	DJIOGUE Séfirin	Chargée de Cours	En poste
26	DONFACK Mireille	Chargée de Cours	En poste

27	GOUNOUE KAMKUMO Raceline	Chargée de Cours	En poste
28	LEKEUFACK FOLEFACK Guy B.	Chargé de Cours	En poste
29	MAHOB Raymond Joseph	Chargé de Cours	En poste
30	MBENOUN MASSE Paul Serge	Chargé de Cours	En poste
31	MOUNGANG Luciane Marlyse	Chargée de Cours	En poste
32	MVEYO NDANKEU Yves Patrick	Chargée de Cours	En poste
33	NGOUATEU KENFACK Omer Bébé	Chargé de Cours	En poste
34	NGUEGUIM TSOFACK Florence	Chargée de Cours	En poste
35	NGUEMBOK	Chargé de Cours	En poste
36	NJATSA Hermine épse MEGAPTCHE	Chargée de Cours	En Poste
37	NJUA Clarisse Yafi	Chargée de Cours	**CD/UBa**
38	NOAH EWOTI Olive Vivien	Chargée de Cours	En poste
39	TADU Zephyrin	Chargée de Cours	En poste
40	YEDE	Chargée de Cours	En poste
41	ETEME ENAMA Serge	Assistant	En poste
42	KANDEDA KAVAYE Antoine	Assistant	En poste
43	KOGA MANG DOBARA	Assistant	En poste
3- DÉPARTEMENT DE BIOLOGIE ET PHYSIOLOGIE VÉGÉTALES (BPV) (26)			
1	AMBANG Zachée	Professeur	Chef Division/UYII
2	BELL Joseph Martin	Professeur	En poste
3	YOUMBI Emmanuel	Professeur	**Chef de Département**
4	MOSSEBO Dominique Claude	Professeur	En poste
5	BIYE Elvire Hortense	Maître de Conférences	En poste
6	DJOCGOUE Pierre François	Maître de Conférences	En poste
7	KENGNE NOUMSI Ives Magloire	Maître de Conférences	En poste
8	MALA Armand William	Maître de Conférences	En poste
9	NDONGO BEKOLO	Maître de Conférences	*CE / MINRESI*

10	NGONKEU MAGAPTCHE Eddy L.	Maître de Conférences	En poste
11	ZAPFACK Louis	Maître de Conférences	En poste
12	MBARGA BINDZI Marie Alain	Maître de Conférences	CT/Univ Dschang
13	MBOLO Marie	Maître de Conférences	En poste
14	ANGONI Hyacinthe	Chargée de Cours	En poste
15	MAHBOU SOMO TOUKAM. Gabriel	Chargé de Cours	En poste
16	ONANA JEAN MICHEL	Chargé de Cours	En poste
17	GOMANDJE Christelle	Chargée de Cours	En poste
18	NGODO MELINGUI Jean Baptiste	Chargé de Cours	En poste
19	NGALLE Hermine BILLE	Chargée de Cours	En poste
20	NGOUO Lucas Vincent	Chargé de Cours	En poste
21	NSOM ZAMO Annie Claude épse PIAL	Chargée de Cours	*Expert national /UNESCO*
22	TONFACK Libert Brice	Chargé de Cours	En poste
23	TSOATA Esaïe	Chargé de Cours	En poste
24	DJEUANI Astride Carole	Assistante	En poste
25	MAFFO MAFFO Nicole Liliane	Assistante	En poste
26	NNANGA MEBENGA Ruth Laure	Assistante	En poste
27	NOUKEU KOUAKAM Armelle	Assistante	En poste

4- DÉPARTEMENT DE CHIMIE INORGANIQUE (CI) (33)			
1	AGWARA ONDOH Moïse	Professeur	*Vice RecteurUniv, Bamenda*
2	ELIMBI Antoine	Professeur	En poste
3	Florence UFI CHINJE épouse MELO	Professeur	*RECTEUR Univ.Ngaoundere*
4	GHOGOMU Paul MINGO	Professeur	*Directeur Cabinet PM*

5	LAMINSI Samuel	Professeur	En poste
6	NANSEU NjikiCharles Péguy	Professeur	En poste
7	NDIFON Peter TEKE	Professeur	*IS1 MINRESI/**Chef de Département***
8	NENWA Justin	Professeur	En poste
9	NGAMENI Emmanuel	Professeur	*DOYEN FS Univ. Dschang*
10	BABALE née DJAM DOUDOU	Maître de Conférences	*Chargée Mission P.R.*
11	DJOUFAC WOUMFO Emmanuel	Maître de Conférences	En poste
12	KEMMEGNE MBOUGUEM Jean C.	Maître de Conférences	En poste
13	KONG SAKEO	Maître de Conférences	*Chargé de Mission au P. M.*
14	NDIKONTAR Maurice KOR	Maître de Conférences	*Vice-Doyen Univ. Bamenda*
15	NGOMO Horace MANGA	Maître de Conférences	*VC/UB*
16	NJIOMOU C. épse DJANGANG	Maître de Conférences	En poste
17	YOUNANG Elie	Maître de Conférences	En poste
18	ACAYANKA Elie	Chargé de Cours	En poste
19	EMADACK Alphonse	Chargé de Cours	En poste
20	KAMGANG YOUBI Georges	Chargé de Cours	En poste
21	NDI NSAMI Julius	Chargée de Cours	En poste
22	NJOYA Dayirou	Chargé de Cours	En poste
23	PABOUDAM GBAMBIE A.	Chargée de Cours	En poste
24	TCHAKOUTE KOUAMO Hervé	Chargé de Cours	En poste
25	BELIBI BELIBI Placide Désiré	Chargé de Cours	En poste
26	CHEUMANI YONA Arnaud M.	Chargé de Cours	En poste
27	NYAMEN Linda Dyorisse	Chargée de Cours	En poste
28	KENNE DEDZO GUSTAVE	Chargé de Cours	En poste
29	KOUOTOU DAOUDA	Chargé de Cours	En poste
30	MAKON Thomas Beauregard	Chargé de Cours	En poste

31	MBEY Jean Aime	Chargé de Cours	En poste
32	NCHIMI NONO KATIA	Chargé de Cours	En poste
33	NEBA nee NDOSIRI Bridget NDOYE	Chargé de Cours	En poste
5- DÉPARTEMENT DE CHIMIE ORGANIQUE (CO) (34)			
1	DONGO Etienne	Professeur	**Vice-Doyen / DPSAA**
2	GHOGOMU TIH Robert Ralph	Professeur	Dir IBAF/UDS
3	MBAFOR Joseph	Professeur	En poste
5	NGOUELA Silvère Augustin	Professeur	En poste
6	NKENGFACK Augustin Ephraïm	Professeur	**Chef de Département**
7	NYASSE Barthélemy	Professeur	*Directeur/UN*
8	PEGNYEMB Dieudonné Emmanuel	Professeur	*Directeur/ MINESUP*
9	WANDJI Jean	Professeur	En poste
10	Alex de Théodore ATCHADE	Maître de Conférences	*DEPE/ Rectorat/UYI*
11	FOLEFOC Gabriel NGOSONG	Maître de Conférences	*En poste*
12	KEUMEDJIO Félix	Maître de Conférences	En poste
13	KOUAM Jacques	Maître de Conférences	En poste
14	MBAZOA née DJAMA Céline	Maître de Conférences	En poste
15	NOUNGOUE TCHAMO Diderot	Maître de Conférences	En poste
16	TCHOUANKEU Jean-Claude	Maître de Conférences	*VR/ UYII*
17	YANKEP Emmanuel	Maître de Conférences	En poste
18	TIH née NGO BILONG E. Anastasie	Maître de Conférences	En poste
19	MKOUNGA Pierre	Maître de Conférences	En poste
20	NGO MBING Joséphine	Maître de Conférences	En poste
21	TABOPDA KUATE Turibio	Maître de Conférences	En poste
22	KEUMOGNE Marguerite	Maître de Conférences	En poste
23	AMBASSA Pantaléon	Chargé de Cours	En poste

24	EYONG Kenneth OBEN	Chargé de Cours	En poste
25	FOTSO WABO Ghislain	Chargé de Cours	En poste
26	KAMTO Eutrophe Le Doux	Chargé de Cours	En poste
27	NGONO BIKOBO Dominique Serge	Chargé de Cours	En poste
28	NOTE LOUGBOT Olivier Placide	Chargé de Cours	Chef Service/Minesup
29	OUAHOUO WACHE Blandine M.	Chargée de Cours	En poste
30	TAGATSING FOTSING Maurice	Chargé de Cours	En poste
31	ZONDENDEGOUMBA Ernestine	Chargée de Cours	En poste
32	NGOMO Orléans	Chargée de Cours	En poste
33	NGNINTEDO Dominique	Assistant	En poste
6- DÉPARTEMENT D'INFORMATIQUE (IN) (25)			
1	ATSA ETOUNDI Roger	Professeur	*Chef DivSys.des systèmes d'information au MINESUP*
2	FOUDA NDJODO Marcel Laurent	Professeur	*Chef Dpt ENS/Chef DivSys.MINESUP*
3	NDOUNDAM Réné	Maître de Conférences	En poste
4	KOUOKAM KOUOKAM E. A.	Chargé de Cours	En poste
5	CHEDOM FOTSO Donatien	Chargé de Cours	En poste
6	MELATAGIA YONTA Paulin	Chargé de Cours	En poste
7	MOTO MPONG Serge Alain	Chargé de Cours	En poste
8	TINDO Gilbert	Chargé de Cours	En poste
9	TSOPZE Norbert	Chargé de Cours	En poste
10	WAKU KOUAMOU Jules	Chargé de Cours	En poste
11	TAPAMO Hyppolite	Chargé de Cours	En poste
12	ABESSOLO ALO'O Gislain	Assistant	En poste
13	BAYEM Jacques Narcisse	Assistant	En poste
14	DJOUWE MEFFEJA Merline Flore	Assistante	En poste

15	DOMGA KOMGUEM Rodrigue	Assistant	En poste
16	EBELE Serge	Assistant	En poste
17	HAMZA Adamou	Assistant	En poste
18	KAMDEM KENGNE Christiane	Assistante	En poste
19	KAMGUEU Patrick Olivier	Assistant	En poste
20	KENFACK DONGMO Clauvice V.	Assistant	En poste
21	MEYEMDOU Nadège Sylvianne	Assistante	En poste
22	MONTHE DJIADEU Valery M.	Assistant	En poste
23	JIOMEKONG AZANZI Fidel	Assistant	En poste
7- DÉPARTEMENT DE MATHÉMATIQUES (MA) (35)			
1	BEKOLLE David	Professeur	*Vice-Recteur UN*
2	BITJONG NDOMBOL	Professeur	*En poste*
3	DOSSA COSSY Marcel	Professeur	En poste
4	AYISSI Raoult Domingo	Maître de Conférences	**Chef de Département**
5	EMVUDU WONO Yves S.	Maître de Conférences	*CD/ MINESUP /Chef de Département (IN)*
6	NKUIMI JUGNIA Célestin	Maître de Conférences	En poste
7	NOUNDJEU Pierre	Maître de Conférences	En poste
8	TCHAPNDA NJABO Sophonie B.	Maître de Conférences	Directeur/AIMS Rwanda
9	AGHOUKENG JIOFACK Jean Gérard	Chargé de Cours	Chef Cellule MINPLAMAT
10	CHENDJOU Gilbert	Chargé de Cours	En poste
11	FOMEKONG Christophe	Chargé de Cours	En poste
12	KIANPI Maurice	Chargé de Cours	En poste
13	KIKI Maxime Armand	Chargé de Cours	En poste
14	MBAKOP Guy Merlin	Chargé de Cours	En poste
15	MBANG Joseph	Chargé de Cours	En poste
16	MBEHOU Mohamed	Chargé de Cours	En poste

17	MBELE BIDIMA Martin Ledoux	Chargé de Cours	En poste
18	MENGUE MENGUE David Joe	Chargé de Cours	En poste
19	NGUEFACK Bernard	Chargé de Cours	En poste
20	POLA DOUNDOU Emmanuel	Chargé de Cours	En poste
21	TAKAM SOH Patrice	Chargé de Cours	En poste
22	TCHANGANG Roger Duclos	Chargé de Cours	En poste
23	TCHOUNDJA Edgar Landry	Chargé de Cours	En poste
24	TETSADJIO TCHILEPECK M. E.	Chargée de Cours	En poste
25	TIAYA TSAGUE N. Anne-Marie	Chargée de Cours	En poste
26	DJIADEU NGAHA Michel	Assistant	En poste
27	MBIAKOP Hilaire George	Assistant	En poste
28	NIMPA PEFOUNKEU Romain	Assistant	En poste
29	TANG AHANDA Barnabé	Assistant	Directeur/MINTP
8- DÉPARTEMENT DE MICROBIOLOGIE (MIB) (12)			
1	ESSIA NGANG Jean Justin	Professeur	DRV/IMPM
2	ETOA François Xavier	Professeur	Chef de Département Recteur Université de Douala
3	NWAGA Dieudonné M.	Maître de Conférences	En poste
4	NYEGUE Maximilienne Ascension	Maître de Conférences	En poste
5	SADO KAMDEM Sylvain Leroy	Maître de Conférences	En poste
6	BOYOMO ONANA	Maître de Conférences	En poste
7	RIWOM Sara Honorine	Maître de Conférences	En poste
8	BODA Maurice	Chargé de Cours	En poste
9	BOUGNOM Blaise Pascal	Chargé de Cours	En poste
10	ESSONO OBOUGOU Germain G.	Chargé de Cours	En poste
11	NJIKI BIKOÏ Jacky	Chargée de Cours	En poste
12	TCHIKOUA Roger	Chargé de Cours	En poste

9.DEPARTEMENT DE PYSIQUE(PHY)			
1	ESSIMBI ZOBO Bernard	Professeur	En poste
2	KOFANE Timoléon Crépin	Professeur	En poste
3	NDJAKA Jean Marie Bienvenu	Professeur	**Chef de Département**
4	NJOMO Donatien	Professeur	En poste
5	PEMHA Elkana	Professeur	En poste
6	TABOD Charles TABOD	Professeur	Doyen Univ/Bda
7	TCHAWOUA Clément	Professeur	En poste
8	WOAFO Paul	Professeur	En poste
9	EKOBENA FOUDA Henri Paul	Maître de Conférences	*Chef Division. UN*
10	NJANDJOCK NOUCK Philippe	Maître de Conférences	*Sous Directeur/ MINRESI*
11	BIYA MOTTO Frédéric	Maître de Conférences	**DG/HYDRO Mekin**
12	BEN- BOLIE Germain Hubert	Maître de Conférences	CD/ENS/UN
13	DJUIDJE KENMOE épouse ALOYEM	Maître de Conférences	En poste
14	NANA NBENDJO Blaise	Maître de Conférences	En poste
15	NOUAYOU Robert	Maître de Conférences	En poste
16	SIEWE SIEWE Martin	Maître de Conférences	En poste
17	ZEKENG Serge Sylvain	Maître de Conférences	En poste
18	EYEBE FOUDA Jean sire	Maître de Conférences	En poste
19	FEWO Serge Ibraïd	Maître de Conférences	En poste
20	HONA Jacques	Maître de Conférences	En poste
21	OUMAROU BOUBA	Maître de Conférences	*En poste*
22	SAIDOU	Maître de Conférences	Sous Directeur/Minresi
23	SIMO Elie	Maître de Conférences	En poste
24	BODO Bernard	Chargé de Cours	En poste
25	EDONGUE HERVAIS	Chargé de Cours	En poste

26	FOUEDJIO David	Chargé de Cours	En poste
27	MBANE BIOUELE	Chargé de Cours	En poste
28	MBINACK Clément	Chargé de Cours	En poste
29	MBONO SAMBA Yves Christian U.	Chargé de Cours	En poste
30	NDOP Joseph	Chargé de Cours	En poste
31	OBOUNOU Marcel	Chargé de Cours	DA/Univ Inter Etat/Sangmalima
32	TABI Conrad Bertrand	Chargé de Cours	En poste
33	TCHOFFO Fidèle	Chargé de Cours	En poste
34	VONDOU Derbetini Appolinaire	Chargé de Cours	En poste
35	WOULACHE Rosalie Laure	Chargée de Cours	En poste
36	ABDOURAHIMI	Chargé de Cours	En poste
37	ENYEGUE A NYAM épse BELINGA	Chargée de Cours	En poste
38	WAKATA née BEYA Annie	Chargée de Cours	*Sous Directeur/ MINESUP*
39	MVOGO ALAIN	Chargé de Cours	*En poste*
40	CHAMANI Roméo	Assistant	En poste
41	MLI JOELLE LARISSA	Assistante	*En poste*
10- DÉPARTEMENT DE SCIENCES DE LA TERRE (ST) (42)			
1	NDJIGUI Paul Désiré	Professeur	**Chef de Département**
2	BITOM Dieudonné	Professeur	*Doyen / FASA / UDs*
3	NZENTI Jean-Paul	Professeur	En poste
4	KAMGANG Pierre	Professeur	En poste
5	MEDJO EKO Robert	Professeur	*Coseiller Technique/UYII*
6	FOUATEU Rose épse YONGUE	Maître de Conférences	En poste
7	NDAM NGOUPAYOU Jules-Rémy	Maître de Conférences	En poste
8	NGOS III Simon	Maître de Conférences	DAAC/Uma
9	NJILAH Isaac KONFOR	Maître de Conférences	En poste

10	NKOUMBOU Charles	Maître de Conférences	En poste
11	TEMDJIM Robert	Maître de Conférences	En poste
12	YENE ATANGANA Joseph Q.	Maître de Conférences	*Chef Div. /MINTP*
13	ABOSSOLO née ANGUE Monique	Maître de Conférences	*Chef div. DAASR / FS*
14	GHOGOMU Richard TANWI	Maître de Conférences	CD/UMa
15	MOUNDI Amidou	Maître de Conférences	*Chef Div. MINIMDT*
16	ONANA Vincent	Maître de Conférences	En poste
17	TCHOUANKOUE Jean-Pierre	Maître de Conférences	En poste
18	ZO'O ZAME Philémon	Maître de Conférences	*DG/ART*
19	MOUNDI Amidou	Maître de Conférences	*CT/ MINIMDT*
20	BEKOA Etienne	Chargé de Cours	En poste
21	BISSO Dieudonné	Chargé de Cours	*Directeur/Projet Barrage Memve'ele*
22	ESSONO Jean	Chargé de Cours	En poste
23	EKOMANE Emile	Chargé de Cours	En poste
24	FUH Calistus Gentry	Chargée de cours	*Sec. D'Etat/MINMIDT*
25	GANNO Sylvestre	Chargé de Cours	En poste
26	LAMILEN BILLA Daniel	Chargé de Cours	En poste
27	MBIDA YEM	Chargé de Cours	*En poste*
28	MINYEM Dieudonné-Lucien	Chargé de Cours	*CD/Uma*
29	MOUAFO Lucas	Chargé de Cours	En poste
31	NGO BELNOUN Rose Noël	Chargée de Cours	En poste
32	NGO BIDJECK Louise Marie	Chargée de Cours	En poste
33	NGUETCHOUA Gabriel	Chargé de Cours	CEA/MINRESI
34	NYECK Bruno	Chargé de Cours	En poste
35	TCHAKOUNTE J. épse NOUMBEM	Chargée de Cours	*CT / MINRESI*
36	METANG Victor	Chargé de cours	En poste

37	NOMO NEGUE Emmanuel	Chargé de cours	En poste
38	TCHAPTCHET TCHATO De P.	Chargé de cours	En poste
39	TEHNA Nathanaël	Chargé de cours	En poste
40	TEMGA Jean Pierre	Chargé de cours	En poste
41	MBESSE CECILE OLIVE	Chargée de cours	En poste
42	ELISE SABABA	Chargé de cours	En poste
43	EYONG JOHN TAKEM	Assistant	En poste
44	ANABA ONANA Achille Basile	Assistant	En poste

Répartition chiffrée des Enseignants de la Faculté des Sciences de l'Université de Yaoundé I

NOMBRE D'ENSEIGNANTS					
DÉPARTEMENT	**Professeurs**	**Maîtres de Conférences**	**Chargés de Cours**	**Assistants**	**Total**
B.C.	5 (1)	10 (5)	19 (10)	3 (1)	**38 (16)**
B.P.A.	11 (1)	9 (3)	20 (8)	3 (5)	**43 (17)**
B.P.V.	4 (0)	9(2)	10 (2)	4 (4)	**27 (8)**
C.I.	9(1)	8(2)	16 (4)	0 (2)	**33 (9)**
C.O.	8 (0)	13 (3)	8 (2)	1 (0)	**30 (5)**
I.N.	3 (0)	1 (0)	8 (0)	12 (3)	**24 (3)**
M.A.	3 (0)	5 (0)	18 (1)	4 (0)	**30 (1)**
M.B.	2 (0)	5 (2)	5 (2)	0 (0)	**12 (4)**
P.H.	8 (0)	17 (0)	15 (2)	2 (1)	**42 (3)**
S.T.	5 (0)	15 (2)	22 (3)	2 (0)	**44 (5)**
Total	**58 (3)**	**92(19)**	**142 (33)**	**31(16)**	**323(71)**

Soit un total de **323(**71**)** dont :

- Professeurs **58 (3)**
- Maîtres de Conférences **92 (**19**)**
- Chargés de Cours **142 (33)**
- Assistants **31** (16**)**

( ) = Nombre de Femmes

Remerciements

Mes premiers remerciements iront au professeur Thomas DJOTIO NDIÉ mon directeur de thèse, pour m'avoir soutenu durant toute ma thèse. J'aimerais lui adresser toute ma gratitude pour toutes ses remarques et suggestions techniques, académiques et professionnelles. Il a toujours su me consacrer des moments de son temps, me guider, me conseiller, et me témoigner son soutien et sa confiance.

Je tiens à témoigner ma reconnaissance au professeur MAURICE TCHUENTE qui m'a accueilli dans ses entités de recherche, respectivement au sein du laboratoire de recherche LIRIMA et d'avoir ainsi permis la réalisation de cette thèse.

Je remercie vivement Dr Gilbert NDJANPONG NANA pour sa contribution scientifique et son soutien extraordinaire de cette thèse. Ce travail n'aurait jamais pu être tel qu'il l'est dans ce manuscrit sans lui.

Je remercie également les membres du département de Génie Informatique de l'ENSP de Yaoundé, les professeurs et les collègues du laboratoire avec qui j'ai partagé ces années de thèse avec beaucoup de bonheur.

Mes prochains remerciements ont une portée de 1500 Km. Ils s'adressent à tous les membres de ma famille résidente au Tchad: mes frères et sœurs.

Je voudrais leur exprimer toute ma profonde reconnaissance et je leur remercie du fond de mon cœur parce qu'ils m'ont constamment aidé, malgré la distance pour la plupart, par leur soutien moral et leurs encouragements pour achever cette thèse.

Je garde une place toute particulière à mon épouse Ngo Ndjem Marthe. Ton sourire angélique m'a fait et me fait toujours du bien. J'espère que je t'aiderai dans le déroulement de ta thèse et dans beaucoup d'autres domaines aussi.

Enfin, si j'ai oublié quelqu'un, je le remercie aussi, ainsi que toute autre personne qui m'a aidé de prêt ou de loin au cours de mon cheminement durant mes années de thèse.

Sommaire

LISTE DES FIGURES

LISTE DES TABLEAUX

Résumé

De nos jours, la technologie réseau et radio mobile a fait l'objet de progrès considérables. On assiste au déploiement de différentes normes des réseaux de télécommunication tels que le GSM, l'UMTS le WiMAX et les réseaux locaux sans fil comme le WiFi(IEEE802.11x). Les réseaux communautaires sans fil, se sont de plus rapidement développés avec l'apparition du WiFi grâce à leur simplicité, rapidité et faible coût de déploiement. Dès lors, ils constituent une alternative intéressante aux réseaux locaux classiques. La gestion de la mobilité dans les réseaux sans fil constitue aujourd'hui un véritable défi dans ce type de réseaux avec la prolifération des terminaux mobiles. Un utilisateur mobile peut changer son point d'accès réseau en se déplaçant, sans interrompre la session de service en cours, c'est-à-dire subir les transferts intercellulaires. Notre étude se situe au niveau des couches hautes du modèle OSI (réseau, application et transport). Le protocole IP Mobile de la couche réseau, est un protocole standardisé par l'IETF qui permet à l'utilisateur de maintenir ses communications en cours et de rester connecté à Internet tout en masquant d'une manière transparente le changement de réseau. La conception de Mobile IPv6 s'est basée sur les expériences acquises du développement de Mobile IPv4 et sur les nouvelles opportunités offertes par le protocole IPv6, telles que le nombre plus important d'adresses, les mécanismes d'auto configuration et la sécurité. Bien que le protocole IPv6 Mobile résolve le problème de mobilité dans IPv6, ce protocole ne peut pas supporter les applications en temps réel qui sont sensibles au délai ou à la perte de paquets.

En effet, dans la version standard de Mobile IP, la nouvelle localisation d'un mobile est toujours signalée à son agent parent. Ce dernier est ainsi averti de tous les déplacements des mobiles qu'il gère. Les pertes de paquets pendant les Handover peuvent être importantes puisque la procédure d'enregistrement est longue, en particulier si l'Agent parent (Home Agent-HA) se trouve à l'autre bout du monde. La durée d'un Handover peut atteindre plusieurs secondes dans l'Internet actuel.

Des améliorations de Mobile IP telles que (HMIP, hierarchical MIP), (FMIP, Fast Handover for MIP) consiste en la réduction du temps de latence du Handover et de la perte de paquets pendant un Hanover. L'idée de base du Fast Handover dans Mobile IP [10] est de permettre au nœud mobile d'obtenir sa nouvelle adresse temporaire avant d'effectuer le Hanover vers le nouveau sous-réseau afin qu'il puisse immédiatement communiquer lorsque la connexion avec son nouveau routeur d'accès est établie. Ceci nécessite une anticipation de mouvements.

Au niveau de la couche application, SIP(Protocole d'Initialisation de Session) est un protocole de contrôle de couche d'application qui peut établir, modifier et terminer les sessions multimédias, telles que les communications téléphoniques par l'Internet.

Le protocole SIP fournit la gestion de la localisation pour la mobilité des terminaux. Le protocole SIP de base ne fournit pas la gestion transparente du transfert intercellulaire [11]. Ainsi, la session SIP se termine lorsque le mobile change de réseau IP car les adresses de raccordement TCP/UDP sous-jacentes ne seront plus valides pour les nouvelles adresses IP. Cependant, le protocole SIP peut être utilisé en conjonction avec d'autres schémas de gestion du transfert intercellulaire: IP(MIP); IP cellulaire (CIP); protocole de transmission de commande de flux mobile (mSCTP, mobile Stream control transmission Protocol).

Parmi les protocoles de mobilité au niveau transport, nous nous intéressons aux protocoles SCTP/mSCTP vu les dispositifs qu'ils offrent. SCTP implémente deux nouveaux mécanismes, le Multihoming et le multisteaming qui le rendent très fiable pour la gestion de la mobilité et des pertes négligeables de paquets. Le mécanisme de Multihoming permet la gestion des adresses IP, le contrôle des adresses empruntées (ou des chemins) et le transfert de données dans une association. La modélisation du protocole de mobilité mSCTP à l'aide de la chaine de Markov nous a permis de choisir le paramètre **δ(seuil fixe ou variable)**permettant le déplacement libre du mobile dans les cellules de grandes probabilités retenu par le protocole.

De plus, dans un contexte où les usagers mobiles engagent de plus en plus d'applications sensibles au délai, la gestion de la mobilité demeure un enjeu prioritaire, exigeant la qualité de service(QoS).

Des fonctions d'agrégation nous ont permis d'apporter un jugement quantifiable sur plusieurs transitions intercellulaires pouvant monter la qualité de service pour les applications de type audio et vidéo. Pour atteindre un consensus sur ces jugements, deux fonctions d'agrégation ont été proposées: la moyenne arithmétique et quasi-linéaire. Le choix est porté sur la moyenne quasi-linéaire grâce au paramètre $\mathbf{w_i}$ **(puissance du signale**), qui représente les poids du Handover et dépend également de l'altitude entre deux antennes en interférence, et aussi les obstacles géographiques.

MOTS CLES :

Réseaux communautaires sans fil (WCN), mobilité, Chaine de Markov, Protocoles de mobilités SCTP/mSCTP, Multihoming, fonctions d'agrégations, qualité de service(QoS).

Abstract

Nowadays, network and mobile radio technology has made considerable progress. We are witnessing the deployment of different telecommunication network standards such as GSM, UMTS WiMAX and wireless local networks such as WiFi (IEEE802.11x). Community wireless networks have also rapidly developed with the arrival of WiFi thanks to their simplicity, speed and low cost of spreading out. Ever since, they are an interesting alternative to traditional local networks. Mobility management in wireless networks is now a real challenge in this type of network with the proliferation of mobile devices. A mobile user can change its network access point by moving, without interrupting the current service session, that is, to undergo handoffs. Our study is based on the high layers of the OSI model (network, application and transport). The Network layer IP Mobile Protocol is by IETF-standardized protocol that allows the user to maintain current communications and stay connected to the Internet while seamlessly masking the network change. The design of Mobile IPv6 was based on the experiences gained from the development of Mobile IPv4 and the new opportunities offered by IPv6, such as the larger number of addresses, self-configuration and security mechanisms. Although IPv6 Mobile protocol solve addresses the problem of mobility in IPv6, this protocol can not support applications in real time that are sensitive to delay or loss of packets.

Indeed, in the standard version of Mobile IP, the new location of a mobile is always reported to its home agent. The latter is thus notified of all the movements of the mobiles he manages. The loss of some Packets during handovers can be important since the registration process is long, especially if the Home Agent-HA is at the other end of the world. The duration of a handover can reach several seconds in the current Internet.

Mobile IP improvement, such as (HMIP, hierarchical MIP), (FMIP, Fast Handover for MIP) is the reduction of handover latency and the loss of packets during a Hanover. The basic idea of the Fast Handover in Mobile IP [10] is to allow the mobile node to obtain its new temporary address before performing the Hanover to the new subnet so that it can immediately communicate when the connection with its new access router is established. This requires an anticipation of movements.

At the application layer level, SIP (Session Initialization Protocol) is control protocol application layer that can establish, modify, and terminate multimedia sessions, such as telephone communications over the Internet.

The SIP protocol provides location management for terminal mobility. The basic SIP protocol does not provide transparent management of handoff [11]. Thus, the SIP session

ends when the mobile changes IP network because the underlying TCP / UDP connection addresses will no longer be valid for the new IP addresses. However, SIP protocol can be used in conjunction with other Handover Management schemes: Mobile IP (MIP); Cellular IP (CIP) mobile stream control transmission protocol (mSCTP).

Among the mobility protocols at the transport level, our concern is in the SCTP / mSCTP protocols given the devices they offer. SCTP implements two new mechanisms, Multihoming and multisteaming that make it very reliable for mobility management and insignificant packet losses. The Multihoming mechanism allows the management of IP addresses, the control of borrowed addresses (or paths) and the transfer of data in an association. The modeling of the mSCTP mobility protocol using the Markov chain allowed us to choose the parameter**δ (fixed or variable threshold)** allowing the free movement of the mobile in the cells of high probability cells retained by the protocol.

In addition, in a context where mobile users are engaging more and more sensitive applications in time, mobility management remains a priority issue, requiring quality of service (QoS).

Aggregation functions have allowed us to make a quantifiable judgment on several intercellular transitions that can increase the quality of service for audio and video applications. To reach a consensus on these judgments, two aggregation functions have been proposed: the arithmetic and quasi-linear average. The choice is focused on the quasi-linear average thanks to the parameter **w_i (power of the signal),** which represents the weight of the handover and also depends on the altitude between two antennas in interference, and also the geographical obstacles.

Keywords:

Wireless community networks (WCN), mobility, Markov chain, SCTP / mSCTP mobility protocols, Multihoming, aggregation functions, quality of service (QoS).

Chapitre I
Introduction

I.1 Contexte et problématique

Les systèmes de télécommunication ont subi en l'espace de deux décennies des évolutions et bouleversements profonds. De nos jours, on assiste à un développement rapide de plusieurs réseaux utilisant des technologies différentes. Ainsi, on a accès au GMS, l'UMTS et au WiMAX dans les réseaux de télécommunications, aux réseaux locaux sans-fil IEEE 802.11(WiFi).

Les réseaux sans fil sont en plein développement du fait de la flexibilité de leur interface qui permet aux utilisateurs de se communiquer directement entre eux ou de se connecter facilement à Internet en onde radio, sans mettre en place préalablement d'infrastructures lourdes, telles que des câbles filaires.

Parmi ces différentes technologies de réseaux de télécommunication(GSM,UMTS, WiMAX) et des réseaux locaux sans fil WLAN (Wireless Local Area Network), utilisant la norme l'IEEE 802.11x/WiFi, la norme l'IEEE 802.11x/WiFi est la plus connue et utilisée pour construire un réseau sans fil à haut débit dans une zone à forte concentration d'utilisateurs, telle que les aéroports, les gares, les campus les sites industriels, etc. Le succès du WiFi est non seulement dû à ses performances, mais aussi au coût des matériels plus acceptable et à son implantation simple et rapide [8,9].Naturellement, les utilisateurs qui se servent de réseaux WiFi souhaitent pouvoir se déplacer tout en améliorer la qualité de service(QoS).

Nous notons également qu'en 1985, la U.S. Fédéral Communications Commission (FCC) a décidé de libérer les bandes réservées aux usages industriels, scientifiques et médicaux (ISM) comprises entre 902 et 928 MHz, 2,4 et 2,483 GHz, et 5,725 et 5,875 GHz, pour utilisation publique sans licence pour la technologie WLAN[14].

La norme 802.11x(WiFi) doit une grande partie de son succès aux initiatives aux réseaux communautaires[1] tels que les réseaux sans fil maillé WiFi(Mesh) pour tenter d'avoir une couverture wifi importante sur des sites de plus ou moins grandes envergures. Ce maillage permet ainsi de partager des connexions internet. Nous vous proposons dans la figure 1 une architecture sans fil maillée wifi, vu son succès dans la construction des réseaux sans fil maillé.

[1] Un réseau communautaire est un réseau maillé formé exclusivement par un ensemble d'utilisateurs qui coopèrent entre eux pour la réalisation de certaines applications ou services.

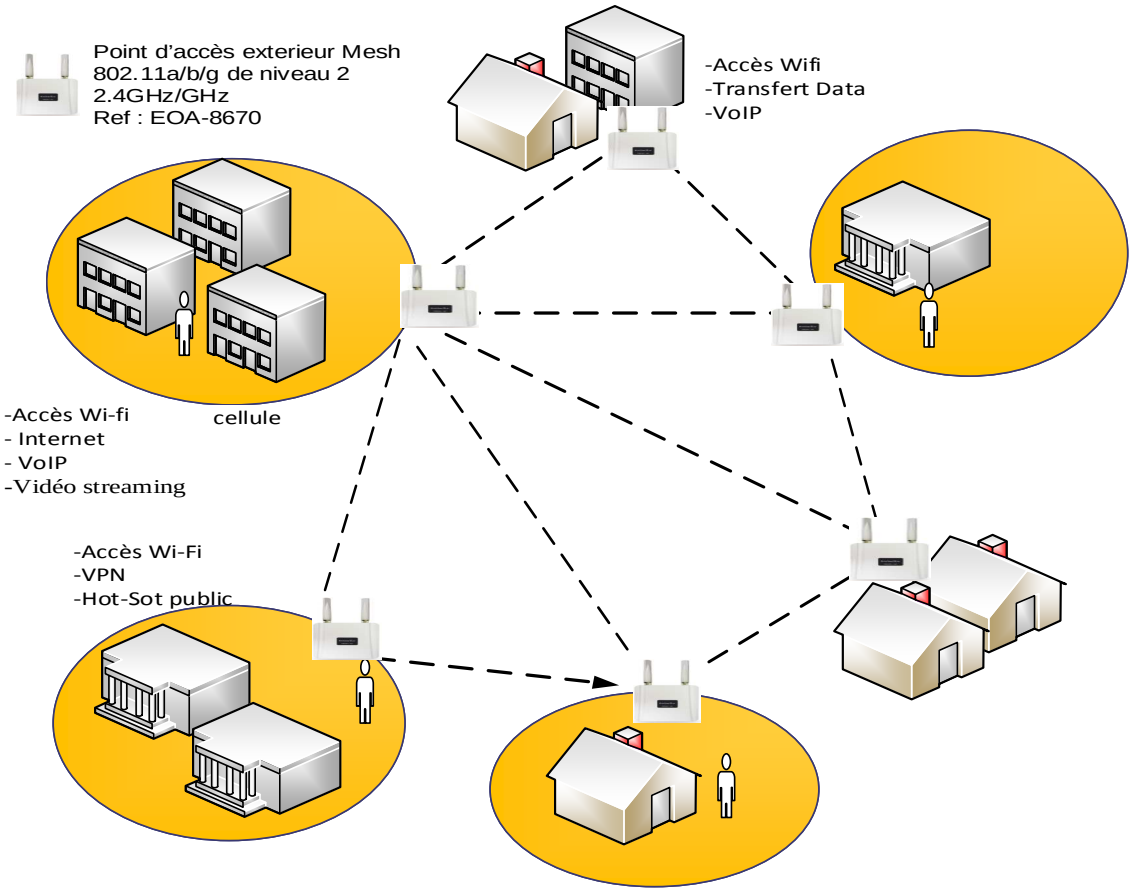


Figure 1 : représentation d'une architecture des réseaux communautaires sans fil.

Cette architecture de réseau communautaire sans fil comprend: un accès sans fil (WI-FI) sur tous les sites; les point d'accès extérieur Mesh 802.11a/b/g de niveau 2 2.4GHz/5GHz; un Hot Spots permettant un accès Internet par WiFi; Le VPN SSL permet de garantir la sécurité des accès aux ressources du réseau interne en utilisant un tunnel SSL entre le client (connecté à un réseau public).

Dans le cadre de cette thèse, nous nous focaliserons, en particulier, sur la gestion de mobilité qui ne désigne pas uniquement la capacité d'un nœud à se déplacer, mais englobe également d'autres questions qui lui sont liées:

- la gestion de la localisation (identifier la localisation du réseau en cours d'un terminal mobile (MT, mobile terminal) et de garder sa trace lorsqu'il se déplace);
- la gestion du transfert intercellulaire(Handover) qui sert à fournir aux mobiles la continuité de session et les possibilités de Multihoming.

Le problème de performance pure du à la latence du Handover (transfert intercellulaire) pour la mobilité des applications dites «temps réelle», peut entrainer de perte de paquet perceptible par l'utilisateur et des interruptions de connexion et de communication.

Ce processus de gestion de mobilité devrait se faire d'une façon transparente pour l'utilisateur. Nous souhaitons également que le réseau garantit la qualité de service (QoS) lors de la mobilité des utilisateurs au sein d'un domaine, les critères de la qualité de service auront une pondération encore plus importante dans les solutions de mobilité proposées vu que les utilisateurs solliciteront d'avantage les applications et les services multimédia.

Nos travaux de la gestion de la mobilité ont été mené sur les couches hautes du modèle OSI (réseau, application et transport), d'où le choix est porté sur le protocole de transport SCTP (Stream Control Transmission Protocol), comparé aux protocoles de transport usuels, présente une meilleure fiabilité grâce à ses principales caractéristiques(Multihoming, Multisteaming), et le Mobile SCTP(mSCTP) qui donne la possibilité au client mobile de passer automatiquement d'une station à une autre sans perte de connexion.

I.2 Motivations et Contributions

La mobilité des utilisateurs et leurs besoins d'accès itinérant aux réseaux informatiques rendent les réseaux traditionnels (filaires) obsolètes. De plus, le besoin accru d'accéder à différents types d'applications via le support radio pousse la recherche vers de nouvelles solutions de plus en plus adaptées à cet environnement. Ainsi, on note ces dernières années des avancées rapides dans la standardisation de nombreuses technologies sans fils allant des réseaux personnels à faible couverture jusqu'aux réseaux à couverture mondiale. Dans notre étude, nous nous intéressons au standard 802.11x, nommé également WiFi (Wireless Fidelity) ou WLAN. Les réseaux locaux sans fil du standard 802.11x, sont des réseaux peu couteux qui ont une couverture de quelques centaines de mètres et qui interconnectent facilement les équipements informatiques de l'entreprise, des universités, des centres de recherches, du domicile, etc. Ces réseaux permettent un débit allant de quelques Mbit/s à quelques centaines de Mbit/s. Plusieurs protocoles de mobilité au niveau des couches haute du modèle OSI (réseau, application et transport) ont été mis sur pieds, d'où Parmi ces protocoles de mobilité, nous nous intéressons aux protocoles SCTP/mSCTP vu les dispositifs qu'ils offrent(le Multihoming et le multisteaming) qui les rendent très fiables pour la gestion de la mobilité.

Notre première contribution pour assurer la mobilité est basée sur la chaine de Markov dont les études nous ont permis de modéliser le protocole mSCTP. L'utilisation d'un vecteur probabilité $\mathbf{V=P_t(i)}$ nous permet d'identifier le mobile se trouvant dans la cellule $\mathbf{C_i}$ à

l'instant t, une matrice de transition homogène $\mathbf{M_{t+1} = P_{ij}]_{t+1}}$ qui modélise les transitions de la dynamique du système de l'instant **t** à l'instant **t+1** et le choit d'un paramètre **δ(variables)ϵ[0,1] ,** permettant au mobile de basculer dans les cellules de grandes probabilités retenu par le protocole.

Une deuxième contribution est l'application des fonctions d'agrégation qui nous ont permis d'apporter un jugement quantifiable sur plusieurs transitions intercellulaires pouvant monter la qualité de service. Pour atteindre un consensus sur ces jugements, des fonctions d'agrégation classiques ont été proposées: la moyenne arithmétique et quasi-arithmétique, la moyenne géométrique et quasi- géométrique, la médiane et bien d'autres encore. Le choix est porté sur la moyenne quasi-arithmétique grâce au paramètre $\mathbf{W_i}$ (puissance du signale), qui représente les poids du Handover et dépend également de l'altitude entre deux antennes en interférence, et aussi les obstacles géographiques, d'ou $W_i \in [0,1]$ et $\sum_{i=1}^{n} W_i = 1$

I.3 Organisation de la thèse

Le plan de la thèse se présente de la façon suivante:

Le chapitre 2 nous présente les différents types de réseaux mobiles et sans fil, ainsi que les différentes approches qui ont abordé la question mobilité, en nous intéressant au réseau local sans fil WLAN utilisant la norme IEEE 802.11/WiFi choisit comme réseau promoteur pour la construction des réseaux communautaires sans fil, compte tenu des avantages qu'ils présentent. A la suite nous faisons un rappel des protocoles IPv4 et IPv6, nous montrons les limitations d'IPv4 qui ont conduit à la transition vers IPv6 et les améliorations qu'apporte le protocole IPv6. Pour finir nous consacrons une grande partie de ce chapitre à la description en détail les protocoles de mobilité au niveau des couches hautes du modèle OSI (réseau, application et transport). Les avantages et les inconvénients de chaque protocole nous ont permis de choisir les protocoles du niveau transport SCTP/mSCTP pour la gestion de la mobilité des réseaux communautaires sans fil compte tenu des avantages qu'ils présentent par rapport aux autres.

Le Chapitre 3 contient notre première contribution. Nous avons fait recours aux chaines de Markov pour la modélisation du protocole mSCTP. Les résultats obtenus par simulation proposés sous la plateforme Matlab, nous ont permis de choisir un paramètre $\boldsymbol{\delta} \in [0,1]$. Ce paramètre nous permet de sélectionner les cellules de grandes probabilités.

Le Chapitre 4 détaille notre deuxième contribution. Dans celui-ci, l'exploitation des fonctions d'agrégation nous permet de montrer une amélioration de la qualité de service(QoS) de type audio et plus excellente de type vidéo par rapport à la précédente.

Cette thèse se termine par une conclusion et les perspectives. Nos travaux de recherche apportent une publication au journal **I**nternational **J**ournal of **E**ngineering and **T**echnology **(IJET**). Sous la référence: DOI: 10.21817/ijet/2017/v9i4/170904405.

Chapitre II
Gestion de la mobilité dans les réseaux IEEE 802.11x: Etat de l'Art

II.1 Réseaux Mobiles et Sans fil

Introduction

L'unité de base de la communication sans fil est l'onde radio. C'est en 1864 que James Clerc Maxwell, un physicien britannique, met en évidence l'existence des ondes électromagnétique. En 1988, Heinrich Hertz, un physicien allemand, prouve que le champ magnétique se propage à la vitesse de la lumière. Ces ondes électromagnétiques sont appelées plus souvent onde radioélectriques ou ondes hertziennes.

L'onde radio révolutionne, plus tard, le monde de la communication sans fil et entre autre les réseaux de données et les réseaux cellulaires. Avant l'utilisation de l'onde radio comme moyen de transmission, les réseaux de communication étaient limités à une structure câblée qui est lourde et coûteuse. La mobilité et le coût minime de l'installation des réseaux de communications sans fil ont favorisé leur développement par rapport aux réseaux câblés.

II.1.1 Les réseaux mobiles

Avec sa première apparition, le réseau mobile était une version analogique connue sous le nom de première génération (1G). Cette génération était limitée du point de vue technologique ce qui a évoqué une évolution de la technologie utilisée par le cellulaire mobile permettant de passer de l'analogique au numérique. Deux grands organismes ont travaillé sur l'évolution de la première génération: la **C**onférence des Administrations **E**uropéennes des **P**ostes et **T**élécommunications (**CEPT**) et l'**E**uropean **T**elecommunications **S**tandard Institute (**ETSI**). La nouvelle génération est numérique et sera nommée (2G) opérant sur la bande de fréquence de 900MHZ et permettant un débit de 9,6 Kbit/s, offrant aux utilisateurs la téléphonie vocale, le fax et la transmission (modérée) de données. L'**U**nion **I**nternationale des **T**élécommunications (**UIT**) définie les normes de la troisième génération (3G) à travers l'International Mobile Telecommunication IMT-2000. Ces spécifications permettront la transmission des données multimédia telles que la vidéo, la vidéo-conférence et l'accès à Internet haut débit. Les principaux standards sont :

i. Global System for Mobile communications (GSM)

Idéal pour la communication de type voix où les ressources ne seront allouées que pour la durée de la conversation. Mis au point par la **CETP** (**C**onférence **E**uropéenne des **A**dministrations des **P**ostes et **T**élécommunications) en 1991 et permet un débit de 9,6

kbit/seconde autour des fréquences 900 Mhz et 1800 Mhz [3, 4, 5]. Le GSM transmet facilement des données numériques de faible volume tel que le Short Message Service (SMS) et les Multi Média Messages (MMS).

ii. General Packet Radio System (GPRS)

General Packet Radio Service (GPRS) nommé génération (2.5G), est une évolution importante du GSM. L'objectif principal de cette évolution est d'accéder aux réseaux IP. Le débit théorique est de l'ordre de 171, 2 kbit/s et réel, de 30 kbit/s[5,6].

iii. Universal Mobile Telecommunication System (UMTS)

Appelé également troisième génération (3G) [6,7], a été développé en 2004 fonctionne sur la bande de fréquences 1900-2000 MHz et permet un débit réel de l'ordre de 384 Kbits/s (8 fois plus rapide que le GPRS). Sa bande de fréquence de fonctionnement est 1900MHz-2000MHz. L'UMTS est compatible avec tous les réseaux du monde du fait de la possibilité de roaming au niveau mondial. Grâce à son débit, l'UMTS ouvre la porte à des applications et services nouveaux (Vidéo Conférence, Audio conférence, Télémédecine, Courier électronique, Télévision, Etc.). Le tableau 1 retrace les principales caractéristiques des standards de la téléphonie cellulaire.

Standard	Génération	Caractéristiques	Débit réel
GSM	2G	Permet le transfert de la voix ou des données numériques de faible volume	9,6 Kbit/s
GPRS	2.5G	Permet le transfert de la voix ou des données numériques de volume modéré	144 Kbit/s
UMTS	3G	Permet le transfert simultané de la voix et des données numériques à haut débit	384 Kbit/s

Tableau 1 : Évolution et caractéristique de la téléphonie cellulaire.

II.1.2. Les réseaux locaux sans fil (Wireless Local Area Network, WLAN)

La portée d'un réseau locaux sans fil (WLAN) est de quelques centaines de mètres (300mètres), il est utilisé souvent dans les entreprises (aéroports, universités, les cafés, etc.), pour former un réseau local sans fil afin de connecter des ordinateurs et des imprimantes. Un exemple très connu de ce type de réseau est le WiFi dont le débit théorique peut atteindre

54Mbp/s et la portée plusieurs centaines de mètres. Notons qu'en 1985, la U.S. Federal Communications Commission (FCC) a décidé de libérer les bandes réservées aux usages industriels, scientifiques et médicaux (ISM) comprises entre 902 et 928 MHz, 2,4 et 2,483 GHz, et 5,725 et 5,875 GHz, pour utilisation publique sans licence[15]. Non seulement cette décision répondait-elle à une demande du secteur des communications commerciales, mais elle a été le point de départ du développement de la technologie WLAN.

II.1.2.1 Le standard IEEE 802.11(WiFi)

C'est un des standards qui permet de déployer un réseau sans fil en faisant communiquer plusieurs appareils (ordinateur, téléphone portable, assistant personnel (PDA), etc.) ensemble, à travers les ondes radioélectriques et ceci à une liaison haut débit sur un rayon de couverture pratiquement égal à quelques dizaines de mètres [22]. La norme **IEEE 802.11** offrait un débit entre 1 et 2 Mbp/s. Pour des raisons d'amélioration de la performance (portée, débit, etc.), cette norme a subi plusieurs évolutions à travers l'apparition de différentes versions. Une brève description de ces évolutions les plus utilisés, suivant la chronologie, est donnée ci-dessous.

Lanorme**IEEE802.11a** offre un débit théorique de 54 Mbps (30Mbps réels). Elle spécifie 8 canaux radio dans la bande de fréquence des 5 GHz. L'IEEE802.11b est la norme WiFi la plus répandue actuellement. Son débit théorique est de 11 Mbps (6Mbps réels) avec une portée pouvant aller jusqu'à 300mètres et spécifie 3 canaux radio dans la bande de fréquence des 2.4 GHz. La norme **IEEE802.11g** offre un haut débit (54 Mbps théoriques, 30 Mbps réels) sur la bande de fréquence de 2.4 GHz, compatible avec la 802.11b. Quant à l'IEEE **802.11n** son but est d'étendre le standard 802.11 pour atteindre un débit de 540 Mbit/s tout en assurant une rétrocompatibilité avec les trois précédents amendements (a, b et g). Il utilise les deux bandes 2,4 et 5 GHz.

II.1.2.2 Les différentes topologies de norme 802.11/WI-FI

Le standard 802.11 définit deux modes opératoires: Le mode Infrastructure dans lequel les clients sans fil sont connectés à un PA (Point d'Accès ou Access Point en anglais). Il s'agit généralement du mode par défaut des cartes 802.11b; Le mode Ad Hoc dans lequel les clients sont connectés les uns aux autres sans aucun PA.

II.1.2.2.1 Le mode Infrastructure

En mode Infrastructure, chaque TM (Terminal Mobile) se connecte à un PA(Access Point, point d'accès) via une liaison sans fil. L'ensemble formé par le PA et les TM situés dans sa zone de couverture est appelé BSS (Basic Set Service soit cellule de base) et constitue une cellule. Chaque BSS est identifié par un BSSID, un identifiant de 6 octets (48 bits). Dans le mode Infrastructure, le BSSID correspond à l'adresse MAC du PA.

Il est possible de relier plusieurs PA entre eux (ou plus exactement plusieurs BSS) par une liaison appelée DS (Distribution System soit système de distribution) afin de constituer un ESS (Extended Service Set soit ensemble de services étendu). Le DS peut être aussi bien un réseau filaire qu'un réseau sans fil, mais les équipements nécessaires à cette dernière solution ne sont pas encore forcément implémentés.

Un ESS est repéré par un ESSID (ESS Identifier), c'est-à-dire un identifiant de 32 caractères de long (au format ASCII) servant de nom pour le réseau. L'ESSID, souvent abrégé en SSID, représente le nom du réseau et représente en quelque sorte un premier niveau de sécurité dans la mesure où la connaissance du SSID est nécessaire pour qu'un TM se connecte au réseau étendu. La figure 2 nous présente l'architecture en mode infrastructure.

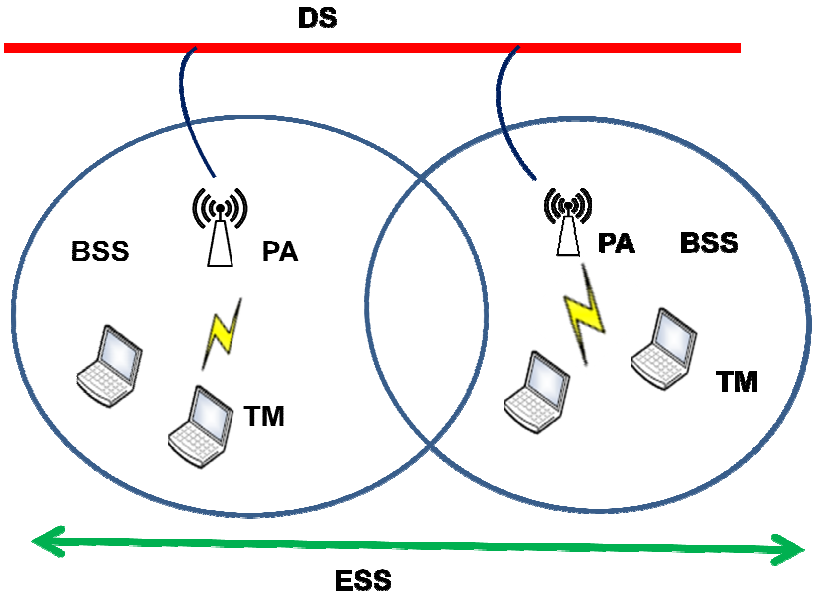


Figure 2: Illustration d'une architecture 802.11 en mode Infrastructure

La communication avec le point d'accès

Lors de l'entrée d'un TM (Terminal Mobile) dans une cellule, celui-ci diffuse sur chaque canal une requête de sondage (probe request) contenant l'ESSID pour lequel il est

configuré ainsi que les débits qu'il supporte. Si aucun ESSID n'est configuré, le TM écoute le réseau à la recherche d'un ESSID. En effet, chaque PA diffuse régulièrement (à raison d'un envoi toutes les 0.1 secondes environ) une trame balise (nommée beacon en anglais) donnant des informations sur son BSSID, ses caractéristiques et éventuellement son ESSID. L'ESSID est automatiquement diffusé par défaut, mais il est possible (et recommandé) de désactiver cette option.

A chaque requête de sondage reçue, le PA vérifie l'ESSID et la demande de débit présent dans la trame balise. Si l'ESSID correspond à celui du PA, ce dernier envoie une réponse contenant des informations sur sa charge et des données de synchronisation. Le TM recevant la réponse peut ainsi constater la qualité du signal émis par le PA afin de juger de la distance à laquelle il se situe. En effet d'une manière générale, plus un PA est proche, meilleur est le débit.

Un TM se trouvant à la portée de plusieurs PA (possédants bien évidemment le même SSID) pourra ainsi choisir le PA offrant le meilleur compromis de débit et de charge.

Lorsqu'un TM se trouve dans le rayon d'action de plusieurs PA, c'est donc lui qui choisit auquel se connecter.

II.1.2.2.2 Le mode Ad Hoc

En mode Ad Hoc les machines sans fil clientes se connectent les unes aux autres afin de constituer un réseau point-à-point, c'est-à-dire un réseau dans lequel chaque TM joue en même temps de rôle de client et le rôle du PA.

L'ensemble formé par les différents TM est appelé IBSS (Independent Basic Service Set soit ensemble de services de base indépendants). Un IBSS est ainsi un réseau sans fil constitué au minimum de deux TM et n'utilisant pas de PA. L'IBSS constitue donc un réseau éphémère permettant à des personnes situées dans une même salle d'échanger des données. Il est identifié par un SSID, comme l'est un ESS en mode Infrastructure.

Dans un réseau Ad Hoc, la portée du BSS indépendant est déterminée par la portée de chaque TM. Cela signifie que si deux des TM du réseau sont hors de portée l'un de l'autre (problème dit de «Hidden Node» soit nœud caché), ils ne pourront pas communiquer, même s'ils "voient" d'autres TM. En effet, contrairement au mode Infrastructure, le mode Ad Hoc ne propose pas de système de distribution capable de transmettre les trames d'un TM à un autre. Ainsi un IBSS est par définition un réseau sans fil restreint. La figure 3 nous présente l'architecture en mode Ad Hoc d'où la communication directe est impossible mais possible uniquement via les TM intermédiaires.

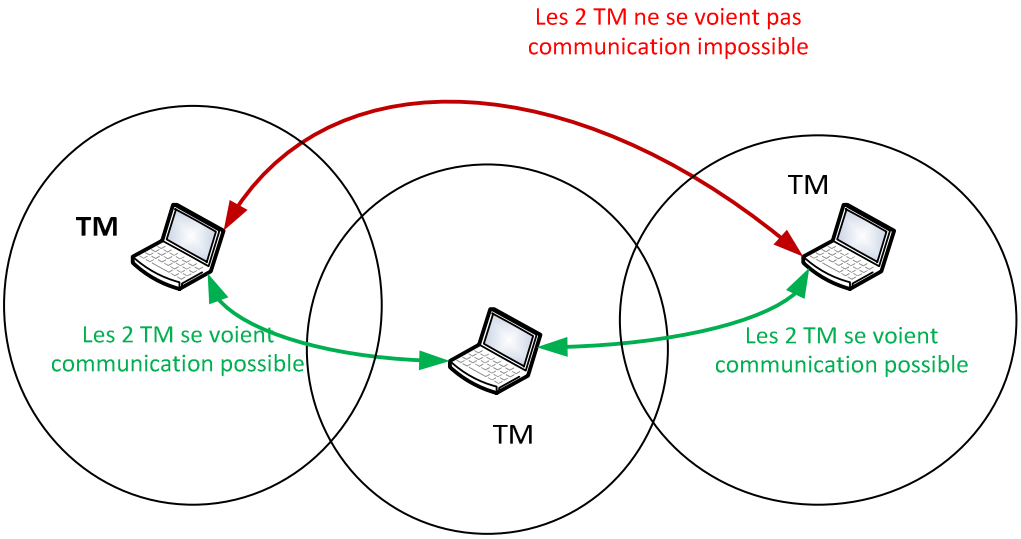


Figure 3: Illustration d'une architecture 802.11 en mode Ad Hoc

II.1.3 Le standard IEEE 802.16 : WiMAX FIXE et MOBILE

Le WiFi offre des services limités en portée, en sécurité et en mobilité et sur une étendue locale, d'où la nécessité de l'évolution des systèmes de communications sans fil. Le Worldwide Interoperability for Microwave Access (WiMAX) est apparu pour répondre aux limitations du WiFi. Il offre un service couvrant une envergure de 50 Km théoriques et un débit qui peut atteindre théoriquement 70 Mbit/s [7, 16,17]. Il faut noter que le standard WiMAX introduit la mobilité et gère le Handover aussi bien qu'il introduit un nouveau mécanisme pour la gestion de la qualité de service. Par ailleurs, WiFi opère dans des zones de fréquence non règlementées, alors que le WiMAX, quant à lui, utilise une bande de fréquence allant de 2 à 66 GHz, ce qui lui permet d'interagir avec plusieurs produits sur le marché, entre autre, avec le WiFi. Le WiMAX était d'abord conçu de telle façon que l'opérateur implante des antennes émettrices externes qui diffusent et transmettent des données sur une fréquence entre 10 et 66 GHz vers les antennes à domiciles. L'onde à haute fréquence n'étant pas, par nature, capable de pénétrer les obstacles, il faut alors que l'antenne émettrice et l'antenne réceptrice soient en ligne de vue, ce qui est connu sous le nom de diffusion en LOS (Line Of Site). Cette limitation a été résolue avec l'apparition d'une nouvelle version WiMAX connue par la norme IEEE 802.16a et qui opère sur une bande de fréquence basse de 2 à 11 GHz ce qui ne demande plus des antennes de transmission alignées face à face. Ce mode de transmission est appelé Non Line Of Site (NLOS). L'évolution du WiMAX a donné naissance à la norme IEEE 802.16d appelée aussi WiMAX fixe. Cette norme ne gère pas la mobilité, d'où la nécessité d'une nouvelle norme baptisée IEEE 802.16e également nommée WiMAX mobile qui sera capable d'offrir des services mobiles, notamment, la téléphonie sur IP opérant dans la bande de fréquence de 2 à 6 GHz. Les différences entre le débit, la portée et la bande de fréquence du WiMAX fixe et WiMAX mobile sont données dans le tableau 2.

Standard	Nom	Bande de fréquence	Débit	Portée
IEEE 802.16d	WiMAX fixe	2-11 GHz	75 Mbits/s	10 km
IEEE 802.16e	WiMAX Mobile	2-6 GHz	30 Mbits/s	3,5 km

Tableau 2: portée et bande de fréquence du WiMAX fixe et WiMAX mobile

II.2 Le Protocole IP

Le protocole IP (Internet Protocol-IP) [33,34] est un protocole standardisé par l'organisation de standardisation des protocoles de l'Internet (en anglais **I**nternet **E**ngineering **T**ask **F**orce-IETF) dans les années 70. Il définit une manière selon la quelle les ordinateurs peuvent communiquer par les équipements intermédiaires du réseau.

Le protocole IP identifie chaque nœud avec une adresse unique. De plus, IP décompose cette adresse en deux parties :

- il identifie dans la première partie le sous-réseau d'appartenance du nœud (préfixe du réseau);
- la seconde partie détermine le nœud dans ce sous-réseau.

L'adresse IP joue alors un double rôle: elle identifie le nœud et définie sa position sur Internet également. Cet adressage assure la cohérence et la sécurité des transmissions, par exemple, si un paquet provenant d'un sous réseau indique l'adresse d'un autre sous-réseau, il sera détruit. Cependant, le déploiement de ce principe pour identifier les nœuds mobiles implique que ces nœuds mobiles doivent configurer leur adresse sur les nouveaux réseaux avec les anciens préfix. La cohérence du protocole IP ne permet pas l'identification d'un nœud localisé dans un réseau **'A'** avec un préfixe correspondant à un réseau **'B'**. C'est pourquoi, un nœud mobile doit obtenir une nouvelle adresse à chaque changement de réseau.

Il existe deux normes du protocole IP. Nous présentons d'abord le protocole IPv4, ensuite, le protocole IPv6 dans les paragraphes suivants.

II.2.1 Protocole IP version 4(IPv4)

Le protocole IPv4 a été standardisé en 1981 et s'adressait initialement à la communauté militaire et scientifique. Il utilise une adresse IP sur 32 bits (2^{32}adresses), c'est-à-dire que 4 294 967 296 adresses sont possibles. Le protocole IPv4 n'a pas été conçu pour assurer la **qualité de service(QoS),** ni **l''auto-configuration d'adresses**, ni **le multicast**, ni **la sécurité**. Il est évident que le protocole IPv4 ne peut plus répondre à la demande des utilisateurs. Les diverses solutions [26] ont été trouvées pour assurer les fonctions ci-dessus, mais elles alourdissent l'ensemble des couches supplémentaires. Par exemple:

- Le protocole NAT (en anglais Network Address Translation) qui permet de résoudre la pénurie d'adresses IPv4, a pour effet de compliquer la gestion des adresses IP privées et publiques, d'alourdir les chemins de routage, de surcharger les tables de

routage et de ralentir le développement des applications temps réel qui fonctionnent de bout en bout;

- Vu que le protocole IPv4 n'est pas prévu à l'origine pour permettre à un terminal d'auto-configurer son adresse IP dans un réseau, il faut les configurer manuellement ou utiliser un serveur doté du protocole DHCP (en anglais **D**ynamic **H**ost **C**onfiguration **P**rotocol) qui supporte la fonction d'auto-configuration d'adresses pour les terminaux;
- La fonction de diffusion, qui s'est développée aujourd'hui dans le protocole IPv4, monopolise une classe complète d'adresses et n'est pas une fonction native d'IPv4.
- Le protocole IPsec est utilisé comme une option dans IPv4. En outre, le NAT complique l'utilisation du protocole IPsec.

II.2.2 IP version 6 (IPv6)

Comme expliqué ci-dessus, IPv4 ne peut pas répondre aux besoins engendrés par la croissance très forte d'Internet, ni aux besoins induits par de nouvelles applications. Toutes les limitations d'IPv4 conduisent à la transition d'IPv4 vers IPv6. IPv6 a été conçu dans la continuité d'esprit d'IPv4, sans réelle rupture technologique. Cependant, le nouveau protocole IPv6 n'en reste pas moins différent et l'interopérabilité entre les deux versions IP n'est pas naturelle.

La caractéristique la plus importante d'IPv6 est qu'il supporte des adresses plus longues qu'en IPv4. L'augmentation de la taille des adresses conduit à une taille d'en-tête de 40octets pour le paquet IPv6, le double de l'en-tête IPv4 sans les options. En outre, le format d'en-tête IPv6 est simplifié et amélioré pour permettre aux routeurs de meilleures performances dans leurs traitements de paquets.

Les principales améliorations de l'en-tête IPv6 sont les suivantes:

- L'en-tête ne contient plus le champ checksum[2] parce que l'en-tête devait être ajustée par chaque routeur en raison de la décrémentation du champ durée de vie. Par contre, pour éviter qu'un paquet soit erroné, tous les protocoles des couches supérieures doivent mettre en œuvre un mécanisme de checksum de bout en bout;
- La taille d'en-tête est fixée. Ainsi le routeur peut facilement déterminer où commence la zone de données utiles ;

[2] Le checksum sert pour la détection des erreurs.

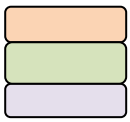
- Les options ont été retirées de l'en-tête et remplacées par des extensions qui peuvent être facilement ignorées par les routeurs intermédiaires;
- Les champs sont alignés sur des mots de 64 bits, ce qui optimise leur traitement, surtout avec les nouvelles architectures à 64 bits;
- La fonction de fragmentation a été retirée des routeurs intermédiaires. IPv6 utilise un mécanisme de découverte du PMTU (en anglais Path Maximum Transfer Unit) pour éviter d'avoir recours à la fragmentation par les routeurs. Si la fragmentation s'avère nécessaire, une extension est prévue;

Le format d'en-tête d'un paquet IPv4 est montré dans la figure 4 [33,34]. L'en-tête du paquet IPv6 est fortement simplifié par rapport à l'en-tête IPv4 (figure 5).

En- tête IPv4

Version	IHL	Type de service	Longueur totale
Identification		Indicateurs	Décalage du fragment
Time To Live(durée de vie)	Protocole	Somme de contrôle d'en-tête	
Adresse source			
Adresse destination			
Options			remplissage

Légende



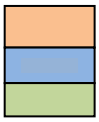
- Noms des champs conservés d'IPv4 à IPv6
- Nom et position modifiés dans IPv6
- Champs non conservés dans IPv6

Figure 4: illustration de la structure de l'en-tête IPv4

En-tête IPv6

Version	**Classe de trafic**	**Etiquetage de flux**	
Longueur des données utiles		En-tête suivant	Limite de nombre de sauts
Adresse IP source			
Adresse IP de destination			

Légende



- Noms des champs conservés d'IPv4 à IPv6
- Nom et position modifiés dans IPv6
- Nouveau champ dans IPv6

Figure 5: illustration de la structure de l'en-tête IPv6

L'en-tête IPv6 offre plusieurs avantages par rapport à l'en-tête IPv4 (figure 6):

1. Une plus grande efficacité du routage pour des performances et évolutivité du débit de transmission;
2. Aucune exigence pour le traitement des sommes de contrôle;
3. Des mécanismes d'en-tête d'extension simplifiés (par rapport au champ d'options IPv4);
4. Un champ d'étiquetage de flux pour le traitement par flux sans avoir besoin d'ouvrir le paquet interne de transport pour identifier les différents flux de trafic.

Les champs d'en-tête de paquet IPv6 incluent :

1. **Version:** contient une valeur binaire de 4 bits indiquant la version du paquet IP. Pour les paquets IPv6, ce champ est toujours 0110;

2. **Classe de trafic:** ce champ de 8 bits est équivalent au champ de services différenciés pour l'IPv4. Il contient également une valeur DSCP de 6 bits utilisée pour classer les paquets et une valeur de notification explicite de congestion de 2 bits utilisée pour contrôler l'encombrement;

3. **Étiquetage de flux:** ce champ de 20 bits fournit un service spécifique pour les applications en temps réel. Ce champ peut être utilisé pour indiquer aux routeurs et aux commutateurs de conserver le même chemin pour le flux de paquets, de telle sorte que l'ordre des paquets ne soit pas modifié;

4. **Longueur des données utiles:** ce champ de 16 bits est équivalent au champ de longueur totale de l'en-tête IPv4. Il définit la taille globale du paquet (fragment), y compris l'en-tête et les extensions facultatives;

5. **En-tête suivant:** ce champ de 8 bits est équivalent au champ de protocole de l'IPv4. Il indique le type de données utiles transportées par le paquet, permettant ainsi à la couche réseau de transmettre les données au protocole de couche supérieure approprié. Ce champ est également utilisé s'il existe des en-têtes d'extension ajoutés au paquet IPv6;

6. **Limite de nombre de sauts:** ce champ de 8 bits remplace le champ de durée de vie (TTL) de l'IPv4. Cette valeur est réduite de 1 chaque fois qu'un routeur transmet le paquet. Lorsque le compteur atteint 0, le paquet est rejeté et 1 message ICMPv6 est transféré à l'hôte émetteur, indiquant que le paquet n'a pas atteint sa destination;

7. **Adresse source:** ce champ de 128 bits identifie l'adresse IPv6 de l'hôte émetteur;

8. **Adresse de destination:** ce champ de 128 bits indique l'adresse IPv6 de l'hôte récepteur.

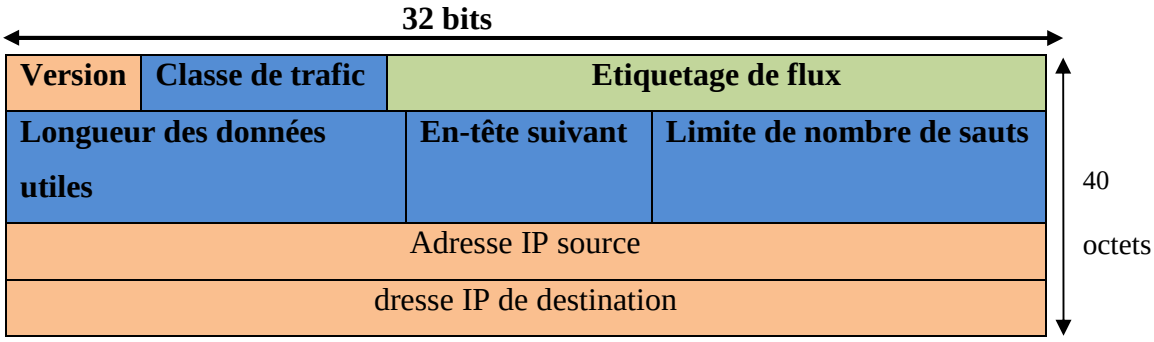


Figure 6: avantages de l'en-tête IPv6 par rapport à l'en-tête IPv4.

Un paquet IPv6 peut également contenir des en-têtes d'extension qui fournissent des informations facultatives de couche réseau. Les en-têtes d'extension sont facultatifs et sont placés entre l'en-tête IPv6 et les données utiles. Ces en-têtes sont utilisés pour la fragmentation, la sécurité, la prise en charge de la mobilité, etc.

Les principales caractéristiques d'IPv6 sont :

- Adressage hiérarchique et capacité augmentée;
- Auto-configuration d'adresses IPv6;
- En-tête d'extension IPv6 pour optimiser le routage;
- Sécurité;
- Qualité de Service (QoS).

Adressage hiérarchique et capacité augmentée

IPv6 dispose d'une adresse sur 128 bits, donc il propose un immense espace d'adresses IPv6 (2^{128} adresses). IPv6 permet ainsi d'éviter l'utilisation du NAT et donc peut promouvoir l'utilisation et le développement des applications temps réels, telles que la Vidéo conférence, la voix sur IP (en anglais Voice Over Internet Protocol - VoIP) ou les jeux multi-joueurs, qui fonctionnent mieux de bout-en-bout.

Différents types d'adresses IPv6

Il y a trois types d'adresses IPv6: unicast, multicast et anycast qui sont caractérisées par leur préfixe [7].

- Une adresse de type **unicast** désigne une interface unique de réseau IPv6. Un paquet envoyé à une telle adresse sera donc remis à l'interface ainsi identifiée.

- Une adresse de type **multicast** désigne un groupe d'interfaces qui en général appartiennent à des nœuds différents. Ces différents nœuds peuvent être situés n'importe où dans Internet. Lorsqu'un paquet a pour destination une adresse de type multicast, il est acheminé par le réseau à toutes les interfaces qui sont membres de ce groupe. Son préfixe est **FF00 :: /8**. Par exemple, FF02:0:0:0:0:0:0:1 représente le groupe de tous les nœuds d'un lien local et FF02:0:0:0:0:0:0:2 représente le groupe de tous les routeurs d'un lien-local.
- Une adresse de type **anycast** désigne un groupe d'interfaces, la différence avec une adresse de type **multicast** étant que lorsqu'un paquet a pour destination une telle adresse, il est acheminé à un des éléments du groupe et non pas à tous. Son adresse est composée par une partie préfixe et une partie identifiant anycast. La partie préfixe est la même que celle utilisée pour les adresses unicast, et la partie identifiant anycast n'est pas encore complètement définie. Pour l'instant, 0x7E est utilisé pour l'agent mère du protocole IPv6 Mobile. Cette adresse est principalement expérimentale.

L'Auto-configuration d'adresses IPv6

Le protocole IPv6, contrairement au protocole IPv4, prévoit la possibilité pour un nœud d'auto-configurer son adresse dans un réseau.

IPv6 spécifie deux méthodes d'auto-configuration d'adresses globale :

- **l'auto-configuration d'adresses avec état** (en anglais Stateful Address Auto configuration): Son fonctionnement s'appuie sur le protocole DHCPv6 (en anglais Dynamic Host Configuration Protocol for IPv6) [33], qui est construit sur une architecture client/serveur. C'est le serveur DHCP qui procure les paramètres de configuration, tels que les adresses, le routage, le DNS, aux clients lorsque ces derniers en font la demande. Avec ces informations, les clients peuvent configurer leur interface réseaux et communiquer. Il est important de noter que l'ensemble des échanges DHCP sont toujours à l'initiative des clients. Le serveur ne fait que répondre à des demandes, il n'est jamais l'initiateur d'un échange. L'auto configuration d'adresses avec état est retenue lorsqu'un site demande un contrôle strict de l'attribution des adresses. Mais la procédure DHCP nécessite plusieurs échanges de messages de signalisation entre le serveur et le client. De plus, le client doit parfois avoir une adresse lien-local et procéder la procédure DAD(Duplicate Address Detection) pour vérifier l'unicité de son adresse lien-local avant d'envoyer la requête auprès du serveur DHCP, en outre, le client doit aussi procéder la procédure DAD pour vérifier l'unicité d'adresse globale attribuée par le serveur DHCP

avant de pouvoir l'utiliser [34]. Tout cela n'est pas adaptable pour les clients mobiles qui s'accommodent mal de ces lourdes procédures. En effet, lorsqu'un client mobile vient de changer de réseau, il doit obtenir et utiliser aussitôt que possible une adresse temporaire CoA (en anglais Care-of Address – CoA) dans ce nouveau réseau pour maintenir ses communications en cours

- **L'auto-configuration sans état** (en anglais State Less Address Auto Configuration) convient principalement aux réseaux de petites tailles, et qui n'ont pas besoin d'une table d'association globale des adresses. Les machines **se débrouillent toutes seules entre-elles**, sans entité décisionnelle centrale. Chaque terminal génère une adresse lien-local et une adresse unicast global, avec le même identifiant d'interface, ce qui lui permet de dialoguer à l'intérieur du LAN comme à l'extérieur. Si un ré-adressage est nécessaire, les machines seront prévenues par les routeurs, qui fourniront le nouveau préfixe du réseau. Ce mécanisme d'apparence simple pose cependant de nombreux problèmes de sécurité (type spoofing et redirect) qu'il faut correctement analyser et contrer.

Sécurité

Pour protéger Mobile Ipv6 contre les attaques il a été prévu dans le protocole de protéger les Binding Updates et les Binding Acknowledgement. Ainsi tout paquet contenant un BU ou un BAck devra être protégé par IPsec[3] (protocole spécifiquement conçu pour sécuriser IPv6), afin de contrer toute tentative de forger des BU ou des BAck par une tierce personne. Plus particulièrement on doit assurer l'authentification de la source, l'intégrité des données et la protection contre le rejet. Cela devra être assuré par le mécanisme de Authenfication Header ou AH comme définit dans IPsec. Si les données doivent aussi être chiffrées on utilisera le mécanisme d'Encrypted Security Payload ou ESP en même temps qu'AH (Authenfication Header).

La qualité de service(QoS)

IPv6 présente également plusieurs avantages permettant de mieux gérer la QoS mais qui ne sont pas encore significatifs. De manière générale, la QoS est gérée de la même façon sous IPv6 que ce qui se fait aujourd'hui sous IPv4. Cependant, les applications temps réel, telles que la vidéo conférence, la VoIP, pourraient trouver un réel intérêt dans IPv6, du fait de son nombre d'adresses qui permet d'éviter d'avoir recours au NAT qui nuisent à ce type de services.

[3]IP Security

II. 3 Les protocoles de mobilité : étude comparative

Depuis quelques années, les terminaux mobiles font partie de notre vie de tous les jours. Néanmoins pour être pleinement utilisables, les téléphones intelligents, tablettes et portables ont une condition nécessaire : être connectés à Internet ou un autre réseau de grande envergure. Les environnements mobiles se caractérisent par la présence de plusieurs terminaux portables ayant chacun un ou plusieurs moyens de communication sans fil. Ces interfaces de communication sans fil permettent aux terminaux, tout en se déplaçant, de communiquer entre eux ou avec des stations fixes. Ces environnements présentent de grandes différences par rapport aux environnements traditionnels ou fixes. Pour des raisons de taille et de poids, les terminaux portables disposent de ressources moins importantes par rapport à celles qu'offrent des stations fixes. On affiche un désir de la part des usagers à bénéficier d'un accès Internet sans discontinuité de leurs applications réseaux usuelles lors de leurs déplacements, de sorte que nous avons des réseaux entiers constitués de dispositifs sans fils se déplaçant ensemble et désirant cette qualité de service. Les fonctionnalités de base de la gestion de la mobilité comportent:

- **la gestion de la localisation** qui permet d'identifier la localisation du réseau en cours d'un terminal mobile et de garder sa trace lorsqu'il se déplace. Avec l'aide de la gestion de localisation, le nœud correspondant est capable de localiser le mobile et d'établir une session via la signalisation appropriée;
- **la gestion du transfert intercellulaire**, quant à elle sert à fournir aux mobiles la continuité de session lorsqu'ils se déplacent dans différentes régions d'un réseau et changent leur point de rattachement au réseau durant une session. Le principal objectif du transfert transparent est de minimiser l'interruption de service due à la perte de données et au retard entre les transferts intercellulaires. La plupart des protocoles de gestion de la mobilité effectuent la gestion de transfert intercellulaire avec un schéma de gestion de la localisation approprié.

Dans cette section nous allons faire une étude des différentes approches de gestion de mobilité incluent des protocoles des couches réseaux **(MIP, mobile IP)**, application**(SIP)** et transport **(SCTP/mSCTP, Mobile SCTP).** Voir les avantages et les inconvénients de chacun et en plus proposer celui qui répond mieux à notre contexte.

II.3.1 Protocoles de mobilité au niveau réseau: IP mobile (MIP, mobile IP)

IP mobile (MIP) est un protocole de prise en charge de la mobilité sur IP qui est spécifié à l'IETF. Il peut se diviser en IPv4 mobile (MIPv4) et IPv6 mobile (MIPv6) selon la version du protocole IP associé [44]. Ces deux protocoles fournissent fondamentalement des fonctionnalités similaires avec quelques exceptions dans le détail des mécanismes de fonctionnement.

Avant d'expliquer le fonctionnement du protocole IP Mobile, nous présentons d'abord ses composants et son architecture comme le présente la figure 7.

Composants d'IP Mobile

- **Nœud Mobile (Mobile Node – MN)**: un terminal qui peut changer de point d'attachement d'un réseau à un autre;
- **Agent parent** (Home Agent - HA**):** C'est un routeur sur le réseau parent d'un mobile, qui envoie les paquets dans un tunnel pour les remettre au mobile lorsqu'il visite un autre réseau. Cet agent met à jour les informations concernant la position du mobile;
- **Adresse parent** (Home Address – HoA):est l'adresse IP du Nœud Mobile(MN) sur son réseau parent. Elle permet d'identifier le Nœud Mobile**(**MN) de façon unique sur tous les réseaux;
- **Agent visité (Foreign Agent-FA):**C'est un routeur sur un réseau visité (Foreign Network - FN) visité auquel le MN est attaché. Il fournit des services de routage au MN lorsque le MN est enregistrée auprès de ce dernier;
- **Adresse temporaire (Care-of Address - CoA):** C'est l'adresse IP de localisation du MN, obtenue au réseau visité, et qui lui permet d'envoyer et recevoir des paquets sur ce réseau;
- **Nœud Correspondant (Correspondent Node - CN):** C'est une machine (mobile ou non) qui dialogue avec un mobile.

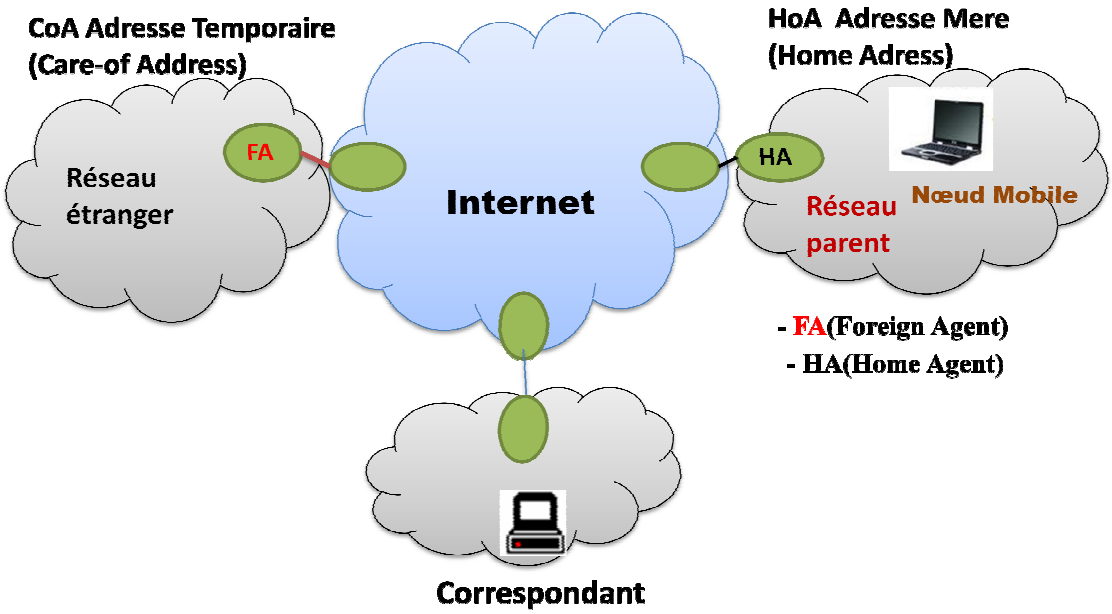


Figure 7: Architecture du protocole IP Mobile

II.3 .1.1 Fonctionnement de MIP

Tout d'abord on distingue deux types de réseaux selon la position du nœud mobile. On appellera réseau parent ou réseau principal auquel est rattaché le nœud mobile administrativement. C'est le réseau dans lequel il est déclaré dans le DNS et sur lequel il obtient une adresse IP principale. D'un autre coté on appelle réseau visité ou réseau étranger, un réseau où le nœud mobile se trouve à un moment donné lors de ces déplacements. Les agents de mobilité, agent parent et agent visité, (ce sont les routeurs d'accès respectivement dans le réseau parent et le réseau visité) maintiennent une liste des nœuds mobiles qu'ils gèrent. Cette liste est appelée «**cache d'association**», elle associe l'adresse principale du mobile à son adresse temporaire. Le rôle principal de ces agents de mobilité est d'encapsuler (respectivement décapsulé) les paquets en transit entre les correspondants et les nœuds mobiles en ajoutant (respectivement en enlevant) un en-tête d'adressage.

Dans MIPv6, les correspondants d'un nœud mobiles détiennent aussi un cache d'association ce qui leur permet de connaître l'adresse temporaire du mobile associée à son adresse principale. Le nœud mobile devra indiquer cette adresse à son agent parent périodiquement pour qu'il puisse maintenir une correspondance entre adresse principale et adresse temporaire. La découverte des agents de mobilité se fait par le protocole de découverte des Agents qui met en place un échange de messages permettant cette décision. Lorsque le mobile détecte qu'il a changé de sous-réseau, il acquiert une nouvelle adresse IP

grâce au protocole DHCP et s'enregistre auprès de son agent parent et de l'agent visité du nouveau réseau.

II.3 .1.1.1 Encapsulation IP dans IP

Mobile IP utilise le principe d'encapsulation IP dans IP, encore appelé tunnel IP, pour transmettre les paquets interceptés par l'agent parent vers la position courante du mobile. L'agent parent ne fait qu'encapsuler les paquets, c'est à dire qu'il ne les modifie pas de telle façon qu'il n'a pas besoin de recalculer les sommes de contrôle (checksum) des couches supérieures. Il se contente donc d'ajouter un nouvel en-tête IP devant l'en-tête du datagramme reçu [6], comme le montre la figure 8. Ainsi, les datagrammes sont facilement redirigés et routés dans l'Internet. L'adresse IP vers laquelle l'agent parent fait suivre les paquets destinés au mobile est la Care-of-Address (CoA).

	Entête IP d'origine	Données d'origine
		:
Nouvelle Entête IP (CoA)	Entête IP interne	Données d'origine

Figure 8: Encapsulation IP dans IP

II.3 .1.1.2 Enregistrement auprès de l'agent parent

Lorsque le nœud mobile détecte qu'il a changé de sous-réseau, il doit acquérir une nouvelle adresse temporaire et s'enregistrer auprès de son agent parent et de l'agent visité. L'acquisition de cette nouvelle adresse se fait grâce au protocole DHCP.

Une fois que le nœud mobile a une adresse temporaire valide, il émet un message **Registration Request** en indiquant la correspondance entre son adresse principale et son adresse temporaire et éventuellement d'autres options. Ce message passe par l'agent visité qui le transmet à l'agent parent du mobile s'il accepte les requêtes du nœud mobile. L'agent parent doit acquitter le **Registration Request** pour bien confirmer la réception et pour informer le nœud mobile de l'acceptation ou du refus de la requête par un **Registration Reply**. A la réception du **Registration Request**, aussi bien l'agent parent que l'agent visité mettent à jour leur cache d'association pour ce nœud mobile [11,32].

II.3 .1.1.3 Communication

La communication entre un nœud mobile et un correspondant quelconque sur Internet est très spécifique et requiert plusieurs mécanismes des agents de mobilité. Comme un nœud correspondant d'un nœud mobile ne connait que l'adresse principale du nœud mobile, les paquets à destination du nœud mobile sont toujours envoyés dans le sous-réseau parent du nœud mobile. Si le nœud mobile ne s'est pas déplacé, les paquets lui seront « livrés » de la même manière qu'un nœud fixe, c'est-à-dire sans opérations supplémentaires. Par contre, si le nœud mobile est dans un sous-réseau visité, son agent parent devra capturer tous les paquets destinés au nœud mobile et les lui transmettre à son adresse temporaire, grâce à son cache d'association (comme illustre Figure 9) [11,37].

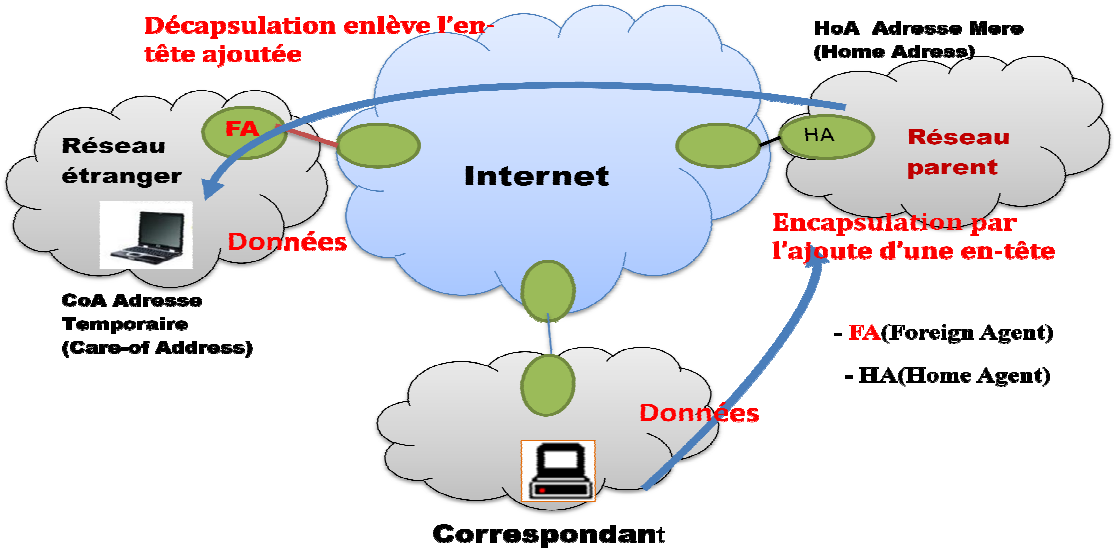


Figure 9 : routage triangulaire : du correspondant au mobile

De l'autre côté, les paquets envoyés par le nœud mobile ont l'adresse du correspondant comme adresse destination et l'adresse principale du mobile comme adresse source. Ceci présente une entorse au modèle de l'Internet puisque l'adresse source des paquets envoyés parle nœud mobile ne correspond pas au préfixe du sous-réseau visité. Les paquets devront alors obligatoirement passer par l'agent visite pour éviter qu'ils ne soient détruits. Par contre, une fois que les paquets ont été routés hors du sous-réseau visité, ils vont directement du nœud mobile au correspondant sans passer par le réseau parent. C'est ce qu'on appelle le routage triangulaire [11,37]. La figure 10 explique le principe.

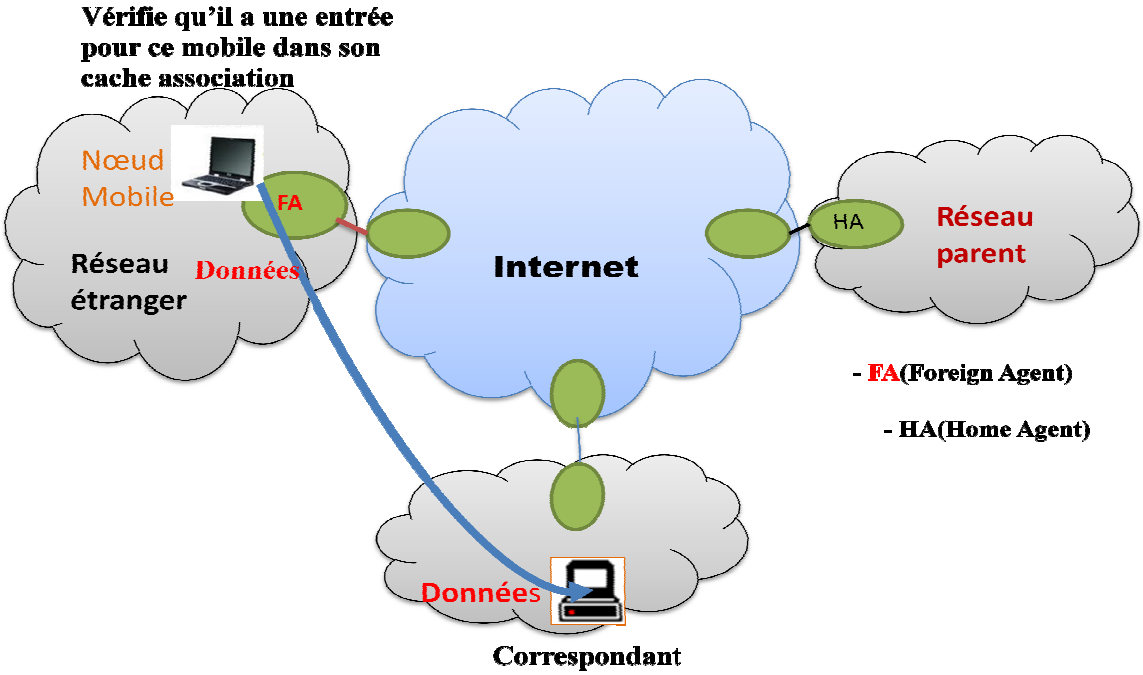


Figure 10: routage triangulaire : du mobile au correspondant

Etudions plus en détail les opérations nécessaires pour effectuer ce routage triangulaire. Tout d'abord, lorsque le nœud mobile se déplace dans un sous-réseau visité, il doit en informer son agent parent à travers un message **Registration Request**. A la réception de ce message, si l'agent parent accepte la requête, en plus de créer ou de mettre à jour l'entrée pour ce nœud mobile, il envoie une requête **ARP (**Address Resolution Protocol) sur le réseau principal afin de faire correspondre l'adresse IP du mobile avec son adresse MAC. Ainsi il peut intercepter les paquets à destination du mobile. Ensuite, l'agent parent doit faire suivre ces paquets à la position courante du mobile. Pour cela, il encapsule chaque paquet en ajoutant un en-tête de destination rempli avec l'adresse temporaire courante du mobile comme adresse destination et avec son adresse comme adresse source avant de mettre dans le tunnel pour l'agent visité. Enfin, chaque paquet est désencapsulé pour l'agent visité (suppression de l'en-tête) et délivré au nœud mobile.

II.3.1.2 La mobilité IPv6 (MIPv6)

Ce protocoleIPv6 est inclut entre autres la mobilité en standard. L'objectif de MIPv6 [11,27] est d'offrir une communication directe entre un nœud mobile et ses correspondants (élimination du routage triangulaire) et éviter les ruptures des communications pendant les déplacements. Bien que MIPv6 reprenne des mécanismes de MIPv4, de nombreuses fonctionnalités supplémentaires ont été mises en place.

II.3 .1.2.1 Fonctionnalités requises

Dans MIPv6, l'agent visité décrit dans MIPv4 n'existe plus. Par contre, l'agent parent est encore un routeur d'accès du sous-réseau principal du nœud mobile. Son rôle est le même que dans le cas de MIPv4, à savoir capturer les paquets à destination du mobile et les lui tunnelier à sa localisation courante.

Par contre, les correspondants doivent mettre en œuvre certains mécanismes supplémentaires. Tout d'abord, ils doivent disposer d'un cache d'association tout comme l'agent parent; dans ce cache sera stockée la correspondance entre l'adresse principale d'un nœud mobile avec lequel il a une communication et son adresse temporaire courante. Il devra donc être capable de traiter des messages de registration envoyés par un nœud mobile. De plus, il devra être capable d'effectuer le routage directement vers le mobile (**routing header**). Ceci constitue un apport important dans le fonctionnement de la mobilité puisque les paquets des correspondants n'auront pas à passer par le réseau parent systématiquement. Mais toutes ces fonctionnalités supplémentaires ne sont faites qu'au niveau de la couche IP ; l'adresse identifiant la communication au niveau applicatif sera toujours l'adresse principale du nœud mobile, la couche IP cachant l'adresse temporaire source (ou destination selon qu'on se situe sur le nœud mobile ou le correspondant).

D'un autre côté, un nœud mobile doit toujours conserver la liste des correspondants aux quels il envoie un message de registration (pour les mises à jour éventuelles) et doit être capable de décapsuler lui-même les paquets qui lui sont transmis ; au niveau application, un nœud mobile utilise toujours son adresse principale, c'est pourquoi la couche IP doit pouvoir décapsuler l'en-tête indiquant l'adresse temporaire. Cette opération était exécutée par l'agent visité dans MIPv4 [27, 33, 34].

Il est alors possible de distinguer deux cas de figures qui sont:

II.3 .1.2.1.1 Nœud mobile dans son réseau parent

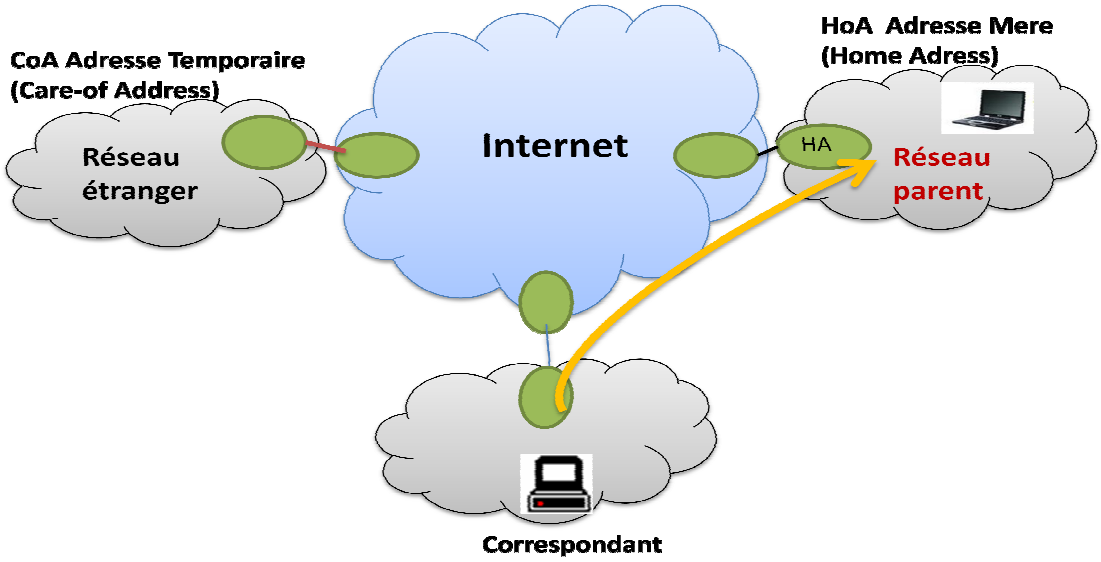


Figure 11: Nœud mobile dans son réseau parent

C'est le cas par défaut. L'équipement communique comme n'importe quel nœud du réseau. Le nœud mobile a en effet récupéré une adresse IPv6 dans ce réseau parent(auto-configuration) et l'utilise pour communiquer (figure 11). L'agent parent n'intervient pas dans cette étape. Néanmoins, une relation forte est établie entre le nœud mobile et ce réseau parent.

Pour découvrir l'agent parent dans le réseau, le nœud mobile envoie un message ICMPv6 à l'adresse Anycast des agents parents du réseau. Lorsqu'il reçoit une réponse positive à sa demande d'association, il a alors trouvé son agent parent.

II.3 .1.2.1.2 Nœud mobile dans un réseau étranger

Lorsqu'un nœud mobile va arriver dans un réseau étranger (comme le montre la figure 12), il va tout d'abord acquérir une adresse IPv6. Cette adresse constituera ce que l'on a appelé care-of-address.

Du côté du nœud correspondant, ce dernier continue à envoyer ses paquets à l'adresse qu'il connait, la home address du nœud mobile. Une fois que le nœud mobile a pu récupérer son adresse temporaire grâce au système d'auto-configuration, il va alors envoyer un message à son l'agent parent, lui signalant son nouvel emplacement en lui donnant son adresse temporaire. Cette opération est appelée **Binding Update**. Le Binding Update est utilisé par tout nœud mobile afin d'informer son Home Agent ou tout autre nœud avec lequel

une communication est établie (correspondent node) de sa nouvelle adresse IP (care-of-address).

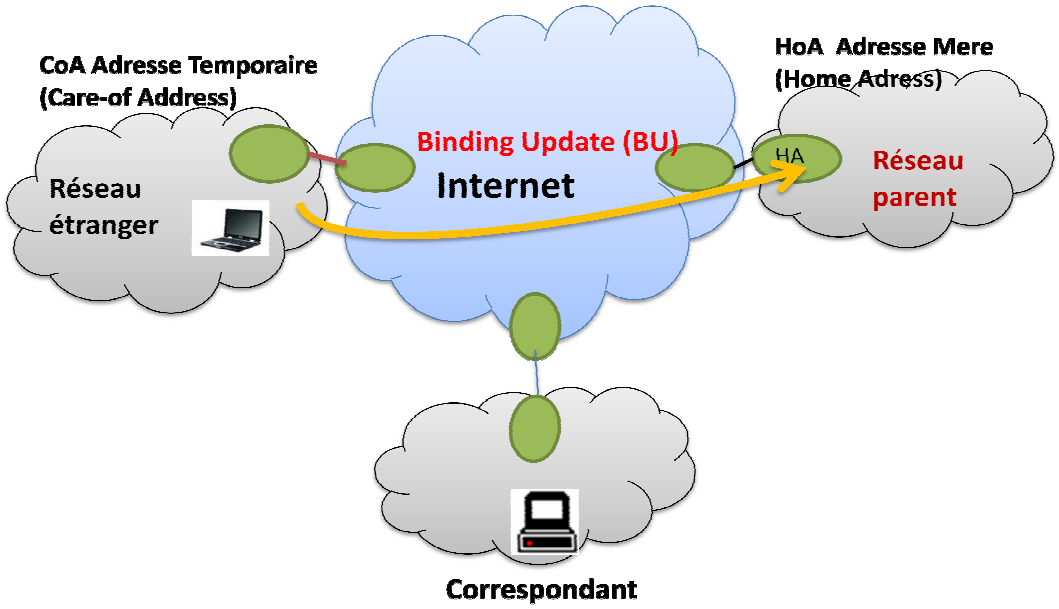


Figure 12 : Binding update vers le réseau parent

L'agent parent va alors ajouter une nouvelle ligne à sa table de correspondance, permettant le lien entre home address et care-of-address pour le nœud mobile. Il va alors pouvoir faire suivre facilement les paquets vers le nœud mobile. Quand l'agent parent va recevoir un paquet provenant du nœud correspondant, il va l'encapsuler dans un nouveau paquet IP grâce à l'extension d'en-tête IP-IP du protocole IPv6.

Pour le nœud correspondant, ce Binding update est donc totalement transparent. Il correspond toujours avec la même adresse destination. Le nœud mobile, quant à lui, va utiliser le même principe. Il va encapsuler sa réponse (qui a donc pour source la HoA du nœud mobile, et comme destination l'adresse du nœud correspondant) avec un nouvel en-tête qui aura, cette fois-ci, comme adresse source la CoA du mobile, et comme destination l'adresse de l'agent parent.

Une fois le paquet récupéré par l'agent parent, ce dernier enlève le premier en-tête, et envoie le paquet vers le nœud correspondant. Pour ce dernier, ce sera exactement comme si le paquet provenait directement du nœud mobile. Il n'est donc pas nécessaire pour le correspondant d'implémenter la mobilité IPv6, car il n'utilise aucun des principes de cette dernière. De son point de vue, il ne fait que de la communication avec adresse IPv6, il ne sait pas qu'il discute avec un nœud mobile.

II.3 .1.2.1.3 Optimisation de routage

Nous aurons remarqué que la mobilité, telle que définie jusqu'ici, n'est pas optimisée dans son routage. En effet, les figures 13 et 14 nous montrent le principe. Lorsqu'un nœud mobile est en déplacement, tous les paquets vont passer par le réseau parent pour atteindre le nœud mobile. Imaginons dès lors un nœud correspondant situé à **Moundou**, un réseau parent situé à **Bongor**, et un nœud mobile en déplacement à **N'djamena**: un paquet de données traversera **Bongor** avant d'arriver à destination. Cet exemple nous montre que le trajet est long (pour atteindre la destination, le mobile doit passer par Bongor qui est une obligation, compte tenu de la position de l'agent parent. Donc il serait bien plus intéressant de communiquer directement entre les deux nœuds (correspondant et mobile) sans passer par le réseau parent [32]. C'est pourquoi la mobilité IPv6 a intégré dans son protocole une optimisation du routage.

Dans un premier temps, pour utiliser cette optimisation de routage, il est dès lors essentiel que le nœud correspondant possède les options de mobilité IPv6 (ce qui n'était pas nécessaire avant). Grâce à cette intégration de la mobilité au sein du nœud correspondant, ce dernier va pouvoir maintenir une table des associations, identique à celle maintenue par l'agent parent. Pour avoir cette table de routage à jour, le nœud mobile va devoir, lors de chaque changement de réseau, envoyer un paquet de **Binding update** au réseau parent, puis au nœud correspondant. De cette manière, le nœud correspondant pourra ajouter ou mettre à jour la ligne dans sa table de correspondance.

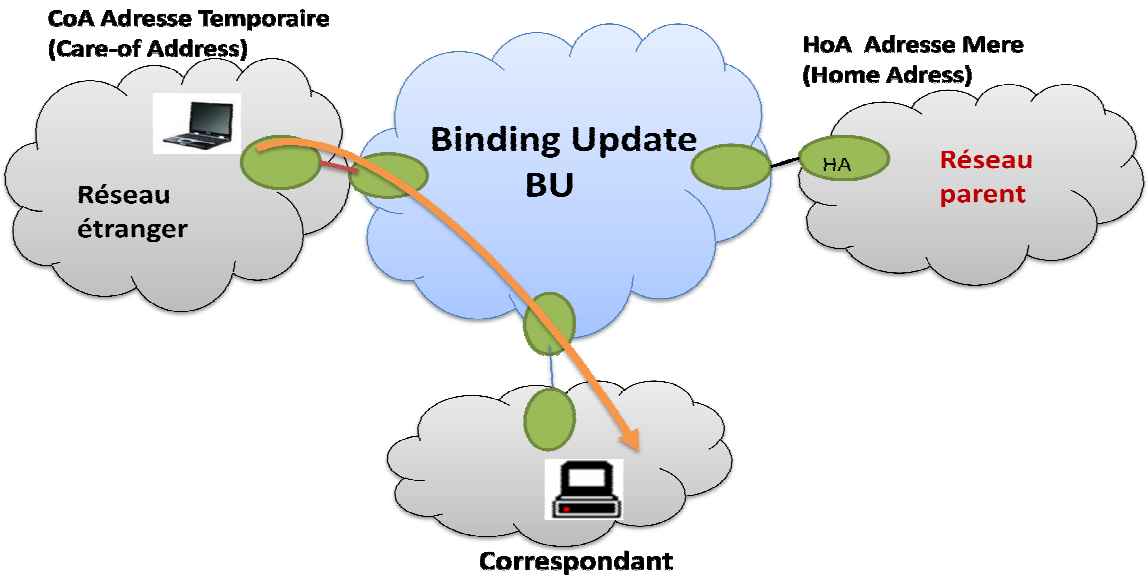


Figure 13 : Binding update vers le nœud correspondant

Connaissant la HoA et la CoA, le nœud correspondant va pouvoir modifier ses paquets pour leur donner comme adresse de destination la CoA du nœud mobile. Cette modification consistera aussi en l'ajout d'une extension d'en-tête de routage particulière contenant l'adresse HoA du nœud mobile comme destination finale. Cette extension d'en-tête de routage est une extension définie pour la mobilité IPv6. De cette manière, les passerelles de sécurité pourront adopter un filtrage différent de celui appliqué pour les autres en-têtes de routage.

Lorsque le nœud mobile cherche à communiquer avec un correspondant, il va d'abord tenter d'envoyer un paquet de mise à jour d'association. Si le nœud correspondant répond qu'il ne comprend pas cette demande, l'optimisation des routes n'est pas possible (le nœud correspondant n'est pas configuré pour la mobilité IPv6). Le nœud mobile utilisera alors la voie classique, passant par son réseau parent. Un message ICMPv6 a été défini pour ce cas où le nœud correspondant « ne parle pas le langage mobile IPv6 ».

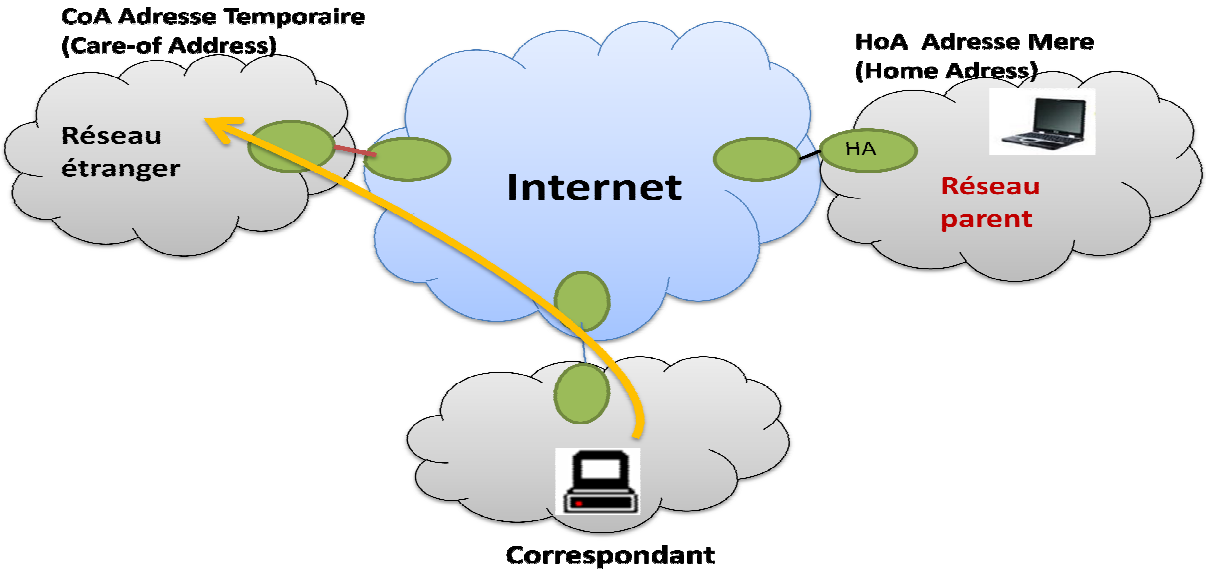


Figure 14: Routage optimisé dans le cadre de la mobilité IPv6

II.3 .1.3 Limites de Mobile IP

Bien que le protocole IPv6 Mobile permette de résoudre le problème de routage de paquets triangulaires utilisé dans le protocole IPv4 Mobile, il souffre encore de plusieurs faiblesses. Parmi ces faiblesses [30], nous citons:

- La latence du Handover et du contrôle du trafic: Le temps que met le MN pour détecter le changement du sous-réseau d'attachement. Ce temps peut être très long car

les mécanismes de détection du mouvement dans mobile IP sont basés sur l'expiration du **timer** dans les messages d'avertissement du FA;

- Latence d'enregistrement: En effet, dans la version standard de Mobile IP, la nouvelle localisation d'un mobile est toujours signalée à son agent parent. Ce dernier est ainsi averti de tous les déplacements des mobiles qu'il gère. Ces opérations génèrent une grande quantité de signalisation. De plus, les pertes de paquets pendant les Handover peuvent être importantes puisque la procédure d'enregistrement est longue, en particulier si le HA se trouve à l'autre bout du monde. La durée d'un Handover peut atteindre plusieurs secondes dans l'Internet actuel.

Pour faire face aux limites du protocole IPv6 Mobile, plusieurs solutions ont été proposées [30,26]. Le processus de Handover peut être amélioré soit en réduisant la perte de paquets, soit en diminuant la charge de la signalisation, soit encore en rendant le processus le plus rapide possible. Parmi les différentes propositions, nous présentons un aperçu sur deux principales solutions : le protocole IPv6 Mobile Hiérarchique(HMIP)[10] et le protocole Fast Handover pour IPv6 Mobile (FMIP) [10,30].

II.3 .1.4 Extensions de MIP: HMIP et FMIP

MIP peut n'être pas efficace si les transferts intercellulaires surviennent fréquemment ou s'il est besoin d'applications en temps réel. Pour résoudre ces problèmes, diverses extensions du protocole MIP ont été proposées: le protocole IPv6 Mobile Hiérarchique(HMIP)[10] et le protocole Fast Handover pour IPv6 Mobile (FMIP) [10,30].

MIP hiérarchique(HMIP)

Dans le cas du protocole IP mobile de base, le mobile a besoin de s'enregistrer (ou effectuer une mise à jour du rattachement) auprès de l'agent HA et/ou CH (lorsque l'optimisation d'acheminement s'applique) chaque fois qu'un mobile change son sous-réseau. Cet enregistrement peut entraîner un délai de transfert intercellulaire et une redondance de signalisation inutiles. Si le transfert survient trop fréquemment ou si l'agent HA est loin du mobile, ce problème devient sévère.

Dans l'architecture HMIP, les réseaux d'accès sont organisés de façon hiérarchique. Les agents locaux de mobilité (LMA, local mobility agent), appelés agents étrangers de passerelle (GFA, gateway foreign agent) dans MIPv4 ou points d'ancrage de la mobilité (MAP, mobility anchor point) dans MIPv6, sont responsables de la gestion de la mobilité des terminaux mobiles au sein des domaines. Le mouvement des terminaux mobiles au sein du

domaine local sera donc caché aux agents HA et CH dans les autres réseaux, et donc le délai d'enregistrement et la redondance de signalisation peuvent être considérablement réduits. On appelle aussi l'architecture HMIP pour MIPv4 "enregistrement régional". Transfert rapide pour MIP les procédures d'enregistrement du protocole MIP ne peuvent commencer qu'après l'achèvement du transfert de la couche Liaison. On note que si les informations appropriées pouvaient être obtenues de la couche inférieure (avant l'achèvement du transfert de la couche Liaison), le délai de transfert de MIP pourrait être réduit. De plus, un tunnel bidirectionnel entre les routeurs d'accès est utilisé pour la prise en charge du transfert intercellulaire à faible perte. Le transfert à faible délai d'IPv4 mobile et le transfert rapide pour IPv6 mobile de l'IETF sont des protocoles possibles. La figure 15 nous montre l'architecture du protocole MIP avec les extensions pour la gestion de la mobilité. Comme indiqué sur la figure15, la gestion de la mobilité entre les agents LMA sera prise en charge en utilisant IP mobile. Chaque agent LMA sert à la gestion de la mobilité locale au sein d'un domaine local. Le protocole de transfert rapide sert à prendre en charge le transfert intercellulaire rapide entre les routeurs d'accès au sein d'un domaine d'agent LMA. Ces agents LMA peuvent être organisés en une hiérarchie à plusieurs niveaux.

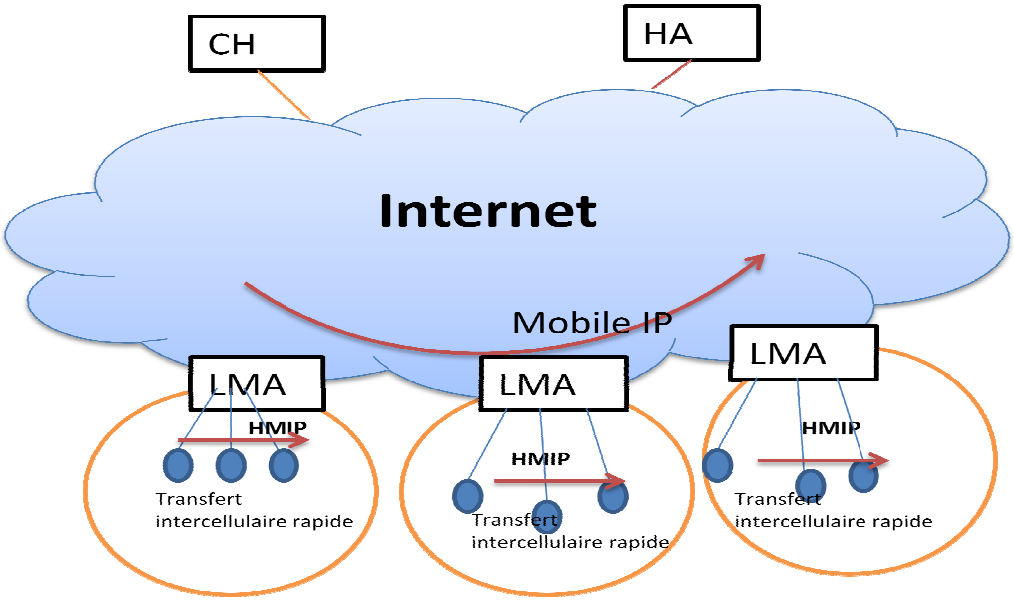


Figure 15: le protocole MIP et ses extensions pour la gestion de la mobilité

Comme il existe des problèmes en termes de délai et de perte de paquets pour la mobilité du MN géré par le protocole IPv6 Mobile, plusieurs propositions sont faites pour résoudre ces problèmes, telles que le protocole HMIPv6, FMIPv6. Cependant, ces propositions sont soit imparfaites, soit non-implantables à cause de leur complexité [30,38].

II.3 .2 Protocoles de mobilité au niveau application: Le Protocole SIP

Le protocole d'initialisation de session (SIP-Session Initiation Protocol) a été spécifié à l'IETF pour la prise en charge du contrôle des sessions multimédias fondées sur IP comme un protocole de signalisation. On trouvera des précisions sur le protocole SIP dans le document RFC 3261 de l'IETF [10].

SIP est un protocole de contrôle de couche d'application qui peut établir, modifier et terminer les sessions multimédias. Le protocole SIP utilise des identificateurs de ressource universelle (URI, Uniform Resource Identifier), qui sont semblables à des adresses e-mail, tout comme leur schéma d'adressage. Il fonctionne indépendamment des protocoles de couche Transport sous-jacents tels que le protocole de commande de transmission (TCP, Transmission Control Protocol), le protocole datagramme d'utilisateur (UDP, user datagram protocol) et le protocole de transport de commande de flux (SCTP, Stream control transmission protocol).

SIP fournit aussi la fonction de gestion de la localisation pour la prise en charge de la mobilité sur la base de l'enregistrement de l'utilisateur auprès d'un registre SIP. Lorsqu'un agent d'utilisateur (AU, user agent) SIP arrive dans une nouvelle région d'un réseau, il enregistre sa localisation actuelle dans la base de données de localisation via un registre SIP. La base de données de localisation est référencée par le serveur mandataire SIP ou le serveur de renvoi pendant l'initialisation de session générée ou terminée par l'agent d'utilisateur (AU).

Les entités fonctionnelles de SIP incluent l'agent d'utilisateur, le serveur mandataire, ou serveur de renvoi, le registre et la base de données de localisation. Les messages SIP sont classés en deux types: (1) des demandes envoyées du client d'agent d'utilisateur (CAU, user agent client) au serveur d'agent d'utilisateur (SAU, user agent server), et, (2) des réponses qui contiennent l'état de la demande.

II.3 .2.1 Gestion de la mobilité fondée sur SIP

Le protocole SIP fournit la gestion de la localisation pour la mobilité des terminaux. Lorsqu'un mobile se déplace dans un nouveau réseau, il enregistre sa localisation actuelle en envoyant un message SIP REGISTER au registre SIP. Le registre peut refuser ou accepter la demande. En cas d'acceptation, le serveur SIP va mettre à jour la base de données de localisation à l'aide des nouvelles informations de localisation.

Lorsque le mobile se déplace dans un nouveau réseau ou système, la procédure d'enregistrement SIP est répétée pour mettre à jour la localisation. Les informations de

localisation mises à jour seront aussi référencées par les serveurs mandataires durant l'initialisation de session générée ou terminée par l'agent d'utilisateur (UA).

Le protocole SIP de base ne fournit pas la gestion transparente du transfert intercellulaire [10]. Ainsi, la session SIP se termine lorsque le mobile change de réseau IP car les adresses de raccordement TCP/UDP sous-jacentes ne seront plus valides pour les nouvelles adresses IP.

Cependant, le protocole SIP, peut être utilisé en conjonction avec d'autres schémas de gestion du transfert intercellulaire: IP mobile (MIP); IP cellulaire (CIP); protocole de transmission de commande de flux mobile (mSCTP).

II.3 .3 Protocoles de mobilité au niveau transport: SCTP/mSCTP

II.3 .3.1 Le protocole SCTP

Les protocoles usuels de transport de l'information dans les réseaux IP sont TCP (Transport Control Protocol) et UDP (User Datagram Protocol). Pour répondre aux nouveaux besoins des applications de télécommunications, l'IETF (Internet Engineering Task Force) a élaboré un protocole de transport spécifique, le SCTP (Stream control transmission protocol). SCTP est un protocole **unicast** et permet l'échange de données en mode bidirectionnel entre deux nœuds ou équipements terminaux SCTP.

SCTP fournit un transport fiable, détecte le rejet, la duplication de données ainsi que les données erronées et retransmet les données corrompues. A ce propos, SCTP gère des temporisateurs plus courts que ceux de TCP car il s'agit de transporter des données de signalisation qui ont des contraintes de temps de livraison plus strictes que celles liées aux données classiques. Alors que dans TCP un flux fait référence à une séquence d'octets, un flux SCTP fait référence à une séquence de messages. SCTP est donc plus simple à interpréter à la réception. Le nom Stream Control Transmission Protocol découle de la fonction **multi-streaming** fournie par SCTP. Un Stream (flux) est un canal logique unidirectionnel permettant l'échange de messages entre équipement terminal SCTP. Lors de l'établissement d'une association SCTP, il est nécessaire de spécifier le nombre de flux que comportera cette association. La fonction multi-streaming permet de partitionner les données dans différents flux de telle sorte que la perte d'un message dans un des flux n'ait d'impact sur le transport des données que sur ce flux.

Une des fonctionnalités principales du protocole SCTP est le **Multihoming**, c'est à dire la capacité pour un **équipement terminal SCTP** de supporter plusieurs adresses IP. Ceci est un avantage comparé à **TCP**. Une connexion TCP est définie par une paire d'adresses de

transport (Adresse IP + numéro de port TCP). Chaque équipement terminal SCTP d'une association SCTP fournit à l'autre extrémité une liste d'adresses IP avec un unique numéro de port SCTP. L'équipement terminal SCTP est donc l'extrémité logique du protocole de transport SCTP. Une association SCTP associe toutes les combinaisons d'adresses sources et destinations entre les deux nœuds impliqués. Chaque équipement terminal SCTP peut être adressé par un autre équipement terminal SCTP à travers plusieurs chemins correspondant à plusieurs adresses de transport.

La fonctionnalité de Multihoming est utilisée à des fins de redondance et non pour permettre un partage de charge entre différentes routes IP. L'état de chaque chemin est supervisé par SCTP en ce qui concerne son accessibilité, le délai et le nombre de retransmissions consécutives. La supervision du chemin (path monitoring), l'utilisation d'un chemin alternatif pour des retransmissions et la sélection d'un chemin à partir de son état font de SCTP un protocole plus robuste que TCP lors de défaillances partielles du réseau.

Association

Comme mentionné précédemment, SCTP est un protocole de transport orienté connexion. Ceci implique que les points terminaux doivent suivre une procédure d'établissement de connexion. Cette relation entre les deux équipements terminaux est appelée **association SCTP**. Un exemple d'association est présenté par la figure 16.

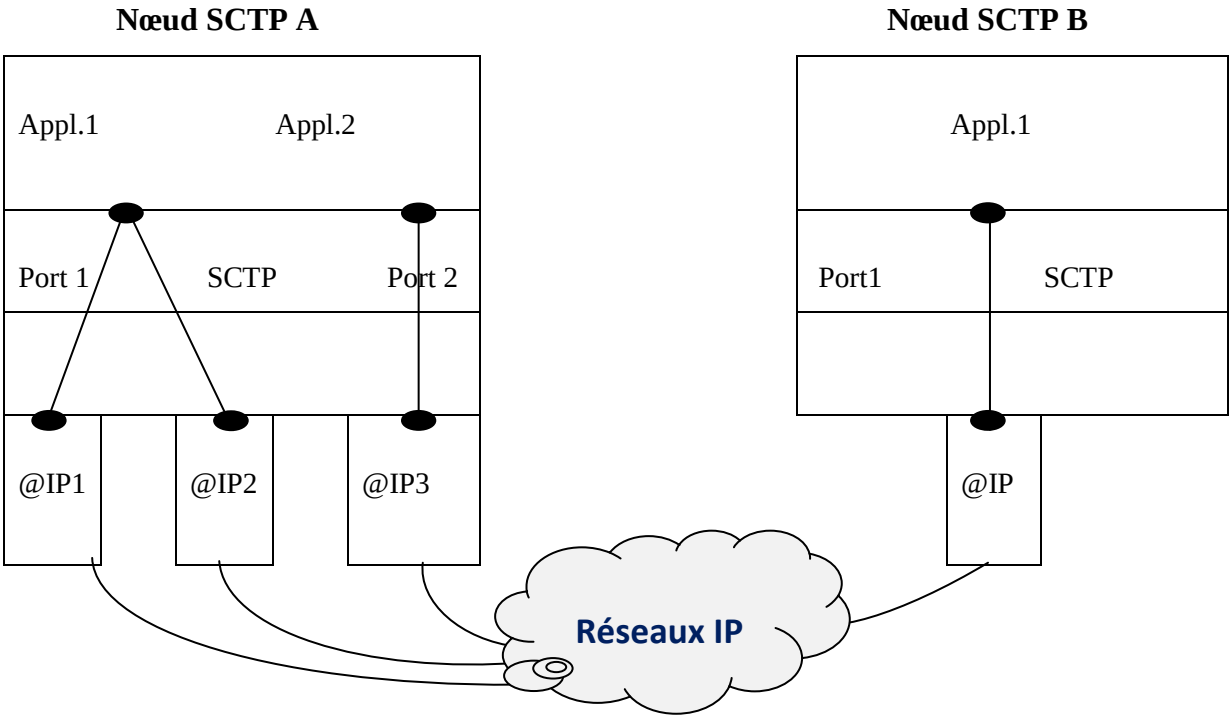


Figure 16 : Diagramme le concept d'une association SCTP

D'un point de vue réseau, un point terminal est l'extrémité logique du protocole de transport SCTP. Dans le cas d'une connexion simple (single-homed), l'identification du point terminal sera mentionnée de la manière suivante : Point terminal = [adresse IP : port SCTP].

Dans le cas d'une connexion multiple (Multihoming), les différentes adresses IP utilisées partagent un port SCTP unique :

Point terminal = [adresse IP_1, adresse IP_2, … adresse IP_n : port SCTP].

En principe c'est l'application utilisatrice du protocole de transport SCTP qui décidera lesquels des interfaces IP participeront à l'association. Cette fonctionnalité est utile lorsque plusieurs applications fonctionnent sur la même machine et que plusieurs associations doivent être établies (vers différents équipements terminaux).

Dans notre exemple (figure 16) l'application 1 du nœud A communique avec l'application 1 du nœud B. L'association établie sera décrite de la manière suivante: Association = {[@IP_1, @IP_2 : $Port_1$] : [@IP : $Port_1$]}.

Multisteaming (multiplexage de flux) et Association

Le protocole SCTP est orienté message alors que TCP est orienté octet. Chaque message est associé à un flux. Contrairement à TCP, une même connexion SCTP permet la transmission de plusieurs flux ou encore multiplexage de flux [45], c'est pour cela qu'on utilise le terme association dans SCTP (figure 17). Les flux ont été définis pour permettre de séparer le contrôle d'erreurs de la remise en séquence des messages aux couches supérieures.

Lors de l'établissement d'une association, le client et le serveur s'informent mutuellement du nombre de flux (streams) possibles dans chaque direction. Ensuite un numéro de séquence (Stream Sequence Number) est attribué aux chunk ou blocs de données de taille variable émis, indépendamment pour chaque flux. De plus, SCTP différencie le transport fiable avec la livraison ordonnée des données, offrant un choix adapté aux besoins des applications. C'est que certaines applications peuvent seulement avoir besoin d'une remise en ordre partielle des datagrammes alors que d'autres pourraient se satisfaire d'un transfert fiable qui ne garantisse aucun ordre de transmission. En effet, le protocole SCTP introduit une indépendance entre la fiabilité de transmission de données et la livraison de celles-ci aux couches supérieures, contrairement au TCP qui relie le transfert fiable de données avec la livraison ordonnée de celles ci. Chaque chunk de données utilise deux niveaux de numérotation :

1. Le TSN (Transmission Sequence Number) qui numérote les chunks au niveau de l'association. Il est utilisé pour le contrôle de la fiabilité des échanges (détection des chunks perdus, acquittements);
2. La paire (Stream ID, SSN (Stream Sequence Number)) : Le Stream ID identifie une application de destination. Le SSN sert à la reconstruction du message utilisateur à partir des chunks (s'il y a eu fragmentation du message utilisateur en plusieurs chunks) et à la remise en séquence des messages à l'application utilisateur.

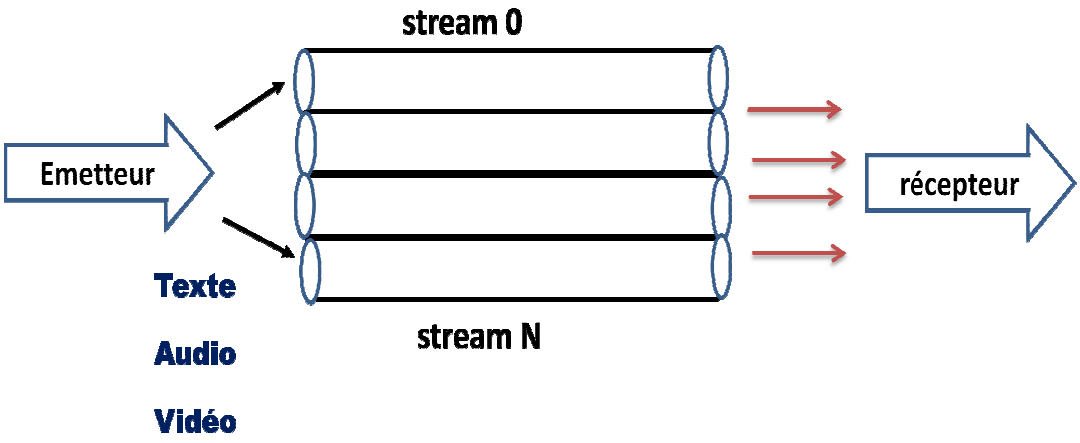


Figure 17: Principe de multisteaming en SCTP

Les chunks de données sont identifiés par leurs TSN. En SCTP le TSN compte les chunks de données émis et non pas les octets transportés par ces chunks comme dans le cas du SN (Sequence Number) de TCP. Deux chunks de données SCTP consécutifs ont deux TSN consécutifs.

Le principe de multisteaming dans les paquets SCTP forme un avantage très intéressant dans l'utilisation quotidienne d'applications diverses (comme : navigateur Web, client FTP, application de vidéo-conférence…). Chacune constituant un flux (Stream) au sein d'une même association alors qu'avec TCP elles nécessitent l'ouverture d'une connexion distincte pour chacune d'elles. Ceci entraîne la multiplication des ports que les firewalls doivent gérer d'où parfois des échecs de connexion avec TCP.

Le paquet SCTP

La PDU (Protocol Data Unit) SCTP est appelée un paquet SCTP. Le paquet SCTP est encapsulé dans un paquet IP, qui est routé à la destination. Le paquet SCTP est composé d'un en-tête commun et de Chunks. Un Chunk contient soit des données de contrôle soit des données utilisateur (Figure 18).

Plusieurs Chunks peuvent être multiplexés dans un même paquet SCTP sauf dans le cas des Chunks de contrôle INIT, INIT ACK et SHUTDOWN COMPLETE. Ces derniers ne peuvent pas être regroupés avec d'autres chunks dans un même paquet SCTP.

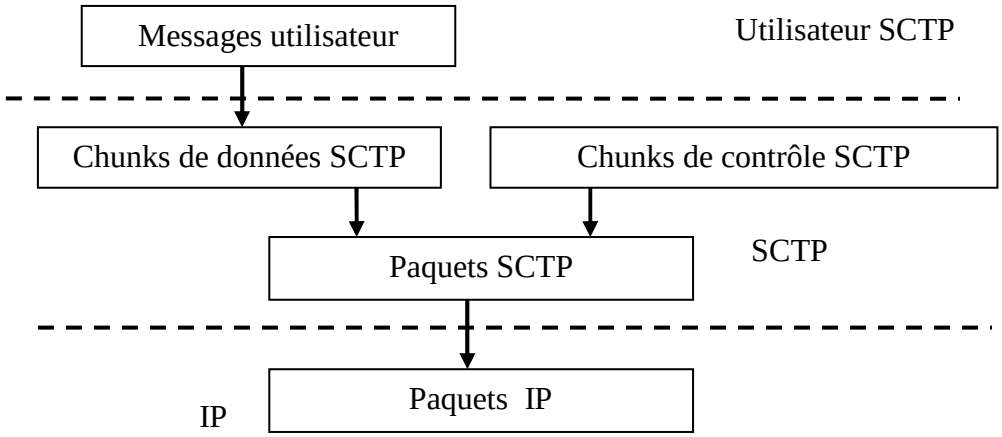


Figure 18: Chunk SCTP

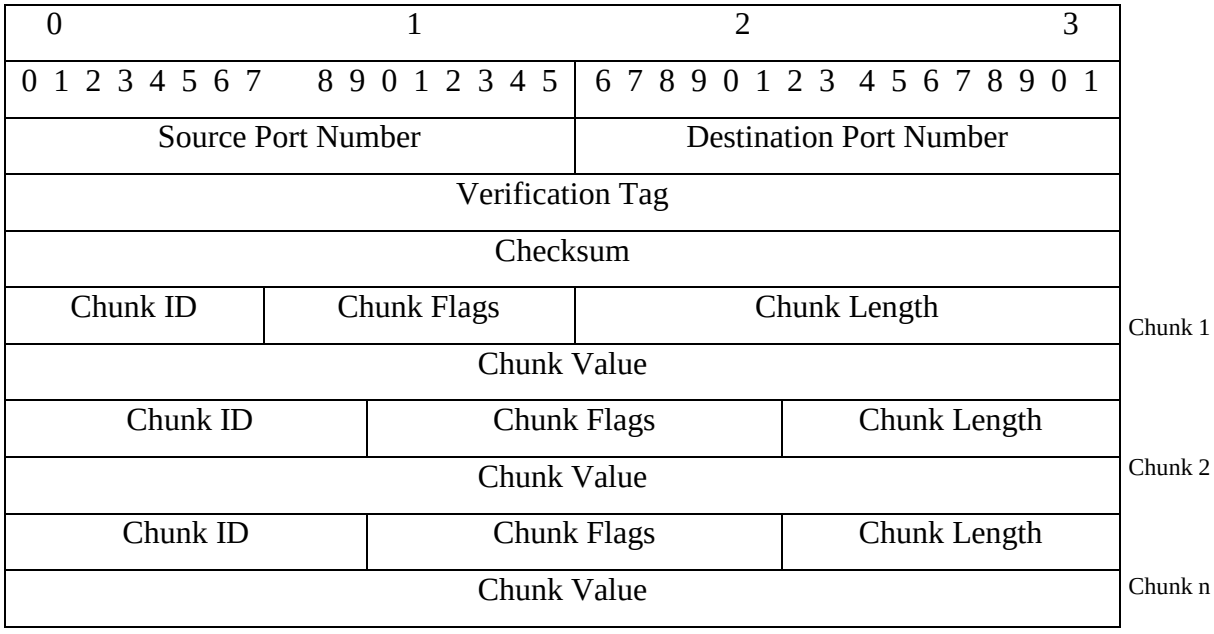


Figure 19 : Format d'un paquet SCTP

L'en-tête SCTP, d'une longueur de 12 octets identifie une association SCTP à travers le même concept de port utilisé par TCP et UDP (Figure 19). Des numéros de port en émission (2 octets) et réception (2 octets) présents dans l'en-tête combinés aux numéros d'adresses IP en émission et réception (inclus dans l'en-tête du paquet IP) identifient sans ambiguïté les équipements terminaux s'échangeant des paquets SCTP. Pour la détection des erreurs de transmission, chaque paquet SCTP est protégé par un total de contrôle (checksum)

sur 4 octets qui est plus robuste que le checksum TCP ou UDP d'une longueur de 2 octets. Un paquet SCTP dont le checksum est invalide est rejeté. L'entête contient enfin une marque de vérification (vérification tag) dont le rôle est décrit plus loin. Chaque Chunk débute par un champ chunk ID indiquant le type de Chunk afin de distinguer les Chunks de données et les différents Chunks de contrôle. Dans le cas d'un chunk de données, la valeur de Chunk ID est égale à 0. Suivent des fanions de Chunk (Chunk Flags), la longueur de Chunk (Chunk Length) nécessaire du fait de la taille variable d'un chunk, et la valeur de Chunk (Chunk Value) qui contient les données utiles du chunk. Le tableau 3 définit l'ensemble des identificateurs de Chunks (Chunk ID) utilisés afin de déterminer le type de Chunk.

Chunk ID	**Chunk Type**
00000000	Payload Data (DATA)
00000001	Initiation (INIT)
00000010	Initiation Acknowledgement (INIT ACK)
00000011	Selective Acknowledgement (SACK)
00000100	Heartbeat Request (HEARTBEAT)
00000101	Heartbeat Acknowledgement (HEARTBEAT ACK)
00000110	Abort (ABORT)
00000111	Shutdown (SHUTDOWN)
00001000	Shutdown Acknowledgement (SHUTDOWN ACK)
00001001	Operation Error (ERROR)
00001010	State Cookie (COOKIE ECHO)
00001011	Cookie Acknowledgement (COOKIE ACK)
00001100	Reserved for Explicit Congestion Notification Echo (ECNE)
00001101	Reserved for Congestion Window Reduced (CWR)
00001110	Shutdown Complete (SHUTDOWN COMPLETE)
00001111 à 11111111	Réservé par l'IETF

Tableau 3: Types de Chunk SCTP

II.3 .3.1.1 Fonctionnement du protocole SCTP

II.3 .3.1.1.1 Etablissement d'une association SCTP

L'établissement d'une association entre deux entités SCTP décrit de [59] se fait généralement par l'échange de quatre chunks: INIT, INIT ACK, COOKIE ECHO et COOKIE ACK comme le montre la figure 20. Comme SCTP hérite les avantages de TCP (fiabilité, contrôle de congestion, ….), le mode de connexion implémenté dans la spécification du SCTP, est similaire au TCP. Avant toutes échange des données, les deux entités doivent établir une association entre eux, cette association SCTP passe par les états: **établissemen**t; **échange**; puis **fermé**.

Chaque association SCTP entre deux hôtes est initialisée par quatre paquets (TCP utilise trois paquets) la bonne nouvelle du SCTP est que les données peuvent être inclus dans le 3eme et le 4^{éme} message [47], ceci peut minimiser le délai tout en augmentant la sécurité. Le premier, un bloc INIT est envoyé, en réponse il reçoit un paquet INIT ACK contenant un témoin (COOKIE). Ce paramètre permet aux associations SCTP de s'affranchir des attaques de type SYN attack ou les demi-connexions (DoS, Denial of Service) possibles avec TCP. Cependant, deux paquets supplémentaires sont envoyés. Le témoin reçoit en réponse un bloc COOKIE ECHO, lequel reçoit enfin un bloc COOKIE ACK pour sécuriser l'association.

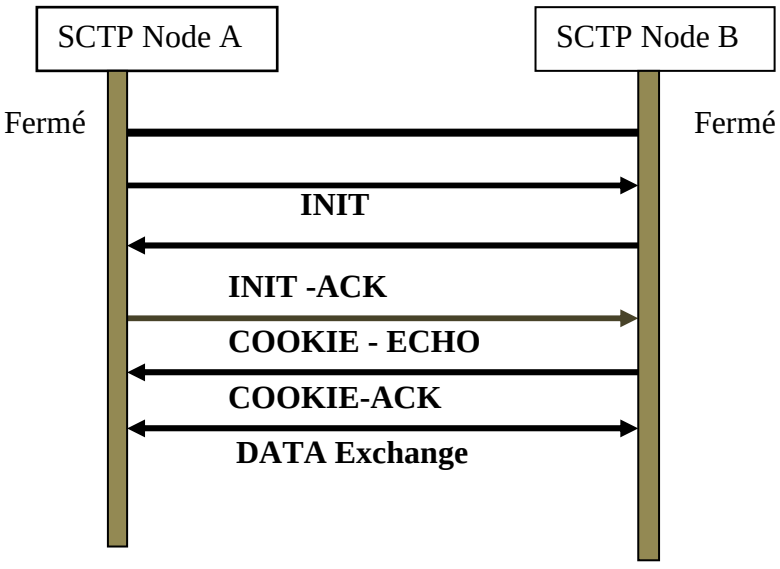


Figure 20: Scénario d'ouverture d'une association SCTP

Chunk INIT

Chaque entité SCTP est initialement dans l'état « fermé ». L'entité qui souhaité établir l'association émet un Chunk de contrôle nommé INIT (Figure 21). Le champ Chunk Flags à une valeur égale à 0. La valeur du champ InitateTag est générée aléatoirement et différente de 0. Le paquet SCTP contenant le Chunk INIT a une étiquette de vérification (Verification Tag) dont la valeur est égale à 0. L'entité réceptrice du Chunk INIT stocke la valeur du champ InitiateTag. Le champ Verification Tag de chaque paquet SCTP émis par l'entité réceptrice sur cette association aura pour valeur celle du champ InitiateTag.

Le Chunk INIT contient par ailleurs un champ **Advertised Receiver Credit Windows (a_rwnd)** qui indique l'espace mémoire en nombre d'octets que l'émetteur a alloué pour l'association qui sera établie. Pendant la durée de vie de l'association, cet espace mémoire ne peut diminuer mais peut augmenter. Le paramètre **Number of Outbound Streams** (**OS**) spécifie le nombre de flux unidirectionnels (streams) que l'émetteur souhaite créer dans cette association. La valeur 0 ne peut pas être utilisée.

Le paramètre **Number of Inbound Streams (MIS)** définit le nombre maximum de flux unidirectionnels (streams) que l'émetteur permet au récepteur de créer dans cette association. La valeur 0 ne peut pas être utilisée.

Le paramètre Initial TSN indique le numéro de TSN (Transmission Sequence Number) initial que l'émetteur utilisera lors de l'envoi du premier Chunk DATA dans cette association. Le paramètre TSN présent dans chaque Chunk DATA permet de numéroter de façon incrémentale ces Chunks dans le contexte d'une association.

Le Chunk INIT peut par ailleurs contenir un nombre de paramètres optionnels ou de longueur variable (Optional/Variable-Length parameters). Parmi ces paramètres figurent l'adresse IPv4 ou IPv6 de l'émetteur. Combinée au numéro de port SCTP de l'émetteur présent dans le paquet SCTP, cette adresse permet à l'émetteur d'indiquer au récepteur l'adresse de transport qu'il supporte pour cette association.

Plus d'un paramètre d'adresse Ipv4 ou IPv6 peut être inclus dans un Chunk INIT si l'entité SCTP émettrice est de type «Multihoming ».

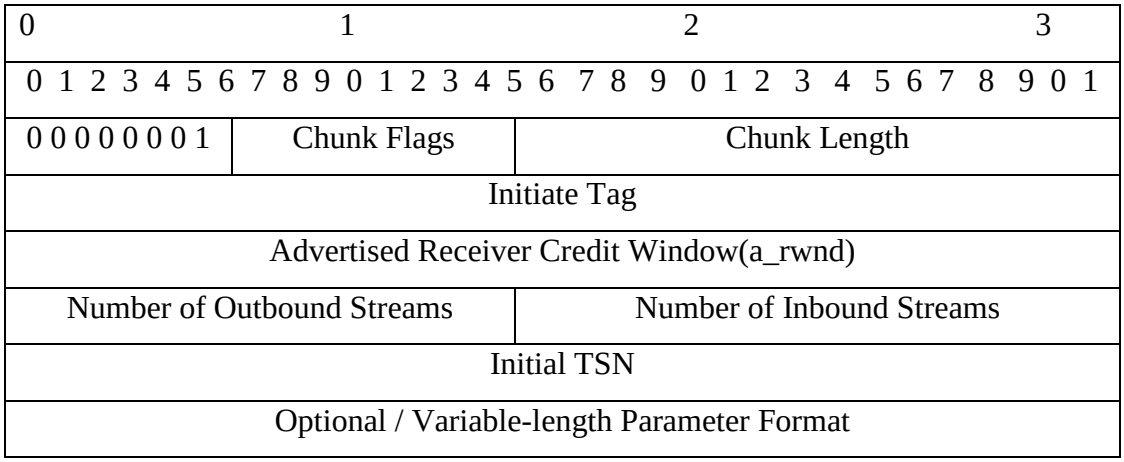


Figure 21: Chunk INIT

Chunk INIT ACK

A la réception du Chunk INIT, l'entité SCTP réceptrice retourne un Chunk INIT ACK .Ce dernier a un format similaire à celui du Chunk INIT. Il rajoute deux paramètres, Cookie State et Unrecognized.

Le récepteur rappelle les valeurs des paramètres qu'il a reçu dans le Chunk INIT. Il ne lui est pas possible de négocier une valeur du paramètre Number of Inbound Streams(MIS) supérieure à celle reçue.

La valeur du paramètre Initial TSN indique la valeur de TSN que l'émetteur du message INITACK utilisera lors de l'envoi de son premier Chunk DATA dans cette association.

Le Chunk INIT ACK contient un nombre de paramètres de longueur variable (Optional /Variable-Length parameters) et éventuellement des paramètres optionnels. Le seul paramètre obligatoire dont la taille est variable est State Cookie.

Parmi les paramètres optionnels figurent la ou les adresses IPv4 et/ou IPv6 de l'entité réceptrice qui seront utilisées dans cette association, ainsi que Unrecognized. Ce dernier sera inclus dans le Chunk INIT ACK lorsque l'entité réceptrice du Chunk INIT ne reconnaît par un des paramètres (figure 22).

0	1	2	3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1			
0 0 0 0 0 0 0 1	Chunk Flags	Chunk Length	
Initiate Tag			
Advertised Receiver Credit Window			
Number of Outbound Streams		Number of Inbound Streams	
Initial TSN			
Optional / Variable-length Parameter Format			

Figure 22: Chunk INIT ACK

Chunk COOKIE ECHO

A la réception du Chunk INIT ACK, l'initiateur de l'association renvoie un Chunk COOKIEECHO afin de finaliser l'établissement de l'association (Figure 23). Ce Chunk doit précéder l'envoi de tout Chunk DATA mais peut partager le même paquet SCTP que des Chunks DATA en étant le premier Chunk du paquet. La valeur du champ Chunk Flags est égale à 0 et ignorée à la réception. Le Chunk COOKIE ECHO doit contenir le paramètre Cookie dont la valeur est celle du paramètre State Cookie reçu dans le Chunk INIT ACK.

0	1	2	3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1			
0 0 0 0 0 0 0 1	Chunk Flags	Chunk Length	
Cookie			

Figure 23: Chunk COOKIE ECHO

Chunk COOKIE ACK

A la réception du Chunk COOKIE ECHO, un Chunk COOKIE ACK est retourné. La valeur du champ Chunk Flags est positionnée à 0 alors que la longueur du Chunk (Chunk Length) est égale à 4 (Figure 24). Ce Chunk doit précéder tout Chunk DATA envoyé par l'émetteur de ce Chunk COOKIE ECHO, et avant tout message SACK acquittant des messages DATA reçus. Par contre, il peut partager le même paquet SCTP que ces Chunks DATA et SACK, mais en première position dans ce paquet.

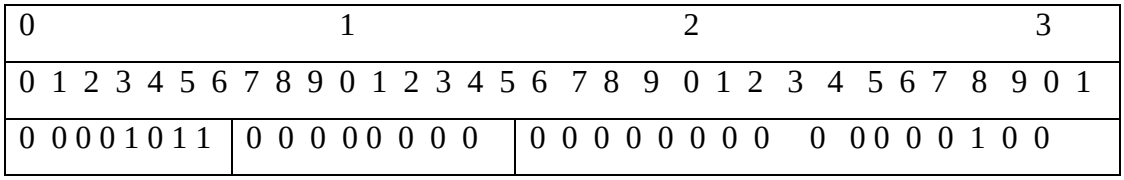


Figure 24: Chunk COOKIE ACK

Le Chunk DATA

Le Chunk DATA est utilisé afin de transporter les données provenant de la couche cliente (Figure 25). Le bit U (Unordered) s'il est positionné à 1 indique que les données doivent être délivrées par SCTP à la couche cliente réceptrice, dans l'ordre reçu. Il est possible de fragmenter un message utilisateur dont la taille est supérieure à celle du paquet SCTP. Les bits B et E sont utilisés afin d'informer le récepteur de cette fragmentation (Voir tableau 4).

Le bit B (Beginning) s'il est positionné à la valeur 1 indique le premier fragment du message utilisateur. Le bit E (End) mis à la valeur 1 précise qu'il s'agit du dernier fragment du message. Pour un message non fragmenté, les bits B et E ont pour valeur 1.

Bit B Begining	**Bit E** Ending	**Signification**
1	0	Première partie d'un message fragmenté
0	0	Partie intermédiaire d'un message fragmenté
0	1	Dernière partie d'un message fragmenté
1	1	Message non fragmenté

Tableau 4: Signification des bits B et E

Lorsqu'un message utilisateur est fragmenté en plusieurs Chunks DATA, le champ TSNs (Transmission Sequence Number) est utilisé afin de réassembler le message. Ce champ TSN identifie le message utilisateur dans le contexte d'une association indépendamment d'un Stream particulier et est incrémenté à chaque envoi d'un Chunk DATA modulo $2^{32} - 1$. Le champ Stream Identifier **(S)** indique le flux (streams) auquel appartient ce Chunk DATA.

Le champ Stream Sequence Number **n** indique la position de ce Chunk DATA dans le flux. Lorsqu'un message utilisateur est fragmenté par SCTP, toutes les parties du message encapsulé dans des Chunks DATA ont le champ SSN positionné à la même valeur.

Le champ Payload Protocol Identifier représente un identificateur de protocole de la couche cliente. La valeur associée est passée par la couche cliente émettrice à SCTP et retournée à la couche cliente réceptrice afin de lui permettre d'identifier le type d'information transportée dans ce DATA Chunk.

Le champ User Data contient le message utilisateur sur un nombre d'octets multiple de 4. Sil a longueur du message utilisateur n'est pas un multiple de 4, des octets de bourrage (au maximum 3) pourront alors être insérés dont la valeur sera « 00000000 ».

Le champ Length indique la longueur du Chunk DATA en octets, à partir du premier champ (Chunk Type dont la valeur est 00000000) jusqu'à la fin du champ User Data en excluant les octets de bourrage. Un Chunk DATA sans données utilisateur à un champ Length positionné à la valeur 16 (00010000).

<table>
<tr><td colspan="6">0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1</td></tr>
<tr><td>0 0 0 0 0 0 0 0</td><td>Reserved</td><td>U</td><td>B</td><td>E</td><td>Length</td></tr>
<tr><td colspan="6">TSN</td></tr>
<tr><td colspan="3">Stream Identifier S</td><td colspan="3">Stream Sequence Number n</td></tr>
<tr><td colspan="6">Payload Prototocol Identifier</td></tr>
<tr><td colspan="6">User Data</td></tr>
</table>

Figure 25: Chunk DATA

Chunk SACK

Le Chunk SACK est émis par une entité SCTP afin d'acquitter les Chunks DATA reçus de l'autre entité SCTP et de l'informer d'éventuels « gaps » ou absences dans les Chunks DATA consécutifs reçus.

II.3 .3.1.1.2 Libération d'une association SCTP

L'association est libérée proprement par un chunk SHUTDOWN ou abandonnée brutalement par un chunk ABORT (figure 26).Quand un utilisateur/application désire fermer le socket SCTP proprement, il utilise le chunk SHUTDOWN. L'endpoint SCTP envoie alors toutes les données encore dans ses mémoires tampon, et ensuite émet le chunk SHUTDOWN. Quand le destinataire reçoit le chunk SHUTDOWN, il arrête d'accepter des données provenant de l'application et cesse d'envoyer des données. Une fois obtenus tous les SACK pour les données, il enverra un chunk SHUTDOWN ACK, et une fois que le côté qui libère l'association a reçu ce chunk, il répondra par un chunk SHUTDOWN COMPLETE. L'association est dorénavant complètement libérée.

Une autre façon de terminer l'association est d'utiliser le chunk ABORT. Mais c'est un moyen plus brutal de terminer une association SCTP. Quand une des deux parties désire terminer une association SCTP instantanément, elle émet ce chunk ABORT. Toutes les données dans les tampons sont alors supprimées et l'association terminée. Le destinataire fait de même après vérification du chunk ABORT.

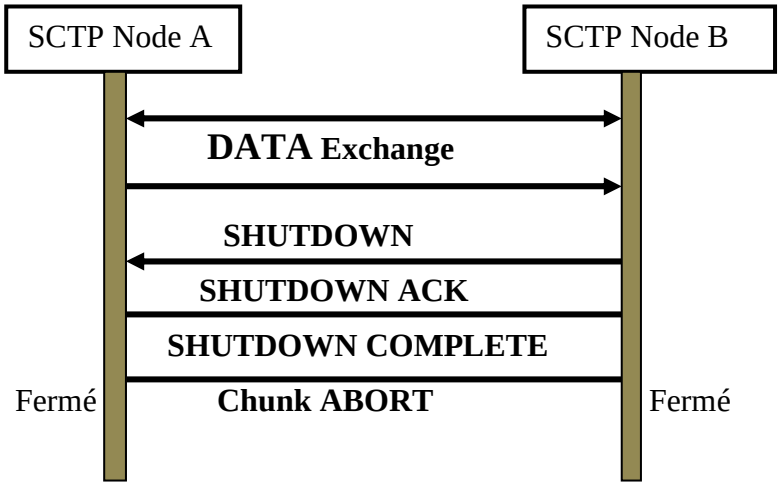


Figure 26: Scénario de Libération d'une association SCTP

Chunk SHUTDOWN

Le chunk SHUTDOWN (figure 27) apparaît quand un des endpoints d'une association désire fermer l'association en cours. L'équipement terminal qui le transmet doit vider tous ses tampons avant d'expédier le chunk SHUTDOWN, et ne doit pas envoyer d'autres chunks DATA par la suite.

Le destinataire doit également vider ses tampons d'émission et ensuite expédier le chunk SHUTDOWN ACK correspondant.IL contient les champs suivants:

- Le champ Chunk Flags dont la valeur est positionnée à 0;
- Le champ Chunk Length qui indique la longueur du Chunk et dont la valeur est égale à 8;
- Le champ Cumulative TSN ACK indique le TSN du dernier Chunk DATA reçu en séquence avant toutes pertes (gap).
- Le champ Cumulative TSN ACK indique le TSN du dernier Chunk DATA reçu en séquence avant toutes pertes (gap).

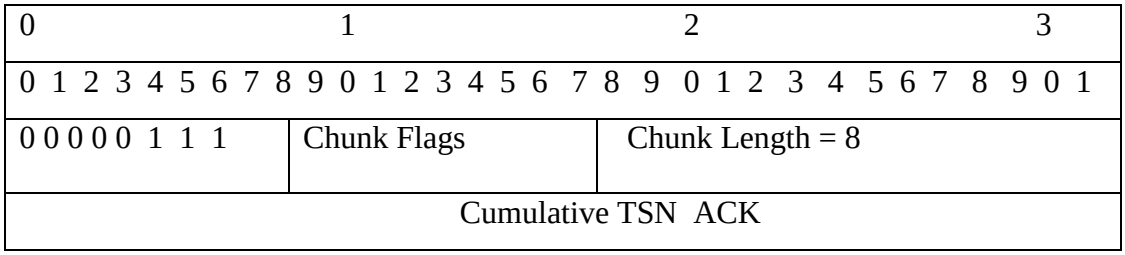


Figure 27: Chunk SHUTDOWN

Chunk SHUTDOWN ACK

Le chunk SHUTDOWN ACK (figure 28) est utilisé pour accuser réception d'un bloc SHUTDOWN reçu. Avant que le bloc SHUTDOWN ACK soit envoyé, toutes les données dans les tampons d'envoi doivent être expédiées, les tampons ne doivent plus accepter aucune donnée provenant de l'application.

Le chunk SHUTDOWN ACK contient les champs suivants:

- Le champ Chunk Flags dont la valeur est positionnée à 0;
- Le champ Chunk Length qui indique la longueur du Chunk et dont la valeur est égale à 4.

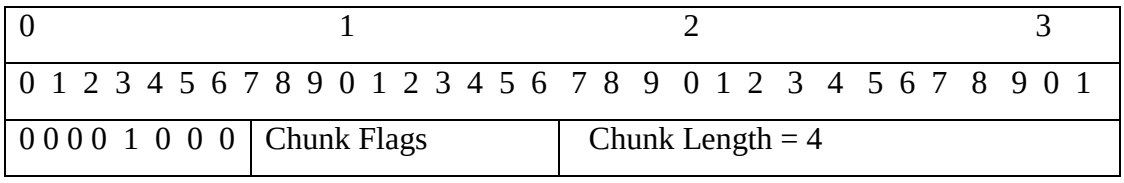


Figure 28: Chunk SHUTDOWN ACK

Chunk SHUTDOWN COMPLETE

Le chunk SHUTDOWN COMPLETE (figure 29) est envoyé, par l'expéditeur du SHUTDOWN, en réponse au chunk SHUTDOWN ACK. Il est expédié pour accuser réception que l'association est totalement fermée. Il contient les champs suivants:

- Le champ Chunk Flags dont la valeur est positionnée à 0;
- Le champ Chunk Length qui indique la longueur du Chunk et dont la valeur est égale à 4.

0 1 2 3			
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1			
0 0 0 0 1 1 1 0	Reserved	T	Chunk Length = 4

Figure 29: Chunk SHUTDOWN COMPLETE

Chunk ABORT

Le chunk ABORT est utilisé pour abandonner une association (figure 30).Parmi les causes d'erreurs qui conduisent à l'envoi du chunk ABORT figurent :

- Out of resource : l'équipement terminal émettant l'ABORT n'est pas en mesure de maintenir l'association à cause de problèmes de ressources internes;
- Unresolvable Address Error : l'équipement terminal a reçu une adresse de hostname de l'autre équipement terminal pendant la phase d'initialisation de l'association. Or cette adresse de hostname ne peut pas être résolue par le DNS en une adresse IP;
- Invalid Mandatory Parameter : Il est possible qu'un des chunks reçus présente un paramètre obligatoire invalide. Par exemple, l'émetteur du chunk INIT a positionné le champ « nombre de streams » à la valeur 0 qui n'est pas une valeur acceptable. Le récepteur du chunk INIT l'acquitte alors par un ABORT en précisant la cause de l'erreur;
- No User Data Error: Si un endpoint SCTP émet un chunk DATA sans données utilisateur, le récepteur est dans l'obligation de retourner un chunk ABORT et de supprimer l'association.

0 1 2 3		
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1		
0 0 0 0 0 1 1 0	Reserved	Length
0 or more Error Causes		

Figure 30: Chunk ABORT

II.3 .3.1.2 Multihoming(Multi-domiciliation)

Le Multihoming est une propriété essentielle de SCTP. Il permet à une association SCTP d'être associée à plusieurs adresses sources et destination. Chaque terminal peut ainsi être atteint via plusieurs adresses IP. SCTP apporte uniquement un mécanisme de sauvegarde de chemin [39]. Un seul chemin est actif à la fois, le partage de charge ne fait pas partie de la spécification actuelle du protocole [39, 40]. Chaque nœud peut être accessible par plusieurs adresses de transport (figure 31) fixées au moment de l'ouverture de l'association. Les adresses de transports (c'est-à-dire, liste d'adresses IP + port SCTP) sont échangées lors de la phase d'initialisation d'une association SCTP (chunks INIT et INIT Ack).L'intérêt majeur du Multihoming dont les transmissions vers des nœuds multihomed peuvent ainsi gagner en robustesse contre les défaillances du réseau ou les problèmes de congestion en choisissant dynamiquement une alternative, à la condition que des chemins différents soient constitués pour chaque adresse IP du nœud. SCTP voit les adresses IP d'un client multihomed comme «différents chemins» possibles pour l'atteindre [**27**]

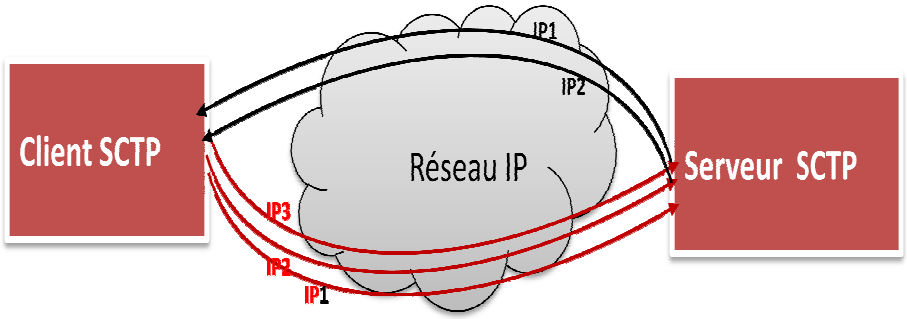


Figure 31: Exemple de nœuds SCTP Multihoming

II.3 .3.1.2.1 Gestion des adresses IP

Les protocoles des couches supérieures (ou ULP-Upper Layer Protocol) déterminent toutes les adresses transport et fixent le chemin primaire (chemin par lequel transite le trafic utilisateur en condition normale). Pour effectuer une transmission vers un nœud Multihoming, l'émetteur choisit préalablement une des adresses possibles qui correspondra au chemin primaire (lors de l'établissement de l'association). L'émetteur ne doit par la suite envoyer des données que par ce chemin primaire. De plus, pour acquitter des paquets SCTP d'un nœud multihomed, l'émetteur des chunks SACK devrait utiliser le même chemin que celui emprunté par les chunks de données reçus [39]. Cependant, lorsque le récepteur obtient plusieurs chunks dupliqués, il peut supposer que ses chunks SACK empruntent un chemin défaillant, il serait alors peut être judicieux d'utiliser une autre adresse secondaire. Lors de retransmissions il serait également intéressant d'utiliser une autre adresse secondaire possible,

la perte de paquets pouvant être liée à un problème de l'adresse primaire, et permet ainsi de réduire les risques de congestion. Lorsque le chemin primaire devient inaccessible (suite à une congestion, ou à une perte de données importante), SCTP basculera tout le trafic sur un des chemins secondaires de l'association considérée (vers une adresse de transport secondaire du nœud de destination). La fonction de Multihoming, est uniquement utilisée à des fins de sauvegarde.

II.3 .3.1.2.2 Contrôle des adresses empruntées (ou des chemins)

SCTP se doit de contrôler régulièrement les différentes adresses d'un nœud multihomed. Pour cela il considère deux états possibles pour chacun des chemins possibles : actif ou inactif. Le chemin primaire étant considéré actif, la disponibilité des alternatives est contrôlée par l'envoi régulier de chunks HEARTBEAT Request, qui doivent être acquittés par un chunk HEARTBEAT ACK. Si une adresse ne répond pas après plusieurs HEARTBEAT infructueux, le chemin est considéré inactif.

La décision sur le fait qu'une adresse est accessible ou non est prise selon un mécanisme d'écoute appelé heartbeating. Un chemin primaire est supposé inactif, si l'émetteur ne peut plus y accéder suite à l'occurrence de plusieurs expirations de timer RTO (Retransmission Time Out) consécutives. Dans ce cas les paquets SCTP seront routés vers une autre adresse supposée active. Le choix de l'adresse IP secondaire de destination à activer se fait en contactant le nœud destination via un chunk Heartbeat Request (figure32). Le nœud SCTP distant doit répondre avec un chunk Heartbeat Ack (figure 33) en indiquant l'adresse IP secondaire qui sera active dans l'association en cours.

Chunk type = 4	Flags	Heartbeat length
Heartbeat Info type = 1	Heartbeat info length	
Sender specific Heartbeat info		

Figure 32: Format du chunk Heartbeat info

Chunk type = 5	Flags	Heartbeat-Ask length
Heartbeat-Ask Info type = 1	Heartbeat-Ask info length	
Sender specific Heartbeat info		

Figure 33: Format du chunk Heartbeat-Ask

Un chunk heartbeat est envoyé périodiquement vers les adresses de transport de destination en veille [40] (peut être active ou inactive) afin de mettre à jour leurs états d'accessibilité. La période est donnée par Hi. La période d'émission d'un chunk heartbeat est contrôlée par le paramètre HB. Interval (30 seconde) [39].

Hi=RTOi + HB.Interval (1+d).

Où, RTOi est le RTO sur le chemin secondaire «i» calculé sur les chunks heartbeat, et d est une valeur choisie aléatoirement dans [-0.5, 0.5] à l'initialisation de l'association. Lors de transfert de données au sein d'une association multihomed des considérations doivent être prises en compte :

1. Quand l'émetteur est multihomed, le récepteur ne doit pas nécessairement envoyer un SACK vers l'adresse de transport primaire de l'émetteur.
2. Lorsque le récepteur est multihomed et que l'émetteur a besoin de retransmettre un ou plusieurs chunks de données, l'émetteur peut considérer la retransmission vers une adresse secondaire de l'association [39].

Il faut noter qu'en cas d'erreur sur la liaison primaire, l'émetteur utilisera un des chemins secondaires pour émettre les données vers le récepteur. Pour une association un seul chemin est considéré comme primaire les autres sont des chemins de secours. Seulement des messages d'écoute(Heartbeat) circulent sur les chemins secondaires dits aussi alternatifs.

II.3 .3.1.2.3 Transfert de données dans une association avec Multihoming

Comme nous l'avons signalé ci-dessus, SCTP supporte la fonctionnalité de Multihoming afin de permettre à des sessions, ou des associations dans la terminologie SCTP, de se maintenir même lorsqu'une adresse IP d'un hôte n'est plus accessible. SCTP a un système intégré de détection et de rétablissement d'erreurs, qui permet aux associations d'envoyer dynamiquement le trafic vers une adresse IP alternative de destination si cela s'avère nécessaire. Comme indiqué dans la [39], l'utilisation du Multihoming en SCTP ajoute au protocole les fonctions de base suivantes :

1. Dans une association, un chemin unique est considéré primaire. Ceci signifie qu'une des adresses IP affectées au récepteur de l'association est choisie pour être l'adresse primaire. Le chemin primaire correspond au chemin réseau qui mène à l'adresse primaire du point terminal qui lui est associé. Sauf contre-indication par l'utilisateur SCTP, un point terminal devrait toujours transmettre sur le chemin primaire;
2. Lors de l'acquittement des chunks reçus, les chunks SACK doivent emprunter le même chemin qui a été emprunté par les chunks reçus;
3. Dans le cas de retransmission de chunk vers un point terminal multihomed, le récepteur doit choisir une adresse de destination autre que celle à laquelle le chunk de données original a été envoyé. Aussi bien, quand un point terminal reçoit un chunk de données dupliqué, il peut changer l'adresse de destination et ne pas utiliser l'adresse source de ce

chunk de données dupliqué pour envoyer un acquittement. En fait, il faut considérer toutes les alternatives d'adresses de transport (source/destination) pour sélectionner l'adresse source-destination la plus adéquate pour la retransmission. Il n'y a aucune stratégie adoptée pour le choix de l'adresse définie par la norme (voir l'algorithme RR: Round Robin)[24].Ainsi le mécanisme Multihoming, supporté par des machines et des équipements réseau, est une solution techniquement faisable et de plus en plus économique [42].

II.3 .3.1.3 Contrôle de flux et de congestion

Dans un système de communication, la congestion peut apparaître soit du côté récepteur soit dans le réseau. Du côté récepteur, la congestion est généralement due à la taille des fils d'attentes de réception tandis que dans le réseau, elle est couramment due à la saturation des liaisons. Dans le premier cas, le problème de congestion est résolu par le champ : Advertised Receiver Windows (a_rwnd) qui se trouve dans les chunks de type INIT, INIT-ACK et SACK. Ce paramètre indique à l'émetteur combien de bytes le récepteur est prêt à recevoir. Dans le deuxième cas, le contrôle de flux se fait moyennant les mêmes algorithmes utilisés par TCP, en l'occurrence, le Congestion Windows (cwnd) qui permet de contrôler le nombre de bytes que l'émetteur peut envoyer et le Slow Start Threshold (ssthresh) qui permet de choisir le bon algorithme de congestion au bon moment[18].En guise de conclusion de cette sous-section, le tableau 5 donne une récapitulation sommaire des propriétés relatives aux principaux protocoles de transport présentés dans le manuscrit.

caractéristique	**SCTP**	**TCP**	**UDP**
Transfert de données fiable	Oui	Oui	non
Contrôle de congestion	Oui	Oui	non
Découverte MTU	Oui	Oui	non
Multiplexage de message	Oui	Oui	non
Support du Multihoming	Oui	non	non
Support du Multisteaming	Oui	non	non
Livraison de données désordonnée	Oui	non	oui
Sécurité	Oui	non	non
Heartbeat intégré	Oui	non	non

Tableau 5: Comparaison entre les protocoles de transport SCTP, TCP et UDP

II.3 .3.2 Multihoming et mobilité

II.3 .3.2.1 Aperçu général

Le protocole de transport des commandes de flux (SCTP), défini dans le document RFC 2960 [44] de l'IETF, est un protocole de bout en bout, orienté connexion, qui transporte des flux de données multiples. Le caractère multirattachement (Multihoming) de SCTP permet aux points de terminaison SCTP de prendre en charge plusieurs adresses IP. Le multirattachement protège une association des défaillances de réseau potentielles en dirigeant le trafic sur les adresses IP de remplacement. Durant l'initialisation d'une association, les points de terminaison SCTP échangent les listes d'adresses IP. Chaque point de terminaison peut donc envoyer et recevoir des messages de toutes les adresses IP dont la liste est détenue par le point d'extrémité. Par exemple, une des adresses IP figurant sur la liste sera désignée comme adresse primaire durant l'initialisation. Si l'adresse primaire perd des paquets de données de façon répétée, tous les paquets de données suivants seront transmis à une adresse de remplacement jusqu'à ce que l'adresse primaire puisse être rétablie.

On note que le caractère multirattachement de SCTP permet de prendre en charge la mobilité sur IP. Plus précisément, le protocole SCTP avec une extension de configuration dynamique d'adresse peut servir à fournir un transfert intercellulaire en douceur aux terminaux (MT) qui passent dans différentes régions de réseaux IP au cours d'une session d'activité. Ceci est appelé SCTP mobile (mSCTP) et s'applique aussi bien à IPv4 qu'à IPv6.

mSCTP est un schéma de transfert intercellulaire prometteur. A la différence des schémas de transfert intercellulaire fondés sur IP mobile qui reposent sur la prise en charge de routeurs réseau pour le tunnelage entre les routeurs d'accès, mSCTP permet la gestion du transfert intercellulaire à la couche Transport sans changement supplémentaire des routeurs existants

II.3 .3.2.2 Mobile-SCTP (mSCTP): Extension de SCTP (Adressage dynamique)

Cette fonctionnalité introduit une extension au SCTP [41,42] qui lui offre la possibilité de :

1. Reconfigurer des adresses IP au cours de l'association en cours;
2. Changer la route primaire (Routage vers une nouvelle adresse primaire);
3. Échanger des informations d'adaptation de couche durant l'établissement d'association. Ce qui assure un basculement de lien sans pertes de données.

Cette extension consiste à la création de deux nouveaux types de chunk : Address Configuration Change Chunk **ASCONF** et Address Configuration Acknowledgement **ASCONFACK**. Ces deux chunks contribueront à l'ajout et la suppression dynamiques des adresses IP à une association ainsi qu'à la génération d'une demande de changement d'adresse primaire au cours de la même association.

Le chunk ASCONF est utilisé pour communiquer au point terminal distant une des demandes de changement de configuration. Ces demandes sont spécifiées par l'un des nouveaux paramètres introduits par cette extension. Ces demandes doivent être acquittées au moyen du chunk ASCONFACK comprenant les paramètres spécifiques pour assurer la réponse à une demande reçue (échec ou succès de l'opération). Ces chunks sont transmis de façon authentifiée.

De nouveaux paramètres sont introduits pour décrire la nature de l'opération exigée par l'un des deux points terminaux d'une association afin de changer sa configuration. Les deux types de chunks associés aux six paramètres nouvellement introduits par cette extension servent pour ajouter et supprimer dynamiquement des adresses IP d'une association et donc de changer d'adresse primaire (changer la configuration d'une association). Les six nouveaux paramètres introduits par cette extension sont :

1. **Add IP Address (ASCONF):** permet d'ajouter une nouvelle adresse IP à l'association en cours;
2. **Delete IP Address (ASCONF):** permet de supprimer une adresse IP de l'association en cours;
3. **Error Cause Indication (ASCONF-ACK):** c'est un paramètre de réponse, qu'est utilisé pour contourner une ou plusieurs causes d'erreur usuelles rencontrées en SCTP;
4. **Set primary IP Address** : ce paramètre peut être intégré dans les chunks ASCONF, INIT ou INITAck. L'intégration de ce paramètre dans INIT ou INIT-Ack peut être utilisée pour indiquer une préférence d'une adresse primaire;
5. **Success Indication (ASCONF-ACK)** : ce paramètre est utilisé pour indiquer le succès de réception des données contenues dans le chunk ASCONF.
6. **Adaptation Layer Indication** : ce paramètre peut apparaître dans les chunks INIT et INIT Ack et devrait être remonté aux protocoles de couche supérieure du récepteur. Ce paramètre ne doit pas apparaître dans le chunk ASCONF. Il est envisagé qu'il soit utilisé pour le contrôle de flux et pour l'adaptation à d'autres couches qui exigent une indication qui soit contenue dans les chunks INIT et INIT-Ack.

II.3 .3.2.3 Scénario mSCTP pour transfert intercellulaire dans la couche transport

mSCTP [44], peut être utilisé pour fournir le transfert intercellulaire à un terminal mobile qui se déplace entre deux réseaux IP différents caractérisés par des préfixes d'adresse IP différents. Le présent paragraphe décrit l'algorithme générique de mSCTP pour le transfert dans les réseaux IP.

Considérons un mobile (MT) qui initialise une association SCTP avec un serveur correspondant(CH). Après l'initialisation d'une association SCTP, le MT passe de la localisation A (routeur d'accès A) à la localisation B (routeur d'accès B), comme indiqué à la figure 34, qui illustre un exemple d'utilisation de mSCTP pour le transfert intercellulaire dans les réseaux IPv6. Les procédures de transfert sont décrites plus en détail ci-dessous. Cet exemple s'applique de façon similaire aux réseaux IPv4.

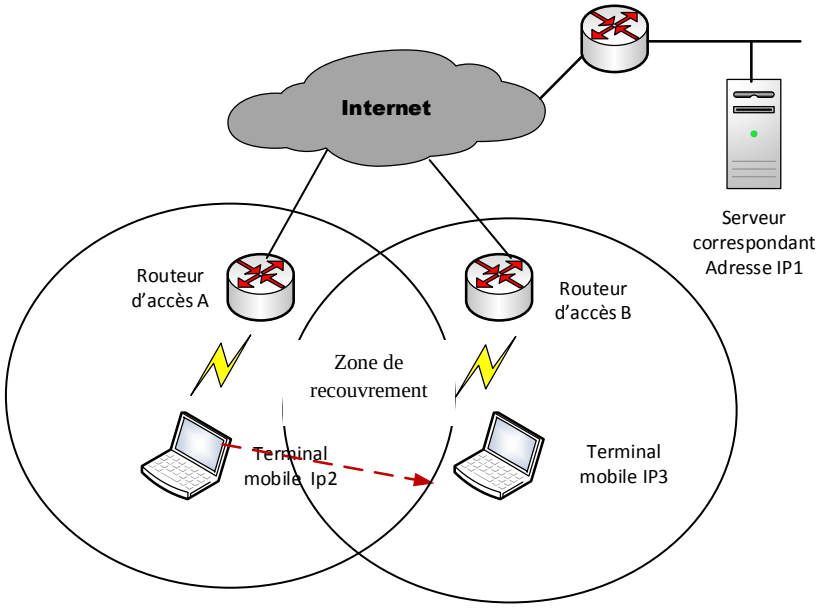


Figure 34: mSCTP pour transfert intercellulaire

Initialisation de session par le mobile

Un MT initialise une association SCTP avec un serveur CH. Le MT obtient une adresse IP du routeur d'accès (AR) A via une auto configuration d'adresse sans état IPv6 ou DHCPv6.

1. **Obtention d'une adresse IP pour une nouvelle localisation**

Le MT passe d'AR A vers AR B et entre dans la région de recouvrement de couverture des deux routeurs d'accès. Le MT obtient une nouvelle adresse IP 3 de l'AR B en

utilisant DHCIPv6 ou l'auto configuration d'adresse sans état IPv6. La nouvelle adresse IP 3 obtenue est signalée au protocole SCTP dans la couche Transport, puis le protocole SCTP lie la nouvelle adresse IP à la liste d'adresses gérée par l'association SCTP.

2. Ajout de la nouvelle adresse IP à l'association SCTP

Après obtention de la nouvelle adresse IP, le SCTP du mobile informe le SCTP du serveur correspondant CH qu'il va utiliser une nouvelle adresse IP. Ceci est fait par l'envoi d'un changement de configuration d'adresse SCTP (ASCONF) au CH. Le MT peut recevoir l'ASCONF-ACK de réponse du CH.

Le MT est alors dans un état de double rattachement. La vieille adresse IP (adresse IP 2) est toujours utilisée comme adresse primaire, jusqu'à ce que la nouvelle adresse IP 3 soit établie comme "Adresse primaire" par le MT. Avant que la nouvelle adresse primaire ne soit établie, l'adresse IP 3 est utilisée comme voie de secours.

3. Changement d'adresse IP primaire

Alors que le MT continue d'avancer vers le routeur AR B, il a besoin de changer la nouvelle adresse IP en adresse IP primaire, conformément à une règle appropriée. La configuration d'une règle spécifique pour déclencher ce "changement d'adresse primaire" est un défi dans le développement de mSCTP.

Une fois l'adresse primaire changée, le serveur CH envoie les données à la nouvelle adresse IP primaire du mobile (adresse IP 3). Toute donnée perdue peut être retransmise à l'adresse IP de secours (ancienne) du mobile (adresse IP 2).

4. Suppression de la vieille adresse IP de l'association SCTP

Alors que le MT continue d'avancer vers le routeur AR B, si la vieille adresse IP (adresse IP 2) devient inactive, le MT la supprime de la liste d'adresses. La règle pour déterminer si l'adresse IP est inactive peut être déterminée en utilisant des informations supplémentaires provenant du réseau sous-jacent ou de la couche Physique.

Les étapes de la procédure décrites ci-dessus pour le transfert intercellulaire transparent sont répétées chaque fois que le mobile se déplace sur une nouvelle localisation, jusqu'à ce que l'association SCTP soit libérée.

Après le bon établissement de l'association mSCTP sera utilisé pour fournir un transfert intercellulaire transparent aux terminaux mobiles. Une fois l'association établie, le transport des données entre le MT et le CH repose seulement sur mSCTP et n'utilise pas MIP.

II.4 Bilan du chapitre

La mobilité a pris une large part dans notre quotidien. En effet avec l'avancement des équipements mobiles, les applications ont la nécessité de rester connecté même si l'utilisateur est en déplacement et change de réseau initial.

La conception de Mobile IPv6 s'est basée sur les expériences acquises du développement de Mobile IPv4 et sur les nouvelles opportunités offertes par le protocoleIpv6, telles que le nombre plus important d'adresses et les mécanismes d'auto configuration.

L'utilisation des options destination d'IPv6, qui fournissent des informations au nœud destinataire final, permet aux informations de contrôle de Mobile IPv6 d'être transportées dans l'entête des paquets IP contrairement à Mobile IPv4 où un paquet UDP spécifique doit être utilisé pour chaque type de message de contrôle. L'optimisation de routage est intégrée dans le protocole Mobile IPv6 puisqu'elle est assurée, comme l'enregistrement avec l'agent parent, par des messages de mise à jour d'associations.

Bien que le protocole IPv6 Mobile permette de résoudre le problème de routage de paquets triangulaire utilisé dans le protocole IPv4 Mobile, il souffre encore de plusieurs faiblesses. Parmi ces faiblesses, nous citons [30]:Le délai du Handover qui est long. Particulièrement, le délai de la phase de détection de mouvement, celui de la phase d'auto-configuration d'adresses et celui de la phase de mise à jour d'association sont très long pour les applications en temps réel; La perte de paquets pendant le Handover peut être importante [26]. (HMIP, hierarchical MIP), (FMIP, Fast Handover for MIP) et F-HMIP sont des améliorations de MIP dans le but de réduire les pertes de paquets. Toutefois, aucune de ces nouvelles solutions ne permet d'avoir un faible trafic de signalisation, un délai de relève minimal et une perte de paquets tolérable.

SIP (Session Initiation Protocol) est un protocole de signalisation de niveau application défini par l'IETF. Il permet l'établissement, la libération et la modification des sessions multimédias. Il s'appuie sur un modèle client/serveur et propose l'adressage URL SIP (Uniform Resource Locator) qui ressemble à une adresse E-mail. Donc un utilisateur du protocole SIP est joignable grâce à son URL SIP. SIP est un protocole candidat intéressant pour la gestion de la localisation dans la gestion de la mobilité.

Le protocole SIP de base ne fournit pas la gestion transparente du transfert intercellulaire. Toutefois, lors d'un mouvement, le protocole SIP ne peut pas garantir le maintien d'une session TCP. Cependant, le protocole SIP peut être utilisé en conjonction avec

d'autres protocoles gestion du transfert intercellulaire tels que: IP mobile (MIP); IP cellulaire (CIP) ou mSCTP (mobile Stream control transmission protocol).

Le protocole de transport des commandes de flux (SCTP), est un protocole de bout en bout, orienté connexion (ou plus précisément nommé association), qui transporte des flux de données multiples. Le Multihoming et multi-streaming qui manquaient au TCP permet aux points de terminaison SCTP de prendre en charge plusieurs adresses IP. Le Multihoming protège une association des défaillances de réseau potentielles en dirigeant le trafic sur les adresses IP de remplacement. Si l'adresse primaire perd des paquets de données de façon répétée, tous les paquets de données suivants seront transmis à une adresse de remplacement jusqu'à ce que l'adresse primaire puisse être rétablie.

On note que le caractère Multihoming de SCTP permet de prendre en charge la mobilité sur IP. Plus précisément, le protocole SCTP avec une extension de configuration dynamique d'adresses peut servir à fournir un transfert intercellulaire en douceur aux terminaux (MT) qui passent dans différentes régions de réseaux IP au cours d'une session d'activité. Ceci est appelé SCTP mobile (mSCTP) et s'applique aussi bien à IPv4 qu'à IPv6.

Il est important de remarquer que tous ces protocoles cités ci-dessus ne se remplacent pas, mais se complètent.

*Chapitre **III***

Modélisation de la solution de mobilité

III.1 Introduction

Les travaux d'Andrei Andreevich Markov (1856-1922) sur la théorie des probabilités l'ont amené à mettre au point les chaines de Markov qui l'ont rendu célèbre. Ceux-ci peuvent représenter les prémisses de la théorie du calcul stochastique.

Au cours des années, plusieurs techniques de spécification et de modélisation de différents types de systèmes ont vu le jour. Certaines de ces techniques traitent des systèmes réels pour lesquels il n'est pas toujours évident de déterminer avec certitude le prochain état après l'exécution d'une action donnée [48].

Un modèle d'évolution dynamique en temps discret dans lequel on fait dépendre l'évolution future de l'état présent et du hasard est une chaîne de Markov. C'est un processus stochastique à temps discret. On en rencontre dans de multiples aspects des sciences de l'ingénieur. Citons notamment les télécommunications, la reconnaissance de formes ou l'administration des réseaux, etc.

On distingue plusieurs types de systèmes probabilistes selon que leur espace d'états est discret ou continu et selon qu'ils fonctionnent en temps discret ou continu. Quelque soit le type auquel il appartient, un système probabiliste à des états, donnant ainsi l'information du système à tout moment. De plus, il effectue des transitions, c'est-à-dire des changements d'états, chacune d'elles associée ou non à une action et une valeur de probabilité.

Dans le cadre de notre travail, nous proposons un modèle inspiré de la chaine markovien en temps continu pour répondre aux besoins de la mobilité des utilisateurs dans les technologies des réseaux cellulaires. Nous considérons un réseau cellulaire composé de **n** cellules et supposons que celles-ci sont toutes homogènes et statistiquement identiques.

III.2 Chaînes de Markov discrètes

Définition 1

Un processus stochastique est une suite de variables aléatoires indicées par le temps. Le cas le plus simple est celui d'une suite de variables aléatoires indépendantes. Ce sont des variables aléatoires qui n'ont aucune influence les unes sur les autres. De point de vue de la modélisation, ces suites de variables aléatoires indépendantes ne sont pas satisfaisantes, car elles ne prennent pas en compte la dynamique des systèmes en évolution, du fait de l'indépendance. Pour introduire cette dynamique, il faut tenir compte de l'influence du passé, ce que font les chaînes de Markov qui sont des processus aléatoires sans mémoire : à chaque instant leur évolution future ne dépend que de leur position, et non de leur trajectoire passée.

Dans ce document, nous considérons uniquement le cas des processus aléatoires à temps discret et à espace d'états E discret.

III.3 Généralités sur les chaines de Markov

On va se limiter ici à une étude élémentaire des chaînes de Markov : c'est un processus où le temps est discret et est assimilé à ℕ, et où l'ensemble des états est fini. On prend donc **E** = {0,....., N} et **X** est à valeurs dans cet ensemble. Les éléments de **E** sont appelés "états" du système. On fait également une hypothèse d'homogénéité temporelle : la probabilité, si on est dans un état i à un temps t, d'être à l'état j au temps t+1, que l'on notera P_{ij}, ne dépend pas de t. Dans la suite on se limitera donc à une chaîne de Markov à homogénéité temporelle. Une telle chaîne est donnée par:

1. le vecteur $V=\begin{pmatrix} X_1(0) \\ \vdots \\ X_N(0) \end{pmatrix}$ (1)

2. décrivant l'état initial : $x_i(X(0)=i))$ (probabilité que $X(0) =$ vaille i).

On a donc ∀i, $x_i(0) \in [0,1]$ et $x_1(0)$ + ...+ $x_N(0) = i = 1$.

3. La matrice P = $(p_{ij}) \in M_N(\mathbb{R})$ (2)

Est dite de transition, les p_{ij}étant définis comme précédemment (probabilité de transition de i à j).

On a donc : (H) : ∀ $ij, p_{ij}) \geq 0$, et ∀ i, $p_{i1}+ p_{i2}$ +.....+ $p_{iN}= 1$.

Les matrices vérifiant (H), c'est à dire étant des matrices de transition d'un processus de Markov, sont appelées matrices stochastiques. On vérifie qu'un produit de matrices stochastiques est encore stochastique.

En particulier ∀n∈ ℕ, p^nest stochastique, ce qui est logique, puisque P^n est la matrice de transition d'un temps t au temps t + n.

On peut également noter que l'ensemble des matrices stochastiques est un compact de $M_n(\mathbb{R})$.

Exemple: une chaîne à deux états

Considérons par exemple un poste téléphonique. Il peut posséder deux états : la ligne est libre (la fonction X à pour valeur 0) ou occupée (X a pour valeur 1). On a donc E = {0, 1}. Le temps est discrétisé. On suppose qu'à un temps t, il y a une probabilité P que la ligne soit occupée, et que, si la ligne est occupée, il y a une probabilité q pour que la ligne soit libre au temps suivant. p et q sont supposés constants. Ils sont dans [0, 1] (probabilités).La matrice de transition est alors:$\begin{pmatrix} 1-P & P \\ q & 1-q \end{pmatrix}$c'est la forme générale d'une chaîne de Markov à deux états.

III .3.1 Probabilité de transition et matrice de transition

La catégorie des processus stochastiques est très large car elle permet de modéliser l'ensemble des phénomènes aléatoires. Cependant, on ne peut pas obtenir mathématiquement beaucoup de résultats sur un processus stochastique trop général. Il faut alors ignorer des hypothèses supplémentaires à n entré dans des classes de processus stochastiques que l'on connait mieux.

On propose de se restreindre à la modélisation des phénomènes aléatoires par des chaines de Markov. Il est donc nécessaire de vérifier deux hypothèses mathématiques que sont la propriété de Markov et l'homogénéité.

Définition 2 (Chaîne de Markov)

Soit $\{X_t,\ t \geq 0\}$ une suite de variables aléatoires à valeurs dans l'ensemble des états E supposé égal à ℕ. On dit que cette suite est une chaîne de Markov si, pour tout $t \geq 0$ et toute suite $(i_0, i_1, \ldots\ldots, i_{t-1}, i, j)$, on a :

$$p(\underbrace{X_{t+1} = j}/\underbrace{X_t = i, X_{t+1} = i_{t+1}, X_{t+2} = i_{t+2}, \ldots\ldots, X_0 = i_0}) = p(\underbrace{X_{t+1} = j}/\underbrace{X_t = i})$$

Le future — Le passé et le présent — Le futur et le présent

Remarques 1

- L'état du processus à l'instant (t + 1) ne dépend que de celui à l'instant t précédent, mais non de ses états antérieurs.
- On dira qu'un tel processus est sans mémoire.

Définition 3 (Chaîne de Markov homogène)

Une chaîne de Markov est dite homogène (dans le temps), si la probabilité précédente (2:1) ne dépend pas de t. ie,

$$p_{ij}(t) = P(X_{t+1} = j/X_t = i) = p_{ij} = P(X_1 = j/X_0 = i), \qquad (t \geq 0).$$

Définition 4 (Probabilité de transition)

On définit la probabilité de transition de l'état i à l'état j entre les instants t et t + 1 par la quantité :

$$p_{ij}(t) = P(X_{t+1} = j/X_t = i) \qquad \forall i, j \in E$$

où, p_{ij}:P (pour que le système soit dans l'état j à l'instant t+1 sachant à l'instant t il se trouvait l'état i).

Définition 5 (Matrice de transition) pour card(E) = r

La matrce $\mathrm{p} = \begin{pmatrix} p_{1,1} & \cdots & \cdots & p_{1,r} \\ p_{2,1} & \cdots & \cdots & p_{2,r} \\ \cdots & \cdots & \cdots & \cdots \\ p_{r,1} & \cdots & \cdots & p_{r,r} \end{pmatrix}$, $\sum_{j \in E} p_{ij} = 1(matrice\ stochastique)$,

dont les coefficients sont des probabilités de transition p_{ij} est appelée matrice de transition (de passage) de la chaîne. C'est une matrice finie, suivant que l'ensemble des états est .ni ou dénombrable. Ici E fini de cardinal r.

Propriété de la matrice p

- p admet 1 comme valeur propre.
- Il existe un vecteur propre à gauche, associé à la valeur propre 1 qui défini une distribution de probabilité.

III .3.2 Probabilités de transition en m étapes

La probabilité conditionnelle d'aller de i à j en m étapes exactement est:

$$p_{ij}(m) = P(X_m = j/X_t = i) = P(X_{t+m} = j/X_t = i), \forall \mathrm{t} \geq 1$$

Cette probabilité est indépendant de m car le processus est homogène et est appelée la probabilité de transition en m étapes de i à j.

La matrice $P^{(m)}$ dont l'élément (i; j) est égal à $p^{(m)}_{ij}$ est appelée la matrice de transition en m étapes.

Théorème 1

Pour tout m ≥ 0 la probabilité $p_{ij}(m)$ de transition de i à j en m étapes est donnée par l'élément (i, j) de la matrice P^m Sous forme matricielle ce résultat s'écrit: $p^{(m)} = p^m$, pour tout m ≥ 0

Preuve

Par induction. Le résultat est vrai pour m = 0 et 1. Supposons le vrai pour m - 1. Utilisant la loi des probabilités totales, nous obtenons, pour tout i, j ∈S, quel que soit $k \geq 0$.

$$p_{ij}(m) = \mathrm{P}[\mathrm{X_m} = \mathrm{j}/\mathrm{X_0} = \mathrm{i}]$$

$$= \sum_{\mathrm{k}\in\mathrm{s}}^{\mathrm{ij}} \mathrm{P}[\mathrm{X_m} = \mathrm{j}/\mathrm{X_{m-1}} = \mathrm{K}]\ \mathrm{P}[\mathrm{X_{m-1}} = \mathrm{K}/\mathrm{X_0} = \mathrm{i}]$$

$$= \sum_{\mathrm{K}\in\mathrm{S}} \mathrm{P}_{\mathrm{Kj}}^{(1)}\ \mathrm{P}_{\mathrm{K}\in\mathrm{S}}^{(\mathrm{m}-1)} = \sum_{\mathrm{K}\in\mathrm{S}} \mathrm{P}_{\mathrm{iK}}^{(\mathrm{m}-1)}\ \mathrm{P}_{\mathrm{Ki}}$$

$$= \sum_{\mathrm{K}\in\mathrm{S}} (\mathrm{P}^{(\mathrm{m}-1)})_{\mathrm{kj}}(\mathrm{P})_{\mathrm{kj}} = p_{ij}(m)$$

III .4 Graphe sous forme de chaîne de Markov

La matrice de transition d'une chaîne de Markov finie peut être associée à un graphe dont les sommets sont les états P_{ij} sont les probabilités de transition d'état (i) vers (j). La figure 37 nous montre le principe.

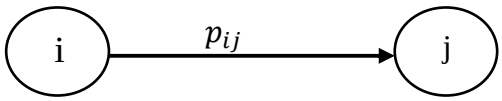


Figure 37 : Lien avec les graphes.

Définition 6

La matrice de transition d'une chaîne de Markov est représentée par un graphe orienté **G = (S, A),** défini comme suit :

1. **S** = {E_1, ..., E_r} = {1, ..., r} (les sommets sont les états de la chaîne);
2. (i, j) ∈A ssi $p_{ij} > 0$ et dans ce cas l'étiquette est p_{ij}. (ou arc qui relie les sommets associes aux états i et j si la probabilité de transition de i à j est positive, c'est-à-dire $p_{ij} > 0$).

III .5 Classification des états d'une chaîne de Markov

III .5.1 Relation de communication entre états

Définition 7 (Etat accessible)

Un état j est dit accessible à partir de l'état i; s.il existe un entier n ≥ 0 tel que $p_{ij}(n) \geq 0$ et l'on note i → j

Proposition 1

La relation d'accessibilité entre états est réflexive et transitive

a) Réflexivité :

$comme \;\; p_{ii}^{(0)} = p(X_0 = i/X_0 = \; i \;) = 1, pour\ tout\ état\ i, on\ a\ bien \;\; i \;\rightarrow\; i$

b) Transitivité :

Supposons que pour les états i,j et k on ait : i → j et j → k alors , il existe m et n , entiers positifs , tels que : $p_{ij}^{(m)} \geq 0$ et $p_{jk}^{(n)} \geq 0$. D'où, on aura

$$p_{ik}^{(m+n)} = \sum_{l \in E} p_{il}^{(m)} p_{lk}^{(n)} \geq p_{ij}^{(m)} p_{jk}^{(n)} > 0$$

Ce qui montre bien que l'on a : i → k une relation transitive.

Définition 8 (Etats communicants)

On dit que deux états i et j d'une chaine de Markov communiquent, si i → j et j→ i. On note i→j

Proposition 2

La relation de communication entre les états d'une chaine de Markov est une relation d'équivalence. On a donc

i. **(Réflexivité)** Tout état i de la chaine communique avec lui-même, ie. i → i.
ii. **(Symétrie)** Si un état i communique avec un état j, alors la réciproque est vraie, ie, i → j ⇔ j → i.
iii. **(Transitivité)** Si un état i communique avec j qui lui-même communique avec un état k, alors l'état i communique avec l'état k, i.e. si i → j et j → k alors i → k.

Remarques 2

1. Il est clair que tout état d.une chaîne de Markov communique avec lui même, puisque l'on a $p_{ii}^{(0)} = 1$. Un état est appelé état de retour, s.il existe n ≥1 tel que $p_{ii}^{(n)} \geq 0$. Il existe des états i tels que pour tout n ≥1 on ait $p_{ii}^{(n)} = 0$. De tels états sont appelés états de non retour.
2. L'ensemble des états E se partitionne en classes d'équivalence, disjointes et non vides, dites classes indécomposables. Si C_1 et C_2 sont deux classes distinctes, on peut éventuellement aller de C_1 à C_2, mais on ne peut alors retourner de C_2 à C_1.En revanche, tous les états d'une même classe communiquent. Certaines classes peuvent ne comporter qu'un seul élément ; ce sont les singletons. Comme exemples
   - Un état de non retour i : $p_{ii}^{(0)} = 1, p_{ii}^{(n)} = 0$ pour n ≥ 1;
   - Un état absorbant i : $p_{ii}^{(0)} = 1; p_{ii}^{(n)} = 1$ pour n ≥1.

Les définitions et propriétés citées ci-dessus nous ont permis de mettre sur pied un modèle inspiré de la chaine Markov en temps continu pour répondre aux besoins de la gestion de mobilité des utilisateurs qui ne désigne pas uniquement la capacité d'un nœud à se déplacer, mais englobe également d'autres questions qui lui sont liées: la gestion de la localisation (identifier la localisation du réseau en cours d'un terminal mobile (MT, mobile terminal) et de garder sa trace lorsqu'il se déplace); la gestion du transfert intercellulaire(Handover) qui sert à fournir aux mobiles la continuité de session et les possibilités de Multihoming, dans les technologies des réseaux cellulaires. Ce model est appelé graphe des états (nœuds) comme le présente la figure 38.

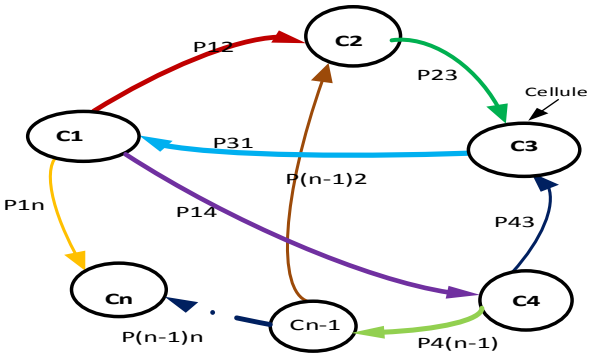


Figure 38:Graphe associe à une matrice de transition entre n états

III .6 Modèle markovien

III .6.1 Le profil de mobilité

Cette section décrit notre proposition concernant le profil de mobilité de l'utilisateur, ce profil est basé sur l'analyse du comportement de l'utilisateur afin de déterminer ses futures localisations. L'espace de mobilité de l'utilisateur est constitué de **N** cellules.

Le profil de mobilité de l'utilisateur est construit en se basant sur ses mouvements suite à **m** associations avec le système constitué de **N** cellules.

Pour modéliser les mouvements de l'utilisateur entre les **N** cellules, nous avons opté pour les chaines de Markov en temps continu. La raison de ce choix est basée sur le faite que les chaines de Markov sont des systèmes sans mémoire, le passage d'un état E_i à un autre état E_j ou transition, ne dépend donc que de ces deux états et s'effectue selon la probabilité conditionnelle : Prob $(E_i/E_j)=P_{ij}$ (probabilité de se trouver dans l'état E_j enfin de transition sachant qu'au début de la transition on était dans l'état initial $E_{i)}$. Lors d'un Handover, le passage d'une cellule à une autre ne dépend que de ces deux cellules, les chaine de Markov en Temps Continu(CMTC) son bien adaptés à ce type de traitement.

Notre système est un modèle pouvant évoluer entre **N** états définis par l'ensemble:

$\mathbf{C}= \{C_1, C_2,\ldots..C_i,\ldots\ldots, Cn\} = \{1, 2, \ldots, i, \ldots, n\}(6)$

qui représente l'ensemble des **N** cellules. Le système est à l'état i si le terminal mobile se trouve dans la cellule C_i.

Notre but est de construire un modèle de comportement de l'utilisateur afin de déterminer son profil de mobilité, ce dernier contiendra les informations suivantes:

- la matrice **M**;
- le vecteur **V**;
- le protocole **mSCTP** (**m**obile-**S**tream **C**ontrol **T**ransmission **P**rotocol).

III .7 Description formelle du modèle

La matrice

M est la matrice de transition qui contient les $\boldsymbol{p_{ij}}$

La matrice $\mathbf{M_{t+1}= [p_{ij}]_{t+1}}$ est une matrice de transition (matrice carrée d'ordre m qui modélise les transitions de la dynamique du système de l'instant t à l'instant t+1).

Après les **m** association avec le système, la probabilité de transition de la cellule i vers la cellule j est calculée de la façon suivante:

$\boldsymbol{p_{ij}}$**=t [i, j] /g(i)** (7)

t [i, j] est le nombre de transitions de la cellule i à la cellule j pendant les **m** associations avec le système.

g(i) est le nombre de transitions qui ont comme point de départ la cellule i pendant les **m** associations avec le système, il est calculé de la manière suivante : $g(i) = \sum_{j=1}^{n} t(i,j)$.

On note également par **I(d)** le nombre de transition dans le système pour les $\mathbf{d^{eme}}$ associations ($1 \leq \mathbf{d} \leq m$).Chaque transition est considérée entre t et t+1.

Le vecteur V

V est le vecteur qui contient les $P_i(t)$ (la probabilité que le terminal mobile se trouve dans la cellule C_i à l'instant t).

$\mathbf{V= [p_t(i)= [N]}$ (8)

Si à l'instant t, l'utilisateur s'associe ou se connecte **k** fois dans la cellule i durant les m associations alors $\boldsymbol{p_t(i)}$**=k/m**. Plus m est grand, plus l'efficacité pour le calcul $P_t(i)$ sera bonne. $\sum_{t=1}^{n} k(i) = m$. La figure 35, nous présente la détermination de la matrice M et du vecteur V.

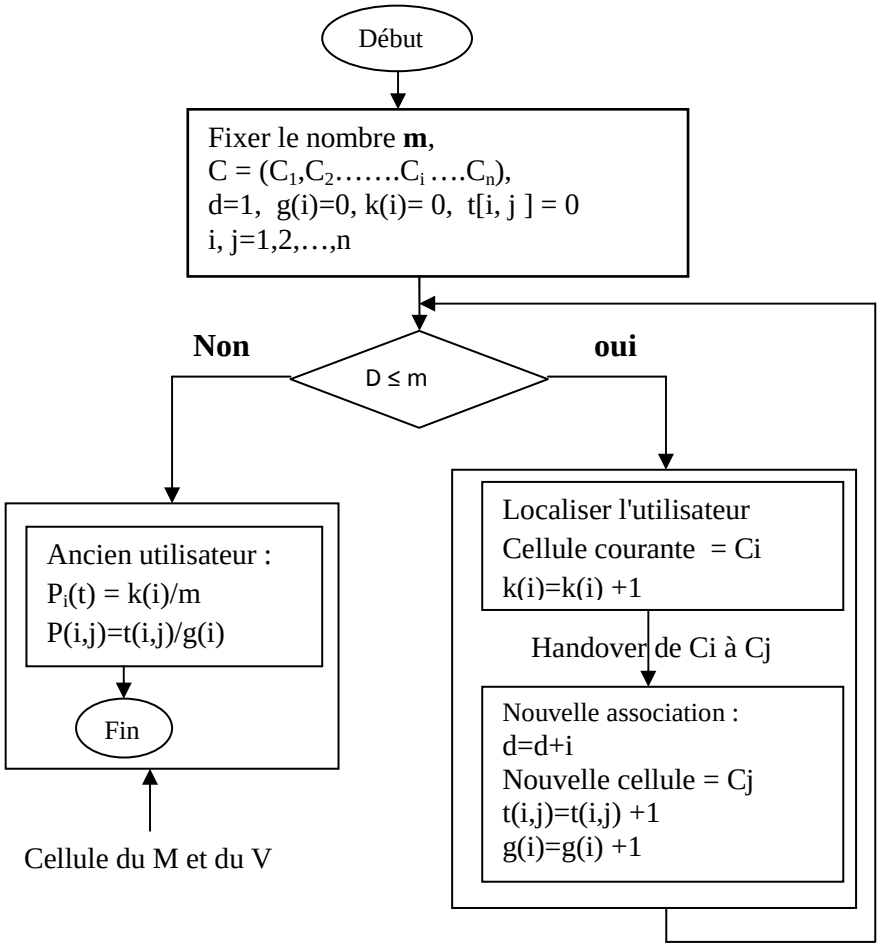


Figure 35: détermination de la matrice M et V

La modélisation du protocole mSCTP

$\boldsymbol{p_{ij}}$, est appelé probabilité de transition de la cellule C_i vers la cellule C_j

$\boldsymbol{p_t(i)}$**,** la probabilité pour que le terminale mobile se trouve dans la cellule C_i à l'instant t, il est question dans ce cas de repérer à chaque moment le mobile ou il se trouve dans n'importe quel sous réseau. En effet c'est un point important dans le cadre de fonctionnalités de base de la gestion de la mobilité,avec $\sum_{i=1}^{m} P_t(i) = 1$

$\boldsymbol{p_{t+1(j)}}$, la probabilité pour que le terminal mobile se trouve dans la cellule C_j à l'instant t+1.

Nous pouvons calculer cette probabilité à l'aide de la formule suivante:

$$P_{t+1}(j) = \sum_{i-1}^{n} P_t(i) * P_{ij} \quad (9)$$

Considérons un paramètre **δ**, avec**δ** ∈ [0,1], le seuil fixe ou variable, pour sélectionner les cellules de grandes probabilités retenu par le protocole **mSCTP**. Alors :

$$\textbf{mSCTP} = \{Cj \ / \ P_{t+1}(j) \geq \ \}. \quad (10)$$

La figure 36 donne la représentation de la détermination du mSCTP.

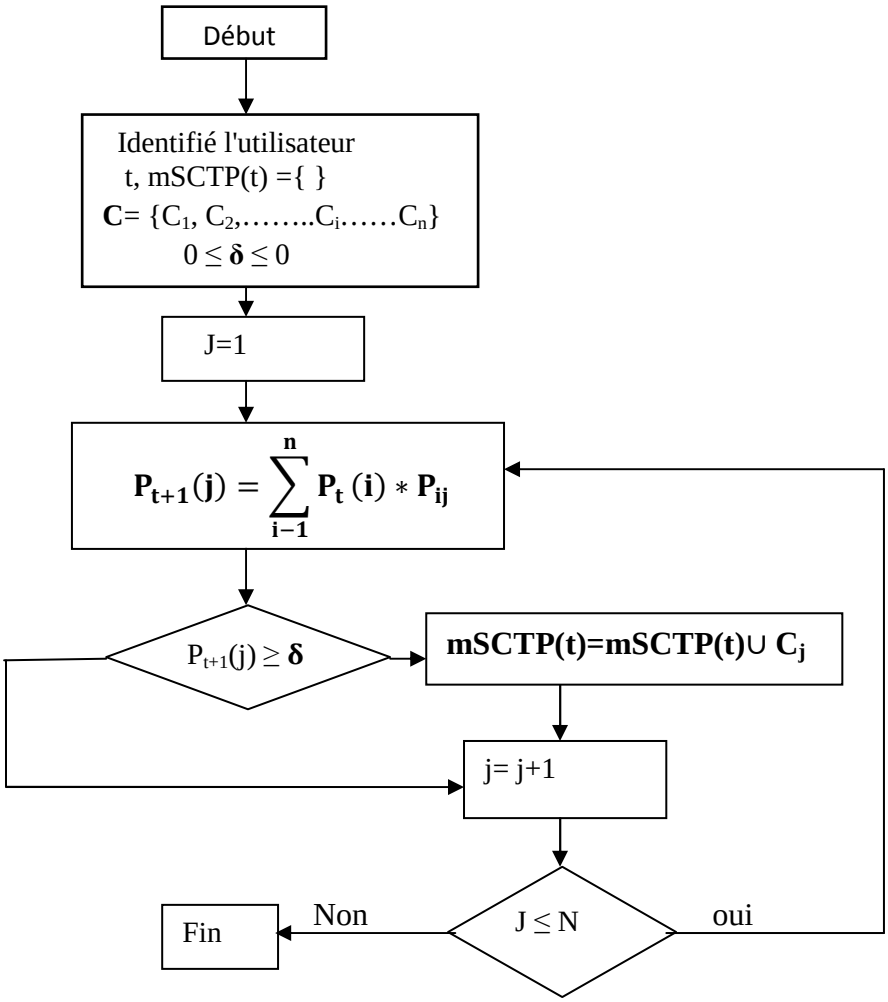


Figure 36: détermination du mSCTP

III .8 Implémentation sous MATLAB de mSCTP du Résultat de Simulation

III.8.1 Introduction à MATLAB

Pour valider notre approche, nous avons utilisé un outil de simulation, il s'agit de MATLAB. Le choix de MATLAB est basé sur le fait que nous avons modélisé mSCTP par la chaine de Markov en temps continu(MCTC).Cette modélisation nécessite des calculs matriciels qui sont plus simples à réaliser à l'aide de Matlab.

Matlab (MATrix LABoratory) est un langage de programmation de haut niveau pour le calcul numérique. Il est particulièrement performant pour le calcul matriciel, car sa structure de données est basée sur les matrices, et il dispose de possibilités d'affichage très riches. Il s'agit d'un langage à interpréter, ce qui permet un développement très rapide mais qui a l'inconvénient de ne pas avoir un temps d'exécution aussi rapide qu'un langage comme C. La figure 39 nous présente une interface de MATLAB.

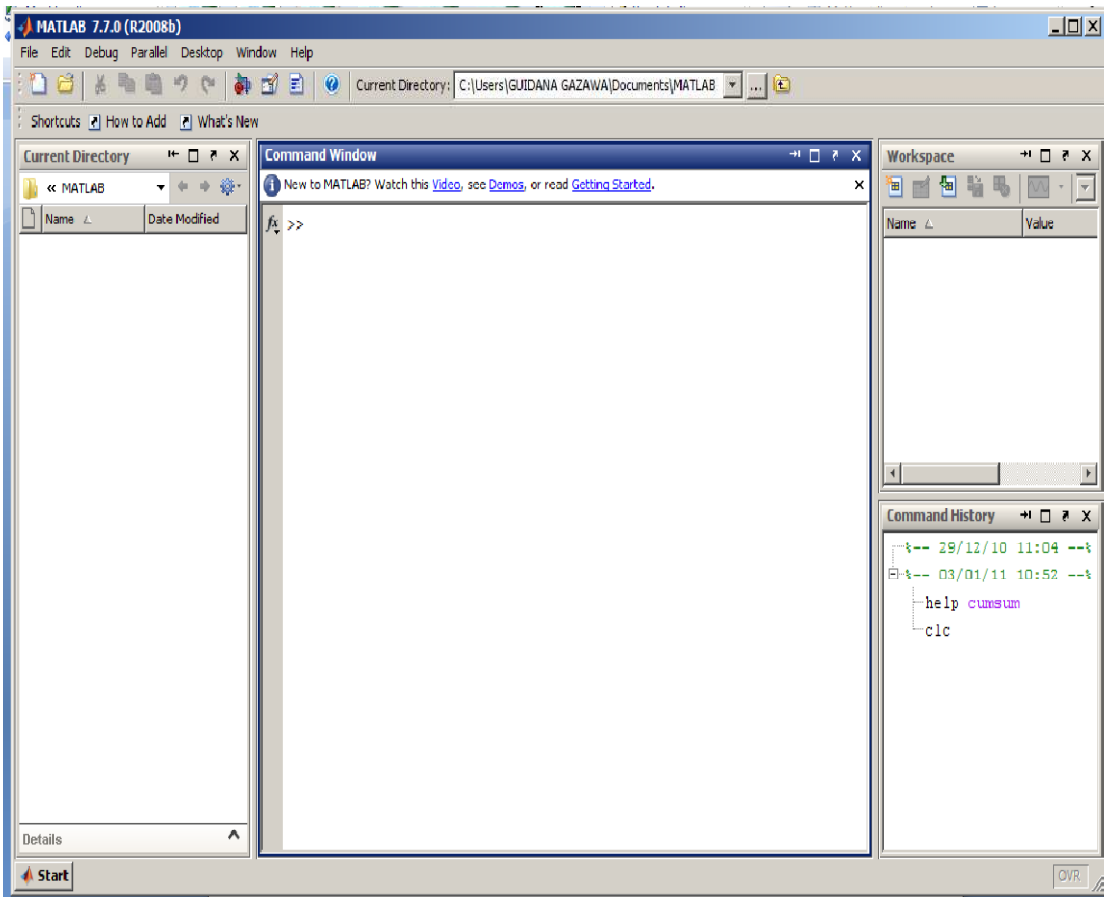


Figure 39: présentation d'une interface de MATLAB

L'interface graphique de MATLAB est sans conteste l'un des points forts du logiciel et facilite le tracé de courbes et l'obtention de graphiques 2D ou 3D de grande qualité (plot, stairs, stem, hist, mesh, surf, plot3).

Le langage MATLAB contient un minimum de structures de programmation (structure itérative, structure conditionnelle, sous-routine) mais reste très rudimentaire. L'avantage est qu'il est très simple et très rapide à programmer, offrant une grande tolérance (syntaxe simple, pas de définition de types, etc.), ce qui permet un gain appréciable en temps de mise au point.

Au logiciel de base s'ajoutent, selon la configuration choisie, les fonctions provenant d'une série de boîtes à outils (toolbox) dédiés à des domaines techniques spécifiques, comme le traitement de signal (signal processing toolbox) ; la régulation automatique (control system toolbox) ; l'identification (system identification toolbox) ; les réseaux de neurones (neural networks toolbox) ; la logique floue (fuzzy logic toolbox) ; le calcul symbolique (symbolic math toolbox) ; et bien d'autres encore.

Ces boîtes à outils sont simplement constituées d'un ensemble de fonctions spécialisées programmées à partir des fonctions de base de MATLAB.

Simulink n'est rien d'autre qu'une boîte à outils de MATLAB permettant au moyen d'une interface graphique évoluée la construction rapide et aisée ainsi que la simulation de schémas fonctionnels complexes, contenant des systèmes linéaires, non linéaires voire non-stationnaires, y compris des opérateurs logiques, des outils mathématiques d'analyse, etc.

III.8.2 Résultat Simulation sous MATLAB

La programmation sous MATLAB nous permet de calculer $P_{t+1}(j) = \sum_{i-1}^{n} P_t(i) * P_{ij}$ qui est la probabilité pour que le terminal mobile se trouve dans la cellule Cj à l'instant t+1.

Nous représentons le graphe de la figure 38composée de 4 cellules (n= 4) et 5 associations (m = 5). Et nous considérons un utilisateur se déplaçant dans le système représentant la figure 40, partant de la cellule C1 à l'instant t à la cellule C3 à l'instant t+1.

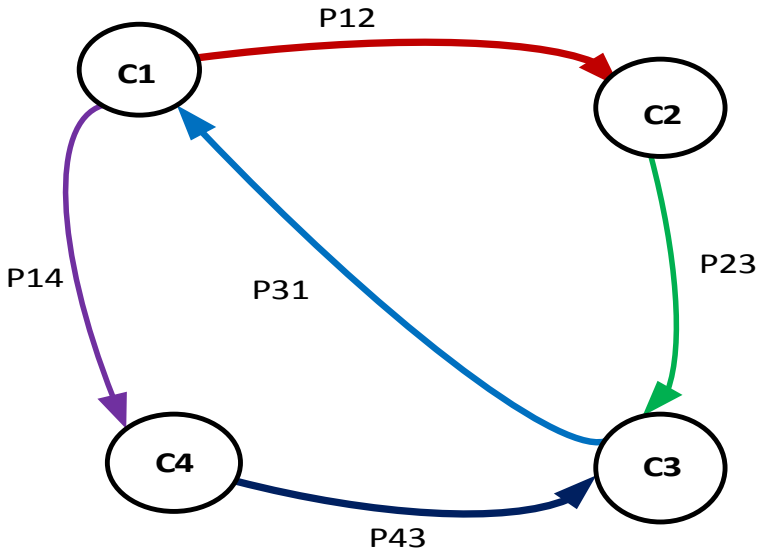


Figure 40: Représentation d'un graphe de 4 cellules et 5 associations

Nous savons que $p_{ij} = t[i,j]/g(i)$ avec $g(i) = \sum_{j=1}^{n} t(i,j)$

$$g(i) = \sum_{j=1}^{4} t(i,j) = t(1,1) + t(1,2) + t(1,3) + t(1,4)$$

Calculons $p_{ij} = t[i,j]/g(i)$ et $p_{t+1(j)} = \sum_{i=1}^{n} P_t(i) * p_{ij}$

On sait que $P_t(i) = K(i)/5$ avec $\sum_{i=1}^{4} K(i) = 5$

K(1) = 1 ; K(2) = 1 ; K(3) = 2 ; K(4) = 1

Donc Pt (1) =1/5 ; Pt(2) = 1/5 ; Pt (3) = 2/5 ; Pt(4) =1/5

on sait également que $P_{t+1}(j) = \sum_{i=1}^{n} P_t(i) * P_{ij}$

alors la matrice représentant le graphe de la figure 38 composée de 4 cellules serait égale à:

$$\begin{bmatrix} P_{t+1}(1) \\ P_{t+2}(2) \\ P_{t+3}(3) \\ P_{t+4}(4) \end{bmatrix} = P_t(1), P_t(2), P_t(3), P_t(4) * M$$

$$\begin{bmatrix} P_{t+1}(1) \\ P_{t+2}(2) \\ P_{t+3}(3) \\ P_{t+4}(4) \end{bmatrix} = P_t(1), P_t(2), P_t(3), P_t(4) * \begin{pmatrix} P_{1,1} & \cdots & \cdots & P_{1,4} \\ P_{2,1} & \cdots & \cdots & P_{2,4} \\ P_{3,1} & \cdots & \cdots & P_{3,4} \\ P_{4,1} & \cdots & \cdots & P_{4,4} \end{pmatrix}$$

Donc $P_{t+1}(1) = (P_t(1)P_{1,1} + P_t(2)P_{2,1} + P_t(3)P_{3,1} + P_t(4)P_{4,1})$

Cette expression nous donne bien $P_{t+1}(j) = \sum_{i=1}^{n} P_t(i) * P_{ij}$

Enfin, la simulation sous la plateforme Matlab est écrite par le programme ci-dessous.

```
function [Cellules] = cellules Markov(T, Theta, tpn)
 %Détermination des g(i)
g = sum(T');
 %Détermination des K(i)
K = sum(T);
 %Détermination des dimensions de T; n:lignes, m:colonnes
[n, m] = size(T);
 %Détermination du nombre d'association
nbAss = sum(K);
 %Détermination du vecteur de probabilité à l'instant 't' ("initiale")
Pt = K./nbAss;
 %Détermination de la matrice de trasition P
for i=1:n
   for j=1:m
      P (i,j) = T(i,j)/g(i);
   end
end
 %Calcul des probalités de chaque cellule
Cell=Pt*P;
for k=2:tpn
    Cell = Cell*P;
```

```
end
 %Détermination des cellules vérifiants le critère "Theta" (les colonnes avec pour valeur
"1")
for j=1:m
    if Cell(j)>= Theta
        Cellules(j)=1;
     else
       Cellules(j)=0;
   end
end
P.
```

Résultats de la simulation

T = [0 1 0 1;0 0 1 0;1 0 0 0;0 0 1 0]

T =

0	1	0	1
0	0	1	0
1	0	0	0
0	0	1	0

[C]=cellules Markov(T,1/3,1)

P =

0	0.5000	0	0.5000
0	0	1.0000	0
1.0000	0	0	0
0	0	1.0000	0

C = 1 0 1 0

= **{C1, C3}**

III.9 Conclusion

Ce chapitre nous a permis de décrire le profil de mobilité de l'utilisateur, ce profil est basé sur l'analyse du comportement de l'utilisateur afin de déterminer ses futures localisations. L'espace de mobilité de l'utilisateur est constitué de C_n cellules. Le profil de mobilité de l'utilisateur est construit en se basant sur son mouvement suite à **m** association avec le système constitué de C_n cellules.

la modelisation des mouvements de l'utilisateur entre les **N** cellules , nous a permit d'opté pour les chaines de Markov en temps continu.La raison de ce choix est basé sur le faite que les chaines de Markov sont des systemes sans mémoire,le passage d'un état Ei à un autre état Ej ou transition, ne dépend donc que de ces deux états et s'éffectue selon la probabilité conditionnelle.Prob(Ei/Ej)=Pij(probabilité de se trouver dans l'état Ej en fin de transition sachant qu'au début de la transition on était dans l'état initial Ei).Lors d'un handover, le passaged'une cellule à une autre ne dépend que des ces cellules. Nous pouvons calculer cette probalilité à l'aide de la formule:

$P_{t+1}(j) = \sum_{i=1}^{n} P_t(i) * P_{ij}$, est la probabilité pour que le terminal mobile se trouve dans la cellule Cj à l'instant t+1.

Considérons un paramètre **δ**, avec **δ** ∈ [0,1], le seuil fixe ou variable, pour sélectionner les cellules de grandes probabilités retenu par le protocole mSCTP.

La chaine de Markov identifie mSCTP comme un ensemble de cellules, selon la valeur de **δ.**

La simulation sous Matlab selon le graphe de la figure 38 composée de 4 cellules (n= 4) et 5 associations (m = 5) et en se fixant un seuil $\boldsymbol{\delta = \frac{1}{3}}$, alors mSCTP à l'instant t+1 est égale à : mSCTP(t+1) = { $C_i / P_{t+1}(j) \geq \delta$}**= {C1, C3}.**

Si le critère de choix dans l'ensemble mSCTP(t+1) est la cellule ayant la plus grande probabilité, alors pour notre exemple l'utilisateur pourra être basculé entre C1 ou C3 sans conséquence.

Chapitre IV

Proposition des fonctions d'agrégation pour montrer la qualité de service(QoS)

IV.1 Généralité sur la qualité de service(QoS)

La notion de qualité de service, ou QoS, concerne certaines caractéristiques d'une connexion réseau relevant de la seule responsabilité du fournisseur du service réseau. Une valeur de QoS s'applique à l'ensemble d'une connexion réseau. Elle doit être identique aux deux extrémités de la connexion, même si cette dernière est prise en charge par plusieurs sous-réseaux interconnectés offrant chacun des services différents [7]. La QoS est décrite à l'aide de paramètres. La définition d'un paramètre de QoS indique la façon de mesurer ou de déterminer sa valeur, en mentionnant au besoin les événements spécifiés par les primitives du service réseau.

Deux types de paramètres de QoS ont été définis :

1. Ceux dont les valeurs sont transmises entre utilisateurs homologues au moyen du service réseau pendant la phase d'établissement de la connexion réseau. Au cours de cette transmission, une négociation tripartite peut avoir lieu entre les utilisateurs et le fournisseur du service réseau afin de définir une valeur pour ces paramètres de QoS;

2. Ceux dont les valeurs ne sont ni transmises ni négociées entre les utilisateurs et le fournisseur du service réseau. Pour ces paramètres de QoS, il est toutefois possible d'obtenir, par des moyens locaux, l'information relative aux valeurs utiles au fournisseur et à chacun des utilisateurs du service réseau.

Les principaux paramètres de QoS sont les suivants :

- **Délai d'établissement de la connexion réseau:** Correspond au temps qui s'écoule entre une demande de connexion réseau et la confirmation de la connexion. Ce paramètre de QoS indique le temps maximal acceptable par l'utilisateur.

- **Probabilité d'échec de l'établissement de la connexion réseau:** Cette probabilité est établie à partir des demandes qui n'ont pas été satisfaites dans le temps normal imparti pour l'établissement de la connexion.

- **Débit du transfert des données:** Le débit définit le nombre d'octets transportés sur une connexion réseau dans un temps raisonnablement long (quelques minutes, quelques heures ou quelques jours). La difficulté à déterminer le débit d'une connexion réseau provient de l'asynchronisme du transport des paquets. Pour obtenir une valeur acceptable, il faut observer le réseau sur une suite de plusieurs paquets et considérer le nombre

d'octets de données transportés en tenant compte du temps écoulé depuis la demande ou l'indication de transfert des données.

- **Temps de transit lors du transfert des données:** Le temps de transit correspond au temps écoulé entre une demande de transfert de données et l'indication de transfert des données. Ce temps de transit est difficile à calculer du fait de la distribution géographique des extrémités. La satisfaction d'une qualité de service sur le temps de transit peut de surcroît entrer en contradiction avec un contrôle de flux.

- **Taux d'erreur résiduelle:** Se calcule à partir du nombre de paquets qui arrivent erronés, perdus ou en double sur le nombre total de paquets émis. C'est donc un taux d'erreur par paquet. Désigne également la probabilité qu'un paquet n'arrive pas correctement au récepteur.

- **Probabilité d'incident de transfert:** Est obtenue par le rapport du nombre d'incident répertorié sur le nombre total de transfert effectué. Pour avoir une estimation correcte de cette probabilité, il suffit d'examiner le nombre de déconnexion du réseau par rapport au nombre de transfert effectué.

- **Probabilité de rupture de la connexion réseau:** Se calcule à partir du nombre de libération et de réinitialisation d'une connexion réseau par rapport au nombre de transfert effectué.

- **Délai de libération de la connexion réseau:** C'est le délai maximal acceptable entre une demande de déconnexion et la libération effective.

- **Probabilité d'échec lors de la libération de la connexion réseau:** C'est le nombre d'échec de libération demandée par rapport au nombre total de libération demandé. Les trois paramètres additionnels suivants permettent de caractériser la qualité de service

- **Protection de la connexion réseau :** Détermine la probabilité que la connexion réseau soit en état de marche durant toute la période où elle est ouverte par l'utilisateur. Il y a plusieurs moyens de protéger une connexion en la dupliquant ou en ayant une connexion de sauvegarde prête à être ouverte en cas de coupure. La valeur pour un réseau téléphonique est de 99,999 %, que l'on appelle les cinq neuf, ce qui équivaut à quelques minutes d'indisponibilité par an. La protection est beaucoup plus faible pour un réseau IP, avec une valeur de l'ordre de 99,9 %, ou trois neuf. Cette valeur pose d'ailleurs problème

pour la téléphonie sur IP, qui demande une protection plus forte des connexions téléphoniques.

- **Priorité de la connexion réseau:** Détermine la priorité d'accès à une connexion réseau, la priorité de maintien d'une connexion réseau et la priorité des données sur la connexion.
- **Coût maximal acceptable:** Détermine si la connexion réseau est tolérable ou non. La définition du coût est assez complexe puisqu'elle dépend de l'utilisation des ressources nécessaires à la mise en place, au maintien et à la libération de la connexion réseau.

IV.2 Exigences de qualité de service pour les applications audio et vidéo

Les applications audio et vidéo font parties des applications les plus exigeantes en termes de QoS, surtout quand elles font intervenir une conversation entre plusieurs participants. Le tableau 6 présente les différentes recommandations de l'ITU-T [59] concernant les paramètres que doivent respecter ces applications pour fonctionner correctement.

On remarque effectivement que les applications de conversation audio et vidéo (vidéoconférence) sont plus exigeantes en termes de délai. Pour garantir un fonctionnement correct, le délai allé doit idéalement être inférieur à 150 ms. Cependant, elles peuvent fonctionner si ce dernier ne dépasse pas les 400 ms, seuil à partir duquel la dynamique de conversation commence à clairement se dégrader.

Par contre, la gigue doit rester très faible (inférieur à 1ms) et dans le cas où elle devient trop importante, un tampon de compensation de gigue doit être utilisé. De plus, l'oreille et l'œil humain peuvent tolérer des pertes d'informations, lorsqu'elles sont faibles mais l'utilisation de codecs de compression performants, utilisant des mécanismes de recouvrement d'erreur par exemple, permet bien souvent de les limiter.

Applications	**Degrés de symétrie**	**Débit**	**Délai aller**	**Gigue**	**Taux de perte de paquets**
Messagerie Vocal	Unidirectionnel	4-128 Kbit/s	Lecture: < 1s Enregistrement: <2s	<1ms	<1%
Conversation audio	Bidirectionnel	4-64 kbit/s	Idéal:< 150 ms Limite:< 400 ms	<1ms	<3%
Audio streaming	Unidirectionnel	16-128 kbit/s	< 10 s	<1ms	<1%
Vidéo conférence	Bidirectionnel	16-384 kbit/s	Idéal:< 150 ms Limite:< 400 ms	<1ms	<1%
Vidéo streaming	Unidirectionnel	16-384 kbit/s	< 10 s	<1ms	<1%

Tableau 6: Recommandations G1010 de l'ITU-T pour les applications sur Internet [58]

En ce qui concerne les applications de streaming, on constate qu'elles sont moins exigeantes en termes de délai ; cependant, elles nécessitent aussi un taux de perte de paquets faible, inférieur à 1 %, pour garantir un fonctionnement idéal.

Il est à noter que ces valeurs ne sont que des recommandations et qu'il est possible que la qualité de service ressentie par un utilisateur soit mauvaise bien que ces valeurs soient respectées et, inversement que l'utilisateur soit satisfait de la qualité de service alors que ces valeurs ne sont pas respectées.

IV.3 Exigences de la qualité de service pour les applications de données

Le tableau 7 présente les exigences de QoS recommandées par l'ITU-T concernant les applications de données.

On peut constater que ces applications sont généralement moins exigeantes que les applications vidéo et audio en termes de délai (excepté pour les jeux interactifs et Telnet), mais par contre, elles nécessitent pour la plupart un taux de perte nul. Dans le cas d'un

transfert de fichiers, par exemple, le délai recommandé pour qu'un utilisateur soit satisfait est très fortement lié à la taille du fichier lui-même.

Dans le cas d'un fichier de plusieurs mégaoctets, l'utilisateur sera plus tolérant que pour un fichier de quelques kilooctets. Par contre, contrairement au cas des conversations audio et vidéo, l'utilisateur souhaite que son fichier soit transmis sans aucune erreur.

Application	**Degré de symétrie**	**Quantités de données typiques**	**Délai aller**	**Taux de perte**
Navigation Web HTML	Unidirectionnel	~ 10 ko	Idéal :< 2s/page Acceptable :< 4 S/page	0 %
Transfert de données	Unidirectionnel	10 ko- 10 Mo	Idéal :< 15 s Acceptable:< 60 s	0 %
Transactions à haute Priorité (ex. e-commerce)	Bidirectionnel	< 10 ko	Idéal :< 2 s Acceptable :< 4 s	0 %
Images fixes	Unidirectionnel	< 100 ko	Idéal :< 15 s Acceptable :< 60 s	0 %
Jeux interactifs	Bidirectionnel	< 1 ko	< 200 ms	0 %
Telnet	Bidirectionnel (asymétrique)	< 1 ko	< 200 ms	0 %
E-mail	Unidirectionnel	< 10 ko	Idéal :< 2 s Acceptable :< 4s	0 %
Fax	Unidirectionnel	~ 10 ko	< 30 s/page	$<10^{-6}$ (BitErrorratio)
Application d'arrière plan (ex. : Usenet)	Unidirectionnel	~ 1 Mo	Plusieurs minutes	0 %

Tableau 7: Recommandations G1010 de l'ITU-T pour les applications de données [57].

IV.4 Le protocole SCTP et la Qualité de service(QoS)

Le protocole SCTP doit garantir la qualité de service(QoS) d'une association des stream (flux) lors d'une association. La procédure de transmission des différents types de données en utilisant les protocoles TCP/UDP s'effectue de la façon suivante: lorsqu'un nœud A transmet au nœud B des types distincts de données, trois approches sont possibles. La première alternative consiste à ouvrir autant de connexion que de types de données. Cependant cette approche nuit au contrôle de congestion puisqu'elle permet à une application d'augmenter sa bande passante au dépend des autres flux de données sur le réseau [59]. Dans la seconde approche, l'émetteur A transmet les différents types de données sur une unique connexion. Les applications utilisant cette approche doivent assurer un multiplexage/démultiplexage complexe et efficace lors des transmissions. La dernière alternative consiste à transmettre les données multimédia en utilisant l'UDP. Cependant, elle impose que l'application gère d'elle même la fiabilité des transmissions.

L'utilisation de SCTP offre une quatrième alternative pour effectuer ce type de transmission. Cette nouvelle possibilité combine les avantages des multiples connexions entre les deux extrémités communicantes et ceux du multiplexage/démultiplexage des différents types de données. En effet, l'utilisation de multiples streams de SCTP permet la distinction des différents types de données dans une même association et assure un contrôle de congestion au niveau de SCTP même, sans impliquer des contrôles complexes au niveau des applications. De plus, aucune application ne consomme un surplus de bande passante au dépend des autres applications. Ainsi, une extrémité SCTP peut requérir autant de streams que de types de données à transmettre. Chaque stream SCTP, étant un canal de communication logique unidirectionnel, il lui sera attribué un buffer indépendant en émission et un autre buffer en réception sur les deux bouts d'une association SCTP. Ces tampons de streams existeront durant la vie de leur association SCTP. La figure 41 montre un exemple d'une association SCTP entre les extrémités A et B. Le nœud A transmet trois types de données sur trois streams libellés de '0' à '2'. De l'autre bout, le nœud B ne transmet qu'un seul type de données. C'est pourquoi, il n'utilise qu'un seul stream libellé '0'.

On peut identifier deux types de transmission selon le nombre de streams déployés. Les associations à un seul flux sont similaires à celle de TCP vu que les applications déposent systématiquement leurs chunks sur ce flux. De ce fait, SCTP ne peut traiter ces chunks que selon leur ordre d'arrivée. Une telle gestion ne répond pas à la qualité de service requise au

niveau des routeurs qui reçoivent en parallèle différents types de données des nœuds intérieurs au réseau.

Lorsqu'une application fait appel à une association SCTP qui déploie plus d'un stream, elle doit préciser le numéro du stream 'NS' pour chaque chunk qu'elle génère. SCTP n'aura qu'à affecter à chaque chunk reçu un numéro de séquence 'SSN' sur son stream. Ce SSN est pris en considération si l'application exige le respect de l'ordre de transmission pour le chunk en question. Autrement, le chunk est livrée à l'application de l'autre extrémité dès sa réception sur le stream SCTP.

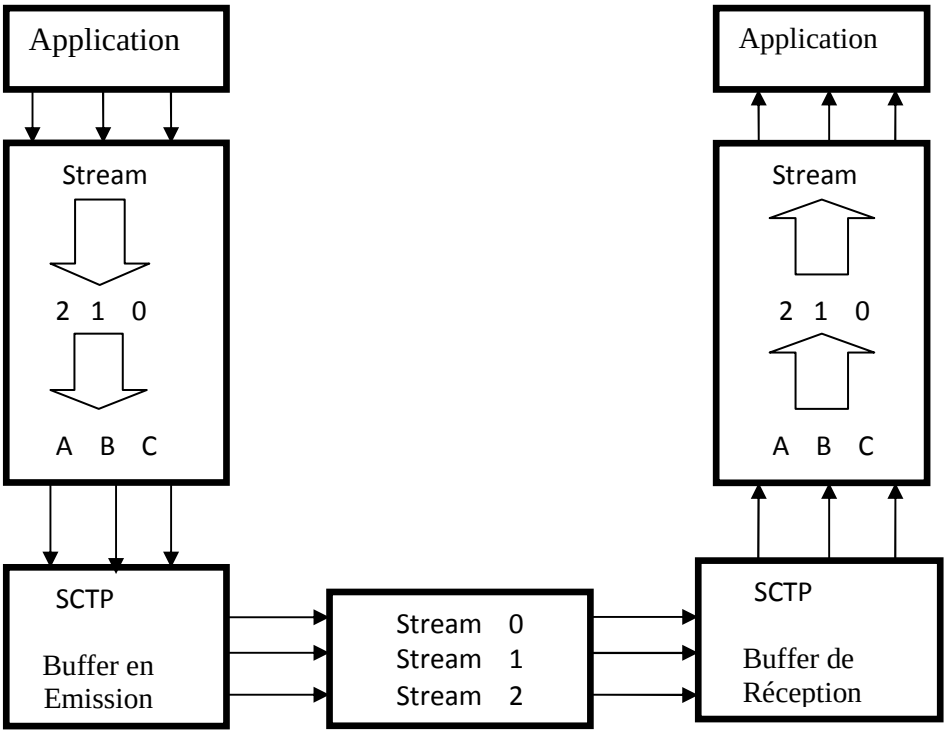


Figure 41: Correspondance entre types de données et numéros de Stream

Cependant, il est entièrement du ressort de SCTP d'attribuer obligatoirement un numéro TSN aux chunks reçus avant de les transmettre à l'autre extrémité. Dans le cadre de flux multiples, cette opération revient à sélectionner un chunk de l'un des stream et l'insérer en queue d'une séquence de chunk à transmettre. Le RFC 2960 [39] qui constitue une référence du fonctionnement de SCTP ne fournit aucune précision sur le procédé de sélection des chunks à transmettre à partir des streams. Néanmoins, le guide d'implémentation de SCTP [56] vient en complément qui détaille quelques fonctionnalités de SCTP dont l'ordonnancement des transmissions de chunks à partir des streams. [56] recommande deux algorithmes : le Round Robin-RR (Cyclique) et le First In First Serve-FIFS.

En utilisant l'algorithme du Round Robin(RR), avec trois streams, selon la figure 42, un nœud 'A' transmet un premier chunk du premier Stream '0'. Il transmet le second chunk à partir du Stream suivant, libellé '1'. Le troisième chunk sera transmis à partir du Stream '2'. Ensuite, le nœud reprend les transmissions à partir du Stream '0'. En utilisant FIFS, le nœud 'A' transmet les chunks de données dans leur ordre de réception de la couche application sans considérer leur Stream. Le déploiement de l'algorithme RR est recommandé vu qu'il assure un passage par tous les streams de l'association.

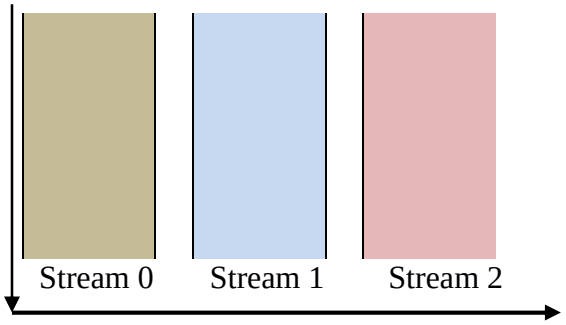


Figure 42 : Ordonnancement entre streams selon leur priorité

Les applications sur internet vont de celles basées sur les l'échange de données essentiellement textuelles, aux applications multimédias, impliquant la manipulation de plusieurs types de média texte, graphisme, audio, vidéo, etc.

Les transmissions se feront à partir des différents streams en favorisant les données les plus dépendantes du temps de transmission. Ainsi, les données audio seront transmises en priorité, les données vidéo viennent en seconde position, en troisième position la messagerie Vocal, et en quatrième position la conversation audio. L'algorithme RR accordera la plus haute priorité de transmission aux streams qui portent les données les plus contraignantes, comme indiqué sur la figure 40. C'est pourquoi, la disposition des données sur les streams devra correspondre à leur priorité de transmission.

La transmission à partir de chaque Stream se déroule périodiquement pour une durée égale à la valeur du seuil de transmission noté **β** du Stream. Lorsque cette durée est consommée, l'ordonnanceur arrête les transmissions à partir du Stream en cours et c'est le Stream suivant qui prend le droit de transmission même s'il reste des chunks sur le Stream actif. Ainsi le choix est porté sur les valeurs (8 s, 8 s, 0,7s, 140ms) pour les streams (0, 1, 2, 3).

IV.5 Fonctions d'agrégation pour la qualité de service

Les fonctions d'agrégation [64], sont généralement définies et utilisées pour combiner et résumer plusieurs valeurs numériques en une seule, de telle sorte que le résultat final de l'agrégation prenne en compte, d'une manière prescrite, toutes les valeurs individuelles. De telles fonctions sont largement utilisées dans de nombreuses disciplines bien connues comme la statistique, l'économie, la finance, l'informatique, etc.

Dans le cadre de contexte, les fonctions d'agrégation nous permettent d'apporter un jugement quantifiable sur plusieurs transitions intercellulaires pouvant monter la QoS. Pour atteindre un consensus sur ces jugements, des fonctions d'agrégation classiques ont été proposées : la moyenne arithmétique et quasi-arithmétique, la moyenne géométrique et quasi-géométrique, la médiane et bien d'autres encore. Le choix d'une fonction d'agrégation pourra satisfaire la plus grande partie des propriétés pour l'agrégation qui montre les différentes transmissions qui peuvent soit être unidirectionnelles (simplex), bidirectionnelles altérées (half-duplex), bidirectionnelles simultanées (full-duplex), etc.

Nous savons que p_{ij} = $P(X_{t+1} = j \mid X_t = i)$: probabilité de transition de l'état i vers l'état j pendant les instant t et t+1.

Nous proposons une fonction d'agrégation qui nous permettra d'apporter un jugement sur plusieurs transitions intercellulaires.

Soit $\mathbf{T_i} = \mathbf{F}\ (T_1, T_2, T_3, ..., T_n) \in [0,1]$ (11)

D'où $\mathbf{T_i}$ est le taux de transmission des $i^{ème}$ associations et qui représente la qualité de service(QoS) et **F** la fonction d'agrégation.

$$\text{Donc} \quad T_i = \frac{Q'_{i+1}}{Q_i} \in [0,1] \qquad (12)$$

avec $Q'_{i+1} \leq Q_i$ quantité d'information transmise entre C_i et C_{i+1}**.** A cet instant de transmission nous supposons que l'utilisateur ne reçoit aucune nouvelle information.

Si **U** est l'ensemble des informations reçues étant dans la nouvelle cellule C_{i+1}, alors

$$T_i = \frac{Q_{i+1}}{Q_i} \in [0,1] \quad \text{avec } Q_{i+1=}\ Q'_{i+1} + \mathbf{U} \quad \text{et} \quad Q_{i+1} \leq Q_i \qquad (13)$$

Q_{i+1} est la quantité d'information mise à la disposition de l'utilisateur à l'entrée de la deuxième zone de transmission.

IV.6 Propriétés pour l'agrégation

Comme nous venons de le dire sur les fonctions d'agrégation, pour choisir un mode d'agrégation raisonnable et satisfaisant, il est utile d'adopter une approche axiomatique et sélectionner ainsi les fonctions d'agrégation qui vérifient certaines propriétés. De telles propriétés peuvent être dictées par la nature des valeurs à agréger.

Ces différentes Propriétés des fonctions d'agrégation montre les différentes transmissions qui peuvent soit être unidirectionnelles (simplex), bidirectionnelles altérées (half-duplex), bidirectionnelles simultanées (full-duplex), etc.

IV.6.1 Hypothèses et notations diverses

Dans cette section, nous considérons que les quantités à agréger sont exprimées par des nombres réels dans l'intervalle [0,1], comme il est d'usage dans les ensembles flous. D'autre part, cette section traitant de manière générale les opérateurs d'agrégation hors contexte décisionnel, nous employons des termes neutres comme "quantité" et "source", dans le sens où les sources délivrent des quantités que l'on doit agréger.

Un opérateur d'agrégation Ψest considéré comme une fonction de $[0,1]^n$ dan [0,1] c'est-à-dire qui agrège n quantités. Pour certaines propriétés (changement d'échelle), il peut être nécessaire de considérer que Ψ est valué sur un intervalle autre que [0,1] voire$\mathbb{R}$ tout entier.

Si nécessaire, on noteΨ^npour indiquer le nombre de quantités à agréger, d'autre part, on notera N={1,2,.....,n} l'ensemble des sources. Enfin, les opérateurs minimum et maximum sont notés $\wedge$ et $\vee$ respectivement.

Nous proposons quelques propriétés fondamentales pour l'agrégation.

Définition 1

$\Psi: E^n \longrightarrow \mathbb{R}$ est symétrique si, pour tout$\pi \in \Pi_N$ on a

$\Psi(x_1,....., x_n) = \Psi(x_{\pi(1)},....., x_{\pi(n)})$ $(x \in En)$.

La propriété de symétrie signifie que l'ordre des X_i est sans importance pour l'agrégation. Ceci est requis notamment lorsque l'on combine des critères d'importances égales ou des opinions d'experts anonymes.

Définition 2

$\Psi: E^n \longrightarrow \mathbb{R}$ est continu au sens habituel.

L'avantage d'une fonction continue est qu'elle ne présente aucun saut brusque suite à de faibles variations des valeurs partielles.

Définition 3

$\Psi: E^n \longrightarrow \mathbb{R}$ est :

- non décroissant si, pour tous x, x'$\in E^n$, on a:

  $x \leq x' \Longrightarrow \Psi(x) \leq \Psi(x')$

- strictement croissant s'il est non décroissant et si, pour tous x, x' $\in E^n$, on a:

  $x \leq x'$ et $x \neq x' \Longrightarrow \Psi(x) < \Psi(x')$

- unanimement croissant s'il est non décroissant et si, pour tous x, x' $\in E^n$, on a:

  $x < x' \Longrightarrow \Psi(x) < \Psi(x')$

Une fonction non décroissante présente un comportement non négatif à tout accroissement des arguments. En d'autres termes, l'accroissement d'une valeur partielle ne fait pas décroitre le résultat. La fonction est strictement croissante si, en plus, elle réagit positivement à tout accroissement d'au moins une valeur partielle.

Enfin, la fonction est unanimement croissante si elle est non décroissante et présente une réaction positive chaque fois que tous les arguments croissent. Par exemple, nous observons que, sur $[0,1]^n$, la fonction maximum $\Psi(x) = \max(X_i)$ est unanimement croissante.

- Unanimité pour les valeurs extrêmes (UVE)

  $$\Psi(0,0,\dots\dots\dots,0) = 0 \quad \Psi(1,1,\dots\dots\dots,1) = 1$$

- Une propriété plus forte est l'idempotence (I) (ou unanimité, consensus) :

  $$\Psi(x,x,\dots\dots\dots,x) = x \quad \forall \in [0,1]$$

- continuité(C): Ψ est une fonction continue de $x_1, \dots\dots\dots, x_n$
- monotonie (M) (non décroissance) par rapport à chaque argument:

  $x'_i > x_i \Longrightarrow \Psi(x, x, x'_i,....,x) \geq \Psi(x, x, x_i,.....,x)$

La monotonie est stricte (SM) si on a l'inégalité stricte à droite.

- Neutralité (N) (ou commutativité, anonymat)

  $\Psi(x_1,....x_n,) = \Psi((x_{\sigma(1)},....., x_{\sigma(n)}), \forall\sigma\in\mathfrak{G}(N)$

ou $\mathfrak{G}$ (N) est l'ensemble de toutes les permutations sur N.

- Compromis(Co)

  $$\bigwedge_{i=1}^{n} x_i \leq \Psi(x_1, x_2, x_3 \dots\dots, x_n) \leq \bigvee_{i=1}^{n} x_i$$

Définition 4

$\Psi: E^n \longrightarrow \mathbb{R}$ est associatif si, pour tout $x \in E^3$, on a

$\Psi(\Psi(x_1, x_2), x_3) = \Psi(x_1, \Psi(x_2, x_3))$

Cette propriété s'étend aux suites des fonctions comme suit :

Définition 5

La suite $(\Psi^{(n)} : E^n \longrightarrow \mathbb{R})^n \geq 1$ est associative si $\Psi^{(1)}(x) = x$ pour tout $x \in E$ et

$\Psi^{(n)}(x_1,.....,x_k, x_{k+1},....., x_n) = \Psi^{(n)}(\Psi^{(k)}(x_1,.....,x_k), \Psi^{(n-k)}(x_{k+1},....., x_n))$

pour tout $x \in E^n$ et tous k, $n \in \mathbb{N}$ tels que $1 \leq k \leq n$.

Ce qui est implicite dans la définition d'une suite associative, c'est la manière de passer très facilement d'une agrégation de n valeurs à une agrégation de n + 1 valeurs. En effet, de la définition, on déduit la formule

$\Psi^{(n+1)}(x_1,....., x_{n+1}) = \Psi^{(2)}(\Psi^{(n)}(x_1,....., x_n), x_{n+1})$, pour tout $n \in \mathbb{N}_0$.

Passons à présent à la propriété de décomposabilité. Dans ce but, nous introduisons la notation suivante :

pour tout $k \in \mathbb{N}_0$ et tout $x \in \mathbb{R}$, nous posons k . x = x,.....,x (k fois).

Par exemple,

$$\Psi(3 .x, 2 . y) = \Psi(x, x, x, y, y).$$

Définition 6

La suite $(\Psi^{(n)} : E^n \longrightarrow \mathbb{R})_{n-1}$ est décomposable si $\Psi^{(1)}(x) = x$ pour tout $x \longrightarrow E$

$\Psi^{(n)}(x_1,.....,x_k, x_{k+1},....., x_n) = \Psi^{(n)}(k .\Psi^{(k)}(x_1,.....,x_k) , (n - k).\Psi^{(n-k)}(x_{k+1},.., x_n))$

pour tout $x \in E^n$ et tous k, $n \in \mathbb{N}$ tels que $1 \leq k \leq n$.

La définition ici est la même que celle de l'associativité, excepté que les agrégations partielles sont dupliquées un nombre de fois égal au nombre de valeurs agrégées.

Cette propriété de décomposabilité a été introduite sous le nom d'associativité des moyennes par Bemporad [62] dans une caractérisation de la moyenne arithmétique. Elle a aussi été utilisée dans [63,71] pour caractériser les moyennes quasi-arithmétiques. Plus récemment, [65] nous propose d'appeler cette propriété "décomposabilité" pour ne pas la confondre avec l'associativité classique. La propriété de bisymetrie, qui résulte simultanément de l'associativité et la symétrie, est définie pour les fonctions à n variables comme suit :

Définition 7

A: $E^n \longrightarrow \mathbb{R}$ est bisymetrique si

$$\Psi(\Psi(x_{11},....,x_{1n}),...., \Psi(x_{n1},....., x_{nn}))$$
$$= \Psi(\Psi(x_{11},.....,x_{n1}),...,\Psi(x_{1n},.....,x_{nn}))$$

pour toute matrice carrée $(x_{ij}) \in E^{n\,x\,n}$.

Pour des fonctions à deux variables, cette propriété a été étudiée d'un point de vue algébrique en l'utilisant principalement dans des structures privées de la propreté d'associativité. Pour une liste de références, voir [61, 66] Pour une suite de fonctions, cette propriété devient :

Définition 8

La suite $(\Psi^{(n)} : E^n \longrightarrow \mathbb{R})_{n\geq 1}$ est bisymetrique si $\Psi^{(1)}(x) = x$ pour tout $x \in E$ et

$$\Psi^{(p)}(\Psi^{(n)}(x_{11},..,x_{1n}),..,\Psi^{(n)}(x_{n1},.., x_{pn}))$$
$$= \Psi^{(n)}(\Psi^{(p)}(x_{11},.., x_{p1}),....,\Psi^{(p)}(x_{1n},.., x_{pn}))$$

pour tous $n, p \in \mathbb{N}_0$ et toute matrice $(x_{ij}) \in E^{p\,x\,n}$.

IV.7 Les principaux opérateurs d'agrégation

Nous nous limitons dans ce qui suit à faire une présentation des opérateurs les plus usuels, sans prétendre à l'exhaustivité. Nous découpons les opérateurs en trois grandes classes.

IV.7.1 Les opérateurs conjonctifs

Les opérateurs conjonctifs effectuent une agrégation des quantités comme le ferait un "et" logique (conjonction). Ainsi le résultat de l'agrégation est élevé (proche de 1) si et seulement si toutes les quantités à agréger sont élevées. Une propriété naturelle est alors d'imposer :

i. $\Psi^2(1, x) = x \quad \forall x \in [0,1]$ (14)

Si on rajoute à (18) les propriétés de non-décroissance, neutralité et associativité, on obtient la famille des normes triangulaires ou t-normes, souvent notées T.

Deux propriétés importantes sont :

- $1 - T(0, x) = 0 \quad \forall x \in [0,1]$
- l'opérateur minimum est une t-norme, et toute t-norme T vérifie $T(a, b) \leq a \wedge b$, ce qui signifie que $\wedge$est la plus grande t-norme.

Il faut noter que les t-normes ne vérifient pas les propriétés d'idempotence, compromis et stabilité pour le changement d'échelle linéaire.

IV.7.2 Les opérateurs disjonctifs

Les opérateurs disjonctifs quant à eux effectuent une agrégation de type “ou” logique (disjonction). Le résultat de l’agrégation est élevé dès que l’une des quantités à agréger est élevée. Ceci peut se traduire par la propriété suivante :

ii. $\Psi^2(0,x) = x \quad \forall x \in [0,1]$ (15)

Si nous rajoutons à (19) les propriétés de non-décroissance, neutralité et associativité nous obtenons la famille des Co-normes triangulaires ou t-conormes, souvent notées S. Les propriétés importantes sont :

- Si S(x, y) est une t-conormes, alors T(x, y)=1 - S(1-x, 1-y) est une t-norme, dite t-norme duale ;
- $S(1,x) = 1 \quad \forall \in [0,1]$;
- l'opérateur maximum est la plus petite t-conorme voir [62, 68]

IV.7.3 Les opérateurs de compromis

Les opérateurs de compromis se situent par définition entre les opérateurs disjonctifs et conjonctifs. Nous citons ici les principaux:

1. La somme pondéré et les opérateurs de moyenne

La somme pondérée ou moyenne arithmétique pondérée est définie par:

$\Psi(x_1, \dots\dots\dots\dots, x_n) = \sum_{i=1}^{n} w_i\, x_i \quad x \in E^n$

ou $W_i \in [0,1]$ sont des poids, tels que $\sum_{i=1}^{n} W_i = 1$

D'autres types de moyenne existent (géométrique, harmoniques, etc.) qui peuvent toutes s'écrire sous la forme :

$M_f(x_1, \dots\dots, x_n) = f^{-1}[\sum_{i=1}^{m} W_i f'(x_i)] \quad \forall \quad x \in E^n$ (16).

D’où f est une fonction continue strictement croissante (moyennes généralisées). Toutes les moyennes généralisées sont idempotentes, continues, strictement monotones. Seule la somme pondérée vérifie la stabilité au changement d’échelle linéaire.

2. Le minimum et maximum pondérés

Ils ont été introduits par Dubois [75]. Et on parle dans ce cadre de la théorie des possibilités. Soit w = (w_1, ...w_n) un vecteur de poids $w_i \in [0,1]$, tel que $\sum_{i=1}^{n} w_i = 1$

Ils sont définis par:

$$\mathrm{Wmin}_w(X_1, \dots\dots\dots, X_n) = \bigwedge_{i=1}^{n} [(1 - W_i) \vee X_i] \qquad (17)$$

$$\mathrm{Wmax}_w(X_1, \dots\dots\dots, X_n) = \bigvee_{i=1}^{n} [W_i \wedge X_i] \qquad (18)$$

Le minimum et maximum usuels sont obtenus par w = (1, 1, ..., 1). Ils vérifient les propriétés d'idempotence, de continuité et de monotonie.

Nous avons défini notre qualité de service par **Ti** = **F**(T_1 , T_2 , T_3,....., T_n) $\in [0,1]$, et nous constatons que **les opérateurs de compromis** prennent en chargent une grande partie des propriétés des fonction d'agrégation et pourront contribuer à la qualifié de service lors d'un transfert intercellulaire.

$$\text{Donc } \bigwedge_{i=1}^{n} T_i \leq F(T_1, T_2, T_3 \dots\dots, T_n) \bigvee_{i=1}^{n} T_i \qquad (19)$$

IV.7.4 Les fonctions de type moyenne

Il ne serait pas convenable de traiter les fonctions d'agrégation sans introduire des fonctions de type moyenne. le concept de moyenne a donné lieu aujourd'hui à un champs d'étude très vaste avec une variété impressionnante d'applications. En fait, une abondante littérature sur les propriétés de plusieurs moyennes (tels que la moyenne arithmétique, géométrique, etc.) a déjà été écrite, surtout depuis le 19^{e} siècle, et continue à se développer aujourd'hui.

En 1930, Kolmogoroff [63] considéraient que la moyenne devrait être plus que simplement une fonction interne ou un égaliseur numérique. Ils définirent alors une valeur moyenne comme une suite décomposable de fonctions:

$M^{(1)}(x_1) = x_1$, $M^{(2)}(x_1, x_2)$,....., $M^{(n)}(x_1, \dots\dots, x_n)$,.....

qui sont continues, symétriques, strictement croissantes, et idempotentes. Ils démontrèrent, indépendamment l'un de l'autre, que ces conditions sont nécessaires et suffisantes pour la

quasi-arithmétique de la moyenne, c'est à dire, pour l'existence d'une fonction f continue et strictement monotone telle que M(n) soit de la forme:

$$F(x) = f^{-1}\left[\frac{1}{m}\sum_{i=1}^{m} f(x_i)\right] \qquad x \in E^n \qquad (20)$$

Les moyennes **quasi-arithmétiques** comprennent la plupart des moyennes algébriques connues (voir tableau 8).

f(x)	**$M^{(n)}(x_1,.....x_n)$**	**Nom**
x	$\frac{1}{n}\sum_{i=1}^{n} x_i$	Arithmétique
x^2	$(\frac{1}{n}\sum_{i=1}^{n} x_i^2)^{\frac{1}{2}}$	Quadratique
Log x	$(\prod_{i=1}^{n} x_i)^{\frac{1}{n}}$	Géométrique
x^{-1}	$\frac{1}{\frac{1}{n}\sum_{i=1}^{n}\frac{1}{x_i}}$	Harmonique
x^{σ} $(\sigma \in \mathbb{R}_0)$	$(\frac{1}{n}\sum_{i=1}^{n} x_i^{\sigma})^{\frac{1}{\sigma}}$	Puissance
$x^{\sigma x}$ $(\sigma \in \mathbb{R}_0)$	$(\frac{1}{\sigma}\ln(\frac{1}{n}\sum_{i=1}^{n} e^{\sigma x_i})$	Exponentielle

Tableau 8: Exemples de moyennes quasi-arithmétiques

La propriété de décomposabilité des moyennes est assez naturelle. Lorsqu'elle est associée à l'idempotence, elle peut s'écrire comme suite:

$$M^{(k)}(x_{1,.....}x_k) = M^{(k)}(x'_{1,.....},x'_k)$$

$$\Downarrow$$

$$M^{(n)}(x_{1,.....}x_k, x_{k+1,.....}x_n) = M^{(n)}(x'_{1,.....},x'_k, x_{k+1,.....},x_n)$$

ce qui signifie que la moyenne ne change pas lorsqu'on modifie certaines valeurs sans modifier leur moyenne partielle.

IV.7.5 Moyennes quasi-arithmétiques

Comme nous venons de le mentionner, les moyennes quasi-arithmétiques ont été introduites à l'aide d'une axiomatique très naturelle. Dans cette sous-section, nous étudions ces moyennes en tant que fonctions à n variables, mais aussi en tant que séquences de fonctions. Des résultats sur cette classe de moyennes peuvent aussi être trouvés dans [70].Il a été démontré par [61,66] que les moyennes quasi-arithmétiques sont les seules fonctions M : $E^n \dashrightarrow E$ qui soient symétriques, continues, strictement croissantes, idempotentes et bisymetrique. L'énoncé de ce résultat peut être formule comme suit :

Théorème 1

M: $E^n \dashrightarrow E$ est une fonction symétrique, continue, strictement croissantes, idempotentes et bisymetrique si et seulement s'il existe une fonction f : $E^n \dashrightarrow \mathbb{R}$ continue et strictement monotone telle que:

$$M(x) = f^{-1}\left[\frac{1}{m}\sum_{i=1}^{m} f(x_i)\right] \quad \text{pour tout} \quad x \in E^n \qquad (21)$$

Les moyennes quasi-arithmétiques(26) sont des fonctions d'agrégation internes et couvrent un large spectre de moyennes, y compris les moyennes arithmétiques, quadratiques, géométriques, et harmoniques (Tableau 8).

La fonction f apparaissant dans (26) est appelée générateur de M. On peut montrer que f est déterminé à une transformation linéaire près : avec f(x), toute fonction

$g(x) = r\, f(x) + s \quad (r; s \in \mathbb{R} ; r \neq 0)$

définit le même M, et uniquement les fonctions de cette forme.

En plus de ce résultat d'Aczel dans [61,66], nous avons également celui de Kolmogoroff-Nagumo dans [63] que nous rappelons ici :

Théorème 2

La suite $(M^{(n)} : E^n \longrightarrow E)$ $n \geq 1$ est une suite décomposable de fonctions symétriques, continues, strictement croissantes et idempotentes si et seulement s'il existe une fonction

f: $E \longrightarrow \mathbb{R}$ continue et strictement monotone telle que:

$$M^{(n)}(x) = f^{-1}\left[\frac{1}{m}\sum_{i=1}^{m} f(x_i)\right] \quad \text{pour tout} \quad x \in E^n \qquad (22)$$

[66] a étudié certaines sous-familles de la classe des moyennes quasi-arithmétiques. Il a démontré le résultat dans [72].

Proposition 1

$E \longrightarrow \mathbb{R}_0^+$ ou un sous interval.

(i) M: $E_n \longrightarrow E$ est une moyenne quasi-arithmétique signifiante pour les mêmes échelles de ratios entrés-sorties si est seulement si Soit M est la moyenne géométrique

$$M(x) = (\prod_{i=1}^{n} x_i)^{\frac{1}{n}} (x \in E^n) \qquad (23)$$

d'ou M est la fonction puissance: il existe $\sigma \in \mathbb{R}_0$ tel que:

$$M(x) = (\frac{1}{n}\sum_{i=1}^{n} x_i^{\sigma})^{\frac{1}{\sigma}} \qquad x \in E^n \qquad (24)$$

(ii) M: $E_n \longrightarrow E$ est une moyenne quasi-arithmétique signifiante pour les même échelles d'intervalles entrées-sorties si et seulement si M es la moyenne arithmétique. Le tableau 9 nous présente une liste de **moyennes quasi-linéaires.**

F(x)	M(x)	Nom de la moyenne pondérée
x	$\sum_{i=1}^{n} w_i x_i$	Arithmétiques
X^2	$(\sum_{i=1}^{n} w_i x_i^2)^{\frac{1}{2}}$	Quadratique
logx	$\prod_{i=1}^{n} x_i^{w_i}$	Géométrique
x^σ $\sigma \in \mathbb{R}_0$	$(\sum_{i=1}^{n} w_i x_i^{\sigma})^{\frac{1}{\sigma}}$	Puissance

Tableau 9: Exemples de moyennes quasi-linéaires

Théorème 3

M : $E_n \longrightarrow E$ est une fonction continue, strictement croissante, idempotente,et bisymetrique si et seulement s'il existe une fonction f : $E \longrightarrow \mathbb{R}$ continue et strictement monotone et des nombres réels $w_{1,} \dots \dots, w_i > 0$ vérifiant les conditions:

$$\sum_{i=1}^{n} W_{i=1} \quad \text{tel que} \quad M(x) = f^{-1}\left[\sum_{i=1}^{m} W_i\, f(x_i)\right] \qquad x \in E^n \qquad (25)$$

M : En $\longrightarrow$ E est une fonction continue, strictement croissante, et bisymetrique si et seulement s'il existe une fonction f : $E \longrightarrow \mathbb{R}$ continue et strictement monotone et des nombres réels $p_1 \dots\dots, p_n > 0$ et $q \in \mathbb{R}$ tels que:

$$M(x) = f^{-1}\left[\frac{1}{m}\sum_{i=1}^{m} P_i\, f(x_i) + q\right] \qquad x \in E^n \qquad (26)$$

Les moyennes quasi-linéaires (25) et les fonctions quasi-linéaires (26) sont des fonctions d'agrégation pondérées.

Deux moyennes font leur entrée dans la contribution des fonctions d'agrégation:

la moyenne arithmétique définie par:

$$F(x) = f^{-1}\left[\frac{1}{m}\sum_{i=1}^{m} f(x_i)\right] \qquad x \in E^n \qquad (27)$$

et la moyenne quasi-linéaire définie par:

$$F(x) = f^{-1}\left[\frac{1}{m}\sum_{i=1}^{m} W_i\, f(x_i)\right] \qquad x \in E^n \qquad (28)$$

Parmi ces deux fonctions, (28) se distingue grâce à son poids $\mathbf{W_i}$ (**puissance du signal),** qui également représente les poids du Handover et dépend de l'altitude entre deux antennes en interférence, et aussi les obstacles géographiques, tout en vérifiant la condition $\sum_{i=1}^{n} W_i = 1$.

IV.8 Résultats de Simulation pour montrer la qualité de service(QoS)

Les tableaux 10, 11, 12,13 nous proposent quatre cas des données lors d'une transmission intercellulaire représentant le graphe de la figure 38 à différents niveaux pour les fonctions d'agrégation f(x)= x et f(x) = log x

Trafic Audio

Pour le trafic vidéo nous avons utilisé **un taux de transfert** compris entre **4-64 kbit/s** avec un **délai aller** Idéal: **< 150 ms Limite: < 400 ms** pris dans: Recommandations G1010 de l'ITU-T pour les applications sur Internet et leurs paramètres [58].

Premier cas: **Handover avec un niveau**

Mesurons la qualité de service lorsque f est une fonction identité c'est à dire f(x)= x alors

$$T = F(x) = M(x) = f^{-1}\left[\sum_{i=1}^{m} W_i\, f(x_i)\right] = \sum_{i=1}^{m} W_i\, x_i$$

Posons: $Q_i = t_i * D_i$ (t_i est le temps aléatoire de transmission pour chaque cellule et D_i le débit).

$T_i = \frac{Q_{i+1}}{Q_i} \in [0,1]$ avec $Q_{i+1=}Q'_{i+1\,+}\mathbf{U}$ (**U**: nouvelles informations).

Nous prenons pour exemple la conversion audio avec 0,139s; 0,138s; 0,137s; 0,140s; 0,145s les temps aléatoires attribués à chaque état et un débit constant de 40kbit/s pour toutes les cellules Ci.

Nous entendons par niveau la variation de la vitesse par rapport au point d'accès (figure 43).

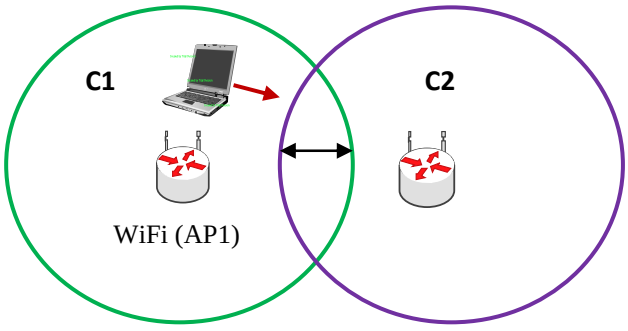


Figure 43: Handover avec un niveau

Nous présentons les résultats de simulation en fonction de f qui est une fonction identité c'est à dire f(x) = x, du poids $\mathbf{w_i}$ et de qualité de service **T**. Le tableau 10 nous donne les transmissions des données intercellulaires avec un niveau.

m	D_i' (constant)	t_i(en (seconde)	Q_i	Q'_{i+1}	U	$Q_{i+1=}$ Q'_{i+1} + U	T_i= Q_{i+1}/Q_i	W_i	.f(x)= x	T
1ere	40kbit/s	0,139	Q1= **6**	Q'2=t2*D1=**5,52**	0,14	Q_2=5,52+0,14	**0,940**	0,24	**0,940**	
2 eme	40kbit/s	0,138	Q2=**6,5**	Q'3=t3*D1=**5,48**	0,13	Q_3=5,48+0,13	**0,863**	0,26	**0,863**	
3 eme	40kbit/s	0,137	Q3=**7,03**	Q'1=t1*D1=**5,56**	0,10	Q_1=5,56+0,10	**0,805**	0,22	**0,805**	**0,82**
4 eme	40kbit/s	0,140	Q1=**7,5**	Q'4=t4*D1=**5,60**	0,16	Q_4=5,60+0,04	**0,768**	0,13	**0,768**	
5 eme	40kbit/s	0,145	Q4=**7,8**	Q'3=t3*D1=**5,8**			**0,743**	0,15	**0,743**	

Tableau 10: Transmissions des données intercellulaires avec un niveau

<u>Deuxieme cas:</u> Handover avec deux niveaux (figure 44)

Mesurons la qualité de service pour la même fonction f(x)= x alors

$$T = f(x) = \sum_{i=1}^{m} W_i x_i$$

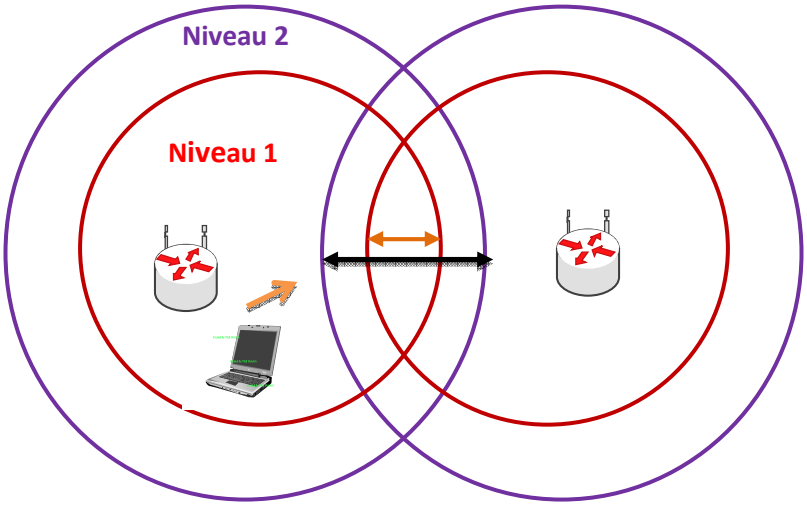


Figure 44**: Handover avec deux niveaux**

Nous constatons qu'au fur et à mesure que le mobile s'éloigne du point d'accès le débit diminue par rapport à chaque niveau(le tableau 11 nous montre le principe). Si Di est constant par niveau: Q'i+1=Dit' + Dit" avec t=t'+t"(t' et t" les temps alloués à chaque niveau des cellules et Qi (connu). Nous maintenons toujours la conversation audio de données: 0,059s ; 0,063s ; 0,059s ; 0,055 s ; 0,071 pour le niveau 1 et 0,08s ; 0,075s ; 0,078s ; 0,85s ; 0,074 pour le niveau 2. Et les débits respectifs de 40 et 30 Kbits/s.

Les associations suivantes sont calculées en fonction des figures 43 et 44 comme le présente les tableaux 11,12 et13.

Première association: Q1=5kbits, Q'2= D1*t'$_2$ + D2*t"$_2$ alors T1=$\frac{Q'2}{Q1}$;

Deuxième association: Q'3=D_1*t'$_3$ +D_2*t"$_3$ alors T_2=$\frac{Q'3}{Q'2}$;

Troisième association: Q'$_1$=D_1*t'$_1$+t"$_1$$D_2$ alors T_3=$\frac{Q'1}{Q'3}$**;**

Quatrième association: Q'$_4$=D_1t'$_4$ + D_2*t"$_4$alors T^4= $\frac{Q'4}{Q'1}$;

Cinquième association: Q"$_3$=D_1*t'$_3$ +D_2*t"$_3$ alors T_5=$\frac{Q'3}{Q'4}$.

Le tableau 11 donne les transmissions intercellulaires à deux niveau pour f(x)= x

m	**Di**		**t_i**		**Q_i**	**Q'$_{i+1}$**	**U**	**Q_{i+1}**	**T_i**	**w_i**	**f(x)=x**	**T**
	Niveau 1	Niveau 2	t'$_i$	t"$_i$								
1er	40kbit/s	30kbit/s	0,059	0,080	Q_1= 5kbit	Q'$_2$=4,77	0,07	Q2= 4,84	0,954	0,24	0,954	0,892
2 **eme**	40kbit/s	30kbit/s	0,063	0,075	Q_2= 5,61	Q'$_3$=4,7	0,05	Q3= 4,57	0,837	0,26	0,837	
3 **eme**	40kbit/s	30kbit/s	0,059	0,078	Q_3= 5,45	Q'$_1$= 4,76	0,09	Q1= 4,85	0,873	0,22	0,873	
4 **eme**	40kbit/s	30kbit/s	0,055	0,085	Q_1= 5,66	Q'$_4$= 4,75	0,06	Q4= 4,81	0,839	0,13	0,839	
5 **eme**	40kbit/s	30kbit/s	0,071	0,074	Q_4= 5,43	Q'$_3$=5,06			0,932	0,15	0,932	

Tableau 11: Transmission des données intercellulaire avec deux niveaux.

Mesurons la qualité de service pour les deux cas précédents, lorsque f(x) = log x c'est à dire

$$T = f(x) = \prod_{i=1}^{m} x_i^{W_i}$$

Transmission intercellulaire(Handover) à un niveau (tableau 12)

m	D$_i$' (constant)	t $_i$(en (seconde)	Q_i	Q'$_{i+1}$	U	$Q_{i+1=}$ Q'$_{i+1}$ +U	**$T_{i=}$ Q_{i+1}/Q_i**	W_i	f(x)= log(x)	T
1^{ere}	40kbit/s	0,139	Q1=**6**	Q'2=t2*D1=**5,52**	0,09	Q2=5,52+0,09	**0,910**	0,24		0,815
2 eme	40kbit/s	0,138	Q2=**6,5**	Q'3=t3*D1=**5,48**	0,06	Q3=5,8+0,06	**0,843**	0,26		
3 eme	40kbit/s	0,137	Q3=**7,03**	Q'1=t1*D1=**5,56**	0,05	Q1=5,4+0,05	**0,791**	0,22		
4 eme	40kbit/s	0,140	Q1=**7,5**	Q'4=t4*D1=**5,60**	0,04	Q4=5,4+0,04	**0,746**	0,13		
5 eme	40kbit/s	0,145	Q4=**7,8**	Q'3=t3*D1=**5,8**			**0,743**	0,15		

Tableau 12: Transmission des données intercellulaire avec un niveau.

Transmission intercellulaire(Handover) à deux niveaux (Tableau 13)

m	Di		t_i		Q_i	Q'_{i+1}	U	Q_{i+1}	T_i	w_i	f(x)= log(x)	T
	Niveau 1	Niveau 2	t'_i	t''_i								
1er	40kbit/s	30kbit/s	0,059	0,080	Q1= 5kbit	Q'2=4,77	0,087	Q2= 5,61	0,954	0,24		0,883
2 eme	40kbit/s	30kbit/s	0,063	0,075	Q2= 5,61	Q'3=4,7	0,075	Q3= 5,45	0,837	0,26		
3 eme	40kbit/s	30kbit/s	0,059	0,078	Q3= 5,45	Q'1= 4,76	0,090	Q1= 5,66	0,873	0,22		
4 eme	40kbit/s	30kbit/s	0,055	0,085	Q'1= 5,66	Q'4= 4,75	0,068	Q4= 5,43	0,839	0,13		
5 eme	40kbit/s	30kbit/s	0,071	0,074	Q4= 5,43	Q'3=5,06			0,932	0,15		

Tableau 13: Transmission des données intercellulaire entre deux niveaux.

Premier cas: résultats de simulation pour mesurer la qualité de service de type audio pour un transfert intercellulaire (Handover) à un niveau (figure 45) pour la même fonction f(x) = x

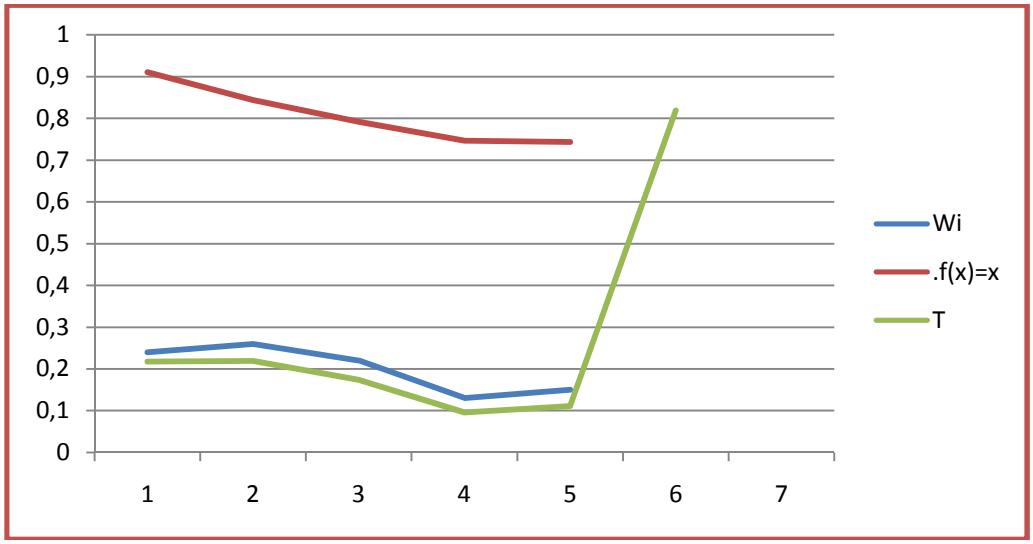


Figure 45:qualité de service lors d'un transfert intercellulaire avec un niveau.
avec T= 0,82∈ [**0**, **1**].

Deuxieme cas: deuxième résultat de simulation pour mesurer la qualité de service de type audio pour **f(x)= x** alors

$$T = f(x) = \sum_{i=1}^{m} W_i x_i$$

pour un transfert intercellulaire (Handover) à deux niveaux (figure 46)

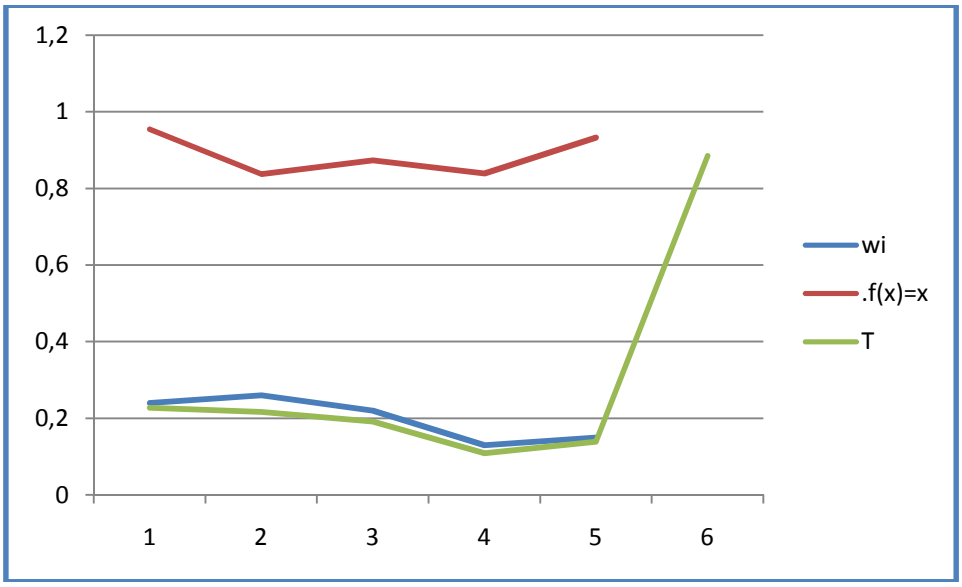


Figure 46: qualité de service lors d'un transfert intercellulaire entre deux niveaux.
avec T= 0,892∈ [**0**, **1**]

Troisième cas: troisième résultat de simulation pour mesurer la qualité de service de type audio pour :

$$T = f(x) = \prod_{i=1}^{m} x_i^{W_i}$$

pour un transfert intercellulaire (Handover) à un niveau (figure 47)

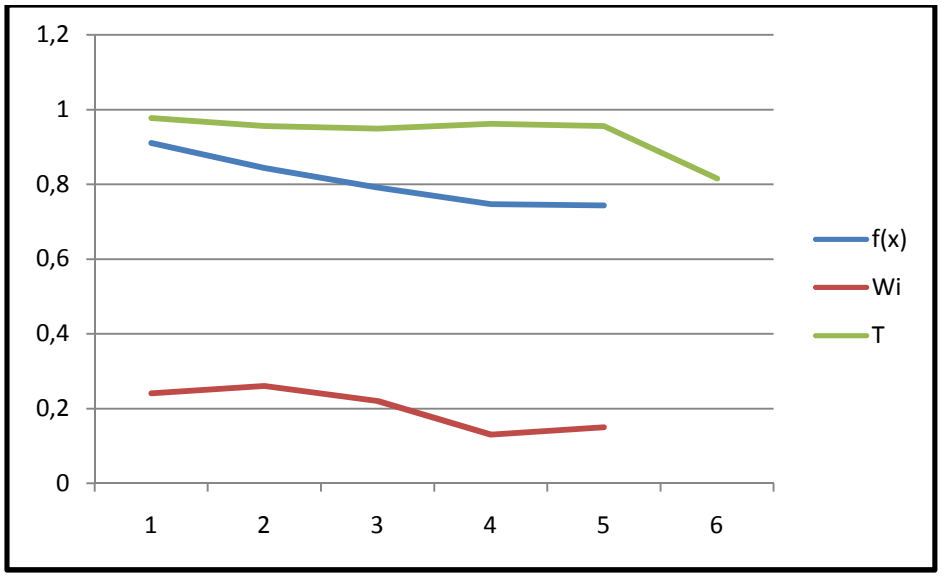


Figure 47: qualité de service lors d'un transfert intercellulaire avec un niveau.
avec T= 0,815∈ [**0**, **1**]

Quatrième cas: quatrième résultat de simulation pour mesurer la qualité de service de type audio pour :

$$T = f(x) = \prod_{i=1}^{m} x_i^{W_i}$$

pour un transfert intercellulaire (Handover) à deux niveaux (figure 48)

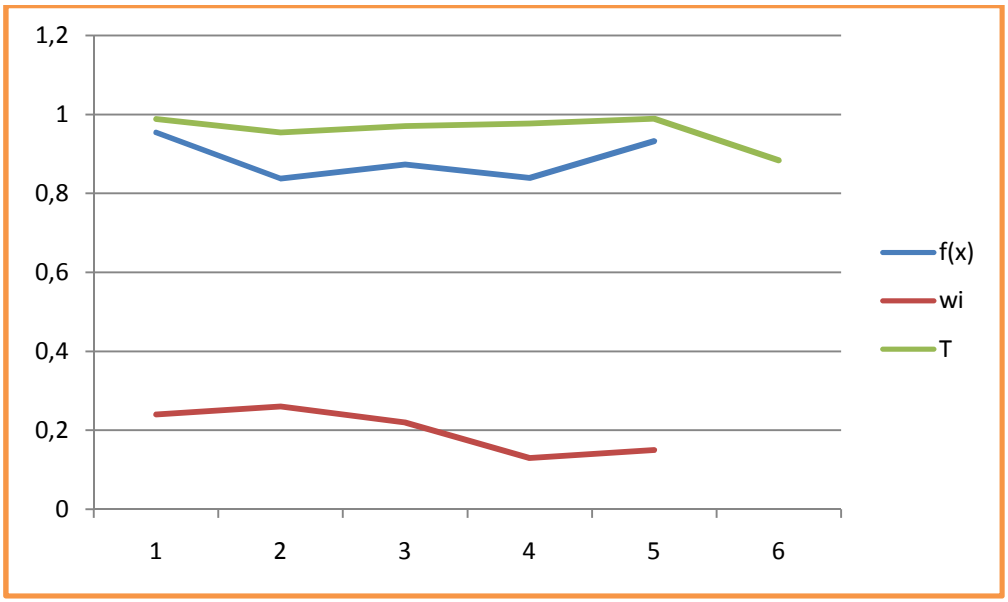


Figure 48:qualité de service lors d'un transfert intercellulaire entre deux niveaux.
avec T= 0,883∈ [**0**, **1**]

Trafic Vidéo

Pour le trafic vidéo nous avons utilisé un **taux de transfert** compris entre**16-384 kbit/s** avec un **délai aller < 10 s** pris dans: Recommandations G1010 de l'ITU-T pour les applications sur Internet et leurs paramètres [58].

Les tableaux 14, 15, 16,17 nous proposent quatre cas des données lors d'une transmission intercellulaire de différents niveaux.

Premier cas: **Handover avec un niveau**

Mesurons la qualité de service **T** lorsque **f** est une fonction identité c'est à dire **f(x) = x,** donc

$$T = f(x) = \sum_{i=1}^{m} W_i x_i$$

Posons: $Q_i = t_i * D_i$(t_i est le temps aléatoire de transmission pour chaque cellule et D_i le débit).

$T_i = \frac{Q'_{i+1}}{Q_i} \in [0,1]$ $Q_{i+1=}Q'_{i+1\,+}\mathbf{U}$ avec (**U**: nouvelles informations).

Nous prenons pour exemple la conversion vidéo avec 3,75s; 4,00s; 3,5s; 4,5s; 3,00s les temps aléatoires attribués à chaque état et un débit constant de 70kbit/s pour toutes les cellules C_i.

1ere association: $T_1=\frac{Q'2}{Q1}$; **2eme association**: $T_2=\frac{Q'3}{Q'2}$; **3emeassociation**: $T_3=\frac{Q'1}{Q'3}$;

4emeassociation: $T4=\frac{Q'4}{Q'1}$; **5emeassociation**: $T_5=\frac{Q'3}{Q'4}$.

m	D_i' (constant)	t_i(en (seconde)	Q_i(kbit)	Q'_{i+1}(kbit)	U (kbit)	$Q_{i+1=}$ $Q'_{i+1\,+}$ U	$\mathbf{T_i=}$ $\boldsymbol{Q_{i+1}/Q_i}$	W_i	f(x)=x	T
1ere	70kbit/s	3,75	Q1=**350**	Q'2=t2*D1=**280**	0,98	Q2=280+0,98 280,98	**0,8**	0,25	0,80	
2 eme	70kbit/s	4,00	Q2=**300**	Q'3=t3*D1=**245**	1,6	Q3=245+1,6 246,6	**0,871**	0,19	0,871	
3 eme	70kbit/s	3,5	Q3=**320**	Q'1=t1*D1=**262,5**	2,1	Q1=262,5+2,1 264,6	**0,851**	0,20	0,851	0,908
4 eme	70kbit/s	4,5	Q4=**205**	Q'4=t4*D1=**227,5**	2,4	Q4=227,5+2,4 229,9	**0,859**	0,18	0,859	
5 eme	70kbit/s	3,00	Q5=**295**	Q'3=t5*D1=**210**			**0,913**	0,24	0,913	

Tableau 14: Transmission des données intercellulaire avec un niveau

Deuxième cas: Handover avec deux niveaux (figure 49)

Mesurons la qualité de service pour la même fonction f(x)= x .

Si Di est constant par niveau: $Q'_2=D_1t'_2 + D_2t''_2$ avec $t=t_2'+t''_2$ et Q_1 connu (860kbit) alors $T_1=\frac{Q'2}{Q1}$

Nous maintenons toujours la conversation vidéo de données pour 70s; 70s;70; 70s;70s pour le niveau 1 et 90s ; 90 ; 90s ; 90s; 90s pour le niveau 2

Les associations suivantes sont calculées en fonction de la figure 54 comme le présente lestableaux14,15,16.

1ere association: Q1=5kbits, Q'2= D1*t2 + D2*t'2 alors $T1=\frac{Q'2}{Q1}$;

2emeassociation: $Q'3=D_1*t'_3 +D_2*t''_3$ alors $T_2=\frac{Q'3}{Q'2}$;

3emeassociation: $Q'_1=D_1*t'_1+t''_1D_2$ alors $T_3=\frac{Q'1}{Q'3}$**;**

4emeassociation: $Q'_4=D_1t'_4 + D_2*t''_4$alors $T^4=\frac{Q'4}{Q'1}$;

5emeassociation: $Q''_3=D_1*t'_5 +D_2*t''_5$ alors $T_5=\frac{Q'3}{Q'4}$.

m	Di		t_i		Q_i	Q'_{i+1}	U	Q_{i+1}	T_i	w_i	f(x)=x	T
	Niveau 1	**Niveau 2**	**t'_i**	**t''_i**								
1er	90kbit/s	70kbit/s	4s	4,2s	Q1= 860kbit	Q'2= 830,5kbit	3,75 kbit	Q2= 834,25kbit	0,965	0,25	0,965	0,956
2 eme	90kbit/	70kbit/s	5,2s	3,75s	Q2= 745kbit	Q'3= 730,5kbits	4,07 kbit	Q3= 734,57kbit	0,980	0,17	0,980	
3 eme	90kbit/	70kbit/s	5,30s	2,57s	Q3= 910kbit	Q'1= 654kbits	3,55 kbit	Q1= 657,5 kbit	0,890	0,22	0,916	
4 eme	90kbit/	70kbit/s	4,25s	3,25s	Q'1= 830kbit	Q'4= 610kbits	2,24 kbit	Q4= 612,24,kbit	0,927	0,19	0,903	
5 eme	90kbit/	70kbit/s	3,75s	3s	Q4= 780kblt	Q'3= 547,5kbit			0,894	0,20	0,842	

Tableau 15: Transmission des données intercellulaire entre deux niveaux.

Mesurons la qualité de service comme les deux cas précédents, lorsque f(x) = log x c'est-à-dire

$$T = f(x) = \prod_{i=1}^{m} x_i^{W_i}$$

Nous maintenons toujours la conversation vidéo: nous proposons les temps aléatoires100s; 100; 100s; 100s; 100s pour le niveau1

<u>Troisième cas</u>: Handover avec un niveau

m	D_i' (constant)	t_i(en (seconde)	Q_i(kbits)	Q'_{i+1}(kbits)	U(kbit)	$Q_{i+1=}$ Q'_{i+1} +U	T_i	W_i	.f(x)= log(x)	T
1ere	100kbit/s	3,2s	Q1=520	Q'2=t2*D1= **450**	3,2	Q2= 453,2	**0,865**	0,32	0,865	0,871
2eme	100kbit/s	4,5s	Q2=**370**	Q'3=t3*D1= **370**	4,7	Q3=374,7	**0,902**	0,30	0,902	
3 eme	100kbit/s	3,7s	Q3=**625**	Q'1=t1*D1= **320**	5,25	Q1=320,25	**0,854**	0,19	0,854	
4 eme	100kbit/s	5,2s	Q1=**715**	Q'4=t4*D1= **520**	2,35	Q4=522,35	**0,990**	0,15	0,990	
5 eme	100kbit/s	5,75s	Q4=**705**	Q'3=t5*D1= **575**	6,15	Q=581,15	**0,883**	0,21	0,883	

Tableau 16: Transmission des données intercellulaire avec un niveau.

Quatrième cas: Handover avec deux niveaux

Nous maintenons toujours la conversation vidéo: 110s; 110; 110s; 110s; 110s pour le niveau1 et 100;100;100;100;100 pour le niveau 2.

m	Di		t_i		Q_i	Q'_{i+1}	U	Q_{i+1}	T_i	w_i	.f(x)= log(x)	T
	Niveau 1	Niveau 2	t'_i	t''_i								
1	110kbit/s	100kbit/s	1,75s	3,2s	Q1= 650kbit	Q'2= 604,2	0,87	Q2= 605,07	0,929	0,25	0,929	0,911
2	110kbit/s	100kbit/s	3,22s	2,5s	Q2= 600kbits	Q'3= 599,7	0,75	Q3= 600,45	0,991	0,26	0,991	
3	110kbit/s	100kbit/s	2,27s	3,5s	Q3= 550kbits	Q'1= 512,5	0,90	Q1= 513,40	0,853	0,22	0,853	
4	110kbit/s	100kbit/s	1,37s	3,2s	Q'1= 490kbits	Q'4= 470,7	0,68	Q4= 471,38	0,916	0,13	0,916	
5	110kbit/s	100kbit/s	2,45s	1,15s	Q4= 520kbits	Q'3= 384,5	0,70	385,40	0,815	0,11	0,815	

Tableau 17: Transmission des données intercellulaire entre deux niveaux.

Premier cas: premier résultat de simulation pour mesurer la qualité de service **T** de type vidéo pour **f(x) = x** pour un transfert intercellulaire (Handover) à un niveau (figure 48).

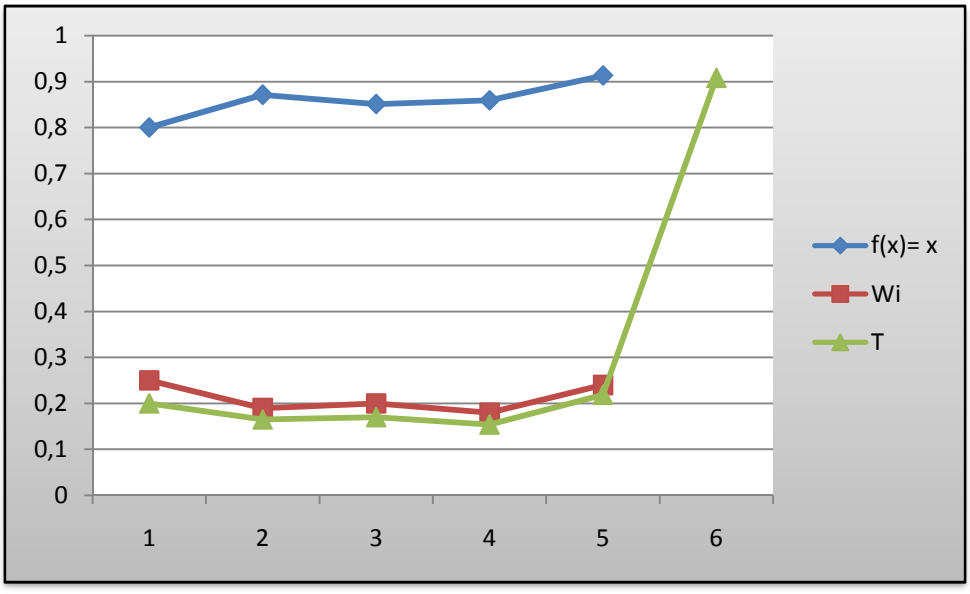


Figure 48: Qualité de service lors d'un transfert intercellulaire entre un niveau avec T = 0,908∈ [**0**, **1**]

Deuxième cas: deuxième résultat de simulation pour mesurer la qualité de service **T** de type vidéo pour **f(x) = x** pour un transfert intercellulaire (Handover) à deux niveaux (figure 49).

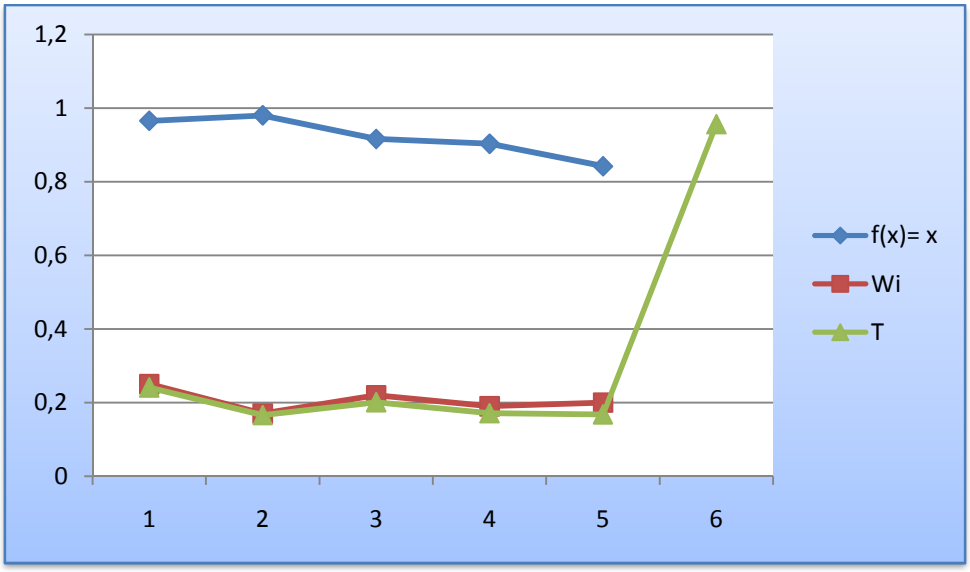


Figure 49: qualité de service lors d'un transfert intercellulaire entre deux niveau avec T = 0,956 ∈ [**0**, **1**]

Troisième cas: troisième résultat de simulation pour mesurer la qualité de service **T** de type vidéo pour **f(x) = log(x)**pour un transfert intercellulaire (Handover) à un niveau (figure 50).

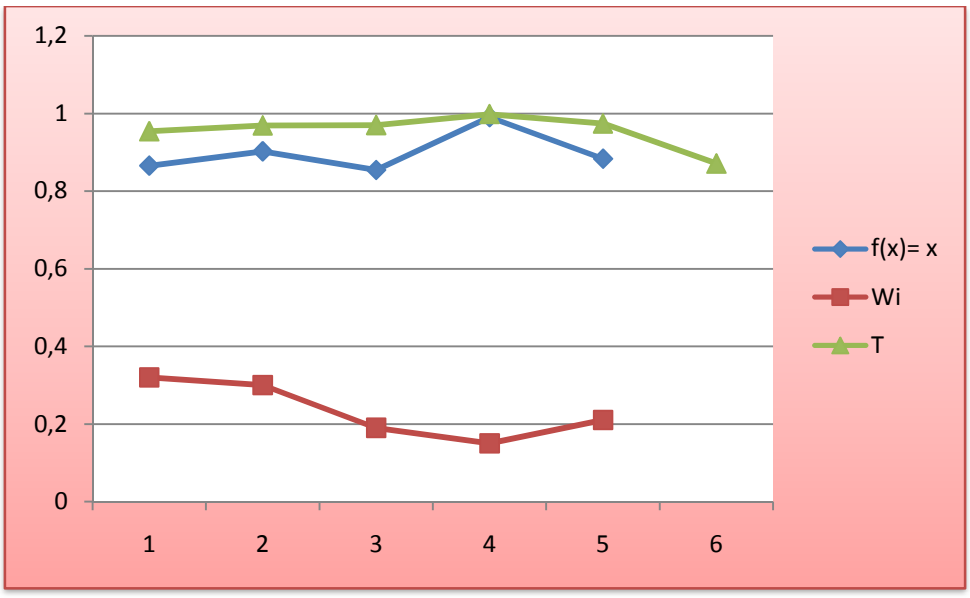


Figure 50: qualité de service lors d'un transfert intercellulaire entre un niveau avec T = 0,871 ∈ [**0**, **1**]

Quatrième cas: quatrième résultat de simulation pour mesurer la qualité de service **T** de type vidéo pour **f(x) = log(x)**pour un transfert intercellulaire (Handover) à deux niveaux (figure 51).

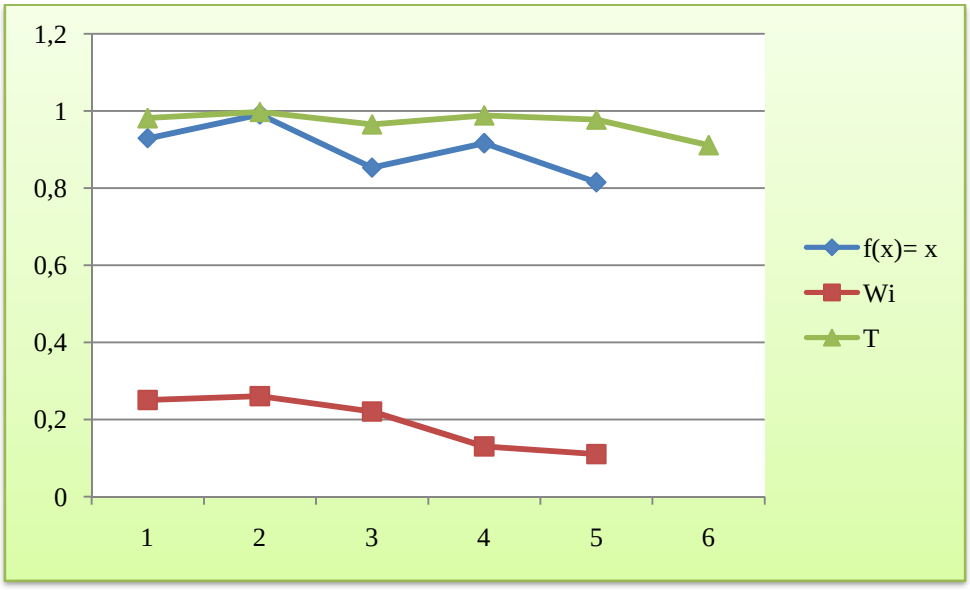


Figure 51: qualité de service lors d'un transfert intercellulaire entre deux niveau avec T = 0,911∈ [**0**, **1**]

IV.9 Conclusion

Les applications audio et vidéo font parties des applications les plus exigeantes en termes de qualité de service (QoS), surtout quand elles font intervenir une conversation entre plusieurs participants. Pour garantir un fonctionnement correct, le délai aller Idéal doit être inférieur à 150 ms et ne dépasse pas les 400 ms, pour l'application de type audio et ne dépasse pas 10 s pour des applications Vidéo [58].

Le protocole SCTP doit garantir la qualité de service d'une association des stream (flux) lors d'une association. Les fonctions d'agrégation nous permettent d'apporter un jugement quantifiable sur plusieurs transitions intercellulaires pouvant monter la QoS.

Pour atteindre un consensus sur ces jugements, des fonctions d'agrégation classiques ont été proposées: la moyenne arithmétique et quasi-arithmétique. Le choix d'une fonction d'agrégation pourra satisfaire la plus grande partie des propriétés pour l'agrégation qui montre les différentes transmissions qui peuvent être soit unidirectionnelles (simplex), bidirectionnelles altérées (half-duplex), bidirectionnelles simultanées (full-duplex), etc. Parmi ces deux fonctions d'agrégation, citées ci-dessus, la moyenne quasi-linéaires se distingue

grâce à son poids **w_i (puissance du signal)** qui représente le poids du Handover et dépend de l'altitude entre deux antennes en interférence, et aussi les obstacles géographiques

Nous constatons pour la transmission audio, les deux premières figures présentent une amélioration de la qualité de services par rapport au second. Nous constatons également que lorsqu'on change la fonction d'agrégation, les taux de transmission de la quatrième figure offre une meilleure qualité de service que le troisième. Par contre pour la transmission vidéo, il se dégage une excellence amélioration de la qualité de service par rapport à la précédente. Cette confirmation montre que les différentes figures présentent des caractéristiques plus proches de la réalité, car il est rare que le débit soit constant dans une cellule, puisqu'au fur qu'on s'éloigne du point d'accès, le débit diminue [9]

Conclusion générale et Perspectives

Il est question pour nous, tout au long de notre rédaction de présenter la gestion de la mobilité dans les réseaux communautaires sans fil propre à nos communautés. Nous avons fait une étude d'exploration des réseaux mobiles (GSM, UMTS) et sans fil [IEEE802.11x (WIFI), IEEE 802.16(WIMAX)], afin de proposer celui qui répond mieux à la construction des réseaux communautaires à moindre coût. Le choit est porté sur le réseau sans fil IEEE802.11x(WIFI) compte tenu des avantages qu'ils présentent(coût des matériels plus acceptable, son implantation simple, rapide et l'utilisation des bandes comprises entre 2,4 et 2,483 GHz, et 5,725 et 5,875 GHz, sans licence pour la technologie WLAN).

Nous avons également fait des études sur différents protocoles de gestion de mobilité au niveau réseau, application et transport tout en relevant les avantages et les inconvénients qu'ils présentent. Choisir celui qui répond le mieux à notre contexte.

Au préalable Mobile IP (MIP) [7,44] a été proposer pour résoudre les problèmes de rupture de communication durant les déplacements des nœuds mobiles dans des réseaux IP, mais [38] nous fais comprendre qu'il ne prend pas en charge le transfert intercellulaire rapide pour les applications sensibles au délai et aux pertes de paquets. Enfin des extensions de MIP, telles que le FMIP (Fast Handover for MIP) et le HMIP (Hierarchical MIP) ont été proposé mais ceux-ci ne garantissent pas un délai de relève minimal et une perte de paquets tolérable [30].

Un second protocole à proposer est SIP. Ce protocole SIP fournit la gestion de la localisation pour la mobilité des terminaux. Mais dans [44], SIP ne fournit pas la gestion transparente du transfert intercellulaire. Toutefois, lors d'un mouvement, le protocole SIP ne peut pas garantir le maintien d'une session TCP ou assurer la mise en correspondance des ports UDP [44]. Au niveau transport les protocoles de mobilité SCTP/mSCTP ont été proposés et grâce à leurs techniques du **Multihoming** qui permet d'ouvrir plusieurs connections IP pour une même association, un mécanisme de contrôle d'erreur qui permet de détecter les pertes, la rupture de séquences ou la duplication de paquets et une configuration dynamique des adresses durant une association. La **Multisteaming** qui permet la transmission de plusieurs streams (ou encore multiplexage de flux) au sein d'une même association [45]. Ces deux techniques nous ont permis de les choisir comme protocoles promoteurs pour la gestion de mobilité dans notre contexte des réseaux communautaires sans fil.

Notre première contribution dans cette thèse est bien définie. Assurer la mobilité basée sur la chaine de Markov, dont les études nous ont permis de modéliser le protocole mSCTP d'ou les résultats nous ont été donnés sous la plate forme Matlab pour n=4(nombre de

cellules), m=5 (nombre d'association), et le choix du paramètre **δ**=1/3, nous montre que l'utilisateur pourra basculer entre les cellules C1 ou C3 sans conséquence.

Une deuxième contribution est l'application des fonctions d'agrégation qui nous ont permis d'apporter un jugement quantifiable sur plusieurs transitions intercellulaires pouvant monter la qualité de service(QoS).

En conclusion, nous pouvons dire que notre principale contribution, à travers cette thèse, à été de proposer des solutions capables d'améliorer la qualité de service dans un environnement IP mobile. Et nos résultats de simulation nous ont permis de minimiser la puissance du signale grâce au paramètre **wi** (puissance du signale), qui représente les poids du Handover et dépend également de l'altitude entre deux antennes en interférence, et aussi les obstacles géographiques. Ces fonction d'agrégation nous ont également permis d'apporté des jugements sur plusieurs transitions intercellulaire, et de montrer une meilleure qualité de service excellente sur les applications de type audio et plus excellentes pour les applications vidéo.

Nous nous intéresserons dans nos travaux futurs, sur la question sécuritaire dans réseaux communautaires sans fil, qui reste ouverte et intéressées aux communautés scientifiques. Nos réseaux communautaires sans fil, où l'écoute dans l'air permet de recueillir l'information qui circule et où la transmission radio permet d'envoyer de l'information sur le réseau. Il ne faut cependant pas oublier que des antennes directives peuvent, dans certaines conditions, augmenter considérablement la portée. Ces antennes directives permettent à une entité étrangère d'écouter ce réseau ou de lui envoyer des informations

Bibliographie

[1] Jean-Baptiste SANGLA. Résumé de l'étude SagaTel sur les marchés du WiFi en France, 2007.

[2] Pantelis A. Frangoudis and George C. Polyzos, Vasileios P. Kemerlis. Wireless Community Networks: An Alternative Approach for Nomadic Broadband Network Access, 2011

[3] Gérard-Michel Cochard. Aspect avancés des réseaux, 2007.

[4] Cédric DEMOULIN, Marc Van Droogenbroeck. Principes de base du fonctionnement du réseau GSM, 2004.

[5] Jean-Philippe Muller**.** Le réseau GSM et le mobile, 2007.

[6] Eric MEURICE. L'UMTS et le haut-débit mobile, 2007.

[7] GUY PULLOLE. Les réseaux, 6^{me} édition septembre, 2006

[8] Philippe ATELIN. Réseaux sans fil 802.11:technologie, déploiement, sécurisation, 2010.

[9] Renaud Garelli – Nicolas Royères – Christian Tschopp. 802.11 vs Hyperlan, 2004 – 2005

[10] Rami LANGAR. Mécanismes de Gestion de la Mobilité et Evaluation de Performance dans les Réseaux Cellulaires tout-IP, Thèse de doctorat, de l'Ecole Nationale Supérieure des Telecommunications de Paris, 3 Juillet 2006

[11] POOL. Prescriptions de gestion de la mobilité au niveau des interfaces de nœuds de réseau pour les systèmes postérieurs aux IMT-2000 (Recommandations UIT-T de la série Q–Supplément 52)

[12] Jérémie Difaye. Les différents types des réseaux sans fil, 2005-2006.

[13] BELABDELLI Abdelheq, OUKAZ Mokhtar. Dimensionnement d'un Réseau Sans Fil Wifi, Mémoire Pour l'obtention du diplôme de Ingénieur d'Etat en Télécommunications, juillet 2012

[14] IMLAZEN**.** Évaluation de la vulnérabilité des réseaux locaux sans fil (WLAN) 802.11 (ITSPSR-21A), Mai 2009.

[15] Michel Duchateau. Analyse et simulation du déploiement d'un réseau sans fil à L'ULB, Mémoire de fin d'études en vue de l'obtention du grade d'Ingénieur Civil Electricien, spécialisé en Télécommunications, 2004-2005.

[16] BARRERE François**.** Les réseaux sans fil, DESS MIAGe 2001-2002.

[17] Jean-Claude. La norme WiMAX, 2011.

[18] P. Sicard. Le contrôle de congestion dans Internet, 26/01/2016

[19] Martin Heusse. Réseaux locaux sans fil: Vers une utilisation efficace du canal radio, 30 novembre 2009.

[20] ANDRE Emmanuel, DE RUGY Guillaume, HERBIET Guillaume-Jean. Réseaux Mobiles maillés, 2005.

[21] Aurélien Géron. WiFi PROFESSIONNEL (la norme 802.11, le déploiement, la Sécurité), 2009.

[22] EL HAJJ Paul, DAHBI Nabil. Etude de la technologie WiMAX mobile, article ,20/01/2010

[23] Viken Toramanian, Rocio Ruz, Michèle Germain. WiMAX à l'usage des Communications haut débit. 15 mars 2008.

[24] TALAI Meriem**.** Etude et implémentation d'algorithme de mobilité de groupe et application au P-learnings. Mémoire présentée en vue de l'obtention du diplôme de magister, 2009/2010.

[25] David Elorrieta. Protocoles de routage pour l'interconnexion des réseaux AdHoc et UMTS Licencié en Informatique, 2006–2007.

[26] GUOZHI WEI. Optimisation du Handover dans le protocole ipv6 mobile avec la méthode e-hcf. Thèse de doctorat, université paris xii, 2007.

[27] DJEBBAR Nadji, ADDAD Rami Akrem, KHETTAB Yacine, MOHAMEDI El Haithem. IPV6 MOBILE, 2014-2015

[28] Christophe. Réseaux informatique: Modèle OSI et protocole TCP/IP, 2011.

[29] C. Perkins, "IP Encapsulation within IP", Internet Engineering Task Force, RFC

2003, Octobre 1996.

[30] Nicolas Montavont. La mobilité dans les réseaux IP, Rapport de D.E.A.Informatique, 2000/2001.

[31] Lina El-Mekkaoui. Services de Mobile IP au dessus de MPLS, Diplôme d'Etudes Approfondies Réseaux de télécommunications, 22/12/2003.

[32] Nathan CASTELEIN, Karim HAMIDOU, César MARCHAL, Christian PATRY Projet d'étude et d'expérimentation – Mobilité IPv6, 2012.

[33] SALMON Nicolas .COURS IPV6, 2010.

[34] Frédéric Roudaut. Le protocole IPv6, Janvier 2009.

[35] DJEBBAR Nadji, ADDAD Rami Akrem, KHETTAB Yacine, MOHAMEDI El Haithem. IPV6 MOBILE, 2015.

[36] S.Tabbane, "Réseaux mobiles", Hermes, page 640, 1997.

[37] Xavier Hick. Analyse de performance de handover vertical entre réseaux UMTS et 802.11, mémoire d'ingénieur civil en informatique. Université libre de Bruxelles, 2005.

[38] EZZOUHAIRI Abdellatif. Intégration et gestion de mobilité de bout en bout dans les réseaux mobiles de prochaine génération, Thèse de doctorat de l' université de Montréal. le Décembre 2009.

[39] R. Stewart, Q. Xie, K. Morneault, C. Sharp, H. Schwarzbauer, T. Taylor, I. Rytina, M. Kalla, L. Zhang, V. Paxson, «Stream Control Transmission Protocol», RFC2960, Engineering Task Force, October 2000.

[40] R. Stewart, Qiaobing Xie, «Stream Control Transmission Protocol (SCTP): a reference guide», Addison wesley, London 2002.

[41] R. Stewart, M. Ramalho, Q. Xie, M. Tuexen, P. Conrad, «Stream Control Transmission Protocol (SCTP) Dynamic Address Reconfiguration»,draft-ietf-tsvwg-addip-sctp- 11.doc, Internet Draft, February 2005 (Work in Progress).

[42] J M. Riegel, M. Tuexen, «Mobile SCTP», draft-riegel-tuexen-mobile-sctp-04.txt,

Internet- Draft, October 2004 (Work in Progress).

[43] Znaty. SCTP: Stream Control Transmission Protocol et Services: http://www.efort.com,2009.

[44] POOL. Prescriptions de gestion de la mobilité au niveau des interfaces de nœuds de réseau pour les systèmes postérieurs aux IMT-2000,Série Q Supplément **52** (12/2004)

[45] Znaty. SCTP : Stream Control Transmission Protocol Protocole et Services, 2009.

[46] TALAI Meriem**.** Etude et implémentation d'algorithme de mobilité de groupe et application au P-learnings, Mémoire présenté en vue de l'obtention du diplôme de magister,2010.

[47] François Buntschu, Rudolf Scheurer, Antoine Delley.CTP (Stream Control Transmission Protocol) Une alternative à TCP et UDP article du Flash informatique n° 9/2003.

[48] Une introduction aux chaînes de Markov, support de cours,2011.

[49] E. Pommies, S. Robin. Introduction aux chaînes de Markov homogènes, 16 juin 2004.

[50] Sébastien Loustau. Chaînes de Markov et Processus markoviens de sauts. Applications aux files d'attente, Année 2008-2009.

[51] Régine André-Obrecht, Julien Pinquier et Sergeï Sol. Chaînes de Markov, 2011**.**

[52] DAVID COUPIER. Processus stochastiques, 2014.

[53] Nils Berglund. Chaînes de Markov, Master 2 de Mathématiques, Université d'Orléans ,Décembre 2007.

[54] Sarah Dendievel , Sophie Hautphenne. Chaînes de Markov et Google, 2012.

[55] E. Pommies, S. Robin Introduction.aux chaines de Markov homogènes, 16 juin 2004.

[56] Thierry Bodineau. Chaînes de Markov et martingales, Novembre 2013.

[57] Recommendation UIT-R M.1079-2,(1994-2000-2003).

[58] Technical Report. International Telecommunication Union (ITU-T-Rec. G.1010). End- user Multimedia QoS Categories. 2001.

[59] J. Gerard, I. I. Heinz, P. D. Amer, “Priorities in SCTP Multisteaming’’, 8th World Multiconference on Systemics, Cybernetics and Informatics SCI , Juillet 2004.

[56] R. Stewart, L. Ong, I. R. Arias, K. Poon, P. Conrad, A. Caro, M. Tuexen, “SCTP Implementers Guide’’, draft-ietf-tsvwg-sctpimp guide -10.txt, 2003.

[57] M. Arif, S. Hafid, T.Brouard, N. Vincent. AWFO (un opérateur d’agrégation) pour la reconnaissance des formes,2005.

[58] Sakuna CHAROENPANYASAK. Optimisation inter-couches du protocole SCTP en réseaux ad hoc, thèse de doctorat de l’université de Toulouse, 23/06/2008

[59] Michel Grabisch Patrice Perny. Agrégation Multicritère, 12 mars 2002.

[60] Jean-Luc Marichal Fonctions d’agrégation pour la décision, 4 avril 2003.

[61] J. Aczel. Lectures on functional equations and their applications. Academic Press, New York, 1966.

[62] J.C. Fodor and M. Roubens. Fuzzy Preference Modelling and Multi-Criteria Decision Aid. Kluwer Academic Publisher, 1994

[63] A. N. Kolmogoroff. Sur la notion de la moyenne. (French).Atti Accad. Naz. Lincei, 12(6) :388–391, 1930.

[64] J.L. Marichal. Aggregation operators for multicriteria decision aid. PhD thesis, University of Liège, 1998.

[65] J.-L. Marichal and M. Roubens. Characterization of some stable aggregation functions. In Proc. 1st Int. Conf. on Industrial Engineering and Production Management (IEPM’93), pages 187–196, Mons, Belgium, June 1993.

[66] J. Aczel and J. Dhombres. Functional equations in several variables. Cambridge University Press, Cambridge, 1989. With applications to mathematics, information theory and to the natural and social sciences.

[67] M. Nagumo. Ubereine klasse der mittelwerte.(German).Japanese Journ. Of Math, 7 :71–79, 1930.

[68] M. Mizumoto. Pictorial representations of fuzzy connectives, part I : Cases of t- norms, t-conorms and averaging operators. Fuzzy Sets & Systems, 31 :217–242, 1989

[69] J. J. Dujmovic. Weighted conjunctive and disjunctive means and their application in system evaluation. Univ. Beograd. Publ. Elektrotehn. Fak. Ser. Mat. Fiz, (461-497) :147–158, 1974.

[70] P. S. Bullen, D. S. Mitrinovic, and P. M. Vasic. Means and their inequalities, volume 31 of Mathematics and its Applications (East European Series). D. Reidel Publishing Co., Dordrecht, 1988. Translated and revised from the Serbo-Croatian.

[71] M. Nagumo. ¨Ubereine klasse der mittelwerte.(German).Japanese Journ. Of Math., 7 :71–79, 1930.

[72] J. Aczel and C. Alsina. Synthesizing judgements : a functional equations approach. Math. Modelling, 9(3-5) :311–320, 1987. The analytic hierarchy process.

[73] E. F. Beckenbach and R. Bellman. Inequalities. Second revised printing. Ergebnisse der Mathematik und ihrer Grenzgebiete. Neue Folge, Band 30. Springer-Verlag, New York, Inc., 1965.

[74] H. Dyckhoff and W. Pedrycz. Generalized means as model of compensative connectives. Fuzzy Sets and Systems, 14(2) :143–154, 1984.

[75] D. Dubois and H. Prade. Weighted minimum and maximum operations in fuzzy set theory. Information Sciences, 39 :205–210, 1986.

Glossaire

A

ACK: Acknowledgment outrame d’acquittement

AH: Authenfication Header

ALG: Application Level Gateway

AP: Access Point

AR: routeur d'accès

ARP: Address Resolution Protocol

ASCII: American Standard Code for Information Interchange

ASCONF: Address Configuration Change Chunk

ASCONF-Ack: Address Configuration Acknowledgement

AU: user agent

AuC: Authenfication Center

B

BAck: Binding Acknowledgement

BSC: Base Station Controller

BSS: Basic Set Service soit cellule de base

BSSID: Basic Service Set Identifier

BTS: Base Transceiver Station

BU: Binding Updates

C

CAU: user agent client

CCA: Clear Channel Assessment

CETP: Conférence Européenne des Administrations des Postes et Télécommunications

CIP: IP cellulaire

CH:serveur correspondant (correspondent host)

CN: Correspondent Node

CoA: Care-of Address

CP: contention Period ou période de contention

CS: Circuit Switched

CSMA/CA: Carrier Sense Multiple Access with Collision Avoidance

CSMA/CA: Carrier Sense Multiple Access with Collision Detection

CTS: Clear To Send ou contrôle de réponse

Cwnd: Congestion window

D

DAD: Duplicate Address Detection

DCF: Distributed Coordination Function ou fonction d'accès distribuée

DHCP: Dynamic Host Configuration Protocol

DIFS : DCF IFS

DNS: Domain Name Server

DS: Distribution System soit système de distribution

DSSS: Direct Sequence Spread Spectrum

E

EIR: Equipment Idendity Register

ESP: Encrypted Security Payload

ESS: Extended Service Set soit ensemble de services étendu

ESSID : Extended Service Set Identifier

ETSI: European Telecommunications Standards Institute

ETSI: European Télécommunications Standards Institute

F

FA: Foreign Agent

FAI: Fournisseur d'Accès Internet

FCC: Federal Communications Commission

FCS Frame: Check Sequence

FHSS: Frequency Hopping Spread Spectrum

FIFS: First In First Serve

FMIP: Fast handover Mobile

FN: Foreign Network

FTP: File Transfer Protocol

G

GFA: gateway foreign agent

GGSN: Gateway GPRS Support Node

GPRS: General Packet Radio Service

GSM: Global System for Mobile communications

H

HA: Home Agent

HLR: Home Location Register

HMIP: MIP hiérarchique

HoA: Home Address

HoA: Home Address

HTTP:HyperText Transfer Protocol

I

ICMPv6: Internet Control Message

IEEE: Institute of Electrical and Electronics Engineers

IETF: Internet Engineering Task Force

IGMP: Internet Group Management Protocol

IMEI: International Mobile Equipment Identity

IMT2000

IP: Internet Protocol

IP: Internet Protocol

IPSec: Internet Protocol Security

IPv4: Internet Protocol version 4

IPv6: Internet Protocol version 6

IR: Infrarouge

ISO: International Standard Organization

L

LAN: Local Area Network

LLC: Logical Link Control

LMA: local mobility agent

LOS: Line Of Sight

M

MAC: Medium Access Control

MAC-ID: Medium Access Control Identifier

MAP: mobility anchor point

ME: Mobile Equipment

MIP: mobile IP

MIS: Number of Inbound Streams

MLD: Multicast Listener Discovery

MN: Mobile Node

MSC: Mobile Switching Center

mSCTP: Protocole de transport des commandes de flux mobile

MT: mobile terminal

N

NAT: (Network Address Translation
NAT-PT: Network Address Translation - Protocol Translation

NAV: Network Allocation Vector

NEMO: NEtwork MObility

NIS: adresses d'annuaires

NLOS: Non Line Of Sight

O

OFDM: Orthogonal Frequency Division Multiplexing

OS: Outbound Streams

OSI: Open Systems Interconnection

P

PCF: Point Coordination Function ou fonction d'accès centralisée

PCF: Point Coordination Function ou Fonction de coordination par point

PDA: bureautiques, des assistants personnels

PDU : Protocol Data Unit

PIFS : PCF IFS

PLCP (Physical Layer Convergence Protocol)

PMD (Physical Medium Dependent)

POP3, IMAP4

PS: Paquet Switched

Q

QoS : Quality of Service

R

RLR: Réseaux Locaux Radioélectriques

RNC: Radio Network Controller

RNIS: Réseaux Numériques à Intégration de Services

RR: Round Robin

RTCP: Réseaux Téléphoniques Commutés Public

RTO: Retransmission Time Out

RA: Router Advertisement

RS: Router Solicitation

RTP: Real-Time Transport Protocol

RTSP: Real Time Streaming Protocol

RWND: Receiver Window

S

SACK: Selective Acknowledgment

SAU: user agent server

SCO: Stabilité Comparative pour les transformations Ordinales

SCTP: Stream control transmission protocol

SGSN: Serving GPRS Support Node

SIFS: Short Inter-Frame Spacing

SIIT: Stateless IP, ICMP Translation Algorithm

SIM: Subscriber Idendity Module

SIP: Session Initiation Protocol

SLAAC: StateLess Address Auto Configuration

SN: Sequence Number

SO: Stabilité pour les transformations Ordinales

SS: stations d'abonnés ou Subscriber Station

SSL: Secure Sockets Layer

SSN: Stream Sequence Number

SHA: Secure Hash Algorithm

SSTHRESH**:**Slow Start Threshold

T

TCP: transmission control protocol

TSN: Transmission Sequence Number

U

UDP: user datagram protocol

ULP: Upper Layer Protocol

UMTS: Universal Mobile Telecommunications Systems

V

VLR: Visitor Location Register

VPN: réseaux privés virtuels

W

W-CDMA: Wide band Code Division Multiple Access

Wi-Fi: Wireless Fidelity WIMAX

WiMAX: Worldwide interoperability for Microwave Access

WLAN: Wireless Local Area Network

WMAN: Wireless Metropolitan Area Network

WWAN: Wireless Wide Area Network

ANNEXES