МИНИСТАРСТВО ОДБРАНЕ
УНИВЕРЗИТЕТ ОДБРАНЕ
ВОЈНА АКАДЕМИЈА

МАСТЕР РАД

ПРЕДЛОГ КОНФИГУРАЦИЈЕ РАДИО МРЕЖЕ УПОТРЕБОМ DYNAMIC TDMA ВРСТЕ РАДА

студент:
капетан прве класе
Тамара Станојевић, дипл. инж.

ментор:
пуковник, ванр. проф.
др Бобан З. Павловић, дипл. инж.

Београд, 2024.

САДРЖАЈ

Увод **4**

1. MAC протоколи **6**

1.1. Случајни приступ 7

1.1.1. Једноставна ALOHA (енгл. *Pure Alloha*) 8

1.1.2. Слотована ALOHA (енгл. *Slloted Alloha*) 9

1.1.3. Вишеструки приступ са ослушкивањем носиоца - CSMA (енгл. *Carrier Sense Multiple Access*) 10

1.1.4. Вишеструки приступ са ослушкивањем носиоца уз откривање колизије – CSMA/CD (енгл. *Carrier Sense Multiple Access with Collision Detection*) 13

1.1.5. CSMA/CA (енгл. *Carrier Sense Multiple Access with Collision Avoidance*) ..15

1.2. Динамичко дељење канала 16

1.2.1. Резервација 16

1.2.2. Polling (прозивање) 18

1.2.3. Прослеђивање токена 20

1.3. Статичка подела канала 21

1.3.1. Вишеструки приступ са поделом фреквенције FDMA (енгл. *Frequency Division Multiple Access*) 21

1.3.2. Вишеструки приступ са кодном расподелом CDMA (енгл. *Code Division Multiple Access*) 25

1.3.3. Вишеструки приступ са временском расподелом - TDMA (енгл. *Time Division Multiple Access*) 28

2. Софтверски радио протокол – СРП **31**

2.1. Радио протоколи засновани на мултиплексирању са временским расподелом....31

2.2. Архитектура софтвера и платформе за извршавање 33

3. SNMP протокол (енгл. *Simple Network Management Protocol*) **35**

3.1. Компоненте SNMP протокола 38

3.1.1. SNMPv1 41

3.1.2. SNMPv2c 42

3.1.3. SNMPv3 42

4. Специфична конфигурација за коришћење Dynamic TDMA у GEOMUX **44**

4.1. Општи принципи 46

4.2. Конфигурација радија 47

4.3. Употреба 48

5. Разматрање могућих конфигурација радио мрежа у Dynamic TDMA моду рада **51**

6. Разматрана конфигурација мреже **56**

6.1. Могућа примена Dynamic TDMA врсте рада 59

7. Анализа реализоване конфигурације 62
7.1. Резултати лабораторијских испитивања реализоване конфигурације 62
Закључак 67
Преглед графичких приказа 69
Списак скраћеница 71
Преглед табела 73
Литература 74

Увод

Потреба за разменом информација постоји од како постоји човечанство. Рани облици комуникација укључивали су димне сигнале и бубњеве. Димни сигнали представљају један од најстаријих облика визуелне комуникације на даљину, који је служио за преношење информација и упозорења о опасности. Овај начин комуникације био је заступљен код различитих цивилизације, укључујући староседеоце Америке, кинеске заједнице дуж Великог зида и античке Грке. Поред визуелних метода, значајну улогу у комуникацији на даљину имали су и бубњеви, који су омогућавали акустични пренос порука, нарочито у шумовитим и тешко прегледним подручјима. Најразвијенији систем употребе бубњева забележен је код народа западне Африке, мада су сличне праксе постојале и у Новој Гвинеји и Амазонији. Бубњеви су такође имали важну функцију у војном контексту, где су коришћени за преношење наређења и обавештења на бојишту; један од познатијих историјских примера јесте систем сигнализације од Плимута до Лондона током напада Шпанске армаде на Енглеску. Касније, проналаском телефона, наизменичне струје и проналаском полупроводничких елемената, развој технологије је постао незаустављив и достигао је брзину развоја која се све теже прати. Толика брзина развоја је у доброј мери условљена развојем војне индустрије, односно развојем наоружања и људске склоности за ратним сукобима, као и због потребе људи да у мирнодопским ситуацијама комуницирају што је лакше могуће.

Радио представља систем бежичне комуникације који подразумева пренос енергије и информација посредством електромагнетних таласа који се шире кроз слободан простор. Ови таласи припадају делу електромагнетног спектра са фреквенцијама нижим од фреквенција видљиве светлости и емитују се из одговарајућих извора. Радио-таласи се користе за пренос информација, а њихово генерисање омогућавају предајници који емитују електромагнетне сигнале кроз ваздух или вакуум, најчешће у свим правцима. Радиотелеграфски системи представљају један од најранијих облика примене радио-технологије, при чему је пренос порука реализован коришћењем Морзеове азбуке, што се сматра почетком развоја радио-станица и радио-комуникације уопште [1].

Радио уређаји су комуникациони системи. Да би се комуникација успоставила, одговарајући радио протоколи морају бити дефинисани и имплементирани. Традиционално се радио уређаји имплементирају као наменске хардверске компоненте. Трендови развоја у последње две деценије су довели до појаве софтверских радија, где се све више компоненти имплементира као софтвер. Ово је случај са радио протоколом, који се тада назива **софтверски радио протокол**. Софтверски радио протоколи су типични системи за рад у реалном времену. У таквим системима активности се реализују софтверским задацима који су временски ограничени. Задаци могу бити зависни од приоритета и користити дељене ресурсе [2].

Војна тактика представља научну дисциплину која се бави проучавањем појава, законитости и принципа употребе војних јединица у борбеним дејствима. Она обухвата процесе припреме, организације и командовања трупама пре, током и након борбе. Тактика чини најнижи ниво војног планирања, будући да је усмерена на непосредне

борбене операције појединачних јединица са циљем остваривања краткорочних циљева на бојишту [3]. Најважније у јединицама тактичког нивоа је њихова комуникација (телекомуникационо информациони системи - ТкИ), тј. правовремено добијање и преношење информација о распореду људства и оруђа, како својих тако и о непријатељским јединицама. Унапређење ТкИ система омогућава брз одзив система, високу тачност и прецизност у преносу података и ефикасна и правовремена дејства оруђа.

У овом раду је приказан предлог поступка унапређења постојећег ТкИ система на нивоу батерије коју чине једна мастер станица и 6 потчињених применом Dynamic TDMA врсте рада. Практични део рада, описан у последњем делу, резултат је разматраних варијанти конфигурационе мреже на нивоу батерије применом Dynamic TDMA врсте рада, а ради што бољег разумевања предлога унапређеног ТкИ система. Објашњене су и описане могућности разматране конфигурационе мреже, као и резултати испитивања мреже у лабораторијским условима.

Након краћег увода, у првом поглављу су описани MAC протоколи чије познавање је неопходно за постизање поуздане и ефикасне комуникације између два суседна уређаја који су међусобно повезани. У овом поглављу описана је намена MAC протокола, приказана подела и карактеристике свих врста протокола.

У другом поглављу описан је софтверски радио протокол (СРП), где су објашњени слојеви СРП када користи TDMA протокол, као и архитектура софтвера и платформе за извршење.

Треће поглавље описује SNMP протокол који управља уређајима и на апликативном нивоу користи TCP/IP као транспортни протокол и тиме не зависи од мрежног хардвера. Такође, у поглављу је описана еволуција овог протокола кроз три верзије.

У четвртом поглављу је описана Dynamic TDMA врста рада у GEOMUX, објашњене су његове карактеристике, конфигурација радија и употреба. Ова врста рада треба да омогући боље карактеристике актуелних ТкИ система.

Пето поглавље је посвећено разматрању могућности конфигурације THALES радио уређаја у Dynamic TDMA моду рада. Приказани су и описани различити начини на које је могуће конфигурисати радио мрежу и што боље искористити карактеристике наведене врсте рада.

У шестом поглављу описана је разматрана конфигурациона мрежа ТкИ подсистема која симулира комуникацију између радарског система као мастер станице и 6 против авионских система (потчињене станице), као и примена предложене врсте рада Dynamic TDMA за побољшање карактеристика ТкИ подсистема.

У седмом поглављу, извршена је анализа могућности реализованог ТкИ подсистема и приказани су резултати лабораторијских испитивања разматране конфигурационе мреже.

1. MAC протоколи

Слој везе података је одговоран за пренос података између два чвора. Његове главне функције су контрола везе података и контрола вишеструког приступа.

Контрола везе података је одговорна за поуздан пренос поруке преко комуникационог канала коришћењем техника као што су уоквиравање, контрола грешака и контрола тока. Ако постоји наменска веза између пошиљаоца и примаоца, тада је довољан слој контроле везе података, међутим, ако не постоји наменска веза, више станица може истовремено да приступи каналу. Због тога су потребни вишеструки приступни протоколи да би се смањила колизија и избегло преслушавање. На пример, у учионици пуној ученика, када наставник постави питање и сви ученици (или станице) почну да одговарају истовремено (шаљу податке у исто време), онда се ствара велики хаос (преклапање података или губитак података), тада је посао наставника (протоколи вишеструких приступа) да управља ученицима (станицама) и да их „натера" да одговарају један по један [4].

Постоје комуникациони канали којима може бити повезан већи број станица тако да могу међусобно да комуницирају, као што су радио канали и одређени облик жичних линкова (коаксијални каблови). Два фундаментална начина дељења канала су временско дељење и фреквенцијско (просторно) дељење. Временско дељење се заснива на међусобној координацији свих станица у циљу временске поделе права приступа преносном медијуму. Фреквенцијско дељење се заснива на подели фреквенцијског опсега између станица тако да се искључи интерференција у случају истовремених преноса.

Постоје два приступа временске расподеле која су заступљена у савременим мрежама:

- Временска расподела вишеструког приступа – **TDMA** (енгл. *Time Division Multiple Access*) и
- Компетитивни протоколи.

Код компетитивних протокола станице се међусобно такмиче за приступ медију без претходно утврђеног временског редоследа, који одређује када која тачка може слати податке, или без просторне резервације која гарантује малу или никакву интерференцију. Компетитивни протоколи су прилагођени за мреже података код којих се саобраћај јавља у налетима и са променљивим интезитетом.

Поступци временског и просторног дељења се најчешће реализују у оквиру комуникационог протокола који се назива MAC (енгл. *Media Access Control*) и они регулишу како да више станица приступи додељеном преносном медијуму. Најчешћи пример дељења комуникационог медијума је од стране радио преноса, у који се убрајају мобилне бежичне мреже, бежичне локалне мреже и друге форме радио комуникација. Основно начело комуникационог медијума је избегавање колизије предајника, која се дешава код истовремених преноса. Протокол треба да обезбеди високу искоришћеност, правичност, ограничено кашњење, динамичност и скалабилност.

Висока искоришћеност се огледа у следећем:

- **Капацитет канала** је ограничени ресурс и треба га ефикасно искористити,
- **Идеал**: коришћење 100% капацитета канала за пренос пакета и
- **Губитак**: слободни периоди, периоди колизије...

Искоришћеност коју протокол достигне је дефинисана као количник укупног оствареног протока и капацитета канала и има вредност између 0 и 1. Правичност се огледа у равноправној подели капацитета између захтева корисника. Индекс правичности F дефинисан је на следећи начин:

$$F = \frac{\left(\sum_{i=1}^{N} x_i\right)^2}{N \sum_{i=1}^{N} {x_i}^2},$$

где су N број станица и x_i проток станице i у датом временском интервалу. Индекс правичности F има вредност између $1/N$ (када једна станица преузима сав капацитет) и 1 (идеална правичност, када све станице имају једнак капацитет). Постоје компромиси између искоришћености и правичности.

Ограничено кашњење је значајно за изохроне комуникације (говор и видео) и мора имати горњу границу чекања на успешан пренос. Динамичност и скалабилност омогућује промену броја станица.

Вишеструки протоколи приступа се могу поделити како је приказано на слици 1.

Слика 1. Подела MAC протокола [5]

1.1. Случајни приступ

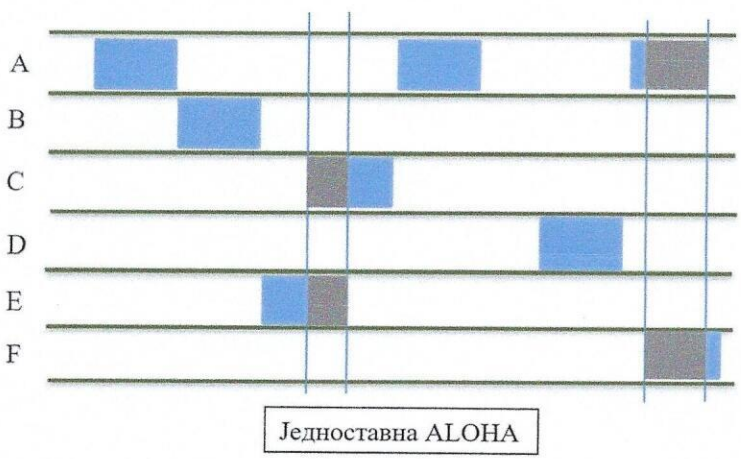
У методи случајног приступа, све станице у мрежи имају једнак приоритет. Одлука о слању фрејма преко линка зависи од његовог стања, да ли је веза заузета или неактивна. Дакле, станица може да пренесе фрејм кад год жели, али пре него што провери стање везе. Протоколи случајног приступа су еволуирали из веома једноставног протокола познатог као ALOHA.

Почетком 1970-их, Универзитет на Хавајима развио је протокол за регулисање преноса података на бежичном LAN-у (енгл. *Local Area Network*) познат као ALOHA. ALOHA протокол има две варијације [5]:

- Једноставна ALOHA (енгл. *Pure Alloha*),
- Слотована ALOHA (енгл. *Slloted Alloha*).

1.1.1. Једноставна ALOHA (енгл. *Pure Alloha*)

Оригинални ALOHA протокол се назива једноставни ALOHA протокол (слика 2). Примењена је стратегија да станица може да пренесе фрејм кад год жели без провере стања везе. Дакле, постоји максимална шанса за колизију, јер друга станица може покушати да пренесе фрејм у исто време. Када се фрејмови са две станице сударе, они се уништавају. Протокол се ослања на потврду пријема. Дакле, када станица емитује фрејм, она очекује потврду за исто. А када не прими потврду пре истека периода, претпоставља да су или фрејм или потврда уништени и поново шаље фрејм. Зна се да до колизије долази када две или више станица покушавају да пошаљу фрејм истовремено. Дакле, чак и ако станице покушају да поново пошаљу фрејм након фиксног времена, фрејмови које шаљу станице ће се поново сударати [5].



Слика 2. Једноставна ALOHA [5]

Дакле, у једноставном ALOHA протоколу, свака станица која дели исту везу чека насумично време пре него што поново пошаље фрејм, да би се избегла колизија.

Време рањивости (дужина времена у којој постоји могућност колизије) за једноставну ALOHA [5] је:

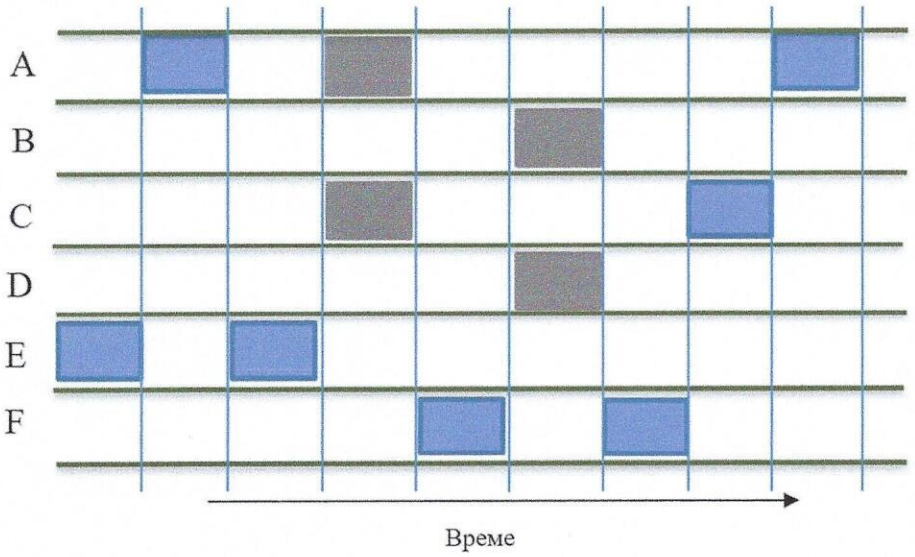
- Рањиво време = $2 \times T_{fr}$, где је T_{fr} време преноса фрејма.

Просечан број успешних преноса за једноставну ALOHA [5] је:

- $S=G*e^{-2G}$, где је G просечан број фрејмова које је генерисао систем током времена преноса једног фрејма.
- Максимални проток S_{max} је за $G = 1/2$, и тада износи 0,184.

1.1.2. Слотована ALOHA (енгл. *Slloted Alloha*)

Слотована ALOHA је развијена да реши проблеме које има једноставна ALOHA. Она дели време на слотове, а ако станица жели да пошаље фрејм на заједнички канал, то може да уради само на почетку новог слота и шаље се само један фрејм по слоту. Ако било која станица није у могућности да постави фрејм на канал на почетку слота, мора да сачека до почетка следећег временског слота. Још увек постоји могућност колизије ако две станице покушају да пошаљу на почетку истог временског слота. Али ипак, број судара који се могу десити је знатно смањен и перформансе постају много боље у поређењу са Једноставном ALOHA.



Слика 3. Слотована ALOHA [5]

На слици 3 је приказан принцип поделе канала на слотове. Станица може започети свој пренос само на почетку слота. Дакле, једини могући услов за колизију је да две или више станица започну пренос у истом слоту. На слици су фрејмови код којих је дошло до коализије означени сивом бојом, у посматраном случају, колизије се јављају између станица A и C, B и D.

Рањиво време одговара T_{fr}, где је T_{fr} време преноса оквира. Успешан пренос за протокол АЛОХА са слотовима износи: $S=G*e^{-G}$, где је G просечан број фрејмова које генерише систем током времена преноса једног оквира. Максимални проток износи S_{max} који се добија за случај када је $G=1$, односно има вредност 0,368 [5].

1.1.3. Вишеструки приступ са ослушкивањем носиоца - CSMA (енгл. *Carrier Sense Multiple Access*)

У методи CSMA, станице иницијално ослушкују заједничку везу пре преноса оквира. Она ради на принципу „ослушните, пре него што пренесете“ [5]. CSMA обезбеђује мање судара, јер је потребно да станица прво детектује медијум (неактиван или заузет) пре него што пренесе податке. Ако је неактиван онда шаље податке, у супротном чека док канал не постане неактиван [4]. Међутим, CSMA само смањује шансе за колизију, али је не елиминише у потпуности. Разлог коализије, односно судара, је кашњење пропагације. Када год станица пошаље фрејм другој станици, потребно је време да први бит стигне до одредишне станице и да га станица прими. Може се десити да одредишна станица ослушне канал и нађе га неактивног, јер први бит послат од пошиљаоца још није примљен. Тада одредишна станица такође почиње да шаље фрејм другим станицама. Тиме ће се, фрејмови од пошиљаоца до одредишта и од одредишта до друге станице сударити и уништити [5].

Технички појам – ***carrier sense*** означава да станица, пре покушаја слања, може да ослушне медијум како би установила да ли је ниво напона или ниво сигнала већи од уобичајеног, када се медијум не користи.

Ако станица установи да је у току пренос неког другог пакета - сматра да је медијум заузет и одлаже слање свог пакета све док станица не установи да је медијум слободан.

Проблем у CSMA је што више станица може скоро истовремено детектовати да је медијум слободан. То ће проузроковати да све оне започну слање пакета скоро истовремено и десиће се колизија, из ових разлога CSMA не може достићи 100% искоришћеност медијума.

Међутим, да би се избегла ова колизија, CSMA је увео неке методе приступа. Ове методе се називају „методама постојаности“. Методе постојаности ће помоћи станици да дели исти медијум кроз одговоре на питања као што су [5]:

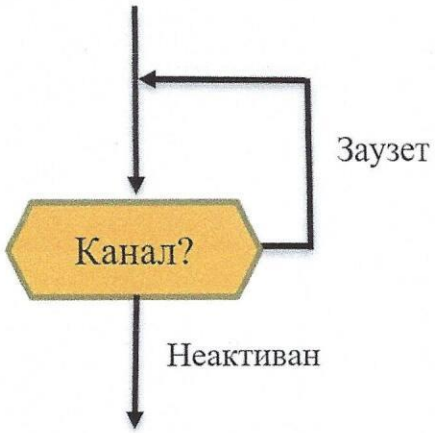
- Шта станица треба да уради ако открије да је канал неактиван?
- Шта станица треба да уради ако утврди да је канал заузет?

Дефинисане су четири методе постојаности [4]:

1. И- Перзистентни метод,
2. Не- Перзистентни метод,
3. П- Перзистентни метод и
4. О- Перзистентни метод.

И- Перзистентни метод

Станица непрекидно детектује канал и чим га нађе у стању мировања, шаље фрејм, због чега је ова метода највише склона колизији (слика 4).



Слика 4. И- Перзистентни метод [5]

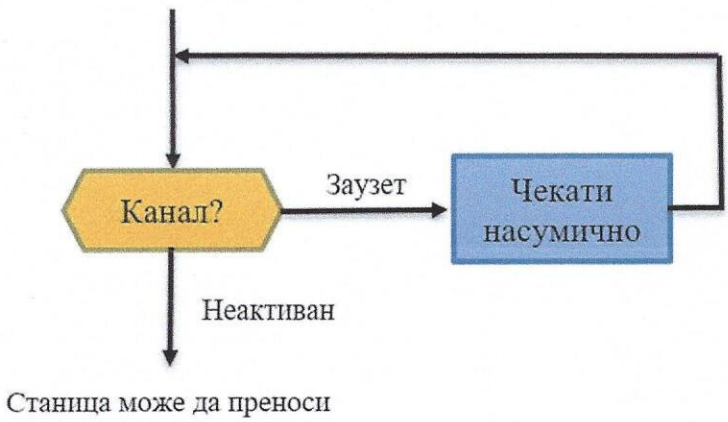
Ако дође до сукоба, чека случајно време и покушава са поновним слањем поруке. Ако је канал заузет, чека да се ослободи.

Успешност слања поруке зависи од времена преноса:

- Колико дуго ће канал након што је примећено да је слободан такав и остати.
- Постоји могућност да нека друга станица започне слање поруке у међувремену.

Не- Перзистентни метод

Станица детектује канал, и ако се нађе заузет канал, чека насумично време и поново проверава канал. Провера се врши док се не пронађе канал у стању мировања. Чим станица примети да је канал неактиван, шаље фрејм. Метод смањује ефикасност мреже, јер се може десити да канал остане неактиван, а да станице и даље покушавају да пошаљу фрејм [5]. Овај метод је приказан на слици 5.



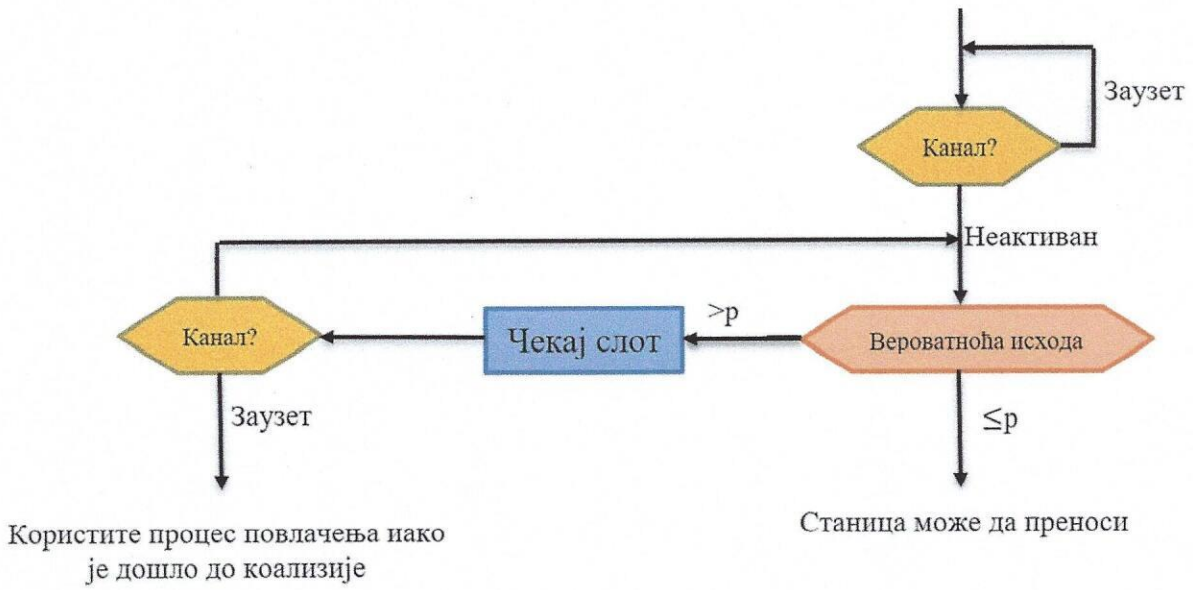
Слика 5. Не- Перзистентни метод [5]

Карактеристике овог метода:

- боље искоришћење,
- већа кашњења него код И-перзистентног CSMA.

П- Перзистентни метод

Мрежа користи п-перзистентни метод где је време подељено на слотове (слика 6). Трајање сваког временског слота мора бити једнако или дуже од максималног времена пропагације.



Слика 6. П- Перзистентни метод [5]

Када станица детектује канал и пронађе га у празном ходу, мора да следи ове кораке [5]:

1. Станица преноси оквир са вероватноћом p.
2. Затим станица чека почетак следећег временског слота са вероватноћом q=1–p. Како почиње следећи временски термин, станица поново проверава.
   а. Ако станица пронађе канал у стању мировања, извршава корак 1.
   б. Ако је канал заузет, станица користи процес повлачења, иако је до колизије дошло [5].

О- Перзистентни метод

У овој методи CSMA надзорни чвор додељује налог за пренос сваком чвору у мрежи. Када је канал у стању мировања, уместо да одмах пошаље податке, канал ће чекати на редослед преноса који им је додељен. Овај режим CSMA дефинише супериорност станице пре преноса података у медијуму. У овом режиму, ако је канал неактиван, све станице ће чекати колико је потребно пре него што почну са преносом података за свој ред [6].

1.1.4. Вишеструки приступ са ослушкивањем носиоца уз откривање колизије – CSMA/CD (енгл. *Carrier Sense Multiple Access with Collision Detection*)

CSMA метода не дефинише шта станица мора да уради ако дође до колизије. CSMA/CD протокол пружа начин за решавање колизије. Станица детектује канал и ако је у стању мировања, шаље фрејм. Након слања фрејма, станица наставља да прати канал да види да ли је дошло до колизије. Ако не дође до колизије, то значи да је пренос био успешан. А ако је дошло до судара, станица шаље ометајући сигнал на мрежу обавештавајући друге станице о судару. Станица затим чека насумично време и поново шаље фрејм [5].

CSMA/CD је метода контроле приступа медијима која се широко користила у раној Ethernet технологији/LAN, када је постојала заједничка топологија магистрале и сваки чвор (рачунар) је био повезан коаксијалним каблом. Посматра се сценарио где постоји '*n*' станица на линку и све чекају да пренесу податке преко тог канала. У овом случају, свака од '*n*' станица жели да приступи линку/каналу да би пренела сопствене податке. Проблем настаје када више од једне станице преноси податке у истом тренутку. У овом случају ће доћи до колизија података са различитих станица. **CSMA/CD** је једна таква техника, где различите станице које прате овај протокол дефинишу заједничке услове и мере детекције колизије којима се обезбеђује ефикасан пренос. Овај протокол одлучује када ће која станица емитовати, тако да подаци стигну до одредишта без оштећења [7].

Како функционише **CSMA/CD**?

- Корак 1: Проверити да ли је пошиљалац спреман за пренос пакета података.
- Корак 2: Проверити да ли је веза за пренос неактивна. Пошиљалац мора да настави да проверава да ли је преносна веза/медијум неактивна. За ово, он непрекидно детектује преносе са других чворова. Пошиљалац шаље лажне податке о линку, ако не прими никакав сигнал колизије, то значи да је веза тренутно неактивна. Ако осети да је носилац слободан и да нема колизија, шаље податке. У супротном, уздржава се од слања података.
- Корак 3: Обавља пренос података и проверава да ли постоји колизија. Пошиљалац преноси своје податке на линку. CSMA/CD не користи систем 'потврде'. Он проверава успешне и неуспешне преносе путем сигнала колизије. Током преноса, ако чвор прими сигнал колизије, пренос се зауставља. Станица затим емитује ометајући сигнал да би обавестила све станице да се догодио сукоб на линку и чека насумичне временске интервале пре него што поново пошаље фрејм. Након неког случајног времена, поново покушава да пренесе податке и понавља претходни процес.
- Корак 4: Ако у пропагацији није откривена колизија, пошиљалац завршава пренос фрејма и ресетује бројаче.

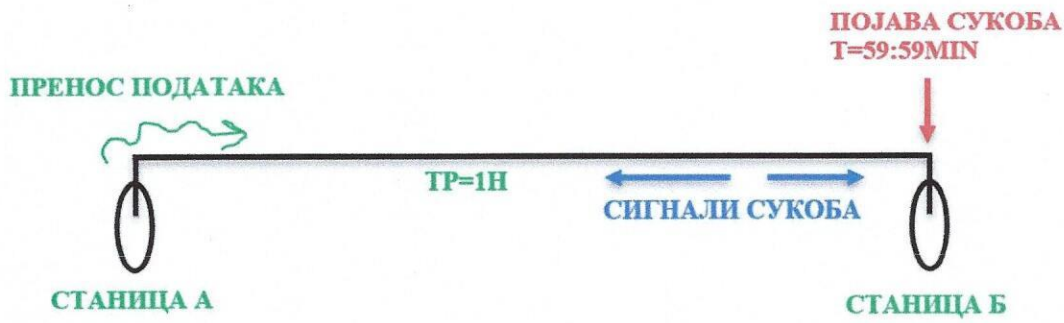
На слици 7 је приказано како станица зна да се њени подаци сударају. Приказане су две станице А и Б, и време простирања *Tp*=1 h. У тренутку *t*=0, станица А преноси своје податке и у тренутку *T*=30 min долази до судара. Након што дође до судара, генерише се сигнал колизије и шаље ка обе станице да их обавести о судару [7].

Слика 7. Приказ сукоба сигнала на половини пута [7]

Пошто се судар догодио на половини пута, сигналу сукоба је потребно 30 минута да стигне и до А и до Б. Према томе у тренутку *t*=1h обе станице примају сигнале судара.

Како да будемо сигурни да су се подаци наше станице сударили? Време преноса (*Tt*) треба да буде веће од времена пропагације (*Tp*) [груба граница], јер се жели да пре него што се пренесе последњи бит података са посматране станице, барем буде обезбеђено да су неки од бита већ стигли на одредиште. Ово осигурава да веза није заузета и да неће доћи до колизија.

На претходном примеру је дата непрецизна граница. Није узето у обзир време које је сигналу коализије потребно да се врати до посматране станице. На слици 8 се разматра најгори сценарио сукоба.



Слика 8. Приказ најгорег сценарија сукоба [7]

У тренутку *t*=0, станица А преноси своје податке, док у тренутку *t*=59:59 min долази до сукоба. Овај судар се дешава непосредно пре него што подаци стигну до станице Б. Сада је сигналу колизије потребно 59:59 минута да поново стигне до станице А. Дакле, станица А прима информације о колизији отприлике након 2 сата, односно након 2**Tp*. Дакле, да би се обезбедила поузданија веза, односно да би се колизија у потпуности открила мора бити испуњен услов: *Tt* >= 2*Tp*. Ово је максимално време

колизије које је систему потребно да открије да ли је колизија настала услед преноса његових сопствених података [7].

Поставља се питање: која би требало да буде минимална дужина пакета за пренос? Време преноса:

$$T_t = L_p/\Delta F,$$

где је L_p дужина пакета и ΔF је пропусни опсег везе [број бита које пошиљалац преноси у секунди]. Заменом изнад, добија се:

$$L_p \geq 2 * T_p * \Delta F \text{ [7].}$$

1.1.5. CSMA/CA (енгл. *Carrier Sense Multiple Access with Collision Avoidance*)

Основна идеја која стоји иза CSMA/CA је да станица буде у стању да прима податке док емитује, да би открила колизију са различитих станица. У жичним мрежама, ако је дошло до колизије, енергија примљеног сигнала се скоро удвостручује, а станица може да осети могућност колизије. У случају бежичних мрежа, највећи део енергије се користи за пренос, а енергија примљеног сигнала се повећава за само 5-10% ако дође до колизије. Због тога је CSMA/CA посебно дизајниран за бежичне мреже [8]. У бежичној мрежи, станице не могу да примете било какве колизије на мрежи јер не постоји физички медијум (кабл). Дакле, уместо да детектује колизију, протокол се фокусира на избегавање судара. Да би се избегла колизија, CSMA/CA протокол ради са три стратегије [5]:

1. **IFS (енгл. *Interframe Space*):** Када станица открије да је канал заузет, поново детектује канал и када станица открије да је канал неактиван, чека временски период који се зове **IFS** време. **IFS** се такође може користити за дефинисање приоритета станице или фрејма, где станице са малим **IFS**-ом имају највиши приоритет [8].
2. ***Contention Window*:** То је количина времена подељена на неколико мини-слотова. Након што сачека **IFS** време, станица поново чека на насумични број мини-слотова. Станица одлучује о броју мини-слотова према бинарној експоненцијалној стратегији повлачења. То значи да након чекања **IFS**-а, станица чека у прозору један мини-слот. Затим станица проверава канал; ако се нађе у стању мировања, онда се преносе подаци. У супротном, ако је заузето, број мини-слотова ће се удвостручити сваки пут након **IFS** -а. Када станица чека у прозору, она проверава канал након завршетка сваког мини-слота [5].
3. ***Acknowledgement* (Потврде):** Позитивне потврде и тајмер могу помоћи да се гарантује успешан пренос оквира. Након слања података, станица поново чека одређени интервал за потврду. Ако је потврда примљена пре истека времена, пренос је успешан. У супротном, поново ће послати податке [5].

Карактеристике CSMA/CA [8]:

- **Carrier Sense**: Уређај слуша канал пре емитовања, како би се уверио да га тренутно не користи други уређај.
- **Вишеструки приступ**: Више уређаја деле исти канал и могу да емитују истовремено.
- **Избегавање судара**: Ако два или више уређаја покушавају да емитују у исто време, долази до колизије. CSMA/CA користи насумичне временске интервале да би се избегла колизија.
- **Потврда (ACK):** Након успешног преноса, пријемни уређај шаље **ACK** да потврди пријем.
- **Праведност**: Протокол осигурава да сви уређаји имају једнак приступ каналу и да ниједан уређај не монополизује тај канал.
- **Бинарно експоненцијално повлачење**: Ако дође до колизије, уређај чека насумични временски период пре него што покуша да поново пошаље. Време одустајања од преноса се експоненцијално повећава са сваким покушајем поновног преноса.
- **Размак између фрејма**: Протокол захтева минимално време између преноса како би канал био празан и смањио вероватноћу колизије.
- **RTS/CTS Handshake**: У неким имплементацијама, RTS (енгл. *Request-To-Send*) и CTS (енгл. *Clear-To-Send*) *handshake* се користи за резервисање канала пре преноса. Ово смањује могућност судара и повећава ефикасност.
- **Квалитет бежичне мреже**: На перформансе CSMA/CA у великој мери утиче квалитет бежичне мреже, као што су јачина сигнала, сметње и загушење мреже.
- **Адаптивно понашање**: CSMA/CA може динамички да прилагоди своје понашање као одговор на промене услова мреже, обезбеђујући ефикасно коришћење канала и избегавајући загушење.

1.2. Динамичко дељење канала

У протоколу контролисаног приступа, станице у мрежи консултују једна другу у циљу идентификације станице која има контролу над каналом. Дакле, станици није дозвољено да емитује све док није овлашћена за емитовање, што елиминише шансе за колизију. У овом случају, дефинисане су методе контролног приступа за ауторизацију станица за пренос [5].

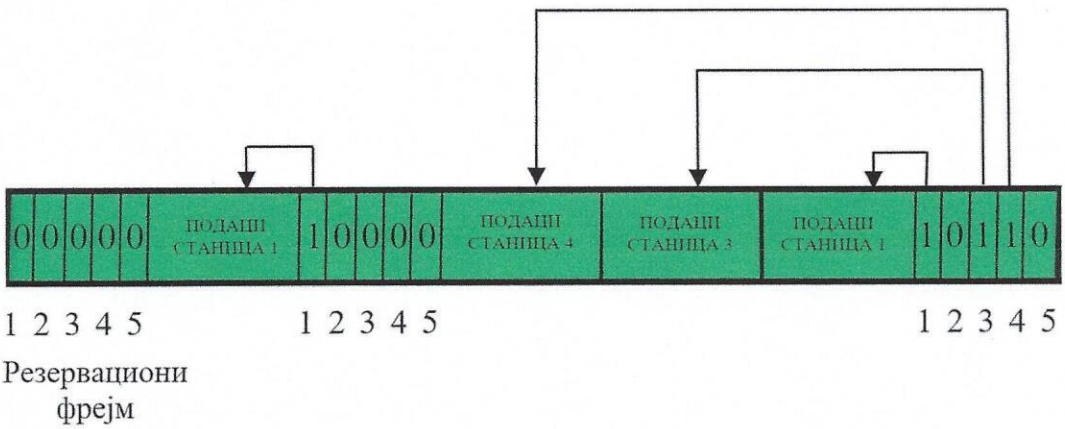
1.2.1. Резервација

У методи резервације, станица треба да изврши резервацију пре слања података. Временска линија има две врсте периода:

- Интервал резервације фиксне временске дужине.
- Период преноса података променљивих оквира.

Ако постоји фрејм за слање, станица преноси 1 бит током слота 1. Ниједна друга станица не сме да емитује током преноса овог слота. Генерално, *i*-та станица може најавити да има фрејм за слање уметањем једног бита у *i*-ти слот. Након провере свих *n* слотова, свака станица зна које станице намеравају да емитују. Станице које су резервисале своје слотове преносе оквире тим редоследом. Након периода преноса података, почиње следећи интервал резервације. Пошто је дефинисан редослед слања, никада неће доћи до судара [9].

На слици 9 је приказана ситуација са пет станица и оквиром за резервацију са пет слотова. У првом интервалу резервисане су само станице 1, 3 и 4. У другом интервалу, само станица 1 је направила резервацију [9].



Слика 9. Приказ оквира резервације [9]

Предности резервације [9]:

- Главна предност резервације су високе и ниске стопе времена приступа подацима дотичног канала које се могу лако предвидети.
- Приоритети се могу подесити да би се обезбедио бржи приступ.
- Предвидиве перформансе мреже: Методе приступа засноване на резервацији могу да обезбеде предвидиве перформансе мреже, што је важно у апликацијама где се кашњење и џитер морају минимизирати, као што је видео или аудио стриминг у реалном времену.
- Смањивање сукоба: Ове методе могу смањити сукобе за мрежне ресурсе, пошто је приступ мрежи унапред додељен на основу захтева за резервацију. На овај начин се може побољшати ефикасност мреже и смањити губитак пакета.
- Подршка за квалитет услуге **QoS** (енгл. *Quality of Service*): Могуће је подржати захтеве **QoS**-а, обезбеђујући различите типове резервација за различите врсте саобраћаја, као што су глас, видео или подаци. Овим приступом се може осигурати да саобраћај високог приоритета има повлашћен третман у односу на саобраћај нижег приоритета.

- Ефикасно коришћење пропусног опсега: Омогућава се ефикасније коришћење доступног пропусног опсега, јер обезбеђују временско и фреквенцијско мултиплексирање различитих захтева за резервацију на истом каналу.
- Подршка за мултимедијалне апликације: Методе приступа засноване на резервацији су погодне за подршку мултимедијалних апликација које захтевају гарантоване мрежне ресурсе, као што су пропусни опсег и кашњење, да би се осигурале перформансе високог квалитета.

1.2.2. Polling (прозивање)

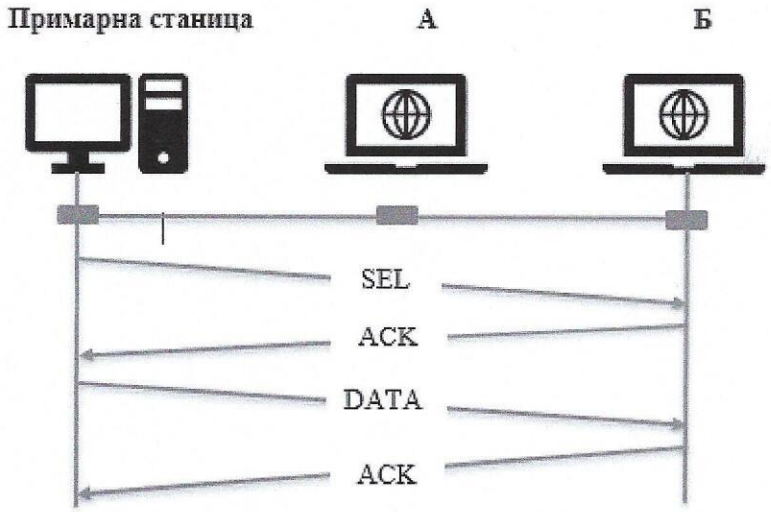
Процес прозивања је сличан прозивци која се изводи на часу. Баш као и наставник, контролор шаље поруку сваком чвору редом. При томе, једна станица делује као примарна станица (контролор), а друге су секундарне станице. Све размене података морају се вршити преко контролора [9].

Дакле, примарна станица одлучује која ће станица користити канал. Када примарна станица жели да пошаље податке, она пита одговарајућу секундарну станицу да ли је спремна за пријем или не преко **функције избора**. Ако примарна станица жели да прими податке, она пита секундарне станице да ли имају нешто да пошаљу преко **функције анкете**. Дакле, само примарна станица покреће комуникацију и има пуну контролу над везом. Ниједна секундарна станица не може сама да покрене комуникацију [5].

Порука коју шаље контролор садржи адресу чвора који се бира за одобравање приступа. Иако сви чворови примају поруку, само чвор на који је адресирана порука одговара на њу и шаље податке ако их има. Ако нема података, обично се враћа порука „одбацивање анкете“ – NAK (енгл. *Negative AcKnowledgement*), негативна потврда. Овде се могу појавити проблеми који се односе на присуство великог броја порука о анкетирању и велику зависност од поузданости контролера [9].

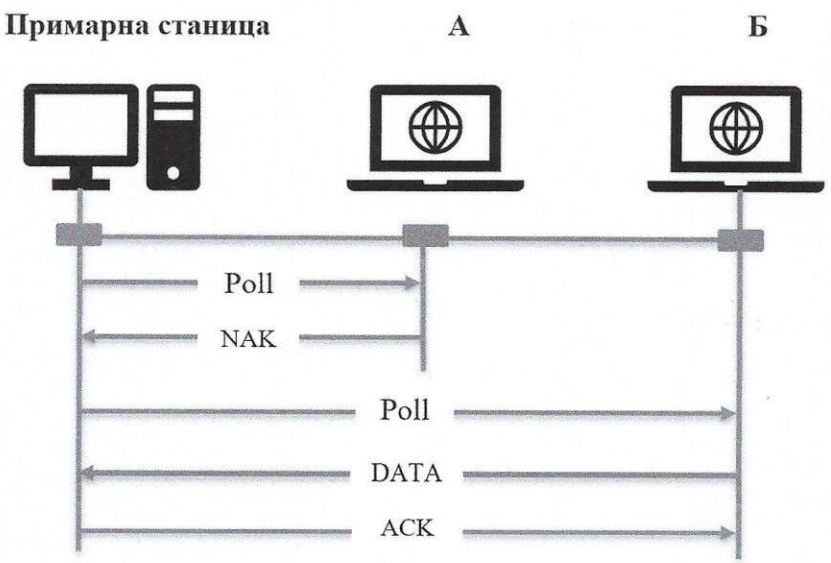
Функција избора: Претпоставиће се да је примарна станица спремна за слање података и да зна да је веза доступна. Оно што треба да се провери јесте да ли је одређена секундарна станица спремна да прими податке. Дакле, упозорава се секундарна станица слањем оквира за одабир – SEL (енгл. *SELect frame*) (Слика 10) [5].

Сада, ако секундарна станица одговори са позитивном потврдом – ACK (енгл. *ACKnowledgement)*, сматра се да је станица спремна да прихвати податке – DATA. Дакле, примарне станице шаљу податке на које опет секундарна станица одговара позитивном потврдом ако је пренос био успешан [5].



Слика 10. Функција избора [5]

Функција анкете: Када примарна станица жели да прими податке, она прозива (енгл. *Poll*) сваку од секундарних станица једну по једну (слика 11). Ако секундарна станица има податке за слање, она одговара на анкету оквиром података - DATA, који примарна станица касније потврђује поруком - ACK, ако је пренос био успешан. У случају да секундарна станица нема шта да пошаље, она ће једноставно одговорити негативном потврдом – NAK [5].



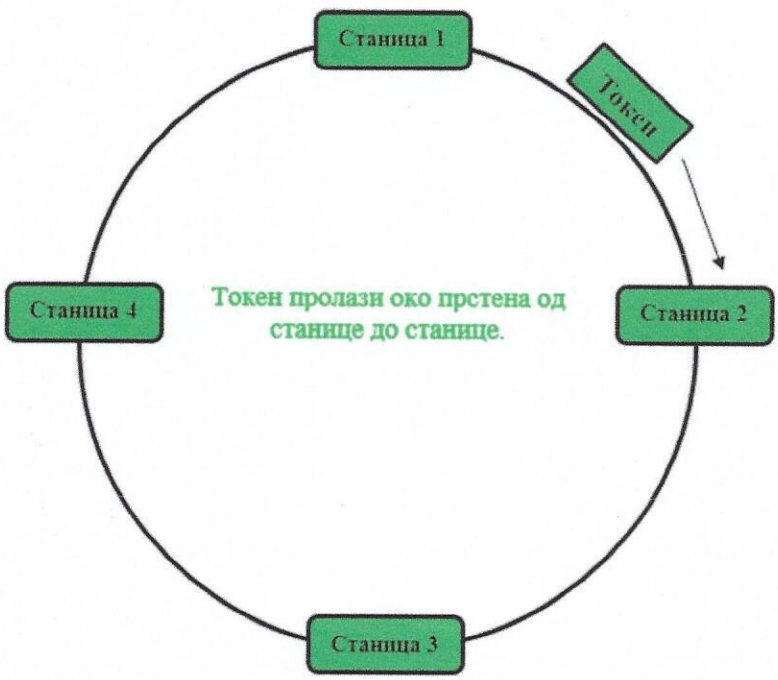
Слика 11. Функција анкете [5]

1.2.3. Прослеђивање токена

У шеми прослеђивања токена, станице су логички повезане једна са другом у облику прстена и приступ станицама је регулисан токенима. Токен је посебан шаблон бита или мала порука, која кружи од једне станице до друге у неком унапред дефинисаном редоследу [9].

У токен рингу, токен се прослеђује са једне станице на другу суседну станицу у прстену, док у случају токен магистрале, свака станица користи магистралу да пошаље токен следећој станици у неком унапред дефинисаном редоследу. У оба случаја, токен представља дозволу за слање. Ако станица има фрејм у реду за пренос када прими токен, она може послати тај фрејм, пре него што проследи токен следећој станици. Ако нема фрејм у реду чекања, она једноставно прослеђује токен [9].

Након слања фрејма, свака станица мора да сачека да свих N станица (укључујући и себе) пошаљу токен својим суседима, а осталих N–1 станица да пошаљу фрејм, ако га имају. Постоје проблеми попут дуплирања токена, губитка токена или уметања нове станице, уклањања станице, што је потребно решити за исправан и поуздан рад ове шеме [9].



Слика 12. Приказ токен ринга [9]

Перформансе токен ринга се могу закључити на основу два параметра [9]:

1. Кашњење је временски интервал између тренутка када је пакет спреман и када је испоручен. Дакле, просечно време (кашњење) потребно да се токен пошаље следећој станици износи a/N, где је N број станица и $a = T_p/T_t$, *при чему су* T_p пропагационо кашњење и T_t кашњење у преносу).

2. Пропусност S је мера успешног преноса саобраћаја, и дефинише се преко:
$S = 1/(1 + a/N)$ за $a<1$ и $S=1/\{a(1 + 1/N)\}$ за $a>1$.

1.3. Статичка подела канала

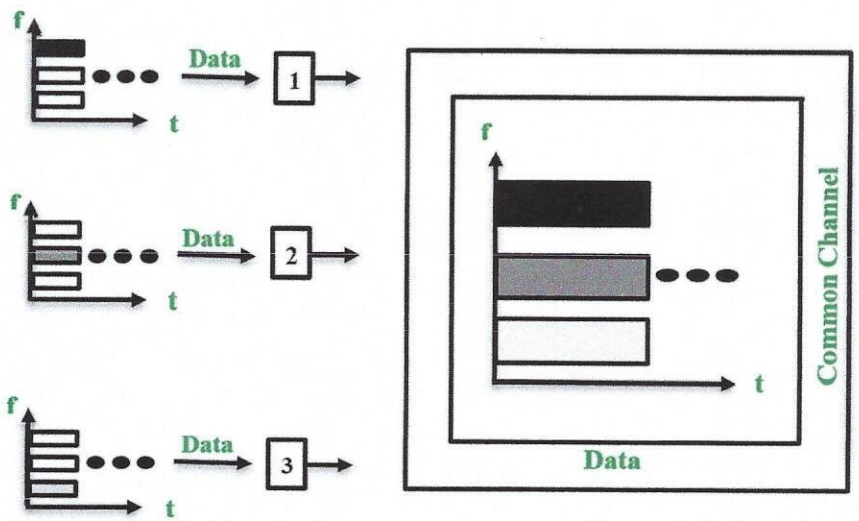
Омогућава да више станица у мрежи приступи каналу поделом доступног пропусног опсега на основу додељене фреквенције, временског слота или кода.

1.3.1. Вишеструки приступ са поделом фреквенције FDMA (енгл. *Frequency Division Multiple Access*)

У методама вишеструког приступа са поделом фреквенција, пропусни опсег канала је подељен на више фреквенцијских опсега. Свакој станици у мрежи је додељен посебан фреквенцијски опсег и овај фреквенцијски опсег је доступан станици све време комуникације (слика 13). Дакле, кад год станица има податке за слање, она једноставно шаље податке на додељеном фреквенцијском опсегу [5].

FDMA се састоји од две главне технике [10]:

1. Пренос са више канала по носиоцу (MCPC – енгл. *Multi-channel-per-carrier*).
2. Пренос са једним каналом по носиоцу (SCPC – енгл. *Single-channel per carrier*).



Слика 13. Приказ FDMA [11]

Техника преноса више канала по носиоцу је технологија испоруке која комбинује више канала у један сателитски носилац и има следеће карактеристике [10]:

- Аналогно мултиплексирање се користило на земаљској станици у ранијим фазама комуникације, при чему се постиже комбиновање великог броја телефонских канала у један сигнал основног опсега и на тај начин се модулише у један РФ носилац.
- Користећи фреквенцијско мултиплексирање (FDM - енгл. *Frequency Division Multiplexing*) телефонски сигнали се могу комбиновати у групу канала, што се ради померањем фреквенције основног опсега на вишу фреквенцију.

- До 1800 телефонских канала у сателиту је мултиплексирано коришћењем FDM, чиме се ствара широки основни опсег који заузима пропусни опсег од 8 MHz.
- Сигнали широког основног опсега се затим модулишу на RF носилац користећи FM (енгл. *Frequency Modulation*), тј. фреквенцијску модулацију.
- За фреквенцијске модулације се користе различити RF носиоци за сваку земаљску станицу.
- Заједнички транспондер за пренос је подељен са различитих земаљских станица за FDM-FM-RF. Ова техника се зове FDM-FM-FDMA.
- Мултиплексирани пренос различитих телефонских канала преко једног РФ носиоца, познат је као МСРС.

Скраћеница FDM-FM-FDMA означава:
- FDM – да су сигнали (нпр. телефонски) мултиплексирани коришћењем фреквенцијске расподеле канала, при чему је за сваки сигнал стандардима одређен подопсег, при чему између подопсега постоји заштитни појас, приближне ширине 4 kHz.
- FM – да се у додељеним подопсезима сваког канала преносе фреквенцијски модулисани сигнали.
- FDMA – да су делови спектра који одговарају транспондерима - додељени различитим корисницима. Сваки корисник прима податак о одређеној делу опсега и подопсега преко којег може да приступи транспондеру.

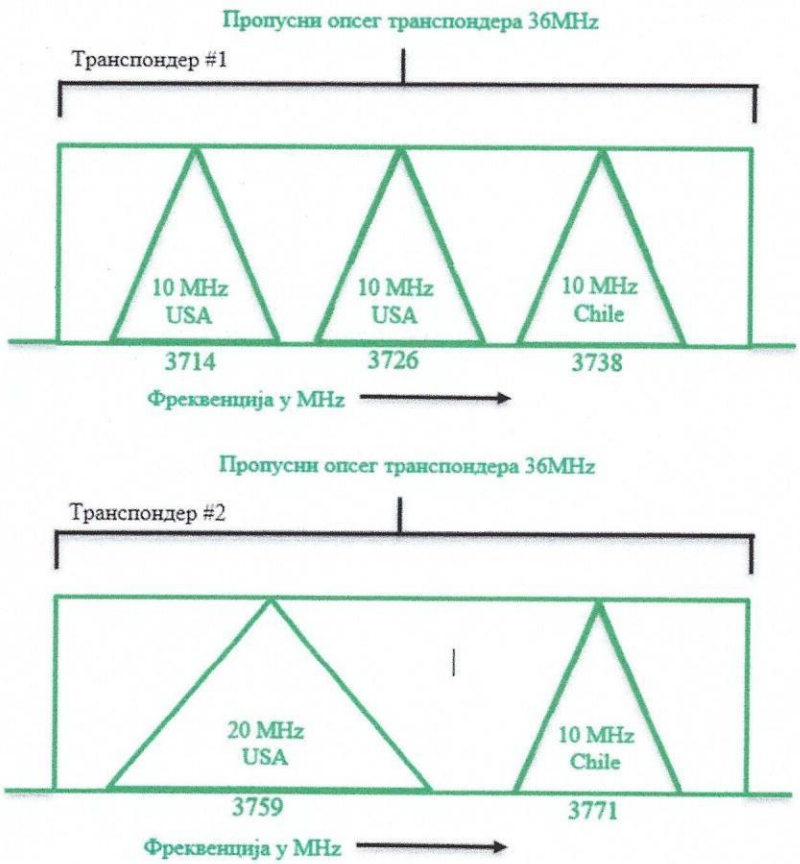
Слика 14 приказује типичан план фиксне доделе FDMA за два транспондера C-опсега. Троуглови представљају RF носиоце са земљом предајне земаљске станице и RF пропусним опсегом приказаним унутар троугла. Сигнали могу бити видео, подаци или гласовни. Приказане фреквенције су за силазну везу са сателита. Троуглови представљају локацију сваког сигнала унутар додељеног пропусног опсега.

Транспондер #1 на слици 14 прима три сигнала различитих земаљских станица, две су у Сједињеним Америчким Државама, а једна је у Чилеу [11].

- Сваки од сигнала има пропусни опсег од 10 MHz.
- Директни, одлазни (енгл. *Uplink*) сигнали са две земаљске станице у Сједињеним Америчким Државама се емитују на носећим фреквенцијама од 5939 MHz и 5951 MHz.
- Директни сигнал са земаљске станице у Чилеу се емитује са носећом фреквенцијом од 5963 MHz.
- Транспондер у повратном линку (енгл. *Downlink*) конвертује сваки примљени сигнал за 2225 MHz на доле дајући фреквенције носиоца повратног линка од 3714 MHz, 3726 MHz и 3738 MHz.
- Све земаљске станице унутар антенског снопа повезане са транспондером #1 могу примити све сигнале које транспондер преноси.
- Свака земаљска станица за пријем може издвојити све сигнале који су намењени тој одређеној земаљској станици.

Транспондер #2 на слици 14 прима два сигнала са различитим пропусним опсегом [11].

- Сигнал ширине 20 MHz долази са земаљске станице у Сједињеним Америчким Државама на фреквенцији носиоца од 5984 MHz.
- Сигнал ширине 10 MHz долази са земаљске станице у Чилеу на фреквенцији носиоца од 5996 MHz.
- Транспондер #2 наниже конвертује ове сигнале за 2225 MHz и преноси их на носећим фреквенцијама од 3759 MHz и 3771 MHz.
- Оба ова сигнала могу примити исте земаљске станице које примају сигнале са транспондера #1.
- Типично, пријемници земаљских станица у C-опсегу имају пропусни опсег пријемног комплета од 500 MHz или 1000 MHz да би омогућили пријем свих носилаца C-опсега.
- Употреба микроталасних филтера за раздвајање транспондера чини приступ фиксног додељивања FDMA веома нефлексибилним.
- Промена фреквенције или пропусног опсега било које земаљске станице која емитује захтева поновно подешавање филтера на неколико земаљских станица за пријем.
- Фиксна додела FDM-FM-FDMA шема илустрованих на слици 6.12 такође чини неефикасним коришћење пропусног опсега транспондера и капацитета сателита.

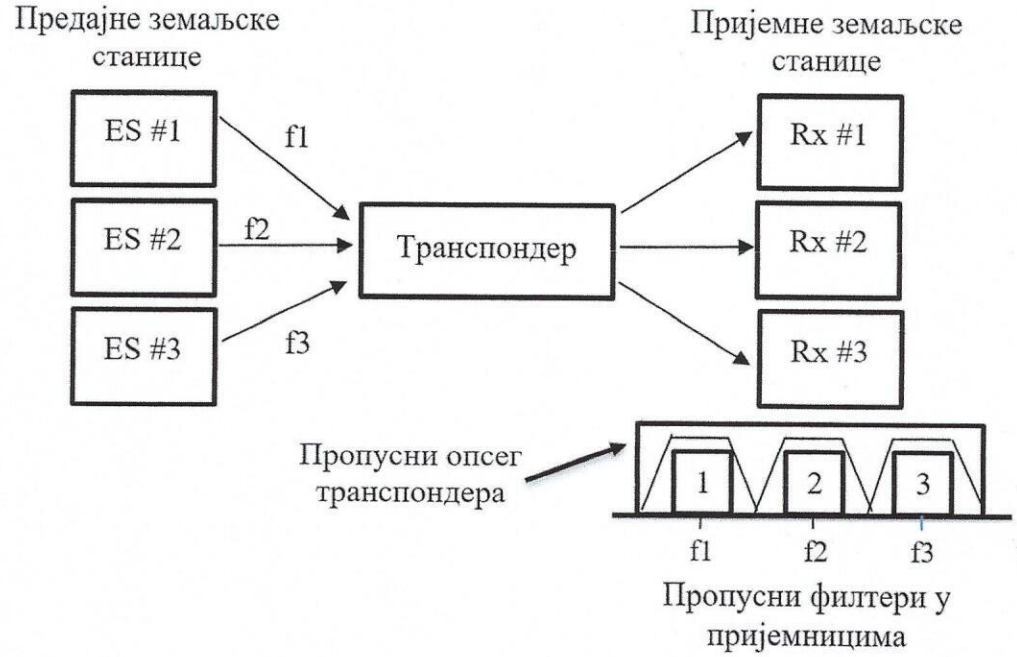


Слика 14. Фреквенцијски план за два транспондера C опсега користећи фиксно додељивање FDMA [11]

FDMA пријемник:

- Свака земаљска станица која ради у FDMA мрежи мора имати посебан IF (енгл. *Intermediate Frequency)* пријемник.
- SCPC системи могу имати веома велики број носилаца у једном транспондеру.

Слика 15 приказује транспондер који ради са FDMA. Три предајне земаљске станице шаљу сигнале на различитим фреквенцијама до једног транспондера на GEO (енгл. *Geostationary Orbit*) сателиту. Транспондер појачава примљене сигнале и поново их емитује ка земаљској станици на фреквенцијама f_1, f_2 и f_3. Све земаљске станице у зони покривања сателита примају сва три сигнала. Три пријемника приказана на слици 15 могу бити на једној земаљској станици или на три одвојене земаљске станице. У оба случаја, BPF (енгл. *Band-Pass Filter*), пропусни филтри са централним фреквенцијама f_1, f_2 и f_3 се користе за одабир жељеног преноса унутар пропусног опсега транспондера. BPF се обично налазе у међуфреквенцијском (IF) делу пријемника да би се поједноставио њихов дизајн.



Слика 15. Илустрација FDMA [11]

Пренос једног канала по носиоцу [10]:

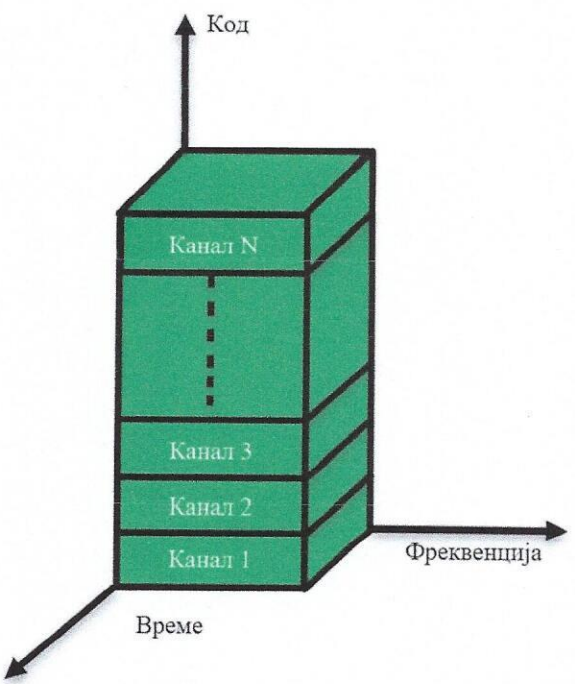
- Када се један сигнал по носиоцу шаље преко земаљске станице, FDMA техника приступа се назива „пренос једног канала по носиоцу".
- Систем у коме се користи велики број малих земаљских станица, на пример мобилних телефона, који приступају преко једног транспондера користећи FDMA, назива се шема вишеструког приступа са фреквенцијском поделом са једним каналом по носиоцу (SCPC-FDMA, енгл. *Single-Channel-Per Carrier Frequency Division Multiple Access*).

- SCPC системи се могу реконфигурисати, што зависи од стања саобраћаја који је акумулиран до тог одређеног система, чинећи га компатибилним са системима за поделу приступа комуникационом каналу у реалном времену.
- Веома важно је истаћи да, када је веза активирана, преноси се само носилац за SCPC канал. На овај начин се смањује потрошња енергије транспондера.

1.3.2. Вишеструки приступ са кодном расподелом CDMA (енгл. *Code Division Multiple Access*)

Методе вишеструког приступа са расподелом кодова омогућавају свим станицама да истовремено преносе податке. Наравно, у овом сценарију постоји могућност судара. Да би се избегла колизија, двема комуникационим станицама је додељен посебан код [5].

Постоји више корисника којима су обезбеђени или додељени различити CDMA кодови и на тај начин корисници могу да приступе целом опсегу фреквенција. Овај метод не ограничава фреквенцијски опсег корисника. Дакле, уз помоћ CDMA, више корисника може да дели исти фреквенцијски опсег без икаквих непотребних сметњи између њих. CDMA користи аналогно-дигиталну конверзију (ADC, енгл. *Analog-to-Digital Conversion*) у комбинацији са технологијом проширеног спектра. Из тог разлога има велику примену у различитим радио-комуникационим технологијама, са акцентом на примену у мобилним комуникацијама [12].



Слика 16. Илустрација CDMA [12]

CDMA технологија је у употреби дуго времена. Дмитриј Агејев је први пут објавио ову тему 1935. године. CDMA је ушла у употребу током Другог светског рата

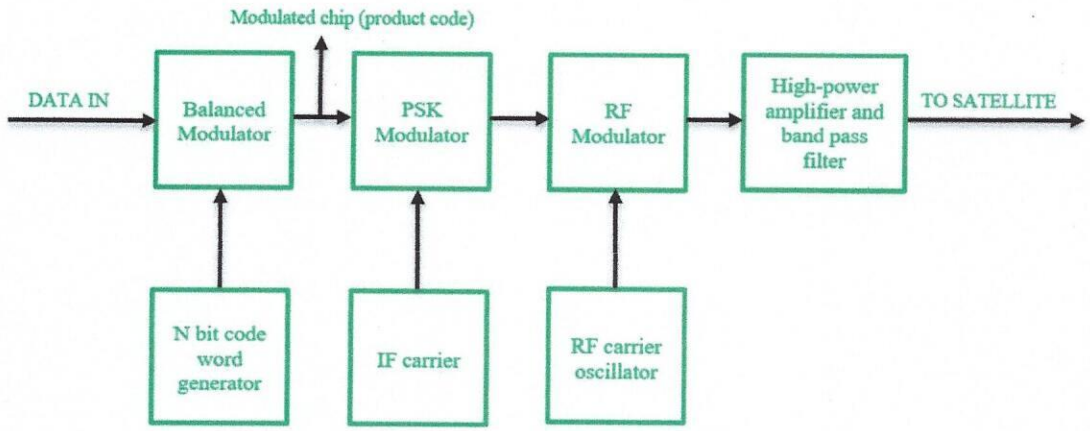
како би се онемогућило ометање преноса. На тај начин је ова технологија добила примену у војсци где се користи за заштиту од ометања, повећање домета, итд. Леонид Купријанович је користио CDMA док је правио модел аутоматског мобилног телефона 1957. године. Коначно, 1993. године, Удружење телекомуникационе индустрије (TIA, енгл. *Telecommunications Industry Association*) је одобрило стандарде за CDMA технологију. У септембру 1998. забележено је 16 милиона претплатника који користе CDMA системе. Према доступним подацима, CDMA подржавају 22 земље [12].

Илустрација CDMA је приказана на слици 16.

Карактеристике CDMA технологије [12]:

- Омогућава да се више корисника повеже у датом тренутку и на тај начин обезбеђује побољшани капацитет преноса података и говора.
- Сви канали у CDMA имају на располагању целокупни спектар.
- CDMA системи користе контролу напајања како би елиминисали сметње и шум, и на тај начин побољшали квалитет мреже.
- CDMA кодира корисничке преносе у различите и јединствене кодове како би осигурао своје сигнале.
- Захваљујући CDMA технологији, у мобилним системима све ћелије могу тако да користе исту фреквенцију.
- CDMA системи имају „меки капацитет". Дакле, не постоји посебно ограничење броја корисника у CDMA систему, али са повећањем броја корисника перформансе система опадају.

Кодер за проширени спектар директне секвенце – DSSS (енгл. *Direct-sequence spread spectrum*) CDMA приказан је на слици 17.

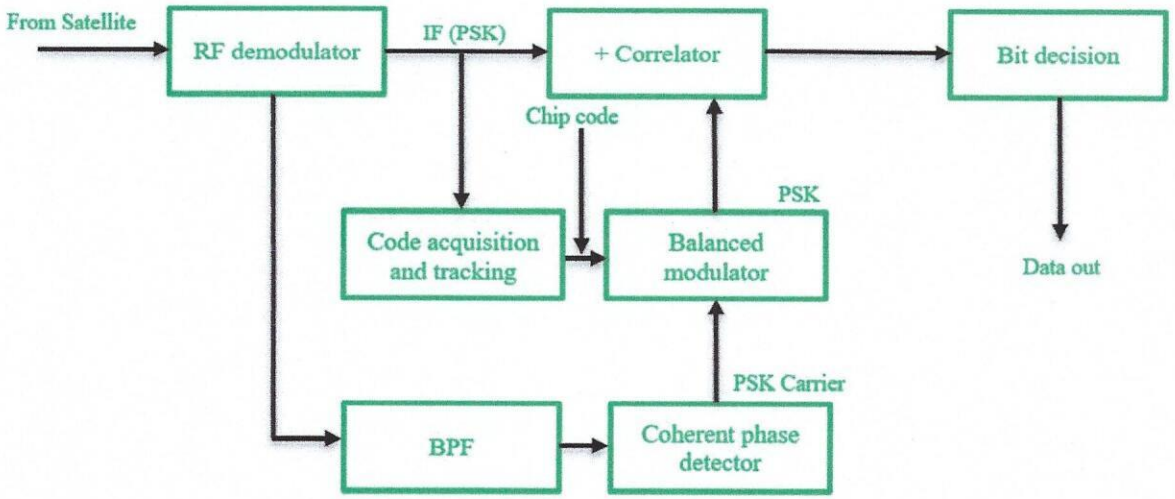


Слика 17. CDMA кодер [13]

Улаз који се обезбеђује CDMA кодеру може бити у облику PCM (енгл. *Pulse Code Modulation*) сигнала, кодираног сигнала говора или може бити дигитални сигнал са рачунара. Множи се са кодном речи дужине *N* бита, која представља јединствени код чипа. Излаз балансног модулатора је модулисани чип (енгл. *chip*), који се преноси променом (PSK модулацијом) фазе таласа IF носиоца константне фреквенције.

Балансни модулатор се понекад назива мултипликатор. Даље, модулисани сигнал се затим претвара у сигнал RF опсега који се даље преноси кроз линију везе. Појачавач велике снаге подиже ниво сигнала на веома високу вредност који се емитује са антене. Други назив за кодер је мултиплексер.

Декодер за технику проширеног спектра са директном секвенцом - DSSS CDMA приказан је на слици 18. Декодер служи за претварање RF сигнала у IF сигнал. Кохерентни PSK носилац је добијен од IF. Пријемник користи шифру чипа и помаже у синхронизацији генератора кода пријемне станице. Излаз PSK демодулатора је IF сигнал, чијом се аквизицијом и праћењем добија опорављени чип. Опорављени чип се затим множи са опорављеним PSK носиоцем, који се добија на излазу фазног детектора, да би се генерисао PSK модулисани сигнал који садржи PSK носилац и код чипа. IF сигнал који је примљен, садржи код чипа, PSK носилац и податке. У корелатору се пореде ова два сигнала, у циљу опоравка оригиналних података. Декодер се такође назива демултиплексером.



Слика 18. CDMA декодер [12]

Предности CDMA технологије [12]:

- Повећани кориснички капацитет је велика предност CDMA јер подржава много више корисника у поређењу са TDMA или FDMA.
- CDMA је безбеднији јер су информације које се преносе испод нивоа шума што отежава продор у спектар.
- CDMA системи имају релативно мање прекида рада него GSM. Дакле, може се користити и у руралним подручјима.
- Цена позива у CDMA је нижа у односу на цену у GSM-у.
- CDMA обезбеђује висок квалитет преноса гласа без присуства буке током позива.
- Проблеми као што су вишеструка путања и ишчезавање се са коришћењем CDMA не јављају.
- CDMA има веома малу потрошњу енергије и убраја се у енергетски ефикасне технологије.

Недостаци CDMA технологије [12]:

- CDMA нема могућност међународног роминга коју обезбеђује GSM.
- Пошто нема ограничења броја корисника, перформансе система опадају са повећањем броја корисника.
- Проблем самоометања јавља се у CDMA системима због губитка ортогоналности.
- Проблем „загађења" канала јавља се у CDMA системима који на тај начин деградирају квалитет преноса говора.

1.3.3.Вишеструки приступ са временском расподелом - TDMA (енгл. *Time Division Multiple Access*)

TDMA протокол је један од MAC протокола, који има широку примену у војсци, као што су NATO тактички Линк16 и Линк22 [13]. У TDMA протоколу, време на каналу је подељено на временске слотове који се не преклапају, а сваком кориснику мреже се додељују одређени слотови за пренос.

TDMA има висок степен праведности, али искоришћеност преносног медијума може бити ниска у случају неуниформног саобраћајног оптерећења станица. Није једноставна за имплементацију у потпуно дистрибуираном систему без централног координатора када број станица динамички варира. Постоје ситуације у којима TDMA добро функционише и такви протоколи се користе у неким мобилним мрежама.

Да би се TDMA протокол реализовао мора да постоји централизовани систем за додељивање ресурса (базна станица у мобилној мрежи) и омогућавање временске синхронизације између станица.

Циљ је остварити равномерну поделу времена на, у општем случају, N станица, на следећи начин:

- Време поделити на једнаке временске интервале – **временске слотове**,
- **Нумерисати их** од 0 са инкрементом 1 и
- Свакој станици доделити **јединствен идентификатор (ID)** у интервалу $[0, N-1]$.

Једноставни TDMA протокол користи следећа правила:

A. Ако је редни број текућег слота t, тада станица са идентификатором $ID = i$ може слати пакет **ако и само ако:**
   - поседује пакет за слање, и ако је
   - $t \bmod N = i$.

B. Ако станица чији је ред да шаље пакет у слоту t нема спреман пакет за слање – тада је тај временски слот „**изгубљен**".

TDMA шема поседује следећа позитивна својства:

- Она је правична – свакој станици је додељено једнако време т.ј., исти број покушаја за слање пакета.

- Протокол спречава могућност колизије у преносу пакета - само једна станица има ексклузивно право слања у једном слоту.
- Услови једноставне имплементације:
    - Број станица фиксан и
    - Постоји централни координатор (мастер станица).

TDMA протокол има и неке недостатке:

- Степен искоришћености зависи од природе самог саобраћаја, ако је саобраћај неизбалансиран – већа је неискоришћеност преносног медијума,
- Ако станице шаљу пакете различите дужине, обезбеђивање коректног рада TDMA шеме је веома захтевно,
- TDMA рад у потпуном дистрибуираном окружењу, без мастер станице, и када се укупан број станица динамички мења је врло сложен и компликован.

Временски слотови стандардног TDMA протокола се додељује различитим мрежним чворовима у фази иницијализације мреже и све време их заузимају чворови. Међутим, када корисник не искористи цео свој слот, неискоришћено време канала се губи. Напротив, када члан има велику количину података за пренос, али његов временски оквир није довољан, мора да сачека следећи круг, чак и ако су други временски интервали увек неактивни. Дакле, искоришћење канала и кашњење су лоши у стандардној TDMA мрежи и постају још лошији када пренос није уједначен или променљив у реалном времену [14].

Табела 1. Разлике између FDMA, TDMA и CDMA

FDMA	**TDMA**	**CDMA**
Дељење пропусног опсега између различитих станица.	Подела времена сателитског транспондера.	Постоји дељење и пропусног опсега и времена између различитих станица.
Није потребна никаква кодна реч.	Није потребна никаква кодна реч.	Кодна реч је неопходна.
Потребни су само заштитни опсези између суседних канала.	Потребно је време чувања суседних слотова.	Неопходни су и заштитни опсези и заштитно време.
Синхронизација није потребна.	Потребна је синхронизација.	Синхронизација није потребна.
Брзина података је ниска.	Брзина података је средња.	Брзина података је висока.
Континуални сигнал.	Пренос података у форми “burst”.	Дигитални сигнал.
Мала флексибилност.	Умерена флексибилност.	Велика флексибилност.

У табели 1 су приказане разлике између FDMA, TDMA и CDMA методе приступа каналу.

Динамички TDMA протоколи су побољшали искоришћеност канала и перформансе кашњења у одређеној мери [15]. Динамички TDMA протоколи могу се класификовати у две категорије на основу различитих начина коришћења слотова: први је TDMA протокол са фиксним величинама слотова и флексибилним расподелама, а други је TDMA протокол са променљивим величинама слотова и нефиксном расподелом. За прву врсту динамичког TDMA протокола, чвор би могао привремено да користи временски слот других чворова, након добијања ауторизације и када има много информација за слање, или би могао да заузме различите слотове у складу са својом величином саобраћаја и приоритетом. Код друге врсте динамичког TDMA протокола, сви чворови динамички прилагођавају величину слота слањем плана додељивања слотова од стране контролног чвора у мрежи. Обе наведене методе користе додатне ресурсе да би постигле циљ: смањење изгубљеног временског интервала, али са ризиком да временски интервали могу бити неусклађени када је пренос неуспешан [14].

2. Софтверски радио протокол – СРП

Радио протокол је скуп правила која треба поштовати како би се комуникација могла успоставити између различитих корисника на истој мрежи. Радио протокол дефинише синтаксу и семантику порука које се размењују између корисника, али и како се комуникација синхронизује између свих корисника. У циљу формирања стек протокола, примењује се више различитих протокола у оквиру истог радија [16].

Софтверски радио протокол (СРП) је софтвер који имплементира комуникациони протокол уграђен у радио станице које су део бежичне мреже. То је софтвер у реалном времену који ради на платформи за контролу и управљање (нпр. оперативни систем и хардвер) и контролише како се физичка опрема радија понаша у смислу преноса/пријема података преко слободног простора. СРП је систем са више временски ограничених задатака који приступају процесорима платформе за извршавање у складу са политиком планирања. Задацима може бити додељен приоритет и синхронизација дељених ресурса [17].

СРП је софтвер који имплементира комуникациони протокол. Већину времена ове радио станице комуницирају у мобилној ад-хок бежичној мрежи. СРП посматра догађаје који се дешавају у мрежи (нпр. појављивање, нестанак станица), преноси/прима поруке и преусмерава их на друге станице када је то потребно. Када се порука прими, СРП може да је пошаље корисничком систему или опреми која може да контролише физички систем у који је СРП уграђен. Претпоставља се да су ефекти недетерминизма у бежичним мрежама, на анализи распореда једне станице, занемарљиви. TDMA је уобичајен комуникациони протокол у СРП-овима [17].

2.1. Радио протоколи засновани на мултиплексирању са временским расподелом

На функционалност радио протокола може утицати метод који радио користи за приступ комуникационом медијуму. TDMA је метод приступа каналу, заснован на мултиплексирању са временском расподелом. Омогућава да више радио станица емитују преко истог комуникационог медијума. У TDMA, време је подељено на неколико временских слотова, који се називају TDMA слотови. На сваком слоту, свака радио станица у мрежи или емитује или прима. Низ слотова је представљен као TDMA оквир [2]. Слика 19 приказује типичан оквир.

TDMA Frame								
S	B	B	T	T	T	T	T	T

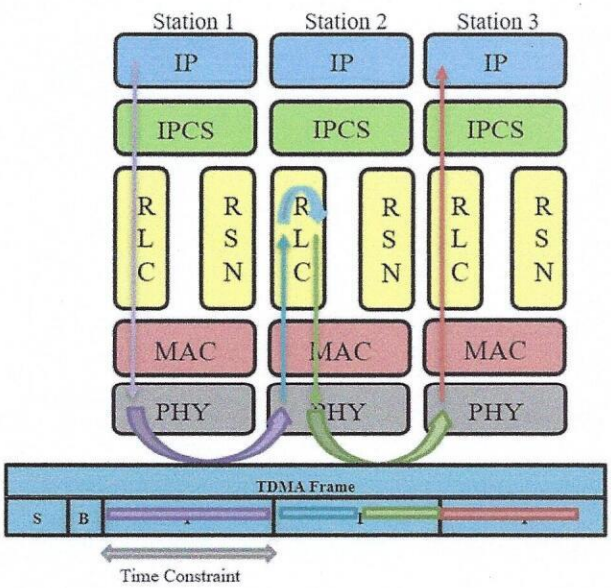
Слика 19. TDMA фрејм[2]

Слотови могу бити различитих типова. На примеру са слике 19, TDMA оквир има три типа слота: S за синхронизацију између станица; B за сигнализацију мреже и T за пренос/пријем података. Слотови различитих типова не морају нужно имати исте карактеристике. Једна од карактеристика слота је његово трајање. Због тога слотови различитих типова немају исто трајање. На пример, на слици 19, трајање B слота је краће од трајања S и T слота. Трајање TDMA оквира је збир трајања његових слотова. Слотови могу бити у режиму преноса (Tx), пријема (Rx) или у мировању.

У Tx слоту, радио станица може да преноси податке. Када радио станица може да емитује у слоту, каже се да је слот додељен станици. TDMA конфигурација дефинише комбинацију слотова, различитих типова, у TDMA оквир. TDMA оквир се понавља након што се заврши. Укупно трајање оквира чини циклус [2].

Када се TDMA користи за приступ комуникационом медијуму, то утиче на функционалности радио протокола и уводи временска ограничења. На пример, операција преузимања пакета података који ће се пренети у Tx слоту је временски ограничена. Метода TDMA је посебан протокол временских токена за комуникацију у реалном времену [18]. Пошто ове методе уводе временска ограничења, задаци који имплементирају систем могу такође имати временска ограничења.

Са системске тачке гледишта, СРП је подељен на неколико слојева. На слици 20 приказан је пример таквих слојева, где се IPCS слој (енгл. *InterProcess Communication System*) повезује са IP стеком корисничког система. Слој RLC (енгл. *Radio Link Control*) управља превођењем између IP пакета и пакета радио протокола. Такође преусмерава долазне пакете ако је потребно (нпр. одредиште примљеног пакета је суседни радио чвор). Слој RSN (енгл. *Relative Sensing Networks*) управља мрежном топологијом и ажурирањима адреса (нпр. појављивање/нестајање адресе суседних станица у мрежи). Када SRP користи TDMA, MAC слој управља TDMA протоколом тако што припрема/прима пакете протокола за/од PHY (енгл. *Physical layer*) слоја који их шаље бежичним путем [17].



Слика 20. Слојеви TDMA СРП [17]

На слици 20, контроле и токови података пролазе кроз различите слојеве. Токови су ограничени TDMA оквиром. TDMA оквир је подељен на неколико временских слотова различитих типова, трајања и режима [17].

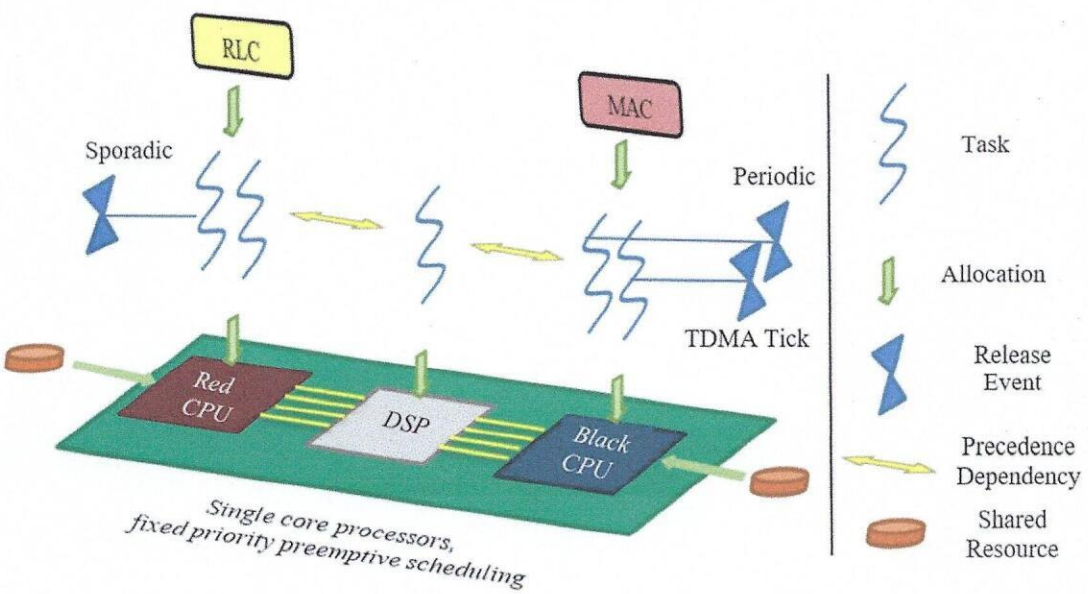
TDMA конфигурација дефинише комбинацију слотова (тип и режим) у TDMA оквиру. TDMA оквир се понавља након што се заврши, са могућношћу измене конфигурације. Претпоставља се да се у TDMA конфигурацији само модови слота мењају из једног TDMA оквира у други [17].

2.2. Архитектура софтвера и платформе за извршавање

У претходном делу је показано како је дизајниран радио протокол. Описана је једна Thales имплементација, названа Софтверски радио протокол. Даље је имплементација описана кроз софтвер и архитектуру платформе за извршавање [2].

Традиционално се функционалности радио протокола имплементирају као наменски хардвер (нпр. ASIC, FPGA). Не постоји истовременост за приступ овим рачунарским ресурсима, стога анализа распореда није неопходна. У случају система развијених у Thales-у, већина функционалности протокола је имплементирана као софтвер који ради на процесору опште намене (General Purpose Processor). Софтверски ентитети су имплементирани од стране неких ентитета у извршној платформи: ОС и хардвер. На слици 21 приказан је пример ових ентитета [2].

Слика 21 приказује неколико протокола (названих RLC и MAC) имплементираних задацима додељеним на процесорима. Систем је вишепроцесорски подељен систем: задаци се додељују процесору и не мењају место. На процесору, задаци се распоређују помоћу политике превентивног планирања FP (енгл. *Fixed Priority*). Приоритети задатака се додељују произвољно према домену стручности [2].



Слика 21. Архитектура за анализу распореда [2]

Они могу имати зависност од приоритета (нпр. комуникација путем семафорске сигнализације и користити заједничке ресурсе. Претпоставља се да су дељени ресурси локални, односно два задатка могу да користе дељени ресурс само ако су додељени истом процесору. Дељени ресурси су заштићени протоколом за приступ ресурсима који спречава неограничен преокрет приоритета за једнопроцесорски систем. Примери таквих протокола за приступ ресурсима су PCP (енгл. *Priority Ceiling Protocol*) и PIP (енгл. *Priority Inheritance Protocol*) [19]. Њихова имплементација се обично може наћи на платформама за извршавање са VxWorks OS. Овај OS је присутан у неким производима које је развио Thales [2].

Одређени задаци могу бити реализовани спорадично. На пример, неки задаци се обично реализују по пристизању IP пакета, што зависи од корисничке апликације. Остали задаци се реализују у унапред одређено време. Ово је случај са задацима протокола MAC. Почетак реализације задатка може бити дефинисан неким периодичним обрасцем или то може бити образац дефинисан TDMA слотовима. Догађаји који се називају TDMA тикови указују на почетак слота и тиме реализацију неких задатака. Задаци који су пуштени на почетку слота такође могу имати времена извршења и рокове који су ограничени слотом [2].

Софтверски радио протокол је систем који покреће време и систем који покреће догађај. Заиста, неке задатке реализују TDMA тикови који указују на почетак слота. Тако се одређени задаци реализују у унапред дефинисаним временима, што је у складу са временски покренутом архитектуром. С друге стране, постоје и задаци који се реализују спорадичним догађајима, на пример по доласку IP пакета. Због зависности од приоритета, задатак се такође може реализовати на основу догађаја који је настао као резултат неког претходног задатка.

3. SNMP протокол (енгл. *Simple Network Management Protocol*)

SNMP је широко распрострањени протокол за прикупљање и организовање информација о уређајима којима управља и за модификацију тих информација ради промене њиховог понашања.

Заснован је да ради на апликативном нивоу користећи TCP/IP као транспортни протокол и тиме не зависи од мрежног хардвера. Сваки уређај у себи садржи хардверски и софтверски део прилагођен преносу података по унапред усаглашеном протоколу. Омогућен је надзор различитих типова уређаја и различитих произвођача. SNMP је еволуирао од верзије V1, преко V2C до C3 у којој је заштита података подигнута на виши ниво [20].

Уређаји који обично подржавају SNMP протокол укључују кабловске модеме, рутере, прекидаче, сервере, радне станице, штампаче итд.

SNMP је веома једноставан протокол. Предвиђене су само две операције, а то су упит и задавање вредности неке променљиве. Проширење протокола је у директној зависности од тога како се дефинише база MIB (енгл. *Management Information Base*). На пример, ако корисник жели да дода нове команде, најпре треба да их дефинише у MIB бази. MIB може да се дефинише као база података у којој се чувају управљани објекти чије се вредности колективно одражавају на актуелно стање мреже [20].

SNMP архитектура се састоји од два кључна елемента Агент и Менаџер. Ради се о клијент-сервер архитектури у којој је агент сервер, а менаџер клијент [20].

- **Агент** је програм који се извршава на сваком управљивом или надзираном чвору мреже и обезбеђује интерфејс ка свим опцијама конфигурације. Ове опције се чувају у MIB бази. Агент има локално знање о управљачким информацијама и преводи их у облик компатибилан са SNMP. Омогућава удаљени приступ опреми за управљање.
- **Менаџер** је софтвер који се извршава на надзорној станици мреже. Улога менаџера је да контактира разне агенте и периодично прозове и прикупи податке. То је клијент страна при надзору и управљању.

SNMP садржи и посебну TRAP (клопка/замка) команду, која омогућава агенту да пошаље поруку у случају дефинисаних, обично критичних догађаја (аларма) [20].

Управљани уређај је мрежни чвор који садржи SNMP агента и који се налази у управљачкој мрежи. Уређај за управљање сакупља и чува управљачке информације и чини их доступнима преко протокола SNMP [20].

Агент извршава апликације које прате и контролишу уређаје за управљање. NMS (енгл. *Network Management System*) осигурава мноштво процесних и меморијских ресурса, опремљених за мрежно управљање. На управљачкој мрежи мора постојати један или више NMS. Уређај за управљање прикупљене информације шаље NMS преко SNMP. Кроз NMS се управља радом свим мрежним елеменатима. Задатак NMS-а је да прикупља све релевантне информације о мрежи (проток информација, стање уређаја, стање система) које затим презентује администраторима. Кроз NMS је могуће приступити уређајима у циљу промене конфигурације. Поред праћења стања и

контроле управљања NMS врши анализу прикупљених података и може да генерише аларм када прикупљени подаци испуне задате услове [20].

Софтвер за надзор користи неки од IP тако да може да контролише уређаје на свим повезаним мрежама, не само на оној на коју је физички повезан. Проблем се појављује ако дође до прекида преносног пута. У том случају, надзор и реконфигурација су немогући. Решење описаног проблема је коришћење резервног преносног пута који ће проследити информације ка неком надзорном центру помоћу стандардног или не стандардног протокола [20].

SNMP протокол се користи за размену информација о управљању између мрежних уређаја. То је један од најчешће коришћених протокола за управљање мрежом. Организације користе SNMP протокол за надгледање и управљање уређајима у локалној мрежи LAN или мрежи ширег подручја VAN (енгл. *Value-Added Network*). Већина мрежних уређаја на тржишту укључује SNMP агенте. Ако не, мрежни администратори могу да инсталирају агенте на неке уређаје.

SNMP порт је крајња тачка SNMP комуникације која идентификује SNMP пренос података. SNMP користи портове 161 и 162 за слање команди и порука. SNMP менаџери комуницирају са SNMP агентима преко одређених SNMP портова. Преноси SNMP порука се дешавају преко корисничког датаграм протокола UDP (енгл. *User Datagram Protocol*). Понекад се користе протоколи TLS (енгл. *Transport Layer Security*) или DTLS (енгл. *Datagram Transport Layer Security*) [21]. Листа бројева портова које наведени протоколи користи за одређене процесе приказана је у табели 2.

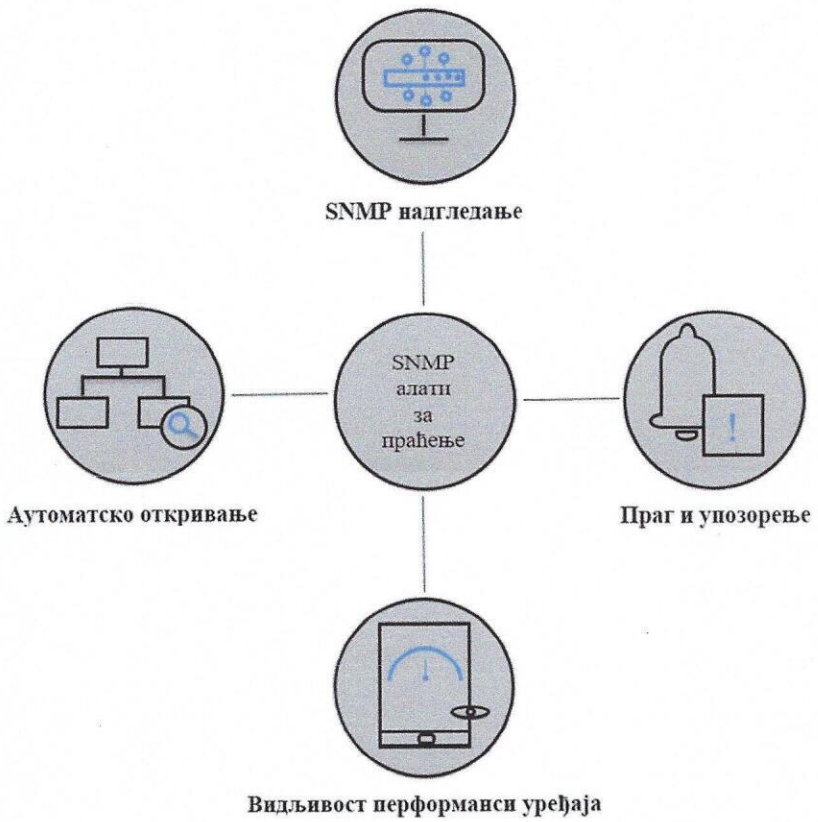
Табела 2. Портови које сваки наведени протоколи користе за одређене процесе [21]

Процес	Протокол	Број порта
Захтев примљен од агента	UDP	161
Комуникација менаџера са агентом	UDP	161
Пријем обавештења од стране менаџера	UDP	162
Генерисање обавештења агента	UDP	Било који доступан
Захтев потврде	TLS/DTLS	10161
Пријем обавештења	TLS/DTLS	10162

Мрежни администратори управљају уређајима у мрежи и додељују или реализују портове, интерфејсе и још много тога да би обезбедили континуирано време рада и мрежне операције без пропусног опсега. Пажљиво праћење SNMP уређаја је значајан део овог процеса. SNMP надгледање захтева од администратора да конфигурише SNMP агента да шаље податке за надгледање SNMP менаџеру. Пошто алат за управљање мрежом брине о надгледању, администратори се могу усредсредити на спровођење корективних мера. На основу увида које пружају ови алати, администратори могу да прате доступност и перформансе SNMP мрежних уређаја и да одреде проблеме како би одржали функционалност мреже. Идеалан алат за праћење SNMP-а прати различите верзије протокола како би помогао IT администраторима да стекну потпуну слику свог мрежног окружења. SNMP софтвер за праћење такође приказује снимљене податке у интуитивним форматима, као што су контролне табле и графикони [21].

SNMP алати за праћење [21] приказани на слици 22 су неопходни за:

- Аутоматско откривање, надгледање и управљање мрежним уређајима.
- Праћење кључне метрике перформанси на нивоу уређаја и интерфејса.
- Добијање потпуне, детаљне видљивости перформанси мрежног уређаја.
- Конфигурисање граничне вредности и генерисање упозорења у случају аномалија.



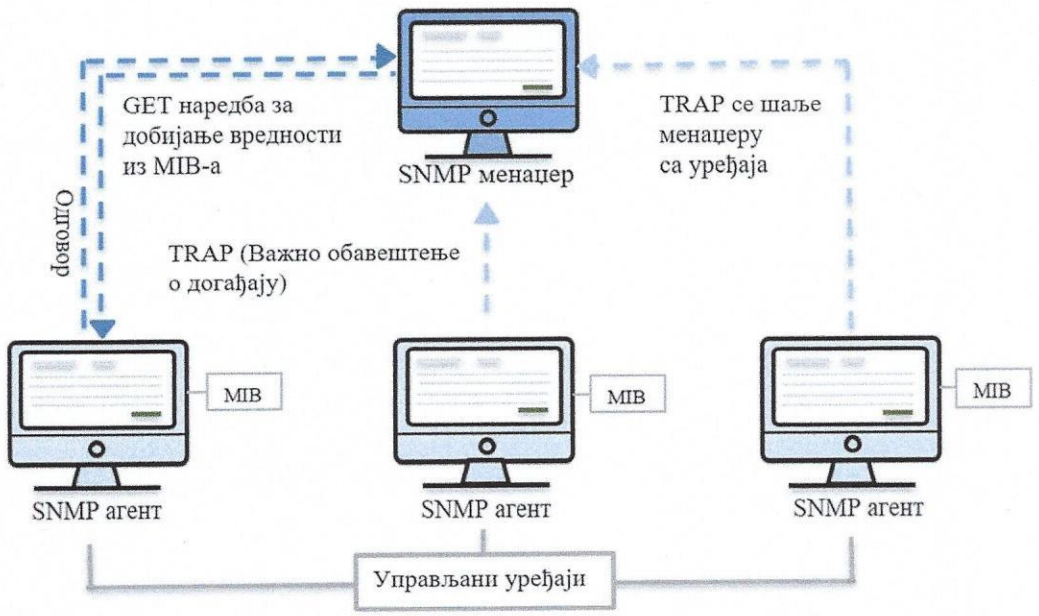
Слика 22. SNMP алати за праћење [17]

SNMP функционише тако што шаље јединице података, такође познате као SNMP GET захтеви, мрежним уређајима који одговарају на SNMP. Све ове комуникације се прате, а алати за праћење мреже користе GET захтеве за преузимање података од SNMP -а. С обзиром да саобраћај долази у мрежу из различитих извора, SNMP протокол комуницира са целом мрежом и уређајима у њој [21].

SNMP је унапред конфигурисан на уређајима, а када се протокол омогући, уређаји ће чувати статистику својих перформанси. Сваки мрежни сервер ће имати базу вишеструких управљачких информација (MIB). Рад SNMP-а се базира на његовим компонентама, при чему свака компонента доприноси управљању ресурсима [21].

3.1. Компоненте SNMP протокола

Компоненте SNMP-а чине: SNMP менаџери, управљани уређаји са SNMP агентом и SNMP MIB који садрже SNMP OID (енгл. *Object Identifiers*) (слика 23).



Слика 23. Компоненте SNMP [21]

SNMP менаџер је централни део система који се користи за праћење SNMP мреже. Такође познат као станица за управљање мрежом NMS (енгл. *Network Management Station*), SNMP менаџер је одговоран за комуникацију с мрежним уређајима који имају имплементиран SNMP агент. Покреће се на рачунару унутар мреже. SNMP менаџер поставља упите агентима, добија одговоре, поставља промењиве и потврђује догађаје од агената [21].

Управљани уређај је SNMP-ом омогућен мрежни ентитет којим управља SNMP менаџер. То су обично рутери, мрежни прекидачи, штампачи или бежични уређаји [21].

SNMP агент је софтверски процес који игра кључну улогу у управљању мрежом. Одговара на SNMP упите од SNMP менаџера како би пружио статус и статистику мрежног чвора. SNMP агент се налази локално у мрежном уређају, одакле агент прикупља, чува и преноси податке за надгледање ка SNMP менаџеру [21].

SNMP MIB представља интегрални део модела управљања мрежом. SNMP MIB је структура која дефинише формат размене информација у SNMP систему. Сваки SNMP агент одржава базу података која описује параметре уређаја којим управља. SNMP менаџер је софтверски систем који користи SNMP за прикупљање података за управљање грешкама, управљање перформансама и планирање капацитета. SNMP менаџер чува прикупљене податке у MIB-у као заједничку базу података између агента и менаџера [21].

MIB-ови се чувају као текстуалне датотеке у одређеном формату који могу разумети уређивачи MIB-а, креатори SNMP агента, алати за управљање мрежом и алати

за симулацију мреже, олакшавајући изградњу, тестирање, имплементацију и операције мреже. Управљани објекти у MIB датотеци називају се идентификаторима објеката OID (енгл. *Object Identifiers*).

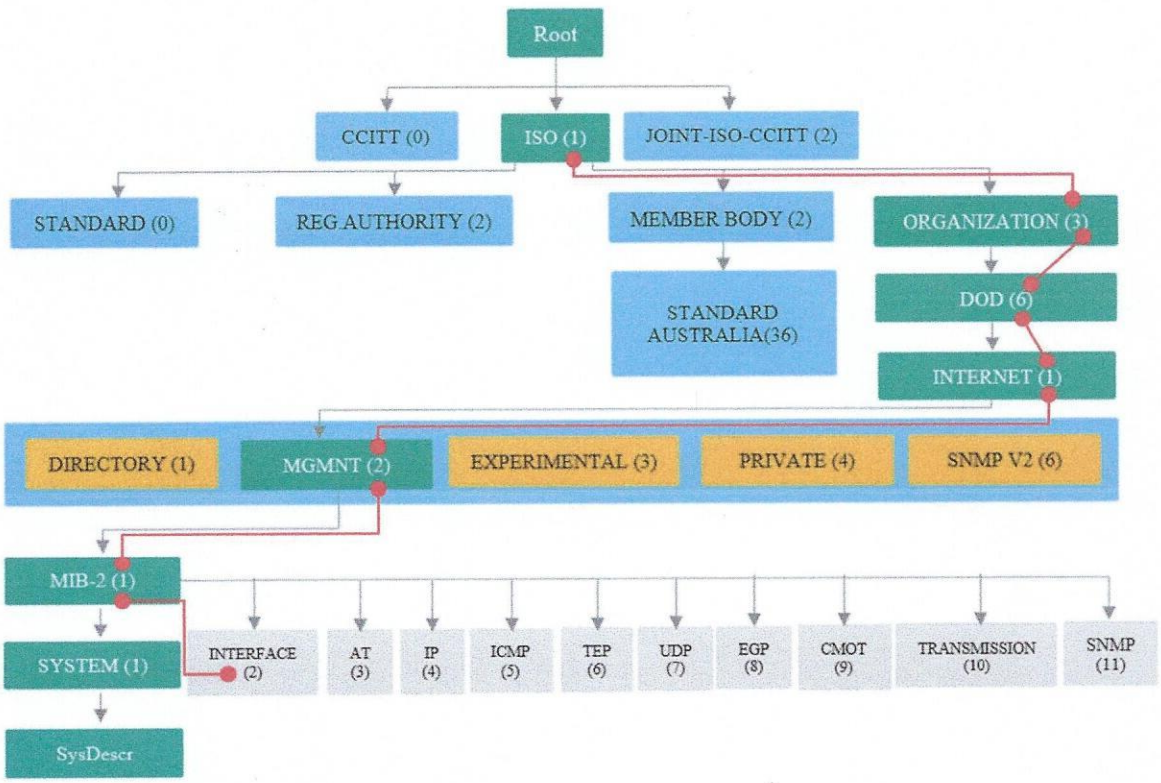
SNMP OID се представљају низом бројева раздвојених тачкама. Постоје две врсте управљаних објеката [21]:

- **Скаларни објекти** дефинисани су једним примерком објекта (тј. може постојати само један резултат).
- **Табеларни објекти** дефинисани су као више повезаних инстанци објеката груписаних у MIB табелама.

MIB-ови хијерархијски организују OID-ове, представљени структуром стабла са индивидуалним идентификаторима променљивих за сваки OID. Ова структура садржи све управљиве карактеристике производа распоређених у њој. Свака грана овог стабла има број и име, а свака тачка је именована по потпуном путу - од врха стабла надоле - који води до те тачке [21].

Сваком чвору хијерархијске структуре MIB-а је додељен идентификатор који се састоји од не-негативног броја и опционог кратког текстуалног описа. Структурни дијаграм MIB-а је приказан на слици 24.

OID је идентификатор који SNMP уређаји користе за управљање сваким ентитетом унутар мреже. База информација о управљању (MIB) је датотека структурирана као стабло, и исти MIB мора бити учитан и у управљане уређаје и у NMS. Произвођачи уређаја обично испоручују потребне MIB датотеке с њиховим производима омогућеним за SNMP [22].



Слика 24. Структурни дијаграм MIB [21]

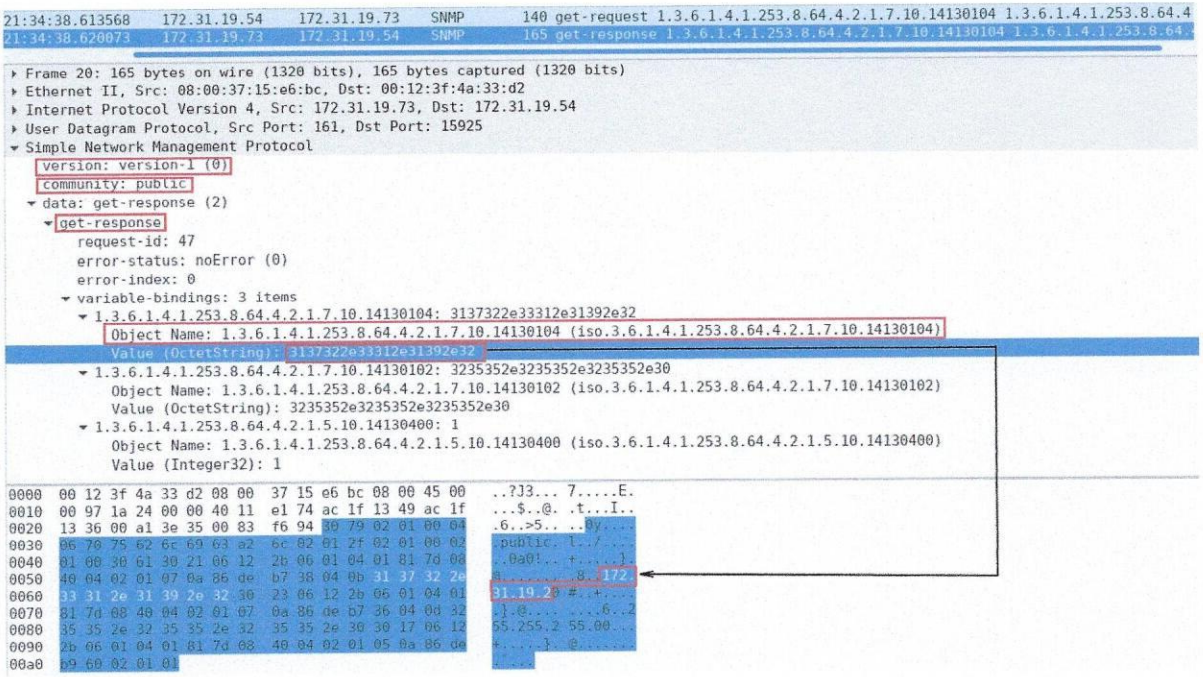
MIB служи као интерфејс између NMS менаџера и агента, те им омогућује међусобну комуникацију. NMS идентификује управљани објект на основу OID-а, чија путања почиње од корена [22].

Сваки управљани објекат представљен је листом чвора и дефинисан је својим именом, синтаксом, режимом приступа, статусом и описом. Такође се може посебно идентификовати својим јединственим положајем унутар стабла. Ова позиција је изражена као серија тачкама раздвојених под-идентификатора који почињу код коренског чвора (ROOT) и завршавају се код под-идентификатора код одређеног објекта лист чвора. На пример, на слици 24 објекат назван интерфејси би био јединствено идентификован низом појединачних под-идентификатора, 1.3.6.1.2.1.2, означено црвеним линијама.

Ако је NMS конфигурисан да надгледа променљиву вредност интерфејса, шаље GET захтев агенту захтевајући вредност OID-а 1.3.6.1.2.1.2. Следећа GET порука може се користити за добијање следећег објекта на листи или таблици унутар агента [22].

За наведени пример, вредности идентификатора представљају следеће [22]:

- 1 – Међународна организација за стандардизацију ISO (енгл. *International Organization for Standardization*),
- 3 – Идентификоване организације према ISO/IEC 6523-2,
- 6 – Министарство одбране САД, DOD (енгл. *Department of Defense*),
- 1 – Интернет протокол,
- 2 – Оперативна група за интернет инжењеринг, IETF (енгл. *Internet Engineering Task Force*),
- 1 – МИБ-2,
- 2 – Интерфејси.



Слика 25. Get Request and Response Messages Exchange [19]

Структура поруке SNMP Get Response је приказана на слици 25. NMS менаџер са IP адресом 172.31.19.54 је послао SNMP Get захтев агенту са IP адресом 172.31.19.73 да преузме вредност промењиве – OID 1.3.6.1.4.1.253.8.64.4.2.1.7.10.14130104. Get Response од агента садржи вредност тражене промењиве – IP адресу 172.31.19.2.

SNMP се може користити и за постављање вредности управљаних објеката коришћењем SNMP SET операције, на пример, како би се интерфејс деактивирао или поставила IP адреса. Табела 3 сумира SNMP функције заједно са верзијама SNMP-а за које су ове функције доступне [22].

Табела 3. SNMP функције

Одлика	**SNMPv1**	**SNMPv2c**	**SNMPv3**
Get	Да	Да	Да
GetNext	Да	Да	Да
Set	Да	Да	Да
GetBulk	Не	Да	Да
Trap	Да	Да	Да
Inform	Не	Да	Да
Community strings	Да	Не	Не
User-based security	Не	Не	Да
Message authentication	Не	Не	Да
Message encryption	Не	Не	Да

SNMP је еволуирао у три верзије: SNMPv1, SNMPv2c и SNMPv3. Све SNMP поруке се преносе преко UDP, а свака верзија подржава GET, GetNext и Set SNMP операције [22].

3.1.1. SNMPv1

Оригинална верзија SNMP-а, позната као SNMPv1, има критичну сигурност и ограничене перформансе.

SNMPv1 пружа аутентификацију, засновану на лозинки (*community string*). Лозинка се шаље као обичан текст између NMS менаџера и агената. Стога, управљани уређај је рањив на неовлашћене кориснике који лако могу реконфигурисати уређај, посебно ако се IP листе за контролу приступа не примењују [22].

Подаци SNMPv1 и SNMPv2c који се размењују између NMS администратора и агената нису крипто заштићени. На пример, *community string* у GET одговору приказаном на слици 25 је "public" [22].

Што се тиче перформанси SNMPv1 протокола, он има ограничен скуп трансакција на GET, SET, и Traps појединачних објеката у MIB-у. Стога, велики сетови информација захтевају неколико трансакција да би се преузео ред информација [22].

3.1.2. SNMPv2c

SNMPv2c је наследник оригиналног SNMPv1. Стандардни MIB2 *integer* је дугачак 32 бита у случају SNMPv1. SNMPv2 дефинише нови *integer* који је дугачак 64 бита. Нови 64-битни бројач може боље управљати високобрзинским интерфејсима јер 32-битни бројачи не пружају довољно капацитета и морају брзо да се упакују. Ово повећава саобраћај у мрежи и негативно утиче на искоришћење процесора како агента тако и менаџера NMS-а [22].

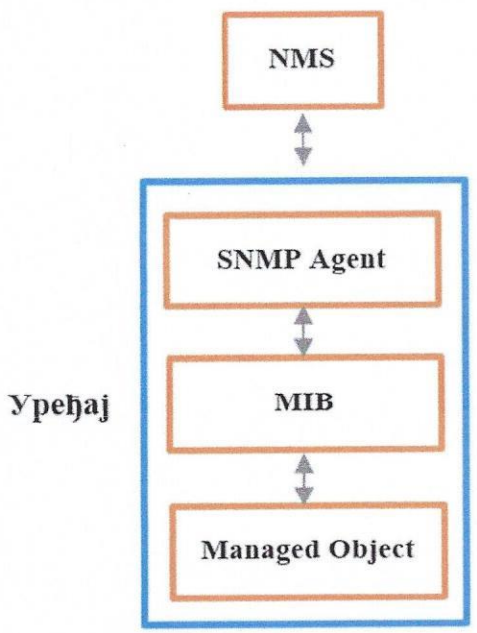
SNMPv2c такође побољшава перформансе SNMPv1 уводећи операцију Get Bulk Requests. Ако менаџер NMS-а жели да преузме велику количину података, он шаље GetBulk поруку агенту уместо Get захтева. Операција GetBulk пружа вредности за све промењиве на листи и много је ефикаснија од слања понављајућих GetNext команди [22].

SNMPv2c уводи нови тип SNMP комуникације - SNMP Inform захтев. Типично, SNMP Inform се користи за комуникацију менаџер-менаџер ради потврде пријема обавештења. Пакет захтева SNMP Inform ће се слати континуирано док менаџер који шаље SNMP не прими SNMP потврду [22].

Обе верзије протокола SNMPv2c и SNMPv1 користе једноставну аутентификацију која се ослања на имена заједнице.

3.1.3.SNMPv3

SNMPv3 је најновији SNMP протокол који решава сигурносне проблеме уведене старијим верзијама SNMP-а. SNMPv3 пружа интегритет поруке, аутентификацију и енкрипцију имплементирањем SNMP View, SNMP Group и SNMP User [22].



Слика 26. Структура MIB [22]

SNMP View дефинише шта одређени корисник SNMPv3 може видети. На пример, могуће је конфигурисати да корисник има приступ само за приказ индекса интерфејса, OID 1.3.6.1.2.1.2 и све што је испод тога. За креирање свих приступа View-а потребно је специфицирати име ISO. MIB има структуру стабла тако да је доступно све што је испод ISO (Слика 26) [22].

SNMP Group је повезан са SNMP View и дефинише тип приступа – само читање или читање/писање. Такође дефинише тип сигурности, који је активан приликом интеракције са уређајем [22]. Типови SNMP Group:

- **noauth** – ни аутентификација ни шифровање,
- **auth** – само аутентификација, без шифровања,
- **priv** – аутентификација и шифровање.

SNMP User је додат групи са нивоом аутентификације и енкрипције. Сигурносни модел мора одговарати групи, нпр. **priv**, тип хеша за лозинку (нпр. SHA - *Secure Hashing Algorithm*), лозинка, алгоритам за енкрипцију (нпр. AES - *Advanced Encryption Standard*) и заједничка тајна за генерисање кључева за енкрипцију [22].

Сигурносни модели SNMPv3 углавном долазе у две форме: аутентификација и шифровање [23].

Аутентификација се користи како би се осигурало да су замке прочитане само од стране намерног примаоца. Како се поруке стварају, добијају посебан кључ заснован на EngineID јединици. Кључ се дели са предвиђеним примаоцем и користи се за примање поруке [23].

Шифровањем се обезбеђује приватност поруке SNMP-а како би се осигурало да је не могу читати неовлашћени корисници. Све пресретнуте клопке ће бити допуњене искривљеним карактерима и биће нечитљиве. Приватност је посебно корисна у апликацијама где SNMP поруке морају бити прослеђене преко Интернета [23].

4. Специфична конфигурација за коришћење Dynamic TDMA у GEOMUX

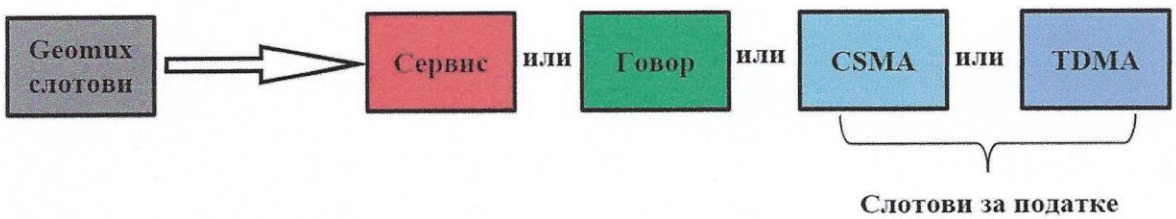
Dynamic TDMA омогућава доделу слотова под истим условима, што значи да је сваком радију дозвољено да користи било који TDMA слот у глобалном циклусу. Идентификатор слота за коришћење обезбеђује екстерна апликација (без аутоматске употребе слота). Доделом слотова динамички управља екстерна апликација (која се налази у систему, ван радија). У исто време је употребљив само један TDMA режим: или статички TDMA или динамички TDMA. [redacted]

Основне карактеристике динамичког TDMA:

- извршава се само на једном наменском каналу или на највише три различита канала,
- може се конфигурисати коришћењем SNMP-а и управља се коришћењем наменске TCP поруке,
- услуга са једним скоком – пренос се мора извршити на нивоу апликације ако је потребно,
- омогућава рад преко великог броја радија,

[redacted]

GEOMUX таласни оквир се састоји од говорних слотова, сервисних слотова и слотова за податке (слика 27). Слотови за податке чине CSMA и TDMA слотови. Однос између ових слотова је подесив.



Слика 27. GEOMUX типови слотова

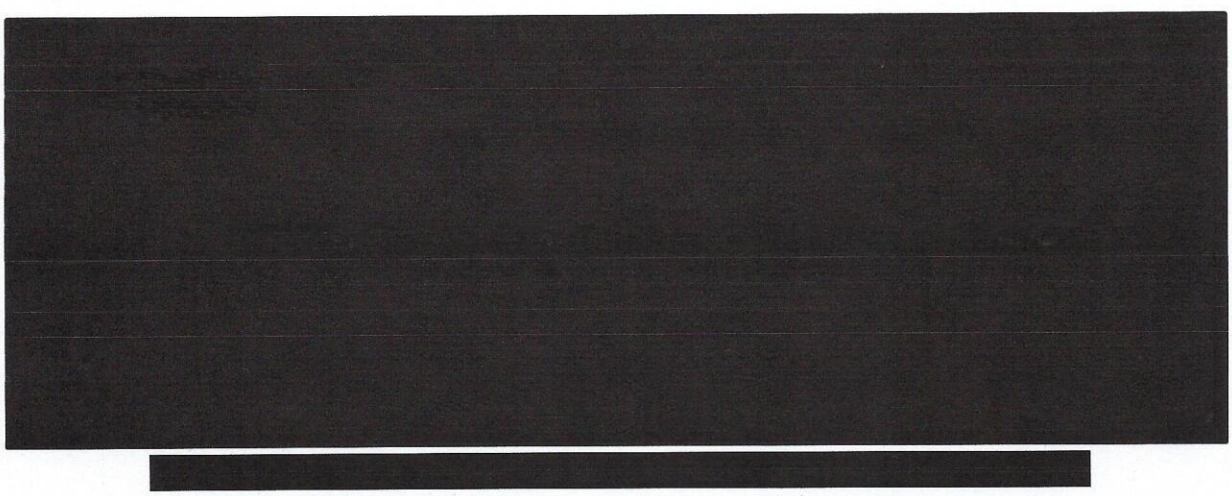
Постоје два типа GEOMUX врсте рада, Static TDMA и Dynamic TDMA.

Static TDMA:

- Омогућава додељивање једног специфичног TDMA слота по радију, у глобалном TDMA циклусу. Сваки радио аутоматски користи свој специфични додељени TDMA слот за слање података.
- Конфигурација TDMA шеме додељивања слотова се врши пре мисије.

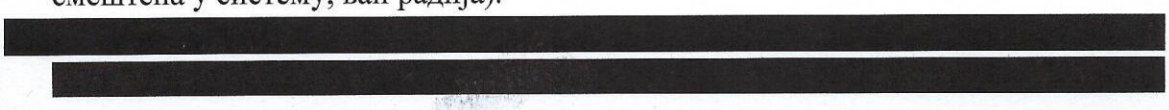
[redacted]

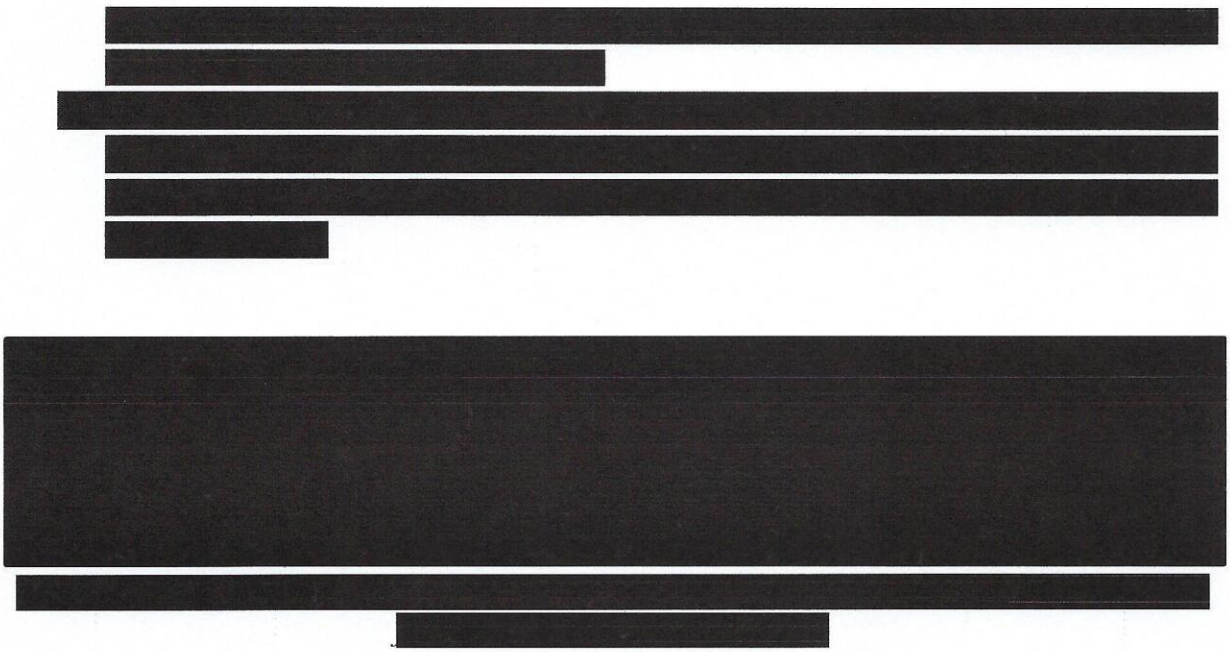
- Static TDMA услуга не захтева доделу свих слотова података за TDMA слотове. CSMA слотови се и даље могу користити (слика 28).
- CSMA користи време мировања. Овај протокол обезбеђује коегзистенцију између корисника когнитивног радија и примарног корисника прилагођавањем снаге преноса и брзине когнитивне радио мреже. Ако је генерисан пакет за CSMA слот и ако је канал неактиван пакет ће одмах бити пренет, ако је канал заузет корисник се повлачи и поново ослушкује канал све док не постане неактиван. Код TDMA протокола пакети се преносе тек када на ред стигну додељени временски слотови. У окружењу бежичних комуникација, број пакета који се могу послати у временском слоту зависи од броја баферованих пакета и стања канала. Може се очекивати да ће у неком временском слоту број послатих пакета бити мали јер је или број баферованих пакета мали или је стање канала лоше. У том смислу, такви временски слотови се не користе ефикасно и бежични ресурс је неефикасно потрошен. Секундарни корисници могу искористити изгубљени бежични ресурс ако се пажљиво дизајнира TDMA шема распореда за примарну мрежу. TDMA ће проценити перформансе примарног корисничког система са једнофреквентним каналом. TDMA је шема вишеструког приступа без сукоба која користи централни ентитет (нпр. базну станицу) за доделу капацитета појединачним корисницима.



Dynamic TDMA:

- Дозвољава доделу слотова под истим условима, што значи да је сваком радију дозвољено да користи било који TDMA слот у глобалном циклусу. Идентификатор слота за коришћење обезбеђује екстерна апликација (без аутоматске употребе слота).
- Нема статичке доделе било ког специфичног идентификатора TDMA слота, пре мисије. Доделом слотова динамички управља екстерна апликација (која је смештена у систему, ван радија).





4.1. Општи принципи

Функција Dynamic TDMA обезбеђује слотове за податке у опсегу који су намењени за употребу TDMA.

Главне карактеристике су:

- Временска скала:
- За Dynamic TDMA HD потребно је да сваки GEOMUX слот за податке буде TDMA слот (дакле, периодичност TDMA слотова је 4 слота на сваких 900 ms).
- За Dynamic TDMA без слотова HD капацитета, периодичност TDMA слотова се може конфигурисати између 1 и 4 слота на сваких 900 ms (Табела 4).

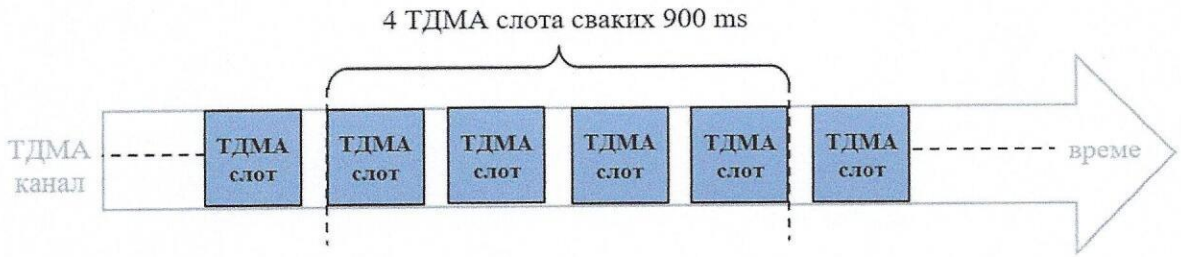
Табела 4. Број TDMA слотова у зависности од TDMA односа

TDMA однос	Број TDMA слотова у GEOMUX фрејму (900ms)
100%	4
75%	3
50%	2
25%	1

- Фреквенцијска скала:
- TDMA слотови моду да емитују/примају податке у фреквенцијском скоку.
- Образац фреквенцијског скакања зависи од канала који се користи за пренос/пријем TDMA слотова.
- Идентификација слотова:
- Слотови се идентификују бројем који почиње од 1 до конфигурабилне величине циклуса.

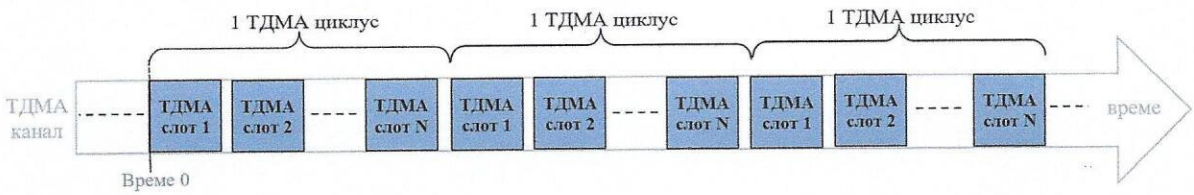
– Радио аутоматски израчунава идентификатор тренутног TDMA слота, на основу величине TDMA циклуса и тренутног времена.

[redacted]



Слика 30. Временска карактеристика Dynamic TDMA

На слици 30 је приказана временска карактеристика Dynamic TDMA врсте рада, где је TDMA однос постављен на 100%. На слици се види један фрејм трајања 900 ms, који се састоји од 4 TDMA слота. Зависно од TDMA конфигурације, један TDMA циклус се састоји од *N* слотова, који се понављају као што је приказано на слици 31.



Слика 31. Dynamic TDMA циклус

4.2. Конфигурација радија

Комбинација свих могућих карактеристика TDMA канала даје велики број могућности. Ради лакшег коришћења, Dynamic TDMA се конфигурише на сваком радију дефинисањем две TDMA конфигурације: примарне и алтернативне конфигурације (табела 5).

За сваку TDMA конфигурацију се дефинише:

[redacted]

– Један канал (за избор између седам унапред подешених канала меморисаних у радију).

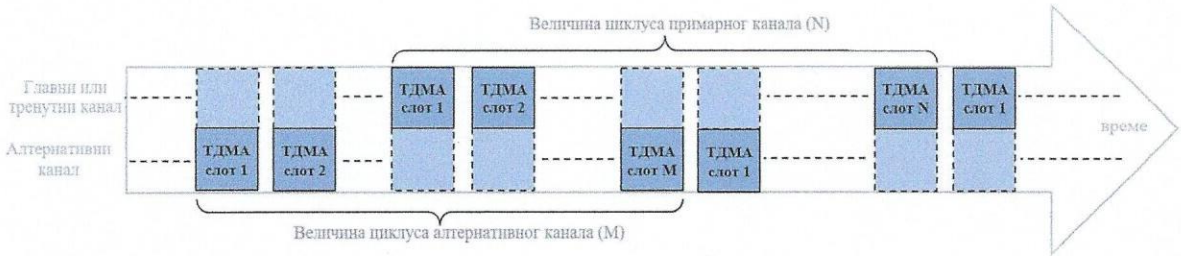
Табела 5. Приказ две конфигурације радио уређаја

	Примарна конфигурација	Алтернативна конфигурација
Величина циклуса	*N*	*M*
Капацитет слота	C1	C2
Канал	G1	G2

За примарну конфигурацију, доступна су два канала:

- „главни канал“, који је у конфигурацији дефинисан параметром G1;
- „тренутни канал“ који је физички канал синхронизације.

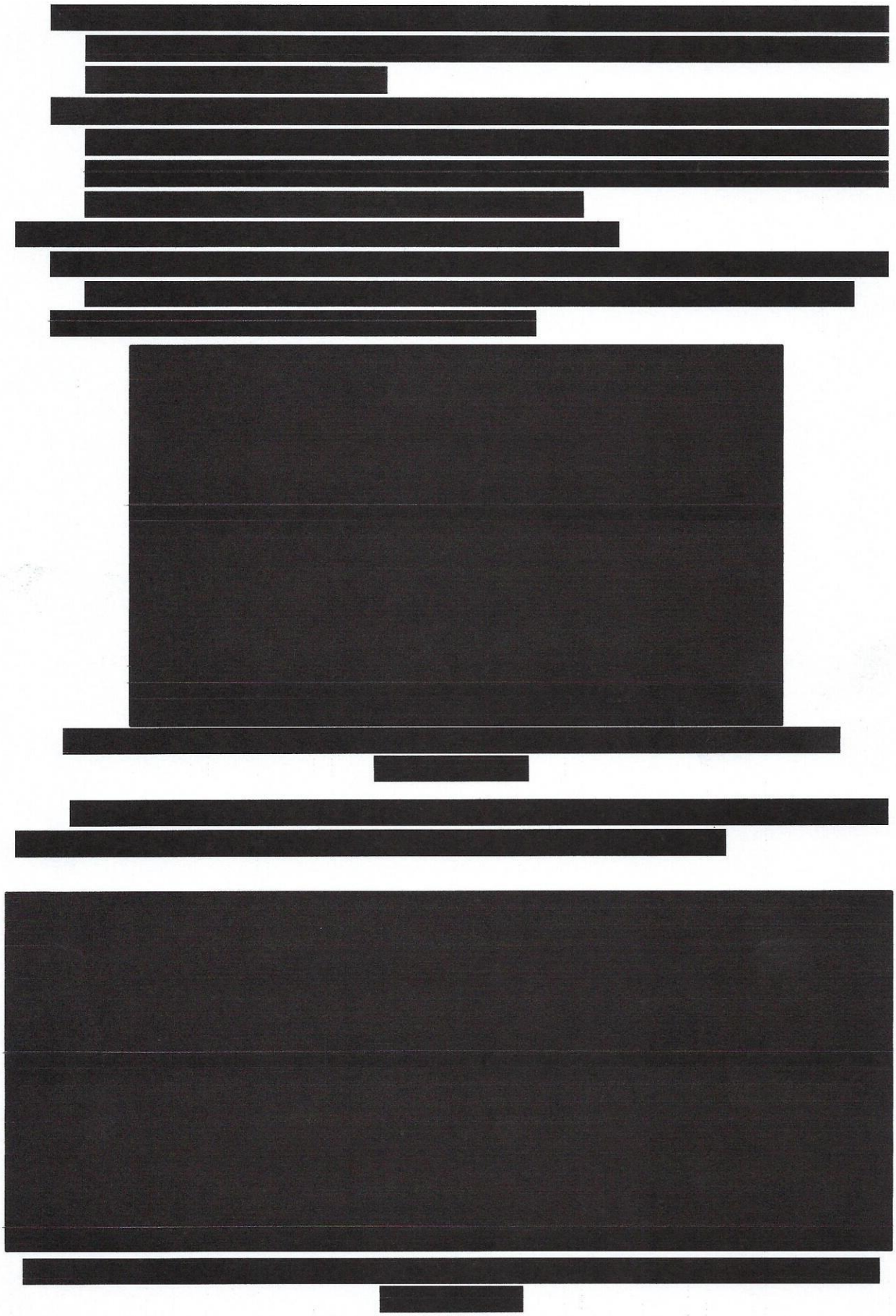
Дакле, у раду, радио је способан да прати два различита TDMA циклуса. На слици 32 је приказан TDMA циклус који прати два канала, са слике се види који канал је активан у ком слоту.

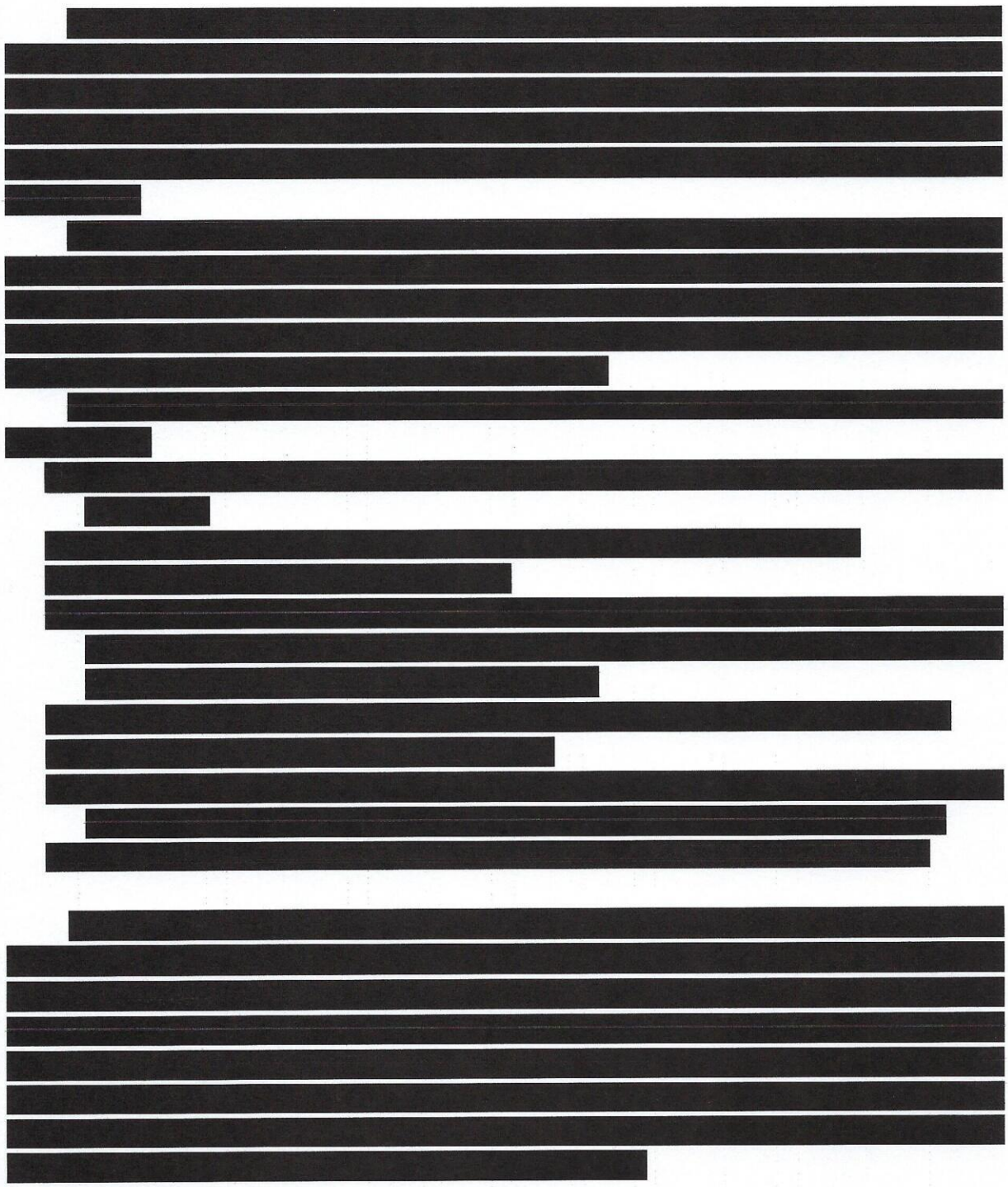


Слика 32. TDMA циклус и TDMA канали

Конфигурација је могућа или преко SNMP протокола (GEOMUX режим мора бити прелиминарно искључен) или аутоматски приликом учитавања почетних елемената у радио станицу (под претпоставком да се овај корак уради током припреме мисије). Промена није могућа када је GEOMUX режим активан.

[redacted]



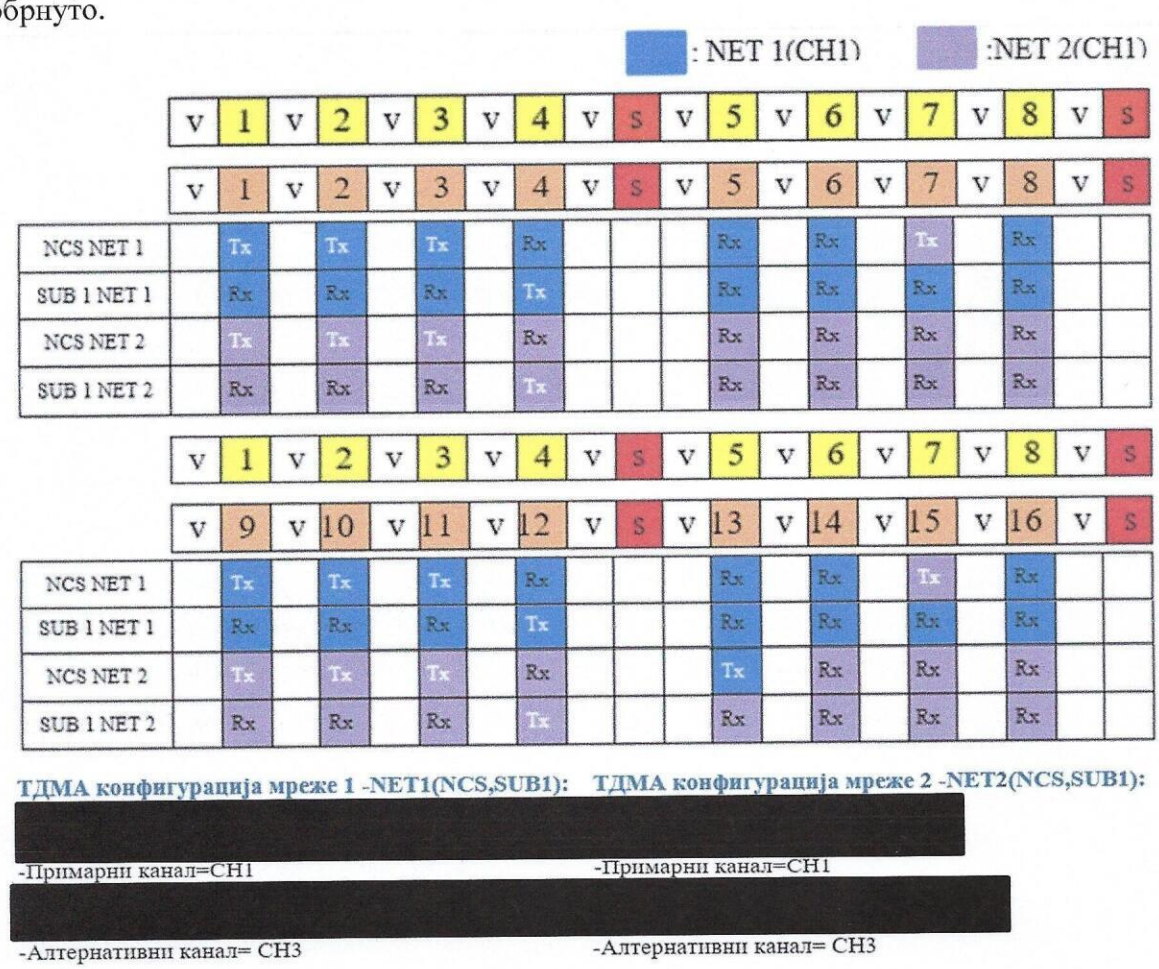


5. Разматрање могућих конфигурација радио мрежа у Dynamic TDMA моду рада

Dynamic TDMA мод рада пружа различите могућности конфигурације радио мрежа, у циљу бољег искоришћења карактеристика радио уређаја. У овом поглављу су приказани начини на које је могуће конфигурисати радио мрежу у Dynamic TDMA режиму рада.

Први пример конфигурације радио мреже које раде у Dynamic TDMA режиму рада је приказан на слици 35.

У овом примеру реализоване су две мреже (NET1 и NET2), које имају по два учесника, једног мастер и једног потчињеног. Као секундарна мрежа у NET1 је подешена примарна мрежа NET2, док је као секундарна мрежа у NET2 подешена примарна мрежа NET1. То значи да учесници мреже 1 могу преко свог трећег канала (CH3) да остваре комуникацију са учесницима мреже 2 на њиховом првом каналу и обрнуто.



Слика 35. Пример 1 конфигурације радио уређаја

Приликом конфигурације и једне и друге мреже извршена су подешавања параметара и примарног и алтернативног TDMA канала. Уколико се упореде ове две кофигурације може се закључити да параметри примарног канала мреже 1 одговарају

параметрима алтернативног канала мреже 2 и обрнуто. Такође се може уочити да је величина примарног циклуса дупло дужа од величине алтернативног циклуса у NET1, док је у NET2 обрнуто, величина алтернативног циклуса је дупло дужа од величине примарног циклуса. Величине примарног и алтернативног циклуса су приказане жутим и наранџастим квадратима са бројевима од 1 до 8 и од 1 до 16, у зависности о којој се мрежи ради (NET1 или NET2). Код обе мреже су капацитети и величине алтернативног канала једнаки капацитету и величини примарног канала супротне мреже, што омогућава међусобну комуникацију између ове две мреже на каналу 3 (CH3). Обе мреже као примарни канал користе CH1 за међусобну комуникацију између својих учесника.

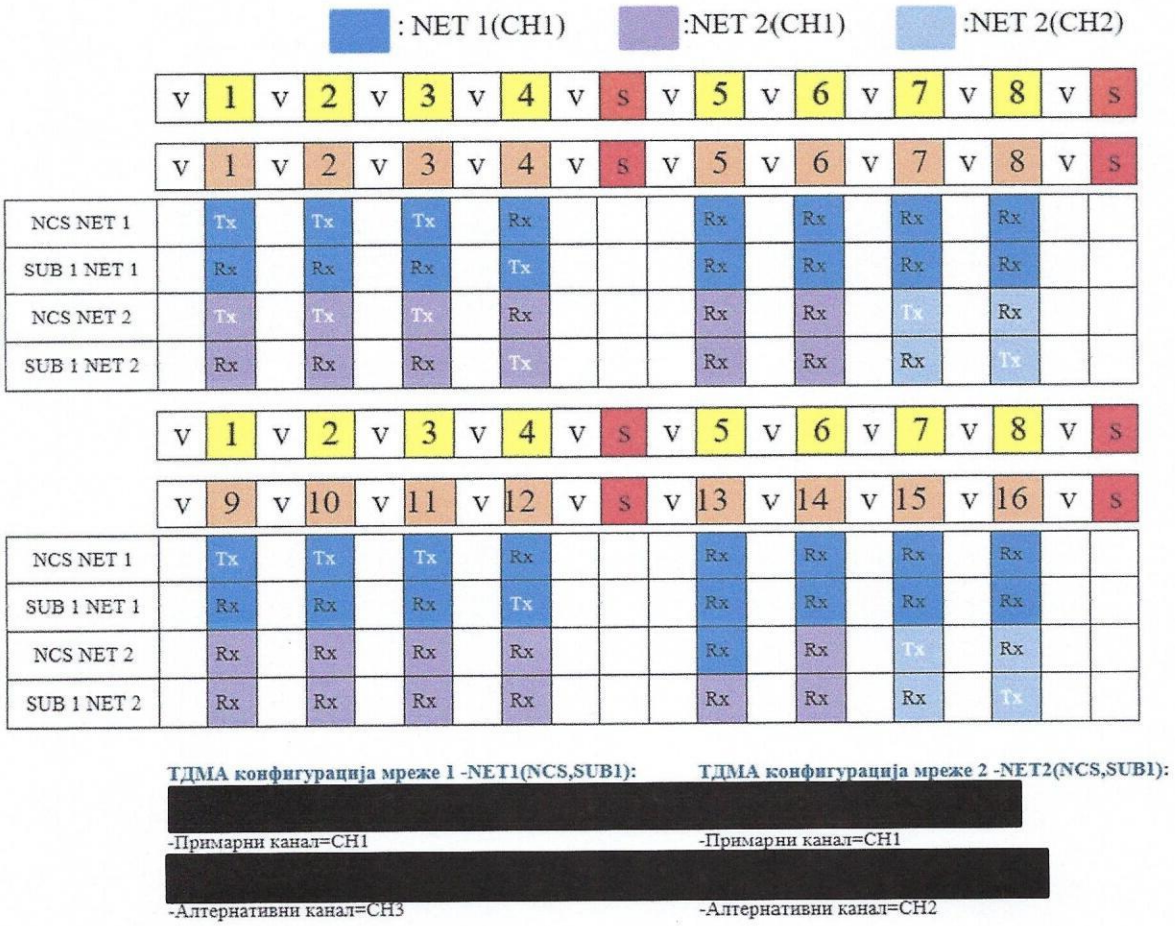
Када се анализирају ове мреже, прва 3 слота примарног канала су додељена NCS станици као предајни слотови, док је 4. слот примарног канала додељен SUB1 станици као предајни слот, код обе мреже. Уколико се анализира слот број 7 мреже 1, он је додељен NCS станици као предајни слот у алтернативној мрежи (означен је бојом мреже 2), што значи да ће учесници мреже 2 на 7. и 15. слоту примарног канала примити поруку од NCS станице мреже 1. С обзиром да је дужина алтернативног канала мреже 1 дупло краћа у односу на дужину примарног канала, NCS станица ће у времену трајања једног циклуса примарног канала два пута послати поруку преко алтернативног канала (CH3). Да би мрежа 2 примила поруку од мреже 1 потребно је да параметри њене примарне кофигурације одговарају параметрима алтернативне конфигурације мреже 1. У случају мреже 2 слот број 13 је додељен NCS станици као предајни слот у алтернативној мрежи (означен је бојом мреже 1), што значи да ће учесници мреже 1 на 5. слоту примарног канала примити поруку од NCS станице мреже 2. С обзиром да је дужина алтернативног канала мреже 2 дупло дужа у односу на дужину примарног канала, NCS станица ће у времену трајања два циклуса примарног канала један пут послати поруку преко алтернативног канала (CH3).

Други пример конфигурације радио мреже које раде у Dynamic TDMA режиму рада је приказан на слици 36.

У овом примеру такође су реализоване две мреже (NET1 и NET2), које имају по два учесника, једног мастер и једног потчињеног. Секундарне мреже су подешене као у претходном примеру. Приликом конфигурације и једне и друге мреже извршена су подешавања параметара и примарног и алтернативног TDMA канала. Уколико се упореде ове две кофигурације може се закључити да алтернативни канал мреже 1 одговара првом каналу мреже 2, али је величина алтернативног циклуса дупло краћа од величине примарног циклуса мреже 2. Алтернативни канал мреже 2 одговара каналу 2 мреже 2, што значи да мрежа 2 нема могућност комуникације са мрежом 1.

Када се анализирају ове мреже, прва 3 слота примарног канала су додељена NCS станици као предајни слотови, док је 4. слот примарног канала додељен SUB1 станици као предајни слот. Уколико се погледају слотови број 7 и 8 мреже 2, они су додељени станицама као предајни/пријемни слот у алтернативној мрежи по каналу 2, што значи да учесници мреже 2 могу да комуницирају унутар своје мреже по каналу 2. Уколико се посматра мрежа са више од два учесника, она омогућава интерну комуникацију између два учесника. Такође у овом примеру учесници мреже 1 имају могућност слања поруке учесницима мреже 2 по алтернативном каналу. С обзиром да је дужина циклуса

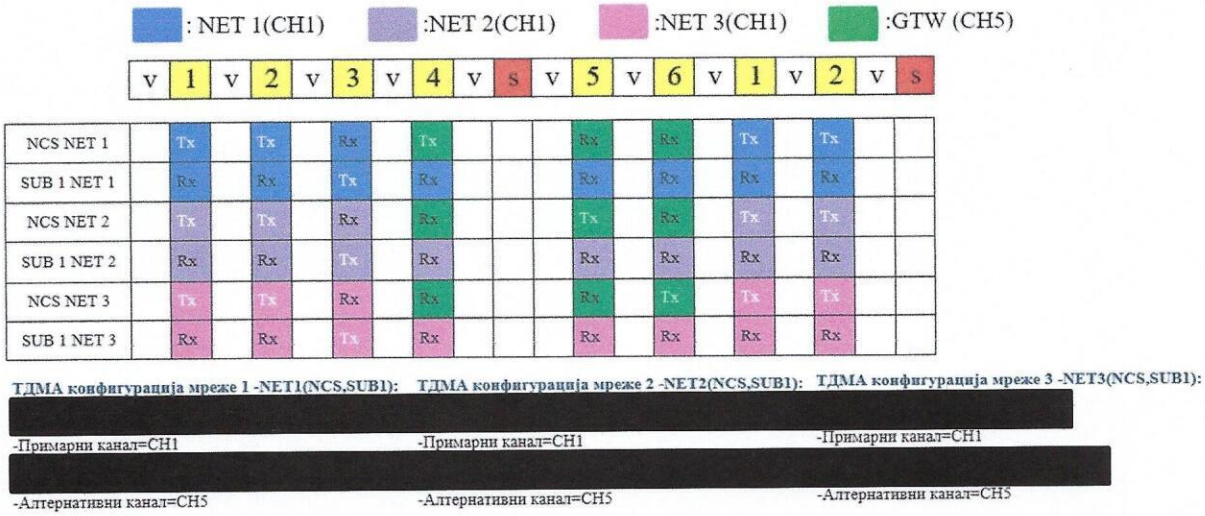
примарног канала мреже 2 дупло дужа у односу на дужину алтернативног циклуса мреже 1, уколико се NCS станици мреже 1 додели слот број 5 као алтернативни, учесници мреже 2 ће у времену трајања једног циклуса примарног канала два пута примити поруку преко алтернативног канала (по слоту 5 и 13).



Слика 36. Пример 2 конфигурације радио уређаја

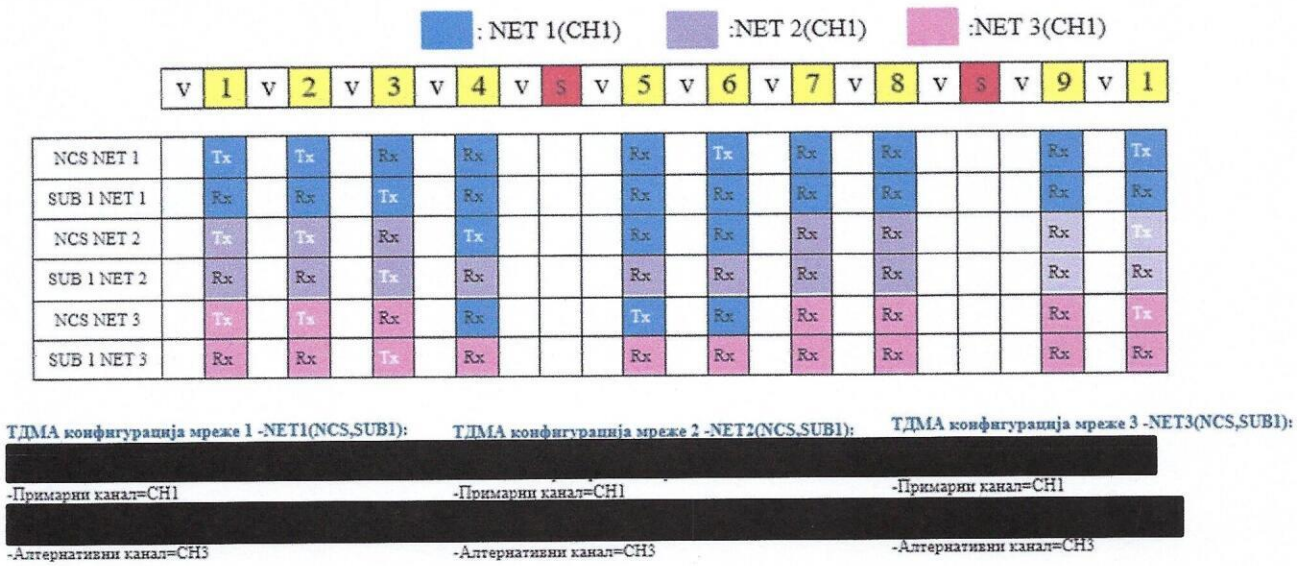
Трећи пример конфигурације се састоји од три мреже са по два учесника, где свака мрежа има свој примарни канал за комуникацију унутар ње, док се за комуникацију између свих учесника све три мреже користи канал 5 као алтернативни канал. Канал 5 је заједнички канал за све мреже и на овај начин учесници више мрежа могу да комуницирају заједно. [redacted] Све три мреже користе прва 3 слота за интерну комуникацију, док се наредна три слота користе као алтернативна за комуникацију између примарних станица ове три мреже, након чега циклус креће испочетка. Алтернативни слотови су на слици обележени зеленом бојом, види се да све три примарне станице имају по један алтернативни слот за емитовање и два алтернативна слота за пријем. Такође се види да SUB станице нису подешене да комуницирају по алтернативном каналу, што значи да оне могу да комуницирају само у оквиру своје мреже. У овом случају SUB станице неће имати комуникацију по слоту број 4, 5 и 6, јер у свакој мрежи има по једна NCS станица. Ако се претпостави да свака

мрежа има више од два учесника, на пример 4 (максималан број учесника би био 6, јер је дужина трајања циклуса 6), SUB станице би могле међусобно да комуницирају по слотовима 4, 5 и 6 уколико имају потребу.



Слика 37. Пример 3 конфигурације радио уређаја

Пример 4 је сличан примеру 3, разлика је у томе што се не користи канал 5 за комуникацију између свих мрежа, већ мреже 2 и 3 као своју секундарну мрежу користе примарну мрежу NET1.



Слика 38. Пример 4 конфигурације радио уређаја

У овом примеру величина свих циклуса је 9, капацитет и примарног и алтернативног канала је 60 B. Све три мреже користе прва 3 слота за интерну комуникацију, док се наредна три слота користе као алтернативна за комуникацију између примарног канала мреже 1 и алтернативних канала мрежа 2 и 3. Примарне станице мрежа 2 и 3 имају по један слот за емитовање по алтернативном каналу, они су

означени плавом бојом и ознаком Tx, док друга два слота користе за пријем поруке по алтернативном каналу и они су означени плавом бојом и ознаком Rx. Такође се види да SUB станице мрежа 2 и 3 нису подешене да комуницирају по алтернативном каналу, што значи да оне могу да комуницирају само у оквиру своје мреже. У овом случају SUB станице неће имати комуникацију по слоту број 4, 5 и 6, јер у свакој мрежи постоји по једна NCS станица. У овом примеру поруке које шаљу NCS станице са мрежа 2 и 3, прима и SUB 1 станица мреже 1, али уколико се не жели да тај учесник у мрежи добија поруке од мрежа 2 и 3, може се онемогућити прослеђивање те поруке од радио станице ка терминалу на коме се налази софтвер за управљање станицом.

6. Разматрана конфигурација мреже

Модернизација постојећих ТкИ система подразумева увођење нове телекомуникационе опреме, која би значајно побољшала карактеристике и могућности комуникације између свих подсистема, учесника радио мреже. Употребом нових радио уређаја омогућава се пренос података у приближно реалном времену коришћењем високог степена заштите, што обезбеђује већу поузданост преноса података. У зависности од потреба већ постојећих система и могућности нових радио уређаја, радио мрежа може да има два и више учесника, од којих један учесник мора да буде мастер (енгл. *master*) и остали учесници слејв (енгл. *slave*). Конфигурација мреже је кружна са мастер станицом у центру круга, што омогућава подједнаку удаљеност слејв станица од мастер станице. На пример, број учесника у радио мрежи може бити седам, при чему је једна мастер станица у центру и шест слејв станица распоређених кружно тако да свака покрива угао од 60^{o}.

У овом раду предложен је телекомуникациони систем са једном мастер станицом и 6 потчињених станица (слејв) који се може применити за комуникацију између различитих система, у овом случају телекомуникациони систем представља симулирану комуникацију између радарског система као мастер станице и 6 против авионских система (оруђа). У оквиру симулираног ТкИ система пренос података и говора, уместо до сада коришћених радио уређаја типа РУ-2/1, реализован је радио уређајима VVF RU TRC-9310-3A произвођача THALES (слика 39). Основни циљ реализованог телекомуникационог система је да се подаци о циљевима у ваздушном простору од конзоле софтверског радарског пријемника проследе ка оруђима бежичним путем у приближно реалном времену, како би оруђе заузело коректан положај за захват и гађање циљева у ваздушном простору.

Слика 39. Радио уређај THALES VVF RU TRC-9310-3A [24]

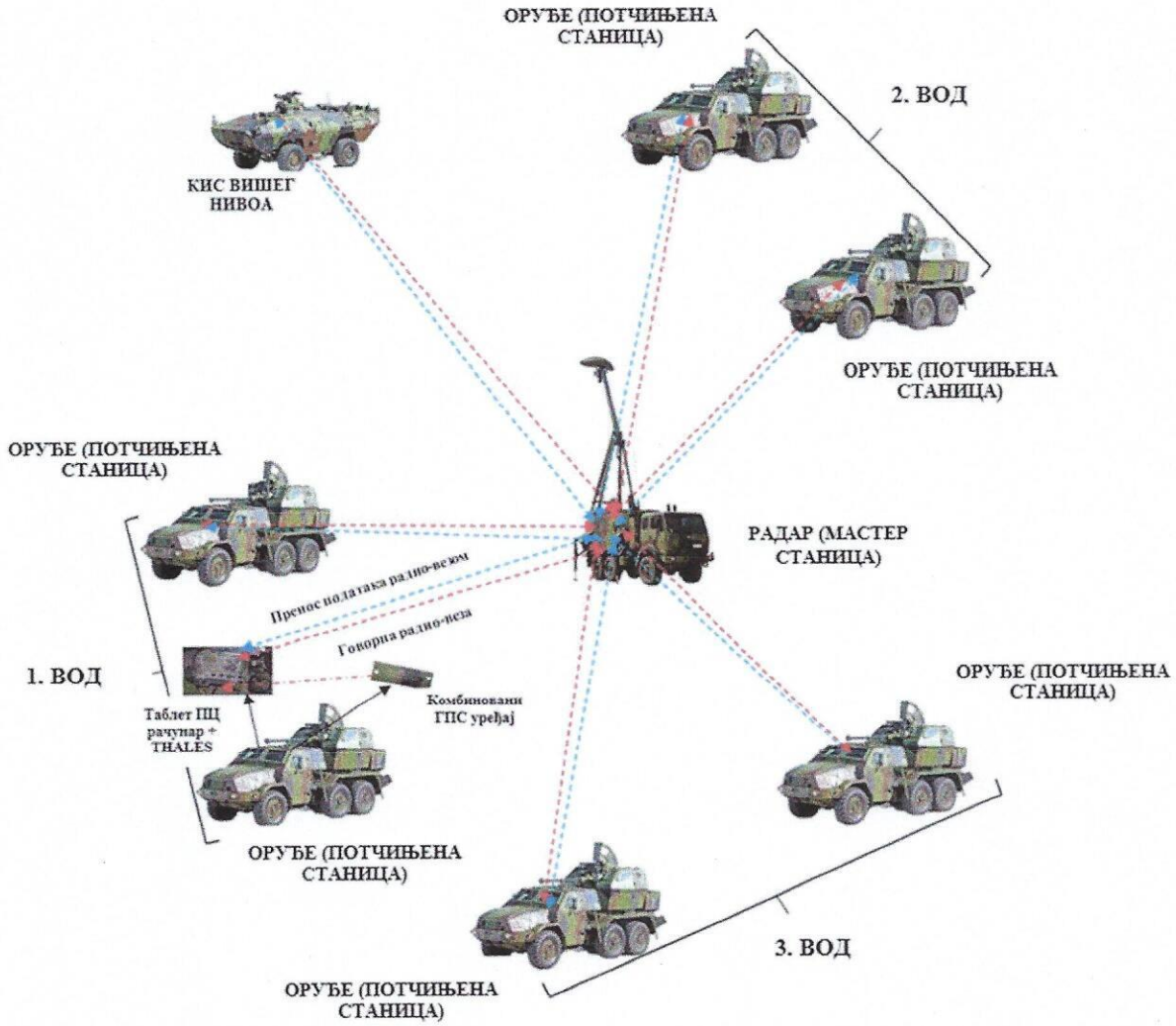
F@stnet радио уређаји су намењени за одржавање радио везе на тактичком нивоу различитих јединица. Ради се о модуларном радио уређају, односно исти примопредајник је део и преносне и превозне верзије. Одговарајући прибор омогућава војнику употребу радио уређаја који носи у ранцу, као и његово постављање на све врсте борбених платформи (покретних и стационарних). F@stnet радио уређаји су програмабилни ускопојасни уређаји који могу да раде у режимима фреквенцијског скакања. Одликује их висок степен заштите од EPM (енгл. *Electronic Protective Measures*) - ECCM (енгл. *Electronic Counter-CounterMeasure*). Дигитални пренос гласа и података је шифрован помоћу COMSEC криптографских кључева. Радио пренос је маскиран кључем TRANSEC. Радио уређаји су опремљени IP рутером и R@dnet софтвером који омогућава једноставну, брзу и ефикасну припрему уређаја за рад у системима који се базирају на пакетском преносу са IP протоколом. Уређаји су опремљени GPS пријемником, захваљујући коме је могуће извести положаје командирским радио станицама, које се могу приказати на дигиталној мапи уз одговарајући број радија [24].

Радио уређај THALES VVF RU TRC-9310-AP је дизајниран за уградњу на све борбене платформе - мобилне и стационарне. Састоји се од ТРЦ 9210 примопредајника и појачавача снаге 50 W. Једноставно се поставља у возила. Може се уградити на монтажну плочу са или без амортизера. Радио има колокационе филтере који омогућавају истовремени рад два радија у истом возилу [24]. Техничке карактеристике радио уређаја TRC-9310-AP су приказане у табели 6.

Табела 6. Техничка спецификација VVF RU TRC-9310-AP [24]

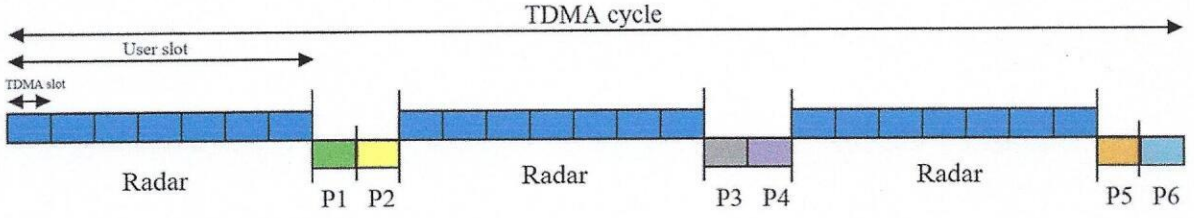
Карактеристике	Вредности
Фреквенцијски опсег	30 ÷ 87,975 MHz, 2320 канала 25 kHz
Осетљивост	-113 dBm
Режими преноса	FH, FFH (*Frequency Hopping* – 300 скокова/s)
	FCS (*Free Channel Searching*)
	MIX (*Mixed Mode* – FFH or FCS)
	DFF (*Digital Fixed Frequency*)
	AFF (*Analog Fixed Frequency*)
Даљинска контрола	SNMP agent
	PARR/PROTEE/SYCOMORE (PPS)
Интерфејси података	Ethernet 10 Mbit/s base-T
	Серијски интерфејс IP/PPP
	Серијски интерфејс RS232
РФ излазна снага	0,5 W; 5 W; 50 W
Улазни напон	18 ÷ 33 V DC
Димензије	290 x 139 x 340 mm
Тежина	< 14 kg
Радна температурни опсег	-40°C ÷ +70 °C
Механички и еколошки захтеви	MIL STD 810 у погледу отпорности на со, маглу, хладноћу, прашину и песак

Ради сликовитог приказа могуће имплементације разматране конфигурације дата је шема реализоване комуникације између радарског система као мастер станице и 6 оруђа као потчињене станице, приказана на слици 40.

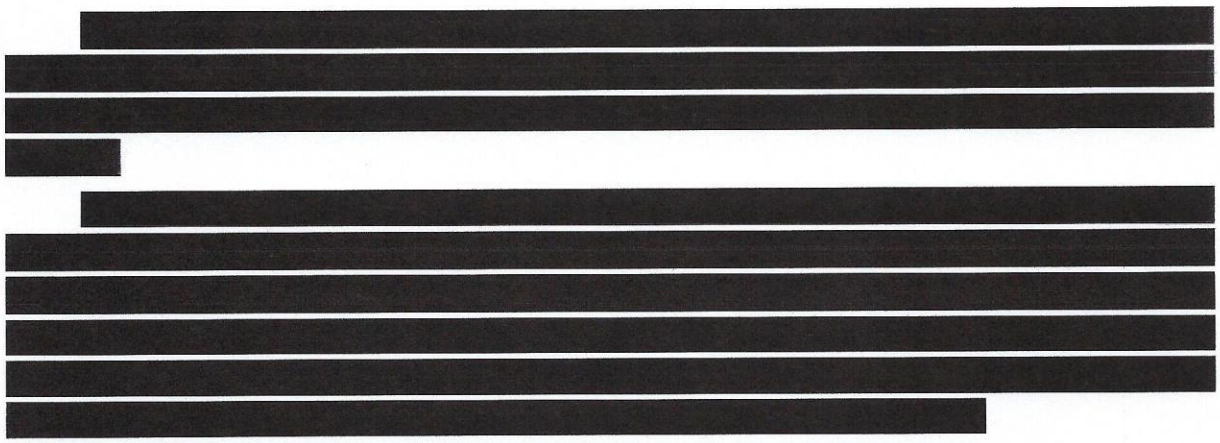


Слика 40. Шема реализоване комуникације између радарског система као мастер станице и 6 против авионских система (потчињене станице)

Имплементацијом и повезивањем радио уређаја ВВФ опсега фирме THALES омогућена је реализација преноса података између мастер станице и 6 потчињених станица у *Pure* TDMA моду рада, као што је приказано на слици 41. Реализовани ТК систем у овом примеру омогућава аутоматску доделу циљева у реалном времену.



Слика 41. TDMA циклус реализованог ТкИ система



Ова врста рада омогућила је софтверско управљање радио уређајем, као и аутоматско навођење оруђа на циљ, али има могућност преноса само података преко једног РУ у *Pure* TDMA моду рада. За пренос говора користи се други радио уређај THALES VVF RU TRC-9310-AP у CNR режиму рада.

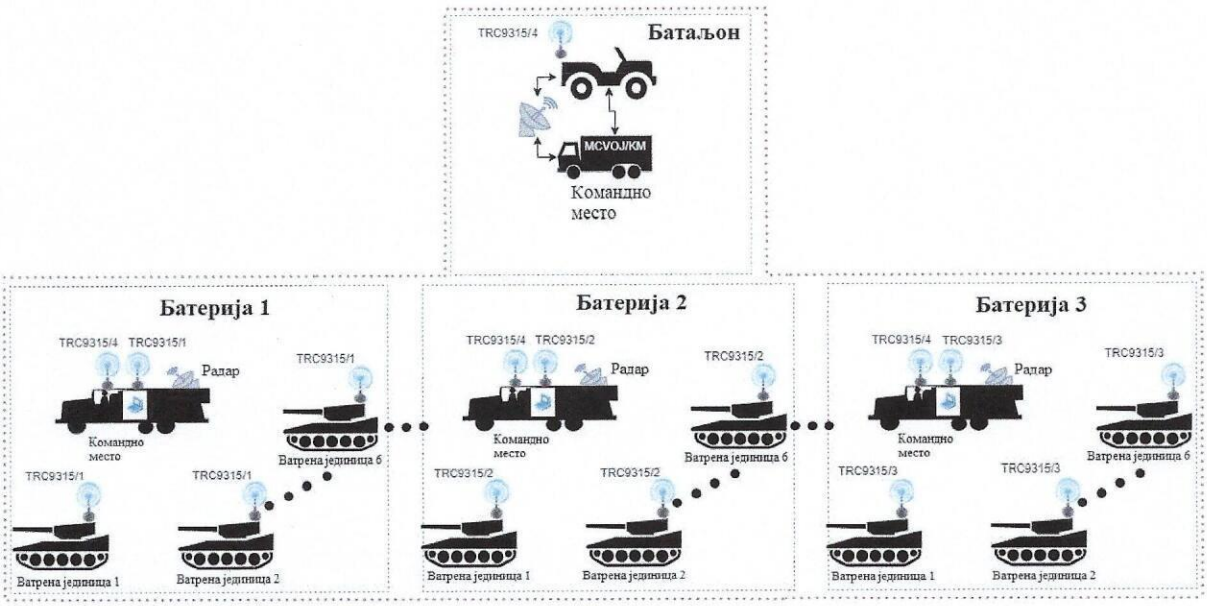
6.1. Могућа примена Dynamic TDMA врсте рада

Увођењем нове врсте рада омогућава се истовремени пренос говора и података преко једног примопредајника и повећава се капацитет навођења ватрених јединица (ВЈ) на циљеве, у зависности од домета радио уређаја.

Предлог унапређеног ТкИ система, који би се састојао од радарског система и 6 оруђа, који ће обезбедити ефикасније и сигурније остваривање размене информација о циљу, унапређење командовања и правовременог навођења ВЈ на циљ, подразумева имплементацију радио уређаја са Dynamic TDMA врстом рада. На слици 42 је приказан предлог шеме комуникације ракетне јединице на нивоу дивизиона, који се састоји од три батерије. Приказана је комуникација унутар дивизиона, која се састоји од комуникационе мреже унутар сваке батерије између КМ Батерије и ВЈ, комуникационе мреже између КМ батерија и КМ батаљона, као и могућност комуникације између КМ батерија.

Унапређени ТкИ систем обезбеђује реализацију комуникације између радара и ватрених јединица употребом једног уместо два радио уређаја. Применом нове врсте рада број ватрених јединица које радар наводи на циљ може бити већи, у зависности од количине података и удаљености ВЈ од радара.

Разматрана радио мрежа на нивоу батерије, применом Dynamic TDMA врсте рада, подразумевала је 7 учесника, 6 ВЈ и КМ батерије, и у овом случају ВЈ представља оруђе и КМ представља радар. Ова мрежа омогућава говорну комуникацију и пренос података у реалном времену између 6 ВЈ и КМ батерије, као и пренос података између КМ батерија.



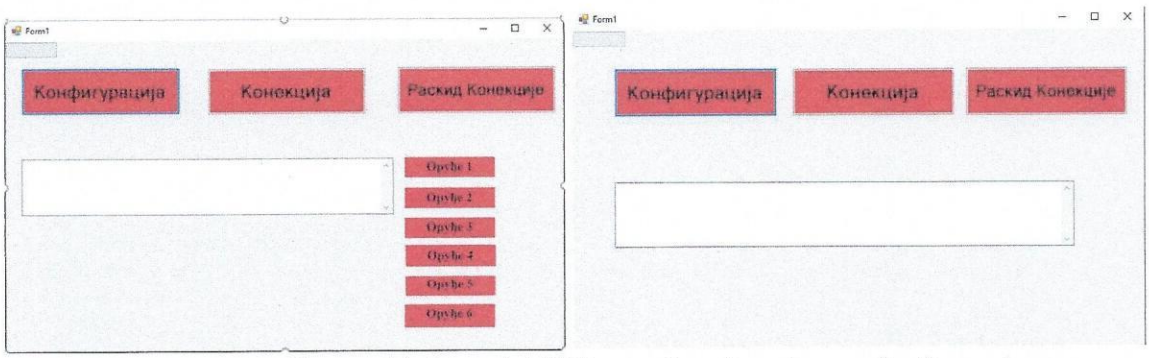
Слика 42. Шема комуникације ракетне јединице на нивоу батаљона

[redacted]

[redacted]

[redacted]

У овом раду реализована су два софтвера (СРП) у које је имплементиран комуникациони протокол, за Dynamic врсту рада, уграђен у радио станице THALES и који у реалном времену извршава и контролише понашање радија у смислу преноса/пријема података. Изглед оба софтвера (за радар и за оруђе) је приказан на слици 44.



Слика 44. Изглед СРП за радар (лево) и оруђе (десно)

Оба софтвера имају тастере за конфигурацију, конекцију и раскид конекције. Конфигурацијом се подешавају сви параметри радио мреже који су потребни за рад РУ у Dynamic врсти рада. Једном када се изврши конфигурација радија, она остаје запамћена све док се или промене параметри или обрише мисија из радија, па је потребно поново извршити конфигурацију.

Да би се успоставила веза са сервером који се налази у радију, потребно је сваки пут након покретања софтвера активирати тастер конекција, након чега се успоставља конекција са РУ и започиње размена података. На крају сваког рада, тастером раскид конекције се прекида ова веза.

Оба софтвера имају и текстуални прозор намењен за праћење комуникације приликом тестирања. Оно што разликује софтвер за радар су лабеле које представљају присуство сваког од 6 оруђа и означени су са бројевима од 1 до 6.

Поред комуникације и размене порука са РУ, „**СРП радара**“ прима циљеве од Софтверског радарског пријемника који је намењен за праћење и доделу циљева ВЈ у радару, док „**СРП оруђа**“ добијени податак о циљу прослеђује софтверу за приказ циља на оруђу, који је намењен за пријем података о циљу и навођење оруђа на циљ.

7. Анализа реализоване конфигурације

Анализа могућности предложене конфигурационе мреже је реализована у лабораторијским условима. За ово испитивање инсталирани су симулатор Софтверског радарског пријемника на једном терминалу, који симулира кретање циљева радара, и софтвер за пријем података о циљу на 5 терминала.

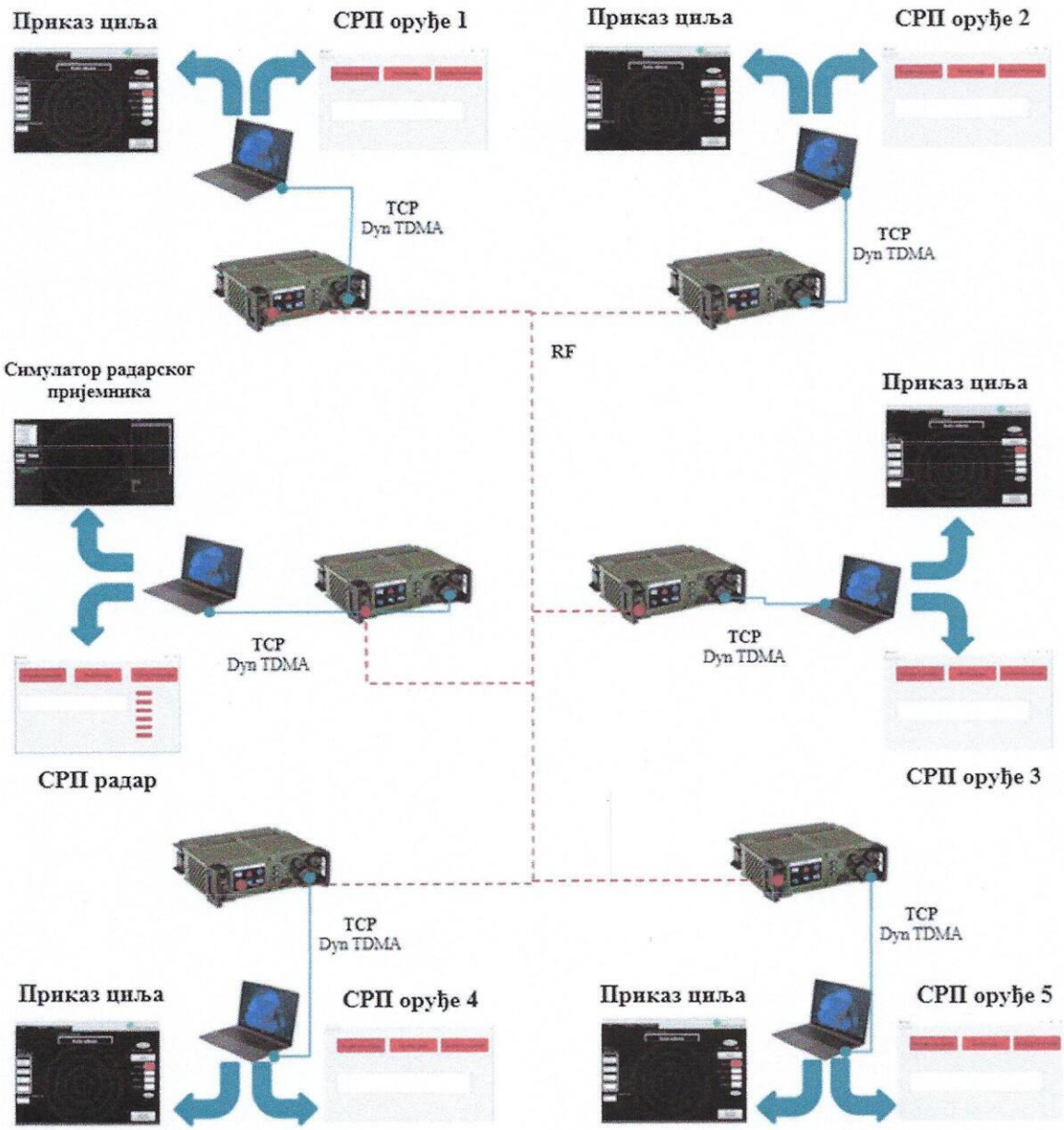
Због недостатка РУ са *Dynamic* врстом рада, тренутно испитивање је реализовано између симулатора радара (мастер) и пет симулатора оруђа (слејв).

7.1. Резултати лабораторијских испитивања реализоване конфигурације

На слици 45 је приказана шема повезивања реализоване радио мреже у лабораторијским условима, која се састоји од 6 учесника, симулатора Софтверског радарског пријемника (мастер) и пет симулатора оруђа (слејв).

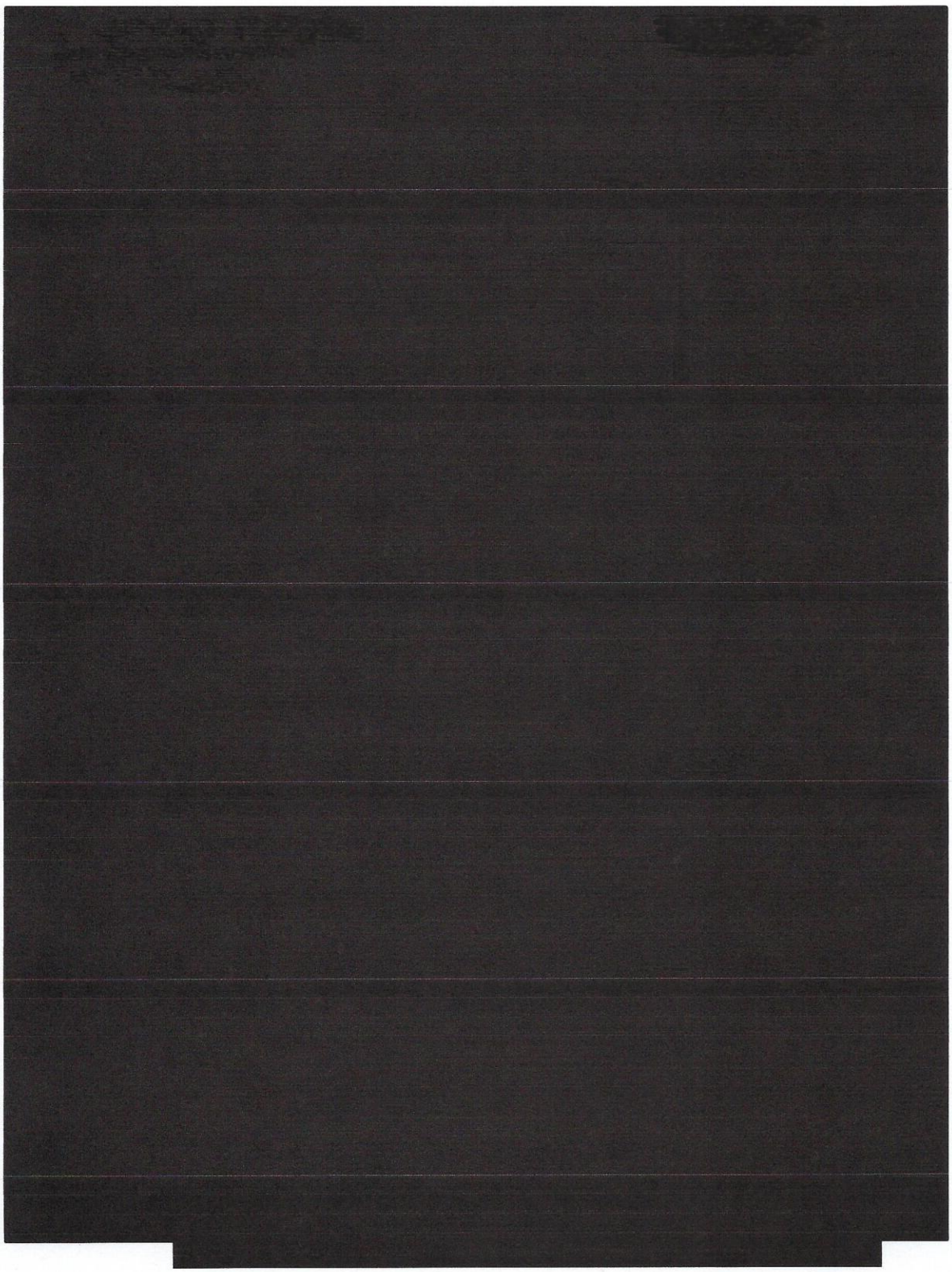
На једном терминалу, који представља мастер станицу, инсталирана је реализована апликација „**СРП радар**“ и симулатор Софтверског радарског пријемника, док је на осталих пет терминала инсталирана реализована апликација „**СРП оруђе**“ и апликација за приказ пријема података о циљу. Пре покретања апликација потребно је подесити IP адресе на терминалима, извршити синхронизацију РУ и детектовање GPS локације на једном РУ.

Након покретања апликација на свим терминалима потребно је извршити конфигурацију РУ, притиском на дугме “Конфигурација”, а затим извршити конекцију са РУ притиском на дугме “Конекција”. Након успешне конекције са РУ, на свим терминалима у текстуалним прозорима исписиваће се долазне порука преко РУ, док ће се на „**СРП радар**“ детектовати присуство пет оруђа (лабеле означене са Оруђе 1 до Оруђе 5 ће променити боју у зелено).



Слика 45. Шема повезивања симулатора Софтверског радарског пријемника (мастер) и 5 симулатора оруђа (слејв)

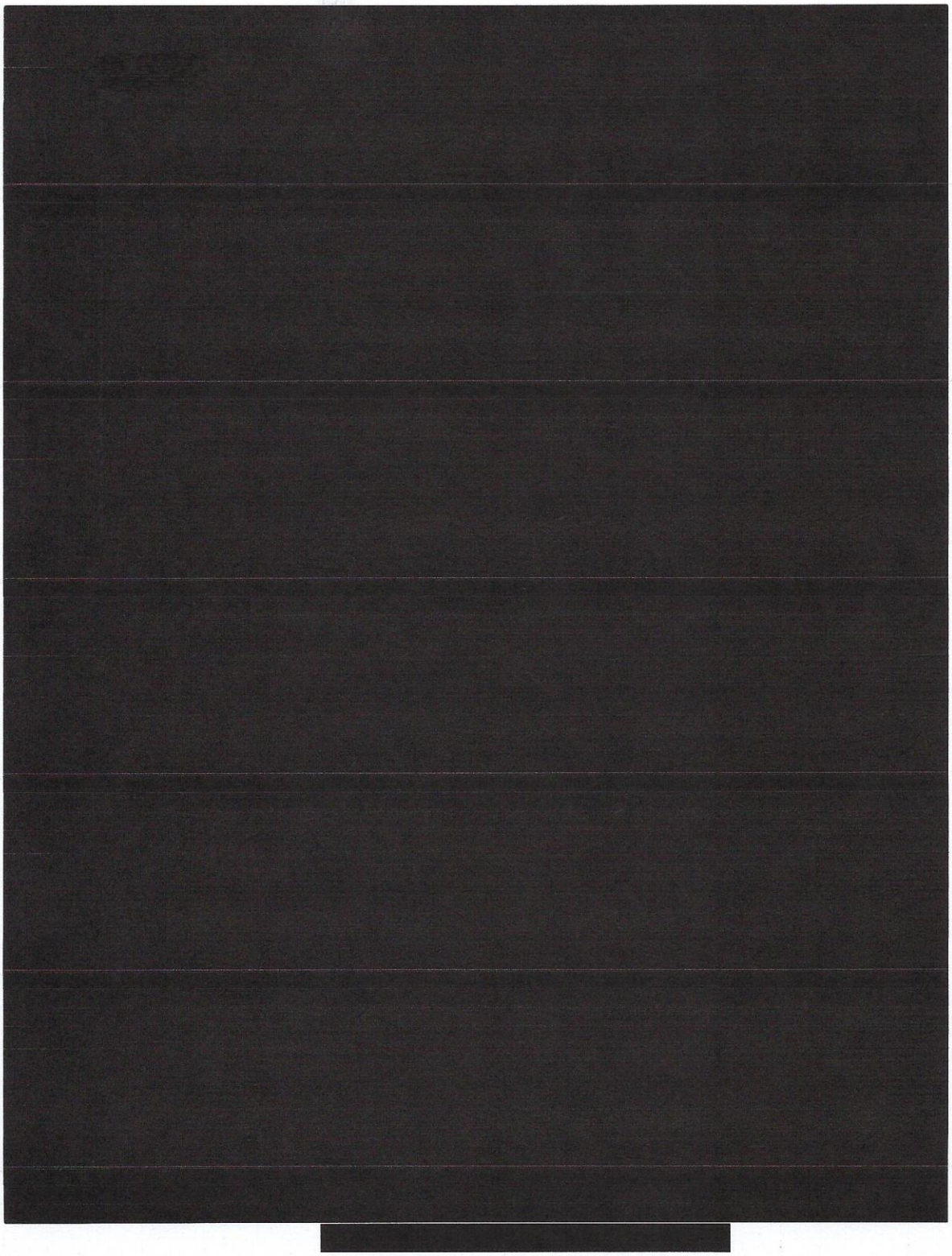
За потребе тестирања и анализе све поруке које долазе преко РУ, заједно са тренутним временом се уписују у txt фајл. На слици 46 је приказан упис података у txt фајл на „**СРП радар**“ у трајању од једног циклуса.



Поруке које долазе од „**СРП оруђе**“ су означене правоугаоницима различитих боја и има их укупно 15, од сваког „**СРП оруђе**“ по 3 поруке. Последња цифра примљене поруке означава ИД слејв станице, при чему се види да се та цифра мења од 1 до 5 што одговара задатом редоследу слања порука са ВЈ. Изнад сваке поруке се налази вредност слота у коме је примљена порука, уколико се ове вредности упореде са вредностима слотова додељених ВЈ на слици 40, види се да се оне поклапају. Уколико

се погледају времена свих примљених порука, може се закључити да дужина трајања једног циклуса износи приближно 9s што одговара очекиваној дужини трајања циклуса.

На слици 47 је приказан упис података у txt фајл на „**СРП оруђе 1**“ у трајању од једног циклуса.



[redacted]

Овакав ТкИ систем се може применити за реализацију и унапређење комуникације различитих система Војске Србије. Dynamic TDMA врста рада омогућава различиту и променљиву конфигурацију радио уређаја у зависности од потребе система. Највећу примену овакви ТкИ системи налазе у радарским и другим системима за навођење, где је потребан пренос података у реалном времену. Дорадом реализованих екстерних апликација могу се боље искористити могућности Dynamic TDMA врсте рада у циљу унапређења већ постојећих ТкИ подсистема ВС.

Закључак

Основни циљ истраживања у овом мастер раду јесте реализација и анализа предлога унапређења конфигурационе мреже ТкИ подсистема применом *Dynamic* TDMA врсте рада радио уређаја THALES. ТкИ подсистем ће омогућити сигурну и поуздану размену информација у току борбене операције између свих учесника.

Процес планирања и конфигурације радио мреже ТкИ подсистема захтева познавање теорије, протокола за приступ дељеном преносном медијуму и радио протокола. Из тог разлога, у овом раду је дат акценат на изучавању MAC протокола, њихових карактеристика и начина функционисања. Посебан акценат је дат на СРП и SNMP, који су неопходни приликом реализације мреже ТкИ подсистема. СРП у реалном времену ради на платформи за извршавање и контролише како се радио уређај понаша у смислу преноса/пријема података преко слободног простора, док је SNMP протокол намењен за прикупљање и организовање информација о радио уређајима којима управља и за модификацију тих информација ради промене њиховог понашања.

Приликом пројектовања саме мреже, водило се рачуна о томе да предложено решење треба да унапреди постојећи ТкИ систем на нивоу батерије и да у блиској будућности омогући проширење мреже и ефикасно искоришћење свих капацитета које пружа *Dynamic* TDMA врста рада радио уређаја. Једно од водећих унапређења представља могућност коришћења РУ истовремено и за пренос говора и за пренос података, и могућност слања података другој мрежи по алтернативном каналу, што се може применити за пренос информација између сопствене и садејствујуће јединице. Применом ове врсте рада РУ, такође је отворен простор бољој контроли саобраћаја радио мреже и бољој искоришћености РУ. Нова врста рада има могућност преноса података великог капацитета, што омогућава пренос **веће количине података** у реалном времену и проширење **броја учесника** радио мреже. Предложена конфигурација радио мреже обезбеђује ефикасније и сигурније остваривање размене података, унапређење командовања и правовремено навођење ВЈ на циљ. Главну примену оваква радио мрежа проналази у системима где је потребно минимално кашњење у преносу података, на пример радарски системи, ПВО системи и други системи за навођење.

Посебан акценат стављен је и на израду софтвера, односно СРП, који је намењен за размену информација између учесника у радио мрежи. Израдом софтвера за управљање РУ обезбеђена је ефикаснија и сигурнија размена информације у реалном времену, са минималним кашњењем, а у циљу унапређења командовања и правовременог доношења одлука у операцијама различитих типова. У СРП је имплементиран комуникациони протокол, за Dynamic врсту рада, уграђен у радио станице THALES, који у реалном времену извршава и контролише понашање радија у смислу преноса/пријема података. Ова два софтвера омогућују да се исти хардвер **реконфигурише** за подршку вишеструких, променљивих радио протокола у реалном времену, једноставном применом софтверског програма. Динамички избор параметара омогућава уређају да се прилагоди различитим параметрима, што је основна карактеристика **софтверски дефинисаних радија**. Софтверски радио омогућава велику

флексибилност и прилагодљивост будућим променама и новим стандардима у бежичним комуникацијама. Дорадом реализованих софтвера могу се боље искористити капацитети Dynamic TDMA врсте рада.

Заменом старе врсте рада РУ новом дошло се до повећања капацитета саобраћаја између учесника у радио мрежи, а самим тим и употребе других, новијих сервиса (могућности). Предложени модел унапређује постојећи ТкИ систем у домену следећих карактеристика:

- Скалабилан је за будућу надградњу по питању капацитета саобраћаја, динамичне доделе слотова и повећања броја учесника;
- Омогућава употребу једног радио уређаја за пренос и говора и података, тј. замену два РУ са једним саобраћајним модом;
- Омогућава комуникацију између садејствујућих јединица, разменом порука употребом једног радио уређаја;
- Употребом SNMP протокола који ради на апликативном нивоу користећи TCP/IP смањује се вероватноћа отказа целокупног система.

Даља истраживања која се односе на тематику овог мастер рада требало би усмерити пре свега ка усавршавању и проширивању предложене радио мреже, као и сагледавању могућности примене *Dynamic* врсте рада за комуникацију између учесника других система различитих нивоа. С обзиром на то да предложени модел представља комплексну комуникациону платформу која се може употребити за развијање нових или унапређење већ постојећих ТкИ система, неопходно је у даљем раду пронаћи решења која ће се односити на унапређење предложеног ТкИ система, а која би се заснивали на преносу података са различитих сензора (дронови, IP камере, извиђачки и акустички пријемници, ометачи, итд.). Овакав систем омогућава увезивање различитих наведених елемената у једну целину, пренос података употребом СРП и унапређење ефикасности одлучивања.

Преглед графичких приказа

СЛИКА 1. ПОДЕЛА MAC ПРОТОКОЛА [5] 7
СЛИКА 2. ЈЕДНОСТАВНА ALOHA [5] 8
СЛИКА 3. СЛОТОВАНА ALOHA [5] 9
СЛИКА 4. И- ПЕРЗИСТЕНТНИ МЕТОД [5] 11
СЛИКА 5. НЕ- ПЕРЗИСТЕНТНИ МЕТОД [5] 11
СЛИКА 6. П- ПЕРЗИСТЕНТНИ МЕТОД [5] 12
СЛИКА 7. ПРИКАЗ СУКОБА СИГНАЛА НА ПОЛОВИНИ ПУТА [7] 14
СЛИКА 8. ПРИКАЗ НАЈГОРЕГ СЦЕНАРИЈА СУКОБА [7] 14
СЛИКА 9. ПРИКАЗ ОКВИРА РЕЗЕРВАЦИЈЕ [9] 17
СЛИКА 10. ФУНКЦИЈА ИЗБОРА [5] 19
СЛИКА 11. ФУНКЦИЈА АНКЕТЕ [5] 19
СЛИКА 12. ПРИКАЗ ТОКЕН РИНГА [9] 20
СЛИКА 13. ПРИКАЗ FDMA [11] 21
СЛИКА 14. ФРЕКВЕНЦИЈСКИ ПЛАН ЗА ДВА ТРАНСПОНДЕРА С ОПСЕГА КОРИСТЕЋИ ФИКСНО ДОДЕЉИВАЊЕ FDMA [11] 23
СЛИКА 15. ИЛУСТРАЦИЈА FDMA [11] 24
СЛИКА 16. ИЛУСТРАЦИЈА CDMA [12] 25
СЛИКА 17. CDMA КОДЕР [13] 26
СЛИКА 18. CDMA ДЕКОДЕР [12] 27
СЛИКА 19. TDMA ФРЕЈМ[2] 31
СЛИКА 20. СЛОЈЕВИ TDMA СРП [17] 32
СЛИКА 21. АРХИТЕКТУРА ЗА АНАЛИЗУ РАСПОРЕДА [2] 33
СЛИКА 22. SNMP АЛАТИ ЗА ПРАЋЕЊЕ [17] 37
СЛИКА 23. КОМПОНЕНТЕ SNMP [21] 38
СЛИКА 24. СТРУКТУРНИ ДИЈАГРАМ MIB [21] 39
СЛИКА 25. GET REQUEST AND RESPONSE MESSAGES EXCHANGE [19] 40
СЛИКА 26. СТРУКТУРА MIB [22] 42
СЛИКА 27. GEOMUX ТИПОВИ СЛОТОВА 44
СЛИКА 30. ВРЕМЕНСКА КАРАКТЕРИСТИКА DYNAMIC TDMA 47
СЛИКА 31. DYNAMIC TDMA ЦИКЛУС 47
СЛИКА 32. TDMA ЦИКЛУС И TDMA КАНАЛИ 48

СЛИКА 35. ПРИМЕР 1 КОНФИГУРАЦИЈЕ РАДИО УРЕЂАЈА 51
СЛИКА 36. ПРИМЕР 2 КОНФИГУРАЦИЈЕ РАДИО УРЕЂАЈА 53
СЛИКА 37. ПРИМЕР 3 КОНФИГУРАЦИЈЕ РАДИО УРЕЂАЈА 54
СЛИКА 38. ПРИМЕР 4 КОНФИГУРАЦИЈЕ РАДИО УРЕЂАЈА 54
СЛИКА 39. РАДИО УРЕЂАЈ THALES VVF RU TRC-9310-3A [24] 56
СЛИКА 40. ШЕМА РЕАЛИЗОВАНЕ КОМУНИКАЦИЈЕ ИЗМЕЂУ РАДАРСКОГ СИСТЕМА КАО МАСТЕР СТАНИЦЕ И 6 ПРОТИВ АВИОНСКИХ СИСТЕМА (ПОТЧИЊЕНЕ СТАНИЦЕ) 58
СЛИКА 41. TDMA ЦИКЛУС РЕАЛИЗОВАНОГ ТКИ СИСТЕМА 58
СЛИКА 42. ШЕМА КОМУНИКАЦИЈЕ РАКЕТНЕ ЈЕДИНИЦЕ НА НИВОУ БАТАЉОНА 60
СЛИКА 44. ИЗГЛЕД СРП ЗА РАДАР (ЛЕВО) И ОРУЂЕ (ДЕСНО) 61
СЛИКА 45. ШЕМА ПОВЕЗИВАЊА СИМУЛАТОРА СОФТВЕРСКОГ РАДАРСКОГ ПРИЈЕМНИКА (МАСТЕР) И 5 СИМУЛАТОРА ОРУЂА (СЛЕЈВ) 63

Списак скраћеница

Скраћеница	Појам на енглеском	Значење
ACD	*Analog-to-digital conversion*	Аналогно-дигитална конверзија
ACK	*Acknowledgement*	Потврда
BPF	*Band-pass filter*	Пропусни филтер
CDMA	*Code Division Multiple Access*	Вишеструки приступ са кодном расподелом
CSMA	*Carrier Sense Multiple Access*	Вишеструки приступ са ослушкивањем носиоца
CSMA/CA	*Carrier Sense Multiple Access with Collision Avoidance*	Вишеструки приступ са чулом носиоца са избегавањем колизије у рачунарском умрежавању
CSMA/CD	*Carrier Sense Multiple Access with Collision Detection*	Вишеструки приступ са ослушкивањем носиоца уз откривање сукобљавања
CTS	*Clear-To-Send*	Брисање за слање
DOD	*Department of Defense*	Министарство одбране САД
DSSS	*Direct-sequence spread spectrum*	Проширени спектар директне секвенце
DTLS	*Datagram Transport Layer Security*	Комуникациони протокол који обезбеђује сигурност апликацијама заснованим на датаграмима
ECCM	*Electronic counter-countermeasure*	Електронске противмере
EPM	*Electronic protective measures*	Електронске заштитне мере
FDM	*Frequency division multiplexing*	Фреквенцијско мултиплексирање
FDMA	*Frequency Division Multiple Access*	Вишеструки приступ са поделом фреквенције
FM	*Frequency Modulation*	Фреквенцијска модулација
FP	*Fixed Priority*	Фиксни приоритет
GEO	*Geostationary orbit*	Геостационарна орбита
IETF	*Internet Engineering Task Force*	Оперативна група за интернет инжењеринг
IF	*Intermediate frequency*	Средња фреквенција
IFS	*Interframe Space*	Међуоквирни простор
ISO	*International Organization for Standardization*	Међународна организација за стандардизацију
LAN	*Local area network*	Локална рачунарска мрежа
MAC	*Media access control*	Контрола приступа медијуму
MCPC	*Multi-channel-per-carrier*	Пренос са више канала по

		носиоцу
MIB	*Management Information Base*	База података за управљање
NAK	*Negative acknowledgement*	Негативна потврда
NMS	*Network Management System*	Систем за управљање мрежом
OID	*Object Identifiers*	Идентификатор објеката
PCM	*Pulse code modulation*	Импулсна кодна модулација
PCP	*Priority Inheritance Protocol*	Протокол о приоритетном наслеђивању
PHY	*Physical layer*	Физички слој
PIP	*Priority Ceiling Protocol*	Протокол горње границе приоритета
QoS	*Quality of Service*	Подршка за квалитет услуге
RLC	*Radio Link Control*	Контрола радио везе
SEL	*Select frame*	Оквир за одабир
SNMP	*Simple Network Management Protocol*	Једноставан протокол за управљање мрежом
SCPC	*Single-channel per carrier*	Пренос са једним каналом по носиоцу
SCPC-FDMA	*Single-channel-per carrier Frequency division multiple access*	Вишеструки приступ са фреквенцијском поделом са једним каналом по носиоцу
TCP	*Transmission Control Protocol*	Трансмисиони контролни протокол
TDMA	*Time Division Multiple Access*	Вишеструки приступ са временском расподелом
TIA	*Telecommunications Industry Association*	Удружење телекомуникационе индустрије
TLS	*Transport Layer Security*	Сигурност транспортног слоја
UDP	*User Datagram Protocol*	Протокол корисничког датаграма
VAN	*Value-added network*	Мрежа са додатом вредношћу

Преглед табела

ТАБЕЛА 1. РАЗЛИКЕ ИЗМЕЂУ FDMA, TDMA И CDMA 29
ТАБЕЛА 2. ПОРТОВИ КОЈЕ СВАКИ НАВЕДЕНИ ПРОТОКОЛИ КОРИСТЕ ЗА ОДРЕЂЕНЕ ПРОЦЕСЕ [21] 36
ТАБЕЛА 3. SNMP ФУНКЦИЈЕ 41
ТАБЕЛА 4. БРОЈ TDMA СЛОТОВА У ЗАВИСНОСТИ ОД TDMA ОДНОСА 46
ТАБЕЛА 5. ПРИКАЗ ДВЕ КОНФИГУРАЦИЈЕ РАДИО УРЕЂАЈА 48
ТАБЕЛА 6. ТЕХНИЧКА СПЕЦИФИКАЦИЈА VVF RU TRC-9310-AP [24] 57

Литература

[1] Šunjevarić M. 2004. *Osnovi radio komunikacija sa radio tehnikom. Beograd. Studio Line.* (in Serbian). ISBN: 86-84997-06-9.

[2] Shuai Li, Frank Singhoff, Stéphane Rubini, Michel Bourdellès. 2017. Scheduling analysis of tasks constrained by TDMA: Application to software radio protocols. *Journal of Systems Architecture,* 76, pp. 58-75. Available at: https://doi.org/10.1016/j.sysarc.2016.11.003.

[3] *TAKTIKA 1 Udžbenik za srednje vojne škole*. 1983. Beograd: Savezni sekretarijat za narodnu odbranu.

[4] Geeksforgeeks. 2024. Multiple Access Protocols in Computer Network [online]. Available at: https://www.geeksforgeeks.org/multiple-access-protocols-in-computer-network/ Accessed: March 2024.

[5] Binaryterms. *Multiple Access Control* [online]. Available at: https://binaryterms.com/multiple-access-control.html Accessed: March 2024.

[6] Scaler. 2024. *Carrier Sense Multiple Access* [online]. Available at: https://www.scaler.com/topics/csma/ Accessed: May 2024.

[7] Geeksforgeeks. 2024. *Collision Detection in CSMA/CD* [online]. Available at: https://www.geeksforgeeks.org/collision-detection-csmacd/?ref=lbp Accessed: April 2024.

[8] Geeksforgeeks. 2024. *Carrier Sense Multiple Access (CSMA)* [online]. Available at: https://www.geeksforgeeks.org/carrier-sense-multiple-access-csma/?ref=lbp Accessed: May 2024.

[9] Geeksforgeeks. 2024. *Controlled Access Protocols in Computer Network* [online]. Available at: https://www.geeksforgeeks.org/controlled-access-protocols-in-computer-network/ Accessed: May 2024.

[10] Geeksforgeeks. 2024. *Frequency Division Multiple Access (FDMA) Techniques* [online]. Available at: https://www.geeksforgeeks.org/frequency-division-multiple-access-fdma-techniques/?ref=header_search Accessed: June 2024.

[11] Slideshare. 2024. *Unit-3_Multiple Access and VSAT Systems.pptx* [online]. Available at: https://www.slideshare.net/slideshow/unit3multiple-access-and-vsat-systemspptx/266885232 Accessed: June 2024.

[12] Geeksforgeeks. 2024. *CDMA Full Form* [online]. Available at: https://www.geeksforgeeks.org/cdma-full-form/?ref=lbp Accessed: May 2024.

[13] SUN Jiyin, FU Guangyuan, CHE Xiaochun. 2009. Tactical Link Technology and System. In: *National Defense Industry Press*, Beijing.

[14] ZHOU De-min, LIU Yun-jiang and LI Man. 2015. A Dynamic TDMA Protocol Utilizing Channel Sense. In: *International Conference on Electromechanical Control Technology and Transportation (ICECTT)*, Zhuhai City, pp.226-231. October 31. Available at: https://doi.org/ 10.2991/icectt-15.2015.44.

[15] LI Xiyang, FAN Pingzhi. 2014. Design and analysis of multi-channel MAC scheduling code for mobile ad -hoc network. *Journal on Communications*, 35(5), p.57-64.

[16] H. Zimmermann. 2003. OSI Reference Model - The ISO Model of Architecture for Open Systems Interconnection. *IEEE Transactions on Communications*, 28(4), pp. 425-432. Available at: https://doi.org/10.1109/TCOM.1980.1094702.

[17] Shuai Li, Stephane Rubini, Frank Singhoff, Michel Bourdelles. 2014. Scheduling Analysis of TDMA-Constrained Tasks: Illustration with Software Radio Protocols. In: *2014 IEEE Intl Conf on High Performance Computing and Communications, 2014 IEEE 6th Intl Symp on Cyberspace Safety and Security, 2014 IEEE 11th Intl Conf on Embedded Software and Syst (HPCC,CSS,ICESS)*, Paris, August 20. Available at: https://doi.org/10.1109/HPCC.2014.90.

[18] N. Malcolm, W. Zhao. 1994. The timed-token protocol for real-time communica-tions. *Computer,* 27(1), pp. 35-41. Available at: https://doi.org/10.1109/2.248878.

[19] L. Sha, R. Rajkumar, J. Lehoczky. 1990. Priority inheritance protocols: an approach to real-time synchronization. *IEEE Transactions on Computers,* 39 (9), pp.1175-1185. Available at: https://doi.org/ 10.1109/12.57058 .

[20] Miroslav M. Lazi, Dragana J. Petrovi. 2010. SNMP u sistemu za daljinski nadzor I upravljanje – SDNU. In: *18. Telekomunikacioni forum TELFOR 2010*, Belgrade, pp.827-830. Novembar 23.

[21] Site24x7. 2024. *What is SNMP?* [online]. Available at: https://www.site24x7.com/network/what-is-snmp.html Accessed: May 2024.

[22] Noction. 2024. *SNMP evolution and version differences. SNMP security models/levels details.* [online]. Available at: https://www.noction.com/blog/snmp-versions-evolution-security Accessed: May 2024.

[23] Dpstele. 2024. *What is SNMPv1, SNMPv2c, and SNMPv3?* [online]. Available at: https://www.dpstele.com/snmp/v1-v2c-v3-difference.php Accessed: May 2024.

[24] Wbgroup 2024. *RRC radios F@STNET family* [online]. Available at: https://www.wbgroup.pl/app/uploads/2017/06/rrc_fastnet_eng_2-1q03.pdf Accessed: June 2024.