	УНИВЕРЗИТЕТ У НОВОМ САДУ ● **ФАКУЛТЕТ ТЕХНИЧКИХ НАУКА** 21000 НОВИ САД, Трг Доситеја Обрадовића 6	Датум: **31.7.2014.**
	ЗАДАТАК ЗА ИЗРАДУ ДИПЛОМСКОГ (BACHELOR) РАДА	Лист/Листова: 1/1

(Податке уноси предметни наставник - ментор)

Врста студија:	☒ Основне академске студије ☐ Основне струковне студије
Студијски програм:	**Рачунарство и аутоматика**
Руководилац студијског програма:	**проф. др Никола Јорговановић**

Студент:	**Александар Зељковић**	Број индекса:	**E13582**
Област:	**Рачунарска техника и рачунарске комуникације**		
Ментор:	**др Илија Башичевић**		

НА ОСНОВУ ПОДНЕТЕ ПРИЈАВЕ, ПРИЛОЖЕНЕ ДОКУМЕНТАЦИЈЕ И ОДРЕДБИ СТАТУТА ФАКУЛТЕТА ИЗДАЈЕ СЕ ЗАДАТАК ЗА ДИПЛОМСКИ (Bachelor) РАД, СА СЛЕДЕЋИМ ЕЛЕМЕНТИМА:

- проблем – тема рада;
- начин решавања проблема и начин практичне провере резултата рада, ако је таква провера неопходна;
- литература

НАСЛОВ ДИПЛОМСКОГ (BACHELOR) РАДА:

РЕАЛИЗАЦИЈА ПРОТОТИПА SAT2IP ПОСЛУЖИОЦА КОЈИ ПОДРЖАВА ЗАШТИТУ ДИСТРИБУИРАНИХ ДИГИТАЛНИХ САДРЖАЈА

ТЕКСТ ЗАДАТКА:

Основа за реализацију овог задатка је SAT2IP послужилац, развијен на истраживачком институту RT-RK. Дати систем подржава SAT2IP стандард верзија 1.2 и омогућава дистрибуцију телевизијских програма преко IP мреже. У тој верзији стандарда нису специфицирани механизми за заштиту дистрибуираног садржаја. Циљ задатка је да се прошири постојећи SAT2IP послужилац подршком за DTCP протокол којим се штити дистрибуирани садржај на деоници од SAT2IP послужиоца до корисничког уређаја. DTCP је протокол за управљање приступом дигиталним садржајима који спречава неовлашћени приступ (копирање итд.) заштићеним дигиталним садржајима. Према овом протоколу две стране у комуникацији (послужилац и кориснички уређај) периодично размењују кључеве којима се шифрује садржај који се преноси по комуникационом каналу који користе. Протокол користи AES-128 алгоритам за шифровање.

Руководилац студијског програма:	Ментор рада:

Примерак за: ☐ - Студента; ☐ - Ментора

УНИВЕРЗИТЕТ У НОВОМ САДУ
ФАКУЛТЕТ ТЕХНИЧКИХ НАУКА У НОВОМ САДУ

Александар Зељковић

Реализација прототипа SAT2IP послужиоца који подржава заштиту дистрибуираних дигиталних садржаја

ДИПЛОМСКИ РАД
- Основне академске студије -

Нови Сад, јул 2014

УНИВЕРЗИТЕТ У НОВОМ САДУ ● **ФАКУЛТЕТ ТЕХНИЧКИХ НАУКА**
21000 НОВИ САД, Трг Доситеја Обрадовића 6

КЉУЧНА ДОКУМЕНТАЦИЈСКА ИНФОРМАЦИЈА

Редни број, **РБР**:		
Идентификациони број, **ИБР**:		
Тип документације, **ТД**:		Монографска документација
Тип записа, **ТЗ**:		Текстуални штампани материјал
Врста рада, **ВР**:		Завршни (Bachelor) рад
Аутор, **АУ**:		**Александар Зељковић**
Ментор, **МН**:		**Др Илија Башичевић**
Наслов рада, **НР**:		**Реализација прототипа SAT2IP послужиоца који подржава заштиту дистрибуираних дигиталних садржаја**
Језик публикације, **ЈП**:		Српски / латиница
Језик извода, **ЈИ**:		Српски
Земља публиковања, **ЗП**:		Република Србија
Уже географско подручје, **УГП**:		Војводина
Година, **ГО**:		**2014**
Издавач, **ИЗ**:		Ауторски репринт
Место и адреса, **МА**:		Нови Сад; трг Доситеја Обрадовића 6
Физички опис рада, **ФО**: (поглавља/страна/ цитата/табела/слика/графика/прилога)		**7/21/0/1/9/0/0**
Научна област, **НО**:		Електротехника и рачунарство
Научна дисциплина, **НД**:		Рачунарска техника
Предметна одредница/Кqучне речи, **ПО**:		**DRM, DTCP-IP, SAT2IP, криптографска заштита дигиталног садржаја**
УДК		
Чува се, **ЧУ**:		У библиотеци Факултета техничких наука, Нови Сад
Важна напомена, **ВН**:		
Извод, **ИЗ**:		**У овом раду је представљена реализација проширења SAT2IP послужиоца подршком за DTCP протокол којим се штити дистрибуирани садржај на деоници од SAT2IP послужиоца до корисничког уређаја.**
Датум прихватања теме, **ДП**:		
Датум одбране, **ДО**:		
Чланови комисије, **КО**:	Председник:	**др Јелена Ковачевић**
	Члан:	**др Милан Бјелица**
	Члан, ментор:	**др Илија Башичевић**

Потпис ментора

UNIVERSITY OF NOVI SAD ● **FACULTY OF TECHNICAL SCIENCES**
21000 NOVI SAD, Trg Dositeja Obradovića 6

KEY WORDS DOCUMENTATION

Accession number, **ANO**:			
Identification number, **INO**:			
Document type, **DT**:		Monographic publication	
Type of record, **TR**:		Textual printed material	
Contents code, **CC**:		Bachelor Thesis	
Author, **AU**:		**Aleksandar Zeljkovic**	
Mentor, **MN**:		**PhD Ilija Basicevic**	
Title, **TI**:		**Implementation of a SAT2IP server application which supports protection of distributed digital content**	
Language of text, **LT**:		Serbian	
Language of abstract, **LA**:		Serbian	
Country of publication, **CP**:		Republic of Serbia	
Locality of publication, **LP**:		Vojvodina	
Publication year, **PY**:		**2014**	
Publisher, **PB**:		Author's reprint	
Publication place, **PP**:		Novi Sad, Dositeja Obradovica sq. 6	
Physical description, **PD**: (chapters/pages/ref./tables/pictures/graphs/appendixes)		**7/21/0/1/9/0/0**	
Scientific field, **SF**:		Electrical Engineering	
Scientific discipline, **SD**:		Computer Engineering, Engineering of Computer Based Systems	
Subject/Key words, **S/KW**:		**DRM, DTCP-IP, SAT2IP, cryptographic protection of digital content**	
UC			
Holding data, **HD**:		The Library of Faculty of Technical Sciences, Novi Sad, Serbia	
Note, **N**:			
Abstract, **AB**:		**This paper describes implementation of a SAT2IP server extension which supports DTCP protocol that protects distributed digital content from SAT2IP server to consumer device.**	
Accepted by the Scientific Board on, **ASB**:			
Defended on, **DE**:			
Defended Board, **DB**:	President:	**PhD Jelena Kovacevic**	
	Member:	**PhD Milan Bjelica**	Menthor's sign
	Member, Mentor:	**PhD Ilija Basicevic**	

SADRŽAJ

SPISAK SLIKA

SPISAK TABELA

SKRAĆENICE

AES - *Advanced Encryption Standard*, Napredni enkripcioni standard

AKE - *Authentication Key Exchange*, Razmena ključeva za autentifikaciju

API - *Application Programming Interface*, Aplikativna programska sprega

CA - *Conditional Access*, Uslovni pristup

CHAL - *Comedia Hardware Abstraction Layer*, Comedia sloj za apstrakciju hardvera

DRM - *Digital Rights Management*, Upravljanje digitalnim pravima

DTCP - *Digital Transmission Content Protection*, Zaštita digitalno prenošenog sadržaja

DTLA - *Digital Transmission Licensing Administrator*, Administrator za licenciranje digitalnog prenosa

DVB-S - *Digital Video Broadcasting* — Satellite, Digitalno video emitovanje - satelit

EMI - *Encryption Mode Indicator*, Indikator moda enkripcije

FTA - *Free To Air*, Slobodno za emitovanje

HTTP - *Hyper Text Transfer Protocol*, Protokol za prenos hiper-teksta

IP - *Internet Protocol*, Internet protokol

RTP - *Real-time Transport Protocol*, Protokol za transport u realnom vremenu

RTSP - *Real Time Streaming Protocol*, Protokol za emitovanje u realnom vremenu

SRM - *System Renewability Messages*, Poruke za obnavljanje sistema

UDP - *User Datagram Protocol*, Protokol korisničkog datagrama

1. Uvod

Poslednjih par decenija došlo je do ogromnog razvoja u domenu multimedijalnih sistema kao i televizije kao najrasprostranjenijeg načina za plasiranje multimedijalnog sadržaja. Zadnjih nekoliko godina došlo je i do velikog napretka u oblasti digitalizacije televizijskog signala, što je otvorilo mogućnost slanja veće količine podataka transportnim tokovima, mogućnost prenosa dodatnih podataka kao što su dodatne informacije o kanalima i emisijama, različite korisničke aplikacije pa čak i mogućnost reprodukcije delova programa koji su se već emitovali ili koji će tek da se emituju.

Još jedna vrlo bitna grana razvoja televizije je mogućnost reprodukcije programa na uređajima koji nisu televizori, kao na primer računari, tableti i mobilni telefoni ali i proširivanje spektra funkcionalnosti televizora, koji su dobili operativne sisteme, mogućnost izvršavanja aplikacija pisanih za druge uređaje, mogućnost internet konekcije itd. Samim tim funkcionalnost televizora se znatno približila funkcionalnosti računara i omogućila razne pogodnosti koje nude računari, kao što su to, već pomenuto, izvršavanje aplikacija, ali i komunikacija između uređaja.

Jedan od protokola koji koriste ove pogodnosti je upravo Sat2IP protokol. To je komunikacioni protokol koji služi za distribuciju satelitskog programa preko IP mreže. Njegova uloga je da korisnicima u određenom objektu (kući, kancelariji, školi itd) obezbedi reprodukciju satelitske televizije koju bi korisnici vrlo lako mogli da koriste pomoću uređaja koji podržavaju mrežnu komunikaciju, kao što su računar, televizor, tablet itd.

Ovaj ubrzani razvoj i digitalizacija televizije, povećanje spektra uređaja koji podržavaju reprodukciju, kao i razvoj komunikacije između tih uređaja otvorio je novo pitanje – pitanje zaštite sadržaja koji nije namenjen slobodnom emitovanju.

Od mnogih standarda koji omogućavaju zaštitu od neovlašćenog pristupa, kao vrlo pogodan na primenu u Sat2IP protokolu izdvojio se DTCP standard. DTCP je tehnologija za upravljanje digitalnim pravima (DRM) koja ima zadatak da šifruje prenosni tok između kućnih multimedijalnih uređaja kao što su televizori, računari, CD I DVD plejeri itd.

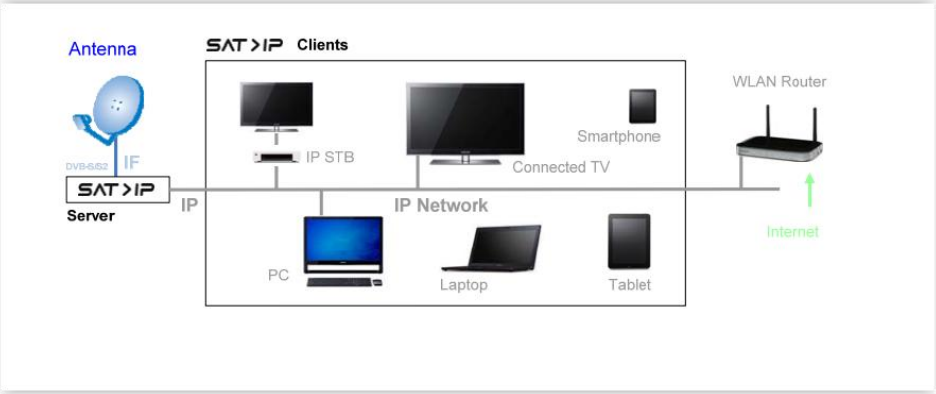
U okviru ovog rešenja realizovano je jedno rešenje implementacije DTCP zaštitnog protokola u Sat2IP protokol. Cilj zadatka je proširivanje postojećeg Sat2IP poslužioca razvijanog na institut RT-RK, podrškom za DTCP protokol na relaciji poslužilac – korisnički uređaj (*source - sink*). Te dve strane periodično razmenjuju ključeve koji služe za šifrovanje sadržaj koji se prenosi preko komunikacionog kanala .

2. Teorijske osnove

U ovom poglavlju biće opisane osnove Sat2IP i DTCP protokola.

2.1 Sat2IP protokol

Sat2IP predstavlja arhitekturu za prijem i distribuciju satelitske televizije bazirana na IP protokolu. Uloga Sat2IP protokola je da primi satelitski DVB-S/S2, da demoduliše signal i da ga konvertuje u signal koji se prenosi IP mrežom. Sat2IP je klijent – server arhitektura, gde klijent pruža mogućnost odabira prijema nekog satelitskog programa, dok server odgovara na zadati zahtev i klijentu prosleđuje traženi televizijski signal u standardom definisanom formatu[1].
U suštini, Sat2IP server uklanja DVB-S/S2 sloj iz primljenog signala i menja ga sa IP transportnim slojem. Posle ove konverzije satelitski program je moguće distribuirati posredstvom IP mreže, kablom ili bežično.



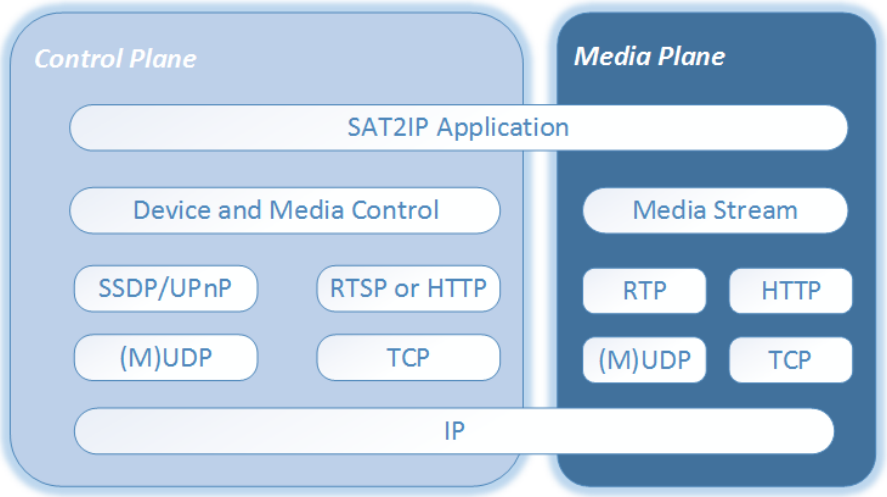
Slika 1: Primer jednog Sat2IP sistema [1]

U Sat2IP-u se koriste sledeći protokoli:

1) UPnP – za adresiranje, otkrivanje i opis uređaja
2) RTSP ili HTTP za kontrolu
3) RTP ili HTTP za transport

Sat2IP protokol stek je dobro organizovan i podeljen je na dve oblasti(slika 2):

- kontrolna oblast
- oblast za upravljanje medijom



Slika 2: Sat2IP protokol stek [1]

Server podržava unicast ili multicast RTP/UDP prenos, kao i HTTP prenos.

Sat2IP uređaji se međusobno identifikuju pomoću UPnP standarda, dok se kontrola toka vrši pomoću RTSP ili HTTP standarda. RTSP upiti se koriste za zahtev RTP unicast ili multicast toka, dok se HTTP upiti koriste za zahtev HTTP toka[2].

Primer RTSP upita:

```
http://192.168.234.43:8080/?src=1&sr=22000&freq=11302&pol=h&fec=23
&msys=dvbs2&mtype=8psk&ro=0.20&pids=109,3583,3587,0
```

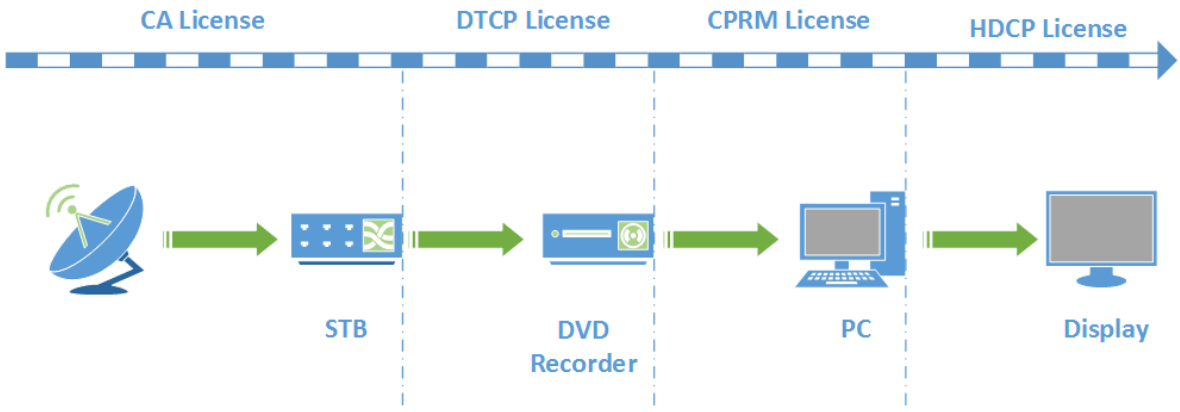
Primer HTTP upita:

```
http://192.168.227.38:8080/?msys=dvbs&src=1&freq=10744&pol=h&sr=22000&
fec=56&mtype=qpsk&pids=0,300,301,302,304
```

Što se tiče prava pristupa emitovanom signalu, Sat2IP je moguće koristiti u okruženjima sa dozvoljenom reprodukcijom (FTA – Free To Air) kao i u okruženjima sa ograničenom reprodukcijom (CA - Conditional Access). Mnogi mrežni uređaji i postojeći Set-Top Box uređaji mogu da se podese za SAT2IP prijem jednostavnom nadogradnjom softvera.

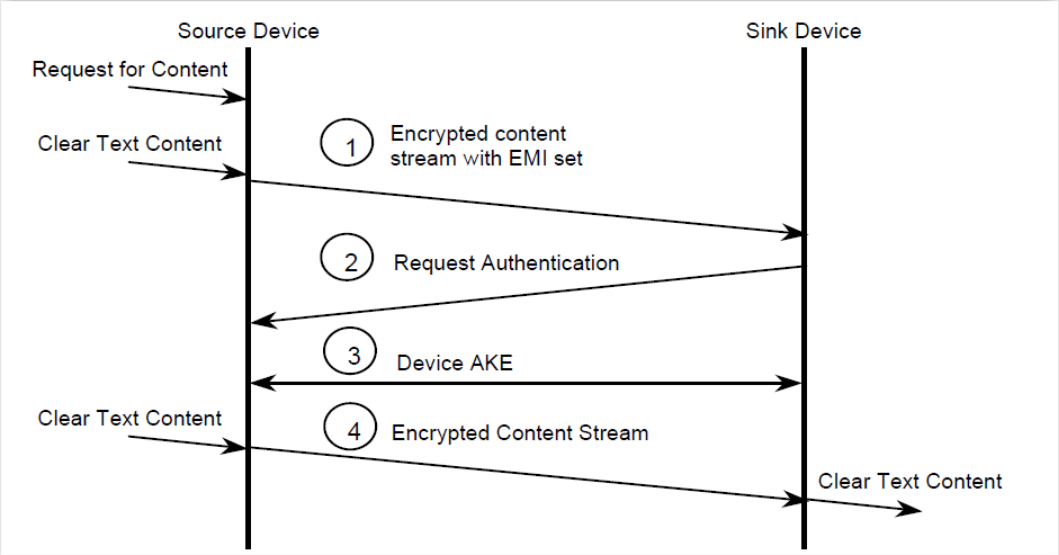
2.2 DTCP protokol

DTCP (Digital Transmission Content Protection) je tehnika za upravljanje digitalnim pravima (DRM – Digital Rights Management) čiji je glavni cilj ograničavanje razmene sadržaja između kućnih multimedijalnih uređaja kao što su npr. televizori, CD i DVD plejeri, korišćenjem šifrovanog sadržaja koji se razmenjuje između uređaja. Standard je nastao 1998. godine kao proizvod saradnje kompanija Hitachi, Intel, Matsushita, Sony i Toshiba u nameri da ustanove standard za zaštitu toka podataka. Zbog navedenih 5 kompanija koje su ga ustanovile, ovaj standard je još poznat i pod imenom "5C".



Slika 3: Opseg primene DTCP standarda [3]

DTLA specifikacija definiše dva uređaja u sistemu a to su *source* – izvor digitalnog sadržaja, i s*ink* – uređaj koji prima sadržaj. Pre bilo kakve razmene sadržaja vrši se autentifikacija uređaja, razmena ključeva i poruka za autentifikaciju. Ukoliko su uređaji uspešno izvršili autentifikaciju i razmenu ključeva, kreće se sa šifrovanjem i razmenom sadržaja. U slučaju da multimedijalni sadržaj nije zaštićen on se direktno razmenjuje upotrebom HTTP protokola. Šifrovanje sadržaja se vrši na izvoru digitalnog sadržaja, zatim se taj sadržaj šalje, a dešifrovanje se radi na strani uređaja koji prima sadržaj. Šifrovanje i dešifrovanje sadržaja se vrše pomoću AES-128 standarda.



Slika 4: Autentifikacija uređaja [4]

Vlasnicima sadržaja DTCP ostavlja mogućnost da odrede na koji način će se koristiti sadržaj koji se emituje. Ovo je urađeno pomoću EMI (Encryption Mode Indicator) parametra koji se nalazi u zaglavlju paketa podataka I može da ima sledeća značenja u zavisnosti od vrednosti bita:

- **11** *copy-never* – kopiranje sadržaja nije dozvoljeno
- **10** *copy-one-generation* – kopiranje sadržaja dozvoljeno jednu generaciju
- **01** *no-more-copies* – već izvršeno copy-one-generation kopiranje
- **00** *copy-free* – slobodno za kopiranje

Uređaji koji podržavaju potpunu autentifikaciju (*Full Authentication*) mogu da prime i obrade SRM (*System Renewability Messages*) poruke . SRM poruke se razmenjuju u okviru AKE-a. Ove poruke kreira DTLA organizacija i distribuira ih kroz nove uređaje. Razmenom SRM poruka obezbeđuje se dugoročni integritet sistema, tj. vrši se opozivanje kompromitovanih uređaja. Na ovaj način se obezbeđuje da samo licencirani uređaji imaju pristup zaštićenom sadržaju i da se uređaji koji ne podržavaju uslove propisane DTLA specifikacijom izbace iz upotrebe [7].

3. Koncept rešenja

U okviru ovog poglavlja data je analiza problema, pregled algoritma, po kom rešenje funkcioniše, kao i diskusija problema, koje je neophodno rešiti.

3.1 Analiza problema

Realizacija ovog zadatka se zasniva na Sat2IP poslužiocu, razvijanom na istraživačkom institutu RT-RK. Dati sistem podržava Sat2IP standard verzija 1.2 i omogućava distribuciju televizijskih programa preko IP mreže. U datoj verziji Sat2IP poslužioca nisu implementirani mehanizmi za zaštitu distribuiranog sadržaja.

DTCP zaštitni protokol koji je potrebno implementirati u Sat2IP poslužilac je takođe razvijan na istraživačkom institutu RT-RK. DTCP je protokol za upravljanje pristupom digitalnim sadržajima koji sprečava neovlašćeni pristup (kopiranje,reprodukcija itd.) zaštićenim digitalnim sadržajima. Prema ovom protokolu dve strane u komunikaciji (poslužilac i korisnički uređaj) periodično razmenjuju ključeve kojima se šifruje sadržaj koji se prenosi po komunikacionom kanalu koji koriste. Takođe, povremeno se proverava i autentičnost uređaja sa kojim se komunicira kako ne bi došlo do neželjenog pristupa prenosnom toku. Protokol koristi AES-128 algoritam za šifrovanje.

Cilj ovog zadatka je da se proširi postojeći Sat2IP poslužilac podrškom za DTCP protokol kojim se štiti distribuirani sadržaj na relaciji Sat2IP poslužilac (*source*) - korisnički uređaj (*sink*).

3.2 SAT2IP TB100 aplikacija

Aplikacija se sastoji iz šest niti (*threads*). Imena niti kao i njihov kratak opis su dati u sledećoj tabeli:

Naziv niti:	Opis niti:
TDAL_Init + TKEL_Init	Veza između srednjeg sloja i drajvera.
TDAL_DMD_Init	Aktivna tokom tune-ovanja na server.
main	Prima komande iz komandne linije.
UPnP	Nit potrebna UPnP biblioteci.
SatIpStreamNew	Nit za slanje toka za svakog klijenta + još jedna nit koja prihvata novu sesiju.
httpThread	Čita podatke sa tjunera i šalje pokazivač na podatke *SatIpStreamNew* niti.

Tabela 1: Niti u Sat2IP aplikaciji

Sat2IP server je organizovan u 5 slojeva [8]:

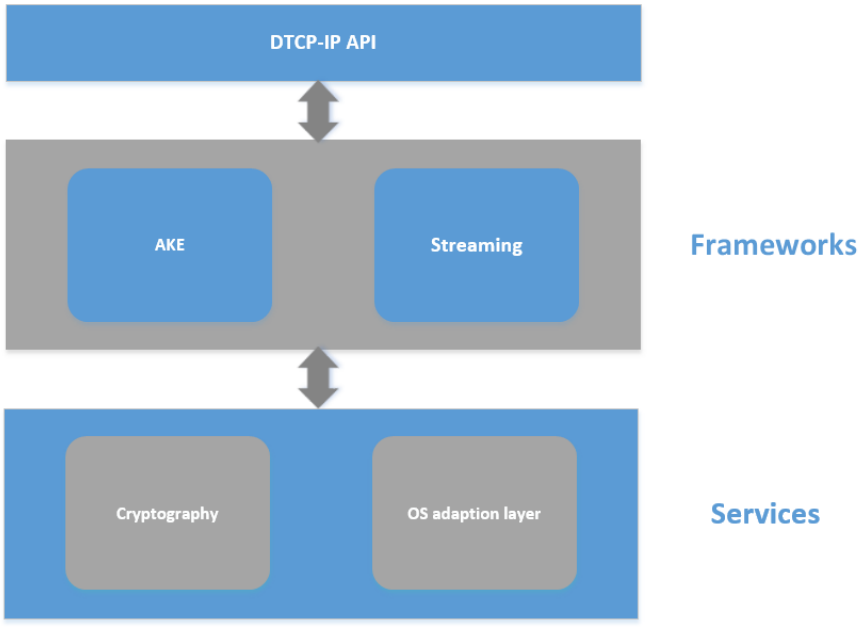
- Aplikativni sloj sa komandnom linijom
- Sat2IP srednji sloj koji implementira Sat2IP protokol i šalje transportni tok prema povezanim IP klijentima. Server koristi lib_UPnP biblioteku za postupak otkrivanja uređaja.
- CHAL (Comedia Hardware Abstraction Layer) – sloj za apstrakciju hardvera
- Platformski API koji implementira TB100 biblioteku
- TB100 hardverska emulacija potrebna za rad aplikacije na PC Linux-u

Premeštanje aplikacije na drugu platformu zahteva promenu adaptivnog sloja, dok se za rad aplikacije na bilo kojoj platformi osim PC Linux-a, sloj sa TB100 hardverskom emulacijom uklanja. Što se tiče implementacije DTCP-a u Sat2IP, za realizaciju datog zadatka korištena su dva Sat2IP sloja: Sat2IP srednji sloj i CHAL.

Deo za prihvatanje sertifikata od strane uređaja koji prima sadržaj kao i razmenu ključeva i autentifikaciju je realizovan u Sat2IP sloju. Odmah po pokretanju serverske aplikacije čeka se sertifikat nekog klijent uređaja, i po njegovom prijemu i proveri, započinje razmena ključeva. To znači da nijedan uređaj koji nije autentifikovan neće moći da komunicira sa serverom, i da je jedina poruka na koju će server da odgovori biti DTCP sertifikat nekog uređaja.

Što se tiče enkripcije, odnosno šifrovanja multimedijalnog toka, ona se vrši nešto niže i ona je smeštena u CHAL sloj. U okviru funkcije koja čita prenosni tok u demodulatoru, implementirane su funkcije za DTCP zaštitu koje vrše pripremu i enkripciju.

3.3 DTCP-IP aplikacija



Slika 5: DTCP-IP protokol stek

DTCP-IP aplikacija se sastoji iz tri celine [9]:

- API sloj koji omogućava korišćenje funkcionalnosti DTCP-IP biblioteke njenim korisnicima.
- Sloj okvira koji sadrži implementacije DTCP-IP specifičnih funkcionalnosti. Ovaj sloj sadrži dva podokvira:
  - AKE – sadrži podršku za autentifikaciju i razmenu ključeva
  - Streaming – sadrži podršku za slanje HTTP i RTP toka
- Servisni sloj koji sadrži najniže funkcionalnosti potrebne sloju okvira da bi radio. Ovaj sloj takođe sadrži dva podokvira:
  - Cryptography – sadrži kriptografske primitive potrebne za DTCP-IP
  - OS Adaptation layer – sadrži servise specifične za operativni sistem koje zahteva DTCP-IP

DTCP-IP funkcionalnosti su bazirane na kriptografskom sistemu eliptične krive (*ECC - Elliptic Curve Cryptography*). Za ovu svrhu se koristi OpenSSL biblioteka (*libcrypto*).

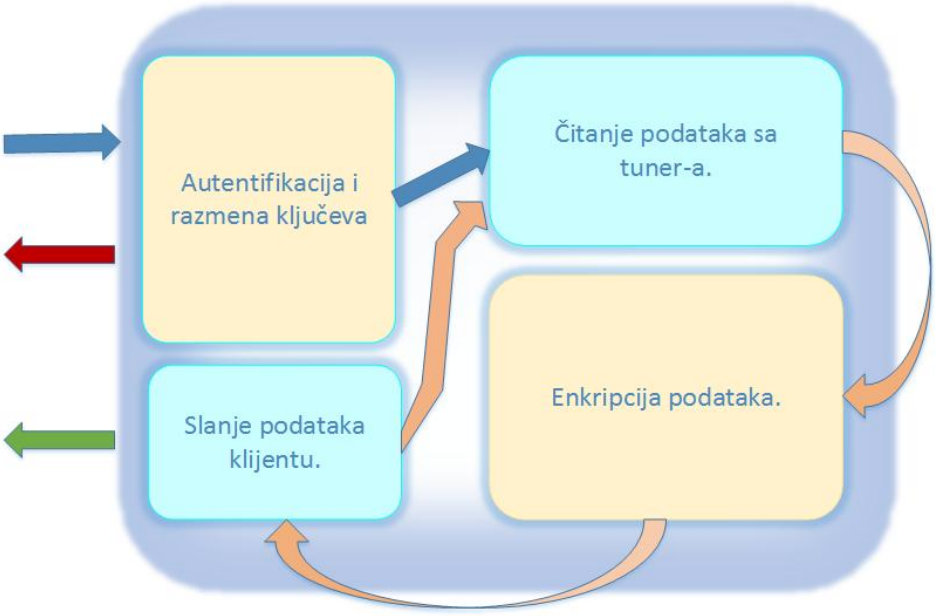
Modul kriptografije podržava sledeće kriptografske funkcionalnosti:

1. SHA-1 - algoritam koji se koristi u DSS-u (*Digital Signature Standard*), za generisanje digitalne poruke.
2. RNG – generator slučajnog broja.
3. ECC sistem se koristi kao osnova za EC-DH (*Diffie-Hellman*) i EC-DSA (*Digital Signature Algorithm*) algoritme. EC-DSA algoritam se koristi za kreiranje potpisa i za njegovu verifikaciju tj. proveru.
4. EC-DH algoritam se koristi kako bi se izračunala vrednost Diffie-Hellman-ove prve faze, a na osnovu vrednosti prve faze, računa se tajna deljena vrednost koja se strogo čuva i koristi dalje u algoritmu prilikom autentifikacije i razmene ključeva.
5. EC-DSA javni ključ - javni ključ uređaja se koristi prilikom autentifikacije uređaja, odnosno prilikom verifikacije DTLA potpisa na podatke. Javni ključ je kreiran od strane DTLA organizacije i dodeljuje se svakom kompatibilnom uređaju.
6. AES-128 algoritmom vrši se šifrovanje nad blokovima podataka veličine 128 bita i pri tom se upotrebljava ključ za šifrovanje veličine 128 bita.

4. Programsko rešenje

U ovom poglavlju dat je prikaz modularne strukture rešenja sa detaljnom analizom realizovanih modula.

4.1 Moduli i njihove funkcije



Slika 6: Blok dijagram sistema

Cilj implementacije DTCP-a u postojeći Sat2IP protokol je zaštita izvora digitalnog sadržaja od neovlašćenog pristupa nekog uređaja koji prima sadržaj kao i zaštita digitalnog

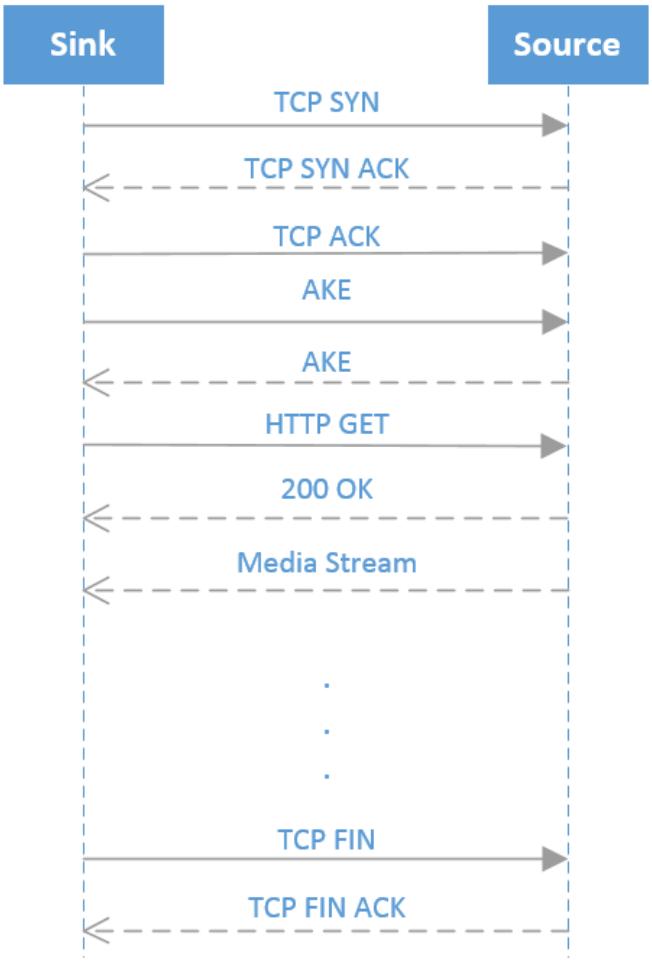
prenosnog toka koji bi mogao da bude presretnut i reprodukovan ili umnožen bez dozvole. Upravo zbog ovoga, u Sat2IP je bilo potrebno implamantirati dva zaštitna modula:

1) Modul za autentifikaciju i razmenu ključeva
2) Modul za enkripciju podataka

Kada se pokrene server i uređaj koji prima sadržaj pokuša da mu pristupi, prvo što će biti potrebno da se pošalje (osim sinhronizacionih poruka) je jedinstveni sertifikat uređaja koji prima sadržaj. Ni jedna druga poruka osim ove neće biti prihvaćena od strane servera, što znači da server neće prihvatiti komunikaciju ni sa jednim uređajem koji nema DTCP sertifikat. Ako se utvrdi da je sertifikat validan, prelazi se na postupak razmene ključeva pomoću kojih, pomoću kojih će se kasnije šifrovati podaci.

Posle ovoga, server je potvrdio autentičnost drugog uređaja, i prelazi se na šifrovanje toka. Šifrovanje se vrši prilikom čitanja podataka sa demodulatora, i ti šifrovani podaci se identično kao i nešifrovani prosleđuju funkciji za slanje i zatim šalju uređaju koji prima sadržaj. Ukoliko se utvrdi da sertifikat nije ispravan, da postoji problem sa ključevima ili da je ključ uređaja na neki način kompromitovan, automatski se prekida sesija, i sever se vraća u stanje čekanja sledećeg sertifikata.

Jednostavnost i modularnost serverske aplikacije su ostali očuvani nakon implementacije DTCP-a. Za instaliranje aplikacije u sistem potrebno je obezbediti određene biblioteke, dok je samo pokretanje i upravljanje ostalo na vrlo jednostavnom nivou uz pomoć konzolne aplikacije. Ukoliko se javi potreba za korišćenjem servera bez podrške za enkripciju, ta opcija se vrlo lako obezbeđuje tako što se zakomentariše DTCP_IP fleg i izbilduje aplikacija.



Slika 7: Komunikacija između uređaja koji prima sadržaj i izvora digitalnog sadržaja

4.2 Modul za autentifikaciju i razmenu ključeva

Modul je implementiran u okviru funkcije `SatIpSrvRun()` koja služi za pokretanje servera i sastoji se od sledećih funkcija:

`dtcp_ip_init(void)` – Funkcija koja vrši inicijalizaciju DTCP-a. Poziva se samo jednom, i potrebno ju je pozvati pre upotrebe bilo koje druge DTCP funkcije.

`dtcp_ip_source_create(dtcp_ip_source_t* source)` – Kreira izvor digitalnog sadržaja. Vraća parameter "source" koji predstavlja referencu na handler.

`dtcp_ip_source_start(dtcp_ip_source_t source, char* host, int port)` – Startuje prethodno kreirani izvor digitalnog sadržaja. Kao ulazno-izlazni parameter prima referencu na handler, dok kao ulazne parameter prima još i IPv4 adresu hosta, kao i DTCP port koji mora da u bude u opsegu od 0 do 65535.

`dtcp_ip_source_stop(dtcp_ip_source_t source)` – Funkcija se poziva prilikom zaustavljanja Sat2IP server, zaustavlja DTCP-IP izvor digitalnog sadržaja.

4.3 Modul za enkripciju podataka

Funkcije za inicijalizaciju i deinicijalizaciju ovog modula se nalaze u *satip_stream* modulu Sat2IP servera. Inicijalizacija se vrši u sklopu funkcije `SatIpStreamNew(int isRtsp)` koja služi za kreiranje novog toka podataka, dok se deinicijalizacija vrši u sklopu funkcije `SatIpStreamDelete(SatIpStream* stream)` koja služi za brisanje toka. Funkcije koje vrše neophodna izračunavanja za enkripciju i samu enkripciju smeštene su u modul *tdal_dmd_pc_hard* tj. njegovu funkciju za čitanje podataka `tTDAL_DMD_Read(void *tuner, void *buf, int size)`. Modul čine sledeće funkcije:

`dtcp_ip_http_enc_create(dtcp_ip_source_t source, dtcp_ip_stream_t *stream, dtcp_stream_params_t *params)` – kreira hendler za HTTP enkripciju. Osim *source* i *stream* hendlera, ova funkcija prima još i struktura sa neophodnim parametrima, koja sadrži EMI (Encryption Mode Indicator), veličinu toka, kao i IPv4 adresu hosta.

`dtcp_ip_http_enc_out_len(dtcp_ip_source_t source, dtcp_ip_stream_t stream, size_t in_len, size_t *out_len, size_t *handled_len)` – izračunava veličinu izlaznog bafera za zadatu ulaznu veličinu. Ovu funkciju je neophodno pozvati pre enkripcije kako bi vratila tačnu veličinu izlaznog bafera pomoću koje bi se alocirala memorija neophodna za enkriptovani sadržaj.

`dtcp_ip_http_enc(dtcp_ip_source_t source, dtcp_ip_stream_t stream, char* peer_addr, void* in_data, size_t in_len, void* out_data, size_t *out_len, size_t *encrypted)` – enkriptuje ulzne podatke i priprema ih za HTTP prenos.

`dtcp_ip_http_enc_destroy(dtcp_ip_source_t source, dtcp_ip_stream_t stream)` - uništava hendler za HTTP enkripciju.

5. Testiranje i verifikacija

Ovo poglavlje se detaljno bavi opisom testiranja i verifikacije datog rešenja.

5.1 Testiranje realizovanog rešenja

Kao što je navedeno u prethodnom poglavlju, u Sat2IP su implementirana dva modula za zaštitu sadržaja: modul za autentifikaciju i razmenu ključeva i modul za enkripciju podataka. Struktura programa omogućava nezavisno testiranje ova dva modula.

Za njihovo testiranje korišćen je testni program uređaja koji prima sadržaj razvijan na institutu RT-RK, ranije korišćen za njihove potrebe. Taj program simulira neki Sat2IP klijent koji u sebi ima integrisanu DTCP-IP podršku i povezuje se na Sat2IP poslužilac autentifikuje se, i zahteva enkriptovani video sadržaj. Kada primi sadržaj, dekriptuje ga i tako dekriptovan video smešta u izlaznu datoteku *out.mpg*, koji je kasnije moguće reprodukovati putem VLC plejera [8], ili nekog drugog podržanog programa za reprodukciju video sadržaja.

Program se pokreće putem komandne linije, a prilikom pokretanja potrebno mu je zadati dva parametra:

1) HTTP upit, koji u sebi sadrži informacije neophodne za povezivanje na izvor digitalnog sadržaja kao i informacije o kanalu na koji uređaj koji prima sadržaj želi da se zakači
2) DTCP prolaz – broj u opsegu od 0 do 65535 koji mora da podržava poslužilac

Ukoliko jedan od ova dva parametra nije zadat u odgovarajućem formatu, uređaj koji prima sadržaj će izbaciti grešku i korisniku će dati primer pravilnog formatiranja parametara.

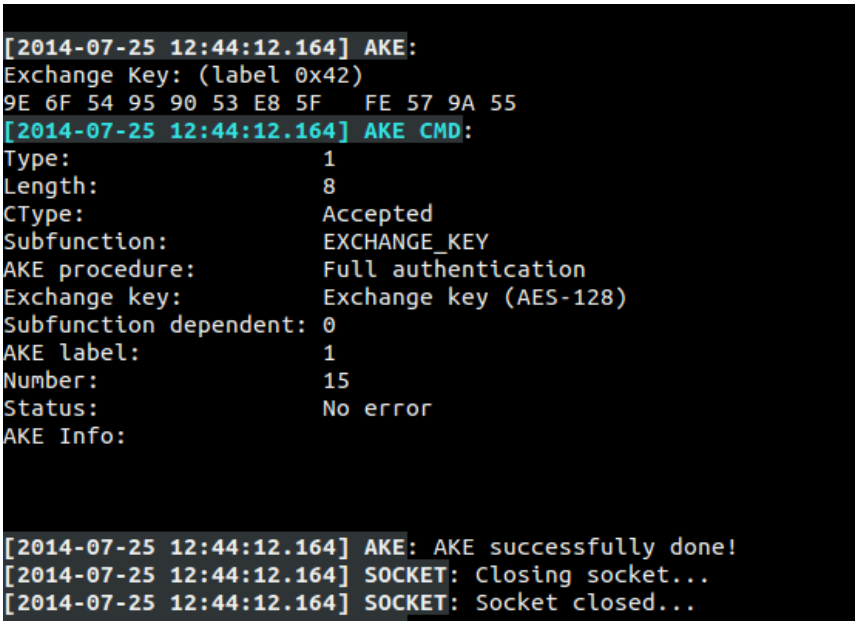
Što se hardverske podrške prilikom testiranja tiče, osim računara na kom su se pokretale aplikacije koje su simulirale izvor digitalnog sadržaja i uređaj koji prima sadržaj, bio je potreban i hardver za prijem satelitskog signala. Ovu funkciju je vršio prijemnik satelitskog signalaTT-connect, model S2-3600. Ovaj prijemnik podržava DVB-S i DVB-S2 satelitske standarde, čiji signal prima putem antenskog priključka, i vrlo lako se povezuje sa računaraom preko USB priključka.

Slika 8: TT-connect S2-3600 prijemnik satelitskog signala [5]

5.2 Testiranje modula za autentifikaciju i razmenu ključeva

Razmena ključeva i autentifikacija predstavljaju proces koji je jednoznačan i tačno određen pa stoga testiranje ovog modula nema puno različitih scenarija. U Sat2IP serveru se eksplicitno zadaju vrednosti ključeva potrebnih za razmenu, kako bi razmena mogla da se testira. Prilikom pokretanja servera, čeka se sertifikat i ključevi aplikacije uređaja koji prima sadržaj, i kada ih primi, i jedna i druga strana će da ispisuju tok razmene ključeva. Ukoliko dođe do problema prilikom razmene kao npr. problem sa sertifikatom ili ključem, preveliko čekanje na ključ i slično, doći će do prekida autentifikacije sa obe strane, i na konzoli će biti ispisana poruka o

neuspešnoj autentifikaciji. Sa druge strane, ukoliko se autentifikacija obavi uspešno, biće prikazana poruka o uspešnoj razmeni, kao i celokupan tok razmene ključeva.



Slika 9: Primer uspešne autentifikacije

5.3 Testiranje modula za enkripciju podataka

Testiranje modula za enkripciju podataka se svodi na proveru izlazne datoteke out.mpg koji posle dekripcije izbacuje uređaj koji prima sadržaj. Prilikom vizuelne provere ove datoteke mogli su se primetiti određeni deformiteti slike (postojanje artefakta), kao i prekidanja zvuka.

Kako je izlaznu datoteku bilo potrebno uporediti sa nekom referentnom datotekom, što nije bilo moguće učiniti pri upotrebi sadržaja satelitske televizije, postavilo se pitanje kako serveru proslediti već postojeću datoteku, kako bi ista mogla da se uporedi sa izlazom izvora digitalnog sadržaja? Ovo pitanje je rešeno korišćenjem modulatora AT290USB kompanije Alitronika.

Slika 10: Alitronika AT290USB [6]

Ovaj uređaj služi za modulisanje transportnog toka sa računara ili nekog drugog izvora, i slanje modulisanog signala na bilo koji uređaj koji je DVB-S, DVB-S2 ili DVB-DSNG kompatibilan.

Uređaju je prosleđena video datoteka, koju je on modulisao i slao na testirani Sat2IP server, na koji se zatim povezao uređaj koji prima sadržaj, koji je preuzimao i dekriptovao dati tok. Dobijenu izlaznu datoteku smo zatim poredili sa datotekom koji smo prosledili modulatoru korišćenjem RT-Executor alata za poređenje razvijenog na institutu RT-RK. Softver za poređenje radi tako što prepoznaje pakete u jednoj ulaznoj datoteci, a zatim pretražuje drugu datoteku da bi pronašao te pakete. Rezultat testiranja datim programom je pokazao da su datoteke različite, pa je stoga urađena provera prenosnog toka na demodulatoru kako bi se otklonile sumnje da se na ulaz modula za enkripciju podataka dovodi signal koji je oštećen. Rezultat poređenja ovog signala i signala sa ulaza u modulator je pokazao da su signali identični, što je pokazalo da nije došlo do oštećenja signala pre ulaza na modulator.

Kako je deo za slanje podataka sa servera takođe uspešno prošao testiranje, uzrok problema sa signalom na serverskoj strani može da bude samo u okviru funkcija za enkriptovanje. Signal sa izlaza ovog modula nije imalo smisla skidati jer je bio enkriptovan, te se nikakvim poređenjem ne bi mogla utvrditi njegova ispravnost. Kao referentna implementacija je u zadatku iskorišćena starija verzija Sat2IP servera, takođe razvijena u RT-RK. Ta verzija koristi različitu (stariju) verziju DTCP biblioteke. Ispitivanjem je utvrđeno da i kod te verzije postoji isti problem - datoteka koja se šalje sa modulatora i datoteka koja je rezultat dekripcije su različite.

Urađena je još jedna provera, DTCP biblioteka korišćena u referentnoj implementaciji je integrisana u SAT2IP server korišćen u ovom zadatku i upoređena je tako dobijena izlazna (dekriptovana) datoteka, sa izlaznom datotekom referentne implementacije i utvrđeno je da sadrže iste pakete.

Ovi rezultati upućuju na postojanje problema ili u modulu za enkripciju ili aplikaciji za prijem sadržaja i potvrđuju da problem postoji i prilikom korišćenja referentne implementacije. Ove dve komponente su u zadatku korišćene kao gotove, unapred pripremljene komponente. Stoga analiza ove dve komponente ostaje kao zadatak daljeg razvoja.

6. Zaključak

U okviru rada realizovana je implementacija DTCP protokola za zaštitu distribuiranog sadržaja u postojeći Sat2IP poslužilac, čija je uloga distribucija satelitskog televizijskog programa preko IP mreže. Za izradu zadatka korišćena je SAT2IP-TB100 aplikacija i DTCP aplikacija razvijane na institutu RT-RK. Rešenje je realizovano kroz dva modula, modul za razmenu ključeva i modul za enkripciju toka. Implementacija DTCP-a nije uticala na prenosivost SAT2IP poslužioca, kao i na njegove performanse. Prilikom razvoja vođeno je računa o modularnosti implementacije, te je omogućeno da se u slučaju potrebe, ista može vrlo jednostavno ukloniti na određeno vreme i ponovo vratiti u sistem. Celokupna programska podrška je razvijena korišćenjem C programskog jezika, a za šifrovanje u okviru DTCP-a korišćen je algoritam AES-128.

Dalji razvoj ove implementacije može da obuhvati rešavanje problema sa izlaznom video datotekom. Mogući uzroci datog problema su neispravnost nekog modula za enkripciju ili dekripciju u okviru DTCP-a, neispravnost aplikacije uređaja koji prima sadržaj ili možda čak i neki problem u hardverskoj arhitekturi.

Takođe, mogla bi da se izvrši implementacija u slučaju kada na serveru postoji CAD/DRM algoritam koji će prvo da dekriptuje sadržaj sa satelita pa tek onda da ga enkriptuje DTCP-IP algoritmom i šalje klijentu, kao i pravljanje posebnog sloja za zaštitu sadržaja koji bi olakšao integraciju nekih drugih načina zaštite pored DTCP-IP-a.

Još jedan pravac u eventualnom daljem razvoju bi mogla da bude implementacija DTCP protokola u odgovarajući modul za prenos putem RTSP standarda, što bi zahtevalo samo dodavanje odgovarajućih funkcija za enkripciju, s obzirom da je modul za razmenu ključeva već uspešno implementiran.

7. Literatura

[1] SAT2IP White Paper: http://www.ses.com/11193301/SATIP-White-Paper.pdf

[2] SAT2IP Protocol Specification, Version 1.2: http://www.satip.info/sites/satip/files/resource/satip_specification_version_1_2.pdf

[3] CONTENT PROTECTION – Methods and Practices for protecting audiovisual content: http://parasam.me/2012/01/25/content-protection-methods-and-practices-for-protecting-audiovisual-content/

[4] 5C: Digital Transmission Content Protection Specification Volume 1(Informational Version) , Jun 2013

[5] http://www.adslgate.com/dsl/showthread.php?t=88681

[6] http://www.preciolandia.com/br/alitronika-at290usb-8qdgth-a.html

[7] Rade Vulin: Jedno rešenje realizacije programske podrške za zaštitu multimedijalnog sadržaja pomoću DTCP-IP protokola, MSc rad - FTN, april 2013

[8] VLC media player: http://www.videolan.org/vlc/