Uporaba Video over IP tehnologij in zaščita

Žana Juvan[1], Matevž Pogačnik[1], Klemen Pečnik[1]

[1]Univerza v Ljubljani, Fakulteta za elektrotehniko, Laboratorij za multimedijo, Tržaška cesta 25, 1000 Ljubljana
E-pošta: zana.juvan@ltfe.org, matevz.pogacnik@ltfe.org, klemen.pecnik@ltfe.org

Usage of Video over IP technologies and security

Abstract. *Rapid development of technology enables transferring video content through IP infrastructure. It is important to ensure proper protection of AV content, transmitted over IP networks in real time. This proves to be a challenge, since encryption should not introduce additional delays. The most commonly used encryption algorithm for protecting AV content is AES-128. This article presents environments and AV over IP technologies, as well as the possibilities for protecting the transmitted content and lastly the impact of encryption on processing time and performance and memory usage.*

1 Uvod

V videoprodukcijskih sistemih se vse pogosteje uveljavljajo sistemi, ki za prenos AV (Avdio Video) vsebin ne uporabljajo več namenskih vmesnikov in standardov kot npr. SDI (serijski digitalni vmesnik - ang. Serial Digital Interface), komponentnega, ali celo HDMI (ang. High-Definition Multimedia Interface), ampak IP (ang. Internet Protocol) arhitekturo in temu primerne IP standarde. Hiter razvoj IP tehnologij, standardov in protokolov omogoča uporabo IP infrastrukture za prenos profesionalnih AV vsebin. Pri tem se lahko uporabljajo popolnoma namenska omrežja brez povezave v javno omrežje, kot tudi obstoječa hibridna IP omrežja, kar zahteva različne prilagoditve in vse pogosteje tudi ustrezno zaščito vsebine. Zaščita AV vsebin v sistemih, kjer je zahtevana visoka zmogljivost in nizka zakasnitev (ang. low latency / zero latency), predstavlja velik izziv, saj enkripcija in dekripcija ne smeta vnašati dodatnih zakasnitev ter morata hkrati čim manj obremenjevati sistemske vire končnih naprav.

2 Tehnologije video preko IP

Na področju AV produkcije in distribucije se v zadnjih letih namesto namenskih vmesnikov in standardov hitro uveljavljajo IP vmesniki in standardi oz. tehnologije. Zaradi hitrega razvoja naprav in počasnega potrjevanja in uveljavljanja standardov veliko proizvajalcev opreme razvija svoje tehnologije in pristope. Na področju radiodifuzne produkcije (ang. Broadcast) in pro AV je v fazi potrjevanja standard SMPTE ST 2110 (ang. Society of Motion Picture and Television Engineers), ki v celoti prevzema prenos vseh signalov v AV produkciji (slika, zvok, podatki, sinhronizacija, nadzor,…) ter omogoča velikosti okvirjev vse do formata 32K. Standard SMPTE ST 2110 je sicer naslednik standarda SMPTE ST 2022, ki v osnovi zajema enkapsulacijo SDI signala v IP, ohranja glave SDI okvirjev in zatemnitvene intervale, kar pomeni, da je s stališča porabe zasedanja pasovne širine manj učinkovit, saj pri videu 4K60p zaseda 16,3% višji bitni pretok, pri 720p50 pa kar 39% višji bitni pretok. Oba standarda sta namenjena sicer prenosu in distribuciji visokokvalitetnih AV signalov brez kompresije ali pa z uporabo brez izgubne kompresije, kar pomeni visoke bitne hitrosti od 1,5 Gbit/s za 1080i50, 12 Gbit/s za 2160p60 HDR (ang. High Dinamic Range) ter še mnogo več za video ločljivosti 8k ali več [1].

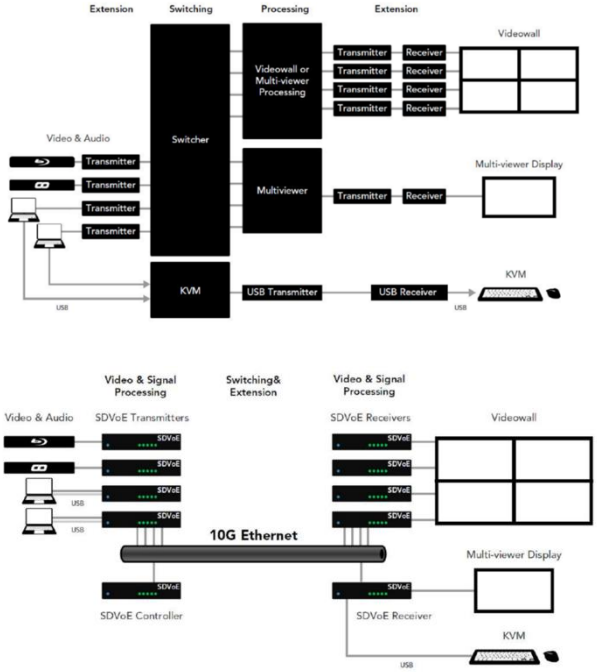
Standard	Video signal (resolucija in število slik)	Bitna hitrost
HD-SDI	1080i30	1.485 Gbps
3G-SDI	1080p60	2.97 Gbps
6G-SDI	2160p30	6 Gbps
12G-SDI	2160p60	12 Gbps

Slika 1: Bitne hitrosti nekompresiranega videa glede na ločljivost [1]

Rešitve, ki temeljijo na standardih SMPTE ST 2022 ali 2110, zahtevajo visokozmogljiva IP omrežja z visokimi bitnimi pretoki. Kot alternativni pristopi se zato razvijajo tudi standardi in tehnologije kot so npr. NDI in NDI HX (Newtek), NMI (Sony), NVX (CRESTRON), SDVoE (SDVoE Alliance), SVSi (AMX) in HDBase-T-IP (HDBaseT Alliance), ki jih razvijajo različni proizvajalci opreme ali povezave, ter se relativno hitro uveljavljajo na različnih področjih. NDI (ang. Network Device Interface) omogoča prenos AV vsebin z bitnimi pretoki, ki so prilagojeni 1 Gbit/s infrastrukturi, saj pretok HD (ang. High Definition) vsebin, ob uporabi NDI izgubnega kodiranja, zaseda zgolj 100-130 Mbit/s, medtem ko pri uporabi NDI HX kodiranja (prilagojen H.264 kodek) prenos HD signala zaseda zgolj 8-20 Mbit/s. S stališča zasedanja virov in potrebah po visokozmogljivih omrežjih je uporaba NDI bistveno bolj primerna, predvsem v okoljih, kjer se že uporabljajo 1 Gbit/s dostopi in 10 Gbit/s vmesniki na hrbteničnem ali agregacijskem segmentu omrežja. Pri NDI je v uporabi namenski NDI video kodek, ki vnaša zakasnitev manjšo od enega okvirja, kodek je izguben samo ob prvem kodiranju in zagotavljata enako kvaliteto ne glede na število kodiranj/dekodiranj (ang. multi-generation stability). Pri NDI HX se uporablja prilagojen H.264 video kodek, ki vnaša zakasnitev med 3 in 4 okvirji [5].

Slika 2: NDI zasnova produkcijskega sistema [5]

Tudi NMI (ang. Networked Media Interface) je protokol oz. postopek, ki je podoben NDI. Izdelalo ga je podjetje SONY, ki je tudi proizvajalec opreme, vendar so se odločili ustaviti razvoj NMI, saj so ga podpirale zgolj SONY naprave, medtem ko NDI vmesnik danes podpira skoraj 90 proizvajalcev strojne in programske opreme, poleg Newteka tudi Panasonic, Sony, JVC, EVS, OBS, Telestream in mnogi drugi. Za razliko od standardov oz. rešitev SMPTE, NDI in NMI, ki so namenjene uporabi v profesionalni in polprofesionalni video produkciji, so vse bolj razširjene tudi rešitve podjetij ali povezav, ki se ukvarjajo z avtomatizacijo pametnih zgradb, digitalnega oglaševanja ali zgolj prenosa AV vsebin preko IP omrežij (NVX, SDVoE (ang. Software-defined Video over Ethernet), SVSi in HDBaseT-IP). Zaradi specifičnih prilagoditev in predvidene uporabe v posebnih omrežjih ali namenskih rešitvah, so npr. NVX rešitve podjetja CRESTRON omejene predvsem na uporabo v namenskih sistemih za distribucijo multimedijskih vsebin, manj pa v samih produkcijskih omrežjih. Poleg ostalih omejitev so rešitve NVX, SDVoE, SVSi in HDBaseT-IP omejene tudi z vhodnimi signali in večinoma podpirajo le vmesnike kot so HDMI in tudi niso vgrajene v same naprave, ki se uporabljajo v AV produkciji [6][7]. Pri omenjenih rešitvah so v uporabi tudi namenski pretvorniki, ki klasične AV signale (HDMI, analogni avdio, serijski vmesnik za nadzor,…) pretvarjajo v IP podatkovne tokove na oddajni strani ter obratno na sprejemni strani, kot je razvidno na Slika 3. Signali iz avdio, video virov ali računalnikov se s pomočjo SDVoE oddajnikov – pretvornikov (ang. SDVoE Transmitters) pretvorijo v IP podatkovne tokove. Vse SDVoE oddajniki se povezuje na IP stikalo (ang. IP switch), ki naj bi bilo po priporočilih 10 gigabitno in imelo vgrajeno tudi možnosti usmerjanja oz t.i. L3 (ang. Layer 3) zmogljivosti. Na drugi strani so nameščeni SDVoE sprejemniki (ang. SDVoE Receivers), ki skrbijo za pretvarjanje IP podatkovnih tokov v avdio, video in kontrolne signale. Nadzor in upravljanje oddajnikov, sprejemnikov, stikala in ostalih SDVoE podprtih naprav se lahko izvaja iz ene toče – SDVoE krmilnika (ang. SDVoE Controller). Pri tovrstnih arhitekturah jedro sistema postane IP stikalo zato je to tudi najpomembnejši del omrežja.



Slika 3: Primerjava SDI (zgoraj) in SDVoE (spodaj) arhitekture [9]

3 Video preko IP okolja

Uporaba standardov SMPTE je predvidena predvsem v profesionalnih radiodifuznih sistemih (RTV okolja), kjer se v skladu z visokimi zahtevami po visoki kvaliteti in višji zmogljivosti omrežja predvideva gradnja zaprtih, ločenih omrežij in s tem tudi zagotavljanje varnosti predvsem na omrežnem nivoju. Tehnologije, kot so NDI, NMI, in NVX, pa razvijajo proizvajalci AV opreme z namenom uporabe obstoječih IP omrežij za potrebe AV produkcije in distribucije. Uporaba obstoječih omrežij omogoča dinamično gradnjo AV omrežja brez dodatnih višjih investicij v infrastrukturo. Združevanje in uporaba obstoječih omrežij pa po drugi strani predstavlja čedalje večja tveganja, zato se pojavljajo tudi potrebe po zaščiti AV vsebin in omejevanju dostopa do medijskih tokov tako v namenskih, kot tudi v obstoječih hibridnih omrežjih. Zaradi uporabe multicast načina prenosa vsebin so vsi prenosni tokovi dostopni vsem napravam, ki so priključene v isto broadcast domeno omrežja. Zato je zaradi visokih bitnih pretokov priporočljiva ustrezna segmentacija omrežja ter učinkovit nadzor nad usmerjanjem in dostopnostjo AV vsebin na omrežnih stikalih pri vseh sistemih, ki so namenjeni AV produkciji, kjer je zahteva po nizkih zakasnitvah in visoki kvaliteti izrazita in ključnega pomena.

Na drugi strani pa sistemi, ki so primarno namenjeni distribuciji AV vsebin, stremijo k širši uporabnosti, razširljivosti, zakasnitve pa niso tako moteče kot pri produkcijskih sistemih.

4 Možnosti zaščite pri posameznih tehnologijah

Zaščito medijskih podatkovnih pretokov pri prenosu AV vsebin preko IP je mogoče zagotavljati na nivoju IP omrežij s pomočjo logičnega ločevanja omrežja (VLANi), omejevanja dostopa ali enkripcije podatkovnih tokov. Najvišjo stopnjo varnosti je mogoče zagotoviti s pomočjo kombinacije vseh treh, vendar vsaka izmed možnosti zahteva ustrezne posege in predstavlja omejitve, ki jih je potrebno upoštevati pri načrtovanju oziroma gradnji sistema.

4.1 Sistemsko zagotavljanje varnosti

IP protokol v osnovi ne vsebuje splošnega mehanizma za zagotavljanje avetentičnosti in zasebnosti podatkov, ki se prenašajo preko IP omrežij. Zaščita vsebin se lahko v IP omrežjih poleg fizičnega omejevanja in ločevanja na virtualna logična podomrežja (VLAN-ov) zagotavlja s pomočjo uporabe protokolov kot npr. IPSec (ang. Internet Protocol Security), MACsec (ang. Media Access Control Security), VPN/SSL (ang. Virtual Private Network / Secure Sockets Layer) in SRTP (ang. Secure Real-time Transport Protocol) [2][1]. Profesionalni Video over IP sistemi za optimalno izrabo omrežja večinoma uporabljajo multicast način distribucije vsebin z uporabo IGMPv2 (ang. Internet Group Management Protocol version 2) ali celo IGMPv3 protokola, zato je za tovrstne sisteme potreben prilagojen način načrtovanja IP omrežja.

Pri omrežno-sistemskemu omejevanju in zagotavljanju varnosti z uporabo ločenih VLAN-ov ali IPSec tunelov med posameznimi izvori/ponori je potreben poseg sistemskih inženirjev in v večini primerov statično nastavljanje omrežnih dostopov na fizičnem, podatkovnem ali omrežnem sloju ISO-OSI modela. Z razvojem programsko definiranega dostopa – SDA (ang. Software Defined Access) in dinamičnega upravljanja omrežja - DNA (ang. Digital Network Architecture) je sicer mogoče bistveno lažje upravljati in omejevati dostope do virov in storitev, saj je s pomočjo virtualnih omrežij, ki so definirani v programskem vmesniku omrežnega nadzornega sistema, mogoče neposredno upravljati dostop in usmerjanje podatkovnih tokov ne glede na lokacijo izvora ali ponora na področju celotnega omrežja. Hkrati je mogoče pri SDA rešitvah dinamično upravljati dostope do storitev ali virov na nivoju posameznega uporabnika ali celo naprave posameznega uporabnika ne glede na to v kateri točki se povezuje v omrežje, torej neodvisno od lokacije. Kljub veliki prilagodljivosti in razširljivosti omrežij je ključnega pomena učinkovito usmerjanje in nadzorovanje AV podatkovnih tokov, saj lahko zaradi velikosti podatkovnih tokov pride do zasičenja omrežja in s tem povečanje tveganja za nedelovanje AV produkcijskega sistema. Pri prenosu AV signalov preko IP omrežij je predvsem pri produkcijskih sistemih zakasnitev ključnega pomena, zato je pomembno tudi, da omrežne naprave poleg naštetih nastavitev omogočajo tudi IEEE 802.1AVB (ang. Avdio Video Bridging) standard [8] ter protokol za rezervacijo pasovne širine 802.1Qat (ang. MSRP – Multiple stream reservation protocol).

4.2 Zagotavljanje varnosti v okviru AV standardov

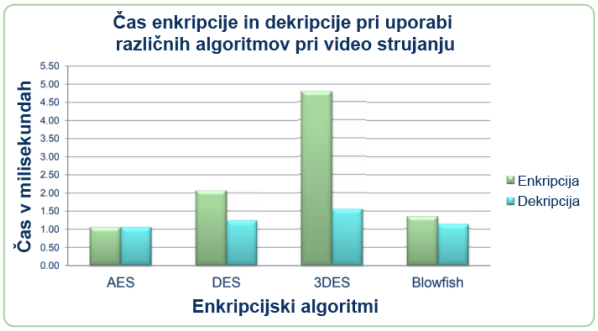
Standardi, ki so v uporabi za AV produkcijo v živo, zaradi zahtev po čim manjših zakasnitvah in prenosu v realnem času, nimajo vgrajenih mehanizmov za zagotavljanje varnosti (npr SMPTE standardi in NDI). NVX, SVSI in SDVoE pa za zaščito AV vsebin uporabljajo avtentikacijo in AES-128 (ang. Advanced Encryption Standard) enkripcijo.

5 Vpliv enkripcije na obremenitve / hitrosti

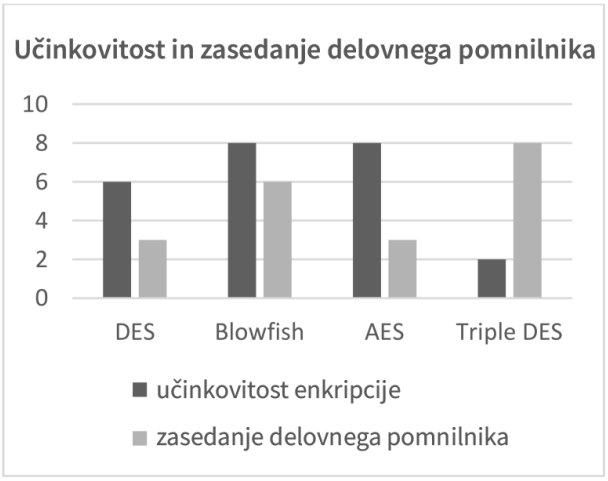
Pri prenosu video tokov preko IP omrežij v realnem času je ključnega pomena, da šifriranje in dešifriranje video okvirjev ne vnaša prevelike dodatne zakasnitve oz da leta ne presega trajanja enega okvirja, kar pri 25 sličicah na sekundo predstavlja 40 ms. Uporaba protokola za upravljanje oz. izmenjavo ključev, kot je TLS (ang. Transport Layer Security), zagotavlja varnost in integriteto podatkov, prenesenih preko IP omrežij, za njihovo dostavo pa se uporablja RTP (ang. Real-time Transport Protocol). Protokol za varno upravljanje ključev je predpogoj za pravilno delovanje enkripcijskih algoritmov.

Pri izbiri šifrirnega algoritma za zagotavljanje varnosti sta pomembni dve značilnosti: čas šifriranja ne sme biti previsok, velikost okvirjev pa mora biti še vedno dovolj majhna, da ne ovira prenosa v realnem času preko IP omrežja. Obstaja več različnih načinov za šifriranje video podatkovnih tokov, ti pa so odvisni od uporabljenega šifrirnega postopka (DES (ang. Data Encryption Standard), 3DES (ang. Tripple Data Encryption Standard), AES, Blowfish,…), načina delovanja (ECB (ang. Electronic Codebook), CBC (ang. Cipher Block Chaining), CFB (ang. Cipher Feedback), OFB (ang. Output Feedback), CTR (ang. Counter), …) in zapolnjevalnega načina (ang. padding mode) (ISO10126, PKCS5 (ang. Public Key Cryptography Standards), brez zapolnjevanja). Glede na meritve in testiranja se je izkazalo, da je najboljša kombinacija za šifriranje videa uporaba šifrirnega algoritma AES v načinu CTR in PKCS5Padding (Slika 5). Izbira temelji na več vidikih, kot so čas obdelave, zmogljivost, varnost, dinamičnost sistema in vpliv širjenja napak [3]. Poleg tega je AES algoritem odporen na vse znane načine napadov, hkrati pa dosega najvišje hitrost enkripcije in dekripcije glede na ostale algoritme, kot je razvidno na Slika 4 [10]. Dodatno je mogoče varnost povečati z dinamičnim časovnim spreminjanjem ključev za šifriranje.

Pri šifriranju se najpogosteje uporablja 128 bitne ključe, sam AES postopek sicer omogoča uporabo do 256-bitnih ključev. Ob primerni uporabi šifrirnih ključev in naključnih števil je sistem dinamičen, kar pomeni, da je težko napovedati oziroma razbrati šifrirano vsebino.



Slika 4: Čas enkripcije in dekripcije za različne algoritme pri video pretočnih vsebinah [10]



Slika 5: Učinkovitost algoritmov [3]

Na kvaliteto, hitrost in učinkovitost zaščite pri prenosu videa preko IP omrežij vplivajo tudi število sličic na sekundo (ang. frame rate) in video kodirni postopki. Rezultati so pokazali, da je najugodnejša hitrost 22 sličic/sekundo, saj dosega manjše izgube okvirjev in paketov ter je hkrati najbližje mednarodnemu standardu 25 sličic/sekundo za prenos videa prek IP omrežij [4]. Prav tako so rezultati poskusov [2] pokazali, da v primerjavi s kodekom MPEG-2, kodek H.264 dosega boljše rezultate za šifriranje, a hkrati slabše za izgubo paketov.

6 Zaključek

S prehodom na IP infrastrukturo se tudi pri sistemih za ustvarjanje in distribucijo AV vsebin vse pogosteje pojavljajo potrebe po zaščiti vsebin. Predvsem pri produkcijskih sistemih, kjer je zaželena minimalna zakasnitev, visoka kvaliteta in zanesljivost, se varnost zagotavlja predvsem sistemsko s fizičnim in sistemskim omejevanjem, šifrirnih postopkov pa se ne uporablja, čeprav je strojna oprema dovolj zmogljiva, šifrirni postopki pa dovolj hitri, da sama zaščita vsebin ne bi predstavljala dodatnih omejitev. Kljub izboljšanim postopkom in bolj učinkoviti strojni opremi se pri sistemih za video produkcijo izloča vse dodatne zakasnitve, ki bi nastale pri dodatni obdelavi vsebin, hkrati se pri teh sistemih zaradi optimizacije učinkovitosti in izrabe virov, načrtuje omrežja, ki so logično ali celo fizično izolirana od ostalih IKT sistemov z namenom izločanja kakršnihkoli dodatnih dejavnikov tveganja, ki bi lahko potencialno povzročili zakasnitve ali popačitve. Pri sistemih primarno namenjenih distribuciji AV vsebin in upravljanju multimedijskih sistemov pametnih zgradb in digitalnem oglaševanju se za zaščito AV podatkovnih tokov najpogosteje uporablja šifrirni postopek AES-128. Šifrirni postopek AES-128 se uporablja pri sistemih za zaščito digitalnih pravic (DRM – Digital Rights Management), kjer se uporablja standard HDCP (ang. High-bandwidth Digital Content Protection), kot tudi pri sodobnejših protokolih, ki se razvijajo za potrebe prenosa visokokakovostnih AV vsebin preko IP omrežij (kot npr. NVX in SDVoE).

Literatura

[1] B. Yamamoto, „The Commercialization and Economic Sphere of Video Over IP Technology”, v Internet Infrastructure Review (IIR) Vol.37, December 19, 2017

[2] L. Sevcik, D. Uhrin, J. Frnda, M. Uhrina, Z. Chmelikova in M. Voznak, „The Impact of Encryption on Video Transmission in IP Network”, v *22nd Telecommunications forum TELFOR 2014*, 2014, str. 123-126.

[3] A. Mustafa in Hendrawan, „Calculation of Encryption Algorithm Combination for Video Encryption using Two Layers of AHP”, v *2016 10th International Conference on Telecommunication Systems Services and Applications (TSSA)*, 2016, str. 1-7.

[4] N. Khalifa, H. Elmahdy, „The Impact of Frame Rate on Securing Real Time Transmission of Video over IP Networks”, v *2009 International Conference on Networking and Media Convergence*, 2009, str. 57-63.

[5] NewTek NDI, https://www.newtek.com/ndi/

[6] HDBseT-IP vs. SDVoE: A Smackdown of AV over IP Standards, https://www.commercialintegrator.com/av/hdbaset-ip-vs-sdvoe-av-over-ip/

[7] SDVoE Alliance, https://sdvoe.org/technology/

[8] C. Hill, S. Orr, „Innovations in Ethernet Encryption (802.1AE - MACsec) for Securing High Speed (1-100GE) WAN Deployments” White Paper, https://www.cisco.com/c/dam/en/us/td/docs/solutions/Enterprise/Security/MACsec/WP-High-Speed-WAN-Encrypt-MACsec.pdf

[9] K. Johnson, „AV over IP and SDVoE System Designs”, https://www.mapyourshow.com/mys_shared/infocomm18/handouts/1030_Johnson_IS078_ppt.pdf

[10] N. Khalifa, „Securing Real-Time Video over Internet Protocol Transmission”, https://scholar.cu.edu.eg/nourmahmoud/files/ppppresentation.pdf?fbclid=IwAR1gXXTo66h-qZmSakyNgkI7HQhQCXAA0__sR0Bv-xm7QU0_RCn6ck2q2OA