sciendo

Műszaki Tudományos Közlemények vol. 13. (2020) 101–104.
DOI: Magyar: https://doi.org/10.33895/mtk-2020.13.17
Angol: https://doi.org/10.33894/mtk-2020.13.17

EME MTSZ MTK

SDMN-ARCHITEKTÚRA AZ 5G-BEN

SDMN ARCHITECTURE IN 5G

Kovács Márk,[1] Agg Péter András,[2] Johanyák Zsolt Csaba[3]

Neumann János Egyetem, GAMF Műszaki és Informatikai Kar, Kecskemét, Magyarország

[1] *kovacs.mark@gamf.uni-neumann.hu*

[2] *agg.peter@gamf.uni-neumann.hu*

[3] *johanyak.csaba@gamf.uni-neumann.hu*

Abstract

Due to the exponentially growing number of mobile devices connected to the Internet the current 4G LTE-A mobile network will no longer be able to serve the nearly 5 billion mobile devices. With the advent of the fifth generation, however, the number of cybercrimes may increase. This requires building an architecture that can adequately protect against these attacks. For wired networks, the SDN-type architecture has been introduced for some time. As a result, a similar design concept has emerged, which is called Software Defined Mobile Networks (SDMN). This article describes this technology to help preventing DoS, DDoS attacks, and IP source spoofing.

Keywords*: SDN, 5G, NFV, SDMN, security.*

Összefoglalás

Az exponenciálisán növekvő internetre csatlakoztatott mobileszközök száma miatt a jelenlegi 4G LTE-A mobilhálózat már nem lesz képes kiszolgálni a már közel 5 milliárd mobileszközt. Az ötödik generáció megjelenésével azonban még nagyobbra nőhet a kiberbűnözés mértéke. Ezen kockázat ellensúlyozásaként egy olyan architektúra felépítése szükséges, amely kellőképpen ki tudja védeni ezeket a támadásokat. A vezetékes hálózatoknál már egy ideje bevezetésre került az SDN-típusú felépítés. Ennek nyomán próbálnak egy hasonló kialakítást megvalósítani az 5G-hálózatoknál is, aminek eredményeképpen megszületett a Software Defined Mobile Networks z (SDMN) fogalma. Cikkünk ezt a technológiát mutatja be annak érdekében, hogy könnyebben kivédhetők legyenek a DoS-, DdoS-támadások, illetve az IP-forráscím-hamisítások.

Kulcsszavak*: SDN, 5G, NFV, SDMN, biztonság.*

1. Szoftver által definiált hálózatok (SDN)

Napjaink az egyik legelterjedtebb és leghatékonyabb hálózati megoldása a szoftver által definiált hálózatok (Software Defined Networks, SDN) [1]. Az SDN legnagyobb újítása a hagyományos hálózatokkal szemben, hogy elválasztja a vezérlősíkot (controlplane) az adatsíktól (dataplane). Ezen módszer segítségével fontos szerepet kap a központosított vezérlés. Az SDN-hálózatoknál három fő réteget különböztetünk meg: az adatsíkot, vezérlősíkot, és az alkalmazási síkot.

Az SDN adatsíkjában gyakorlatilag a kapcsolók és forgalomirányítók találhatóak (közös nevükön SDN-kapcsolók), melyeknek feladatuk csak a csomagok eljuttatása a célcímig felsőbb utasítás alapján, melyet a vezérlősíktól kapnak. Ezek az eszközök az úgynevezett déli interfészen (SouthboundInterface) keresztül kapják meg az utasításokat, és végrehajtásukhoz szükségük van arra, hogy OpenFlow [2] protokoll-kompatibilisek legyenek.

A vezérlősík biztosítja az itt használt programok segítségével a hálózat automatikus konfigurálását, a dinamikus hozzáférést és vezérlést az igények-

nek megfelelően. Egyik legfontosabb rétege ennek a síknak a virtualizáció, amely azonban nem keverendő össze a hálózati funkciók virtualizációjával (NFV [3], Network Function virtualization). (Az SDN és az NFV kapcsolatáról a következő részben beszélünk.) Ebben a síkban található a hálózati operációs rendszer is (Network Operating System), amely az esetlegesen felmerülő hálózatmenedzsmenti problémák kezelésére szolgáltat megoldásokat. A vezérlősík közvetlen kapcsolatban van az SDN harmadik síkjával, az úgynevezett alkalmazási síkkal. A köztük lévő kommunikációért az északi interfész (NorthboundInterface) felel.

Az SDN harmadik síkja az alkalmazási sík, melyben három alréteg található: a nyelvalapú virtualizáció (Language-basedvirtualization), a programozási nyelvek (Programminglanguage) és a hálózati alkalmazások (Network Applications). Feladatuk a megfelelő utasítások kiadása a vezérlés felé, melyek biztosítják a gyors és megbízható kommunikációt központi felügyelet mellett.

2. SDN és NFV

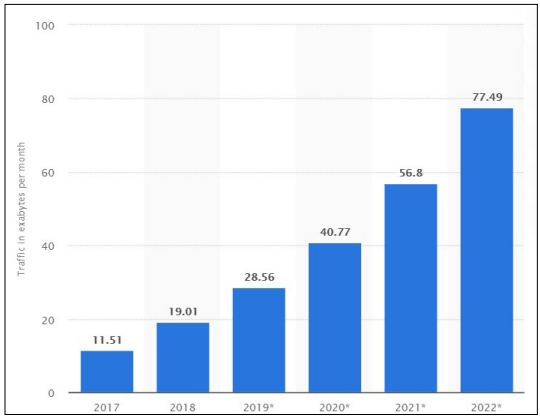
A hálózati virtualizációnál nagyon sokszor emlegetik az SDN-t és NFV-t együtt, bár ezek nem függenek egymástól. A két megoldásnak van kapcsolata, úgyis mondhatnánk, hogy kiegészítik egymást.

Az SDN a hálózati eszközöket virtualizálja (kapcsolók, forgalomirányítók), a hagyományos továbbító eszközök helyett használ olcsóbb, gyorsabb, központilag vezérelhető hardverelemeket, illetve természetesen egy vagy több vezérlőkontrollert, amelyek segítségével biztosíthatja a megfelelő központosított védelmet, adminisztrálhatóságot, illetve a gyors reagálást a felhasználói igényeknek megfelelően.

Az NFV a hálózati funkciók virtualizálását tekinti elsődleges feladatnak. Az NFV-virtualizáció segítségével gyors telepíthetőséget, költségcsökkentést, rugalmasságot biztosít. Segítségével olyan szolgáltatásokat tudunk szoftveresen igénybe venni, amelyeket korábban hardverben valósítottak meg (pl. hálózati címfordítás (NAT), tűzfalszolgáltatások, DHCP). Fontos megjegyezni, hogy az NFV-szolgáltatások megvalósításának nem feltétele az SDN-hálózat megléte.

3. Jelenlegi mobilhálózatok hiányosságai

A mobilkommunikáció az 1980-as években kezdődött el, ami kezdetben csak és kizárólag hanghívásokra volt használható mindössze 56 kbps adatátviteli sebességgel. Napjainkban azonban ez



1. ábra. *Globális mobil adatforgalom 2017 és 2022 között* [4]

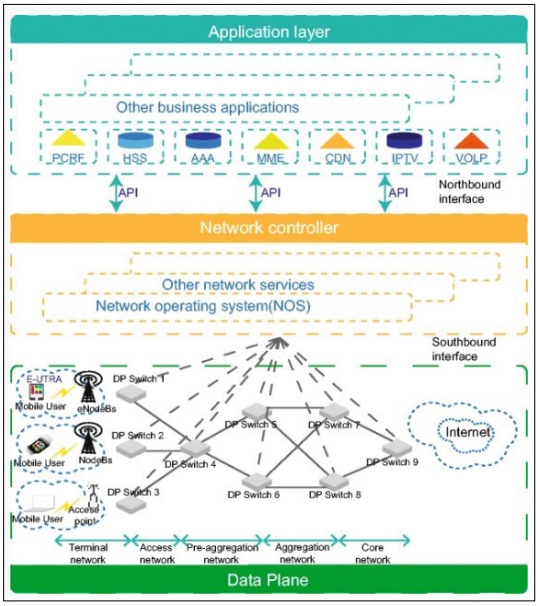
a kezdetleges szolgáltatás kinőtte magát egy külön nagy hálózattá, amely képes kapcsolódni a világhálóra, és ennek köszönhetően a hanghívásokon kívül videóhívásokra, nagy felbontású online videók átvitelére, online játékokra is használható [5].

A jelenleg használt mobilhálózatokat több hiányosság is jellemzi:

- *Megfelelő skálázhatóság hiánya*: a forgalom gyorsan növekszik az új nagy sávszélességet igénylő mobilszolgáltatások miatt, és a jelenlegi statikus hálózatok túl rugalmatlanok, ezért jövőbeni működésük túl költséges lesz.
- *Komplex hálózati menedzsment*: a fizikai hálózati eszközökhöz nincs biztosítva egy közös vezérlő interfész, ezért még egy kisebb feladathoz is nagy szakértelem szükséges, ami a legtöbb rendszerleállási hiba forrása is egyben.
- *Komplex és drága hálózati eszközök*: néhány eszköznek túl sok feladatot kell elvégeznie (pl. forgalomfigyelés, számlázás, QoS vagy éppen a szülői felügyelet), ami növeli az eszköz összetettségét és költségét.
- *Magas költségek*: az üzemeltetők nem tudják összeegyeztetni a különböző olcsóbb gyártók eszközeit, ami növeli a költségeket, illetve a kézi beállítás és rugalmatlanság miatt magas az üzemeltetési költség is.
- *Rugalmatlanság*: a szabványosítási hosszú folyamat miatt sokáig elhúzódik egy új szolgáltatás bevezetése.

4. Szoftver által definiált mobilhálózatok (SDMN)

Az SDN eredetileg vezetékes hálózatokhoz lett tervezve, azonban a fejlesztők észrevették a lehe-



2. ábra. *SDMN architektúra* [6]

tőséget, hogy ez a megoldás működhet vezeték nélküli környezetben is.

Az SDMN egy programozható, rugalmas és forgalomközpontú hálózati konstrukció, amely az SDN-t, NFV-t és felhőalapú számolás kombinációjából áll. A jelenleg működő mobilhálózatoktól annyiban tér el, hogy a forgalomközpontú modell segítségével integrálják a drága hardveres eszközöket, és központosított logikai vezérlőt helyeznek az optimális működés érdekében.

Az SDN-hez hasonlóan az SDMN is három részből áll: adatsíkból, vezérlősíkból és az alkalmazási síkból.

Bár az SDN-koncepció sajnos nem oldja meg az előző fejezetben említett összes problémát, de növeli a rugalmasságot, skálázhatóságot és ezáltal a teljesítményt is. A jelenlegi mobilhálózatot egy forgalomközpontú modell felé irányítja, melynek segítségével olcsó hardvert és logikailag központosított vezérlőt alkalmaz. Az SDN-kompatibilis kapcsolók, útválasztók és átjárók az SDN-vezérlőn és a hálózati operációs rendszeren (NOS) keresztül vezérelhetők. A vezérlősík virtuális összetevőként telepíthető egy operátorfelhőben. Az **2. ábra** a SDMN felépítését szemlélteti [7].

4.1. DP réteg

Infrastrukturális rétegnek is szokás nevezni, ahol a hálózati eszközök találhatóak, mint a kapcsolók és forgalomirányítók. A bázisállomások határkapcsoló adatsík kapcsolóihoz vannak csatlakoztatva. Az internethez kapcsolódnak a másik oldal határkapcsolói.

4.2. Hálózati vezérlő

A logikailag központosított vezérlő segítségével lehet a DP eszközeit konfigurálni, vezérelni. Egy vezérlőprotokollt használ (pl. OpenFlow) a DP-elemek eléréséhez, illetve az forgalomszabályozások telepítéséhez. A hálózativezérlő- és a DP-réteget az SDN-architektúrához hasonlóan a déli irányú API köti össze. A vezérlőn fut a NOS, a vezérlési szolgáltatások támogatásához.

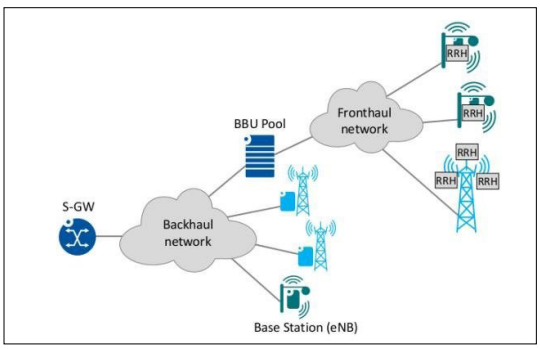
4.3. Alkalmazási réteg

Itt található meg az összes vezérlő- és üzleti alkalmazás, mint a házirend, előfizetői szerver, azonosítás, jogosultságkezelés, könyvelés. Az alkalmazási réteg és a hálózati vezérlő között az északi határú API biztosítja a kapcsolatot.

5. Biztonsági hiányosságok

Az SDN-ből származó biztonsági rések itt is megtalálhatók:

– A központosított felügyelet integrálja a hálózati konfigurációt, a hálózati szolgáltatás-hozzáférés vezérlését és a szolgáltatás telepítését a vezérlőrétegen. Ha a támadó sikeresen megszerzi az irányítást az SDN-ben, akkor a hálózati szolgáltatás megbénul, és ez az egész hálózatot érinti [8].
– Az SDN programozhatóságának főbb problémája a harmadik féltől származó alkalmazásokon és vezérlőn alapuló bizalom. A rosszindulatú alkalmazások kockázatát hordozza magában, ezért meg kell erősíteni a hitelesítési eljárást az alkalmazás és a vezérlőrétegek között a vezérlő védelme érdekében.
– Az NFV és az SDN kombinációja biztonsági problémák sorozatát jelentheti. Például az OpenFlow,



3. ábra. *Backhaul és Fronthaul hálózatok közötti kapcsolat* [9]

az NFV, a szoftver által definiált Fronthaul hálózati biztonsági problémák és a terminálproblémák stb. A szoftver által definiált fronthaul esetében a virtualizált támadás veszélyt jelent.
– A szoftver által meghatározott Fronthaul-, (SDF) vezeték nélküli programok szempontjából az SDMN-biztonságot fenyegető veszély lehet a MAC-hamisítás és a rosszindulatú RF-interferencia is. **[10]**

Összegzés

A növekvő forgalom miatt egyre nagyobb igény van egy jól megtervezett hálózati architektúrára a mobilhálózatok terén is. Ennek nyomán számos kutatás folyik az új generáció technológiájának jól kialakított, azonban biztonságos kialakítására.

Köszönetnyilvánítás

Köszönettel tartozunk a kutatás támogatásáért, amely az EFOP-3.6.1-16-2016-00006 „A kutatási potenciál fejlesztése és bővítése a Neumann János Egyetemen” pályázat keretében valósult meg. A projekt a Magyar Állam és az Európai Unió támogatásával, az Európai Szociális Alap társfinanszírozásával, a Széchenyi 2020 program keretében valósul meg.

Szakirodalmi hivatkozasok

[1] Ramos F. M. V., Kreutz D., Verissimo P.: *Software-defined networks: On the road to the softwarization of networking*. Agile Product Management & Software Engineering Excellence, Business Technology & Digital Transformation Strategies Cutter Business Technology Journal, 28. (2015) 6–13.

[2] Lara A., Kolasani A., Ramamurthy B.: *Network innovation using OpenFlow: A survey*. IEEE Communications Surveys & Tutorials, 16/1 (2014), 493–512.

[3] Bo Han, Vijay Gopalakrishnan, Lusheng Ji, Seungjoon Lee: *Network function virtualization: Challenges and opportunities for innovations.* IEEE Communications Magazine 53/2. (2015) 90–97. DOI: 10.1109/MCOM.2015.7045396

[4] Statista: *Global mobile data traffic from 2017 to 2022*. (letöltve: 2020. február 20). https://www.statista.com/statistics/271405/global-mobile-data-traffic-forecast/

[5] Militano L., Araniti G., Condoluci M., Farris I., Iera A.: *Device-to-Device Communications for 5G Internet of Things*. EAI Endorsed Transactions on Internet of Things 1/1. (2015) 150598. https://doi.org/10.4108/eai.26-10-2015.150598

[6] Chen, M., Qian, Y., Mao, S. et al. Software-Defined Mobile Networks Security. Mobile Netw Appl 21, 729–743 (2016). https://doi.org/10.1007/s11036-015-0665-5

[7] Liyanage M., Gurtov A., Ylianttila M.: *Software Defined Mobile networks (SDMN) Beyond LTE network architecture*. Wiley, 2015.

[8] Ji, X., Huang, K., Jin, L. et al.: *Overview of 5G security technology.* Sci. China Inf. Sci. 61, 081301 (2018). https://doi.org/10.1007/s11432-017-9426-4

[9] Hailu D. H., lema G. G., Bjørnstad S.: *Performance Evaluation of Ethernet Network for Mobile Fronthual Networks*. IJEESC 7/1. (2017) 287–298.

[10] Liyanage M. et al.: *Enhancing Security of Software Defined Mobile Networks.* IEEE Access, 5 (2017) 9422–9438.