Wi-Fi şəbəkəsində təhlükəsizlik məsələləri

Təbriz Ağaşov
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
tabriz@science.az

Xülasə ─ Məqalədə IEEE 802.11 (Wi-Fi) naqilsiz şəbəkələrinin informasiya təhlükəsizliyinə baxılmışdır. OSI şəbəkə modelinin əsasən fiziki və kanal səviyyəsinə edilən hücum növləri və onlardan müdafiə üsulları təhlil edilmişdir.

Açar sözlər ─ mobil trafik; IEEE 802; OSI modeli; frame; trafikin indikasiya xəritəsi (TİM)

I. GİRİŞ

Müasir dövrdə İnternetlə işləmək üçün kompakt qurğuların meydana gəlməsi informasiya texnologiyaları mütəxəssislərinin qarşısında yeni bir məsələ – kabelləşdirilmiş İnternet mərkəzlərindən, provayderlərdən uzaq məsafədə yerləşən və kabelləşdirilməsi çətin olan yerlərdə, şəbəkəyə çıxışı təmin etmək məsələsi dayanmışdır.

Wi-Fi (Wireless Fidelity) – naqilsiz lokal (Wireless LAN) şəbəkələrin təşkili üçün nəzərdə tutulan genişzolaqlı radiorabitə avadanlıqları standartıdır. Bu texnologiya şəbəkəyə əlyetərliyi təmin etmək üçün istifadə edilən texniki vasitələrin inkişafında yeni bir addımdır. Belə texnologiyaların inkişafı hal-hazırda da davam etdirilir. Bir çox şirkətlərin apardığı tədqiqatlara əsasən, tezliklə smartfon və planşetlərdən gedən mobil trafikin daha çox hissəsi 2G/3G/4G/5G şəbəkələri vasitəsilə deyil, məhz Wi-Fi şəbəkələri ilə ötürüləcəkdir. Yaxın gələcəkdə bütün dünya mobil operatorlarında ümumi trafikin yalnız 40%-i istifadə ediləcək. 2020-ci ilə qədər isə 802.11 şəbəkələri üzrə ötürülən verilənlərin həcminin 30000 pbaytdan 115000 pbayta qədər yüksələcəyi proqnozlaşdırılır. Belə artım Şimali Amerikanın və Avropanın bir çox ərazilərində fəal olaraq reallaşacaqdır [1].

Aparılan tədqiqatlar əsasında o qənaətə gəlmək olar ki, həm şəbəkələrin əhatə dairəsinin genişlənməsi, həm də istifadəçilərin sayının artması, Wi-Fi komplekslərinin təhlükəsizliyi haqqında ciddi tədbirlər həyata keçirməyə zəmin yaradır.

Naqilsiz şəbəkələrə mümkün hücumlardan danışmazdan əvvəl, nəzərə almaq lazımdır ki, şəbəkənin quraşdırılması prosesi çoxlu mərhələlərdən ibarətdir və bu mərhələlərin hər birinin təhlükəsizliyinin təmin edilməsi çox vacib məsələlərdir. Lakin, əgər şəbəkənin qurulması və sazlanması prosesində müəyyən səbəblərdən səhvlər edilərsə və tədbirlərin yerinə yetirilməsində çətinliklər meydana çıxarsa, bu zaman naqilsiz şəbəkəyə hücumlara şərait yaranacaqdır.

II. OSI MODELİ VƏ ONUN SƏVİYYƏLƏRİ

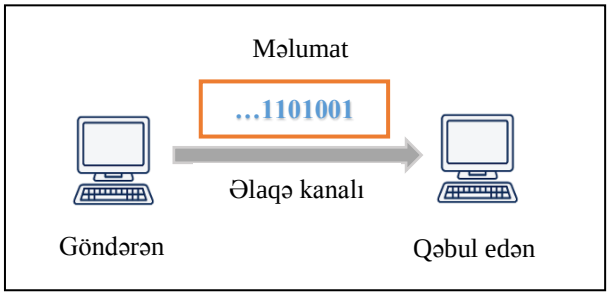
Kompüter şəbəkələrini yaradan zaman əsas məsələ müxtəlif xarakterli kommunikasiya avadanlıqlarının bir yerdə işləməsinin təmin edilməsi, informasiyanın formalaşması və mübadiləsi sisteminin (nəzərdə tutulan proqram və verilənlərin) bir-birinə uyğunlaşmasıdır. 1980-ci ildə Ümumdünya Standartlar Təşkilatı (ISO – International Standards Organization) tərəfindən irəli sürülmüş və hazırlanmış texniki təkliflər (standartlar) əsasında qarşılıqlı əlaqəsi olan şəbəkə avadanlıqlarının inkişaf etdirilməsinə başlanılmışdır. Bu baxımdan yeni bir etalon model (OSI – Open Systems Interconnection) işlənib hazırlandı. Bu model kompüter şəbəkələrinin inkişafında mühüm rol oynadı. OSI modeli şəbəkədə müxtəlif sistemli avadanlıqların arasındakı fərqi müəyyən etməklə yanaşı, həmin sistemlərin yerinə yetirdiyi funksiyaları da müəyyənləşdirir. Bir kompüterdən digərinə məlumat göndəriləndə baş verən proseslər standartlaşdırılmış formada bütün kompüterlərdə eyni ardıcıllıqla aparılır. OSI modeli yeddi səviyyədən ibarətdir [2]:

- Tətbiqi səviyyə (Application);
- Təqdimetmə səviyyəsi (Presentation);
- Seans səviyyəsi (Session);
- Nəqliyyat səviyyəsi (Transport);
- Şəbəkə səviyyəsi (Network);
- Kanal səviyyəsi (Data Link);
- Fiziki səviyyə (Physical).

Wi-Fi şəbəkələrinin əsasını IEEE 802 beynəlxalq standartlar ailəsi təşkil edir ki, bu da lokal hesablama şəbəkələrinin və meqapolislərdə yerləşən şəbəkələrin işini tənzimləyir. Bu standartlar ailəsinin xidmət və protokolları OSI şəbəkə modelinin iki aşağı səviyyələrində işləyir: fiziki və kanal səviyyələrində [2-4].

DOI: 10.25045/NCInfoSec.2018.25

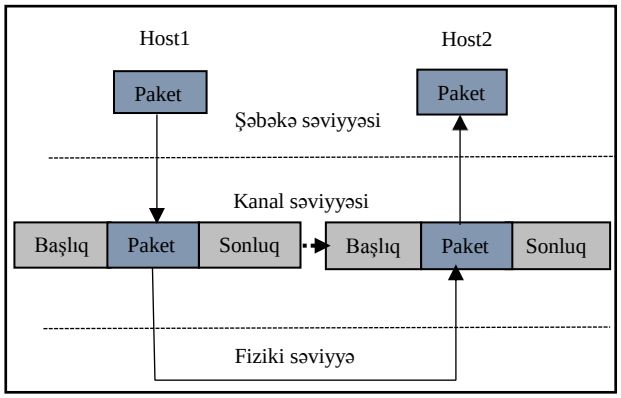
Fiziki səviyyə - bir qurğudan digərinə ikilik kombinasiya (bitlər) şəklində olan verilənlərin real fiziki ötürülməsi metodunu müəyyən edir. Fiziki səviyyə kanal səviyyəli məlumat ötürmə səviyyəsindən məlumat paketlərini qəbul edir, sonra onları 0 və 1 ikili kodlarına uyğun optik və ya



Şək. 1. Fiziki səviyyədə məlumatın ötürülməsi

elektrik siqnallarına çevirir (şək. 1). Bu siqnallar qəbuledici qovşağa ötürülür və qeyd edək ki, proses zamanı ötürülən informasiya analiz edilmir. Bu səviyyədə elektrik siqnallarının səviyyəsi, kodlaşdırma tipi, siqnalların ötürülmə sürəti və s. təyin edilir. Fiziki səviyyə fiziki şəbəkə mühitinə (məsələn: şəbəkə kabelinə, wi-fi nöqtəsinə) ən yaxın olan səviyyədir. Əsas vəzifəsi məlumatı ötürücülərlə ötürmək və qəbul etməkdir.

Fiziki səviyyədə baş verən proseslər əlaqə kanalının xassələrindən (kanalın ötürmə qabiliyyətindən (bit/s), vaxtdan və səhvlərin sayından) asılıdır. Əlaqə kanalı məlumatların ötürülmə istiqamətinə görə üç növə bölünür: simpleks (bir istiqamətə), dupleks (eyni vaxtda hər iki istiqamətə) və yarımdupleks (hər iki istiqamətə növbə ilə) ötürmələr. Fiziki əlaqə kanalı kimi, koaksal kabel, burulmuş cütlər, optovolokon kabel, radiodalğalar və s. nəzərdə tutulur.



Şək. 2. Kanal səviyyəsində kadrların formalaşması və ötürülməsi

Kanal səviyyəsi – şəbəkənin fiziki səviyyə ilə qarşılıqlı əlaqəsini və əlaqə kanalı ilə məlumatların ötürülməsini təyin edir. Kanal səviyyəsi şəbəkə səviyyəsindən məlumatı paket formasında qəbul edir, paketə başlıq və sonluq əlavə edir. Nəticədə başlıqdan, məlumat paketindən və sonluqdan ibarət tam məlumat qrupu – kadr (frame) əmələ gəlir. Bu kadrlar şəbəkənin fiziki səviyyəsindən keçərək növbəti hostun kanal səviyyəsinə qəbul edilir (şək. 2). Kanal səviyyəsi hər bir kadrın düzgünlüyünü təyin edir. Kadrların nəzarət cəmini hesablayaraq onu hər bir kadrın əvvəlinə və sonuna əlavə edir. Qəbuledicidə nəzarət cəm hesablanır. Onlar eyni olduqda informasiya qəbul edilir. Səhvlər təyin edildikdə isə ötürmə təkrar icra olunur. IEEE 802 spesifikasiyasına əsasən bu səviyyə iki altsəviyyəyə bölünür: MAC (Media Access Control) və LLC (Logical Link Control).

Wi-Fi şəbəkəsi naqilli şəbəkədən fərqli olaraq, tamamilə açıq şəbəkə olduğu üçün, ona İnternetdən müdaxilə ilə yanaşı, həm də qonşu ofisdən və ya digər mərtəbədəki həmkarlar tərəfindən “qulaqasma” cəhdi təhlükə törədir. Bu isə belə hərəkətlərin, naqilsiz şəbəkədən, nəinki istifadə etməyə, həm də ona müdaxilə yollarını tapmağa gətirib çıxarır. Əgər şəbəkənin təhlükəsizliyinə lazımi diqqət yetirilməzsə, belə şəbəkəni tamamilə ümumi istifadəli kimi saymaq olar ki, bu da onun fəaliyyətində yaxşı şəkildə əks olunmayacaq və problemlərə yol açacaqdır [5]. Aşağıdakı bəndlərdə Wi-Fi şəbəkəsinə olunan hücumlar və onlardan müdafiə üsulları araşdırılmışdır.

III. ŞƏBƏKƏYƏ HÜCUM EDƏNLƏR

Qeyd edək ki, Wi-Fi şəbəkələrində təhlükəsizlik sistemini yaratmazdan əvvəl, şəbəkəyə müdaxilə edənin özü haqqında təsəvvür əldə etmək lazımdır. Bunu başa düşmək üçün şəbəkəyə müdaxilə edənin potensial modelini tərtib etmək lazımdır.

Şəbəkəyə müdaxilə edənləri üç əsas kateqoriyaya bölmək olar [6]:

1. *Həvəskarlar*. Bu kateqoriyadan olanlar özlərini təsdiq etmək və ya əyləncə üçün şəbəkəyə müdaxilə edirlər. Onların əksəriyyəti şəbəkənin təhlükəsizliyinə ciddi təhlükə törətmirlər, bəziləri isə, hətta tapılan zəifliklər haqqında administratora məlumat verə bilərlər. Belə adamlar öz vərdişləri və bacarıqlarına lazımi diqqət yetirsələr informasiya təhlükəsizliyi üzrə yaxşı mütəxəssislərə çevrilə bilərlər.

2. *Peşəkarlar* – əlaqə kanalına müdaxilə edənlər. Bu kateqoriyadan olan müdaxiləçilər informasiya mübadiləsi iştirakçılarının bir qədər başqa qrupunu təmsil edirlər. Bu şəxslərin marağı müxtəlif kontenti şəbəkəyə ötürmək üçün özgə şəbəkələrdən istifadə cəhdinə istiqamətlənmişdir. Çox vaxt bu tip kontentlər və verilənlər o qədər də qanuni xarakter daşımasalar da, özgə şəbəkəyə daxil olma cəhdi belə, beynəlxalq qanunvericiliyə əsasən həbs edilməyə qədər ciddi nəticələrə səbəb ola bilər.

3. *Cinayətkarlar*. Üçüncü kateqoriya ən təhlükəlidir. Onun təmsilçiləri Wi-Fi şəbəkəsinə icazəsiz müdaxilələri daha professional şəkildə həyata keçirməyi bacarırlar. Naqilsiz şəbəkələrdə mövcud olan anonimliklər və kanalların əhatə dairəsindən kənar əlyetərli olması xüsusiyyətləri onları müdaxiləni reallaşdırmağa cəlb edir. Şəbəkəyə qoşulmuş çox sayda qurğulara malik olan şirkətdə verilənlərin ötürülməsinin hansı qurğular vasitəsilə baş verdiyini izləmək çətindir. Ən

güclü hücumlar kompüter texnologiyaları sahəsində yaxşı təhsilə malik olan və radiofizikanın prinsipləri ilə yaxından tanış olan bir qrup şəxslər tərəfindən törədilir.

IV. HÜCUMUN NÖVLƏRİ VƏ TƏSNİFATI

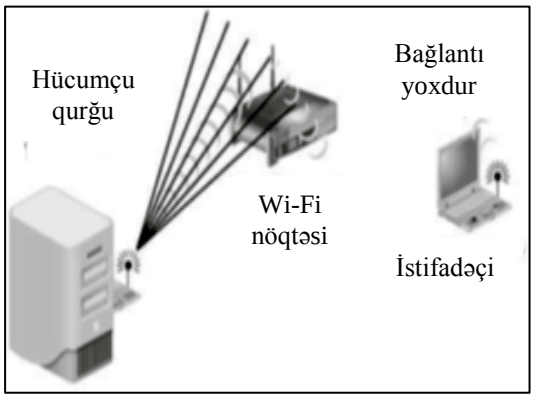
Wi-Fi şəbəkələrinin təhlükəsizlik sistemini yaratmaq üçün şəbəkəyə müdaxilə edənlər tərəfindən tətbiq oluna bilinəcək müxtəlif hücum növləri haqqında da təsəvvürə malik olmaq lazımdır.

Sistemə hücum – müdaxilə edənin informasiya sisteminə giriş əldə etməyə yönələn fəaliyyəti və yaxud fəaliyyət yığımıdır [7].

Hücumların mahiyyətini asan başa düşmək üçün onları ümumi xassələrinə görə, adətən müxtəlif qruplarda birləşdirirlər:

1. Wi-Fi şəbəkələrində parametrlərin dəyişdirilməsinə yönəlmiş hücum

Belə hücumlardan biri enerjinin qənaət rejimində parametrlərin sazlanmasına edilən hücumdur və şəbəkənin kanal səviyyəsində icra edilir. Hücüm edən kliyentin “gözləmə” rejimi vəziyyətində olan qurğusunda bəzi parametrləri dəyişir və həmin qurğularda saxta kadrların yığılmasını həyata keçirir. Saxta kadrları kliyentə göndərilir. Kliyent kadrları qəbul etdikdən sonra Wi-Fi nöqtəsində bufer (müvəqqəti saxlama yeri) təmizlənir və beləliklə, kliyent öz kadrlarını ala bilmir. Kadrların saxta düzəldilməsi ilə reallaşan bu üsul yeni paketlərin olmaması haqqında məlumat verən trafikin indikasiya xəritəsinin (TIM - Traffic Indication Map) tətbiqi zamanı həyata keçirilir. Belə hücumları reallaşdırmaq hücum edilən hostlarda TIM kadrlara girişin qapadılması əməliyyatının yerinə yetirilməsi hesabına çox mürəkkəbdir [8].



Şək. 3. Maneə yaradan qurğu ilə hücum

2. DoS hücumlar

DoS hücumlar (Denial of Service − xidmətdən imtina) şəbəkə resurslarının normal işini pozmaq və ya çətinləşdirmək məqsədilə həyata keçirilən hücum üsullarından biri kimi tətbiq edilir. Fiziki səviyyədə informasiyanın ötürülməsini reallaşdıran radiodalğaların təbiəti və Wi-Fi protokollarına məxsus xüsusiyyətlər səbəbindən, yəni onlarda mövcud olan boşluqlara görə ötürülən informasiyalar hücumlardan müdafiə oluna bilməzlər. Belə hücumlar öz növbəsində bir neçə növə bölünürlər:

- Maneə yaradan qurğu ilə edilən hücum – belə əməliyyat xüsusi konfiqurasiya edilmiş ötürücünün və ya naqilsiz kartın köməyi ilə şəbəkənin fiziki səviyyəsində icra edilir, bu da əlaqə kanalını icazəsiz trafiklə doldurur (şək. 3). Belə əməliyyatın əsas çatışmazlığı maneə yaradan qurğunun hücum edilən şəbəkənin bilavasitə yaxınlığında yerləşdirilməsi tələbidir.
- Əlaqə kanalının saxta freymlərlə doldurulması – maneə yaradan qurğu ilə edilən hücum kimi belə hücumlar da, praktiki olaraq dəf olunmayandır. Əvvəlki hücum növündən fərqli olaraq, burada aparat hissəsi ilə yanaşı proqram təminatından da istifadə edilir. Məhz belə proqramlar saxta freymlər generasiya edir və onları ötürücü qurğu vasitəsilə göndərir [9].
- Düzgün formalaşdırılmayan autentifikasiya verilənlərinin köməyi ilə hücum – bu halda müdaxilə edən autentifikasiya olmaq üçün Wi-Fi nöqtəsinə sorğu tipli məlumatlar göndərir. Bu məlumatlarda saxta nöqtənin ünvanı, kliyentin ünvanı və belə saxta nöqtə üçün autentifikasiyaya giriş alqoritmi yazılır. Nəticədə, Wi-Fi nöqtəsi bu sorğuya cavab olaraq belə məlumat verə bilər: “Gözlənilməyən tranzaksiya nömrəsi ilə autentifikasiya məlumatı alınmışdır”. Bunun nəticəsində də əlaqə kəsilir.
- Wi-Fi nöqtəsinin müvəqqəti saxlama yerinin (buferinin) doldurulması.
- Wi-Fi nöqtəsinə qoşulmaq üçün edilən sorğuların həddən artıq olması. Belə əməliyyat əlaqəyə girən qurğunun MAC-ünvanının daim dəyişdirilməsi hallarında baş verə bilər.
- Kadrların ləğv edilməsi yolu ilə hücum.
- Verilənlərin nəzarət cəminin (CRC-32) dəyişdirilməsi ilə edilən hücum. CRC-32 ötürülən məlumatın tamlığını (düzgün olub-olmadığını) yoxlayan bir alqoritmdir. Əgər məlumatda bu ədəd dəyişdirilibsə, onda host bu məlumatı qəbul etmir və Wi-Fi nöqtəsi qoşulmaq üçün edilən sorğunu rədd edir. Həmin anda göndərənə hostdan həqiqi məlumatın müvəffəqiyyətlə qəbul edilməsini təsdiqləyən saxta bir məlumat gəlir. Məlumatın nəzarət cəminin (sonuncu dörd bayt) ötürülməsi anında, küy əngəlləri yaratmağın çətinliyi, belə hücumun reallaşdırılmasını çətinləşdirir. Belə hücumdan müdafiə kifayət qədər problemlidir [10].

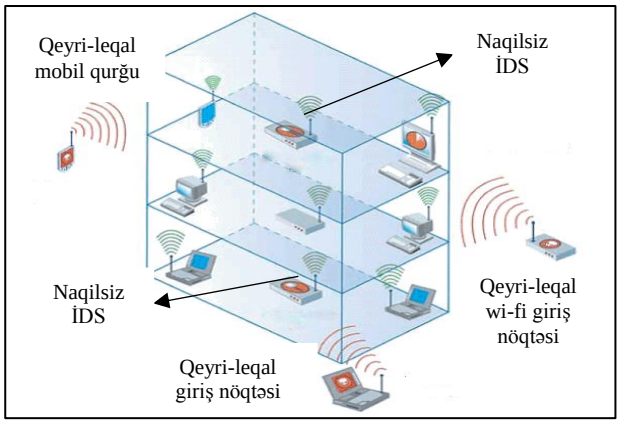
3. Autentifikasiya sisteminə hücumlar

MAC-ünvanların filtrasiyasına əsaslanan hücumlar. Belə

hücumu həyata keçirmək üçün hücum edən MAC-ünvanların axtarışı məqsədilə şəbəkə trafikini analiz edərək, növbəti hərəkətləri yerinə yetirir: ona lazım olan hostun şəbəkədə aktiv olmasını yoxlayır və bu hostun şəbəkədən deaktivləşməsini gözləyir. Bəzən, hücum edən MAC-ünvanı istifadə edilən kliyentlə bir şəbəkədə olur, belə halda o, ARP-ni (ing. Address Resolution Protocol - ünvanı təyin etmə protokolu) söndürür və şəbəkələrarası ekranın istifadəsindən imtina edir. Əlavə olaraq hücum edən IDS-in (ing. Intrusion Detection Systems) işə düşməsindən qaçmaq üçün bu hostdan paketlərin göndərilməsini və ICMP (ing. Internet Control Message Protocol – məlumatlara nəzarət protokolu) üzrə porta girişin olmaması haqqında məlumatların davamlı olaraq izlənməsini zəruriləşdirir. Bəzən, ziyankar öz MAC-ünvanını hücum edilən hostun ünvanına dəyişməsi üsulunu tətbiq etməklə hücum edilən hostu söndürə bilir [9].

V. HÜCUMLARDAN MÜDAFİƏ ÜSULLARI

Naqilsiz şəbəkəyə edilən hücumların müəyyən edilməsini və şəbəkənin hər bir qovşağının bu hücumlardan təhlükəsizliyini reallaşdırmaq üçün, hücumları aşkar edən sistemlərdən (monitorinq sistemi - proqram təminatı) istifadə



Şək. 4. Wi-Fi şəbəkəsinin təhlükəsizliyini təmin edən monitorinq sisteminin iş sxemi

edilir (şək. 4).

Belə proqramlar aşağıdakı məqsədlərə nail olmağa imkan verir:

- ✓ Hücum edəni tapır, yəni şəbəkənin monitorinqini yerinə yetirməklə, istənilən qeyri-leqal wi-fi nöqtəsini və bu nöqtədən istifadə edərək istifadəçinin trafikini izləməyə cəhd göstərəni aşkarlayır;
- ✓ Şəbəkəni yoxlayır, yəni şəbəkədə olan naqilsiz avadanlıqlarda sazlamaların keyfiyyətinə nəzarət edir və müəyyən edilmiş boşluqların aradan qaldırılmasını təmin edir;
- ✓ İstifadəçiləri müdafiə edir, yəni şəbəkənin naqilsiz seqmentindəki qovşaqları qeyri-leqal girişlərdən və hücumlardan müdafiə edir.

IEEE 802.11 şəbəkələrinin fiziki və kanal səviyyəsində təhlükəsizliyini təmin etmək üçün əlavə olaraq aşağıdakı tədbirləri də yerinə yetirmək lazımdır:

- radioəhatə zonasını azaltmaq (əgər siqnal nəzarət edilən zonanın hüdudlarından kənara çıxmasa, müdaxilə riski azalar);
- administratorun yeni parolunu dəyişmək (susmaya görə qəbul olunmuş paroldan fərqli olaraq);
- MAC-ünvanlara görə filtrasiyanı qoşmaq;
- şəbəkənin standart identifikatorunu (SSID - Service Set Identifier) dəyişmək və bu prosesi dövri olaraq yerinə yetirmək;
- şəbəkədaxili şifrələməni aktivləşdirmək;
- müəyyən müddətlərdən sonra şifrələmə açarını dəyişmək;
- şəbəkələrarası ekranları və antivirusları qurmaq;
- şəbəkələrarası ekranlarda trafikin filtrasiyası alqoritmlərinin reallaşdırılmasını təmin etmək;
- şəbəkədə quraşdırılmış avadanlığın rezervini və proqram təminatının surətinin xüsusi sxemini hazırlayaraq, ehtiyat tədbirləri məqsədilə saxlamaq;
- şəbəkədə işləyən avadanlığa dövri nəzarəti həyata keçirmək.

Bütün bu tədbirlər müəssisənin təhlükəsizlik siyasətində nəzərə alınmalı və istənilən tip avadanlıqda reallaşdırma imkanına malik olmalıdır. Qeyd edək ki, bu tələblərin reallaşması praktiki olaraq bütün müasir qurğularda mümkündür.

NƏTİCƏ

Məqalədə Wi-Fi şəbəkələrinə edilən hücumlar və onlardan müdafiə üsullarına baxılmışdır. Şəbəkənin fiziki və kanal səviyyələrinə edilən hücumların vaxtında müəyyən edilməsi və bu hücumlardan davamlı olaraq qorunmaq üçün həll yolları göstərilmişdir. Yaxın gələcəkdə Wi-Fi şəbəkələri üçün yeni təhlükəsizlik standartları meydana gələcəkdir, bu da ümumi təhlükəsizlik səviyyəsini qaldırmağa imkan verəcəkdir.

ƏDƏBİYYAT

[1] Wi-Fi to Carry up to 60% of mobile traffic by 2019// Hamphir UK.– 2015, http://www.juniperresearch.com/press/press- releases/wifi-to-carry-60pc-of-mobile-data-traffic-by-2019.

[2] G.Bora1, S. Bora, S.Singh, S.M.Arsalan, OSI Reference Model: An Overview, International Journal of Computer Trends and Technology, 2014, vol. 7, no. 4, pp. 2014-218.

[3] 802.11-1999 - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications.

[4] А. Б. Бакытов, Я. А. Ратахин, Ж. К Ташенова. Технология широкополосного беспроводного доступа // Актуальные вопросы технических наук: материалы III Междунар. науч. конф. (г. Пермь, апрель 2015 г.). — Пермь: Зебра, 2015. — С. 41-43. https://moluch.ru/conf/tech/archive/125/7424/

[5] Е. Патий, “Проблемы безопасности в беспроводных сетях”, http://www.iso27000.ru/chitalnyi-zai/bezopasnost-bezprovodnyh-

setei/problemy-bezopasnosti-v-bezprovodnyh-setyah/.

[6] A. Masiukiewicz, “Security Threats in Wi-Fi Networks”, Engineering and Science 2016, vol. 1, no.3: pp. 6–11.

[7] А.Я. Приходько Словарь-справочник по информационной безопасности. - М.: Синтег, 2001. - 124 с.

[8] В.Б. Щербаков, С.А. Ермаков Безопасность беспроводный сетей: стандарт IEEE 802.11. - М: РадиоСофт, 2010. - 255 с.

[9] M. H. Yilmaz, E.G. Guvenkaya, H. M. Furqan, S.Kose, H. Arslan. “Cognitive Security of Wireless Communication Systems in the Physical Layer”, Journal of Wireless Communications and Mobile Computing, 2017, pp. 4-5.

[10] R.M. Əliquliyev, N. Ağayev, R.M. Alıquliyev Plagiatlıqla mübarizə texnologiyaları. Bakı, “İnformasiya Texnologiyaları” nəşriyyatı, 2015, səh. 120-124.

SECURITY ISSUES IN WI-FI NETWORK

Tabriz Agashov

Institute of Information Technology of ANAS,

Baku, Azerbaijan

depart4@iit.ab.az, tabriz@science.az

Abstract – Article explores the information security of IEEE 802.11 (Wi-Fi) wireless networks. The layers of the OSI model are showen, and attacks on physical and channel levels are analyzed. Types of these attacks and defense methods are studied.

Keywords – mobile traffic; IEEE 802; OSI model; frame; traffic indication map (TIM).