AZƏRBAYCAN RESPUBLİKASI TƏHSİL NAZİRLİYİ
AZƏRBAYCAN DÖVLƏT İQTİSAD UNİVERSİTETİ

"MAGİSTRATURA MƏRKƏZİ"

Əlyazması hüququnda

AĞAZADƏ TEYMUR TALEH

"SİMSİZ ŞƏBƏKƏLƏRDƏ MƏHSULDARLIĞIN YÜKSƏLDİLMƏSİ ÜSULLARININ TƏDQİQİ"

mövzusunda

MAGİSTR DİSSERTASİYASI

İxtisasın şifri və adı: 060632 - **"İnformasiya texnologiyaları və sistemləri mühəndisliyi"**

İxtisaslaşma: **"İnformasiya texnologiyaları və telekommunikasiya sistemləri**

Elmi rəhbər:
f.- r.e.n., dos. T.Ə.ƏLİYEVA

Magistr proqramının rəhbəri:
akad. Ə.M.ABBASOV

Kafedra müdiri: akad. Ə.M.ABBASOV

BAKI – 2020

MÜNDƏRİCAT

İXTİSARLAR VƏ İŞARƏLƏR

AdHoc	Xüsusən seçilmiş	**NOS**	Şəbəkə əməliyyat sistemi
CDF	Məcmu sıxlıq funksiyası	**OFDM**	Ortoqonal tezlik-bölmə multiplexing
DSSS	Birbaşa ardıcıllıqla yayılmış spektr	**PAN**	Fərdi şəbəkə
EAP	Genişləndirilmiş identifikasiya protokolu	**PHY**	Fiziki qat
FDD	Tezlik bölgüsü Dupleks	**RF**	Radio tezlik
FHSS	Tezlik atlama yayılması spektri	**RSSI**	Qəbul siqnal gücü göstərici
IoT	Əşyalar internet	**RTS/CTS**	Yoxlama siqnalı
ISM	Sənaye, elmi və tibbi	**SNR**	Səs-küy nisbəti
LAN	Lokal şəbəkə	**SSID**	Xidmət dəsti identifikatoru
Li-Fi	İşıq sahəsi	**TCP/IP**	Transmissiya nəzarət protokolu / internet protokolu
MAC	Fiziki ünvan	**TDD**	Vaxt bölüşdürmə
MAN	Regional şəbəkə	**TKIP**	müvəqqəti açar bütövlüyü protokolundan
MANET	Mobil adhoc	**VoWLAN**	Səsli Simsiz lokal şəbəkə
MIMO	Çox giriş çox çıxış	**VPN**	Virtual özəl şəbəkə
MRC	Maksimum nisbətli birləşm	**Wi-Fi**	Simsiz sahə
MU-MIMO	Çox istifadəçili MİMO	**WiMAX**	Mikrodalğalı giriş üçün dünya miqyasında işləmə qabiliyyəti
NIC	Şəbəkə kartı	**WLAN**	Simsiz lokal şəbəkə

GİRİŞ

Mövzunun aktuallığı. Simsiz rabitə texnologiyası ənənəvi simli şəbəkələrə müasir alternativdir. Simli şəbəkələr rəqəmsal cihazları bir-birinə bağlamaq üçün kabellərə əsaslanırsa, simsiz şəbəkələr simsiz texnologiyalara əsaslanır. Simsiz texnologiyalar müxtəlif məqsədlər üçün həm evdə, həm də iş kompüter şəbəkələrində geniş istifadə olunur. Simsiz texnologiyaların mütləq faydaları çox olsa da, bəzi çatışmazlıqlar da var.

Fərqli ssenarilərdə simsiz şəbəkəni dəstəkləmək üçün çox sayda texnologiya hazırlanmışdır. Əsas simsiz texnologiyalara aşağıdakılar daxildir:

- Xüsusilə ev şəbəkələrində və simsiz isti nöqtə texnologiyası olaraq məşhur Wi-Fi.
- Aşağı güc və quraşdırılmış tətbiqlər üçün.Bluetooth
- 5G, 4G və 3G mobil internet.
- ZigBee və Z-Wave kimi simsiz ev avtomatlaşdırma standartları.
- 5G mobil internet və Li-Fi görünən işıq rabitəsi kimi inkişaf mərhələsində olan və lakin gələcəkdə simsiz şəbəkələrdə böyük rol oynaya biləcək digər texnologiyalar.

Simsiz kompüter şəbəkələri simli şəbəkələrlə müqayisədə bir sıra fərqli üstünlüklər təklif edir.

Simsiz texnologiyanın istifadəsinin əsas və ən açıq üstünlüyü təklif etdiyi nəhəng hərəkətlilikdir, simsiz bir cihazı divara bağlanmayan cihazlardan istifadə etməyə imkan vermir, həm də qaçılmaz şəkildə simli şəbəkələrdə işləməli olan zəif kabelləri də aradan qaldırır.

Simsiz çatışmazlıqlar əlavə təhlükəsizlik problemlərini də ehtiva edir. Artıq cihazlarınıza yalnız əl ilə fiziki giriş əldə edilə bilməz, onlara haker otaqları və ya bəzən simsiz giriş nöqtəsindən uzaq olan binalar daxil ola bilər. Simsiz texnologiyalardan istifadənin digər bir mənfi cəhəti hava, digər simsiz qurğular və ya divar kimi maneələrə görə radio müdaxiləsi üçün artan potensialdır.

Əslində, simli və simsiz şəbəkələri müqayisə edərkən dəyər, performans və etibarlılıq kimi bir sıra digər amillər də var.

İnternet xidmətinin ənənəvi formaları telefon xətlərinə, kabel televiziyası xətlərinə və fiber-optik kabellərə etibar edir. İnternetin əsas nüvəsi simli qalsa da, bir neçə alternativ internet texnologiyası evləri və müəssisələri birləşdirmək üçün simsiz istifadə edir. Məsələn, evdə olmadığınız zaman simsiz giriş üçün ictimai Wi-Fi şəbəkələri, evdə simsiz internet üçün sabit simsiz geniş zolaq, peyk interneti və digərləri kimi simsiz internet xidmətləri var.

IoT konsepsiyasının nəticəsi, simsizin əvvəllər istifadə edilmədiyi yerlərə getdikcə daha çox inteqrasiya olunduğunu görürük. Ev şəbəkəsindən başqa, saatlar, soyuducular, nəqliyyat vasitələri və bir çox cihaz - bəzən hətta geyim də tədricən simsiz rabitə imkanları ilə təchiz olunur. Simsiz texnologiyanın təbiətinə görə, bu cihazların hamısı bir-biri ilə sorunsuz inteqrasiya üçün birləşdirilə bilər. Məsələn, telefonu tərk edərkən evinizin istiliyini tənzimləmək üçün ağıllı termostatını işə sala bilər, evə çatdıqda ağıllı işıqlarınızı yandıra bilər və ağıllı tərəzi kilo vermə tərəqqinizə dair nişanları saxlaya bilər.

Simsiz şəbəkə qurmaq üçün müəyyən növ kompüter avadanlığı tələb olunur. Telefonlar və tabletlər kimi portativ cihazlarda quraşdırılmış simsiz radiolar mövcuddur. Simsiz genişzolaqlı marşrutlaşdırıcılar bir çox ev şəbəkəsini gücləndirir. Digər avadanlıq növləri xarici adapterlər və sıra genişləndiriciləridir.

Simsiz şəbəkə avadanlığı inkişaf etdirmək üçün mürəkkəb ola bilər. İstehlakçılar simsiz marşrutlaşdırıcıların və əlaqəli ev şəbəkəsi ötürücülərinin məşhur marka adlarını tanıyırlar, lakin əksəriyyəti daxili komponentlərin ölçüsü və istehsalın fərqliliyi barədə kifayət qədər məlumata malik deyil.

Simsiz texnologiyalar, kompüterlər arasında simsiz rabitə kanallarını qorumaq üçün radio dalğaları və ya mikrodalğaları istifadə edir. Wi-Fi kimi simsiz protokollar arxasında olan bir çox texniki detalları tez-tez başa düşmək vacib olmadıqda, Wi-Fi haqqında əsasları bilmək bir şəbəkəni konfiqurasiya edərkən və problemlərin aradan qaldırılmasında çox kömək edə bilər.

Bu gün bildiyimiz simsiz texnologiya, elmi araşdırmalarda bir neçə onilliklərə gedib çıxdı. Nikola Tesla, məsələn, simsiz şarj kimi istifadə üçün bu gün aktiv bir təhsil sahəsi olmağa davam edən simsiz elektrik işıqlandırması və elektrik ötürülməsi sahəsini önə çəkdi.

Tədqiqat işinin məqsədi: Bu tədqiqat işində əsas məqsədimiz simsiz şəbəkələrin araşdırılıb daha optimal olan şəbəkənin seçilməsi və əsas fundamental bilikləri öyrənməkdir.

Tədqiqatın predmeti: Tədqiqat işinin predmeti simsiz şəbəkə texnologiyalarının inkişaf perspektivləri və cəmiyyətin gələcək həyatındakı rolunu çatdırmaqdan ibarətdir.

Tədqiqatın metodoloji bazası: Tədqiqat işində bir sıra informasiya texnologiyası şirkətlərində adı çəkilən texnologiyaların tətbiqini əsaslandıran faktlar mühüm amil kimi qəbul edilmiş və iş bu sahədə məşhur tədqiqatçıların araşdırmalarının əsasında tamamlanmışdır.

Tədqiqatın mənbəyi: Tədqiqatın obyektinin öyrənilməsi məqsədilə çoxsaylı xarici mənbələrə müraciət edilmiş və xüsusi texniki ədəbiyyat araşdırılmışdır.

Elmi yenilik: Tədqiqat işində simsiz şəbəkə texnologiyası bütün aspektlərdən tədqiq olumuş, bu texnologiyanın gündəlik istifadədə rolu nəzərə alınmaqla onun imkanları naqilli şəbəkə texnologiyalarının müasir alternativi kimi qiymətləndirilmiş və onun tətbiqi zamanı həyata keçiriləcək təhlükəsizlik tədbirlərinin öyrənilməsi və izahına səy göstərilmişdir.

İşin praktiki əhəmiyyəti: Tədqiqat mövzusu müasir informasiya-kommunikasiya texnologiyalarının ən mütəhərrik tərkib hissəsi olan böyük tətbiqi əhəmiyyətə malik simsiz şəbəkə texnologiyasının geniş istifadə imkanları, səmərəliliyi və perspektivliliyi, həmçinin optimal tətbiq xüsusiyyətləri barədə tamamlanmış tədqiqat işi kimi nəzəri cəlb edir.

İşin strukturu və həcmi: Tədqiqat işi girişdən, üç fəsildən, nəticə və təkliflərdən, həmçinin 29 şəkildən və 19 cədvəldən ibarətdir. İşin sonunda istifadə olunan yerli və xarici tədqiqatçıların müəllifi olduğu ədəbiyyat siyahısı verilmişdir.

Dissertasiya işinin girişində mövzunun aktuallığı əsaslandırılmış və simsiz texnologiyaların cəmiyyətdə və məişətdə tətbiqi və üstünlükləri qeyd olunmuşdur.

Dissertasiya işinin üç paraqrafdan ibarət *birinci fəslində* simsiz şəbəkə topologıyaları və cihazları haqqında ümumi məlumat verilmiş, müxtəlif topologiyalı şəbəkələrdə qarşıya çıxan texniki problemlərin səbəbləri izah edilmiş, simsiz şəbəkələrin təhlükəsizlik göstəricilərinin xüsusiyyətləri öyrənilmiş və bu texnologiyaların qurulmasına qoyulan tələblər dəyərləndirilmişdir.

İşin ikinci fəsli 3 paraqrafdan ibarətdir. Bu fəsildə simsiz lokal şəbəkələrin planlaşdırılması və layihələndirilməsi məsələləri, təhlükəsizlik təhdidləri və problemləri tədqiq edilmiş və fəslin sonuncu paraqrafında isə yaranan problemlərin həll yolları qeyd olunmuşdur.

Dissertasiyan işinin *üçüncü fəsli* 2 paraqrafdan ibarət olmaqla simsiz texnologiyaların məhsudladarlığının təhlilinə həsr olunmuşdur. Birinci paraqrafda AdHoc texnologiyasının tətbiqi, üstünlüyü və mənfi xüsusiyyətləri, ikinci paraqrafda MIMO texnologiyasının növləri və üstün cəhəti, üçüncü paraqrafda isə MIMO texnologiyasının məhdudiyyət amilləri qeyd olunmuşdur.

I FƏSİL. SİMSİZ ŞƏBƏKƏ TEXNLOGİYALARI: TƏKAMÜL, TOPOLOGİYALAR VƏ CİHAZLAR

1.1. Simsiz şəbəkə topologiyaları və cihazları

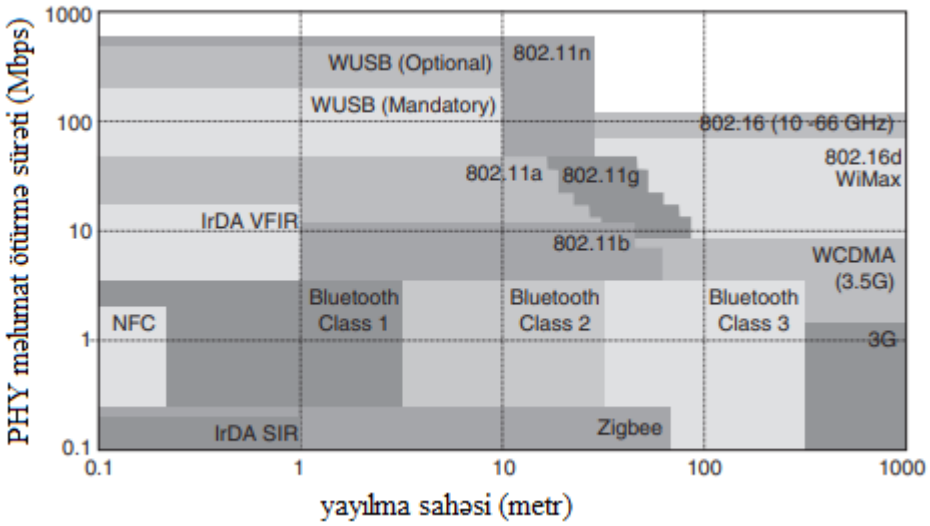
Radio tezliyə əsaslanan simsiz şəbəkənin mənşəyi 1970-ci illərdə Havay Universitetinin ALOHANET tədqiqat layihəsinə aiddir. Simsiz şəbəkənin XX əsrin əvvəllərində yüksək sürətlə böyüyən texnologiyalarından biri olmuşdur. 1997-ci ildə IEEE 802.11 standartı və Wi-Fi Alliance (əvvəllər WECA) tərəfindən qarşılıqlı sertifikatlaşdırmanın sonrakı inkişafına səbəb oldu.

1970-1990-cı illərin əvvəllərinə qədər simsiz bağlantıya artan tələbat, yalnız müxtəlif texnologiyalardan istifadə edərək, fərqli istehsalçıların avadanlıqlarının qarşılıqlı işləməməsi, təhlükəsizlik mexanizmlərinin olmaması və zəif performans təklif edən bahalı qurğuların olması əsas səbəb oldu.

802.11 standartı simsiz şəbəkənin inkişafında mühüm mərhələ güclü və tanınan bir marka - Wi-Fi üçün başlanğıc nöqtəsidir. Bu, avadanlıq xidmət təminatçılarının işinə diqqət yetirir və simsiz şəbəkələrin böyüməsinə əsas texnologiyaların gücü qədər kömək edir.

Orijinal 802.11 standartından meydana gələn müxtəlif Wi-Fi variantları son on ildə sərlövhələrin çoxunu tutduğuna baxmayaraq, digər simsiz şəbəkə texnologiyaları oxşar bir qrafiki izlədi, ilk IrDA spesifikasiyası 1994-cü ildə nəşr olundu. Ericsson 1999-cu ildə IEEE 802.15.1 İşçi qrupu tərəfindən Bluetooth-un qəbul edilməsinə səbəb olan mobil telefonlar və aksesuarlar arasındakı əlaqə mövzusunda araşdırmalara başladı.

Bu sürətli inkişaf dövründə simsiz şəbəkə texnologiyalarının müxtəlifliyi məlumat ötürmə sürəti (həm yüksək, həm də aşağı), əməliyyat diapazonu (uzun və qısa) və enerji istehlakı (aşağı və çox aşağı) üçün bütün tələbləri təmin etmək məqsədilə genişlənmişdir.

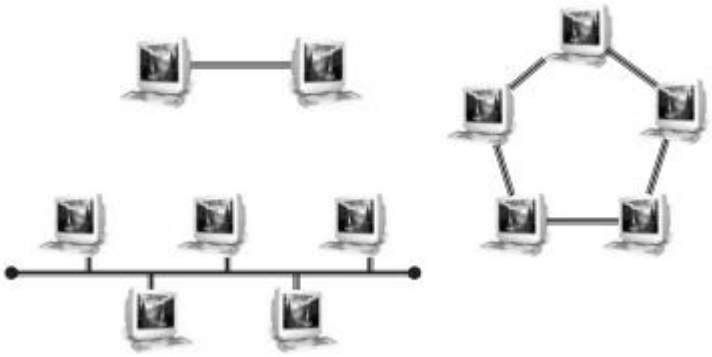


Şəkil 1.1. Simsiz şəbəkə göstəricisi

Bu tələblər şəkil 1.1-də göstərilmişdir. İndi isə əsas şəbəkələrin qurulmasında istifadə olunan topologiyaları nəzərdən keçirək.

Şəkil 1.2-də göstərilən sadə nöqtə, simli şəbəkələrə nisbətən simsiz olaraq daha çox yayılmışdır, çünki müxtəlif simsiz vəziyyətlərdə tapıla bilər, məsələn:

- birranqlı və ya Ad-hoc Wi-Fi əlaqələri
- simsiz MAN əks əlaqənin təmini
- LAN simsiz körpü
- Bluetooth
- İrDA



Şəkil 1.2. Şin və halqavari topologiyalar

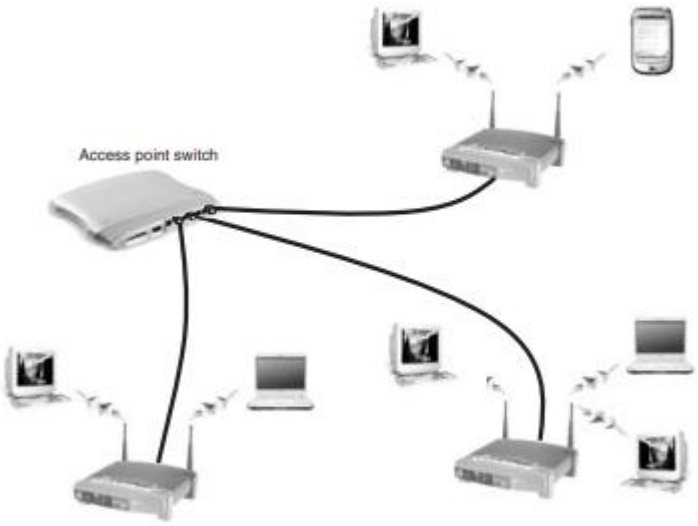
Simsiz şəbəkələr bir ulduz topologiyaya (şəkil 1.3) mərkəzində qovşaq, bu WiMAX baza stansiyası, Wi-Fi giriş nöqtəsi, Bluetooth Master cihaz və ya bir

ZigBee PAN koordinatoru olub, simli bir şəbəkə mərkəzə oxşar rol oynayır. Fərqli simsiz şəbəkə texnologiyaları bu mərkəzi idarəetmə qovşaqları tərəfindən müxtəlif funksiyaların genişləndirilməsini tələb edir və imkan verir.

Şəkil 1.3. Simsiz şəbəkələrdə ulduz topologiyası

Simsiz mühitin tamamilə fərqli təbiəti o deməkdir ki, kommutasiya və keçid olmayan qovşaqlar arasındakı fərq, ümumiyyətlə, simsiz şəbəkələrdə idarəetmə qovşaqları üçün uyğun deyildir, çünki hər bir cihaz üçün ayrıca xəttin birbaşa simsiz ekvivalenti yoxdur. WLAN kommutator və ya kontroller (şəkil 1.4), məlumatları hər paketin ünvanlanan təyinat məntəqəsinə xidmət edən giriş nöqtəsinə ötürən bir simli şəbəkə cihazıdır.

Bu ümumi qaydanın istisnası baza stansiyaları və ya giriş nöqtəsi cihazları sektor və ya serial antenalarından istifadə edərək ayrı-ayrı stansiyaları və ya stansiyalar qruplarını ayrıca ayırdıqda baş verir. Şəkil 1.5, hər biri 90° sektorlu bir antenadan istifadə edərək dörd baza stansiya ötürücüsünü təqdim edən bir keçid olan simsiz MAN-a misaldır.



Şəkil 1.4. Simsiz bir giriş nöqtəsi keçidindən istifadə edərn ağac topologiyası

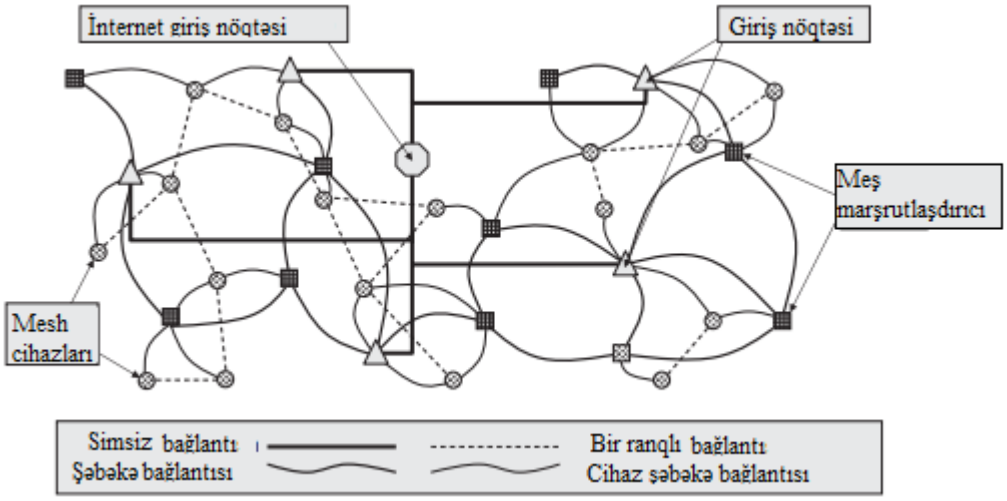
WLAN vəziyyətində, bir giriş nöqtəsi serialı adlanan yeni bir sinif istifadə edərək, WLAN nəzarətçisini şəbəkə tutumunu çoxaltmaq üçün sektor antenaları ilə birləşdirən bir boşluq istifadə edə bilərik. Ayrı-ayrı fəza zonalarına və ya yayılma yollarına müraciət etməklə şəbəkə ötürmə qabiliyyətinin çoxalmasının ümumi üsulu kosmik bölgü multipleksiyası kimi tanınır.

MANET olaraq da bilinən mesh şəbəkələri, düyünlərin mobil olduğu yerli və ya böyük şəhər şəbəkəsidir və mərkəzi nəzarətçilərə ehtiyac olmadan birbaşa qonşu qovşaqlarla əlaqə qurur. Ümumiyyətlə, şəkil 1.5-də göstərilən bir şəbəkənin topologiyası düyünlər şəbəkəyə daxil olduqda və çıxdıqda davamlı dəyişə bilər və məlumat paketləri paralel olaraq qovşaqdan qovşaq hədəflərinə ötürülür.

Məlumatların yönləndirilməsi funksiyası bir və ya daha çox xüsusi cihazın nəzarəti altında deyil, bütün mesh boyunca paylanır. Bu, məlumatların İnternetdə dolaşması ilə bir paketin bir cihazdan digərinə təyinat nöqtəsinə çatana qədər atlanmasına bənzəyir, baxmayaraq ki, mesh şəbəkələrdə, yönləndirmə imkanları yalnız xüsusi marşrutlaşdırıcılarda deyil, hər qovşaq daxil edilir.

Bu dinamik marşrutlaşdırma qabiliyyəti hər bir cihazdan marşrut məlumatlarını bağladığı hər bir cihazla əlaqələndirməsini və qovşaqların içərisində hərəkət etməsini, birləşməsini tələb edir.

Bu paylanmış nəzarət və davamlı konfiqurasiya, yüklənmiş, etibarsız və ya pozulmuş yolların ətrafında yenidən istiqamətlənməyə imkan verir, mesh şəbəkələrinin alternativ yolları təmin etmək üçün düyünlərin sıxlığının kifayət qədər yüksək olması şərti ilə öz-özünə bərpa və çox etibarlı olmağa imkan verir. Yönləndirmə protokolunun dizaynındakı əsas problem, məlumat mesajlarının yönləndirilməsi ilə alınan məlumat ötürmə qabiliyyəti baxımından bu davamlı yenidən konfiqurasiya qabiliyyətinə, idarəolunan yerüstü imkan ilə nail olmaqdır.



Şəkil 1.5. Mesh Şəbəkə topologiyası

Bir mesh şəbəkədəki yolların çoxluğu simli şəbəkə açarları və sektorlu simsiz şəbəkələr üçün göstərilən çox sayda yol olduğuna görə ümumi şəbəkə ötürücüsünə oxşar təsir göstərir.

Mesh şəbəkəsinin tutumu düyünlərin sayına və buna görə istifadə edilə bilən alternativ yolların sayına görə böyüyəcəkdir ki, tutum sadəcə meshə daha çox qovşaq əlavə etməklə artırıla bilər.

Marşrutlaşdırma məlumatlarının səmərəli toplanması və yenilənməsi problemi ilə yanaşı, mesh şəbəkələri bir sıra əlavə texniki problemlərlə üzləşirlər:

■ **Simsiz bağlantı etibarlılığı** - bir hub və hop konfiqurasiyasındakı tək bir hopa görə qəbul edilə bilən bir paket xətası sürətlə birdən çox hops üzərində birləşəcək və bir meshin böyüdüyü və təsirli qalacağını məhdudlaşdıracaqdır.

■ **Mütəmadi rouminq** - hərəkətsiz qovşaqların bir-birinə bağlanması və yenidən qurulması simsiz şəbəkə standartlarının əksəriyyətində tələb olunmur,

baxmayaraq ki, 802.11 Tapşırıq Qrupları (TGr və TGs) bu mövzuya müraciət edirlər.

■ **Təhlükəsizlik** - sabit bir infrastrukturu olmayan bir şəbəkə istifadəçilərini necə eyniləşdirmək olar?

Praktik nöqteyi-nəzərdən, mesh şəbəkələrinin özünü tənzimləyən, özünü optimallaşdıran və özünü müalicə edən xüsusiyyətləri geniş miqyaslı simsiz şəbəkə yerləşdirmələri ilə əlaqəli bir çox idarəetmə və texniki vəzifəni aradan qaldırır.

ZigBee açıq bir şəkildə LAN şəbəkələrini dəstəkləyən və IEEE 802.11 TG-lər WLAN mesh şəbəkələrini əhatə edən standartı hazırlamaq mərhələsindədir. Artıq 802.11s mesh təkliflərini, Wi-Mesh Alliance və SEEMesh (Sadə, Səmərəli və Genişlənən Mesh) təşviq etmək üçün iki standart orqanı quruldu. Şəbəkə toplogiyalarına baxdıq, indi isə şəbəkələrin qurulmasında istifadə olunan cihazlara baxaq.

NIC bir PDA, laptop və ya masaüstü kompüter kimi bir cihazı simsiz bir stansiyaya çevirir və cihazın bir ranqlı şəbəkəsində və ya bir giriş nöqtəsi ilə digər stansiyalarla əlaqə qurmasına imkan verir.

Simsiz NIC-lər PC və PCI kartları daxil olmaqla müxtəlif forma faktorlarında, xarici USB cihazları, USB ötürücü və ya PDA-lar üçün kompakt flaşlarda mövcuddur. Simsiz NIC-lərin əksəriyyəti inteqrasiya edilmiş antenalara malikdir, lakin bir neçə istehsalçı NIC-ləri xarici antenna bağlantısı və ya simsiz diapazonun həddinə yaxın işləyərkən yüksək gəlirli bir anten əlavə etmək üçün yararlı ola bilər.

Bir simsiz NIC-ni digərindən ayıran xüsusiyyətlər azdır. Maksimum ötürücü güc yerli tənzimləmə tələbləri ilə məhdudlaşır və standartlara əsaslanan avadanlıq üçün müvafiq qurum tərəfindən sertifikatlaşdırma (802.11 üçün Wi-Fi sertifikatı kimi) müxtəlif istehsalçıların avadanlıqlarının qarşılıqlı fəaliyyətini təmin edəcəkdir. İstisna, bəzi istehsalçılar tərəfindən 802.11n təsdiqlənmədən əvvəl elan edilmiş əvvəlcədən avadanlıq kimi standart təsdiqlənmədən əvvəl buraxılmış xüsusi uzantılar və ya avadanlıqlar olacaqdır.

Yüksək səviyyəli mobil məhsullar, xüsusən laptop kompüterlər, inteqrasiya olunmuş simsiz NIC ilə getdikcə daha çox göndərilir və İntelin Centrino® texnologiyası ilə WLAN interfeysi əsas çipset ailəsinin bir hissəsi oldu.

Giriş nöqtəsi WLAN şəbəkədəki digər stansiyalarla simsiz rabitə mərkəzi təmin edir. Giriş nöqtəsi ümumiyyətlə simli bir şəbəkəyə qoşulur və simli və simsiz qurğular arasında bir körpü təmin edir.

İndi fat giriş nöqtələri adlandırılan ilk nəsil giriş nöqtələri 1999-cu ildə IEEE 802.11b standartını təsdiqlədikdən sonra görünməyə başladı və hər bölmənin daxilində emal və nəzarət funksiyalarının tam çeşidini təmin etdi:

- identifikasiya və şifrələmə dəstəyi kimi təhlükəsizlik xüsusiyyətləri
- siyahılar və ya filtrlər əsasında giriş nəzarəti
- SNMP konfiqurasiya imkanları

Adətən, veb əsaslı bir interfeys istifadə edərək giriş səviyyəsinin istifadəçi konfiqurasiyasını tələb edən güc səviyyəsi parametrlərini, RF kanal seçimi, təhlükəsizlik şifrələməsi və digər tənzimlənən parametrləri ötürür.

Bu əsas funksiyanı təmin etməklə yanaşı, ev və ya kiçik ofis simsiz şəbəkə üçün nəzərdə tutulmuş giriş nöqtələri, cədvəl 1.1-də göstərildiyi kimi, bir sıra əlavə şəbəkə xüsusiyyətlərini də əhatə edir.

Xüsusi giriş nöqtəsinin işləməsi ***Cədvəl 1.1.***

Xüsusiyyət	**Təsvir**
Internet Gateway	Bir sıra funksiyaları dəstəkləyən: marşrutlaşdırma, Şəbəkə Ünvanı Tərcümə, Müştəri stansiyalarına dinamik IP ünvanlarını təmin edən DHCP server və VPN.
kommutasiya hub	Bir sıra Ethernet cihazları üçün keçid mərkəzi imkanlarını təmin edən bir neçə simli Ethernet portu daxil edilə bilər.
Simsiz körpü və ya təkrarlayıcı	Bir rele stansiyası kimi fəaliyyət göstərə bilən, başqa bir giriş nöqtəsinin işləmə dairəsini genişləndirmək və ya iki şəbəkə arasında qovşaq-qovşaq simsiz körpü kimi çıxış edə bilən giriş nöqtəsi.
Şəbəkə saxlama server	Simsiz stansiyalar üçün mərkəzləşdirilmiş sənəd saxlamağı və ehtiyat nüsxəni təmin edən xarici yaddaşa qoşulmaq üçün daxili sabit disklər və ya limanlar.

Yuxarıda təsvir olunan birinci nəsil "fat" giriş nöqtəsindən fərqli olaraq, zəruri RF rabitə funksiyalarına giriş nöqtəsi imkanlarını məhdudlaşdıran və WLAN keçidindəki idarəetmə funksiyalarının mərkəzləşdirilməsinə güvənən "thin" giriş nöqtələri də mövcuddur.

Şəkil 1.6. Birinci nəsil simsiz giriş nöqtələri (Belkin Corporation, D-Link (Europe) Ltd. və Linksys (Cisco Systems Inc-in bir bölməsi) nəzarəti)

Böyük bir simsiz şəbəkədə, ümumiyyətlə onlarla və bəlkə də yüzlərlə giriş nöqtəsi olan bir korporativ mühitdə, giriş nöqtələrini fərdi şəkildə konfiqurasiya etmək WLAN idarəçiliyini mürəkkəb bir vəziyyətə gətirə bilər. WLAN kommutatorları, geniş miqyaslı WLAN-ların yerləşdirilməsini və idarə edilməsini asanlaşdırır. WLAN kommutatoru, bir sıra asılı və ya thin giriş nöqtələri adından müxtəlif funksiyaları idarə etmək üçün hazırlanmış bir şəbəkə infrastrukturu cihazıdır (Şəkil 1.7) .

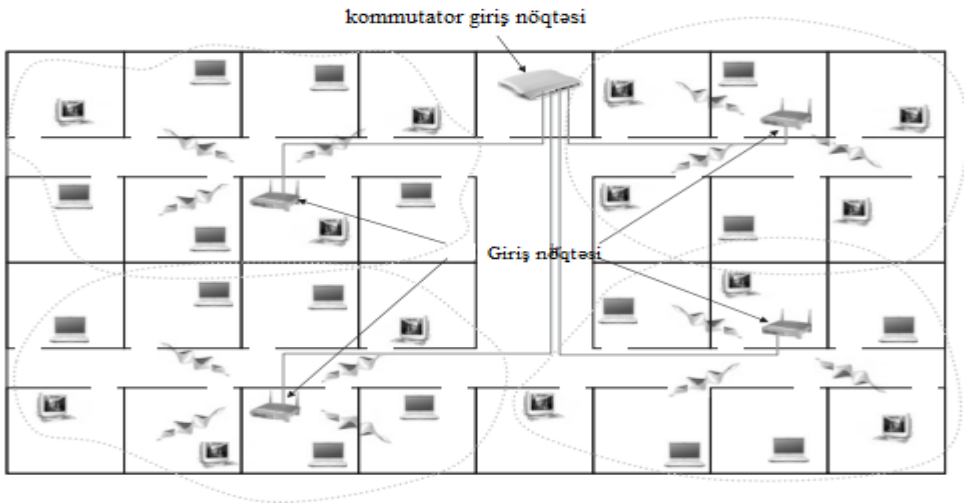
Cədvəl 1.2-də göstərildiyi kimi, bu geniş WLAN tətbiqetmələri, xüsusən səs xidmətləri dəstəkləyənlər üçün bir sıra üstünlüklər təqdim edir. Simsiz keçidin inkişafının arxasında dayanan driver, simsiz şəbəkələrin böyüdükcə getdikcə mürəkkəbləşən və vaxt aparan şəbəkə konfiqurasiyası və idarə edilməsi vəzifəsini təmin etməkdir. Simsiz keçid, müəssisə miqyaslı WLAN-da zəruri olan konfiqurasiya, təhlükəsizlik, performans monitorinqi və problemlərin aradan qaldırılması üçün mərkəzləşdirilmiş idarəetmə təmin edir.

"İncə" giriş nöqtəsinin üstünlükləri ***Cədvəl 1.2.***

Üstünlük	Açıqlama
Aşağı qiymət	İncə giriş nöqtəsi, ilkin avadanlıq qiymətini, həmçinin gələcək təmir və yenilənmə xərclərini azaltmaqla, simsiz rabitə funksiyalarını səmərəli həyata keçirmək üçün optimallaşdırılmışdır.
Sadələşdirilmiş giriş nöqtəsi idarəetməsi	Təhlükəsizlik nöqtələri daxil olmaqla giriş nöqtəsi konfiqurasiyası şəbəkə idarəetmə vəzifəsini asanlaşdırmaq üçün mərkəzləşdirilmişdir.
Təkmilləşdirilmiş rouminq performansı	Rouminq təhvil vermə şərti giriş nöqtələri ilə müqayisədə daha sürətli olur və səs xidmətlərinin işini yaxşılaşdırır.
Sadələşdirilmiş şəbəkə yeniləmələri	Mərkəzləşdirilmiş əmr və idarəetmə qabiliyyəti, inkişaf edən WLAN standartlarına cavab olaraq şəbəkəni yeniləməyi asanlaşdırır, çünki yeniləmələr yalnız keçid səviyyəsində tətbiq olunmalı və fərdi giriş nöqtələrinə deyil.

Təhlükəsizliyi nümunə olaraq götürək, WEP, WPA və 802.11i ilə, hamısı eyni vaxtda böyük bir WLAN yerləşdirilməsində istifadə olunur, əgər təhlükəsizlik konfiqurasiyası fərdi giriş nöqtələri, şifrələmə açarlarının müntəzəm idarə edilməsi və dövri yenilənmə hər quraşdırılmış giriş nöqtəsi üçün təhlükəsizlik standartları ayrı-ayrılıqda işlənsə şəbəkə idarəolunmaz hala gəlir.

Simsiz bir kommutator tərəfindən təmin edilmiş mərkəzləşdirilmiş təhlükəsizlik arxitekturası ilə bu idarəetmə işləri yalnız bir dəfə yerinə yetirilməlidir.



Şəkil 1.7. WLAN Topologiyasında simsiz kommutatordan istifadə

Nöqtəli WLAN və ya WMAN əlaqələrini təmin edən simsiz körpü komponentləri, bir sıra istehsalçılardan, açıq havada istifadə üçün hava keçirməyən

kassalarda qablaşdırılır (Şəkil 1.8). D-Link DWL 1800, 25 km məsafəni çatdırmaq üçün 24 dBm və ya 14 dBm ötürmə gücünü təmin edən 2.4 GHz radio ilə 16 dBi düz panelli antenanı birləşdirən bir nümunədir.

Şəkil 1.8. Xarici simsiz körpülər

Bir çox sadə WLAN giriş nöqtələri də şəbəkə körpüsünü dəstəkləyir və ya bu imkanı təmin etmək üçün bir firmware yenilənməsi ilə artırıla bilər.

Bu cihazların konfiqurasiyası sadəcə digər nöqtənin MAC ünvanını hər stansiyanın giriş nəzarət siyahısına daxil etməyi özündə cəmləşdirir ki, hər stansiya yalnız körpünün digər uc nöqtəsi ilə ötürülən paketləri açar. WLAN şəbəkələrin qurulmasında istifadə olunan cihazları nəzərdən keçirdik. İndi biz PAN şəbəkələrin qurulmasında istifadə olunan əsas cihazları nəzərdən keçirək.

Fərdi ev şəbəkəsi ilə ən çox təyin olunan Bluetooth-dan ZigBee-yə qədər, ilk növbədə ev və sənaye nəzarət cihazları şəbəkəsini yaratmağa yönəlmiş geniş çeşidli PAN texnologiyaları təsvir ediləcəkdir. Əslində, Wi-Fi cihazlarının aralığını bərabər tuta bilən yüksək gücü Bluetooth radioları ilə PAN və LAN şəbəkə arasındakı sərhəd mövqedə durur və mövcud məlumat sürətinin məhdudlaşdırılması daxilində WLAN cihazlarının əksəriyyəti Bluetooth texnologiyasından istifadə edərək eyni dərəcədə yaxşı qurula bilər. Bluetooth cihazlarının ən çox yayılmış növləri və onların əsas xüsusiyyətləri cədvəl 1.3-də ümumiləşdirilmiş və Şəkil 1.9-da göstərilmişdir.

Şəkil 1.9. Müxəlif Bluetooth cihazları.

Bluetooth cihazları və xüsusiyyətləri ***Cədvəl 1.3.***

Bluetooth cihazı	**Əsas Xüsusiyyətlər**
Cib telefonu	Bluetooth səssiz qulaqlıq ilə interfeys. Faylları köçürmək və ya geri qaytarmaq üçün PDA və ya PC-yə qoşulun. Digər Bluetooth cihazları ilə əlaqə məlumatlarını (vizit kartları), təqvim girişlərini, şəkilləri və s.
PDA	Faylları köçürmək və ya geri qaytarmaq üçün PC-yə qoşulun. Bluetooth giriş nöqtəsi ilə İnternetə qoşulun. Digər Bluetooth cihazları ilə əlaqə məlumatlarını (vizit kartları), təqvim girişlərini, şəkilləri və s.
Səs ötürücü	Bir kompüterdən və ya hi-fi sistemindən Bluetooth qulaqlıqlarına səs axını.
Giriş nöqtəsi	Bluetooth effektiv cihazları daxil etmək üçün bir LAN genişləndirin. Bluetooth cihazları üçün İnternet bağlantısı.
Bluetooth adapterləri	Bluetooth, dizüstü və ya PDA kimi bir sıra cihazları aktivləşdirir. WLAN NICS-ə gəldikdə, bunlar bir sıra forma amillərində mövcuddur, USB dongles ən populyardır. Hər hansı bir seriyalı RS-232 cihazına plug-play bağlantısı üçün seriya adapter.

Simsiz USB kimi simsiz PAN texnologiyaları inkişaf etdikcə bu şəbəkələri dəstəkləmək üçün müqayisə edilə bilən bir sıra cihaz inkişaf etdiriləcəkdir. Bu yeni texnologiyalara xas olan yeni imkanlar yeni xidmətlər təklif edən yeni cihaz növləri ilə nəticələnəcəkdir. Bu nümunə çox lentli OFDM radiosunun simsiz USB stansiyasını fasiləsiz tapmaq imkanı verir və yer mərkəzli xidmətlərə etibar edən cihazların potensialını təklif edir.

ZigBee,bu, əvvəlcə ev avtomatlaşdırılmasına yönəldiləcək, lakin daha yüksək məlumat dərəcəsi tələb etməyən tətbiqlərdə Bluetooth üçün əvəzolunma da daxil olmaqla geniş tətbiq tapacaqdır.

Hal-hazırda mövcud və gözlənilən ZigBee cihazlarının bir sıra əsas xüsusiyyətləri cədvəl 1.4-də ümumiləşdirilmişdir.

ZigBee Cihazları və Xüsusiyyətləri ***Cədvəl 1.4.***

ZigBee cihazı	Əsas Xüsusiyyətlər
PC giriş cihazları	Bir PC siçanı və ya klaviatura ilə simsiz əlaqə.
Avtomatlaşdırma cihazları	İstilik, işıqlandırma və təhlükəsizlik kimi ev və sənaye avtomatlaşdırma funksiyaları üçün simsiz idarəetmə cihazları.
Simsiz uzaqdan idarəetmə	Televizor və s. üçün uzaq məsafəni əvəz etmək və mənzərə və hizalanma məhdudiyyətini aradan qaldırmaq.
Sensor modem	Ev və ya sənaye avtomatlaşdırılması üçün mövcud bir sıra mövcud loop sensorlar üçün simsiz şəbəkə interfeysi təmin edir.
Ethernet Şlyüz	ZigBee son cihazlarını və ya Ethernet şəbəkəsindən marşrutlaşdırıcıları əmr etməyə imkan verən bir ZigBee şəbəkə koordinatoru.

Təcrübədə, PAN əməliyyat diapazonu ümumiyyətlə on metrdən aşağı olduğundan, Bluetooth və digər PAN cihazları adətən sadə inteqrasiya edilmiş omnidirectional antenalardan istifadə edəcəklər. Bununla birlikdə 2.2 GHz ISM radio lentini 802.11b/g WLAN ilə bölüşən Bluetooth kimi PAN-lar üçün PAN cihazlarının geniş diapazonda işləməsini təmin etmək üçün yuxarıda təsvir olunan geniş WLAN xarici antenaları da mövcuddur. Simsiz fərdi şəbəkələrinin (WPAN) əsas cihazlarını antenayla bitirək. Son olaraq MAN şəbəkələrinin qurulmasında istifadə olunan cihazlara baxaq.

WLAN və PAN-lar çox müxtəlif topologiyalar təqdim edir və cihaz növləri, bu günə qədər simsiz MAN cihazları yalnız sabit bir qovşaq-qovşaq və çox qovşaqlı topologiyaya xidmət göstərmişdir, bunlar əslində yalnız iki cihaz növünü, baza stansiyasını və müştəri stansiyasını tələb edir.

Bununla birlikdə, 802.16e standartının (həmçinin 802.16-2005 təyin olunduğu) təsdiqlənməsindən sonra, genişzolaqlı İnternet tezliklə mobil qurğulara təqdim ediləcək və mobil telefonlar və PDA-ların yaxınlaşmasına səbəb olan bir sıra yeni mobil simsiz MAN cihazları yaranır.

Sabit simsiz MAN tətbiqetmələri üçün simsiz şəbəkə qurğuları, əslində son mil genişzolaqlı internet çıxışı üçün iki kateqoriyaya bölünür - əsas stansiya avadanlığı və müştəri binaları avadanlığı (CPE).

Şəkil 1.10. Mikro və Makro WMAN əsas stansiyası avadanlığı

Fərqli miqyaslı simsiz MANları dəstəkləmək üçün baza stansiyası avadanlıqlarının bəzi nümunələri Şəkil 1.10-də göstərilmişdir. Göstərilən makro miqyaslı baza stansiyası sıx metropoliten bölgələrində minlərlə abunəçini dəstəkləyə bilər, mikro miqyaslı avadanlıq isə seyrək kənd yerlərində daha az istifadəçi sayını dəstəkləmək üçün hazırlanmışdır. Baza stansiyası və CPE cihazlarının bəzi növləri və əsas xüsusiyyətləri cədvəl 1.5-də ümumiləşdirilmişdir.

Simsiz MAN cihazları və xüsusiyyətləri ***Cədvəl 1.5.***

WMAN cihazı	**Tipik xüsusiyyətlər**
Susmaya görə sazlanmış qapalı CPE	Müştəri PC və ya şəbəkəsinə əsas WMAN bağlantısı. Görmə qabiliyyəti olmayan qəbulu yaxşılaşdırmaq üçün çoxsaylı müxtəliflik və ya uyğunlaşdırıcı serial antenaları.
Açıq CPE	Xarici antenna və radio. Daha yüksək anten qazanma və daha uzun diapazon təmin edir.
Əsas stansiya avadanlığı	Modul və ölçülən bir tikinti. Makro və sıx bir şəhər və ya seyrək kənd qurğuları üçün mikro konfiqurasiyalar. Çevik bir RF kanalından istifadə, bir antendən çox sektora qədər bir kanaldan bir anten sektoruna qədər çox kanala qədər.
İnteqrasiya edilmiş şəbəkə qapısı	Şəbəkə qapısı funksiyaları ilə MAN interfeysi (Marşrutlaşdırma, NAT və firewall imkanları). İstəyə uyğun inteqrasiya olunmuş WLAN giriş nöqtəsi ilə. VoIP telefoniya kimi əlavə WISP xidmətlərini dəstəkləmək üçün quraşdırılmış CPU.

Sürətli istifadəçiyə genişzolaqlı internet təmin edən mobil simsiz MAN xidmətləri və cihazlarının ilk tətbiqi, WiBro standartının sürətli inkişafı ilə izah edilən Cənubi Koreyanın bazarında olmuşdur. Lisenziyalı spektrin istifadəsi və 2005-ci ildə üç telekom şirkətinə əməliyyat lisenziyalarının verilməsi ilə kommersiya alışları da sürətləndi.

Mobil internet xidmətləri təqdim edən cihazların forma faktoru, telefon və PDA imkanlarını birləşdirmək ehtiyacını - WAP telefonlarında yaşanan

məhdudiyyətləri aradan qaldırmaq üçün daha böyük bir ekran və QWERTY girişi əks etdirir. Şəkil 1.11, Samsung tərəfindən hazırlanmış iki erkən WiBro telefonu göstərir.

Şəkil 1.11. Simsiz MAN İşləyən Telefonlar

1.2. Simsiz şəbəkələrin səmərəlilik göstəriciləri

OPNET [1] istər hərbi, istərsə də ticari simsiz şəbəkələri bir zaman kritik tədqiqat ssenarisində təhlil etmək üçün kifayət qədər sədaqətlə modelləşdirmə qabiliyyətinə malikdir. TMM, ərazi təsirləri səbəbiylə siqnal itkisini nəzərə alaraq OPNET simulyasiyalarınızın dəqiqliyini artırmağa imkan verir. TMM hər iki fiziki xüsusiyyətdən (məsələn, dağlar və yerin əyriliyi) və ətraf mühit amilləri (yer keçiriciliyi və yerüstü refraktivlik) siqnal itkisini hesablamaq üçün giriş kimi istifadə edə bilər.

Bu yazıda müxtəlif ərazilərin simsiz rabitəyə təsirini araşdırmaq üçün TMM-dən istifadə etdik. Buraya iki yayılma modeli daxildir: **Azad zona və Longley-Rice**. TIREM yayma modeli OPNET-dən əlavə bir modul olaraq mövcuddur. Bundan əlavə, lazım olduqda xüsusi yayma modelləri yarada bilərsiniz. TMM OPNET və Simsiz modul quraşdırıldıqda bir neçə imkan əlavə edir: 1) yol itkisi hesablamalarında ərazi effektlərinin nəzərə alınması, 2) yüksəklik xətlərinin arxa

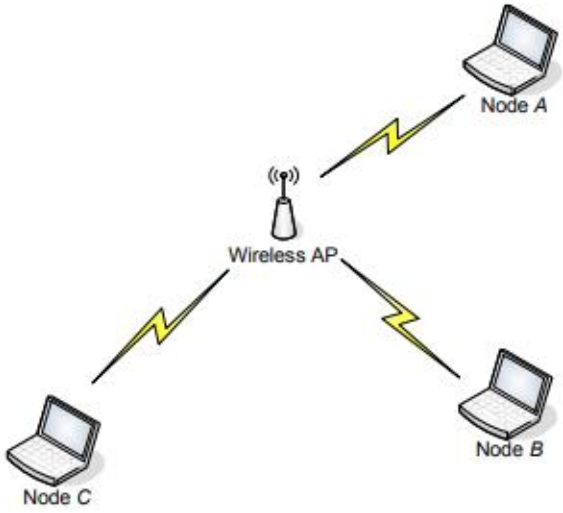
plan və ya görüntüdə göstərilməsi və 3) müəyyən edilmiş yol boyu ərazi və siqnal gücünün görüntülənməsi.

Əlavə olunan bu imkanlar simsiz şəbəkə simulyasiyasının düzgünlüyünə aşağıdakı üstünlükləri gətirir: 1) ötürücülərin ərazi səbəbi ilə əlaqə qura biləcəyini müəyyən etməyə kömək edir; 2) ətraf mühit şəraitinin kommunikasiyaya təsirini təyin etməyə kömək edir; 3) dəqiqliyi artırır yayılma itkisi, siqnal gücü və səs-küyü təyin edir.

Bundan əlavə, RTS / CTS mexanizminin WLAN-da toqquşma təsiri burada araşdırılmışdır. WLAN-da toqquşma aşkarlanması çətindir, çünki bütün simsiz stansiyalar hər zaman bir-birini dinləyə bilməyəcəklər. Bir stansiya bütün digər stansiyaların aralığında olmaya bilər. Şəkil 1.12-də A, B və C qovşaqları giriş nöqtələri arasındadır, lakin hər biri digərləri daxilində deyil.

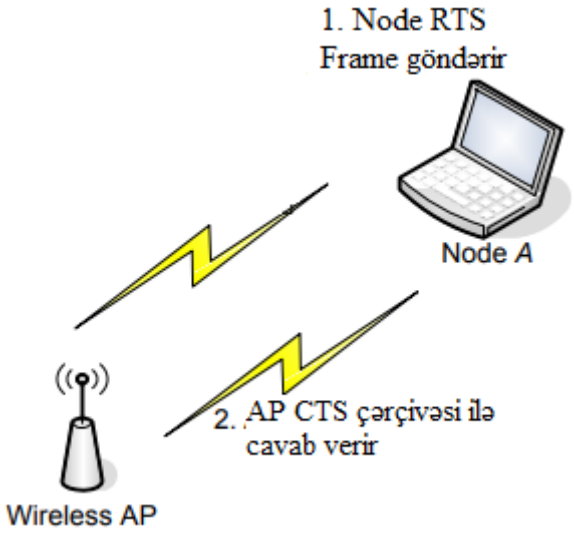
Qovşaq A Qovşaq C-dən B ötürülməsini aşkarlaya bilər, lakin Qovşaq C-dən deyilsə, Qovşaq C heç bir trafik eşitmirsə, Qovşaq C əslində ötürüldüyündə mühitin sərbəst olduğunu güman edə bilər. Bu problem gizli terminal problemi (və ya gizli qovşaq problemi) kimi tanınır [2]. Bu vəziyyətdə, A Qovşaq ötürülməyə başlasa, toqquşma baş verəcəkdir. Nəticədə, həm Qovşaq A, həm də Qovşaq C, daha yüksək yerüstü və aşağı ötürmə qabiliyyəti ilə nəticələnən paketlərini geri göndərməlidirlər. Gizli qovşaq səbəbindən toqquşma baş verdikdə stansiyaya girişə nəzarət etmək üçün RTS / CTS (Göndərmək üçün Göndərmə / Göndərmək üçün Sil) funksiyasının əlavə bir xüsusiyyəti IEEE 802.11 standartına [3] daxil edilmişdir. Bu seçim virtual daşıyıcı sensasiya kimi də tanınır. Düzgün istifadəsi ilə yanaşı, RTS / CTS mexanizminin WLAN-da toqquşma təsiri bu sənəddə araşdırılmışdır.

RTS / CTS-in düzgün istifadəsi ilə WLAN əməliyyatını dəqiq tənzimləyə bilərik, çünki gizli qovşaq problemini həll edir və toqquşmadan əlavə qorunma təmin edir [4].



Şəkil 1.12. Gizli Node problemi

Müəyyən bir stansiyada RTS / CTS təmin etsəniz, stansiya bir giriş nöqtəsi kimi başqa bir stansiya ilə RTS / CTS əlaqəsini tamamlayana qədər məlumat çərçivəsini göndərməkdən çəkinəcəkdir. Bir stansiya bir RTS çərçivəsi göndərərək prosesi başlatır. Giriş nöqtəsi (AP) və ya başqa bir stansiya RTS alır və CTS çərçivəsi ilə cavab verir. Məlumat stansiyası göndərməzdən əvvəl stansiya CTS çərçivəsini almalıdır.



Şəkil 1.13. RTS / CTS-dən istifadə edərək xəttin rezervasiyası

CTS ayrıca, digər stansiyaların RTS-i işə salan stansiya məlumatlarını ötürərkən orta səviyyəyə girməməsi üçün xəbərdarlıq edən bir zaman dəyərini ehtiva

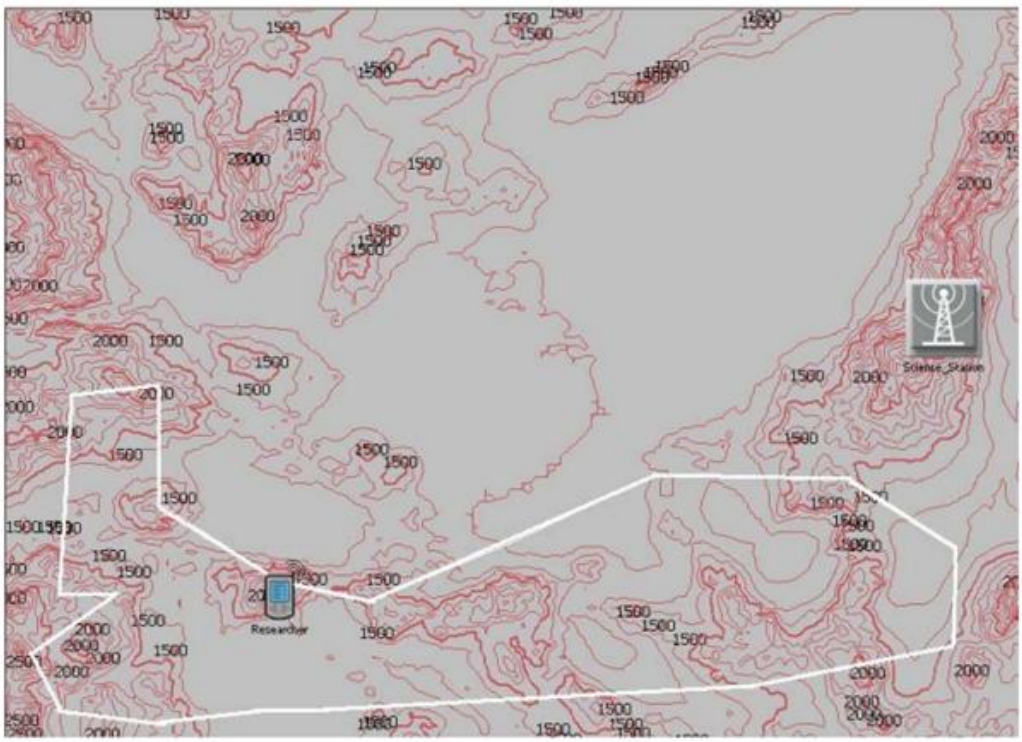
edir. Beləliklə, RTS / CTS-dən istifadə toqquşmaların sayını azaldır və WLAN-ın işini yaxşılaşdırır.

Yerüstü tətbiqetmənin (yəni, RTS / CTS çərçivələri) tətbiqi və yerüstü keçidin azaldılması (yəni daha az ötürmə) RTS / CTS istifadə WLAN-ın işini artıracaqdır. Şəbəkədə heç bir gizli qovşaq yoxdursa, RTS / CTS-dən istifadə yalnız ötürücülük miqdarını artıracaq və ötürmə qabiliyyətini azalda bilər. Bu vəziyyətdə, əlavə RTS / CTS çərçivələri qazandığınızdan daha çox köçürmələri azaltmaqla xərci çoxalır. Üstəlik, məlumat çərçivəsi RTS çərçivəsindən daha uzun olduqda, xüsusilə RTS / CTS istifadəsi daha faydalıdır [5].

Bu yazıda RTS / CTS mexanizminin IEEE 802.11 şəbəkəsinin fəaliyyətinə təsirini qiymətləndiririk. İki fərqli ssenarini simulyasiya etmək və nəticələri müqayisə etmək üçün OPNET Modeler [6] istifadə edirik. Növbəti hissələrdə TMM və RTS / CTS vəziyyətləri üçün simulyasiya mühitlərini müzakirə edirik və simulyasiya təcrübələrimizin nəticələrini təhlil etdik. Sonda əldə etdiyimiz nəticələri müzakirə etdik. Növbəti simulyasiyanı izah edək.

Burada şərqdə yerləşən ötürücü ilə daimi bir əlaqə olan bir simsiz cihazı olan bir hərəkət edən bir tədqiqatçı var. Hərəkət traektoriyasının hər bir hissəsi 10 dəqiqəlik bir addım üçün təyin edilir və simulyasiya beş saatlıq müddətə tətbiq olunur. Bu simulyasiya zamanı simsiz cihazın hündürlüyü 500 ilə 2500 fut arasında dəyişir.

Anten hündürlüyünün, yüksəlişin və ötürücü ilə qəbuledici arasındakı məsafənin dəyişməsi səbəbindən radio siqnal gücünə müxtəlif təsirləri müəyyənləşdiririk. Kök dağlarda (müxtəlif ərazilərdə) yayılan radio siqnallarını simulyasiya edərək, qəbuledicinin bir çox yüksəklik dəyişikliyindən keçən bir simulyasiya edilmiş bir yol üzərində hərəkət etdiyi üçün siqnal gücündəki dəyişiklikləri görə bilirik. Şəkil 1.14 ötürücü, qəbuledici və traektoriya daxil olmaqla vəziyyəti göstərir.



Şəkil 1.14. TMM üçün simulyasiya quraşdırma

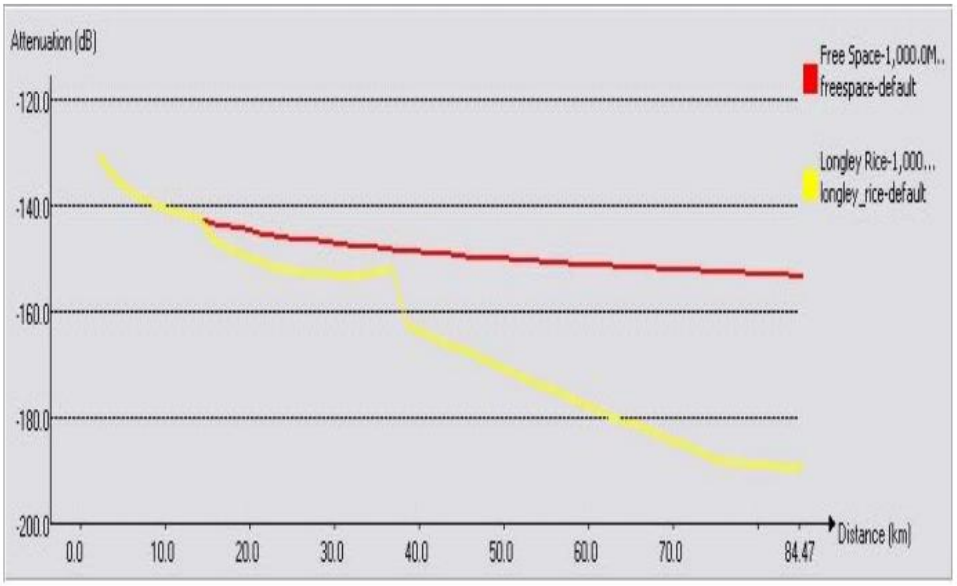
Siqnal gücünü daha yaxından nəzərdən keçirmək üçün təsirlərini hesablamaq üçün iki tanınmış yayılma modelindən istifadə etmək qərarına gəldik.

- Boş ərazi modeli.
- Longley-Rice Model.

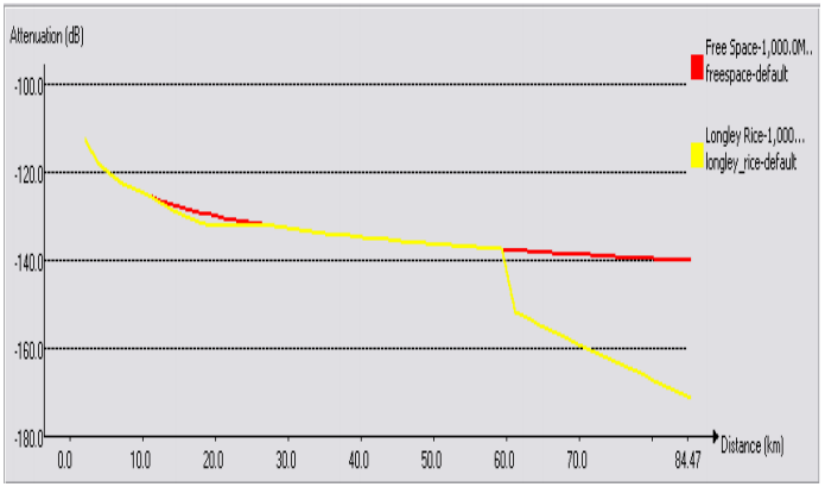
Boş yer modeli, əsasən ötürücü və qəbuledici arasındakı məsafəni izah edən daha sadə bir modeldir [7]. Mükəmməl yayılma şəraiti və ötürücü və qəbuledici arasında aydın bir görüş xətti qəbul edir. Enerji itkisinin, bəzi gücə qədər artırılan T-R ayrılma məsafəsinin bir funksiyası olaraq alındığını təxmin edir [8].

Longley-Rice modeli, siqnal gücünü simulyasiya edərkən meydana çıxa biləcək bir çox fərqli dəyişənliyi izah etməyə çalışan daha mürəkkəb bir modeldir. Bu mühit dəyişkənlərindən bəziləri bunlardır: şaquli və ya üfüqi qütbləşmə, qırılma, yerin əyriliyi, keçiricilik, və yeddi fərqli əvvəlcədən hazırlanmış iqlim kodları [9]. Bu model, müxtəlif iqlim və ərazilərdə siqnal gücü real dəyişiklikləri təmin etmək üçün xüsusilə faydalıdır. Simulyasiyanın qurulub yoxlandıqdan sonra indi nəticələrin izahına keçək.

Şəkil 1.15-də sarı xətt (aşağı xətt) Longley-Rice yayılma modelini, qırmızı xətt (yuxarı xətt) isə Azad yer modelini təmsil edir. Ötürücü və qəbuledici 20 m yüksəklikdə şaquli olaraq qütbləşmək üçün qurulmuşdur. Gördüyünüz kimi, qəbuledici ötürücüdən nə qədər uzaqlaşırsa, siqnaldakı gərginlik bir o qədər yüksəkdir. Longley-Rice modeli daha detallı olduğundan, sarsıntı daha yüksəkdir və ehtimal ki, daha realdır. Sərbəst boşluq modeli məsafə və gərginlik arasında daha çox xətti tipli əlaqəyə malikdir, bu simulyasiya zamanı yüksəliş dəyişikliyini nəzərə alaraq çox real deyil.



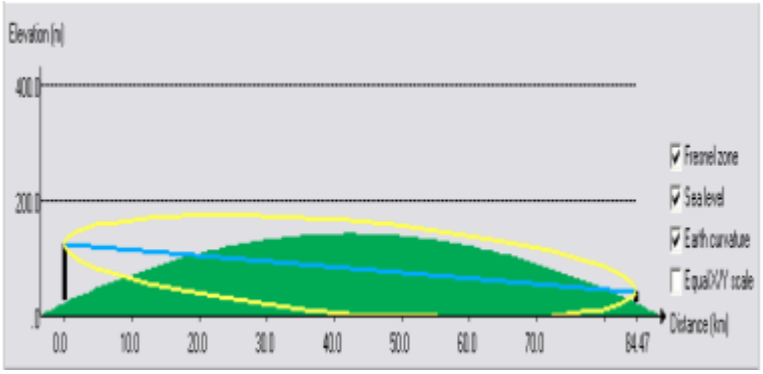
Şəkil 1.15. Fərqli Məsafələrdəki Gərginlik Nəticəsi



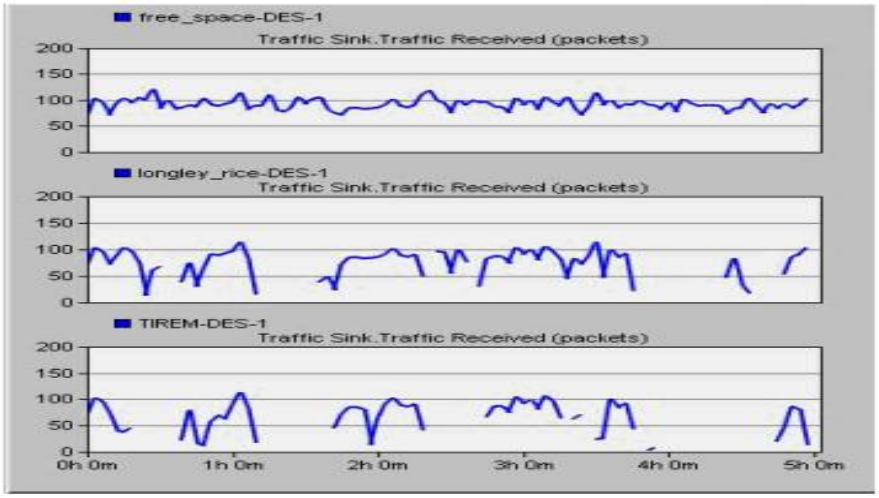
Şəkil 1.16. Yüksələn Antena üçün Gərginlik Nəticəsi

Yüksəklik dəyişikliyinin siqnal gücünə təsirini göstərmək üçün ötürücü antenanın hündürlüyü 100 m-ə qaldırıldı. Antenin hündürlüyü siqnal gücünə böyük təsir göstərir. Şəkil 1.16-da göstərildiyi kimi longley-rice modelindəki enişlər, azad zona modelinin uzun müddətə bənzədildiyi görünür. Longley-Rice hesablama modelində nəzərə alınan digər dəyişənlərə nisbətən görmə xəttinin daha yüksək əhəmiyyət verildiyini göstərir. 60 m məsafədə, Şəkil 1.16-da göstərilən sarı (aşağı) xətt və qırmızı (yuxarı) xətt göstərildiyi kimi ayrılmağa başladılar.

Şəkil 1.17-də 100 metr yüksəklikdə bir ötürücü və 20 metr hündürlüyündə bir qəbuledici olan bir anten üçün təxmin edilən Fresnel zonasını görə bilərsiniz. Fresnel zonası, ötürücü və qəbuledici antenlər arasındakı mənzərə yolunu əhatə edən elliptik bölgədir. Fresnel zonaları siqnal yolunun maneəsini hesablamaq üçün istifadə olunur.



Şəkil 1.17. Yüksələn Anten üçün Fresnel Bölgəsi



Şəkil 1.18. Alınan trafik

Bu şəkil 1.18 simulyasiya zamanı sinkdə (ötürücü və ya baza stansiyası) alınan trafiki göstərir. Hər qrafın istifadə edilən yayılma modelindən asılı olaraq çox fərqli olduğunu görə bilərsiniz. Mükəmməl yayılma şərtlərini ehtiva edən boş yer modeli, alınan trafikdə heç bir dəyişiklik göstərmir. Digər iki real model (Longley-Rice və TIREM) əslində yüksəkliyə tənlik daxil edir. Aşağı hündürlüyün, ötürücü anten ilə sabit bir əlaqə səbəbiylə paketlərin düşməsinə səbəb olduğunu göstərir.

1.3. Simsiz şəbəkə texnologiyalarına qoyulan tələblərin qiymətləndirilməsi

WLAN böyük bir istifadəçi qrupunu dəstəkləmək üçün tətbiq olunarsa, bəlkə də bir anket istifadə edərək və ya müsahibə yolu ilə istifadəçi tələblərinə dair geniş fikir toplamaq vacibdir. İlk addım olaraq, potensial istifadəçi qrupuna texnologiyanı nümayiş etdirərək məlumatları artırmaq lazım ola bilər ki, onlar tələblər barədə məlumatlı bir fikir verə bilsinlər.

İstifadəçi tələbləri konkret texnologiyalardan asılı olduqları üçün hər hansı bir həll yolu və ya texniki atributdan daha çox istifadəçi təcrübəsi baxımından ifadə edilməlidir. Məsələn, performans gözləntiləri ilə əlaqədar olaraq, bir PHY qatının məlumat dərəcəsi texniki bir atributdur, halbuki müəyyən edilmiş böyük bir fayl ölçüsü üçün ötürmə müddəti istifadəçinin həqiqətən narahat olduğu şeydir.

İstifadəçi tələblərinin demək olar ki, bütün aspektlərində gələcək sübut məsələsi də yaranır; istifadəçilərin iş proseslərində gələcək inkişaf, istifadəçilərin işində tətbiq olunan texnologiyaların növü, biznesin böyüməsi və s. İstifadəçi tələblərinin növü olan texniki tələbləri izah edək.

Texniki tələblər istifadəçi tələblərini yerinə yetirmək üçün lazım olan xüsusi texniki atributlara çevirərək istifadəçi tələblərindən irəli gəlir. Məsələn, böyük sənədlərin sürətli köçürülməsi üçün bir istifadəçi tələbi varsa, məsələn, video tənzimləmə tətbiqləri üçün bu, yüksək effektiv bir məlumat sürəti üçün texniki bir tələbə çevriləcəkdir.

Bəzi texniki atributlar, məsələn işləmə zonası, müdaxilə və eyni zamanda işləməklə əlaqəli olanlar, sayt araşdırması və şəbəkə qurğusunun fiziki planının ilkin planlaşdırılmasından sonra aydınlaşdırılacaqdır. Növbəti tələb olaraq mövcud texnologiyalara baxaq.

İstifadəçinin tələblərinə cavab vermək üçün lazım olan texniki xüsusiyyətləri müəyyənləşdirdikdən sonra mövcud texnologiyalar birbaşa bu xüsusiyyətlərə qarşı qiymətləndirilə bilər. Qiymətləndirməni göstərmək üçün cədvəldə göstərilən nümunəyə bənzər sadə bir cədvəl istifadə edilə bilər və nəticədə mövcud həllərin şəffaf və obyektiv müqayisəsi aparılır.

Daha mürəkkəb qiymətləndirmə metodları da tətbiq oluna bilər, məsələn, hər bir tələbə bir ağırlıq amili və tələblərə cavab verən dərəcədən asılı olaraq hər bir texniki həll üçün bir bal təyin etməklə.

Ümumi tələb olunan şəbəkə tutumu, şəbəkədə gözlənilən eyni vaxtda istifadəçi sayının eninə tələbatların cəminə görə müəyyən ediləcək, bu maksimumun nadir hallarda baş verəcəyi və qısa müddət ərzində yüksək istifadə zamanı fəaliyyətlərin məhdud bir pozulmasının məqbul ola biləcəyi üçün bəzən icazə verilir. Bu tələb tək giriş nöqtəsinin həcmini aşarsa, mövcud üst-üstə düşməyən kanalların sayına qoyulan həddədək birdən çox giriş nöqtəsi tələb olunur. Bu həddə müəyyən edilmiş 802.11 şəbəkə üçün ümumi şəbəkə tutumu müəyyən edilmişdir.

802.11h aksesuarları 5 GHz diapazonunda əlavə 12 OFDM kanal açır və 802.11a şəbəkələri üçün əldə edilə bilən şəbəkə tutumunu iki qat artırır.

Simsiz bir şəbəkə bağlantısının işləmə diapazonu, şəbəkənin işlədiyi binanın inşasında istifadə olunan materialların təbiətinə və modulyasiya və kodlaşdırma sxemindən tutmuş geniş amillərə təsir göstərir.

Tipik bir ofis mühitində dəyişən PHY qatının məlumat dərəcələri üçün 802.11a /b/g şəbəkələri üçün işləmə diapazonu 802.11a / b üçün 100 mW, 802.11g üçün 30 mW gücünə əsaslanaraq.

Tələblərin təhlili mövcud texniki seçimlər arasında bəlli bir qalibə işarə edə bilsə də, 2.4 və ya 5 GHz diapazonlarında işləmə arasında seçim edilməlidirsə, sonrakı hissədə təsvir olunan RF-nin araşdırması giriş kimi aparılmalıdır.

Eynilə, tələblər şəbəkə tutumunun tək bir kanalın keçidindən kənarda, məsələn, üst-üstə düşməyən kanalları tam istismar edən bir çox giriş nöqtəsi ilə uzanması lazım olduğunu diktə edirsə, onda hər iki 2.4 və 5 GHz seçimi üçün ilkin fiziki plan hazırlanması lazım ola bilər.

Bəzi yerdəki fiziki testlər son qərarı verməzdən əvvəl də dəyərli ola bilər, məsələn, 5 GHz şəbəkəsi məhdud bir qapalı şəraitdə təmin ediləcəyi təqdirdə əldə edilə bilən diapazonu təsdiqləmək üçün.

Gələcək hardware inkişafları tezliklə 2.4 ilə 5 GHz arasında seçim edə bilər. Artan həcmli ikitərəfli radioların 802.11g / b və 802.11a dəstəklədiyi və qiymətlər tək lent məhsulları ilə paritetə düşdükcə hər iki RF bantının xüsusiyyətlərdən ən yaxşı şəkildə istifadə edən WLAN ikili lent tətbiq etmək səmərəli olacaqdır.

II FƏSİL. SİMSİZ LOKAL ŞƏBƏKƏ TEXNLOGİYALARININ TƏDQİQİ

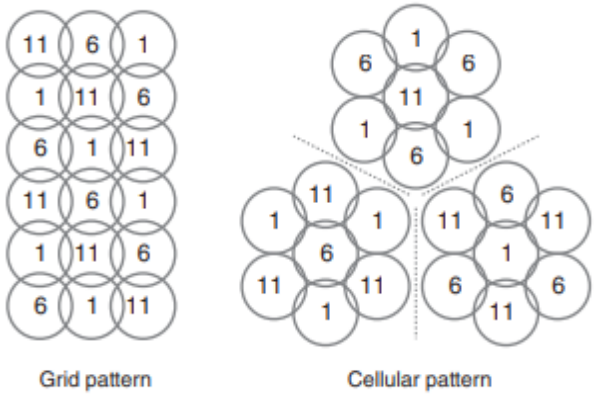
2.1. Simsiz lokal şəbəkənin planlaşdırılması və layihələndirilməsi

Erkən WLAN planları tez-tez giriş nöqtələrini müvəqqəti yerləşdirməklə, siqnal gücü və keçid ölçməsini (əsas etibarilə bir sayt araşdırmasını təkrarlamaqla) aparmaq və daha sonra RF əhatə dairəsində müəyyən edilmiş boşluqları doldurmaq üçün giriş nöqtələrini köçürmək və ya əlavə etməklə sınaqlar əsasında hazırlanmışdır.

WLAN Fiziki Memarlığına təsir edən amillər ***Cədvəl 2.1.***

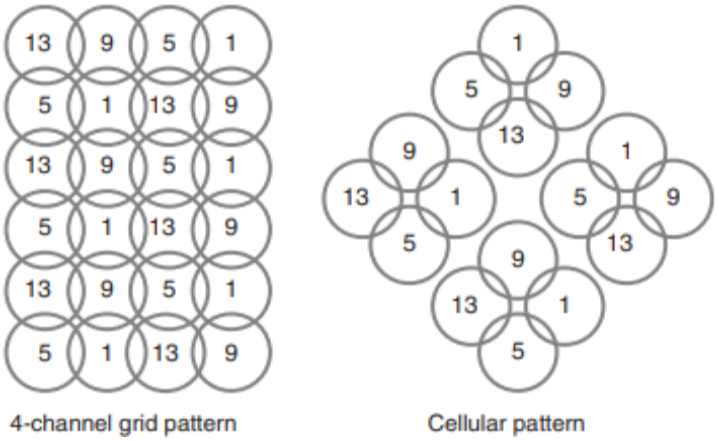
Parametr	Fiziki memarlığa təsir edən amillər
Say	Bir giriş nöqtəsindəki ümumi əməliyyat sahəsini yayılma və siqnal gücünün araşdırılması ilə müəyyən edilmiş əhatə dairəsinə bölməklə ilkin hesablama aparıla bilər. Sahə tələb olunan məlumat sürətinin saxlanıla biləcəyi kontura aparılmalıdır. Yaxınlıqdakı maneələr nəticəsində yayılma nümunəsi hamar istiqamətdən uzaq olsa, giriş nöqtəsinin effektiv əhatə dairəsi azalacaq.
Optimal anten yeri	Bir yönləndirici antenna ilə bir giriş nöqtəsi üçün optimal yer ümumiyyətlə əhatə ediləcək ərazinin mərkəzinə yaxın, müştəri stansiyaları üçün mənzərəni daha da artıran və maneələr, xüsusən sənəd vermə kimi metal əşyalara yaxın bir vəziyyətdə olacaqdır. kabinetlər. Yüksək bir yer çox təsirli ola bilər, məsələn, tavana quraşdırılmış bir vahid.
Əməliyyat kanalı	Əhəmiyyətli fon və ya sporadik səs-küy göstərən hər hansı bir kanaldan çəkinmək lazımdır. Mövcud üst-üstə düşməyən kanallar daha sonra ilkin yerlərinə görə giriş nöqtələrinə ayrıla bilər.
Güc qəbulu	Ümumiyyətlə, icazə verilən ötürmə gücündən istifadə olunarsa, giriş nöqtələrinin sayı minimuma endiriləcəkdir. Daha aşağı bir güc qəbulu səbəbləri, bina yayılmasının azaldılması və ya digər RF sistemlərinə müdaxilənin qarşısını almaq ola bilər. Yüksək RF səs-küyünün və ya yüksək yol itkisinin yerli şəraiti ilə mübarizə aparmaq üçün əksinə yüksək güc parametrləri tələb oluna bilər.

Simsiz Sahənin "LAN Planner" kimi planlaşdırma vasitələri mövcuddur və WLAN dizaynını şəbəkənin gözlənilən performansını qrafik görüntü ilə təkmilləşdirir. Qəbul edilmiş siqnal gücü göstəricisi, müdaxilə nisbəti siqnalı , səs-küy nisbəti, ötürmə qabiliyyəti və bit səhv dərəcəsi (BER) kimi məlumatlar, mürəkkəb mühitlərdə daha dəqiq planlaşdırmağa imkan verən rəqəmsal sayt planlarında göstərilə bilər.



Şəkil 2.1. Üç üst-üstə düşməyən kanallarla 802.11b giriş nöqtələri üçün kanal ayrılması nümunəsi

Şəbəkə komponentlərinin avtomatlaşdırılmış yerləşdirilməsi və konfiqurasiyasından başqa, bu alətlər avtomatik olaraq sənədlər və təmir qeydləri yaratmaqla həyata keçirilmənin sonrakı mərhələlərini də asanlaşdıra bilər.



Şəkil 2.2. Dörd üst-üstə düşməyən kanal üçün kanal bölüşdürmə nümunələri

Şəbəkə trafikinin stansiyalar arasında keçid yolunu dəyişdirməklə yanaşı, xüsusən də genişmiqyaslı WLAN qurğularında dizayn və sonrakı konfiqurasiya prosesinə kömək edən daxili alətlər də təqdim edir. Adətən bir simsiz keçid alət dəsti daxildir;

- Tutum və əhatə dairəsi üçün avtomatik layout planlaması
- Çox giriş nöqtələrinin və WLAN kommutatorlarını bir klik konfiqurasiyası

■ Əməliyyat nöqtələrini aradan qaldırmaq və şəbəkə fəaliyyətini optimallaşdırmaq üçün yaramaz giriş nöqtələrinin aşkarlanmasından tutmuş avtomatik ötürücü güc tənzimlənməsinə qədər sadə izləmə və əməliyyat.

Əgər WLAN tələbləri iki ayrı əməliyyat sahəsinin əlaqələndirilməsini, məsələn, bir binada WLAN-dan bir saniyədə simli və ya WLAN ilə əlaqəni təmin edərsə, onda nöqtə-nöqtə bağlantısının hazırlanması lazımdır.

İstədiyiniz məlumat ötürmə sürətinə çatmaq üçün kifayət qədər qəbul edilmiş siqnal gücünü çatdırmaq üçün lazım olan ötürmə gücünün və anten qazancının lazımi birləşməsi, əlaqə aralığı və nəzərdə tutulan RF diapazonu nəzərə alınmaqla müəyyən edilə bilər. WLAN şəbəkənin konfiqurasiyasına baxaq.

İlkin konfiqurasiya WLAN parametrlərinin quraşdırılmış giriş nöqtələri və stansiyalar arasında əlaqəni təmin etmək üçün qurulduğunu və qonşu BSS-lərin birlikdə olmasını təmin edəcəkdir. Giriş nöqtələri və stansiyaların konfiqurasiyasını tamamladıqdan sonra şəbəkə əməliyyat sistemi də konfiqurasiya oluna bilər.

Giriş nöqtəsi konfiqurasiyasının təfərrüatları seçilmiş xüsusi aparatdan asılı olacaq, lakin cədvəl 2.2 bütün hallarda tətbiq ediləcək əsas konfiqurasiya parametrlərinin xülasəsini verir. Əgər giriş nöqtəsi birdən çox radio ilə ikili və ya üçlü bir cihazdırsa, hər biri ayrı konfiqurasiyaya ehtiyac duyur. Bəzi giriş nöqtələri digər bir PHY qat parametrlərini, məsələn parçalanma həddi və ya bir paket atılmazdan əvvəl maksimum təkrar cəhd kimi parametrlərin qurulmasına imkan verə bilər.

Giriş nöqtəsi konfiqurasiya parametrləri ***Cədvəl 2.2.***

Parametr	**Konfiqurasiya mülahizələri**
IP ünvanı (üstəgəl alt şəbəkə maskası standart şlüz)	Giriş nöqtəsində bir veb brauzer vasitəsilə birbaşa bağlantı təmin edəcək bir istehsalçı tərəfindən müəyyən edilmiş bir standart IP ünvanı ola bilər. Alternativ olaraq bir IP ünvanı giriş nöqtəsinə simli şəbəkədəki bir DHCP server tərəfindən təyin edilə bilər və ya bir PC ünvanı giriş nöqtəsinin konfiqurasiya portuna qoşularaq statik bir IP ünvanı (üstəgəl şəbəkə maskası və standart şlüz) təyin edilə bilər.
SSID	Xidmət dəsti identifikatoru hər şəbəkədə əsas təhlükəsizlik tədbiri olaraq standart dəyərindən dəyişdirilməlidir. Böyük WLAN qurğuları üçün SSID təyin edilməsi üçün bir siyasət təyin edilə bilər.
SSID yayımı	Mayak çərçivələrdəki SSID yayımı ya aktiv ola bilər, ya da əlil ola bilər. SSID yayımının deaktiv edilməsi, 8-ci fəsildə müzakirə olunan daha bir təhlükəsizlik tədbiridir.
Maksimum ötürmə gücü	Maksimum icazə verilən ötürmə gücünün səviyyəsini yerli qaydalara uyğun olaraq təyin etmək.

Radio kanalı	Əməliyyat kanalının yerli qaydalarla icazə verilən həddə seçilməsi. Bəzi giriş nöqtələri ən az yığılmış kanal üçün avtomatik axtarış daxil ola bilər.
İş rejimi	802.11g şəbəkələri vəziyyətində, 802.11b stansiyalarının da şəbəkədə işləyəcəyindən asılı olaraq qarışıq rejim və g-only rejimi arasında seçim edilə bilər.
Təhlükəsizlik	Təhlükəsizlik rejimlərinin seçilməsi (64 bitlik WEP, 128 bitlik WEP, WPA-PSK və s.) Və parol və ya şifrləmə açarlarının daxil edilməsi, açar və identifikasiya rejimini ötürmək (8-ci fəsildə daha çox təsvir olunur).
Anten konfiqurasiyası	Çox antenalı bir giriş nöqtəsi, müəyyən bir antendən istifadə etmək və ya bütün antenləri müxtəliflik rejimində istifadə etmək üçün konfiqurasiya edilə bilər - ən güclü siqnal verən antenanı seçmək.

WLAN mövcud simli bir şəbəkənin bir uzantısıdırsa, əlavə bir NOS konfiqurasiyası tələb olunmur. Bununla birlikdə, WLAN yeni bir şəbəkə qurursa, bir sıra NOS konfiqurasiya işləri də tamamlanmalıdır. Detallar istifadə edilən xüsusi NOS-dan asılı olacaq, lakin tipik vəzifələr daxil olacaq;

■ TCP / IP kimi şəbəkə protokollarının quraşdırılmasını təmin etmək

■ şəbəkə proqramının quraşdırıldığına əmin olmaq fayl və printer mübadiləsi üçün

■ Resursları bölüşən istifadəçilərin işçi qruplarını müəyyənləşdirmək

■ ümumi və ya işçi qruplarına giriş üçün şəbəkə fayl sisteminin hissələrini təmin etmək

■ paylaşılan giriş üçün printerlər, skanerlər və s. kimi cihazları təmin etmək.

Birinci nəsil və ya "fat" giriş nöqtələrinə əsaslanan ənənəvi WLAN yerləşdirilməsi məhdud və ya daxili şəbəkə idarəetmə imkanlarına malik deyildir və ilkin konfiqurasiya və davam edən idarəetmə ümumiyyətlə veb əsaslı istifadəçi interfeysi istifadə edilərək həyata keçiriləcəkdir. Təhlükəsizlik parametrlərinin dəyişdirilməsi, RF əməliyyat kanalı, güc ötürmə və ya giriş siyasəti kimi şəbəkə idarəetmə vəzifələri hər bir giriş nöqtəsində fərdi olaraq yerinə yetirilməlidir. Korporativ WLAN üçün giriş nöqtələrinin sayı artdıqca bu çox vaxt aparacaq və tez idarə olunmayacaqdır.

Simsiz kommutator şəklində ikinci nəsil WLAN avadanlığı, bir çox giriş nöqtəsi olan WLAN-larda bu idarəetmə tapşırıqlarını yerinə yetirmək və Cədvəl 2.3-də ümumiləşdirildiyi kimi bir sıra avtomatlaşdırılmış konfiqurasiya və idarəetmə vasitələrini təmin etmək üçün hazırlanmışdır.

Şəbəkə fəaliyyətinin monitorinqini aparaq. Orta və geniş miqyaslı WLAN tətbiqetmələri üçün, şəbəkə inzibatçısı, hər hansı bir problemin xarakterini və yerini müəyyənləşdirmək və diaqnoz etmək üçün tez bir şəkildə şəbəkə performansını nəzərdən keçirməlidir.

Simsiz kommutator avtomatlaşdırılmış konfiqurasiya və idarəetmə vasitələri

Cədvəl 2.3.

Simsiz kommutator xüsusiyyəti	**Təsvir**
Avtomatik konfiqurasiya	Giriş nöqtələri yerləşdirildikdən sonra simsiz açarları ən yaxşı RF kanalını təyin edərək avtomatik konfiqurasiyanı təmin edə bilər və fərdi giriş nöqtələri üçün güc parametrlərini ötürə bilər, tətbiqetmə müddətini və əl konfiqurasiyasına xas olan səhvlərin riskini azaldır.
Giriş nəzarəti	Giriş nöqtələri yerləşdikləri bina və ya mərtəbə kimi kateqoriyalara görə qruplaşdırıla bilər və xüsusi müştərilərin hansı giriş nöqtələrinə və ya qruplarına qoşulmalarına icazə verildiyi siyahılar tərtib edilə bilər. Giriş nəzarəti stansiyanın rouminq tarixini və bant genişliyi istifadəsini izləyə bilər.
RF rəhbərliyi	Bəzi simsiz keçid məhsulları səs-küy və müdaxilədən təsirlənməyən kanalların qarşısını almaq üçün RF əməliyyat kanallarını və güc parametrlərini dəyişdirərək RF mühitindəki dəyişikliklərə davamlı uyğunlaşa bilər.
İnkişaf etmiş təhlükəsizlik	RF saytları araşdırmaları, yaramaz giriş nöqtələrini və icazəsiz istifadəçiləri və ya ad-hoc şəbəkələri aşkar etmək və tapmaq üçün aparıla bilər.

Bu performans monitorinqini asanlaşdırmaq üçün müxtəlif WLAN idarəetmə vasitələri mövcuddur. Adətən qurma planları və ya əməliyyat sahəsinin digər planlarına əsaslanan bir qrafik interfeys, şəbəkə inzibatçısı giriş nöqtələrindən və interfeys kartlarından toplanmış performans məlumatlarını görməyə imkanı verir.

SNMP sorğularından istifadəçi nöqtələrinə və stansiyalara, habelə sistem proqramlarından istifadə edərək toplanan bu real vaxt performans məlumatlarını müəyyən edə biləcək;

■ Aktiv giriş nöqtələri və müştəri stansiyaları

■ Orta məlumat mübadilə sürəti, təkrar cəhd dərəcələri və ümumi şəbəkədən istifadə

■ Səs-küy səviyyəsi və əraziyə müdaxilə

■ Şəbəkə sahələri və ya fərdi giriş nöqtələri əhəmiyyətli səhv dərəcələrini.

Yaxşı düşünülmüş fiziki quruluş və konfiqurasiya planı əsasında WLAN quraraq, şəbəkənin effektivliyini qorumaq üçün gələcək dəyişikliklərə eyni dərəcədə düşüncə və planlaşdırma verilməlidir.

Bəlkə bir əhatə dairəsi boşluğunu doldurmaq və ya istifadəçilərin yeni bir konsentrasiyası üçün əlavə şəbəkə tutumu təmin etmək məqsədi ilə bir giriş nöqtəsinin əlavə edilməsi, yeni qurğu mövcud quruluşla bir araya gəlmək üçün konfiqurasiya edilmədiyi təqdirdə asanlıqla əks təsir göstərə bilər və müvafiq kanal seçimi ilə güc və təhlükəsizlik parametrlərini ötürə bilər.

Sənədləşdirilmiş şəbəkə siyasətinin dəstəyi və dəyişikliyə nəzarət proseduru gələcək dəyişikliyin performansın qorunub saxlanması və ya artırılması üçün idarə olunmasını təmin edəcəkdir. Şəbəkə siyasətləri kimi problemləri həll edə bilər;

■ Dəstəklənən standartlar (məsələn, 802.11b / g)

■ Dəstəklənən cihaz satıcıları və ya NIC modelləri

■ SSID rəhbərliyi

■ Təhlükəsizlik və şifrələmə tələbləri (məsələn, şəxsi firewall, WEP / WPA).

Dəyişikliklərə nəzarət proseduru, quraşdırma, təklif olunan dəyişikliklərin, o cümlədən hardware, proqram təminatı və konfiqurasiya parametrlərinin texniki cəhətdən nəzərdən keçiriləcəyini və həyata keçirilmədən əvvəl təsdiqlənməsini müəyyənləşdirməlidir. Prosedur əhatə etməlidir;

■ Prosedurun əhatə dairəsi - hansı dəyişikliklərə nəzarət olunur

■ Dəyişiklik təklif etmək üçün tələb olunan proses və sənədlər

■ Rəyçilərin və qərar verənlərin rolu və vəzifələri

■ Müxtəlif dəyişiklikləri təsdiqləmək üçün səlahiyyətlilər.

2.2. Simsiz lokal şəbəkənin təhlükəsizlik təhdidləri

WLAN-nın üzləşdiyi təhlükəsizlik təhdidlərinin növü çox və müxtəlifdir və əvvəlcə PHY və MAC təbəqələrinə yönəldilsə də, son məqsəd tətbiq qatında məlumat və ya fəaliyyətə giriş və ya pozmaqdır. Əsas zəifliklərdən bir neçəsi aşağıda təsvir edilmişdir.

■ Xidmət (DoS) hücumlarının rədd edilməsi - təcavüzkar həddindən artıq trafiklə bir şəbəkə qurğusunu yükləyir, normal girişə mane olur və ya ciddi şəkildə yavaşlatır. Bu, bir neçə səviyyəyə yönəldilə bilər, məsələn, bir veb serveri səhifə

tələbləri və ya bir əlaqə nöqtəsi olan bir giriş nöqtəsi və ya identifikasiya tələbləri ilə doldurmaq.

■ Tıxanma - bir təcavüzkarın RF bandını yüklədiyi DoS-in bir forması, WLAN əlaqəsinin dayandırılmasına səbəb olur. 2.4 GHz diapazonunda bu, Bluetooth cihazları, bəzi simsiz telefonlar və ya mikrodalğalı sobadan istifadə etməklə edilə bilər!

■ Daxiletmə hücumları - təcavüzkar, icazəsiz yoxlanış edilmədiyi və ya təcavüzkarın səlahiyyətli istifadəçi kimi maskalanması səbəbindən icazəsiz bir müştəri stansiyasını giriş nöqtəsinə bağlaya bilər.

■ Təkrar hücum - təcavüzkar bir parol kimi şəbəkə trafikini qarışdırır və şəbəkədən icazəsiz giriş əldə etmək üçün sonradan istifadə edir.

■ Yayım monitorinqi - zəif bir konfiqurasiya edilmiş şəbəkədə bir giriş nöqtəsi bir keçid yerinə bir mərkəzə bağlanarsa, hub simsiz stansiyalar üçün nəzərdə tutulmayan məlumat paketlərini yayacaq və bunlar təcavüzkar tərəfindən ələ keçirilə bilər.

■ ARP Spoofing (və ya ARP cache zəhərlənməsi) - təcavüzkar, həssas məlumatları hücumçunun simsiz stansiyasına yönəltməklə, MAC və IP ünvanı cütlərinin saxlandığı ARP cache-ə daxil olmaq və pozmaqla şəbəkəni aldada bilər.

■ Sessiya qaçırılması (və ya orta səviyyəli hücum) - təcavüzkarın bir stansiya olaraq giriş nöqtəsi ilə əlaqəsini kəsərək, stansiya kimi ayrılması və özünü ayırması və sonra giriş nöqtəsi kimi pozduğu bir hücum növü. stansiyanı təcavüzkarla əlaqələndirmək.

■ Rogue giriş nöqtəsi (və ya pis əkiz tutma) - təcavüzkar düzgün SSID (əkiz) ilə icazəsiz giriş nöqtəsi quraşdırır. Siqnal bir gücləndirici və ya yüksək qazanc antenası istifadə edərək gücləndirilərsə, müştəri stansiyaları üstünlük olaraq yaramaz giriş nöqtəsi ilə əlaqələndiriləcək və həssas məlumatlar pozulacaqdır.

■ Kriptoanalitik hücumlar - təcavüzkarın kriptoqrafiya sistemini pozmaq üçün nəzəri zəifliyindən istifadə etdiyi bir hücum.

Buna misal olaraq WEP-də zəifliyə səbəb olan RC4 şifrəsinin zəifliyini göstərmək olar.

■ Yan kanal hücumları - təcavüzkar kriptoqrafik sistem haqqında məlumat əldə etmək üçün enerji istehlakı, vaxt məlumatı və ya akustik və ya elektromaqnit emissiyaları kimi fiziki məlumatlardan istifadə etdiyi bir hücum. Bu məlumatın təhlili təcavüzkarın birbaşa şifrələmə açarını və ya açarın hesablana biləcəyi düz mətn mesajını təyin edə bilər.

Təhdidlərin dairəsi geniş və müxtəlif olsa da, əksər hallarda bu tip hücumları həyata keçirmək haker tərəfindən yüksək səviyyədə texniki təcrübə tələb edir. Aşağıdakı hissələrdə təsvir olunan bütün təhlükəsizlik tədbirlərini təmin etməklə şəbəkə təhlükəsizliyi üçün risk əhəmiyyətli dərəcədə azaldıla bilər.

Cədvəl 2.4, WLAN-ları yuxarıda təsvir edilən təhdid və zəifliklərdən qorumaq üçün hazırlanmış ümumi təhlükəsizlik tədbirlərinin cəmini ümumiləşdirir.

Orijinal 802.11 standartına yalnız məhdud identifikasiya və zəif şifrələmə daxil edilmişdir. Aksessuarların 802.11 təhlükəsizliyinə aralıq inkişafı və yerləşdirilməsi, WPA və WPA2-nin sərbəst buraxılması ilə Wi-Fi Alyansı tərəfindən aparılmışdır.

Orijinal 802.11 standartının çatışmazlıqları 2004-cü ildə WPA və WPA2 üçün standart bazası təmin edən 802.11i standartının təsdiqlənməsi ilə aradan qaldırıldı. WLAN təhlükəsizliyinə aid mütərəqqi aksesuar və bu inkişafların altındakı texnologiyalar təsvir edilmişdir. Sonra WLANlarda, simsiz hotspotlarda və VoWLAN təhlükəsizliyinin bəzi spesifik aspektlərində təhlükəsizliyin təmin edilməsinin praktik aspektlərinə qayıdın.

WLAN Təhlükəsizlik tədbirləri ***Cədvəl 2.4.***

Təhlükəsizlik tədbiri	**Təsvir**
İstifadəçi identifikasiyası	Şəbəkə əldə etməyə çalışan istifadəçilərin kim olduqlarını söylədiklərini təsdiqləyir.
İstifadəçi girişinə nəzarət	Şəbəkəyə yalnız giriş icazəsi olan təsdiq edilmiş istifadəçilərə giriş imkanı verir.
Məlumat gizliliyi	Şəbəkə üzərindən ötürülən məlumatların qulaq asma və ya digər icazəsiz giriş şifrələməsi ilə qorunmasını təmin edir.
Açar idarəetmə	Məlumatların və digər mesajların şifrlənməsi üçün istifadə olunan açarların yaradılması, qorunması və yayılması.

Adından göründüyü kimi, WEP-nin məqsədi simli şəbəkəyə bərabər səviyyəli təhlükəsizlik səviyyəsini təmin etmək idi, baxmayaraq ki, bu istək

fundamental kriptoqrafik zəifliyə görə alınmadı. Cədvəl 2.4-də ümumiləşdirilmiş təhlükəsizlik tədbirləri siyahısından, WEP, giriş nöqtəsinə daxil olan və hər hansı bir stansiya tərəfindən tanınması tələb olunan gizli bir açardan, adətən bir paroldan istifadə etməklə məhdud dərəcədə girişə nəzarət və məlumatların məxfiliyini təmin edir.

WEP şifrələməsi parolu 64 bitlik şifrələmə açarı yaratmaq üçün 24 bit başlanğıc vektoru əlavə olunan 40 bitlik gizli açarına çevirir. WEP şifrələməsini gücləndirmək üçün müvəqqəti bir cəhd olaraq, bəzi satıcılar açar uzunluğunu 128 bitə artırdılar. Bu, çox dərəcədə kosmetik inkişaf etdiricisi oldu, çünki aşağıda təsvir olunduğu kimi, əsas zəiflik, 40 bitli və ya 104 bitli açarların istifadə olunduğundan qulaq asma cihazının hələ də təxminən 4 milyon ötürülən çərçivəni təhlil edərək açarı əldə edə biləcəyini ifadə etdi.

Düz mətn kimi kriptoqrafik terminologiyada bilinən giriş məlumat axını, şifrəli şifrə mətnini yaratmaq üçün XOR (eksklüziv OR) əməliyyatındakı yalançı təsadüfi açar bit axını ilə birləşdirilir. WEP, 256 mümkün baytın hamısının permutasiyası olan bir ardıcıllıqla S-dən yalançı təsadüfi seçim etmək üçün RC4 alqoritmindən istifadə edərək əsas bit axını yaradır.

RC4 əsas axındakı növbəti baytı seçir;

Addım (1) i sayğacın dəyərini artırmaq,

Addım (2) ardıcıllıqla S (i), i-ci baytın qiymətini j-in əvvəlki dəyərinə əlavə etməklə ikinci sayğacın artırılması, j

Addım (3) iki sayğac tərəfindən indekslənmiş iki bayt S (i) və S (j) dəyərlərini axtarır və onları birlikdə 256 modul əlavə edir

Addım (4) S (i) + S (j) ilə indekslənmiş bayt K-ı çıxarır

yəni K = S (S (i) + S (j)).

Baytların S (i) və S (j) dəyərləri sonrakı baytı seçmək üçün addım (1) -ə qayıtmadan əvvəl mübadilə olunur.

S baytların ilkin permutasiyası baytların şəxsiyyət permutasiyasından başlayaraq S daxilində baytların oxşar manipulyasiyasından istifadə edən açar

planlaşdırma alqoritmi ilə müəyyən edilir, lakin hər addımda (2), sayğac artırıldıqda sayğaca 64 bit və ya 128 bit şifrələmə açarından bir bayt da əlavə olunur.

WEP ayrıca şifrələmədən əvvəl məlumat blokuna əlavə edilən 32 bitlik bütövlüyünün yoxlanılması dəyərini (ICV) hesablamaq üçün bir dövri boşluq yoxlanışı istifadə edərək məhdud mesaj bütövlüyünün yoxlanılmasını təmin edir.

Tam WEP hesablama ardıcıllığı aşağıdakı kimidir ;

Addım (1), məlumat blokunun çərçivəyə ötürülməsi üçün **ICV** hesablanır.

Addım (2), məlumat blokuna əlavə edilir.

Addım (3) Başlanğıc vektoru tam şifrləmə açarı yaratmaq üçün gizli açarla birləşdirilir.

Addım (4) RC4 alqoritmi şifrləmə açarını açar axına çevirmək üçün istifadə olunur.

Addım (5) əsas axın və Addım (2) çıxışı arasında bir XOR əməliyyatı aparılır.

Addım (6) başlanğıc vektoru şifrə mətni ilə birləşdirilir.

WEP, təsadüfi qulaq asma qulaqcıqlarına qarşı ağlabatan bir təhlükəsizlik təmin etsə də, zəif cəhətləri 802.11 standartının bir hissəsi kimi buraxıldıqdan dərhal sonra tanındı. 2001-ci ildə kriptoqraflar Scott Fluhrer, Itsik Mantin və Adi Shamir başa düşdülər ki, RC4 açarları planlaşdırma alqoritmində zəif olduğuna görə çıxış açarı axını əhəmiyyətli dərəcədə təsadüfi deyil. Bu, şifrələmə açarını açardan istifadə edərək şifrələnmiş kifayət qədər çox sayda məlumat paketini analiz etməklə müəyyən etməyə imkan verir.

Əslində, WEP şifrələnmiş açar haqqında məlumatı şifrələnmiş mesajın bir hissəsi kimi ötürür ki, lazımi alətlərlə təchiz olunmuş hacker şifrləmə açarını çıxarmaq üçün ötürülən məlumatları toplaya və təhlil edə bilsin. Bunun üçün bir neçə milyon paketin tutulması və təhlil edilməsi tələb olunur, lakin yenə də bir saat ərzində yüksək bir trafik şəbəkəsində həyata keçirilə bilər. WEP, eyni zamanda WLAN-da işləyən hər bir cihazda yeni açarın və ya parolun yenidən əllə daxil edilməsindən başqa açarın dəyişdirilməsi üçün bir mexanizm olmadığı üçün statik paylaşılan bir açardan istifadə edir.

802.11-də istifadə olunan şifrələmə alqoritminin gücünü məhdudlaşdıran texnoloji məhdudiyyətlər deyildi, amma maraqlısı odur ki, məlumatların şifrlənməsi texnologiyasının ixracı ABŞ hökuməti tərəfindən milli təhlükəsizliyə təhdid hesab edildi və nəticədə WEP sxemi beynəlxalq standart olaraq qəbul ediləcəyi təqdirdə ən güclü ola bilmədi. Bu məhdudiyyətlər qaldırıldı və yeni, daha güclü şifrələmə üsulları, məsələn, Advanced Encryption Standard hazırlanmışdır.

Orijinal 802.11 təhlükəsizlik tətbiqində bu məlum zəiflikləri aradan qaldırmaq üçün, Wi-Fi Alliance, hədəf hücumlardan geniş qorunma təmin etmək üçün bir vasitə olaraq Wi-Fi Protected Access (WPA) inkişaf etdirdi. WPA, 802.11i standartının bir hissəsi olaraq 802.11 TGi tərəfindən hələ inkişaf etdirilən gücləndirilmiş təhlükəsizlik mexanizmlərinin alt hissəsinə əsaslanan müvəqqəti bir tədbir idi.

WPA, açar idarəetmə üçün TKIP istifadə edir və müəssisə WLAN təhlükəsizliyi (Müəssisə rejimi) üçün EAP ilə birlikdə 802.1x identifikasiya çərçivəsini və ya daha əvvəlcədən paylaşılan açarı (PSK) identifikasiya serveri olmayan şəxsi və ya kiçik ofis şəbəkəsi üçün identifikasiya (Şəxsi rejim) təklif edir.

Əvvəlcə Wi-Fi uyğun cihazlarda proqram təminatının yenilənməsi kimi mövcud olan bu tədbirlər ilk dəfə 2003-cü ilin əvvəlində bazara çıxdı. 2004-cü ildə ikinci nəsil WPA2-də şifrələmənin daha da gücləndirilməsi tətbiq olundu. Bu, hələ də WPA-da istifadə olunan RC4, 2004-cü ilin iyununda 802.11i standartının bir hissəsi kimi təsdiqlənmiş inkişaf etmiş şifrələmə standartı (AES) ilə əvəz edilmişdir.

WEP şifrələməsinin zəifliyi WPA-da iki yeni MAC təbəqəsi xüsusiyyətləri ilə həll edildi: TKIP və bir mesaj bütövlüyünün yoxlanılması funksiyası adlı əsas yaradılması və idarəetmə protokolu.

Bir stansiya təsdiqləndikdən sonra, ya bir autentifikasiya serveri tərəfindən hazırlanmış və ya əl ilə daxil edilmiş bir seans üçün 128 bitlik müvəqqəti bir açar yaradılır. TKIP, açarı stansiyaya və giriş nöqtəsinə paylamaq və sessiya üçün açar idarəetmə qurmaq üçün istifadə olunur. TKIP, müvəqqəti açarı hər stansiyanın MAC ünvanı, üstəgəl TKIP ardıcıllığı sayğacı ilə birləşdirir və məlumat şifrələməsi üçün ilkin açarları istehsal etmək üçün 48 bit başlanğıc vektoru əlavə edir.

Bu yanaşma ilə hər bir stansiya ötürülən məlumatları şifrələmək üçün müxtəlif açarlərdən istifadə edəcəkdir. TKIP, təhlükəsizlik tələblərindən asılı olaraq hər paketdən bir dəfə 10.000 paketə qədər ola bilən bir konfiqurasiya edilə bilən açar müddəti bitdikdən sonra bütün şifrələmə açarlarının yenilənməsini və yayılmasını idarə edir. Eyni RC4 şifrəsi şifrləmə açarı axını yaratmaq üçün istifadə olunsa da, TKIP-in əsas qarışdırma və paylama metodu WLAN təhlükəsizliyini əhəmiyyətli dərəcədə yaxşılaşdırır, WEP-də istifadə olunan vahid statik açarı 280 trilyon mümkün açarlardan dinamik dəyişən seçimlə əvəz edir.

WPA, TKIP-i bir təcavüzkarın məlumat paketlərini ələ keçirdiyini, dəyişdirdiyini təyin edən bir mesaj bütövlüyünün yoxlanılması ilə tamamlayır.

Dürüstlük hər bir məlumat paketində bir riyazi bir funksiyanı hesablayan ötürücü və qəbuledici stansiyalar tərəfindən yoxlanılır.

IEEE 802.1x istifadəçilərin identifikasiyası ilə şəbəkələrin qorunmasını təmin edən bir giriş nəzarət protokoludur. Uğurlu identifikasiyadan sonra şəbəkəyə giriş üçün giriş nöqtəsində bir virtual port açılır, identifikasiya uğursuz olduqda rabitə bloklanır. 802.1x identifikasiyası üç elementi müəyyənləşdirir;

■ Tətbiqçi - identifikasiyası istəyən simsiz stansiyada işləyən proqram

■ Authenticator - müraciət edən adından identifikasiyası tələb edən simsiz giriş nöqtəsi

■ Authentication Server - bir identifikasiya məlumat bazasından istifadə edərək mərkəzləşdirilmiş identifikasiya və giriş nəzarətini təmin edən RADIUS və ya Kerberos kimi bir identifikasiya protokolunu işləyən server.

Standart, uzadıla bilən identifikasiya protokolunun (EAP) məlumat bağlantısı təbəqəsi tərəfindən müraciət və identifikasiya serveri arasında identifikasiya məlumatlarını ötürmək üçün necə istifadə olunduğunu müəyyənləşdirir. Həqiqi identifikasiya prosesi istifadə olunan xüsusi EAP tipindən asılı olaraq müəyyənləşdirilir və idarə olunur və təsdiqləyici kimi çıxış nöqtəsi, müraciət edənə və autentifikasiya serverinə əlaqə yaratmağa imkan verir.

Müəssisə WLAN-da 802.1x identifikasiyasının tətbiqi, şəbəkə daxilində təsdiq edilmiş istifadəçilərin adları və etimadnamələrini saxlanan siyahısına qarşı

identifikasiya edə biləcək bir identifikasiya serverinin olmasını tələb edir. Ən çox istifadə edilən identifikasiya protokolu, WPA uyğun giriş nöqtələri tərəfindən dəstəklənən və mərkəzləşdirilmiş identifikasiya, avtorizasiya və mühasibat xidmətləri təmin edən uzaqdan identifikasiya yığma istifadəçi xidmətidir (RADIUS).

Bir giriş nöqtəsi vasitəsilə şəbəkə əldə etmək istəyən bir simsiz müştərini eyniləşdirmək üçün RADIUS serverində bir müştəri olaraq çıxış nöqtəsi, tələb olunan bağlantı parametrləri haqqında məlumat ilə birlikdə istifadəçinin etimadnaməsini ehtiva edən serverə RADIUS mesajı göndərir. RADIUS server hər iki halda cavab mesajını göndərərək istəyi təsdiqləyir və ya təsdiq edir və ya rədd edir.

RADIUS mesajı hər bir atribut tələb olunan bağlantı haqqında məlumat parçasını göstərərək RADIUS başlığı və RADIUS atributlarından ibarətdir. Məsələn, bir giriş-sorğu mesajında istifadəçi adı və etimadnaməsi, istifadəçi tərəfindən tələb olunan xidmət növü və bağlantı parametrləri, Giriş-Qəbul mesajı isə icazə verilən əlaqə növü üçün atributları ehtiva edir.

Bütün təhlükəsizlik zəifliklərinin tanınması və həll edilməsini təmin etmək üçün hər WLAN tətbiqində təhlükəsizlik üçün üç aspekt - idarəetmə, texniki və əməliyyat nəzərdən keçirilməlidir. Bu üç sahədəki ən yaxşı təcrübə təhlükəsizliyi tədbirlərinin geniş siyahısı, ABŞ Milli Elm və Texnologiya İnstitutu tərəfindən nəşr edilmişdir.

İdarəetmə təhlükəsizlik tədbirləri WLAN-ı hazırlayarkən və tətbiq edərkən nəzərə alınmalı olan problemləri həll edir. NIST nəzarət siyahısında ən yaxşı təcrübə kimi tövsiyə olunan bəzi əsas idarəetmə təhlükəsizlik tədbirləri Cədvəl 2.5-də təsvir edilmişdir.

WLAN İdarəetmə Təhlükəsizlik tədbirləri ***Cədvəl 2.5.***

İdarəetmə təhlükəsizlik tədbiri	Təsvir
Simsiz texnologiyanın istifadəsinə müraciət edən təşkilat üçün təhlükəsizlik siyasətini inkişaf etdirin	Təhlükəsizlik siyasəti etibarlı WLAN üçün əsas yaradır və təşkilatın tələblərinə daxil olmağa nəzarət, parol istifadəsi, şifrələmə, avadanlığın quraşdırılması və idarəolunmasına nəzarət və s.

Müdafiəyə ehtiyacı olan təşkilatdakı aktivlərin dəyərini başa düşmək üçün bir risk qiymətləndirməsini həyata keçirin	Təşkilatın aktivlərinə icazəsiz daxil olmağın dəyərini və potensial nəticələrini başa düşmək tələb olunan təhlükəsizlik səviyyəsinin qurulması üçün zəmin yaradacaqdır.
Bütün giriş nöqtələri və simsiz cihazların tam bir inventarını aparın	Quraşdırılmış cihazların fiziki inventarlaşdırılması WLAN qeydləri ilə, habelə naməlum qurğular üçün dövri RF süpürgələri (çirkin giriş nöqtələri) ilə çapdan keçirilməlidir.
Xarici divarlar və pəncərələrin yanında binaların içərisinə giriş nöqtələrini tapın	Daxili yer RF ötürülməsinin lazımi əməliyyat sahəsindən kənara çıxmasını məhdudlaşdıracaq və qulaq kəsilməsinin baş verə biləcəyi yerləri aradan qaldıracaq.
Giriş nöqtələrini etibarlı ərazilərə qoyun	Fiziki təhlükəsizlik, icazəsiz giriş və aparat manipulyasiyasının qarşısını alacaqdır.

Texniki təhlükəsizlik tədbirləri WLAN qurarkən diqqət edilməli olan problemləri həll edir. Cədvəl 2.5 NİST yoxlama siyahısında tövsiyə olunan bəzi texniki texniki tədbirləri təsvir edir.

Disable olmadığı müddətdə SSID yaxınlıqdakı stansiyaları xəbərdar etmək üçün hər saniyə on dəfə bir giriş nöqtəsi tərəfindən ötürülən mayak çərçivələrinə daxil edilir. Hər bir giriş nöqtəsi standart bir SSID dəsti ilə fabrikdən ayrılır və təcavüzkarlar bu şəxsiyyət sənədlərini standart dəyərlərdən dəyişdirilmədikdə təmin edilməmiş şəbəkələrə daxil olmaq üçün istifadə edə bilərlər.

SSID-nin başqa bir dəyərə dəyişdirilməsi təhlükəsizliyin artırılması üçün ilk addımdır. Bu giriş nöqtəsi ilk konfiqurasiya edildikdə edilməlidir, çünki SSID-ə daxil olmaq giriş nöqtəsinə qoşulacaq hər bir müştəri stansiyası üçün konfiqurasiya prosesinin bir hissəsidir. Yaxşı bir təcrübə, WLAN-ı işlədən şirkət və ya qurumu tanımayan bir anonim SSID istifadə etməkdir.

Standart SSID dəyişdirildikdən sonra, bəzi istehsalçılar SSID-in mayak çərçivələrində yayımlanmaması üçün bir seçim təqdim edirlər.

Bu, təsadüfi qulaq asma cihazının SSID əldə etməsinə mane olacaq, lakin müəyyən edilmiş hakerin fəaliyyətini dayandırmayacaqdır. SSID, qoşulmağa çalışan bir müştəri stansiyası tərəfindən göndərilən bir Probe sorğusuna cavab verərkən bir giriş nöqtəsi tərəfindən ötürülən Probe Reaksiya çərçivəsinə şifrələnməmiş şəkildə daxil edilmişdir, buna görə "Sniffer" proqram təminatı ilə təchiz edilmiş bir haker bu mesajlardan SSID çıxara bilər.

SSID bir təhlükəsizlik funksiyasını yerinə yetirmək üçün nəzərdə tutulmamışdır və SSID-i standart olaraq dəyişdirmək və SSID yayımlarını dayandırmaq yalnız təsadüfi icazəsiz girişə qarşı təsirli olacaqdır. Məqsədli bir hücumdan qorunmaq üçün daha sərt tədbirlər tələb olunur.

WLAN Texniki Təhlükəsizlik tədbirləri ***Cədvəl 2.5.***

Texniki təhlükəsizlik tədbiri	Təsvir
Standart SSID dəyişdirin və SSID yayımını deaktiv edin	WLAN-a təsadüfi girişin qarşısını alır və birləşmək istəyərkən SSID-yə uyğun bir müştəri stansiyasını tələb edir.
Giriş nöqtələrində bütün mənfi olmayan idarəetmə protokollarını deaktiv et	Hər bir idarəetmə protokolu mümkün hücum marşrutunu təmin edir, buna görə istifadə olunmamış protokolları ləğv etmək təcavüzkarın istifadə edə biləcəyi yolları minimuma endirir.
Defolt paylaşılan açarları ən azı 128 bit açarları ilə dəyişdirildiyini və vaxtaşırı dəyişdirilməsini təmin edin	TKIP quraşdırılmadığı təqdirdə əl açarlarının idarə edilməsi lazım olacaqdır (Bölmə "Müvəqqəti Bütövlük Protokolu, səh. 212"). Ən uzun dəstəkləyən açar uzunluğundan istifadə etmək üçün ən yaxşı təcrübədir.
MAC giriş nəzarət siyahılarını yerləşdirin	MAC süzgəcinə əsaslanan giriş nəzarəti, "MAC Ünvanı Filtrləmə, B." Bölməsində təsvir olunduğu kimi əlavə təhlükəsizlik təmin edir. 234 ", texniki cəhətdən müəyyən edilmiş bir hücumçuya qarşı etibarlı deyildir.
İstifadəçi identifikasiyası və giriş nöqtəsi idarəetmə interfeysləri üçün güclü inzibati parolları aktivləşdirin	Giriş nöqtələrindəki idarəetmə nəzarət funksiyaları, şəbəkə trafikindən daha yaxşı olmadıqda qorunmalıdır. Təhlükəsizlik siyasəti istifadəçi identifikasiyası və güclü şifrələrə olan tələbi göstərməlidir.

Fundamental kriptoqrafik zəiflik tanınıb və həll olunmasına baxmayaraq, əvvəlcədən 802.11i şəbəkələrində simli ekvivalent məxfilikdən (WEP) istifadə edərək məlumatların şifrlənməsini təmin etmək və ən uzun dəstəklənən ortaq açar uzunluğundan istifadə etmək hələ də yaxşı təhlükəsizlik praktikasıdır.

MAC ünvanının süzülməsi işə salınsa, giriş nöqtəsi yaddaşında olan bir icazə siyahısına qarşı giriş üçün hər bir sorğu nəzərdən keçirəcəkdir. İcazə siyahısı, bütün səlahiyyətli müştəri stansiyalarının MAC ünvanlarını saxlayır və giriş nöqtəsi yalnız tələb olunan MAC ünvanı siyahıda tapıldıqda giriş əldə edəcəkdir.

MAC filtrləmə yüksək effektiv təhlükəsizlik tədbiri kimi görünür, lakin MAC ünvanları ötürülən məlumat paketlərinə daxil edildiyi üçün bir hacker icazə verilən MAC ünvanlarını simsiz trafiklə "sniffing(havadan tutaraq)" bərpa edə bilər.

MAC ünvanı fabrik dəsti müəyyənləşdiricisidir, yəni, fərdi bir adapter kartı üçün unikal olsa da, bir cihazın başqa bir cihaz kimi maskalanmasına (və ya

korlanmasına) icazə vermək üçün bir MAC ünvanı da proqram tərəfindən müvəqqəti olaraq yenidən qurula bilər.

Əməliyyat təhlükəsizliyi tədbirləri WLAN-ın müntəzəm istifadəsi zamanı nəzərə alınmalı olan problemləri həll edir. NIST yoxlama siyahısında tövsiyə olunan əsas əməliyyat təhlükəsizlik tədbirləri cədvəl 2.6-da ümumiləşdirilmişdir.

WLAN Əməliyyat Təhlükəsizliyi tədbirləri ***Cədvəl 2.6.***

Əməliyyat təhlükəsizliyi tədbiri	**Təsvir**
Giriş nöqtəsinin konfiqurasiyası üçün SNMP v3 kimi şifrəli bir protokoldan istifadə edin	SNMP v3 giriş nöqtəsini idarəetmə mesajlarının şifrələməsini təmin edir, halbuki SNMP v1 və v2 eyni səviyyədə təhlükəsizlik təmin etmir.
RADIUS və Kerberos kimi simsiz şəbəkə üçün istifadəçi identifikasiyasının digər formalarını nəzərdən keçirin	Risk qiymətləndirməsi icazəsiz girişi əsas risk olaraq müəyyənləşdirirsə, RADIUS və Kerberos kimi identifikasiya xidmətləri və ya protokollar məxfi məlumatları qorumaq üçün yüksək səviyyədə giriş təhlükəsizliyini təmin edə bilər.
Qeyri-qanuni giriş və ya fəaliyyət aşkar etmək üçün hücumçu aşkarlamasını WLAN-a yerləşdirin	Rogue giriş nöqtələri və ya digər icazəsiz fəaliyyət müdaxilə aşkarlanması proqramı ilə aşkar edilə bilər. Bu simsiz açarların standart bir xüsusiyyəti, "WLAN açarları və ya nəzarətçiləri" bölməsində təsvir edilmişdir. 48 ”.
Aparat yeniləndikdə köhnə avadanlıqların atılmasından əvvəl konfiqurasiya parametrlərinin yenidən qurulduğundan əmin olun	Giriş nöqtələri atıldıqda etibarlı konfiqurasiya parametrləri ilə qalarsa, bu həssas məlumatlar şəbəkəyə hücum üçün istifadə edilə bilər.
Giriş nöqtəsi qeydlərini aktiv edin və mütəmadi olaraq nəzərdən keçirin	Giriş nöqtəsi qeydləri şəbəkə trafikinin dövri yoxlanılması üçün əsas verir - həm səlahiyyətli, həm də icazəsiz. Bir çox müdaxilə aşkarlama vasitələri bu vəzifəni avtomatik olaraq effektiv şəkildə yerinə yetirmək üçün konfiqurasiya edilə bilər

Uzaqdan identifikasiya yığma istifadəçi xidməti (RADIUS) mərkəzləşdirilmiş identifikasiya, avtorizasiya və mühasibat xidmətlərini təqdim edən ən çox istifadə olunan identifikasiya protokoludur.

Kerberos Massachusetts Texnologiya İnstitutu tərəfindən hazırlanmış və identifikasiya və xüsusilə müştəri/server tətbiqləri üçün güclü şifrələmə üçün vasitələr təqdim edən başqa bir identifikasiya protokoludur. Mənbə kodu MIT-dən sərbəst istifadə olunur və bir sıra ticarət məhsullarına daxil edilmişdir.

Giriş aşkarlama proqramı WLAN-da fasiləsiz işləmək və hər hansı bir icazəsiz cihaz, məsələn, yaramaz giriş nöqtəsi aşkar edildikdə həyəcan yaratmaq üçün işlədilə bilər. Ümumiyyətlə müdaxilə monitorinqi, cədvəl 2.7-də göstərildiyi

kimi normal, səlahiyyətli WLAN cihazlarını və trafikini təyin edən parametrlərin təyin edilməsinə əsaslanır.

İntruziya aşkarlama parametrləri ***Cədvəl 2.7.***

Təhlükəsizlik parametric	**Təsvir**
Səlahiyyətli RF PHY xüsusiyyətləri	WLAN-da hansı PHY təbəqə standartlarının işlədildiyini müəyyənləşdirir (məs. 802.11a, 802.11b / g).
Səlahiyyətli RF kanal istifadəsi	RF kanallarının fərdi giriş nöqtələrinin istifadə üçün konfiqurasiya olunduğunu göstərir.
Səlahiyyətli cihaz MAC ünvanları	Giriş nöqtəsi səviyyəsində MAC giriş nəzarətinə bənzər, lakin bütün WLAN-a yayılmışdır.
SSID siyasəti	Səlahiyyətli SSID-lərin siyahısını verir.
Avadanlıq satıcısı	WLAN-da işləməyə icazə verilən avadanlıq istehsalçısını göstərir. MAC ünvanının ilk hissəsi avadanlıq istehsalçısını göstərdiyindən bu, qismən MAC filtrini təmin edir.

Göstərilən parametrlərdən kənara çıxan qurğular və ya şəbəkə fəaliyyəti müəyyən edildikdə ya parametrlər siyahısını təmizləmək və ya WLAN menecerinə müdaxilə cəhdi barədə xəbərdarlıq etmək və müəyyən edilmiş yaramaz cihazın birləşməsini maneə törətmək və ya WLAN ilə əlaqə saxlamaq kimi əks tədbirləri başlamaq üçün istifadə edilə bilən bir siqnal yaradılır.

Giriş aşkarlama proqramı, həmçinin DoS hücumları və ya sessiya yüksək səviyyəli oyun kimi WLAN-a hər hansı bir hücumu aşkar etmək və bütün səlahiyyətli cihazların qüvvədə olan təhlükəsizlik siyasətinə uyğunluğunu təmin etmək üçün şəbəkə fəaliyyətini izləyə bilər.

Wi-Fi hotspotları qəhvəxana, otel və hava limanları kimi rahat ictimai yerlərdə internetə simsiz qoşulma təmin edir. Asan açıq əlçatanlıq tələbi, şifrələmənin aktiv olmadığını bildirir, çünki 802.11i-dən əvvəl 802.11 standartlarında lazımi əsas idarəetmə mexanizmləri yox idi. Nəticədə simsiz əlaqə üzərindən göndərilən məlumatların təhlükəsizliyi üçün məsuliyyət hotspot istifadəçisinin üzərinə düşür.

Təhlükəsiz hotspot xidmətləri əldə olunana qədər, ictimai hotspotlardan istifadə edərkən cədvəl 2.8-də təsvir edilmiş texniki və əməliyyat təhlükəsizlik tədbirlərinə diqqət yetirilməlidir.

Simsiz hotspot təhlükəsizlik tədbirləri *Cədvəl 2.8.*

Hotspot təhlükəsizlik tədbiri	Təsvir
Simsiz şəbəkə bağlantısını yalnız üstünlük verilən nöqtələrə qoşulmaq üçün qurun	Tercih edilmiş giriş nöqtələrinin müəyyən edilmiş siyahısına avtomatik qoşulmanın məhdudlaşdırılması naməlum giriş nöqtəsinə qoşulma riskini azaldır. Bununla birlikdə, SSID-ləri asanlıqla korlamaq mümkün olduğu üçün bu, yaramaz giriş nöqtələrindən yaranan riski aradan qaldırmaz.
Korporativ şəbəkəyə qoşulmaq üçün VPN istifadə edin	VPN, İnternet və ya simsiz isti nöqtə bağlantısı kimi etibarlı bir əlaqə vasitəsilə qorunan "tunel" təmin etmək üçün əlavə şifrələmə səviyyəsindən istifadə edir.
İsti nöqtələrdən istifadə edən mobil kompüterlərdə fərdi firewall quraşdırın	Bir firewall, isti nöqtə bağlantısı vasitəsi ilə mobil kompüterə icazəsiz girişin qarşısını almaq üçün bir maneə rolunu oynayır. Giriş nöqtəsindən alınan məlumatlar firewallın konfiqurasiyasından asılı olaraq icazə veriləcək və ya bloklanacaqdır. Simsiz şəbəkə trafikinə ictimai giriş nöqtəsini istifadə edərkən "etibarlı olmayan" status verilməlidir.
Şifrə və ya şifrələmədən istifadə edərək mobil cihazdakı faylları və qovluqları qoruyun. Fayl paylaşımını deaktiv edin.	PC əməliyyat sistemində mövcud olan məxfilik mexanizmlərindən istifadə, təcavüzkarın mobil cihazla icazəsiz əlaqə qurmağına baxmayaraq, faylların və məlumatların qorunmasını təmin edəcəkdir.
Giriş nöqtəsinə ötürülən məlumatları qorumaq	E-poçtlar da daxil olmaqla məxfi məlumatlar ötürülmədən əvvəl şifrələnməlidir və ya etibarlı bir sock qat (SSL) elektron poçt xidmətindən istifadə edilə bilər.
İstifadə olunmayanda simsiz NIC-i deaktiv edin	İstifadə edilmədikdə simsiz NIC radiosunu söndürmək, potensial hücum marşrutunu aradan qaldıracaq və mobil qurğular üçün batareya gücünə qənaət edəcəkdir.
İctimai yerlərdə müşahidə riskindən çəkinin	Məxfi məlumatların nəzarətdən qorunmasını təmin etmək üçün ictimai yerlərdə PİN və ya şifrələri daxil edərkən ayıq-sayıq olun.
Əməliyyat sistemi və təhlükəsizlik proqramlarını yeniləyin	Təhlükəsizliyə töhfə verən bütün proqramların - əməliyyat sistemi, firewall və antivirus proqramı - bütün məlum təhlükələrə qarşı mübarizə aparmaq üçün yenilənməsini təmin etmək üçün təhlükəsizlik yamaları mütəmadi olaraq yüklənməlidir.

2.3. Simsiz lokal şəbəkənin problemləri

Hər hansı bir problem həll etmə təcrübəsi olduğu kimi, WLAN problemlərini həll etmək üçün əvvəlcə mümkün səbəbi azaltmağa çalışmaq üçün simptomları təhlil etmək və sonra potensial həll yollarını araşdırmaq üçün sistematik bir yanaşma tələb olunur.

Problemin mahiyyətini və dərəcəsini aydınlaşdırmaq üçün bir sıra suallar verməyə başlayın (cədvəl 2.9). Bu, mümkün kök səbəblərinin aralığını daraltmağa kömək edəcəkdir.

WLAN problemlərinin aradan qaldırılması ***Cədvəl 2.9.***

Problem identifikasiyası	**Mülahizələr**
Bir əlaqə problemi varmı?	WLAN-larla əlaqəli problemlərin əsas bir kateqoriyası müştəri stansiyası əlaqələrinə aiddir; fərdi istifadəçilər və ya istifadəçilər qrupları əvvəllər əldə edilən şəbəkə mənbələrinə qoşula bilmirlər.
Bir performans problemi varmı?	Problemlərin ikinci böyük kateqoriyası performansla əlaqədardır; şəbəkə əhatə dairəsi, sürət və ya cavab müddəti gözlənildiyi kimi və ya əvvəllər olduğu kimi deyil.
Problem nə dərəcədə genişdir?	Problem yalnız bir qurğuya təsir edir və ya bir çoxunun yaşadığı eyni problemdir? Məsələn, problem şəbəkəyə bağlantıdırsa, yalnız bir müştəri təsirlənirsə, cihazın NIC-in qurğusundan və qurulmasından şübhələnin. Bütöv bir BSS təsirlənsə, giriş nöqtəsinin hardware və konfiqurasiyasını yoxlayın.
Problem nə qədər nizamlıdır?	Fasiləsiz, günün müəyyən vaxtlarında - məsələn, işçilər günorta otağında mikrodalğalı sobadan istifadə edərkən baş verirmi?

Diaqnoz üçün başlanğıc nöqtəsi, cədvəl 2.10-da ümumiləşdirildiyi kimi, şəbəkə aparatında və ya konfiqurasiyada, iş mühitində və ya istifadə qaydasında son dəyişikliklərin nəzərdən keçirilməsi olmalıdır.

WLAN problemlərinin aradan qaldırılması - İlk mülahizələr ***Cədvəl 2.10.***

Son WLAN dəyişiklikləri	***Mülahizələr***
Aparat dəyişikliyi	Şəbəkəyə yeni bir hardware cihazı əlavə edildi? Mövcud hardware ilə eyni istehsalçıdan gələn yeni bir cihaz, yoxsa qarşılıqlı əlaqə üçün sertifikat almış birisi?
Konfiqurasiya dəyişir	Bu yaxınlarda hər hansı bir konfiqurasiya parametrləri dəyişdirilibmi? İşləyən kanal dəyişikliyi, təhlükəsizlik mexanizmləri işə salındı, açarlar və ya parollar dəyişdirildi?
Proqram dəyişiklikləri	Bu yaxınlarda proqram və ya firmware yeniləmələri quraşdırılmışdır? Müştəri kompüterinə və ya şəbəkə əməliyyat sistemlərinə, cihaz sürücülərinə və ya proqram təminatlarına yeni quraşdırılmış yamalar nəticəsində quraşdırılmış dəyişikliklər tələb olunurmu?
Ətraf mühitdəki dəyişikliklər – fiziki	Bu yaxınlarda bir RF nöqtəsi yarada bilən bir giriş nöqtəsi kimi hər hansı bir cihaz köçürüldü? Arxa divarlar və ya mebel (metal veril dolabları) əməliyyat bölgəsində yenidən qurulub, RF-nin yayılma modelinə təsir göstərə bilərmi?
Ətraf mühitdəki dəyişikliklər - RF mühiti	İş şəraitində və ya qonşuluqda yeni simsiz şəbəkələr və ya digər RF mənbələri quraşdırılıbmı? (Məsələn, ortaq divar boyunca mikrodalğalı sobaları olan növbəti binada sürətli yemək restoranı.)
İstifadə qaydası dəyişir	WLAN-dan istifadə edən, xüsusən də yüksək davamlı və ya yüksək bant genişliyi tələb edən yeni tətbiqlər quraşdırılmışdırmı? Şəbəkə istifadəsində hər hansı bir dəyişiklik olubmu, məsələn, yüksək genişliyə ehtiyacı olan yeni bir istifadəçi qrupu?

Bu sualların bəzilərinə cavab vermək, RF müdaxiləsinin artması performansın pozulmasının mümkün bir səbəbidirsə, RF-nin təkrar araşdırılması kimi əlavə araşdırma tələb edə bilər.

Cədvəl 2.11-də təsvir olunan strategiyalardan istifadə edərək problemin mümkün həllərini sınaqdan keçirərkən sistematik yanaşma davam etməlidir.

WLAN problemlərinin əksəriyyəti iki kateqoriyaya, bağlantı - bir və ya bir neçə müştəri stansiyası şəbəkəyə bir əlaqə qura bilmədikdə və performans - məlumat ötürmə qabiliyyəti və şəbəkənin cavab müddəti istifadəçi gözləntilərinə və ya əvvəlki təcrübəyə uyğun gəlmədikdə. Bu iki kateqoriyalı problem aşağıdakı hissələrdə nəzərdən keçirilir.

WLAN problemlərinin aradan qaldırılması - Həll strategiyaları Cədvəl 2.11.

Həll yanaşması	Təsvir
Bir anda bir hipotezi sınayın	Bir konfiqurasiya qəbulu və ya sınanan fiziki bir quruluş olsun, təsirləri birbaşa bir səbəbə aid etmək üçün bir-bir dəyişiklik edin.
Bilinən bir işləmə əvəzedicisini istifadə edərək cihazı sınayın	Bir cihaz qüsurunu müəyyənləşdirməyin ən asan yolu şübhəli elementi məlum iş yerində əvəz etməkdir - CAT 5 kabelinin uzunluğu, NIC və ya giriş nöqtəsi olsun.
Qeyd edin	Edilən dəyişikliklər, dəyişdirilən hər hansı ilkin parametrlər və nəticədə sistemin cavabını qeyd edin. Bu, köhnə prospektləri yenidən araşdırmaq üçün vaxtın boşa çıxmayacağını və dəyişikliklər daha da pisləşəcəyi təqdirdə əvvəlki quruluşun bərpa olunacağını təmin edəcəkdir.
Gözlənilməyən yan təsirlərin olub olmadığını yoxlayın	Bir problemin həll edildiyini elan etməzdən əvvəl, orijinal problemin həlli nəticəsində yeni istenmeyen simptomların ortaya çıxmadığını mümkün qədər yoxlayın.
Qalan hər şey uğursuz olduqda ... təlimatları oxuyun	Təchizat satıcısının quraşdırma təlimatlarını oxuyun və ya yenidən oxuyun və Veb saytını problem diaqnozu və problem aradan qaldırılması ilə bağlı xüsusi məlumat üçün yoxlayın.

Bağlantı problemlərinin PHY və ya MAC səviyyəsində kök səbəbi ola bilər, məsələn, RF cihazı ilə əlaqəli fiziki və ya konfiqurasiya problemləri və ya daha yüksək səviyyələrdə, məsələn istifadəçi identifikasiyası prosesində bir uğursuzluq səbəbindən cədvəl 2.12-də göstərilən yoxlama siyahısı bağlantı problemlərinin diaqnozu üçün başlanğıc nöqtəsi kimi istifadə edilə bilər.

WLAN problemlərinin aradan qaldırılması - bağlantı problemlərinin yoxlanılması siyahısı ***Cədvəl 2.12.***

Problem əlamətləri	**Yoxlama məntəqələri**
Tək bir istifadəçi heç bir giriş nöqtəsinə qoşula bilmir	Simsiz NIC-nin işləmədiyini və stansiyanın adekvat qəbul edilmiş siqnal gücü olduğunu yoxlayın. Problem yerində başqa bir müştəri stansiyasının qoşula biləcəyini yoxlayın. Təhlükəsizlik parametrləri daxil olmaqla müştəri stansiyasının simsiz şəbəkə bağlantısını yoxlayın. MAC filtri kimi giriş nöqtəsi təhlükəsizlik mexanizmlərinin müştəri stansiyası üçün düzgün qurulduğunu yoxlayın. Hər hansı bir şübhəli simsiz NIC-ni bilinən bir işləmə əvəzçisi ilə əvəz edin.
Heç bir istifadəçi bir giriş nöqtəsinə qoşula bilmir	Təhlükəsizlik parametrləri daxil olmaqla giriş nöqtəsinin konfiqurasiyasını yoxlayın. Təhlükəsizlik parametrləri ilə əlaqəni müvəqqəti olaraq deaktiv edin. Şübhəli giriş nöqtəsini bilinən bir iş yerinə dəyişdirin.
İstifadəçilər bir giriş nöqtəsinə qoşula bilər, lakin şəbəkəyə daxil ola bilmirlər	Müştəri stansiyası və giriş nöqtəsinin DHCP serverindən alınan və ya əl ilə daxil edilmiş etibarlı IP ünvanları, alt şəbəkə maskaları və standart şlüz ünvanları olub olmadığını yoxlayın. Müştəri stansiyasından giriş nöqtəsinə və giriş nöqtəsindən simli şəbəkə kompüterinə addım-addım bağlantı yoxlamaq üçün pəncərəni OS istədiyi (məsələn, DOS istəyi) istifadə edin. 802.1x identifikasiyası yerindədirsə, simli bağlantı üzərində identifikasiya serverinin konfiqurasiyasını və işləməsini yoxlayın.

İstismar problemləri WLAN-larda ya ötürülmə səs-küy nisbətinə lazımi şəkildə aşkar və şifrələnməməsi üçün çatma stansiyasına çatmadığı və ya bir giriş nöqtəsinin həddən artıq yükləndiyi və trafikin həcminin öhdəsindən gələ bilməməsi səbəbindən baş verir. Öz növbəsində, SNR problemləri aşağı siqnal (örtmə çuxurları) və ya yüksək səs-küy (müdaxilə) ilə əlaqədar ola bilər. Cədvəl 2.13-dəki yoxlama siyahısı fəaliyyət problemlərini həll etmək üçün başlanğıc nöqtəsi kimi istifadə edilə bilər.

WLAN problemlərinin aradan qaldırılması - Performans problemlərinin yoxlanılması siyahısı ***Cədvəl 2.13.***

Kök səbəbi	**Təsviri**
Zəif SNR - aşağı siqnal gücü	Təsirə məruz qalan yerdə siqnal gücünü yoxlamaq üçün sayt araşdırması alətindən istifadə edin ("WLAN analizatorlarından istifadə edərək problemlər, s. 243" bölməsi). Anten yerini və istiqamətini tənzimləyərkən siqnal gücünə nəzarət edin. Siqnal gücü az qaldıqda anten artımını və ya gücünü (tənzimləmə həddinə qədər) və ya giriş nöqtələrini köçürməyi düşünün.
Zəif SNR - yüksək səs-küy səviyyəsi	Digər 802.11 transmis sionları və 802.11 olmayan müdaxilə siqnallarını müəyyən etmək üçün bir sayt araşdırması vasitəsindən istifadə edin. Səs-küy səviyyəsi yüksək olduqda adi şübhəli şəxsləri (mikrodalğalı sobalar, simsiz telefonlar, Bluetooth) axtarın və aradan qaldırın.
Giriş nöqtəsinin həddən	İstifadəçilərdə tətbiqetmələrdə və ya istifadə qaydalarındakı hər hansı bir dəyişiklik üçün sorğu aparın. Performans problemi ilə qarşılaşan giriş nöqtəsi üçün logu yandırın və nəzərdən keçirin. Yaxşı bir SNR şəraitində yüksək bir cəhd sayı, yarışan trafik səbəbiylə

artıq yüklənməsi	yenidən cəhdlərin göstəriləcəyini göstərir. Gücü artırmaq üçün üst-üstə düşməyən kanallarda və ya ikili rejim şəbəkələrində (məsələn, 802.11a və g) əlavə giriş nöqtələrini nəzərdən keçirin.

Xüsusi WLAN analizatorları müəssisə miqyaslı qurğuları izləmək və aradan qaldırmaq üçün mövcuddur. Bu sistemlərə sayt araşdırması, təhlükəsizlik qiymətləndirilməsi, şəbəkə performansının monitorinqi və WLAN-ların layihələndirilməsi, tətbiqi, təhlükəsizliyi və nəhayət aradan qaldırılması vəzifələrində şəbəkə inzibatçısına kömək edə biləcək vasitələr daxildir.

Analizatorlar ya ayrıca bir cihaz, ya da bir dizüstü və ya əl kompüterində işləyə biləcək bir proqram paketi olaraq mövcuddur.

Bəzi WLAN analizator məhsulları spektr və ya protokol təhlili kimi bir tətbiq sahəsinə yönəlir, digərləri bu xüsusi imkanları daha ümumi performans və təhlükəsizlik təhlili vasitələri ilə birləşdirir. Bu analiz vasitələrinin tipik istifadəsi Cədvəl 2.14-də ümumiləşdirilmişdir.

802.11i-nin gəlməsi və WLAN-larda 802.1x identifikasiyasının artması ilə müvəffəqiyyətli identifikasiya müştəri stansiyasının şəbəkəyə müvəffəqiyyətlə qoşulmadan əlavə bir addım olur. WLAN analizatoru, EAP identifikasiyası prosesinin hər bir addımını izləyə biləcək və bu prosesin pozulmasının istifadəçi identifikasiyasına və girişinə maneə törətdiyini görəcəkdir. Doğrulama serveri bir istifadəçi girişi rədd edərsə, analizatorun nəticələri, problemin istifadəçinin giriş hüquqları və ya təhlükəsizlik konfiqurasiyasına və ya identifikasiya serverinin özünə aid olub olmadığını müəyyən etməyə kömək edəcəkdir.

WLAN analizatorları - Təhlil alətləri və tipik istifadə ***Cədvəl 2.14.***

WLAN analiz vasitələri	**Tipik istifadə**
Sayt araşdırması	802.11 olmayan müdaxilə mənbələrini tapmaq. Müdaxilə nəticəsində yaranan aralıq əlaqə problemlərinin araşdırılması. Bütün 802.11a / b / g kanallarının monitorinqi. Səs-küy döşəməsini təyin etmək və yüksək səs-küy və ya aşağı SNR problemlərini müəyyənləşdirmək. Giriş nöqtəsi kanalının istifadəsini və güc səviyyəsini yoxlayın. Kanalın üst-üstə düşdüyü problemlər. Quraşdırma əvvəli modelləşdirmə aparmaq və qeyri-kafi əhatə dairəsi ilə problemli sahələri müəyyənləşdirmək. Sayt araşdırması nəticələrini xüsusi texniki tələblər, məsələn, analiz etmək VoWLAN tətbiqləri üçün.
Təhlükəsizlik qiymətləndirilməsi	Giriş nöqtələrinin siyasətə uyğun təhlükəsizlik konfiqurasiyasına təmin edilməsi. Şifrəli şəbəkə trafikinin görünməsi (WEP, WPA, WPA2). İcazəsiz simsiz

	stansiyaların aşkarlanması və fiziki yeri. Simsiz təhlükəsizlik hücumlarının aşkarlanması. Rədd edilmiş birlik tələblərinin müəyyənləşdirilməsi. Rouminq müştərilərinin fiziki yeri
Aradan qaldırma	Assosiasiya və identifikasiya problemləri. Lokallaşdırılmış WLAN performansı. Şəbəkə ötürmə sürətinin gözlənilənindən daha aşağı. Zamanla WLAN performansında dəyişikliklər.

Bluetooth (802.15.1) radio, 2.4 GHz ISM diapazonunu 802.11b və g şəbəkələri ilə bölüşdüyünə görə, bu iki texnologiya arasında RF müdaxiləsi üçün bir potensial var. Əslində 802.11 FHSS və 802.15.1 spesifikasiyaları eyni 79 açıcı kanaldan istifadə edir və 802.11 DSSS kanalının 22 MHz genişliyi, bitişik kanallar daxil olduqda, 79 atlama kanalından 24-nə müdaxilə edəcəkdir.

Bu radiolar arasındakı müdaxilənin nəticəsi 802.11 şəbəkəsindəki yayılma spektrinin növündən, iki sistemin ötürücü gücündən və aparılan xidmət növündən asılı olacaqdır. İki müdaxilə edən FHSS sistemi üçün 802.11 sistemi daha pis çıxacaq, çünki onun atlama sürəti Bluetooth radiosundan 160 dəfə yavaş olur.

Bu o deməkdir ki, 79 kanalın üstündən keçərkən Bluetooth radiosunun hər ötürülən 802.11 paketi üçün bir neçə dəfə 802.11 radio ilə eyni tezlikdə eniş etməsi deməkdir. 802.11 MAC itirilmiş paketləri təkrarlamaq üçün davamlı sorğular verəcək və şəbəkə ötürmə qabiliyyəti pozulacaqdır. Xoşbəxtlikdən, az sayda 802.11 sistemi FHSS PHY təbəqə xüsusiyyətlərini istifadə edir.

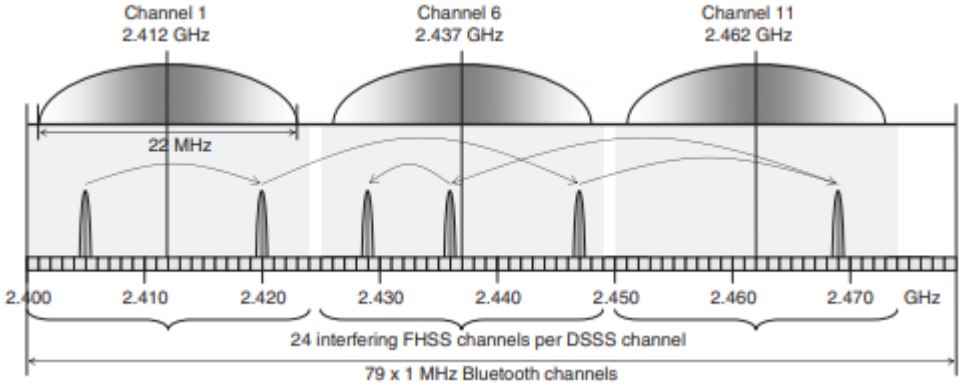
Vəziyyət DSSS 802.11 sistemi üçün bir az daha mürəkkəbdir (şəkil 2.3), çünki birbaşa ardıcıllığın aşkarlanması dar lent müdaxiləsinə qarşı daha möhkəmdir və FHSS paketi ilə DSSS paketi arasında toqquşma ehtimalı asılıdır. WLAN məlumat paketi uzunluğu. Bu vəziyyətdə, Bluetooth bağlantısının müdaxiləyə daha həssas olması ehtimalı yüksəkdir, çünki DSSS müdaxiləsi 79 atış kanalının 24-nə təsir göstərəcəkdir, beləliklə WPAN paketlərinin 30% -i itirilə bilər. Bu, xüsusən Bluetooth qulaqlığına səs ötürülməsi kimi sinxron bağlantılar üçün keçid qabiliyyətini ciddi şəkildə pisləşdirəcəkdir.

IEEE 802.15 Tapşırıq Qrupu TG2 802.11 və 802.15.1 radioları arasındakı müdaxiləni azaltmaq üçün iki növ birlikdə yaşamaq mexanizmindən - birgə və qeyri-əməkdaşlıqdan istifadə edərək tövsiyə olunan təcrübələr hazırlamışdır.

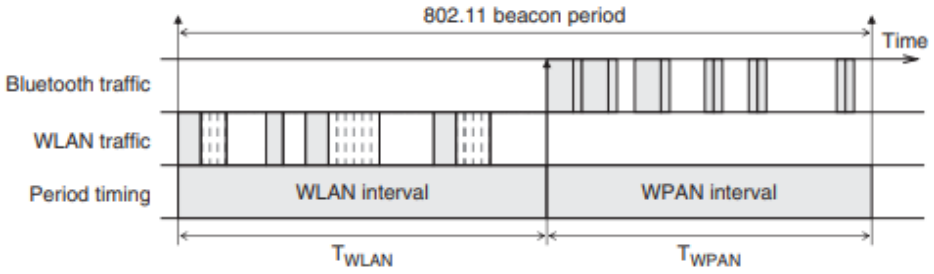
Birgə mexanizmlər, müdaxiləni minimuma endirmək üçün WLAN və WPAN arasında mübadilə edilə biləcəyi zaman mümkündür, əməkdaşlıq olunmayan mexanizm iki şəbəkə arasında məlumat mübadiləsini tələb etmir, lakin mahiyyət etibarilə az effektivdir. Tövsiyə olunan qeyri-əməkdaşlıq yanaşma növləri uyğunlaşma tezliyi atlama, adaptiv paket seçimi və ötürmə gücünə nəzarətdir.

Alternativ simsiz orta giriş (AWMA) adlandırılan birgə TDMA rejimi də tövsiyə edilmişdir, burada mövcud ötürmə müddəti şəkil 2.4-də göstərildiyi kimi WLAN və WPAN ötürmələri arasında bölünür. İki şəbəkə arasında bir rabitə bağlantısına ehtiyac olduğuna görə, bu əməkdaşlıq mexanizmi yalnız iki radio bir ana cihazda olduqda işləyə bilər - məsələn, həm Bluetooth, həm də Wi-Fi üçün aktiv bir noutbuk.

Daha bir əməkdaşlıq mexanizmi deterministik tezlik nulling adlanır. Buradakı konsepsiya, 802.11b qəbuledicisində bu tezliyi ləğv edərək 1 MHz genişliyində FHSS siqnalından dar bant müdaxiləsini azaltmaqdır. Bunu etmək üçün 802.11b qəbuledicisi Bluetooth ötürücüsünün atış və hərəkət müddətinə əməl etməlidir və buna 802.11b qəbuledicisi daxilində Bluetooth qəbuledicisini yerləşdirməklə nail olur.



Şəkil 2.3. Bluetooth və 802.11 DSSS Spectrum üst-üstə düşür



Şəkil 2.4. AWMA-da müəyyən edilmiş WLAN və WPAN ötürmə dövrləri

III FƏSİL. SİMSİZ TEXNLOGİYALARIN MƏHSULDARLIĞININ TƏHLİLİ

3.1. AD-HOC (Advanced Developers Hands on Conference) şəbəkələrinin infrastrukturunun tədqiqi

Ad-hoc şəbəkələri, sabit hesablama cihazlarının sabit bir şəbəkə infrastrukturu olmadıqda və ya istifadə edilməməsi halında mobil hesablama cihazlarının şəbəkə tətbiqetmələrini tələb etdiyi hallarda yaradılır. Bu hallarda, mobil qurğular rabitə ehtiyacları üçün qısa müddətli bir şəbəkə qura bilərdi. Ad-hoc şəbəkələri mərkəzləşdirilməmiş, self organizing şəbəkələrdir və heç bir sabit infrastruktura güvənmədən rabitə şəbəkəsi yaratmağa qadirdirlər.

Şəkil 3.1-də simsiz ad-hoc şəbəkələr ənənəvi simsiz mobil şəbəkələrə nisbətən konseptualdır. Simsiz multi-hop ad hoc şəbəkələri müəyyən bir coğrafi ərazidə yayılmış bir mobil istifadəçi və ya mobil cihaz tərəfindən yaradılır. Şəbəkə qovşaqlarını təşkil edən istifadəçilərə və ya cihazlara zəng edirik.

Ad-hoc şəbəkə xidməti, qovşaqların paylandığı bütün coğrafi ərazidir. Hər bir qovşaq, digər qovşaqlarla əlaqə qurmağa imkan verən bir radio ötürücü və qəbuledici ilə təchiz edilmişdir. Mobil ad-hoc şəbəkələri öz-özünə qurulmuş şəbəkələr olduğundan, ad-hoc şəbəkələrdə rabitə mərkəzi baza stansiyası tələb etmir. Ad-hoc şəbəkəsinin hər bir qovşağı şəbəkədəki digər qovşaq üçün məlumat yarada bilər. Lazım gələrsə, bütün qovşaqlar məlumat paketlərinin son təyinat yerlərinə yönəldilməsi üçün relay stansiyaları kimi işləyə bilər. Mobil ad-hoc şəbəkəsi xüsusi şlüzlər və ya şlüzlər kimi işləyən qovşaqlar, digər sabit şəbəkələrə və ya internetə qoşula bilər. Bu vəziyyətdə mobil ad-hoc şəbəkəsi sabit şəbəkə xidmətlərinə girişi genişləndirir.

Ad-Hoc şəbəkələri praktikada çox istifadə olunur, bu bölmədə ad-hoc şəbəkələrə istinad edərkən həmişə çox hop ad-hoc şəbəkələri nəzərdə tuturuq. Bir-birinin birbaşa radio diapazonundan kənarda qovşaqlar arasında əlaqəni mümkün

edən ad-hok şəbəkələrdəki çox hop dəstəyi, ehtimal ki, mobil ad-hok şəbəkələri və digər simsiz rabitə sistemləri arasındakı ən əhəmiyyətli fərqdir.

Wi-Fi şəbəkələrinin əksəriyyəti infrastruktur rejimində işləyir. Şəbəkədəki cihazların hamısı ümumiyyətlə simsiz yönləndiricisi olan bir giriş nöqtəsi ilə əlaqə qurur. Məsələn, deyək ki, hər biriniz eyni simsiz şəbəkəyə qoşulmuş iki dizüstü kompüteriniz var. Bir-birinin yanında oturanda belə birbaşa əlaqə qurmurlar. Bunun əvəzinə simsiz giriş nöqtəsi ilə dolayı əlaqə qururlar. Paketləri giriş nöqtəsinə göndərirlər - ehtimal ki, simsiz bir yönləndirici - və paketləri digər noutbuka geri göndərir. İnfrastruktur rejimi bütün cihazların qoşulduğu mərkəzi bir giriş nöqtəsini tələb edir.

Şəkil 3.1. Adhoc şəbəkəsində istifadə olunan simsiz marşrutlaşdırıcı

Ad-hoc rejimi "bir ranqlı" rejimi kimi də tanınır. Ad-hoc şəbəkələri mərkəzləşdirilmiş bir giriş nöqtəsini tələb etmir. Bunun əvəzinə simsiz şəbəkədəki qurğular birbaşa bir-birinə bağlanır. İki noutbuku ad-hoc simsiz rejimdə qurarsanız, mərkəzləşdirilmiş bir giriş nöqtəsinə ehtiyac duymadan birbaşa bir-birlərinə bağlanardılar. Adhoc şəbəkələrinin mənfi və müsbət xüsusiyyətlərinə də baxaq

Yalnız mərkəzləşdirilmiş bir giriş nöqtəsi tələb etmədən iki cihazı bir-birinə bağlamaq istəyirsinizsə, ad-hoc rejimi qurmaq daha asandır. Məsələn, deyək ki, iki noutbukunuz var və otel otağında Wi-Fi olmadan otursunuz. Routerə ehtiyac

duymadan müvəqqəti bir Wi-Fi şəbəkəsi yaratmaq üçün onları birbaşa ad-hoc rejimi ilə bağlaya bilərsiniz. Yeni Wi-Fi Direct standartı, ad-hoc rejimi üzərində qurulur və cihazlara birbaşa Wi-Fi siqnalları ilə əlaqə qurmağa imkan verir.

Daha davamlı bir şəbəkə qurarsanız, infrastruktur rejimi idealdır. Giriş nöqtəsi kimi işləyən simsiz marşrutlaşdırıcılar ümumiyyətlə daha geniş ərazini əhatə edə bildikləri üçün daha yüksək gücü simsiz radio və antenalara malikdirlər. Simsiz şəbəkə qurmaq üçün bir dizüstü kompüterinizdən istifadə edirsinizsə, noutbukun simsiz radiosunun gücü ilə məhdudlaşacaqsınız, bu da router kimi güclü olmayacaq.

Ad-hoc rejiminin digər çatışmazlıqları da var. Bu daha çox sistem qaynaqlarını tələb edir, çünki fiziki şəbəkə düzeni qurğular hərəkət edərkən dəyişəcək, infrastruktur rejimində bir giriş nöqtəsi isə ümumiyyətlə sabit qalır. Bir çox cihaz ad-hoc şəbəkəsinə qoşulsa, daha çox simsiz müdaxilə olacaq - hər bir kompüter bir giriş nöqtəsindən keçmək əvəzinə bir-birinə birbaşa əlaqə qurmalıdır. Bir cihaz qoşulmaq istədiyi başqa bir cihazın xaricindədirsə, məlumatı yolda digər cihazlardan ötürür. Məlumatları bir neçə kompüterdən keçmək, bir giriş nöqtəsindən keçməkdən daha yavaş olur. Ad-hoc şəbəkələri yaxşı miqyas vermir.

Şəbəkənin hər növünü nə vaxt istifadə edəcəyinizə qərar vermək əslində olduqca sadədir. Bir giriş nöqtəsi kimi işləmək üçün simsiz bir yönlendirici qurarsanız, onu infrastruktur rejimində tərk etmək istərdiniz. Bir neçə cihaz arasında müvəqqəti simsiz şəbəkə qurursan, ad-hoc rejimi yaxşı olar.

Burada daha bir böyük tutma var. Məhdudiyyətlərə görə bir çox cihaz ad-hoc rejimini dəstəkləmir. Android cihazları, simsiz printerlər, Google-un Chromecast və bir çox digər Wi-Fi effektiv cihazları ad-hoc şəbəkələrinin problemləri ilə məşğul olmaq istəmir və yalnız infrastruktur rejimində şəbəkələrə qoşularaq onlara qoşulmaqdan imtina edəcəklər. Bu barədə edə biləcəyiniz çox şey yoxdur; sadəcə bir ad hoc rejimində deyil, infrastruktur rejimində bir şəbəkədən istifadə etməlisiniz.

3.2. MİMO (Multiple input, multiple output) texnologiyasının üstünlükləri və məhdudiyyətləri

MIMO texnologiya simsiz rabitə sistemlərində birdən çox məlumat axını eyni anda ötürmək üçün bir çox antenaya əsaslanır. MIMO eyni anda bir neçə terminal ilə əlaqə qurmaq üçün istifadə edildikdə, çox istifadəçi MIMO-dan danışırıq.

Mobil sistemlərindəki MU-MIMO dörd istiqamətdə inkişaf edir:

• verilənlərin sürəti artdı, çünki antenlər nə qədər çox olarsa, daha müstəqil məlumat axınları göndərilə bilər və eyni vaxtda daha çox terminal təmin edilə bilər;

• gücləndirilmiş etibarlılıq, çünki daha çox antennalar radio siqnalının yayıla biləcəyi daha fərqli yollardır;

• Enerji səmərəliliyinin yüksəldilməsi, çünki baza stansiyası yayılan enerjisini yerləşdiyini bildiyi məkan istiqamətlərinə yönəldə bilər; və

• baza stansiyası yayılan müdaxilənin zərərli olacağı istiqamətlərə ötürülməsinin qarşısını ala biləcəyi üçün müdaxiləni azaldır.

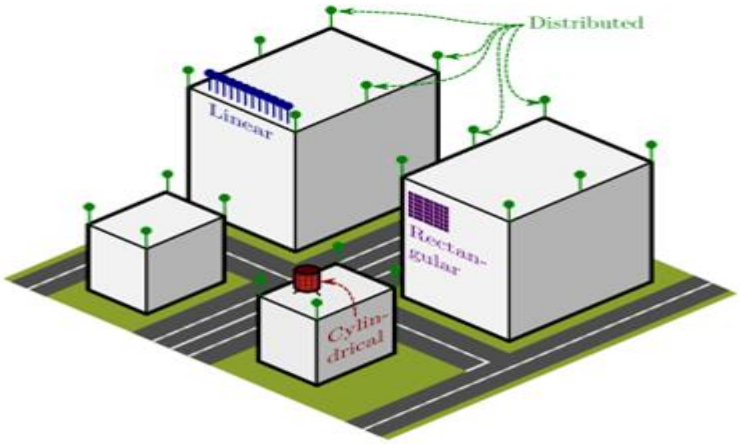
Bütün inkişaflara eyni vaxtda nail olmaq mümkün deyil və yayılma şərtlərinə dair tələblər var, lakin yuxarıdakı dörd istiqamət ümumi faydadır. Ənənəvi simsiz rabitə üçün MU-MIMO texnologiyası yetkinləşir və 4G LTE və LTE-Advanced kimi son və inkişaf edən simsiz genişzolaqlı standartlara daxil edilmişdir. Baza stansiyası (və ya terminallar) nə qədər çox antena ilə təchiz olunarsa, yuxarıda göstərilən dörd cəhətdən ən azı TDD rejimində işləmək üçün daha yaxşı bir performans göstərər. Bununla birlikdə, bu gün istifadə olunan antenaların sayı uyğunlaşdırılır. Ən müasir standart, LTE-Advanced, baza stansiyasında 8 antena birləşməsinə sahib olmağa imkan verir və bu gün qurulan avadanlıqlarda bundan daha az anten var.

Kütləvi MIMO, inkişaf etmiş bir texnologiyadır, MIMO-nu cari vəziyyətlə müqayisədə böyük ölçü sifarişinə görə genişləndirir. Bu yazıda, son üç ildə baş verən

hadisələrə diqqət yetirərək, əvvəllər ekspozisiyamızı nəzərdən keçiririk: ən çox enerji səmərəliliyi, həddindən artıq azadlıqların istismarı, TDD kalibrlənməsi, pilot çirklənmə ilə mübarizə üsulları və tamamilə yeni kanal ölçmələri.

Kütləvi MIMO ilə eyni vaxt tezlik mənbəyində eyni vaxtda çox sayda onlarla terminala xidmət edən bir neçə yüz anten ilə anten seriallarını istifadə edən sistemləri düşünürük. Kütləvi MIMO-nun əsas yeri daha böyük miqyasda şərti MIMO-nun bütün faydalarını yığmaqdır. Ümumiyyətlə, kütləvi MIMO, enerjiyə qənaətli, etibarlı və möhkəm olacaq və spektrdən səmərəli istifadə edəcək gələcək genişzolaqlı (sabit və mobil) şəbəkələrin inkişafına imkan yaradır. Bu, gələcəkdə rəqəmsal cəmiyyət quruluşu üçün insanların İnternetini, əşyaların İnternetini buludlarla və digər şəbəkə infrastrukturları ilə birləşdirəcək bir fürsətdir.

Kütləvi MIMO sistemi tərəfindən istifadə edilən həqiqi anten serialları üçün bir çox fərqli konfiqurasiya və yerləşdirmə ssenarisini görmək olar (şəkil 3.2)



Şəkil 3.2. Kütləvi MIMO əsas stansiyası üçün bəzi mümkün anten konfiqurasiyaları və yerləşdirmə ssenariləri.

Kütləvi MIMO məkan multipleksasiyasına güvənir, bu da öz növbəsində həm yuxarı, həm də enmə nöqtəsində kifayət qədər yaxşı kanal bilgisi olan baza stansiyasına etibar edir. Yuxarıda, baza stansiyası terminalların hər birinə kanal cavablarını qiymətləndirdiyinə görə terminalların pilot göndərməsini təmin etməklə bunu etmək asandır. Aşağı əlaqə daha çətindir. Adi MIMO sistemlərində, LTE standartı kimi, baza stansiyası pilot dalğa formalarını göndərir, bunun əsasında

terminallar kanal cavablarını qiymətləndirir, alınan təxminləri ölçür və yenidən baza stansiyasına göndərir. Kütləvi MIMO sistemlərində, ən azı yüksək hərəkətli bir mühitdə işləyərkən iki səbəbə görə mümkün olmayacaqdır. Birincisi, optimal endirmə pilotları antenlər arasında qarşılıqlı ortogonal olmalıdır. Bu o deməkdir ki, pilot şkalası antenaların sayı qədər azaltmaq üçün lazım olan vaxt çatışmazlığı mənbələrinin miqdarı, beləliklə kütləvi MIMO sistemi adi bir sistemdən yüz qat daha çox bu cür resurs tələb edir. İkincisi, hər bir terminalın hesablamalı olduğu kanal cavablarının sayı da əsas stansiya antenlərinin sayına mütənasibdir. Beləliklə, baza stansiyasını kanal cavabları barədə məlumatlandırmaq üçün lazım olan yüksək mənbələr adi sistemlərə nisbətən yüz qat daha böyük olacaqdır. Ümumiyyətlə, həll TDD rejimində işləmək yuxarı və aşağı xətt kanalları arasındakı qarşılıqlılığa güvənməkdir - baxmayaraq bəzi hallarda FDD əməliyyatı mümkün ola bilər .

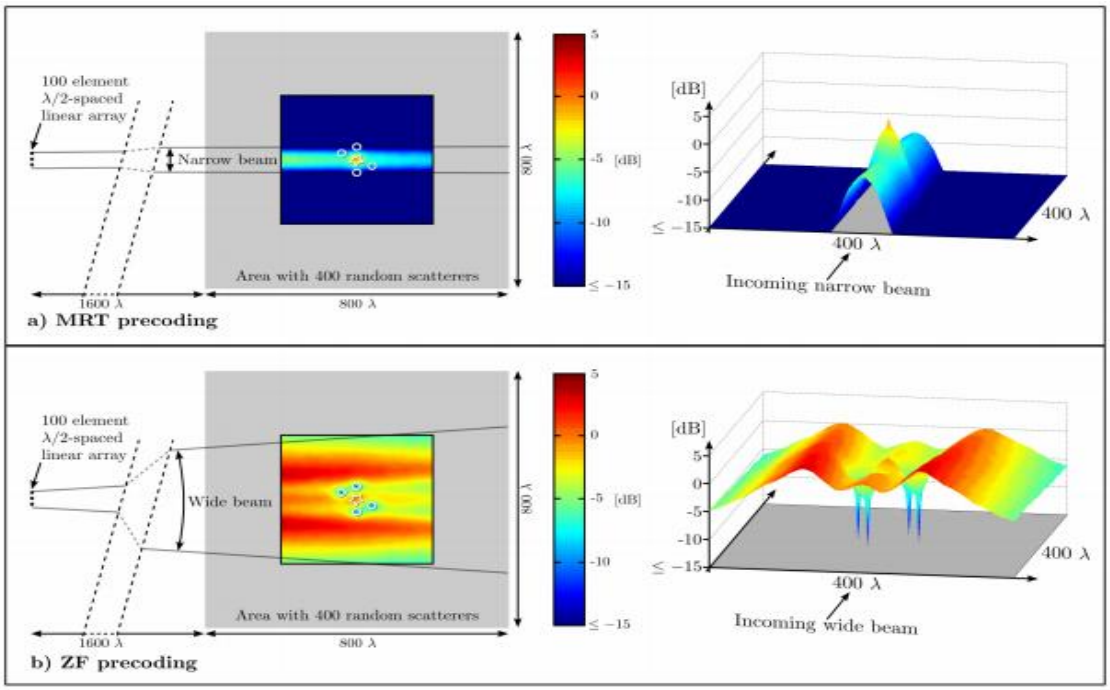
Kütləvi MIMO anlayışları bu günə qədər əsasən nəzəri olmuşdur və xüsusən təsadüfi matris nəzəriyyəsi və əlaqəli riyaziyyatda çox tədqiqat stimullaşdırılsa da, əsas çarpayılar mövcuddur və ilkin kanal ölçmələri aparılmışdır.

Kütləvi MIMO texnologiyası baza stansiyasındakı bütün antenlərdən gələn siqnalların faza əlaqəli, lakin hesablama baxımından çox sadə işlənməsinə əsaslanır. Kütləvi MU-MIMO sisteminin bəzi xüsusi üstünlükləri bunlardır:

Kütləvi MIMO gücü 10 dəfə və ya daha çox artıra bilər və eyni vaxtda radiasiya olunan enerji effektivliyini 100 dəfə artıra bilər.

Tutumun artması kütləvi MIMO-da istifadə olunan aqressiv məkan multipleksasiyası nəticəsində baş verir. Enerji səmərəliliyinin kəskin artmasını mümkün edən əsas prinsip, çox sayda antena ilə enerjinin kosmosdakı kiçik bölgələrə həddindən artıq kəskinliklə yönəldilməsidir. Antenalar tərəfindən göndərilən siqnalları düzgün şəkildə formalaşdıraraq, baza stansiyası, bütün antenlər tərəfindən yayılan bütün dalğa cəbhələrinin nəzərdə tutulan terminalların yerləşdiyi yerlərdə konstruktiv şəkildə artdığına, lakin demək olar ki, hər yerdə dağıdıcı (təsadüfi) olduğuna əmin ola bilər. Terminallar arasındakı müdaxilə, məsələn, sıfır

məcburetmə (ZF) istifadə etməklə daha da sıxışdırıla bilər. Bununla birlikdə, Şəkil 3.3-də göstərildiyi kimi, daha çox ötürülən gücün dəyəri ola bilər.



Şəkil 3.3. Baza stansiyası 1600λ sola yerləşdirildiyi zaman 800λ × 800λ ölçülü bir səpələnmə mühitində bir hədəf terminalının ətrafındakı nisbi sahə gücü. İki fərqli xətti prekoder istifadə edildikdə, orta sahə gücü 400 səpələnmənin 10000-dən çox təsadüfi yerləşdirilməsində hesablanır: a) MRT prekoderləri və b) ZF prekoderləri. Solda: mərkəzdə hədəf istifadəçi mövqeləri olan və yaxınlığında digər dörd istifadəçi olan orta sahə qüvvələrinin yalançı rəngli sahələri. Sağ: fəza fokuslanmasına alternativ bir görünüş verməyə imkan verən səth sahələri kimi orta sahə gücləri.

Daha kəmiyyətcə, şəkildə enerji sərfiyyatı arasında Joule-yə ötürülən bitlərin ümumi sayına (toplama dərəcəsi) sərf olunan enerjiyə xidmət və spektral effektivlik baxımından enerji səmərəliliyi arasındakı əsas dövriyyəsi və istehlak olunan radio spektrinin vahidinə ötürülən bitlərin ümumi miqdarı (cəmi-dərəcəsi) təsvir edir. Şəkil, terminallardan baza stansiyasına qədər yüksəlmə ilə əlaqəni göstərir (aşağı bağlama işi bənzərdir). Rəqəm üç hal üçün ticarət dövriyyəsini göstərir:

- vahid bir terminala (bənövşəyi) xidmət göstərən bir anten ilə istinad sistemi;

- şərti şüa düzəldici (yaşıl) istifadə edərək bir terminala xidmət edən 100 anten ilə bir sistem.

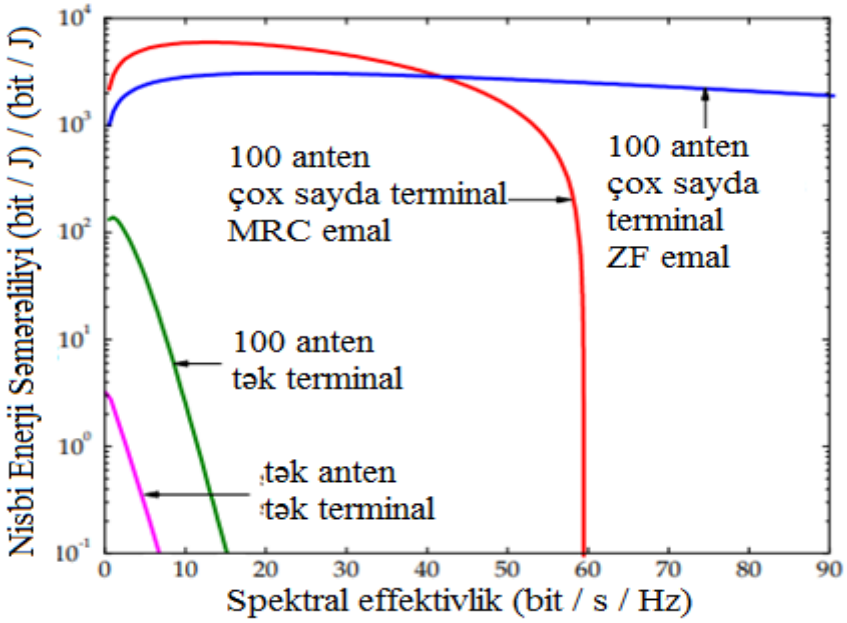
- eyni vaxtda birdən çox (təxminən 40-a yaxın) terminallara xidmət edən 100 anten ilə kütləvi MIMO sistemi (qırmızı, maksimum nisbəti birləşdirən və mavi, zeroforcing istifadə edərək).

ZF ilə müqayisədə maksimum nisbətli birləşmənin (MRC) cəlbediciliyi təkcə hesablama sadəliyi deyil - alınan siqnalların birləşmiş kanal cavabları ilə çoxaldılması, eyni zamanda hər bir anten bölməsində müstəqil olaraq paylanmış şəkildə həyata keçirilməsidir. ZF şərti və ya orta ölçülü MIMO sistemi üçün kifayət qədər yaxşı işləməsinə baxmayaraq, MRC ümumiyyətlə etmir. MRC-nin kütləvi MIMO üçün bu qədər yaxşı işləməsinin səbəbi, müxtəlif terminallar ilə əlaqəli kanal cavablarının əsas stansiya antenlərinin sayı çox olduqda ortogonal olmağına görədir.

Şəkil 3.3-dəki proqnoz, yüksək sürətlə hərəkətli bir mühitdə kanal vəziyyətinə dair məlumat əldə etmək üçün pilotların istifadəsinin bant genişliyi və enerji xərclərini nəzərə alan məlumat-nəzəri təhlilə əsaslanır. MRC qəbuledicisi ilə, məlumat nəzəriyyəsinin səs-küylə məhdud bir rejimində işləyirik. Bu, hər bir terminalın mürəkkəb ölçüdə təxminən 1 bit dərəcəsi təmin etməsi deməkdir (1 bp / Hz). Kütləvi MIMO sistemində, MRC istifadə edərkən və "yaşıl" rejimdə işləyərkən, yəni ümumi spektral effektivliyə, çox istifadə müdaxiləsinə və aparat qüsurlarının təsirinə ciddi təsir etmədən gücün mümkün qədər azaldılması və termal səs-küy meyli daha yüksəkdir. Ümumi spektral effektivliyin hələ də adi MIMO ilə müqayisədə 10 qat daha yüksək ola biləcəyinin səbəbi, on minlərlə terminalın eyni vaxt tezlik mənbəyində eyni vaxtda xidmət göstərməsidir. Bu rejimində işləyərkən intersymbol müdaxiləsinin əlavə istilik səs-küyü kimi qiymətləndirilə biləcəyinə dair bir sıra sübutlar var [10], buna görə də intersymbol müdaxiləsi ilə mübarizə vasitəsi kimi OFDM ilə müzakirə yolunu təklif edir.

Kütləvi MIMO-nun təklif etdiyi tutum qazancının miqyasını başa düşmək üçün, ümumi gücü 120 Vatt (yəni, ümumi güc amili 6400 × (λ / 2) 2 ≈ 40 m2) olan

6400 omniyönlü antenalardan ibarət bir plan düşünün Kütləvi MIMO-nun təqdim etdiyi tutum qazancının miqyasını başa düşmək üçün, PCS bantında 20 MHz bant genişliyi ilə 120 Vat gücündə ötürülən 6400 omn yönlü antenadan ibarət bir sıra düşünün. Dövrədə, ardıcıllığın(array) mərkəzində 6 km radiusda olan diskdə təsadüfi olaraq paylanan min (1000) sabit terminala xidmət edir, hər terminalı 8 dB qazanc anteninə sahibdir. Anten serialının hündürlüyü 30 m, terminalların hündürlüyü 5 m-dir. Hata-COST231 modelini istifadə edərək, yol itkisinin 1 km aralığında 127 dB, aralığın zəifləməsi isə 3.52 olduğunu görürük. 8 dB standart sapma ilə log-normal kölgə solma da var. Qəbuledicidə 9 dB səs-küy forması var. Vaxtın dörddə biri TDD kanalının qiymətləndirilməsi üçün yuxarı pilotların ötürülməsinə sərf olunur və kanalın qazancını kifayət qədər dəqiqliklə qiymətləndirmək üçün kanalın 164 ms aralıqdan əhəmiyyətli dərəcədə sabit olduğu güman edilir.



Şəkil 3.4. Yarım güc - iki dəfə güc : Uplink spektral səmərəliliyini 10 dəfə artırmaq və eyni zamanda kütləvi MIMO texnologiyası ilə enerjini və enerjini nəzərə alaraq kütləvi MIMO texnologiyası ilə 100 dəfə radiasiya gücünün səmərəliliyini 100 dəfə artırmaq. kanal vəziyyəti haqqında məlumat əldə etmə qabiliyyəti.

Dağıtma məlumatları, ən yüksək kanallara sahib olan terminalların 5% -i xidmətdən xaric edildiyi güc idarəetmə ilə birləşdirilmiş şüa şəklində ötürülür.

Yavaş solma, yaxın / uzaq effektlər və güc nəzarətini təmin etmək üçün genişləndirilmiş və qəbuledici səs-küy, kanal qiymətləndirmə səhvləri, pilot ötürülməsinin yerüstü dəyəri və MRT şüalanmasının qüsurlarını nəzərə alan bir tutumdan istifadə edirik. 950 terminalın hər birində bərabər siqnal-toferensiya və səs-küy nisbətini təmin edən optimal maksimum güc nəzarətindən istifadə edirik.

Təsadüfi terminal yerləri və kölgə solma üzərində ortalama, terminalların 95% -inin 21,2 Mb/s terminal ötürmə qabiliyyətinə sahib olacağını göstərir. Ümumiyyətlə, bu nümunədəki serial 1000 bit/s/Hz-lik cəmi-spektral səmərəliliyi ilə nəticələnən 20 Gb/s ümumi endirmə ötürmə qabiliyyətini təklif edəcəkdir. Bu, məsələn, min evin hər birinə 20 Mbit/s genişzolaqlı xidmət göstərmək üçün kifayət edərdi. Maksimum gücə nəzarət eyni vaxtda 950 terminala bərabər xidmət göstərir. Vaxt bölgüsü multipleksasiyası ilə birlikdə gücə nəzarətin digər növləri, daha böyük bir sıra terminalların heterojen trafik tələblərini ödəyə bilər.

MRC qəbuledicisi (uplink üçün) və onun həmkarı MRT kodlaşdırması (aşağı əlaqə üçün) ədəbiyyatda uyğunlaşmış filtrləmə (MF) kimi də tanınır. Kütləvi MIMO ucuz, aşağı gücə malik komponentlərlə inşa edilə bilər.

Massive MIMO həm nəzəriyyə, sistem və tətbiq baxımından oyun dəyişdirən bir texnologiyadır. Kütləvi MIMO ilə, adi sistemlərdə istifadə olunan bahalı, ultra xətti 50 vatt gücləndiricilər, milli-vatt diapazonunda çıxış gücü olan yüzlərlə aşağı qiymətli gücləndiricilərlə əvəz olunur. Yüksək güclü gücləndiricilərdən qidalanan bir neçə anten istifadə edən klassik serial dizaynlarına ziddiyyət vacibdir. Böyük bir koaksial kabellər kimi bir neçə bahalı və həcmli əşyalar tamamilə aradan qaldırıla bilər. Kütləvi MIMO, hər bir fərdi gücləndiricinin və RF zəncirinin dəqiqliyi və doğruluğuna olan məhdudiyyətləri azaldır. Əhəmiyyətli olanların hamısı birlikdə hərəkətlərdir. Bir şəkildə, kütləvi MIMO, çox sayda antennadan gələn siqnalların havada bir yerə yığılmasından əmin olmaq üçün səs-küyün, solğunluq və hardware qüsurlarının ortadan qalxdığına əmin olmaq üçün çox sayda qanuna əsaslanır. Kütlənmiş MIMO-nun solğunluğa qarşı davamlı olmasını təmin edən eyni

xüsusiyyət, eyni zamanda bir və ya bir neçə anten cihazının işləməməsi üçün texnologiyanı son dərəcə möhkəm edir.

Kütləvi MIMO sistemi böyük bir sərbəstlik dərəcəsinə malikdir. Məsələn, 20 terminala xidmət edən 200 anten ilə 180 dərəcə sərbəst istifadə edilmir. Bu sərbəstlik dərəcələri, cihaz üçün dostluq siqnalının formalaşdırılması üçün istifadə edilə bilər. Xüsusilə, hər bir anten, artan ümumi radiasiya gücü baxımından çox kiçik bir zirvə-ortalama nisbəti və ya hətta sabit zərf olan siqnalları çox cəlbedici şəkildə ötürə bilər. Belə (yaxınlıqdakı) zərf siqnalları son dərəcə ucuz və enerjiyə qənaətli RF gücləndiricilərinin istifadəsini asanlaşdırır. Bu üsullar adi şüa dəyişdirmə üsulları və ya bərabər gücdə çəki şüa dəyişdirmə üsulları ilə qarışdırılmamalıdır. Bu fərq şəkil 3.5-da izah edilmişdir. Zəruri davamlı zərfdə çox istifadəçi kodlaşdırması ilə şüalar əmələ gəlmir və hər bir antendən yayılan siqnallar bir simvolu çəkməklə əmələ gəlmir. Əksinə, dalğa sahəsi yaradılmışdır ki, bu dalğa sahəsi terminalların yerləşdiyi yerlərdə nümunə götürüldükdə, terminallar onların görmək istədiyimiz siqnalları dəqiq görürlər.

Mümkün olan kütləvi MIMO kanalının əsas xüsusiyyəti, kanalın böyük bir boşluq olmasıdır: demək olar ki, hər şeyi terminalların gördüklərinə təsir etmədən bu boşluğa qoymaq olar. Xüsusilə, ötürülən dalğa formalarının istənilən zərf məhdudiyyətlərini ödəməsini təmin edən komponentləri bu boşluğa qoymaq olar. Buna baxmayaraq, baza stansiyası və terminalların hər biri arasındakı təsirli kanallar hər hansı bir siqnal bürcünü giriş kimi qəbul edə bilər və PSK tipli modulyasiyanın istifadəsini tələb etmir.

Kəskin surətdə təkmilləşdirilmiş enerji səmərəliliyi kütləvi MIMO sistemlərinə cari texnologiyadan daha az ümumi iki çıxış əmri ilə işləməyə imkan verir.

Bu vacibdir, çünki mobil baza stansiyalarının enerji istehlakı dünyada artan bir narahatlıqdır. Bundan əlavə, daha az gücdə bir çox sifariş istehlak edən baza stansiyaları külək və ya günəşlə təchiz oluna bilər və buna görə də heç bir elektrik

şəbəkəsinin olmadığı yerlərdə asanlıqla yerləşdirilə bilər. Bir bonus olaraq ümumi yayılan güc kəskin şəkildə kəsilə bilər və buna görə baza stansiyası əhəmiyyətli dərəcədə az elektromaqnit müdaxilə yaradacaqdır. Bu, elektromaqnit təsirinin artması ilə əlaqədar vacibdir.

• Kütləvi MIMO hava interfeysində gecikməni əhəmiyyətli dərəcədə azaltmağa imkan verir.

Simsiz rabitə sistemlərinin fəaliyyəti normal olaraq solğunluqla məhdudlaşır. Solğunluq alınan siqnal gücünü bəzi vaxtlarda çox az göstərə bilər. Bu, bir baza stansiyasından göndərilən siqnal terminala çatmadan çox yoldan keçəndə baş verir və bu çoxsaylı yollardan gələn dalğalar dağıdıcı şəkildə müdaxilə edir. Məhz bu solğunluq aşağı gecikmə simsiz bağlantıları qurmağı çətinləşdirir. Terminal solğun bir dalğa içində qalsa, yayılma kanalının hər hansı bir məlumat alınana qədər kifayət qədər dəyişməsini gözləmək lazımdır. Kütləvi MIMO solğunlaşmanın qarşısını almaq üçün çox sayda qanununa və şüa düzəltməyə güvənir ki, solğunluq artıq gecikməni məhdudlaşdırmır.

• Kütləvi MIMO çox giriş qatını asanlaşdırır.

Çox sayda qanuna görə kanal sərtləşir ki, tezlik-domen planlaşdırması artıq işləmir. OFDM ilə, kütləvi bir MIMO sistemindəki hər bir subcarrier əhəmiyyətli dərəcədə eyni kanal qazancına sahib olacaqdır. Hər bir terminala fiziki təbəqə nəzarət siqnalının çoxunu təmin edən bant genişliyi verilə bilər.

• Kütləvi MIMO, həm də insan tərəfindən hazırlanmamış müdaxilələrə və qəsdən tıxanma hallarına davamlılığı artırır.

Mülki simsiz sistemlərin qəsdən tıxanması artan narahatlıq və ictimaiyyətə az məlum kimi görünən ciddi bir təhlükədir. Sadə tıxacları İnternetdən bir neçə 100 dollara almaq olar və hərbi dərəcədə istifadə olunan avadanlıqlar, bir neçə min dollara satışdan kənar proqram təminatlı radio əsaslı platformalardan istifadə edərək bir yerə yığıla bilər. Son zamanlarda baş verən çoxsaylı hadisələr, xüsusən də ictimai təhlükəsizlik tətbiqləri problemin miqyasını göstərir. 2001-ci ildə İsveçin Göteborq

şəhərində keçirilən AB sammiti zamanı nümayişçilər yaxınlıqdakı bir mənzildə olan tıxacdan istifadə etdilər və iğtişaşların kritik mərhələlərində baş komandir məşğul olan 700 polis işçisindən heç birinə çata bilmədi.

Bant genişliyinin azlığı səbəbindən məlumatların tezlik üzərində yayılması mümkün deyil, buna görə simsiz rabitənin möhkəmliyini artırmağın yeganə yolu çoxlu antenlərdən istifadə etməkdir. Kütləvi MIMO, qəsdən sıxışanların siqnallarını ləğv etmək üçün istifadə edilə bilən bir çox həddən artıq azadlıq təklif edir. Kütləvi MIMO kanal qiymətləndirilməsi üçün yüksək pilotlardan istifadə etməklə həyata keçirilsə, ağıllı tıxacçılar təvazökar ötürmə gücünə zərərli müdaxilə edə bilər. Bununla birlikdə, ortaq kanalın qiymətləndirilməsi və kodlaşdırmadan istifadə edərək daha ağıllı tətbiqlər bu problemi əhəmiyyətli dərəcədə azaltmağı bacarmalıdır. MIMO texnologiyasının üstünlüklərindən danışdıq indi isə onu məhdudlaşdıran amilləri nəzərdən keçirək.

TDD əməliyyatı kanal qarşılıqlılığına əsaslanır. Yayılma qəribə maqnit xüsusiyyətləri olan materiallardan təsirlənməsə, yayılma kanalının özünün mahiyyətcə qarşılıqlı olması barədə ağlabatan bir fikir var. Bununla birlikdə, baza stansiyasında və terminal ötürücülərində olan cihaz zəncirləri yuxarı və aşağı xətt arasında qarşılıqlı olmaya bilər. Dəstək zəncirlərinin kalibrlənməsi ciddi bir problem yaratmır və praktikada müəyyən dərəcədə sınanmış kalibrləmə əsaslı həllər mövcuddur [11]. Xüsusilə, 64 antenna sistemi üçün qarşılıqlı hesablama kalibrini bəzi təfərrüatlarla həll edir və uğurlu bir təcrübə tətbiqini tələb edir.

Diqqət yetirin ki, kütləvi MIMO-nun tam şüa meydana gətirən qazanclarını əldə etmək üçün terminalın yuxarı və aşağı bağlama zəncirlərinin kalibrlənməsi tələb olunmur: baza stansiyası avadanlıqları düzgün kalibrlənmişsə, serial həqiqətən mütənasib bir şüa ötürəcəkdir. (Terminalın qəbuledici zəncirində hələ də uyğunsuzluq olacaq, lakin bu, pilotları şüa vasitəsilə terminala ötürməklə həll edilə bilər; bu əlavə pilotlar üçün yerüstü yük çox azdır.) Serialda mütləq kalibrləmə tələb olunmur. Bunun əvəzinə, antenlərin birinə bir istinad kimi baxıla bilər və siqnallar istinad anteni ilə digər antenaların hər biri arasında bu antena görə bir kompensasiya

amili əldə etmək üçün satıla bilər. Tamamilə serial daxilində qarşılıqlı hesablama kalibrindən imtina etmək mümkündür; məsələn yuxarı bağlama zənciri ilə aşağı bağlama zənciri arasındakı maksimal faza fərqi 60 dərəcədən az olsaydı, qazancın 3 dB azalmasına baxmayaraq əlaqəli şüa əmələ gəlməsi hələ də davam edəcəkdir.

İdeal olaraq Massive MIMO sistemindəki hər bir terminala ortoqonal uplink pilot ardıcıllığı verilir. Lakin mövcud ola biləcək ortogonal pilot ardıcıllıqların maksimum sayı kanalın gecikmə-yayılmasına bölünən uyğunluq intervalının uzunluğu ilə məhdudlaşır [12], tipik bir əməliyyat ssenarisi üçün, bir milisaniyəlik uyğunluq aralığında ortogonal pilot ardıcıllıqlarının maksimum sayının təxminən 200 olduğu təxmin edilir. Çox mobilli bir sistemdə ortogonal pilot ardıcıllığı tükənmək daha sadədir.

Pilotların bir hücrədən digərinə təkrar istifadəsinin təsiri və əlaqəli mənfi nəticələr "pilot çirklənməsi" adlanır. Daha dəqiq desək, xidmət seriyası, alınan pilot siqnalını müəyyən bir terminal ilə əlaqəli pilot ardıcıllığı ilə əlaqələndirəndə, əslində eyni pilot ardıcıllığı bölüşən digər kanallara kanalların xətti birləşməsi ilə çirklənmiş bir kanal qiymətləndirməsini əldə edir. Çirklənmiş kanalın təxmininə əsaslanan aşağı əlaqə şüaları eyni pilot ardıcıllığı bölüşən terminallara yönəlmiş müdaxilə ilə nəticələnir. Bənzər müdaxilə məlumatların yüksək ötürülməsi ilə əlaqələndirilir. Bu yönəldilən müdaxilə istədiyi siqnal ilə eyni nisbətdə xidmət antenlərinin sayı ilə artır. Hətta qismən korrelyasiya edilmiş pilot ardıcıllığı yönəldilmiş müdaxilə ilə nəticələnir.

Pilotun əsas fenomen kimi çirklənməsi həqiqətən kütləvi MIMO üçün spesifik deyil, lakin kütləvi MIMO-ya təsiri klassik MIMO-ya nisbətən daha dərin görünür [13]. Ən azı pilot əsaslı kanal hesablamasına güvənən qəbuledicilərlə, antenaların sayının artırılmadan artırıldığı zaman performansın son həddi olduğu iddia edildi. Bu arqument yaxınlarda mübahisə edilsə də, heç olmasa istifadə edilən güc nəzarətinə dair müəyyən fərziyyələrə əsasən, pilot çirklənməsinin bu və ya digər şəkildə həll edilməsi lazım olduğu görünür. Bu bir neçə yolla edilə bilər:

• Pilot dalğa formalarının ayrılması optimallaşdırıla bilər. Bir ehtimal pilotların daha az təsirli bir tezlik istifadəsi amillərindən istifadə etməkdir (lakin yükləmə məlumatları üçün mütləq deyil). Bu qarşılıqlı çirkləndirici Mobilləri bir-birindən daha da uzaqlaşdırır. Pilotların istifadəsini koordinasiya etmək və ya şəbəkədəki fərqli terminallara uyğunlaşdırıcı şəkildə pilot ardıcıllığı ayırmaq da mümkündür [14]. Hal hazırda optimal strategiya məlum deyil.

• Ağıllı kanal qiymətləndirmə alqoritmləri və ya pilotların tamamilə istifadə edilməsini maneə törədən kor texnikalar [15], pilot çirklənmənin təsirini yumşalda bilər və ya aradan qaldıra bilər. Ən perspektivli istiqamət, kanalları və yükləmə məlumatlarını birlikdə qiymətləndirən kor texnikalardır.

• Şəbəkə quruluşunu nəzərə alan yeni kodlaşdırma üsulları, məsələn, pilot çirklənmə kodlaşdırması [16], şüa formalaşdırma əməliyyatından kənarda çoxlu hüceyrələr üzərində kooperativ ötürülmədən, ən azı qismən, pilot nəticəsində yaranan müdaxiləni ləğv etmək üçün istifadə edə bilər. çirklənmə. Terminallar və çirkləndirici hüceyrələrin xidmət zonaları arasındakı həqiqi kanalların qiymətləndirilməsini tələb edən çoxsaylı hüceyrələr üzərində əlaqələndirilmiş şüa düzəltmədən fərqli olaraq, pilot çirklənmə kodlaşdırması yalnız müvafiq yavaşlayan əmsalları tələb edir. Praktik pilot-çirklənmə kodlaşdırması inkişaf etdirilməkdədir.

Kütləvi MIMO, əlverişli yayılma adlanan radio mühitinin bir xüsusiyyətinə çox bağlıdır. Sadəcə olaraq, əlverişli yayılma o deməkdir ki, baza stansiyasından fərqli terminallara yayılan kanal cavabları kifayət qədər fərqlidir. Kütləvi MIMO sistemlərinin davranışını öyrənmək üçün, real antenna seriallarından istifadə edərək kanal ölçmələri aparılmalıdır. Bu, böyük seriallardan istifadə edən kanal davranışının adi kiçik seriallardan istifadə etməklə ümumiyyətlə təcrübəli olduğundan fərqli olmasıdır. Ən əhəmiyyətli fərqlər serialda geniş miqyasın azalması ola bilər və serialda kiçik miqyaslı siqnal statistikası da dəyişə bilər. Əlbəttə ki, bu, müxtəlif istiqamətlərə işarə edən antenna elementləri olan fiziki cəhətdən daha kiçik massivlər üçün də doğrudur. Şəkil 3.5, bu sənəddə bildirilən ölçmələr üçün istifadə olunan iki kütləvi MIMO seriallarının şəkillərini göstərir. Sol

tərəfdə 128 anten portu olan kompakt dairəvi kütləvi MIMO serialı var. Bu sıra, bir dairədə düzülmüş 16 cüt qütblü yamaq antenna elementlərindən ibarətdir, 4 ədəd bu dairələr bir-birinin üstünə yığılmışdır. Kompakt olmağın üstünlüyünə əlavə olaraq, bu sıra müxtəlif yüksəkliklərdə dağınıqları həll etmək imkanı da verir, lakin məhdud diyaframa görə azimutda daha pis qətnamədən əziyyət çəkir. Fərqli terminallara cavab olaraq 128 fərqli mövqeyə köçürülən fiziki cəhətdən böyük bir xətti (virtual) bir sıra, ən kiçik və böyük ölçüdə yayılmaq eyni ölçüləri olan həqiqi serial üçün başqa bir statik mühitin yayılmasına baxmaqdır.

Kanal cavablarını özündə cəmləşdirən matrisanın ən çox yayılmış tək-tək dəyərlərinin nə dərəcədə fərqli olduğunu müəyyənləşdirməyin bir yolu, fiziki cəhətdən böyük tək qütblü xətti sıra və ya yığcam cüt qütblü dairəvi sıra kimi qurulmuş 4 istifadəçi terminalı və müvafiq olaraq 4, 32 və 128 antenna portu olan bir baza stansiyası üçün bir vəziyyət göstərir. Daha dəqiq desək, rəqəm fərqli hallarda müxtəlif ölçülən (ensiz) tezlik nöqtələri üçün ən kiçik və ən böyük tək dəyər arasındakı fərqin məcmu sıxlıq funksiyasını (CDF) göstərir. Bir arayış olaraq tez-tez nəzəri tədqiqatlarda istifadə olunan ideal müstəqil, eyni dərəcədə paylanmış kanal matrisləri üçün simulyasiya edilmiş nəticələr göstərir. Ölçmələr Lund universiteti şəhərciyi ərazisində açıq havada aparıldı. Mərkəz tezliyi 2.6 GHz və 50 MHz ölçmə bantı idi. Silindrik silsilədən istifadə edərkən RUSK Lund kanal qurucusu işə yarandı, sintetik xətti sıra ölçmələri üçün bir şəbəkə analizatoru istifadə edildi.

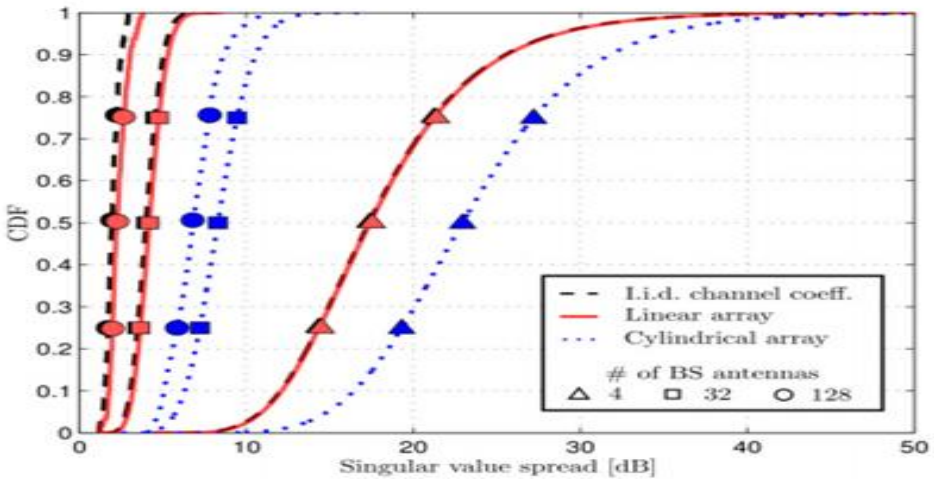
Şəkil 3.5. Ölçmələr üçün istifadə olunan kütləvi MIMO antenna serialları.

4 elementli serial üçün tək dəyər yayılmasının medianı müvafiq olaraq 23 dB və 18 dB təşkil edir. Bu nömrə, bütün istifadəçilərə ağlabatan qəbul edilən siqnal gücü ilə xidmət etmək üçün istifadə edilməli olan əlavə gücün azalması səviyyəsidir. Kütləvi xətti sıra ilə yayılma 3 dB-dən azdır. Bundan əlavə, qıvrımların heç birində əhəmiyyətli bir quyruq olmadığını unutmayın. Bu o deməkdir ki, ölçülən bant genişliyindən artıq hər hansı bir yerdə 3 dB-dən çox yayılmış tək bir dəyərin görünmə ehtimalı olduqca azdır.

Baza stansiyasında müxtəlif sayda anten elementlərinin təsirini və anten konfiqurasiyasını daha da aydınlaşdırmaq üçün 4 yaxın məsafəli istifadəçi üçün (təxminən 40 m məsafədə hər istifadəçi arasında 2 metrdən az) nisbət nisbətini çəkirik. baza stansiyasından) MRT-ni əvvəlcədən kodlaşdırma kimi istifadə edərkən görünməyən bir xətt ssenarisində.

Ötürücü gücü normallaşdırılır ki, orta hesabla terminallarda müdaxilənin sərbəst səs-küyə nisbəti 10 dB-dir.

Şəkil 3.6-dan göründüyü kimi, baza stansisyasında antenlərin sayı artdıqca, nisbət dərəcəsi nəzəri müdaxiləsiz davaya yaxınlaşır. Qırmızı (xətti sıra üçün) və mavi (dairəvi massiv üçün) rəngli rəngli sahələr, fərqli genişzolaqlı tezlik reallaşdırmaları üçün məbləğ nisbətlərinin 90 faizlik etibarlılığını göstərir. Əvvəlki kimi, miqdar nisbətinin dəyişməsi antenaların sayı artdıqca azalır, ancaq ölçülmüş kanallar üçün yavaş-yavaş dəyişir.

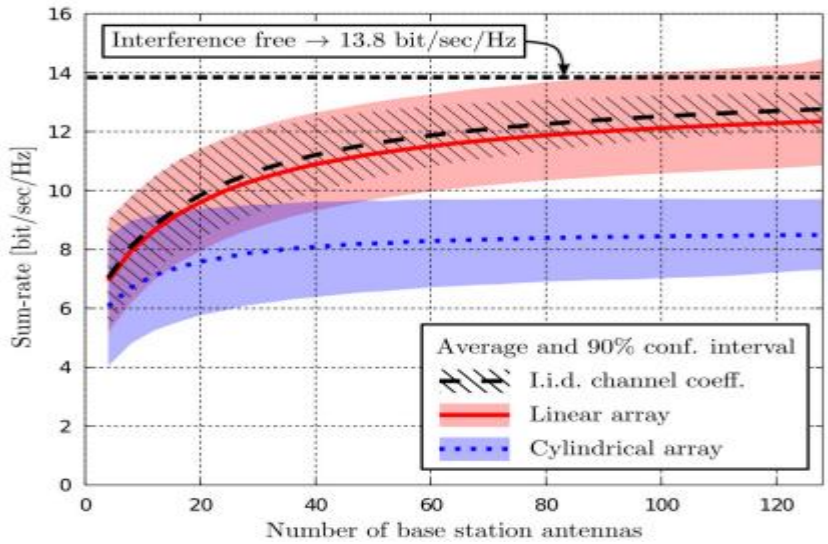


Şəkil 3.6. MIMO sistemləri üçün 4 terminal və üç fərqli sayda BS antenaları olan yayılmış tək dəyərin CDF: 4, 32 və 128. Nəzəri i.i.d. kanal bir istinad olaraq göstərilir, digər iki hal isə BS-

də xətti və silindrik massiv quruluşa malik kanallardır. Qeyd: Xətti sıra üçün ayrilik 4 BS üçün kanal.

Yavaş eniş, ən azı qismən, seriallarda baş verən kölgənin solması ilə əlaqələndirilə bilər. Dizi boyunca xarici cisimlər tərəfindən kölgə şəklində olan xətti massiv üçün və yanlış istiqamətə yönəldilmiş yönləndirici antenna elementlərindən yaranan kölgə kimi silindrik massiv üçün fiziki cəhətdən böyük bir sıra performans nəzəri antenaların sayı böyüyür. Yığcam dairəvi massiv, kiçik diyaframı sayəsində xətti sıra ilə müqayisədə daha aşağı performansa malikdir - dağınıqları, həm də fiziki cəhətdən böyük bir sıra yerləri həll edə bilmir - və bəzən səhv istiqamətə işarə edən yönləndirici anten elementləri var. Səpələnmişlərin əksəriyyətinin eyni üfüqi bucaqda göründüyünə görə, müxtəlif yüksəkliklərdə səpələnmələri həll etmək imkanı bu ssenaridə cəmi nisbətinə cüzi töhfələr verir.

Burada qeyd etmək lazımdır ki, biraz daha mürəkkəb, lakin yenə də xətti, minimum sıfır məcburetmə və ya minimum orta kvadrat səhv, i.i.d-ə yaxınlaşma kimi kodlaşdırma metodlarından istifadə edərkən. Kanal işləməsi daha sürətli olur və baza stansiyası antenlərinin sayı artdıqca məbləğ nisbətinin dəyişməsi daha azdır.



Şəkil 3.7. MRT kodlaşdırmadan istifadə edərək, dörd tək antenli terminal və 4 ilə 128 arasında əsas stansiya antenaları ilə əldə edilmiş downlink

Diqqətə çatdırmaq lazım olan digər bir cəhət, gözə görünən şəraitdə yaxın məsafədə yerləşdirilmiş istifadəçilər kimi çox çətin bir yayılma ssenarisi üçün də

böyük serialın istifadəçilərin fərqli məkan imzalarından istifadə edərək ağlabatan dərəcədə ayıra biləcəyi görünür. İstifadəçilər genişlənmiş məkan həlli səbəbiylə baza stansiyasına sahibdirlər. Bu adi MIMO ilə mümkün olmazdı. Bu nəticələr başqa açıq ölçmə kampaniyasının təsvir olunduğu və təhlil edildiyi müşahidələrə uyğundur.

Ümumiyyətlə, kütləvi MIMO-nun əsasını təşkil edən əlverişli yayılma ilə bağlı fərziyyələrin praktikada əhəmiyyətli dərəcədə etibarlı olduğuna dair sübutlar mövcuddur. Geniş serialın dəqiq konfiqurasiyasından və ideal performansa yaxınlaşmadan istifadə olunan əvvəlcədən kodlaşdırma alqoritmlərindən asılı olaraq antenlərin sayı artdıqca daha sürətli və ya yavaş ola bilər. Bununla birlikdə, istifadəçi sayından təxminən 10 qat daha çox baza stansiyası antenalarına sahib olduqda, nəzəri cəhətdən ideal performansdan da sabit bir nəticə əldə etmək mümkündür ki, normal olaraq çox çətin yayılma şərtləri hesab olunur.

NƏTİCƏ VƏ TƏKLİFLƏR

Təqdim olunmuş dissertasiya işində kompüter şəbəkələrinin iki növü - naqilli şəbəkə texnologiyaları və simsiz şəbəkə texnologiyaları tədqiq edilmiş və aşağıdakı nəticələr alınmışdır:

1. XX əsrin ortalarından ARPANET-dən başlayaraq istifadə olunan naqilli şəbəkə texnologiyalarına alternativ meydana gəlmiş daha müasir texnologiyaların - simsiz şəbəkə texnologiyalarının əsas xarakteristikaları tədqiq edilmişdir.
2. Məlumdur ki, kompüter şəbəkələrinin qurulması müəyyən topologiyaya əsaslanır. Tədqiqat işində kompüter şəbəkələrinin qurulmasında istifadə olunan şin, halqavari, ulduz, ağacvari və qarışıq (Mesh) topologiyalara uyğun texnologiyaların optimallığı tədqiq edilmişdir.
3. Kompüter şəbəkələrinin qurulma həcminə görə təsnifatını əsas götürərək bu texnologiyaların səmərəliliyi, onların həyatımızın müxtəlif sahələrinə təsiri, ümumi inkişaf istiqamətləri və gələcək perspektivləri araşdırılmışdır.
4. Daha sonra ümumi LAN şəbəkələrinin səmərəliliyi, onların qurulmasına qoyulan texniki tələblər və simsiz texnologiyalar vasitəsilə LAN və WLAN şəbəkələrinin konfiqurasiyası ətraflı şəkildə öyrənilmişdir.
5. Simsiz lokal şəbəkənin planlaşdırılması və layihələndirilməsi, WLAN şəbəkələrinin konfiqurasiyasının və parametrlərinin onların quraşdırılma mühitindən, mövqeyindən asılı olaraq məxfiliyinin qorunması və onlara daxil olan WEP, WPA, WPA, 802.1x şifrələnməsinin tətbiqi məsələləri tədqiq olunmuş, buraya daxil olan RADİUS server texnologiyasının əhəmiyyəti izah edilmiş və simsiz şəbəkə texnologiyalarında yaranan problemlərin həlli yolları göstərilmişdir.
6. Əlavə olaraq AD HOC şəbəkəsi və ona daxil olan MIMO texnologiyasının da əsas perspektivləri və onu məhdudlşdıran amillər araşdırılmışdır.

Təklif:

ADHOC şəbəkəsi və ona daxil olan MIMO texnologiyasının araşdırılmasının nəticəsi olaraq UNEC-də Kampus şəbəkəsi qurula bilər. Burada əsasən WLAN şəbəkə texnologiyasının tədris binalarında tətbiqi, şəbəkənin müraciət nöqtələri ilə əlaqələndirilməsi və idarəetmə əlverişliliyinin təmini üçün 1 radius serverin qurulması və bunun vasitəsilə mac ünvana uyğun olaraq 1 istifadəçi adı, mac ünvanla şəbəkə arasında əlaqələnmənin təşkilidir. Bu da universitet nəzdində yerləşən tədris binalarının lokal şəbələləri arasında təhlükəsizliyin yüksək səviyyədə qorunmasını təmin edəcək.

İSTİFADƏ OLUNMUŞ ƏDƏBİYYATIN SİYAHISI

1. Blendin, Rucker, J. Leyman, N., Schygud, G., Hasher, D.: Position paper: software-defined network servicrd chaining. 2014
2. Steve Rackley - Wireless Networking Technology 2007
3. G. Pei, M. Gerla. Mobilti Management in Hierarchical Multihops Wireles Network. Internet Draaft.
4. Gaoc, F.Tufveson, Edfor, and F.Russek, Mesureds propagation characteristis for verylarge MIMO at 2,6 GHz 2012.
5. Casado, M., Fredman, M., Petit, J., Luo, J., Keown, N., Shener, S.: Ethane: taking control of the enterprise. SIGCOMM Comput. Commun. (2007)
6. G. Pei, M. Gerla, X. Hosng, C-C. Ciang. A Wireles Hierachical Routing Protocols with Groups Mobility. Internets Draft.
7. J. Hodic and S. Den Bring, Chanels measurements for large antena array, in IEEE International Simpossium on Wireles Communications System France, Aug. 2012.
8. Costanzo, S., Galucio, L., Morabito, G., Palazo, S.: Software defined wireless networks: unbridlings. 2012
9. C. Shepad, H. Yu, N. Anads, L. E. Li, T. L. Marzetta, R. Yang, and L. Zhon, Argos: Practicals many-antenna basic station, in ACM Int. Confi. Mobiles Comuting and Networking , Turkey Aug. 2012.
10. Dason-Hagerty, Tavakkoli, Culler Hydro a hybrid routing protocol for low-power and losy networks 2010
11. Q. Ngo, G. Larson and T. L. Martzeta, “Energy and spectal efficiency of very large multuser MIMO systems,” IEEE Trans. Commun 2013.
12. Dixit, Hao, F., Mukherje, S., Laksman, Towards an elastic distributed sdn controller. 2013
13. J. Nam, A. Adhikary, and G. Caire. Joint divison and mutiplexing: Realising masive MIMO gain with limits channel state informations. 2012.
14. Galuccio, Milardo, Morabito, G. Palazo, Sdn-wise: design, prototiping and experimentation of a stateful son solution for wireless sensor networks (2015)

15. Pitarokolis, S. Mohamed, and E. Larson, On the optimality of single-carier transmision in large-scale antenna systems, Wireless Commun. Lett. 2012.
16. C. Studer and E. G. Larson, "PAR-aware large-scale multi-user MIMO-OFDM downlink." 2013.
17. F. Katenberger, J. Hayong, M. Guilaud, and R. Knop, Relative channel reciprociti calibration in MIMO/TDD systems, 2010.
18. J. Hoydi, S. Brink, and M. Debbah, "Massive MIMO in the UL/DL of cellular networks." 2013.
19. R. Muller, M. Vehkapere, and L. Cotateluci, "Blind pilot decontamination." 2013.
20. H. Yin, D. Gesbert, M. Filippou, and Y. Liu, "A cordinated approach to channel estimation in large-scale multiple-antena systems." 2013.
21. Yeganeh, Gandali, Kando: A framework for efficient and scalable ofloading of control application.
22. Zabil İbayev-Kompüter Şəbəkləri 2008
23. http://mimoza.marmara.edu.tr/~mujdat.soyturk/papers_web/bilisim_01.PDF
24. https://www.ietf.org/standards/rfcs/
25. https://www.howtogeek.com/180649/htg-explains-whats-the-difference-between-ad-hoc-and-infrastructure-mode/
26. http://home.ustc.edu.cn/~wfsun/lab/course/wireless/Stevez20Rackley%20-%20Wireless%20Networking%20Technology.pdf?fbclid=IwAR2IB84Qnad40Ii09qgBz1ZxG-2nCcEAtEBRi3gCABK5hDF8M1foAn3Ay1U
27. https://www.fieldengineer.com/blogs/what-is-wireless-lan
28. https://www.cisco.com/c/m/en_za/solutions/wireless-lan.html
29. https://www.cisco.com/c/en_dz/solutions/index.html
30. http://www.technet.az/2013/05/05/simsiz-s%C9%99b%C9%99k%C9%99l%C9%99r/
31. https://www.springer.com/journal/11276
32. https://www.techopedia.com/definition/26186/wireless-network
33. https://heimdalsecurity.com/blog/home-wireless-network-security/

34. https://www.cybintsolutions.com/this-is-what-you-need-to-know-about-wireless-network-security/
35. https://www.kaspersky.com/resource-center/preemptive-safety/protecting-wireless-networks
36. https://www.cs.bham.ac.uk/~mdr/teaching/modules03/security/students/SS7/Wireless%20Networking%20Security.htm

РЕЗЮМЕ

В представленной диссертации были изучены два типа компьютерных сетей - технологии проводных сетей и технологии беспроводных сетей, и были получены следующие результаты:

1. Изучены основные характеристики более современных технологий - технологий беспроводных сетей, которые появились в качестве альтернативы технологиям проводных сетей, используемым с середины двадцатого века.

2. Известно, что построение компьютерных сетей основано на определенной топологии. В исследовании изучалась оптимальность технологий в соответствии с топологией шины, кольца, звезды, дерева и смешанной (Mesh) сетью, используемой при построении компьютерных сетей.

3. На основе классификации компьютерных сетей по объему построения изучалась эффективность этих технологий, их влияние на различные сферы нашей жизни, общие тенденции развития и перспективы на будущее.

4. Затем была подробно изучена эффективность общих сетей ЛВС, технические требования к их установке и настройке сетей ЛВС и WLAN с использованием беспроводных технологий.

5. Были изучены планирование и проектирование беспроводной локальной сети, защита конфиденциальности конфигурации и параметров сети WLAN в зависимости от среды их установки, местоположения и применения шифрования WEP, WPA, WPA, 802.1x, объяснена важность технологии RADIUS-сервера. и решения проблем с технологиями беспроводных сетей.

6. Кроме того, были изучены основные перспективы сети AD HOC и технологии MIMO, а также факторы, ограничивающие ее.

SUMMARY

In the presented dissertation two types of computer networks - technologies of wire networks and technologies of wireless networks were studied, and the following results were obtained:

1. The main characteristics of more modern technologies - technologies of wireless networks, which appeared as an alternative to the technology of wire networks, used since the middle of the twelfth century.

2. It is known that the construction of computer networks is based on a defined topology. The study studied the optimality of the technology in relation to the topology of the bus, ring, star, tree and mixed (Mesh) network used in the construction of computer networks.

3. On the basis of the classification of computer networks in terms of the volume of construction studied the effectiveness of these technologies, their impact on different areas of our lives, the general trends of development and prospects for the future.

4. Then the effectiveness of LAN networks, technical requirements for their installation and configuration of LAN and WLAN networks using wireless technologies was studied in detail.

5. Planned and designed a wireless local area network, protecting the confidentiality of the configuration and parameters of the WLAN network, depending on the environment in which they are installed, locations and applications of encryption WEP, WPA, W2A, WPA, 80, WPA, 80 and problem solving with wireless networking technologies.

6. Besides, the main perspectives of the AD HOC network and MIMO technologies have been studied, as well as the factors limiting it.