**Simsiz Sensor Şəbəkələri və Təhlükəsizliyi**

**Simsiz Sensor Şəbəkələri**

Simsiz sensor şəbəkələri kiçik sensor qurğularının paylanmış şəkildə yerləşdirildiyi sistemlərdir. Bu qurğular müxtəlif mühitlərdə məlumat toplamaq, emal etmək və bu məlumatları bir əsas mərkəzə (baza stansiyasına) ötürmək üçün geniş bir sensor düyünü şəbəkəsindən ibarət texnologiyalardır. SSŞ-dəki sensor düyünləri mühitdən fiziki parametrləri (məsələn, temperatur, rütubət, təzyiq) ölçərək bu məlumatları digər düyünlərə və baza stansiyasına ötürürlər.

**SSŞ-nin Yaranma Tarixi**

SSŞ-nin ilkin inkişafı 1970-ci illərə təsadüf edir. İlk dövrlərdə bu texnologiyalar əsasən hərbi məqsədlər üçün hazırlanmışdı, çünki uzaqdan müşahidə və nəzarət üçün çox əlverişli idi. Bu şəbəkələrin müasir dövrdə istifadəsi isə 1990-cı illərdə inkişaf etdi və mülki sahələrdə, xüsusilə elmi tədqiqatlar, ətraf mühitin monitorinqi və təhlükəsizlik tədbirləri kimi geniş tətbiqlərdə istifadə olunmağa başladı.

**SSŞ-nin Komponentləri**

Bir SSŞ-nin əsas komponentləri sensor düyünləridir. Hər bir sensor düyünü müxtəlif komponentlərdən ibarətdir:

* Sensorlar: Mühitin dəyişən parametrlərini ölçürlər (məsələn, temperatur, təzyiq).
* Mikrokontroller: Toplanmış məlumatları emal edir.
* Simsiz transceiver: Məlumatların ötürülməsi və alınması üçün istifadə olunur.
* Enerji mənbəyi: Adətən batareyalarla təmin olunur və sensor düyünlərinin enerji tükənməsi şəbəkənin ömrünü məhdudlaşdırır.
* Yaddaş Bloku: Məlumatların saxlanması və emal üçün istifadə olunan müvəqqəti və ya daimi yaddaş (RAM və ya Flash yaddaş).

**Simsiz sensor şəbəkələrində (SSŞ) istifadə olunan sensor qurğularına** aşağıdakı nümunələri göstərə bilərik:

* Temperatur Sensoru (məsələn, LM35): Temperaturu ölçmək üçün istifadə olunur. Bu sensor, müxtəlif mühitlərdə istilik səviyyəsini monitorinq etmək üçün geniş yayılmışdır.
* Rütubət Sensoru (məsələn, DHT11): Hava rütubətini ölçmək üçün istifadə olunur. Bu sensor kənd təsərrüfatında və ətraf mühit monitorinqində istifadə olunur.
* Təzyiq Sensoru (məsələn, BMP180): Atmosfer təzyiqini ölçmək üçün istifadə olunur. Bu sensor meteoroloji stansiyalarda tətbiq edilir.
* Hərəkət Sensoru (məsələn, PIR Sensoru): Hərəkəti aşkar etmək üçün istifadə olunur. Bu sensor, təhlükəsizlik sistemlərində və smart ev sistemlərində geniş yayılmışdır.
* Vibrasiya Sensoru (məsələn, SW-420): Vibrationu aşkar etmək üçün istifadə olunur. Bu sensor, struktur sağlamlığı monitorinqi üçün tətbiq edilir.

Bu sensor qurğuları müxtəlif mühitlərdə məlumat toplama və monitorinq funksiyalarını həyata keçirir.

**Praktiki Tətbiq Sahələri**

Simsiz sensor şəbəkələri müxtəlif sahələrdə geniş tətbiq olunur. Məsələn:

* Kənd Təsərrüfatında Sensorlar: Kənd təsərrüfatında suvarma sistemlərinin optimallaşdırılması üçün sensorlar istifadə olunur. Bu sensorlar torpağın nəm səviyyəsini izləyir və bu məlumatı analiz edərək suvarma sistemini avtomatik idarə edir. Məsələn, "AgriSense" adlı sistem, fermerlərin məhsuldarlığını artırmaq üçün nəm səviyyəsini ölçərək suvarma sistemlərini tənzimləyir.
* Ağıllı Şəhərlər: Ağıllı şəhərlərdə trafik axını idarə etmək üçün sensorlardan istifadə olunur. Məsələn, “SmartTraffic” sistemində sensorlar yol hərəkətini izləyir və real vaxtda məlumat toplayaraq yol siqnal sistemlərini avtomatik olaraq tənzimləyir. Bu, tıxacların azaldılmasına kömək edir.
* Səhiyyə Tətbiqləri: Sağlamlıq monitorinqi üçün simsiz sensor şəbəkələri, məsələn, “HealthMonitor” sistemində istifadə olunur. Bu sistem, xəstələrin vital əlamətlərini izləyir və həkimlərə məlumat göndərərək təcili müdaxilə etməyə imkan tanıyır.
* Sənaye Tətbiqləri: Sənaye mühitlərində sensorlar, məsələn, "SmartFactory" sistemində, avadanlıqların monitorinqi və təmir ehtiyaclarını proqnozlaşdırmaq üçün istifadə olunur. Bu sensorlar avadanlıqların performansını izləyərək, nasazlıqların əvvəlcədən aşkar olunmasına kömək edir.

**Simsiz Sensor Şəbəkəsi Topologiyaları**

Radio rabitə şəbəkələri üçün SSŞ-nin strukturu aşağıda göstərilən müxtəlif topologiyaları əhatə edir.

* Ulduz topologiyası hər bir düyünün birbaşa keçid qapısına (gateway) qoşulduğu bir rabitə topologiyasıdır. Tək bir keçid qapısı bir neçə uzaq düyünə mesaj göndərə və ya ala bilər. Ulduz topologiyalarında düyünlər bir-biri ilə mesaj göndərə bilməzlər. Bu, uzaq düyünlər və keçid qapısı (baza stansiyası) arasında az gecikməli rabitəyə imkan yaradır.Şəbəkənin idarə edilməsi bir düyündən asılı olduğu üçün, keçid qapısı bütün fərdi düyünlərin radio yayım sahəsi daxilində olmalıdır. Üstünlüklərdən biri uzaq düyünlərin enerji istehlakını minimum səviyyədə saxlamaq və sadə şəkildə idarə etməkdir. Şəbəkənin ölçüsü mərkəzə edilən əlaqələrin sayından asılıdır.
* Ağac topologiyası kaskadlı ulduz topologiyası olaraq da adlandırılır. Bu topologiyada hər bir düyün daha yüksəkdə yerləşdirilən düyünə və daha sonra keçid qapısına qoşulur. Ağac topologiyasının əsas üstünlüyü şəbəkənin genişləndirilməsinin asan olması və səhvlərin aşkar edilməsinin asanlaşmasıdır. Lakin bu şəbəkənin dezavantajı odur ki, əsas kabeldən çox asılıdır; əgər o qırılarsa, bütün şəbəkə çökə bilər.
* Mesh topologiyaları, məlumatların bir düyündən digərinə, radio rabitə sahəsində olan bir düyünə ötürülməsinə imkan verir. Əgər bir düyün digərinə mesaj göndərmək istəyirsə, lakin bu düyün radio rabitə sahəsindən kənardadırsa, o zaman istənilən düyünə mesajı ötürmək üçün aralıq bir düyün lazımdır. Mesh topologiyasının üstünlüyü şəbəkədəki nasazlıqların asanlıqla izolyasiya olunması və aşkarlanmasıdır. Dezavantajı isə şəbəkənin böyük olması və böyük sərmayə tələb etməsidir.

**SSŞ-də Təhlükəsizlik Məhdudiyyətlərinə Baxış**

Simsiz Sensor Şəbəkəsi (SSŞ) ənənəvi kompüter şəbəkəsi ilə müqayisədə bir çox məhdudiyyətlərə malik xüsusi bir şəbəkədir. Buna görə də mövcud təhlükəsizlik texnikalarından ideyalar alarkən effektiv təhlükəsizlik mexanizmləri yaratmaq üçün bu məhdudiyyətləri bilmək və anlamaq vacibdir.

• Yaddaş və enerji məhdudiyyətləri: Sensor kiçik ölçülü bir cihazdır və yalnız az miqdarda yaddaşa və təhlükəsizlik alqoritmləri üçün məhdud yaddaş sahəsinə malikdir. Effektiv təhlükəsizlik mexanizmi yaratmaq üçün təhlükəsizlik alqoritminin kod ölçüsünü məhdudlaşdırmaq vacibdir. Enerji, simsiz sensor şəbəkələrinin ən böyük məhdudiyyətidir. Sensor düyünləri şəbəkəyə yerləşdirildikdən sonra onların dəyişdirilməsi və ya yenidən enerji ilə təmin edilməsi yüksək əməliyyat xərcləri səbəbindən çətin olur.

• Etibarsız rabitə: Bu, sensor şəbəkələri üçün əsas təhlükələrdən biridir. Şəbəkənin təhlükəsizliyi çox vaxt rabitəyə bağlı olan protokollardan asılıdır. Əsas parametrlərə etibarsız ötürmə, gecikmə və münaqişələr daxildir.

• Təhlükəsizlik tələbləri:

* Autentifikasiya: Hər hansı bir qərar qəbul etmə prosesində məlumatları alan düyünlər məlumatın etibarlı mənbədən gəldiyinə əmin olmalıdır. Şəbəkədə idarəetmə məlumatlarının mübadiləsi zamanı autentifikasiya tələb olunur.
* Məlumatın bütövlüyü: Transitdə olan məlumatlar düşmənlər tərəfindən dəyişdirilə bilər. Zərərli bir düyünün mövcud olmadığı şəraitdə belə, məlumatın itməsi və ya zədələnməsi baş verə bilər.
* Məlumatın məxfiliyi: Müşahidə və sənaye sirrləri kimi tətbiqlər məxfiliyə əsaslanmalıdır. Məxfiliyin qorunması üçün standart üsul şifrələmədən istifadədir.
* Məlumatın yeniliyi: Məlumatın yeni olduğunu və köhnə mesajların təkrar ötürülmədiyini təmin edir. Bu tələb paylaşılan açarlarla işləyən şəbəkələrdə xüsusilə əhəmiyyətlidir.
* Özünü təşkil etmə: SSŞ-lər özünü təşkil etməli və çoxpilləli marşrutlamanı dəstəkləməlidir.

• Zaman sinxronizasiyası: Enerji qənaəti üçün hər bir sensor düyünü periodik olaraq sönə bilər. Təhlükəsizlik mexanizmi də zamanla sinxronlaşdırılmalıdır.

• Təhlükəsiz lokallaşma: Sensor şəbəkəsi çox vaxt dəqiq və avtomatik yer məlumatına ehtiyac duyur. Təhlükəsiz yer məlumatı olmayan sistemlərdə hücum edən saxta siqnallar verərək və ya siqnalları təkrarlayaraq məlumatları manipulyasiya edə bilər.

**SSŞ-də Təhlükəsizlik Təhdidləri və Hücumlar**

Hücumçular SSŞ-ni (simsiz sensor şəbəkələrini) qeyri-sabit hala gətirmək üçün müxtəlif təhlükəsizlik təhdidləri yarada bilərlər. Simsiz şəbəkələrdə ötürmə mühitinin yayılması təbiətinə görə təhlükəsizlik hücumlarına daha həssasdır.

**Təhlükəsizlik Təhdidləri**

Hücumçunun imkanlarına görə SSŞ-lərdə təhdidləri aşağıdakı kateqoriyalara bölmək olar:

* Xarici və daxili hücumlar: Xarici hücumlar, SSŞ-yə aid olmayan cihazlardan gəlir və şəbəkədəki kriptoqrafik məlumatlara çıxış imkanı yoxdur. Bu hücumlar məlumatların dinlənilməsi, saxta məlumatların daxil edilməsi və DoS hücumları ilə nəticələnə bilər. Daxili hücumlar isə, şəbəkənin etibarlı iştirakçıları tərəfindən həyata keçirilir, əməliyyatları pozmaq və resurslardan sui-istifadə etmək məqsədilə icazəsiz davranışları əhatə edir.
* Passiv və aktiv hücumlar: Passiv hücumlar şəbəkədə ötürülən paketlərin dinlənilməsi ilə, aktiv hücumlar isə məlumat axınında dəyişiklik edərək və ya saxta məlumatlar yaradaraq həyata keçirilir.
* Sensor sinifli və güclü cihazlarla edilən hücumlar: Sensor sinifli hücumlar, şəbəkəyə sensor cihazlara bənzər güclərə malik cihazlarla həyata keçirilir. Güclü cihazlarla edilən hücumlar isə daha yüksək hesablama gücü və enerji ehtiyatlarına malik cihazlar tərəfindən həyata keçirilir, bu da şəbəkəyə ciddi ziyan vurur.

**Təhlükəsizlik Hücumları**

Şəbəkələrə və kompüter sistemlərinə edilən hücumlar ümumiyyətlə aşağıdakı növlərə bölünür:

* İnterruptiya (dayandırma): Şəbəkənin əlçatanlığına edilən hücumdur. Məsələn, cihazların fiziki ələ keçirilməsi, mesajların korlanması və ya zərərli kodun daxil edilməsi ilə xidmətlərin dayandırılması (DoS) baş verə bilər.
* İntersepsiya (dinləmə): Bu, şəbəkənin konfidensiallığına edilən hücumdur. Hücumçu şəbəkəni sındıraraq sensor cihazlara və ya saxlanılan məlumatlara icazəsiz giriş əldə edə bilər.
* Modifikasiya (dəyişiklik): Bu hücum məlumatların bütövlüyünə zərbə vurur. Hücumçular məlumatları əldə etməklə onları dəyişdirə bilər. Məsələn, ötürülən məlumat paketlərini dəyişdirə və ya şəbəkəni saxta məlumatlarla dolduraraq xidmətin dayandırılmasına (DoS) səbəb ola bilər.
* Fabrikasiya (saxta məlumat daxil edilməsi): Hücumçular şəbəkəyə saxta məlumatlar daxil edərək onun etibarlılığını pozur. Bu hücum mesajların autentifikasiyasını təhlükə altına alır və nəticədə DoS hücumlarını asanlaşdırır.

Hücumlar həm də cihaz əsaslı və şəbəkə əsaslı olmaqla iki yerə bölünür:

* Cihaz əsaslı hücumlar: Bu hücumlar üç növə ayrılır: proqram təminatının pozulması, avadanlığın zədələnməsi və istifadəçinin aldadılması. Proqram təminatının pozulması sensor cihazlarında işləyən proqramdakı zəifliklərdən istifadə edərək həyata keçirilir (məsələn, "buffer overflow" kimi zəifliklər). Avadanlığın zədələnməsi isə sensor cihazlarındakı proqram kodları, məlumatlar və açarların ələ keçirilməsi ilə baş verir. İstifadəçinin aldadılması isə şəbəkə istifadəçilərindən vacib məlumatları əldə etmək üçün fırıldaq üsullarından istifadə edilməklə həyata keçirilir.
* Şəbəkə əsaslı hücumlar: Bu hücumlar məlumatların tranzit vaxtı oğurlanması və ya protokollara riayət edilməməsi yolu ilə baş verir. Hücumçu şəbəkədən qeyri-qanuni istifadəyə nail olaraq şəbəkə resurslarını ələ keçirir.

**Təbəqələrə əsaslanan hücumlar**

SSŞ üçün rabitə protokollarının standart təbəqələşdirilmiş quruluşu olmasa da, ISO-OSI modelinin təbəqələri üzrə ola biləcək hücumları və onların təhlükəsizlik həllərini göstərmək olar.

Ad-hoc(birbaşa əlaqəli şəbəkə) və sensor şəbəkələr üçün təklif olunan əksər yönləndirmə protokolları təhlükəsizlik məsələlərini həll etmək üçün nəzərdə tutulmayıb. Buna görə də, onlar hücumlara məruz qala bilər.

Fiziki səviyyədə olan iki əsas hücum sıxışdırma və fiziki müdaxilədir.

* Sıxışdırma: Bu, yüksək enerji siqnalı yayımlamaqla şəbəkənin fəaliyyətini pozmağa çalışan rəqibin etdiyi xidmətdən imtina (DoS) hücumudur. Bu hücuma qarşı müdafiə vasitəsi kimi yayılma spektr texnologiyalarından istifadə edilə bilər.
* Fiziki müdaxilə: Sensor şəbəkələri adətən açıq ərazilərdə fəaliyyət göstərir. Nəticədə, onların paylanmış və nəzarətsiz təbiətinə görə sensor düyünləri fiziki hücumlara qarşı çox həssasdır. Rəqib düyünü ələ keçirib, kriptoqrafik açarları oğurlaya, dövrələri dəyişdirə və ya proqram kodlarını modifikasiya edə bilər.

Link səviyyəsi hücumları:

* Davamlı Kanal Girişi (Exhaustion): Hücumçu bir düyün, kanal üzərində davamlı olaraq ötürmə edərək digər düyünlərin resurslarını tükəndirir. Bu cür hücumlardan müdafiə vasitəsi olaraq qəbul idarəetməsinə məhdudiyyət qoymaq mümkündür.
* Toqquşma: Eyni tezlikdə eyni anda iki düyün ötürmə edəndə toqquşma baş verir. Bunun nəticəsində alınan çərçivə səhv kimi tanınır və atılır. Hücumun qarşısını almaq üçün kiçik çərçivələrdən istifadə etmək mümkündür.
* DoS hücumları: Sensor şəbəkələri, məhdud enerji və resurslarına görə bu cür hücumlara çox həssasdır. Ən sadə DoS hücumu artıq lazımsız paketlər göndərərək, zərərçəkən düyünün resurslarını tükəndirir və qanuni istifadəçilərin şəbəkəyə çıxışını məhdudlaşdırır.

Şəbəkə səviyyəsi hücumları:

* Yönləndirmə məlumatlarının təhrif edilməsi və ya yenidən oynanılması: Bu, bir yönləndirmə protokoluna qarşı ən çox yayılmış hücumdur. Rəqib yönləndirmə məlumatlarını təhrif edərək döngələr yarada, trafiki öz tərəfinə çəkə və ya saxta məlumatlar yarada bilər.
* Sybil hücumu: Bu hücum zamanı bir düyün çoxsaylı saxta identifikasiyalar təqdim edir və digər düyünlər tərəfindən çox şəxsiyyətli kimi qəbul olunur. Bu, şəbəkə strukturu ilə bağlı məlumatların təhrif edilməsinə səbəb ola bilər.
* Wormhole hücumu: Şəbəkədə iki uzaq nöqtə arasında gizli və sürətli keçid yaradan hücumdur. Bu hücumun qarşısını təsdiq mexanizmləri və ya çoxqatlı yönləndirmə protokolları ilə almaq olar.

Nəqliyyat səviyyəsi hücumları:

* Flooding hücumu: Rəqib, şəbəkənin resurslarını tükəndirmək məqsədilə çoxlu bağlantı sorğuları göndərir. Buna qarşı həll yolları limitlər qoymaqla və ya resurs üçün tapşırıqlar verməklə mümkündür.
* De-synchronization hücumu: Mövcud əlaqəni pozmağa çalışan hücumdur. Hücumçu yanlış məlumatları ötürərək çərçivələrin yenidən göndərilməsini tələb edir.

**Təhlükəsizlik Protokolları**

Simsiz sensor şəbəkələrində (SSŞ) ən vacib təhlükəsizlik protokolları aşağıdakılardır:

1. Wi-Fi Protected Access (WPA/WPA2/WPA3): Bu protokollar simsiz şəbəkələrdə məlumatın şifrələnməsini təmin edərək, məlumatların müdaxilədən qorunmasını təmin edir. WPA3 ən son versiyadır və daha güclü şifrələmə mexanizmləri təklif edir, xüsusi ilə də şəbəkəyə hücumların qarşısını almaq üçün daha yüksək səviyyədə qorunma təmin edir.
2. Secure Socket Layer (SSL) və Transport Layer Security (TLS): Bu protokollar məlumatların ötürülməsi zamanı təhlükəsiz şifrələnmiş kanal yaradır. Onlar server və cihazlar arasında məlumat mübadiləsinin gizliliyini və bütövlüyünü təmin edərək, hücumların qarşısını almağa kömək edir.
3. Internet Protocol Security (IPsec): Bu protokol şəbəkələrarası əlaqələrdə məlumatların təhlükəsizliyini qorumaq üçün istifadə edilir. IPsec məlumatları şifrələyərək onların müdaxilədən qorunmasını təmin edir və məlumatların dəyişdirilməsinin qarşısını alır.
4. Lightweight Extensible Authentication Protocol (LEAP) və Protected Extensible Authentication Protocol (PEAP): LEAP və PEAP identifikasiya prosesində istifadə olunur və cihazların şəbəkəyə təhlükəsiz şəkildə qoşulmasını təmin edir.
5. Elliptic Curve Cryptography (ECC): Bu metod şifrələmə və imzalama üçün istifadə olunur və daha az hesablama gücü ilə yüksək təhlükəsizlik təmin edir, buna görə də SSŞ-də məhdud resurslara malik cihazlar üçün uyğundur.

**Açar İdarəetmə Protokolları**

Açar idarəetməsi SSŞ-lərdə təhlükəsizliyin təmin edilməsində əsas mexanizmlərdən biridir. Bu protokolun əsas məqsədi şəbəkədəki sensor düyünləri arasında açarların təhlükəsiz şəkildə yaradılmasını və bölüşdürülməsini təmin etməkdir. Açar idarəetmə protokolları mərkəzləşdirilmiş və ya paylanmış ola bilər. Mərkəzləşdirilmiş yanaşmada, açarların yaradılması, yenidən yaradılması və paylanmasını idarə edən vahid bir qurum mövcuddur, bu quruma Açar Paylanma Mərkəzi (KDC) deyilir.

Açar idarəetmə bir neçə mərhələdən ibarətdir:

1. Açar Yaradılması
2. Açar Saxlanması
3. Açar Paylanması
4. Açar İstifadəsi
5. Açar Ləğvi
6. Açarın Yenilənməsi

Bir çox SSŞ protokolu ehtimallara əsaslanaraq, sensor düyünləri arasında açar paylaşımını təmin edir. LEAP kimi protokollar, şəbəkə daxilində məlumatların emalı və təhlükəsiz rabitə üçün yaradılıb və fərdi düyünlər üçün müxtəlif açar növləri təmin edir.

**Məlumatların Təhlükəsiz Yığılması**

Simsiz sensor şəbəkələri (SSŞ) enerji və bant genişliyi baxımından məhduddur, buna görə sensor düyünləri ilə əsas stansiyalar arasındakı məlumat mübadiləsini azaltmaq enerji qənaətinə kömək edir. Yığılmış sensor şəbəkələri istifadə edərək, “toplayıcılar” adlanan ara düyünlər xam məlumatları yığır, emal edir və yalnız emal edilmiş nəticəni göndərir. Bu, ötürülən məlumatların miqdarını azaldır və şəbəkənin ömrünü uzadır. Lakin, aktiv hücumçu saxta nəticələr göndərə bilər. Məlumatların yayılması üçün istifadə olunan multicast və broadcast texnikaları isə müvafiq autentifikasiya və şifrələmə mexanizmləri ilə təmin edilməlidir.

**Təhlükəsiz Marşrutlama**

Təhlükəsiz marşrutlama protokolu SSŞ-də mesajların bütövlüyünü, autentifikasiyasını və mövcudluğunu təmin edir. Müxtəlif tətbiqlərdə təhlükəsiz marşrutlama vacibdir. Müəlliflər, hücumçuların şəbəkədə məqsədlərinə çatmasını əngəlləmək üçün təhlükəsiz marşrutlama protokollarının atributlarını müəyyən etmişlər. Bu atributlar marşrutlama protokollarının mümkün təhdidlərə qarşı müdafiəsini artırır. Hazırkı təkliflər əsasən statik SSŞ üçün uyğundur, lakin bəzi alqoritmlərin enerji istehlakı və təhlükəsizlik təsirlərini göstərmədiyi qeyd olunur.

**İcazəsiz Girişin Aşkarlanması (IDS)**

Simsiz sensor şəbəkələrində (SSŞ) İcazəsiz Girişin Aşkarlanması (Intrusion Detection Systems - IDS), şəbəkə daxilində baş verən zərərli və anormal fəaliyyətlərin qarşısını almaq üçün vacib bir texnologiyadır. Bu sistemlər SSŞ-lərdə baş verən anomaliyaları analiz edərək, zərərli hücumları vaxtında aşkar edir. İki əsas növ IDS mövcuddur:

1. Anomaliya aşkarlama sistemləri: Normal fəaliyyətləri modelləşdirərək onlardan kənara çıxan hər hansı fəaliyyəti anomaliya kimi qəbul edir. Bu metod xüsusilə SSŞ-lərdə effektivdir, çünki hücumların təbiəti müxtəlif ola bilər.
2. İmza əsaslı aşkarlama sistemləri: Məlum hücum imzalarını aşkarlayaraq həmin hücumların baş verdiyini bildirir. Lakin bu sistemlər yeni hücum növlərinə qarşı effektiv ola bilməz.

SSŞ-lərdə mərkəzləşdirilməmiş aşkarlama metodları daha çox tətbiq edilir. Mərkəzləşdirilmiş sistemlər şəbəkənin mərkəzi nöqtələrinə çox böyük yük gətirdiyindən enerji və yaddaş baxımından qeyri-effektiv olur. Wang və digərlərinin təklif etdiyi model, qonşu sensor düyünləri arasında əməkdaşlıq yolu ilə düyünlərin zərərli olub-olmadığını aşkarlayır. Bu mərkəzləşdirilməmiş metod resurslara qənaət baxımından üstünlük təşkil edir. . Lakin icazəsiz girişin aşkarlanması texnikalarını vahid aparat platformasına inteqrasiya etmək çətin və bahalıdır. Zhu və digərləri (IHOP) sxemi təklif etmişlər. İcazəsiz girişin aşkarlanması üçün müxtəlif texnikalar tətbiq edilmişdir və bu sahədə ən populyar sistemlər arasında müqayisə aparılmışdır.

**Simsiz sensor şəbəkələrinin (SSŞ) təhlükəsizliyi sahəsində bir çox problemlər mövcuddur ki, bu da gələcək araşdırmalar üçün imkanlar açır:**

1. Effektiv Kriptoqrafik Metodlar: Sensor düyünlərinin məhdud resurslarına uyğun yüngül və səmərəli kriptoqrafik metodların inkişafı. Simmetrik və asimmetrik metodların birləşdirilməsi üzərində tədqiqatlar davam etdirilməlidir.
2. Nəqliyyat Təbəqəsi Təhlükəsizliyi: SSŞ-lərdə daha çox link təbəqəsi təhlükəsizliyi təmin edilsə də, nəqliyyat təbəqəsi təhlükəsizliyi zəifdir. Daha effektiv təhlükəsizlik həllərinin tapılması vacibdir.
3. Açarların İdarə Edilməsi: Açarların paylanması və autentifikasiyası məsələləri, xüsusilə açıq açar şifrələməsi istifadə edildikdə, hələ də həllini gözləyir. Yenilikçi metodların tapılması təhlükəsizliyi artıracaq.
4. Resursların İdarə Edilməsi: Enerji və hesablama resurslarının məhdudluğu səbəbindən təhlükəsizlik protokollarının effektiv istifadəsi vacibdir. Daha enerji qənaətli və sürətli protokolların inkişafı mühüm araşdırma sahəsidir.

**Real Həyatda Simsiz Sensor Şəbəkələrinə Hücumlar**

Simsiz sensor şəbəkələrində (SSŞ) baş vermiş bəzi real həyatda qeydə alınan hücumlar ciddi təhlükəsizlik problemlərinə səbəb olmuşdur:

**2009 - İraq Müdafiə Sisteminin Komprometasiya Edilməsi**: ABŞ ordusunun "Predator" pilotsuz uçan aparatlarına hücum edərək, İraq döyüşçüləri "SkyGrabber" proqramı vasitəsilə video siqnallarını dinlədilər. Nəticədə, ABŞ ordusunun əməliyyatlarını izləmək üçün bu məlumatlardan istifadə olundu.

**2013 - Jeep Cherokee-nin Hak Edilməsi**: İki təhlükəsizlik mütəxəssisi, Jeep Cherokee avtomobilinin simsiz sensor şəbəkələrini hack edərək avtomobilin idarəsini ələ keçirdilər. Bu hücum, avtomobil istehsalçılarına təhlükəsizlik tədbirlərini gücləndirmək üçün ciddi siqnallar verdi.

**2016 - Mirai Botnet Hücumu**: SSŞ elementləri olan təhlükəsizlik kameraları və yönləndiricilərin komprometasiya edilməsi ilə başlayan bu hücum, botnet yaradaraq nəhəng DDoS hücumu həyata keçirdi və internetin geniş hissəsini iflic etdi. Bu, SSŞ-lərin kütləvi miqyasda zəifliklərinin istismar oluna biləcəyini göstərdi.

**Üstünlüklər:**

* **Aşağı qiymət**: Simsiz sensor şəbəkələri (SSŞ) kiçik, aşağı qiymətli sensorlardan ibarətdir ki, bu da onları çoxsaylı tətbiqlər üçün sərfəli bir həll edir və yerləşdirilməsini asanlaşdırır.
* **Simsiz rabitə**: SSŞ-lər simli əlaqəyə ehtiyacı aradan qaldırır, bu da həm bahalı, həm də quraşdırılması çətin ola bilər. Simsiz rabitə həmçinin şəbəkənin çevik yerləşdirilməsini və yenidən konfiqurasiya edilməsini təmin edir.
* **Enerji səmərəliliyi**: SSŞ-lər enerji istehlakını azaltmaq üçün aşağı güc istehlak edən qurğular və protokollardan istifadə edir, beləliklə tez-tez batareya dəyişdirməyə ehtiyac olmadan uzunmüddətli işləməyə imkan verir.
* **Miqyaslana bilənlik**: SSŞ-ləri asanlıqla genişləndirmək və ya kiçiltmək mümkündür. Yeni sensorlar əlavə edərək və ya mövcud olanları çıxararaq şəbəkəni müxtəlif tətbiqlər və mühitlər üçün uyğunlaşdırmaq olar.
* **Real-vaxt monitorinqi**: SSŞ-lər ətraf mühitdə baş verən fiziki hadisələri real-vaxt rejimində izləməyə imkan verir və qərar qəbul etmə və idarəetmə üçün vaxtında məlumat təmin edir.

**Mənfi cəhətlər:**

* **Məhdud diapazon**: SSŞ-lərdə simsiz rabitənin diapazonu məhduddur, bu da genişmiqyaslı tətbiqlər üçün və ya radio siqnallarını maneə törədən mühitlərdə çətinliklər yarada bilər.
* **Məhdud emal gücü**: SSŞ-lər aşağı gücə malik qurğulardan istifadə etdikləri üçün bu qurğuların emal gücü və yaddaşı məhdud ola bilər, kompleks hesablama aparmaq və ya qabaqcıl tətbiqləri dəstəkləmək çətin ola bilər.
* **Məlumat təhlükəsizliyi**: SSŞ-lər məlumatların məxfiliyini, tamlığını və əlçatanlığını poza biləcək casusluq, dəyişdirmə və xidmətdən imtina hücumları kimi təhlükələrə qarşı həssasdır.
* **Müdaxilə**: SSŞ-lərdə simsiz rabitə digər simsiz cihazlardan və ya radio siqnallarından müdaxilələrə məruz qala bilər ki, bu da məlumat ötürülməsinin keyfiyyətini azalda bilər.
* **Yerləşdirmə çətinlikləri**: SSŞ-lərin yerləşdirilməsi düzgün sensor yerləşdirmə, enerji idarəetməsi və şəbəkə konfiqurasiyası ehtiyacı səbəbindən çətin ola bilər ki, bu da xeyli vaxt və resurs tələb edə bilər.

**Simsiz Sensor Şəbəkələri (SSŞ) üçün Təhlükəsizlik Həlləri**

Simsiz sensor şəbəkələrində (SSŞ) təhlükəsizliyin təmin edilməsi çox vacibdir, çünki bu şəbəkələr açıq mühitlərdə fəaliyyət göstərir və müxtəlif təhdidlərə məruz qalırlar. Təhlükəsizliyi təmin etmək üçün əsas yanaşmalardan biri kriptoqrafiya üsullarından istifadə etməkdir. Kriptoqrafiya vasitəsilə məlumatlar şifrələnir, autentifikasiyası yoxlanılır və məlumatların təzə olduğu təmin edilir.

1.Kriptoqrafiya: SSŞ-lərdə təhlükəsizliyin təmin edilməsi üçün kriptoqrafik əməliyyatlar vacibdir. Buraya məlumatların şifrələnməsi və autentifikasiyası daxildir. Sensor düyünlərinin məhdud resursları olduğundan, asimmetrik kriptoqrafiya üsulları çox vaxt çətin olur. Buna görə də, simmetrik kriptoqrafiya kimi daha səmərəli və resurs baxımından daha qənaətcil metodlar tətbiq olunur.

Simmetrik Kriptoqrafiya: Bu üsul, hər iki tərəfin eyni açardan istifadə etdiyi şifrələmə prosesidir və çox effektivdir. SPSN (Security Protocols for Sensor Networks) kimi protokollar bu məqsədlə təklif olunmuşdur. SPSN iki əsas təhlükəsizlik modulu ilə işləyir:

* SNEP (Sensor Network Encryption Protocol): Bu modul məlumatların məxfiliyini, iki tərəfli autentifikasiyanı və məlumatların təzəliyini təmin edir.
* μTESLA: Az resurs tələb edən mühitlər üçün autentifikasiya olunmuş yayımı təmin edir.

Açıq Açar Kriptoqrafiyası: Açıq açar kriptoqrafiyası (Public Key Cryptography) əvvəlcə SSŞ üçün praktik hesab olunmurdu, lakin son tədqiqatlar göstərir ki, bu üsul da SSŞ-də tətbiq oluna bilər. Buna baxmayaraq, açarların autentifikasiyası və nəqliyyat təbəqəsi təhlükəsizliyi kimi problemlər qalmaqdadır.

2.Təhlükəsizlik İnkişafı: Simsiz sensor şəbəkələrində məlumatların təhlükəsizliyini artırmaq üçün müasir şifrələmə standartları, məsələn, AES (Advanced Encryption Standard), tətbiq edilməlidir.

3.Avtorizasiya: Sensor düyünlərinin şəbəkəyə qoşulması zamanı güclü avtorizasiya mexanizmləri (məsələn, iki faktorlu identifikasiya) istifadə olunmalıdır.

4.Firewall: Hər bir düyündə lokal firewall tətbiqi, qeyri-qanuni trafikin bloklanmasına kömək edir.

5.Şəbəkə Monitorinqi: Məlumat axınını daimi izləməklə anomaliyalara vaxtında müdaxilə edilə bilər.

6. İstifadəçi Maarifləndirməsi: İstifadəçilərin sensor şəbəkələrinin təhlükəsizliyi barədə məlumatlandırılması vacibdir. Gələcək tədqiqatlar, istifadəçi təhsili proqramlarının hazırlanmasına yönəlməlidir ki, bu da məlumatların sızma riskini azaldacaq.