SIMSIZ TARMOQ XAVFSIZLIGIGA TAHDILAR VA ULAR YECHIMLAR

Po'latov Doston Normurod o'g'li
Roziqov Abdug'ani Ilhomjon o'g'li
Jumaboyev Javlonbek Sherqul o'g'li
Shonazarov Sarvarbek Maqsud o'g'li

ANNOTATSIYA

Simsiz xavfsizlik - bu simsiz tarmoqlardan foydalanadigan kompyuterlarga noqonuniy kirish yoki buzilishning oldini olish. Texnologiyaning uzluksiz rivojlanishi bilan simsiz ulanish imkoniyati ofis va jamoat muhitida tobora kengayib bormoqda, chunki u katta afzalliklarga ega.Simsiz tarmoqni himoya qilish so'nggi yigirma yil ichida ma'lumotlarga noqonuniy kirishni oldini olish uchun xavfsizlik usulini qo'llash kerak bo'lgan oldindan yechim topmagan tadqiqot bo'ldi.Ushbu tahdidlardan xalos bo'lish uchun birinchi navbatda bu tahdidlarni tushunish kerak, keyin esa ularni hal qilish yo'llarini topish kerak. Ushbu maqolada asosiy xavfsizlik tahdidlari muhokama qilinadi va simsiz tarmoq xavfsizligini ta'minlash uchun ularning echimlari tavsiflanadi.

Kalit so'zlar:-Simsiz tarmoq, simsiz tahdidlar tarmoq xavfsizligi, WAP2, WEP, xakerlar, xavfsizlik devori,simsiz xavfsizlik

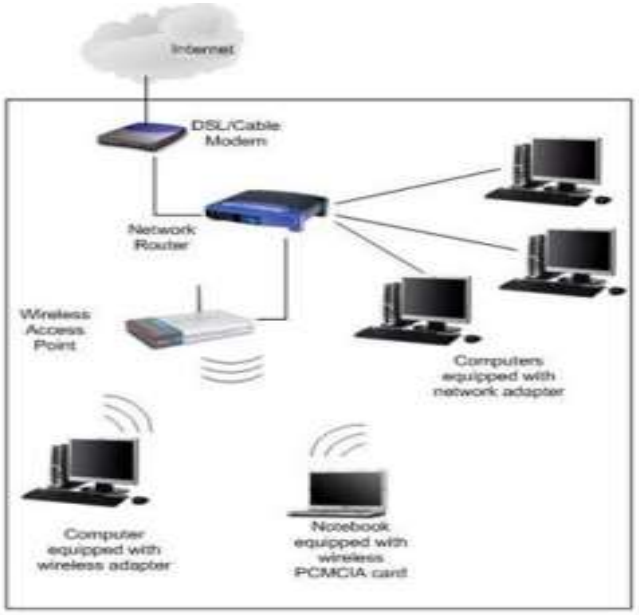
ABSTRACT

Wireless security is the prevention of unauthorized access or tampering with computers using wireless networks. With the continuous development of technology, the possibility of wireless connection is becoming more and more widespread in office and public environment, because it has great advantages. Wireless network protection has been a pre-emptive solution to prevent illegal access to data in the past two decades. In order to get rid of these threats, it is necessary to first understand these threats and then find ways to solve them. This article discusses the main security threats and describes their solutions to ensure wireless network security.

Keywords: - Wireless network, wireless threats network security, WAP2, WEP, hackers, firewall, wireless security

KIRISH

Simsiz tarmoq - radio yordamida o'rnatilgan tarmoq kompyuterlar o'rtasida muloqot qilish uchun signal chastotasi va boshqa tarmoq qurilmalari, ba'zan u Wi-Fi deb ataladi. tarmoq yoki WLAN va u tufayli bugungi kunda mashhur bo'lib bormoqda oson o'rnatish xususiyati va kabelni talab qilmaydi. Simsiz Internetga kirish texnologiyasi ikkalasida ham asta-sekin yo'lga qo'yilmoqda ofis va jamoat joylari, shuningdek, Internet orqali uyda foydalanuvchilar.



1-rasmda simli tarmoq ham, simsiz tarmoq ham noutbuklar/kompyuterlar yoki marshrutizatordan har qanday mobil qurilmalar o'rtasida ma'lumot almashish uchun ma'lumotlarni oladi, simsiz tarmoq uchun simsiz ulanish nuqtasi noutbuklar uchun ma'lumotlarga kirishni ta'minlaydi, simli tarmoq uchun router ma'lumotlarga kirishni ta'minlaydi. noutbuklar / kompyuterlar. Ikkalasi ham (simli tarmoq va simsiz tarmoq) tizim yaxlitligini buzmasdan qat'iy maxfiylikni talab qiladi, shu bilan birga vakolatli foydalanuvchilar uchun ma'lumotlarga va tegishli tizimlarga kirishni davom ettiradi.

Turli xil topologiyalar, texnikalar va protokollar to'plamlariga ega simsiz tarmoqlarning keng tarqalganligi va keng qo'llanilishi xavfsizlik mexanizmlarini takomillashtirish zaruratini keltirib chiqardi

Simsiz xavfsizlik - bu simsiz tarmoqlardan foydalangan holda kompyuterlarga ruxsatsiz kirish yoki shikastlanishning oldini olish. Simsiz xavfsizlikning eng keng tarqalgan turlari simli ekvivalent maxfiylik (WEP) va Wi-Fi himoyalangan kirish (WPA) [3]. Bu simli tarmoq xavfsizligidan boshqacha fikrlashni talab qiladi, chunki u xakerlar yoki tajovuzkorlarga transport vositalariga oson kirish imkonini beradi va bu kirish har qanday xavfsizlik arxitekturasi bilan kurashishi kerak bo'lgan tahdidni oshiradi.

Simsiz tarmoq xavfsizligi bilan ishlashda haqiqiylik, yaxlitlik, maxfiylik va rad etmaslik juda muhim jihatlardir, chunki har qanday samarali simsiz tarmoq xavfsizligi quyidagilarga ishonch hosil qilishi kerak [4]:

Mavjudlik: istalgan tarmoq xizmatlari hujumlarga qaramay, istalgan vaqtda mavjud bo'lishini kafolatlaydi. Mavjudlikni ta'minlaydigan tizimlar xizmat ko'rsatishni rad etish va energiya ochligi hujumlariga qarshi kurashishga intiladi.

Haqiqiylik: bir tugundan boshqasiga aloqaning haqiqiyligini kafolatlaydi. Bu zararli tugun ishonchli tarmoq tugunini maskarad qila olmasligini ta'minlaydi.

Maxfiylik: maxsus tarmoqlar uchun xavfsizlikning asosiy elementi bo'lib, u berilgan xabarni istalgan qabul qiluvchi(lar)dan boshqa hech kim tushuna olmasligini

kafolatlaydi.

Butunlik: bir tugundan boshqasiga yuborilgan ma'lumotlarning haqiqiyligini bildiradi. Ya'ni, u A tugunidan B tuguniga yuborilgan xabarni uzatish paytida C zararli tugun tomonidan o'zgartirilmaganligini kafolatlaydi.

Rad etmaslik: xabar kelib chiqishi qonuniy ekanligini kafolatlaydi. ya'ni, bir tugun boshqasidan noto'g'ri xabar olganida, rad etmaslik birinchisini noto'g'ri xabarni yuborishda ayblash imkonini beradi va boshqa barcha tugunlarga bu haqda bilish imkonini beradi.

FOYDALANISH VA ADABIYOT SO‘ROQ

a) TARMOQ XAVFSIZLIGI MUAMMOLARI, HUJUMLAR VA TAHDILAR

Simsiz tarmoqga ko‘ra, tarmoqdagi tahdidlar 2000-yillar atrofida simsiz uskunalar narxi pasayguniga qadar jamoatchilikka ma’lum bo‘lmagan, bu sanaga qadar armiya, ayniqsa sovuq urush davrida simsiz xavfsizlik mahsulotlarining birinchi raqamli mijozi bo‘lgan, ammo hozirgi kunlarda. Har bir inson, kompaniya va hatto harbiylar tarmoq xavfsizligini juda yaxshi biladi.

[3] ga ko'ra, Xizmatni rad etish (DoS) hujumi turli xil xavfsizlik xavflari orasida eng jiddiy xavfsizlik tahdididir, chunki DoS keng polosali simsiz tarmoqning mavjudligi va yaxlitligini buzishi mumkin.

[4], axborot texnologiyalari o'zgarishi sharoitida bugungi kunda simsiz tarmoqda qabul qilingan eng yangi texnologiya hisoblash haqida muhokama qilindi, ammo xavfsizlik va maxfiylik uning zamonaviy texnologik axborotda keng qo'llanilishiga asosiy to'siqlar sifatida qabul qilinadi.

[5], simsiz ad-hoc tarmoqlarda tajovuzni aniqlashni ta'minlash muammolarini ko'rib chiqdilar, ular ad-hoc marshrutlash infratuzilmasiga qarshi hujumlarni aniqlash bo'yicha joriy harakatlarni, shuningdek, mobil tugunlarga qarshi qaratilgan hujumlarni aniqlashni ko'rib chiqdilar, shuningdek, hujumlarni aniqlashni ko'rib chiqdilar. turli xil simsiz reklama uchun ishlatilishi mumkin bo'lgan arxitekturalar

hoc tarmoq infratuzilmalari, shuningdek, hujumga javob berishning tavsiya etilgan usullari.

Internetga ulanishni taklif qilish uchun simsiz tarmoqli tarmoqlardan (WMN) foydalanish simsiz Internet-provayderlar uchun mashhur tanlovga aylandi, chunki bu tarmoqni tez, oson va arzon joylashtirish imkonini beradi, ammo [6, 7] WMN-larda xavfsizlik hali ham o'z darajasida ekanligini aniqladi. go'daklik, chunki tadqiqot hamjamiyati tomonidan bu mavzuga juda kam e'tibor berilgan.

[8], mavjud Internet protokollari va xavfsizlik arxitekturalarining qo'llanilishi va cheklovlari bilan narsalar Interneti kontekstida joylashtirish modeli va zarur bo'lgan umumiy xavfsizlik, so'ngra IP-ga asoslangan xavfsizlik echimlari va talablari haqida

umumiy ma'lumot berish orqali chiqdi. standart IP xavfsizlik protokollarining o'ziga xos texnik cheklovlarini ta'kidladi.

"Sarlavhali maqolalarida*Mobil IPv6 da marshrutni optimallashtirish uchun xavfsiz va engil yondashuv, [9],*foydalanuvchilar xavfsizligiga bevosita ta'sir ko'rsatadigan mobillikni qo'llab-quvvatlashda xavfsizlik zaifligini aniqladilar, chunki bu qurilmalar va foydalanuvchilar o'rtasidagi farqni yashiradi va ular mobillikni qo'llab-quvvatlashdagi zararli va autentifikatsiya qilinmagan xabar tajovuzkorlar uchun xavfsizlik teshigini ochishi mumkinligini aniqladilar. tajovuzkor tomonidan tanlangan joyga davom etayotgan seansni o'g'irlaydigan hujumni boshlash uchun oson vositani taqdim etish, shuning uchun ular shubhali xabarni autentifikatsiya qilish orqali seansni o'g'irlash hujumini qanday oldini olish bo'yicha yechim topadilar.

Qog'ozda "*Simsiz datchiklar tarmog‘idagi xavfsizlik tahdidlarining tahlili” [10] tomonidan,*simsiz sensor tarmoqlarida xavfsizlik bilan bog'liq muammolarni o'rganib chiqdi, chunki simsiz aloqa texnologiyasi sensorli tugunlarning qarovsiz o'rnatilishi tufayli turli xil xavfsizlik tahdidlarini keltirib chiqaradi, chunki sensor tarmoqlari nozik ma'lumotlar bilan o'zaro ta'sir qilishi va/yoki qarovsiz muhitda ishlashi mumkin.

[11], “Internet of Things” (IoT) ni uch qatlamli istiqbol sifatida tushuntirdi: idrok qilish qatlami, transport qatlami va dastur qatlami, ular har bir qatlamning xavfsizlik muammolarini alohida tahlil qildilar va yangi muammolar va echimlarni topishga harakat qildilar, shuningdek, o'zaro faoliyatni tahlil qildilar. qatlamli heterojen integratsiya masalalari va xavfsizlik masalalari batafsil ko'rib chiqildi va umuman IoT xavfsizligi masalalarini muhokama qildi va ularga yechim topishga harakat qildi.

[12] tomonidan muhokama qilinganidek, ma'lumotlar hayotining barcha bosqichlarida bulutli hisoblash bilan bog'liq ma'lumotlar xavfsizligi va maxfiylikni himoya qilish muammolarining ba'zi joriy echimlari.

Xavfsizlik masalalari bulutli hisoblash va avtomobil tarmoqlarida katta e'tiborga olingan bo'lsa ham, [13] avtomobil bulutlariga (VC) xos bo'lgan xavfsizlik muammolarini aniqladi, masalan, yuqori harakatchanlikdagi transport vositalarini autentifikatsiya qilish, masshtablilik va yagona interfeys, chigal identifikatorlar va boshqalar. joylashuvlar va uzluksiz qisqa masofali aloqalar tufayli bir nechta o'yinchilar o'rtasida ishonch munosabatlarini o'rnatishning murakkabligi va nihoyat ular muhokama qilingan bir nechta muammolarni hal qiladigan xavfsizlik sxemasini taqdim etdi.

sarlavhali maqola*VANET xavfsizlik muammolari va mumkin bo'lgan kriptografik echimlar bo'yicha so'rov*[14] tomonidan VANET-larning aloqa arxitekturasini taqdim etdi va bunday tarmoqlar xavfsizligini amalda qo'llash uchun engib o'tish kerak bo'lgan maxfiylik va xavfsizlik muammolarini belgilab berdi, so'ngra ular VANET-dagi barcha mavjud xavfsizlik muammolarini aniqladilar va ularni kriptografik nuqtai nazardan tasnifladilar. [15].

O'zlarining ilmiy maqolalarida [16], oddiy va oqlangan tarzda kuchli davriy o'zaro autentifikatsiya, kuchli kalit kelishuvi va rad etmaslik xizmatini taqdim etish orqali tarmoqqa kirishda 3G protokollarining xavfsizligini yaxshilagan.

[17], shaxsiy ma’lumotlarni o‘g‘irlash, xalqaro kredit kartalaridagi firibgarlik, aloqa firibgarligi va korporativ firibgarlik kabi xavfsizlik muammolari simsiz texnologiyalarning o‘sishiga va simli texnologiya mavqeini egallashiga to‘sqinlik qiluvchi asosiy to‘siqlardan biri ekanligini aniqladilar, shuning uchun ular xavfsizlikning zaif tomonlarini o‘rganishdi. 802.11b simsiz LAN va uning asosiy zaifliklari uchun yechimlarni taqdim etdi.

[18] ga ko'ra, qurt teshigi hujumi simsiz tarmoqlarda, xususan, ko'plab maxsus tarmoq marshrutlash protokollari va joylashuvga asoslangan simsiz xavfsizlik tizimlariga nisbatan, hozirgi maxsus tarmoq marshrutlash protokollariga misol qilib, himoya qilishning ba'zi usullarisiz jiddiy tahdiddir. qurt teshigi hujumiga qarshi, ular topa olmaydilar

marshrutlar bir yoki ikkita hopdan uzunroq va shu tariqa aloqani jiddiy ravishda buzadi.

[19] ga ko'ra, maxfiylik va yaxlitlikni yo'qotish va xizmat ko'rsatishni rad etish tahdidi (DoS) hujumlari odatda simsiz aloqa bilan bog'liq xavflardir, chunki ruxsatsiz foydalanuvchilar agentlik tizimlari va ma'lumotlariga kirishlari, agentlik ma'lumotlarini buzishi, iste'mol qilishi mumkin. tarmoq o‘tkazuvchanligi, tarmoq unumdorligini pasaytirish va avtorizatsiya qilingan foydalanuvchilarning tarmoqqa kirishiga to‘sqinlik qiluvchi hujumlarni boshlash yoki boshqa tarmoqlarga hujumlarni boshlash uchun agentlik resurslaridan foydalanish.

[20] ga ko'ra, tadqiqotchilar xavfsiz aloqani ta'minlash uchun zarur bo'lgan mobil maxsus tarmoqlar bilan bog'liq marshrutlash va xavfsizlik masalalariga e'tibor qaratdilar. Hujumlarning o'zaro ta'sirining tabiati asosida MANETga qarshi hujumlar faol va passiv hujumlarga bo'lingan. Tarmoqqa qarshi tajovuzkorlarni ikki guruhga bo'lish mumkin: ichki va tashqi. Autsayder tajovuzkor tarmoqning qonuniy foydalanuvchisi bo'lmasa, ichki tajovuzkor vakolatli tugun va MANET-lardagi marshrutlash mexanizmining bir qismidir.

[21], taqdim etdi*shoshilinch hujum*, qarshi ishlatilganda xizmat ko'rsatishni rad etishga olib keladigan yangi hujum*hammasi*oldingi talab bo'yicha ad-hoc tarmoq marshrutlash protokollari. Masalan, DSR, AODV va ularga asoslangan Ariadne, ARAN va SAODV kabi xavfsiz protokollar ushbu hujumga duchor bo'lganda ikki hopdan uzunroq marshrutlarni aniqlay olmaydilar, hujum ham zarar keltiradi, chunki uni nisbatan zaif hujumchi. Ular nima uchun oldingi protokollar ushbu hujum ostida muvaffaqiyatsizlikka uchraganini tahlil qilishdi va keyin ishlab chiqishdi*Shoshilinch hujumning oldini olish (RAP)*, talab bo'yicha protokollar uchun shoshilinch hujumga qarshi umumiy himoya. RAP sodir bo'ladi*xarajat yo'q*asosiy protokol ish marshrutini

topa olmasa va u hatto eng kuchli shoshilinch hujumchilarga qarshi ishonchli xavfsizlik xususiyatlarini ta'minlamasa.

[22] ga ko‘ra, amaldagi simsiz texnologiyalar xakerlarga uzatilayotgan ma’lumotlarning yaxlitligini kuzatish va hattoki o‘zgartirish imkonini beradi, shuning uchun qat’iy xavfsizlik standartlarining yo‘qligi kompaniyalarning simsiz tarmoqlarini himoya qilish uchun millionlab mablag‘ sarflashiga sabab bo‘ldi, bu juda qimmat.

b) TARMOQ XAVFSIZLIGIDA OSI MODELI Tarmoqning yaxlitligini etarli darajada ta'minlash uchun ma'murlar turli protokollarni amalga oshirish uchun ramka standartlarini talab qiladi. TCP/IP-ni almashtirish va ushbu shartni qondirish uchun Ochiq tizim o'zaro bog'liqligi (OSI) modeli etti qatlamli tizimda apparat va dasturiy ta'minot o'rtasidagi ma'lumotlar almashinuvini tahlil qilish uchun tarmoq mos yozuvlar modeli sifatida joriy etildi.

Juda noyob vazifalarni bajarayotganda, har bir qatlam yuqoridagi qatlamni qo'llab-quvvatlash va mos ravishda ostidagi qatlamga xizmat ko'rsatish uchun tayinlangan.

[23] ga ko‘ra, OSI qatlamlari funksiyalariga qarab ikki guruh qatlamlariga bo‘linadi va bu qatlamlar 1-4 qatlamlar bo‘lib, ular qatlamning pastki qatlamlari hisoblanadi.

Protokol steklari va ma'lumotlarni uzatish va ko'chirish uchun mas'ul bo'lgan media qatlamlari va tizimning yuqori xost qatlamlari hisoblangan va dastur darajasidagi ma'lumotlar bilan bog'langan 5-7 qatlamlari.

1-jadval: Yetti qatlamli arxitektura va ularning funksiyalari [24].

	OSI Model : 7 Layers & Architecture			
	Assigned Layer Number	*Data units type*	*OSI model layer*	*Layer function*
Host Layers	7	Data	Application	• Applications interface • Interpreting program requests & info requirements
	6	Data	Presentation	• Data compression • Data representation • Encryption
	5	Data	Session	• Communications of interhost
Media Layers	4	Segments	Transport	• End-to-end connections • Properly sequence of packets
	3	Packets / datagram	Network	• Establish network connection • Translate network addresses • Transmitting individual packets across a network • Logical addressing: IP
	2	Bit / frames	Data link	• Physical addressing
	1	Bits	Physical	• Physical network connection signal management • Binary bit transmission • Media

Jismoniy qatlam zaifliklari o'z ichiga oladi:Quvvatni yo'qotish, atrof-muhit nazoratini yo'qotish, ma'lumotlar va apparat vositalarining jismoniy o'g'irlanishi, ma'lumotlar va apparat vositalarining jismoniy shikastlanishi yoki yo'q qilinishi, funktsional muhitga ruxsatsiz o'zgartirishlar (ma'lumotlar ulanishlari, olinadigan vositalar, resurslarni qo'shish/o'chirish), jismoniy ma'lumotlar havolalarini uzish, Ma'lumotlarni aniqlab bo'lmaydigan ushlab turish va tugmachalarni bosish va boshqa kirish jurnali.

Havola qatlamining zaifligi quyidagilarni o'z ichiga oladi:MAC manzilini buzish (stansiya boshqasining identifikatorini da'vo qiladi), VLANni chetlab o'tish (stansiya quyi tarmoqlar va xavfsizlik devorlari kabi mantiqiy boshqaruvni chetlab o'tib, boshqa stantsiyalar bilan to'g'ridan-to'g'ri aloqani majburlashi mumkin.), Spanning Tree xatolari tasodifiy yoki tasodifiy bo'lishi mumkin.

Maqsadli ravishda joriy qilingan, ikkinchi darajali muhit paketlarni cheksiz tsikllarda uzatishiga olib keladi, Simsiz media holatlarida, ikkinchi darajali protokollar ruxsatsiz shaxslar tomonidan tarmoqqa bepul ulanish imkonini beradi yoki zaif autentifikatsiya va shifrlash noto'g'ri xavfsizlik hissini keltirib chiqarishi mumkin, Kommutatorlar VLAN-ga ulangan har qanday qurilma tomonidan ma'lumotlarni ushlab turish imkonini beruvchi, tegishli portlarga tanlab yo'naltirish o'rniga, barcha VLAN portlariga trafikni to'ldirishga majbur.

Tarmoq qatlamining zaifliklari quyidagilarni o'z ichiga oladi:Marshrutni buzish - noto'g'ri tarmoq topologiyasini tarqatish, IP-manzilni zararli paketlarda noto'g'ri manba manzilini buzish, Identity & Resource ID zaifligi - Resurslar va tengdoshlarni aniqlash uchun manzilga tayanish mo'rt va zaif bo'lishi mumkin.

Transport qatlamining zaifliklari quyidagilarni o'z ichiga oladi:Noma'lum, noto'g'ri aniqlangan yoki "noqonuniy" shartlarni noto'g'ri ishlatish, transport protokolini amalga oshirishdagi farqlar "barmoq izlari" va xost ma'lumotlarini boshqa sanab o'tish imkonini beradi, port raqamlari kabi transport qatlami mexanizmlarining haddan tashqari yuklanishi trafikni samarali filtrlash va kvalifikatsiya qilish imkoniyatini cheklaydi, uzatish. mexanizmlar ishlangan paketlar va oqim va uzatish qiymatlarini bilimli taxmin qilish asosida aldash va hujumga duchor bo'lishi mumkin, bu esa aloqalarni boshqarishni buzish yoki tortib olishga imkon beradi.

Seans qatlamining zaifliklari quyidagilarni o'z ichiga oladi:Zaif yoki mavjud bo'lmagan autentifikatsiya mexanizmlari, foydalanuvchi identifikatori va parol kabi seans hisob ma'lumotlarini aniq o'tkazish, ushlab turish va ruxsatsiz foydalanishga ruxsat berish, Seans identifikatori soxtalashtirish va o'g'irlash mumkin, muvaffaqiyatsiz autentifikatsiya urinishlari asosida ma'lumotlarning chiqib ketishi, Cheksiz muvaffaqiyatsiz seanslarga ruxsat kirish ma'lumotlariga qo'pol kuch hujumlari.

Taqdimot qatlamining zaifliklari quyidagilarni o'z ichiga oladi:Kutilmagan

kiritilgan ma'lumotlarning noto'g'ri ishlashi dasturning ishdan chiqishiga yoki o'zboshimchalik bilan ko'rsatmalarni bajarish uchun boshqaruvning topshirilishiga olib kelishi mumkin, boshqaruv kontekstlarida tashqaridan kiritilgan ma'lumotlardan qasddan yoki noto'g'ri foydalanish masofadan manipulyatsiya yoki ma'lumotlarning chiqib ketishiga yo'l qo'yishi mumkin, maxfiylik himoyasini chetlab o'tish uchun kriptografik kamchiliklardan foydalanish mumkin.

Ilova qatlamining zaifliklari quyidagilarni o'z ichiga oladi:Ochiq dizayn muammolari dastur resurslaridan nomaqbul shaxslar tomonidan bepul foydalanish imkonini beradi, Backdoors va dastur dizaynidagi kamchiliklar standart xavfsizlik nazoratini chetlab o'tadi, Noadekvat xavfsizlik nazorati “hammasi yoki hech narsa” yondashuvini majburlaydi, bu esa haddan tashqari yoki yetarlicha kirishga olib keladi, Haddan tashqari murakkab ilovalar xavfsizligini boshqarish tendentsiyasi chetlab o'tish yoki noto'g'ri tushunish va amalga oshirish uchun dastur mantiqiy kamchiliklari tasodifiy yoki ataylab dasturlarni buzish yoki istalmagan xatti-harakatlarga olib kelishi mumkin.

Quyidagi rasmda OSI modelining turli qatlamlari uchun MANETS uchun xavfsizlik hujumlarining aniq tasnifi ko'rsatilgan

1-rasm: MANETS da turli qatlamlar uchun xavfsizlik hujumlarining tasnifi [27].

Ba'zi hujumlar kriptografiya bilan bog'liq bo'lmagan, boshqalari esa kriptografik ibtidoiy hujumlardir. Quyidagi 2-jadvalda kriptografik ibtidoiy hujumlar va misollar keltirilgan[28].

Jadval 2. Kriptografik ibtidoiy hujumlar

Kriptografik Primitiv hujumlar	**Misollar**
Pseudorandom raqamlar hujumi	Nonce, vaqt tamg'asi, ishga tushirish vektori (IV)
Raqamli imzo hujumi	RSA imzosi, ElGamal imzosi, raqamli imzo standarti (DSS)
Hash to'qnashuvi hujumi	SHA-0, MD4, MD5, HAVAL 128, RIPEMD

c) TARMOQ XAVFSIZLIGINI BA'ZI ECHIMLARI[29], yangi marshrutlash usulini taklif qildi: Security Aware ad hoc Routing (SAR) bu maxsus marshrutni aniqlash parametrlari sifatida xavfsizlik atributlarini o'z ichiga oladi, shuning uchun SAR reklama tomonidan ta'sirlanadigan marshrutlarning ahamiyatini yaxshilash uchun

xavfsizlikni muhokama qilinadigan o'lchov sifatida foydalanishga imkon beradi. hoc marshrutlash protokollari, keyin ular marshrutlash protokoli xavfsizlik ko'rsatkichlarining ikki darajali tasnifini ishlab chiqdilar va maxsus marshrutlash yo'llarida xavfsizlik atributlarini o'lchash va qo'llash uchun asosni taklif qildilar.

[30] ga ko'ra, marshrutni xizmat ko'rsatishni rad etish hujumlaridan himoya qilish uchun maxsus tarmoqlarda bir nechta marshrutlar o'rtasida o'ziga xos ortiqchalik afzalliklaridan foydalanish taklif qilingan.

tugunlar, ular shuningdek, yuqori darajada xavfsiz va qulay kalitlarni boshqarish xizmatini yaratish uchun replikatsiya va yangi kriptografik sxemalardan, masalan, chegara kriptografiyasidan foydalanganlar. [18], aniqlash va shu tariqa qurt teshigi hujumlaridan himoya qilish uchun paketli tasmalar deb ataladigan umumiy mexanizmni taqdim etdi va keyin tasmalarni amalga oshiradigan TIK deb nomlangan maxsus protokolni taqdim etdi.

[31] tomonidan taklif qilinganidek, VANETlarni himoya qilishning oddiy yechimi bu kompyuter tarmoqlaridagi an’anaviy tahdidlardan himoya qilish uchun allaqachon keng qo‘llanilgan kriptografik algoritmlar va yondashuvlardan foydalanishdir.

[28], kriptografiyani autentifikatsiya, maxfiylik, yaxlitlik va rad etmaslik kabi xavfsizlik xizmatlarini taklif qiluvchi imperativ va dominant xavfsizlik vositasi sifatida taklif qildi, ammo har qanday holatda ham ko'plab kriptografik ibtidoiylarga hujumlar mavjud bo'lsa

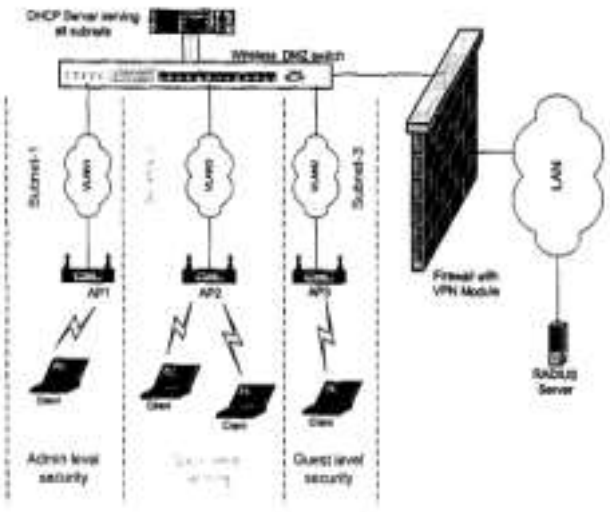
ham, ular hali oshkor etilmagan. Kriptografik primitivlar xavfsiz deb hisoblanadi, ammo so'nggi paytlarda ba'zi muammolar aniqlandi, masalan, xesh funktsiyasiga to'qnashuv hujumlari, masalan. SHA-1, Pseudorandom raqamli hujumlar, raqamli imzo hujumlari va xesh-to'qnashuv hujumlari, ularni himoya qilish juda qiyin.

"Sarlavhali maqolalarida*Simsiz tarmoqlar uchun xavfsiz agregatsiya*[32], buzg'unchilar qurilmalari va bitta qurilma kalit imtiyozlari uchun kuchli bo'lgan simsiz tarmoqlar uchun xavfsiz agregatsiya mexanizmini ta'minlovchi protokolni taqdim etdi, ularning protokoli hisoblash, xotira va quvvat iste'moli chegaralarida ishlash uchun mo'ljallangan edi.

xarajat sensori qurilmalari, lekin simsiz tarmoq xususiyatlaridan, shuningdek, qurilmalar va tayanch stantsiya o'rtasidagi quvvat nosimmetrikligidan foydalanadi.

[33] ga ko'ra, foydalanuvchi sirini ta'minlaydigan yangi va samarali simsiz autentifikatsiya protokoli taqdim etilgan bo'lib, u hash funksiyasi va smart-kartalarga asoslangan bo'lib, mobil foydalanuvchilar faqat simmetrik shifrlash va shifrni ochishni amalga oshiradilar, ularning protokolida bu xabar almashinuvining faqat bir bosqichini oladi. mobil foydalanuvchi va tashrif buyurilgan tarmoq o'rtasida va tashrif buyurilgan tarmoq va tegishli uy tarmog'i o'rtasida xabar almashishning bir bosqichi.

[34], simsiz mahalliy tarmoqlar xavfsizligida xavfsizlik devorlari yoki VPN shlyuzlaridan foydalanilganda, autentifikatsiya qilish uchun markazlashtirilgan serverga asoslangan yechimlardan foydalanish mumkinligi, masalan, masofaviy autentifikatsiya foydalanuvchi xizmati RADIUS serverida (RADIUS) foydalanish mumkinligi tavsifi bilan chiqdi. , ularning arxitekturasi (quyidagi 2-rasmda bo'lgani kabi) boshqalardan farq qiladi, chunki ular kirishni boshqarishda foydalanuvchi imtiyozlari bilan birga joylashuv ma'lumotlaridan foydalanadilar va ular IP quyi tarmoq ma'lumotlaridan mijozning joylashishini aniqlashni tanlashdilar, bu foydalanilgan boshqa tadqiqotlar bilan solishtirganda ancha sodda. Shunga o'xshash maqsad uchun GPS texnologiyasi.



2-rasm: RADIUS yordamida tavsiya etilgan xavfsizlik arxitekturasi [34]. [35], Wi-Fi himoyalangan kirish Wi-Fi tarmog‘i xavfsizligiga ma’lum bo‘lgan barcha sezgirliklarni tiklaydi va joriy va kelajakdagi Wi-Fi simsiz LANlarida ma’lumotlar xavfsizligi va kirish nazoratini sezilarli darajada yaxshilaydi, shuningdek, tezkor, kuchli, standartlarga asoslangan ulanishni ta’minlaydi, degan xulosaga keldi. , asl WEP-asosidagi xavfsizlikdagi barcha ma'lum xatolarni ko'rib chiqadigan birgalikda ishlaydigan xavfsizlik yechimi.

Ping Guo*Va*al [36], xizmatga yo'naltirilgan WMN'lar uchun engil va bardoshli autentifikatsiya yo'nalishi bo'yicha yangi dizayn prototipini taklif qildi, o'zgaruvchan chegara qiymatli autentifikatsiya (VTA) arxitekturasi bo'lib, unda VTA ning kirishga chidamliligi rag'batlantirilgan bir qator tugunlarni loyihalash uchun kafolatlangan. Tizim shaxsiy kalitining t va n chegara qiymatlarini o'zgarishsiz qoldirish mexanizmlari Tahlil va simulyatsiya natijalari shuni ko'rsatadiki, VTA nafaqat ushbu statik chegara qiymat sxemalarining kamchiliklarini bartaraf etishi mumkin, balki asosiy mexanizmlar bilan jihozlanmagan sxemalar bilan bog'liq tizim xarajatlarini oshiradi. WMNs.

3. XULOSA

Simsiz tarmoq unumdorlikni oshirish va xarajatlarni kamaytirish uchun ko'plab imkoniyatlarni taqdim etadi. Simsiz tarmoqdan kelib chiqadigan barcha tahdidlarni butunlay yo'q qilish qiyin bo'lsa-da, tahdidlarni tushunish va keyinchalik xavfni boshqarish uchun tizimli yondashuvni qo'llash orqali oqilona xavfsizlik darajasiga erishish mumkin. Ushbu maqolada simsiz aloqa bilan bog'liq tahdidlar va xavflar muhokama qilindi va xavflarni bartaraf etish va simsiz tarmoq xavfsizligini oshirish uchun ba'zi qadamlarni aniqlash uchun ishlatilishi mumkin bo'lgan keng tarqalgan echimlar ko'rib chiqildi.

Ma'lumotnomalar

W. A. Arbaugh,*Haqiqiy 802.11 xavfsizligi: Wi-Fi bilan himoyalangan kirish va 802.11 i*: Addison-Wesley Longman Publishing Co., Inc., 2003 yil.

[2] M. Bishop, "Kompyuter xavfsizligi nima?,"*IEEE Xavfsizlik va Maxfiylik*,jild. 99, b. 67-69, 2003 yil.

S. Xon, K.-K. Loo, T. Naeem va M. A. Khan, "Xizmat hujumlarini rad etish va keng polosali simsiz tarmoqlardagi muammolar"*8; 7*,2008 yil.

Gast, M. 802.11 Simsiz tarmoqlar: Simsiz tarmoqlarni yaratish va boshqarish bo'yicha aniq qo'llanma, O'Reilley Publishing, 2002 yil aprel.

Simsiz tarmoq xavfsizligi: zaifliklar, tahdidlar va qarshi choralar Xalqaro multimedia jurnali va ubiquitous muhandislik jild. 3, № 3, iyul, 2008 yil.

K. Ren, C. Vang va Q. Vang, "Ommaviy bulut uchun xavfsizlik muammolari",*IEEE Internet Computing*,jild. 16, b. 69-73, 2012 yil.

P. Brutch va C. Ko, "Simsiz ad-hoc tarmoqlar uchun tajovuzni aniqlashdagi qiyinchiliklar"*Ilovalar va Internet seminarlari, 2003. Ish materiallari. 2003 yildagi simpozium*, 2003 yil, 368-373-betlar.